

**DIPLOMADO DE PROFUNDIZACIÓN - CISCO
(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS)**

PRESENTADO POR:

**NECTARIO CANCEMANSE DAZA
*CÓDIGO: 1085688534***

TUTORA:

**NANCY AMPARO GUACA
*INGENIERA ELECTRÓNICA Y DE TELECOMUNICACIONES***

GRUPO 203092_19

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

MARZO 26 DE 2017

Contenido

RESUMEN.....	4
INTRODUCCIÓN	5
OBJETIVOS.....	6
Objetivo general.....	6
Objetivos específicos.....	6
7.3.2.4 Lab - Configuring Basic RIPv2 and RIPng.....	7
Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos.....	7
Parte 2: configurar y verificar el routing RIPv2	21
Parte 3: configurar IPv6 en los dispositivos.....	37
Parte 4: configurar y verificar el routing RIPng	46
8.2.4.5 LAB - CONFIGURING BASIC SINGLE-AREA OSPFV2.....	56
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	58
Parte 2: Configurar y verificar el enrutamiento OSPF	61
Parte 3: cambiar las asignaciones de ID del router.....	68
Part 2: configurar las interfaces pasivas de OSPF	72
Parte 4: cambiar las métricas de OSPF	78
8.3.3.6 LAB - CONFIGURING BASIC SINGLE-AREA OSPFV3.....	88
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	90
Parte 2: configurar el routing OSPFv3	93
Parte 3: configurar las interfaces pasivas de OSPFv3	104
10.1.2.4 LAB - CONFIGURING BASIC DHCPV4 ON A ROUTER.....	112
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	112
Parte 2: configurar un servidor de DHCPv4 y un agente de retransmisión DHCP	115
10.1.2.5 LAB - CONFIGURING BASIC DHCPV4 ON A SWITCH.....	120
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	122
Parte 2: cambiar la preferencia de SDM.....	124
Parte 3: configurar DHCPv4	126
Parte 4: configurar DHCPv4 para varias VLAN.....	130
Parte 5: habilitar el routing IP	132
10.2.3.5 LAB - CONFIGURING STATELESS AND STATEFUL DHCPV6.....	136
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	139
Parte 2: configurar la red para SLAAC	140
Parte 3: configurar la red para DHCPv6 sin estado.....	146

Parte 4: configurar la red para DHCPv6 con estado.....	154
10.3.1.1 IOE AND DHCP INSTRUCTIONS	166
11.2.2.6 LAB - CONFIGURING DYNAMIC AND STATIC NAT.....	169
Parte 1: armar la red y verificar la conectividad	170
Parte 2: configurar y verificar la NAT estática	175
Parte 3: configurar y verificar la NAT dinámica.....	179
11.2.3.7 LAB - CONFIGURING NAT POOL OVERLOAD AND PAT	185
Parte 1: armar la red y verificar la conectividad	186
Parte 2: configurar y verificar el conjunto de NAT con sobrecarga	188
Parte 3: configurar y verificar PAT.....	191
4.4.1.2 PACKET TRACER - CONFIGURE IP ACLS TO MITIGATE ATTACKS.....	193
Part 1: Verify Basic Network Connectivity.....	193
Part 2: Secure Access to Routers.....	196
Part 3: Create a Numbered IP ACL 120 on R1	200
9.2.1.10 - CONFIGURING STANDARDACLs.....	209
Part 1: Plan an ACL Implementation.....	210
Part 2: Configure, Apply, and Verify a Standard ACL.....	211
9.2.1.11-PACKET TRACER - CONFIGURING NAMED STANDARD ACLS.....	217
Part 1: Configure and Apply a Named Standard ACL.....	218
Part 2: Verify the ACL Implementation.....	219
9.2.3.3 PACKET TRACER - CONFIGURING AN ACL ON VTY LINES.....	222
Part 1: Configure and Apply an ACL to VTY Lines.....	223
Part 2: Verify the ACL Implementation.....	224
9.5.2.6 PACKET TRACER - CONFIGURING IPV6 ACLS.....	227
Part 1: Configure, Apply, and Verify an IPv6 ACL.....	227
Part 2: Configure, Apply, and Verify a Second IPv6 ACL.....	228
REFERENCIAS BIBLIOGRÁFICAS.....	238

RESUMEN

La presente actividad se basa en el montaje de diferentes escenarios de redes, permitiendo brindar conectividad a los diferentes dispositivos que se encuentran en un área de trabajo, compartiendo la conexión a Internet, distribución y envío de paquetes, documentos y archivos de una manera fácil y segura. Las redes son herramientas útiles para compartir recursos computacionales, usted puede acceder a una impresora desde diferentes computadores o archivos localizados en el disco duro de otro computador. Las redes son usadas también para jugar entre varios PCs, por lo tanto las redes no son solo para trabajo sino también para diversión. De esta manera vemos que la tecnología constituye un elemento importante en la configuración de las condiciones de vida y del trabajo

INTRODUCCIÓN

Daremos inicio a la construcción de nuestra topología seleccionando los dispositivos y el medio que los conectan (conectores). Varios tipos de dispositivos y conectores de red pueden ser usados. Para esta práctica lo haremos simple solo usando: Dispositivos terminales (End Devices), Router, (Switches), y conectores (Connections).

Estas prácticas tratan de dar un mejor entendimiento de la herramienta de simulación de redes diseñada por Cisco, y así poder establecer las funcionalidades básicas, generales y avanzadas. Packet Tracer permite diseñar redes de computadores, sin la necesidad de tener dispositivos de hardware o software adicionales a la máquina en la que está instalado. Lo anterior permite al usuario no necesitar tener dos computadores, routers, interfaces, cables, etc, para saber el comportamiento físico y real de una red, a la vez muchos paquetes de configuración de routers y switches utilizando

OBJETIVOS

Objetivo general

Realizar simulaciones en la herramienta o programa cisco packet tracer versión 7.1. Adquiriendo los conocimientos básicos para el manejo de la Herramienta CISCO PACKET TRACER.

Objetivos específicos

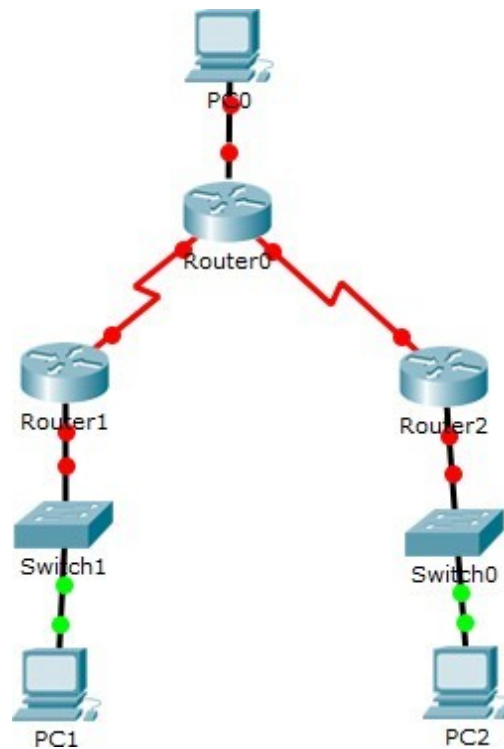
- Realizar configuraciones de dispositivos de red servidor WEB y DNS, computadores, switches, router.
- Crear topologías de red mediante la selección de los dispositivos, interconexión y su respectiva ubicación en un área de trabajo, utilizando la interfaz gráfica de packet tracer.
- configurar una contraseña a la línea de consola, vty, interfaz
- Aplicar todos los conceptos adquiridos de la unidad 2

DESARROLLO DE EJERCICIOS PRACTICOS

7.3.2.4 Lab - Configuring Basic RIPv2 and RIPvng

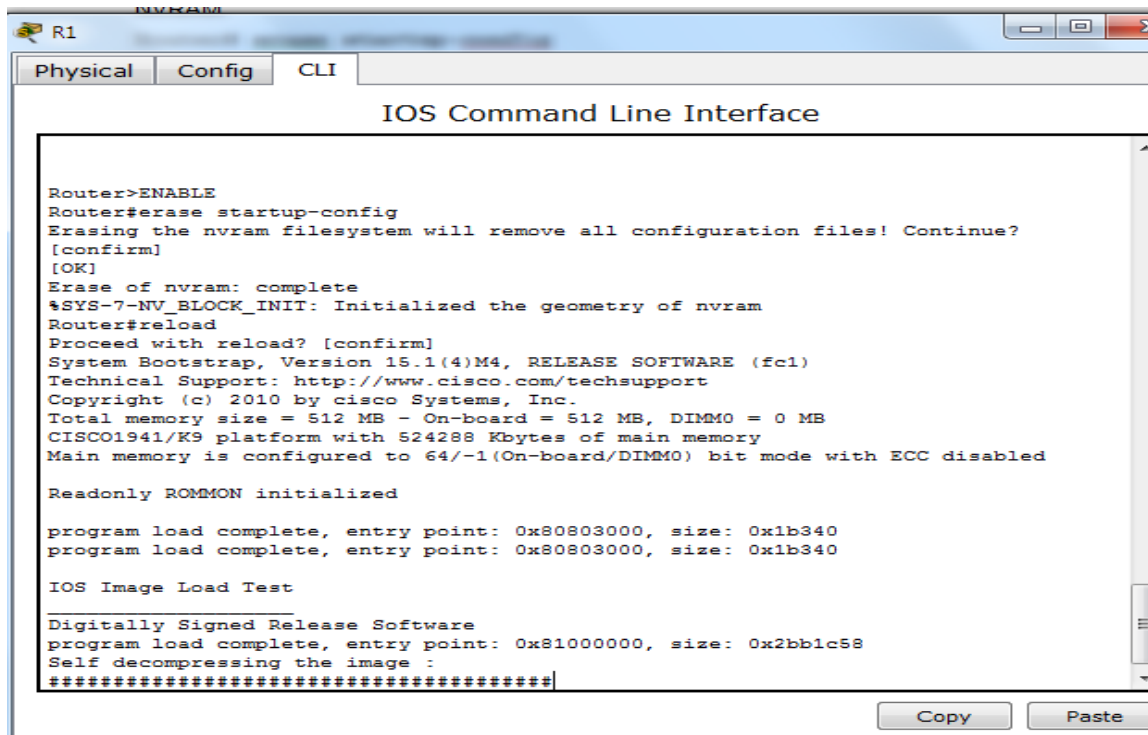
Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

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



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

Dispositivo S1



```
R1
Physical Config CLI
IOS Command Line Interface

Router>ENABLE
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, DIMMO = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMMO) bit mode with ECC disabled

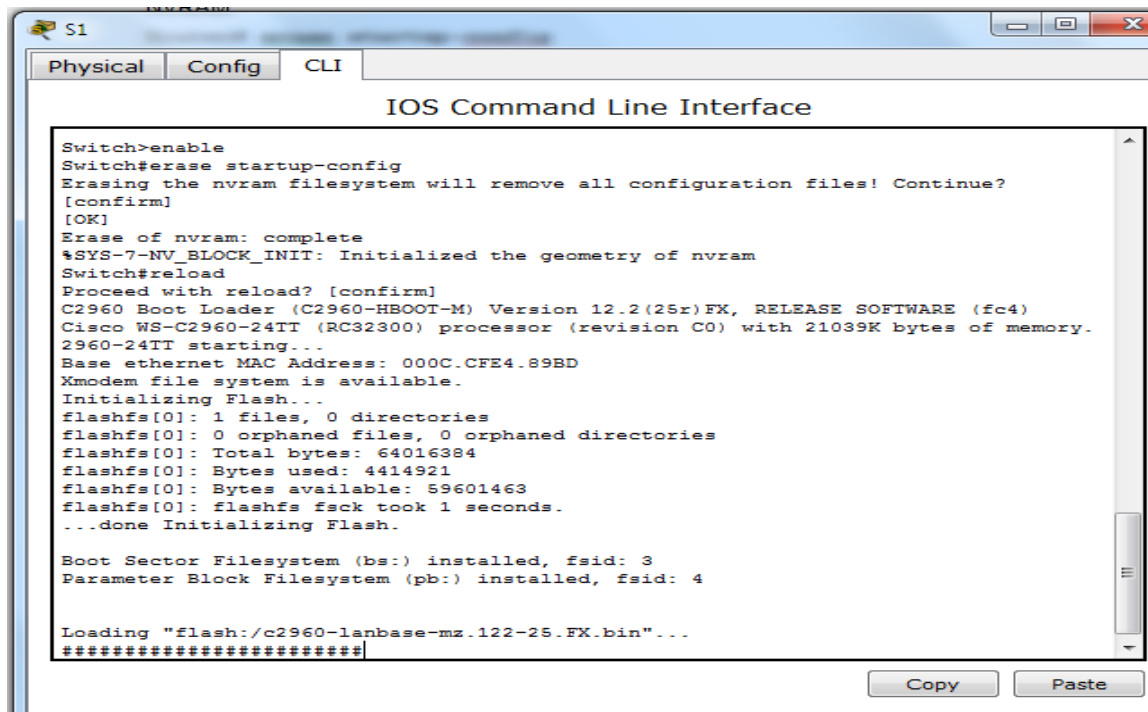
Readonly ROMMON initialized

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 :
*****
```

Dispositivo S2



```
S1
Physical Config CLI
IOS Command Line Interface

Switch>enable
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: 000C.CFE4.89BD
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"...
*****
```

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

a. Desactive la búsqueda del DNS

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#
```

Copy Paste

b. Configure los nombres de los dispositivos como se muestra en la topología.

```
R1#CONFIGURE TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#
```

Copy

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
```

Copy

```
Router>ENABLE
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#
```

Copy Paste

```
Switch(config)#hostname S1
S1(config)#

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#
```

c. Configurar la encriptación de contraseñas

```
R1(config)#service password-encryption
R1(config)#

R2(config)#service password-encryption

R3(config-if)#service password-encryption

S1(config)#service password-encryption
S1(config)#

S3(config)#service password-encryption
S3(config)#enable password class
```

d. Asigne class como la contraseña del modo EXEC privilegiado

```
R1(config)#enable password class
R1(config)#

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#service password-encryption
R2(config)#enable password class
R2(config)#

R3(config-if)#service password-encryption
R3(config)#enable password class

S1(config)#enable password class
S1(config)#

S3(config)#service password-encryption
S3(config)#enable password class
```

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

```
R1(config)#line console 0
R1(config-line)#password cisco
^
% Invalid input detected at '^' marker.

R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#exit
R2#
```

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#exit
R3#
```

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

```
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
```

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

```
R1(config)#banner motd "This is a secure system. Authorized Access Only!"
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2(config)#banner motd "This is a secure system. Authorized Access Only!"
R2(config)#
```

Copy F

```
R3(config)#banner motd "This is a secure system. Authorized Access Only!"
R3(config)#
```

Copy

```
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy

Paste

```
S3(config)#banner motd "This is a secure system. Authorized Access Only!"
S3(config)#
```

Copy

g. Configure logging synchronous para la línea de consola

```
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#
```

```
R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#line vty 0 4
R2(config-line)#
```

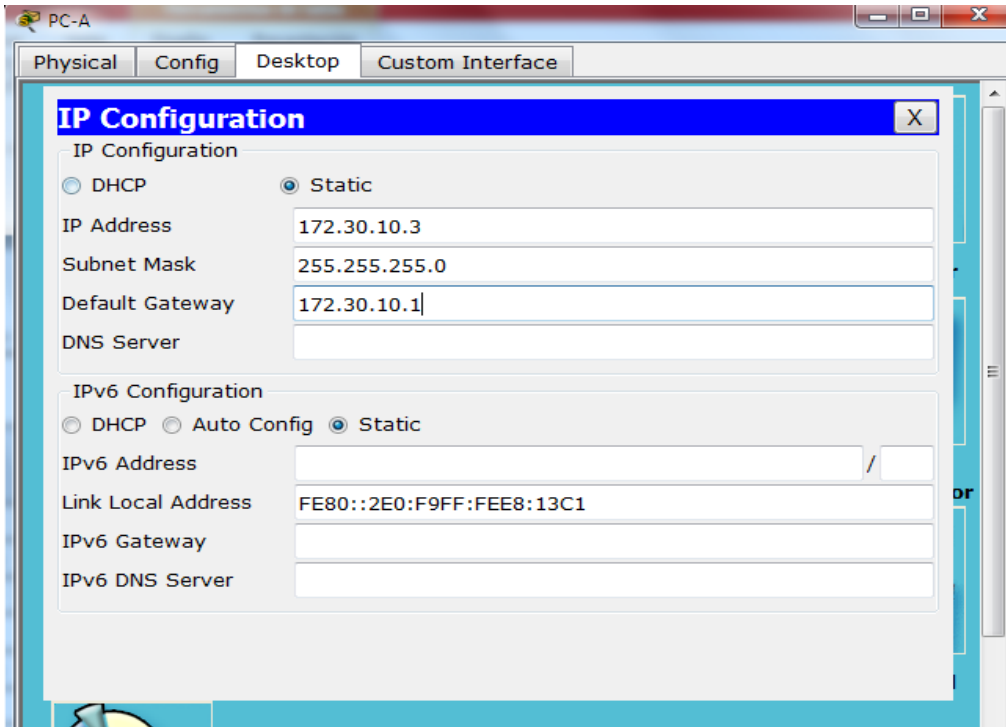
```
R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#line vty 0 4
R3(config-line)#exit
```

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#logging synchronous
S1(config-line)#line vty 0 4
S1(config-line)#
```

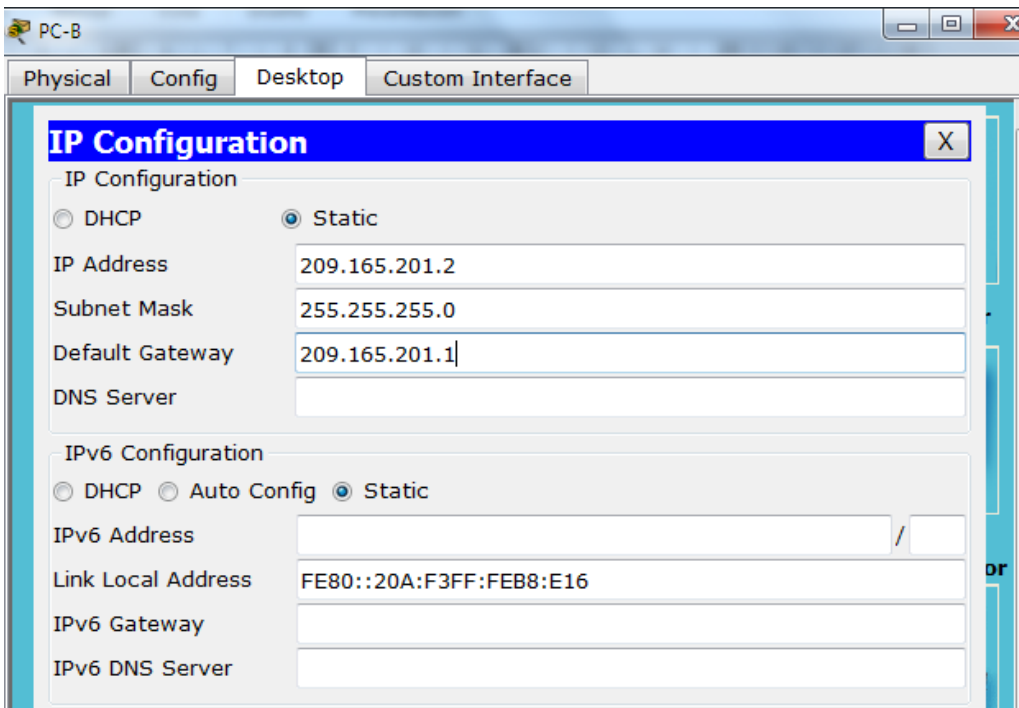
```
S3(config)#line console 0
S3(config-line)#logging synchronous
S3(config-line)#line vty 0 4
S3(config-line)#
```

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

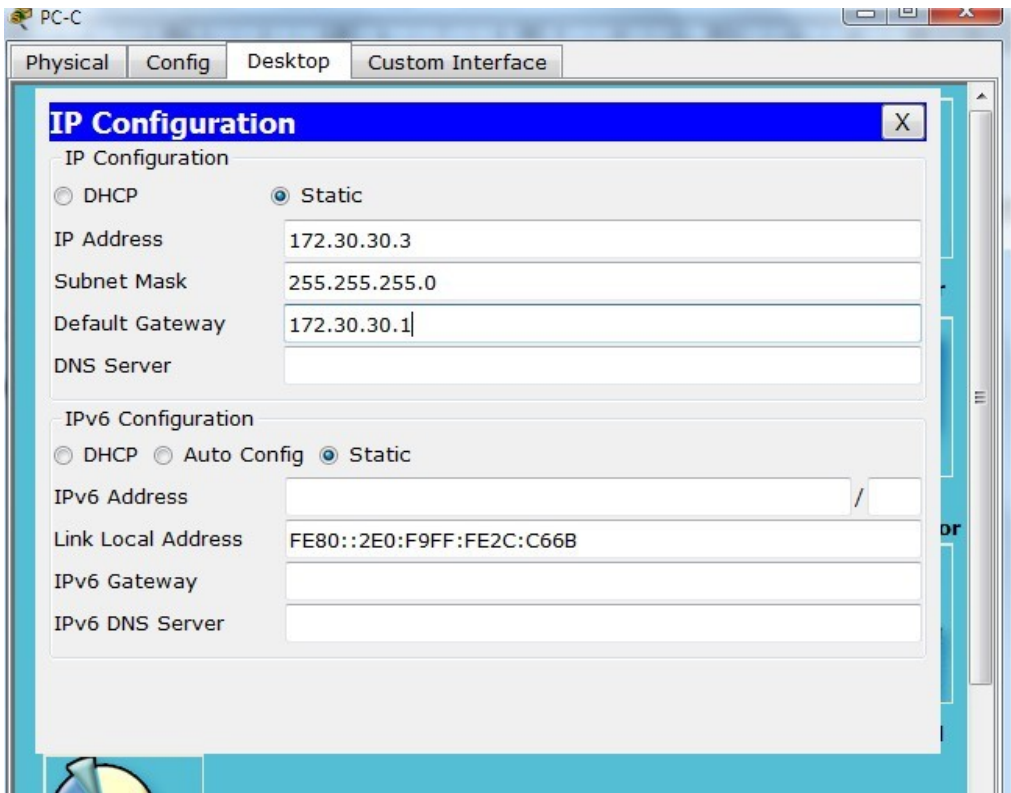
Dispositivo PC-A



Dispositivo PC-B



Dispositivo PC-C



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

Dispositivo R1

```
R1(config)#int g0/1
R1(config-if)#ip address 172.30.10.1 255.255.255.0
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,
to up

R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#exit
R1(config)#clock rate 128000
^
% Invalid input detected at '^' marker.

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

R1#
```

Dispositivo R2

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int g0/0
R2(config-if)#ip address 209.165.201.1 255.255.255.0
R2(config-if)#no shutdown

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

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

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

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

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

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

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#int s0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#
```

Dispositivo R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/1
R3(config-if)#ip address 172.30.30.1 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

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

Copy

Paste

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

```
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown
```

```
R2(config-if)#ip address 10.2.2.2 255.
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#
```

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

Copy

Paste

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

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

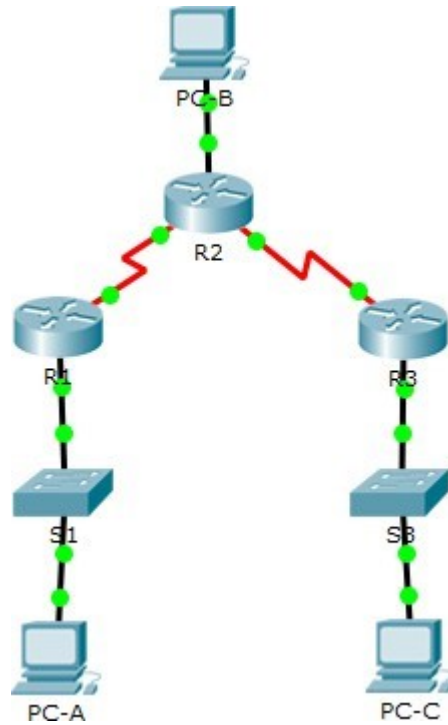
Copy

```
S1>enable
Password:
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Copy

Paste

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



Paso 4. configurar los equipos host.

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

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

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.

Dispositivo PC-A

```

Packet Tracer PC Command Line 1.0
PC>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

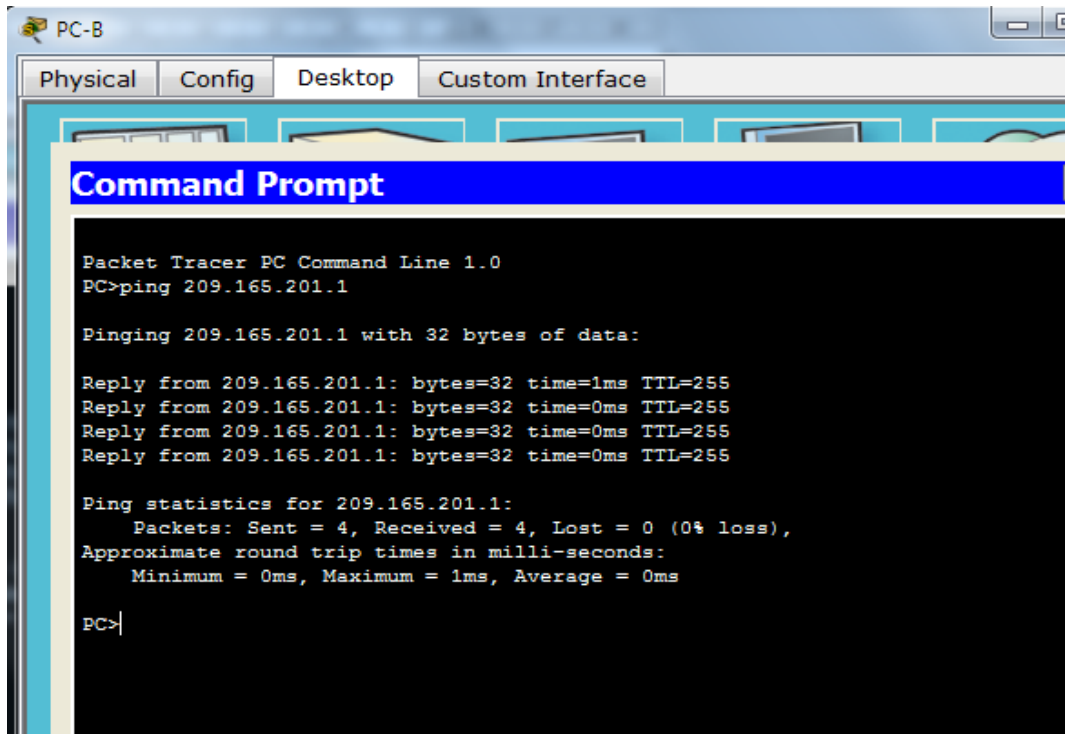
Reply from 172.30.10.1: bytes=32 time=34ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255
Reply from 172.30.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 34ms, Average = 8ms

PC>

```

Dispositivo PC-A



The screenshot shows a Packet Tracer window for PC-B. The window has tabs for Physical, Config, Desktop, and Custom Interface. A Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 209.165.201.1

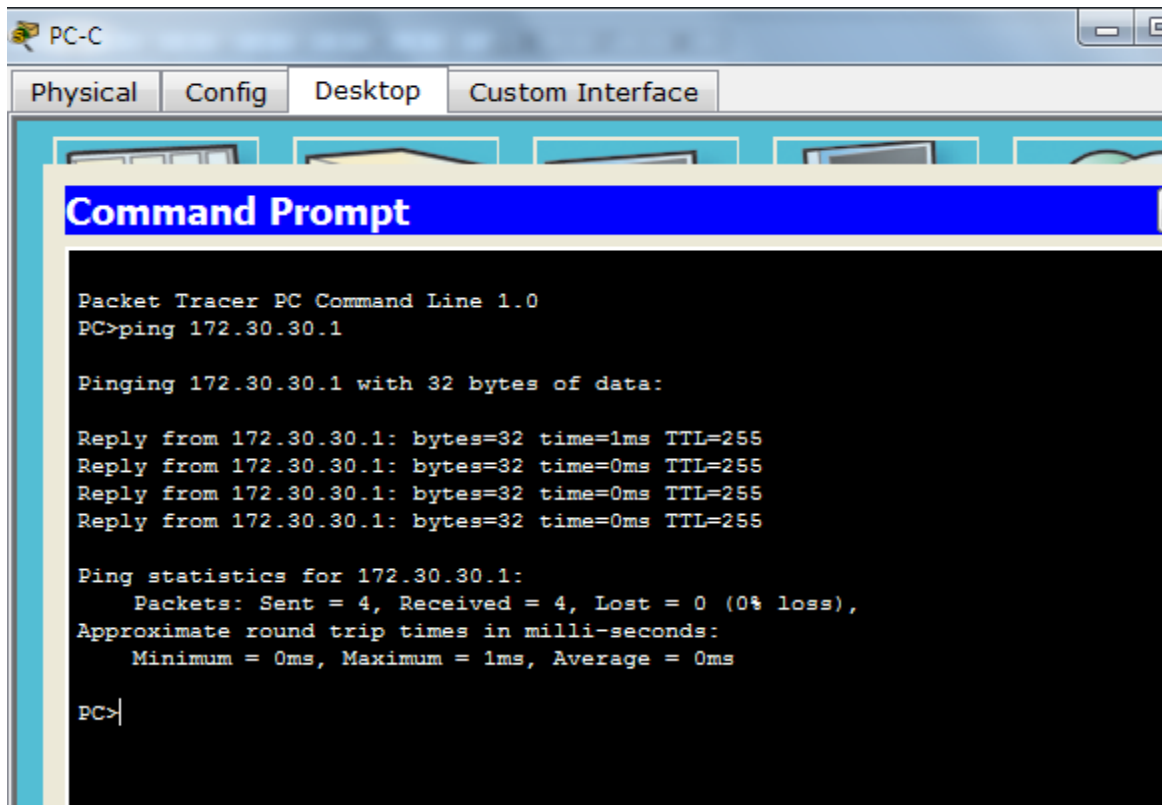
Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255
Reply from 209.165.201.1: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Dispositivo PC-A



The screenshot shows a Packet Tracer window for PC-C. The window has tabs for Physical, Config, Desktop, and Custom Interface. A Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255
Reply from 172.30.30.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

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

Dispositivo R1

```
This is a secure system. Authorized Access Only!  
  
R1>ping 209.165.201.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
  
R1>ping 172.30.30.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
  
R1>
```

Copy Paste

Dispositivo R2

```
Password:  
Password:  
  
R2>ping 172.30.10.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.30.10.1, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
  
R2>ping 172.30.30.1  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.30.30.1, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
  
R2>
```

Copy Paste

Dispositivo R3


```
Password:

R3>ping 172.30.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R3>ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R3>
```

Copy Paste

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

Copy

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

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

- d. 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.

```
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#passive-interface g0/0
R2(config-router)#no passive-interface g0/0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Copy

Paste

Paso 2. examinar el estado actual de la red.

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

R2# `show ip interface brief`

```

R2
Physical Config CLI
IOS Command Line Interface

Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#passive-interface g0/0
R2(config-router)#no passive-interface g0/0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0      209.165.201.1  YES manual  up          up
GigabitEthernet0/1      unassigned      YES unset   administratively down down
Serial10/0/0            10.1.1.2       YES manual  up          up
Serial10/0/1            10.2.2.2       YES manual  up          up
Vlan1                   unassigned      YES unset   administratively down down
R2#
Copy Paste

```

b. Verifique la conectividad entre las computadoras.

¿Es posible hacer ping de la PC-A a la PC-B? NO ¿Por qué? No hay ruta para pc-B

```

PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

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

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

PC>

```

¿Es posible hacer ping de la PC-A a la PC-C? NO ¿Por qué? No hay ruta para estas.

```
PC>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

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

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

PC>
```

¿Es posible hacer ping de la PC-C a la PC-B? No ¿Por qué? No hay ruta para estas

```
PC>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

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

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

PC>
```

¿Es posible hacer ping de la PC-C a la PC-A? No ¿Por qué? No hay ruta para estas

```
PC>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

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

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

PC>
```

c. Verifique que RIPv2 se ejecute en los routers

```
R1
Physical Config CLI
IOS Command Line Interface

This is a secure system. Authorized Access Only!

R1>enable
Password:
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
    Interface          Send Recv Triggered RIP  Key-chain
  Serial0/0/0          2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.1.2         120           00:00:25
Distance: (default is 120)
R1#
```

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

```
User Access Verification

Password:

R2>enable
Password:
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops

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

R2#
```

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

The screenshot shows the CLI of router R2. The window title is 'R2' and it has tabs for 'Physical', 'Config', and 'CLI'. The main title is 'IOS Command Line Interface'. The output shows several RIPv2 update messages. The following lines are highlighted in blue:

```
R2#RIP: sending v2 update to 224.0.0.9 via Serial10/0/0 (10.1.1.2)
RIP: build update entries
  10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial10/0/1 (10.2.2.2)
RIP: build update entries
  10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
```

Other visible output includes:

```
R2#RIP: received v2 update from 10.2.2.1 on Serial10/0/1
  172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: received v2 update from 10.1.1.1 on Serial10/0/0
  172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: received v2 update from 10.2.2.1 on Serial10/0/1
  172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: received v2 update from 10.1.1.1 on Serial10/0/0
  172.30.0.0/16 via 0.0.0.0 in 1 hops
R2#RIP: sending v2 update to 224.0.0.9 via Serial10/0/0 (10.1.1.2)
RIP: build update entries
  10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial10/0/1 (10.2.2.2)
RIP: build update entries
  10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
R2#undebg all
All possible debugging has been turned off
```

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

The screenshot shows the CLI of router R3. The window title is 'R3' and it has tabs for 'Physical', 'Config', and 'CLI'. The main title is 'IOS Command Line Interface'. The output shows the configuration for RIPv2, with the following lines highlighted in blue:

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

Other visible configuration includes:

```
no ip address
clock rate 2000000
shutdown
!
interface Serial10/0/1
ip address 10.2.2.1 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ~CThis is a secure system. Authorized Access Only!~C
!
!
!
line con 0
password 7 0822455D0A16
```

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

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

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:20, Serial0/0/1
           [120/1] via 10.1.1.1, 00:00:27, 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
R2#
```

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

R1# show ip route

```
R1
Physical Config CLI
IOS Command Line Interface

This is a secure system. Authorized Access Only!

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

Gateway of last resort is not set

      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
C       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
R1#
```

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

R3# **show ip route**

```
R3#
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

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:13, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
C       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
R3#
```

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


```
R2
Physical Config CLI
IOS Command Line Interface

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, 00:00:20, Serial0/0/1
    [120/1] via 10.1.1.1, 00:00:27, 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
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
    172.30.0.0/16 via 0.0.0.0 in 1 hops

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

R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
    172.30.0.0/16 via 0.0.0.0 in 1 hops

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

R2#
```

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

Paso 3. Desactivar la sumarización automática.

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

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

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

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#
```

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

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

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

The image displays three sequential screenshots of Cisco IOS terminal windows. The first screenshot shows R1 in configuration mode, where the user enters `clear ip route *` and then `end` to exit configuration mode. The second screenshot shows R2 in configuration mode, where the user enters `router rip`, `no auto-summary`, and `clear ip route *`. The terminal shows two error messages: "% Invalid input detected at '^' marker." for the first attempt and another for the second attempt, indicating that the asterisk in the command is not recognized. The third screenshot shows R3 in configuration mode, where the user enters `router rip`, `no auto-summary`, and `clear ip route *`. Similar to R2, the terminal shows two error messages: "% Invalid input detected at '^' marker." for the first attempt and another for the second attempt. Each terminal window has a "Copy" button at the bottom right.

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

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

```
R2# show ip route
```

```
R2
Physical Config CLI
IOS Command Line Interface

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

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
L       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, 00:01:42, Serial0/0/1
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:28, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:13, Serial0/0/1
C       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
R2#
```

R1# show ip route

```
R1
Physical Config CLI
IOS Command Line Interface

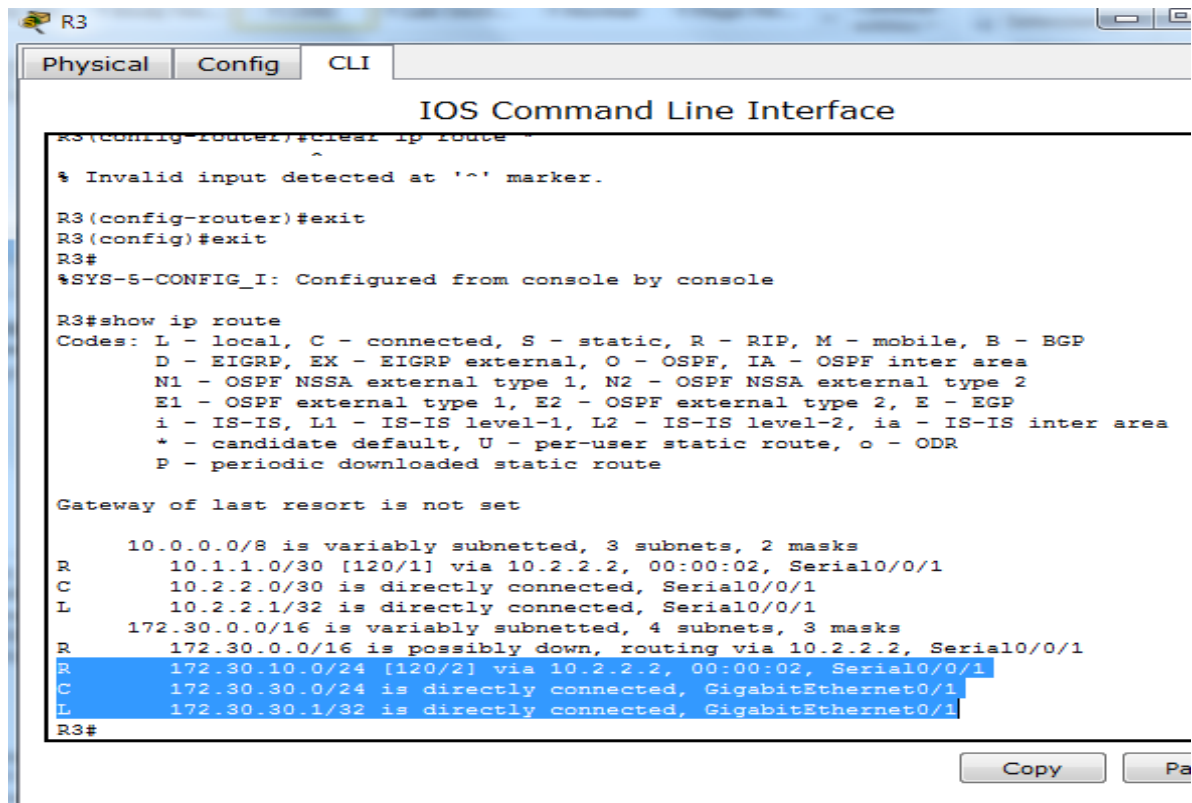
This is a secure system. Authorized Access Only!

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

Gateway of last resort is not set

    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, 00:00:08, Serial0/0/0
L       172.30.0.0/16 is variably subnetted, 4 subnets, 3 masks
R       172.30.0.0/16 [120/2] via 10.1.1.2, 00:00:08, Serial0/0/0
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, 00:00:08, Serial0/0/0
R1#
```

R3# show ip route



```
R3 (config-router)#clear ip route *
^
% Invalid input detected at '^' marker.
R3 (config-router)#exit
R3 (config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:02, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 3 masks
R       172.30.0.0/16 is possibly down, routing via 10.2.2.2, Serial0/0/1
R       172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:02, Serial0/0/1
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
R3#
```

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?

```

R2
Physical Config CLI
IOS Command Line Interface
172.30.30.0/24 via 0.0.0.0 in 1 hops
R2#debug ip rip
RIP protocol debugging is on
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
R2#no debug ip rip.
^
% Invalid input detected at '^' marker.
R2#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
172.30.30.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
172.30.0.0/16 via 0.0.0.0, metric 16, tag 0
172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
172.30.10.0/24 via 0.0.0.0, metric 2, tag 0
R2#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
172.30.10.0/24 via 0.0.0.0 in 1 hops
R2#no debug ip rip
RIP protocol debugging is off
R2#
Copy Paste

```

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

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

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

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

```

R2#no debug ip rip
RIP protocol debugging is off
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#
Copy Paste

```

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

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

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

```

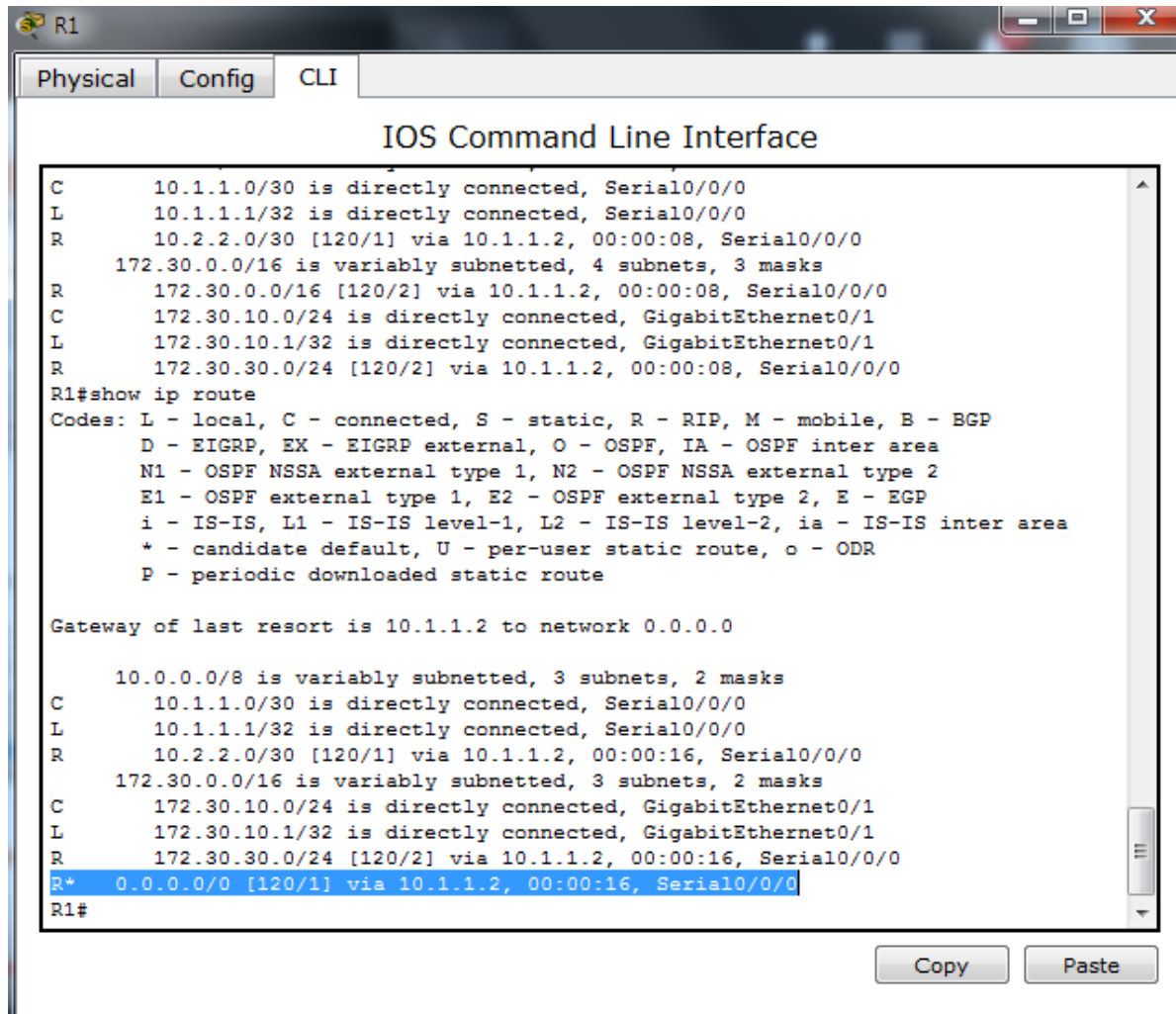
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#
Copy

```

Paso 5. Verificar la configuración de enrutamiento.

c. Consulte la tabla de routing en el R1.

R1# show ip route



```
R1
Physical Config CLI
IOS Command Line Interface
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, 00:00:08, Serial0/0/0
  172.30.0.0/16 is variably subnetted, 4 subnets, 3 masks
R 172.30.0.0/16 [120/2] via 10.1.1.2, 00:00:08, Serial0/0/0
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, 00:00:08, Serial0/0/0
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

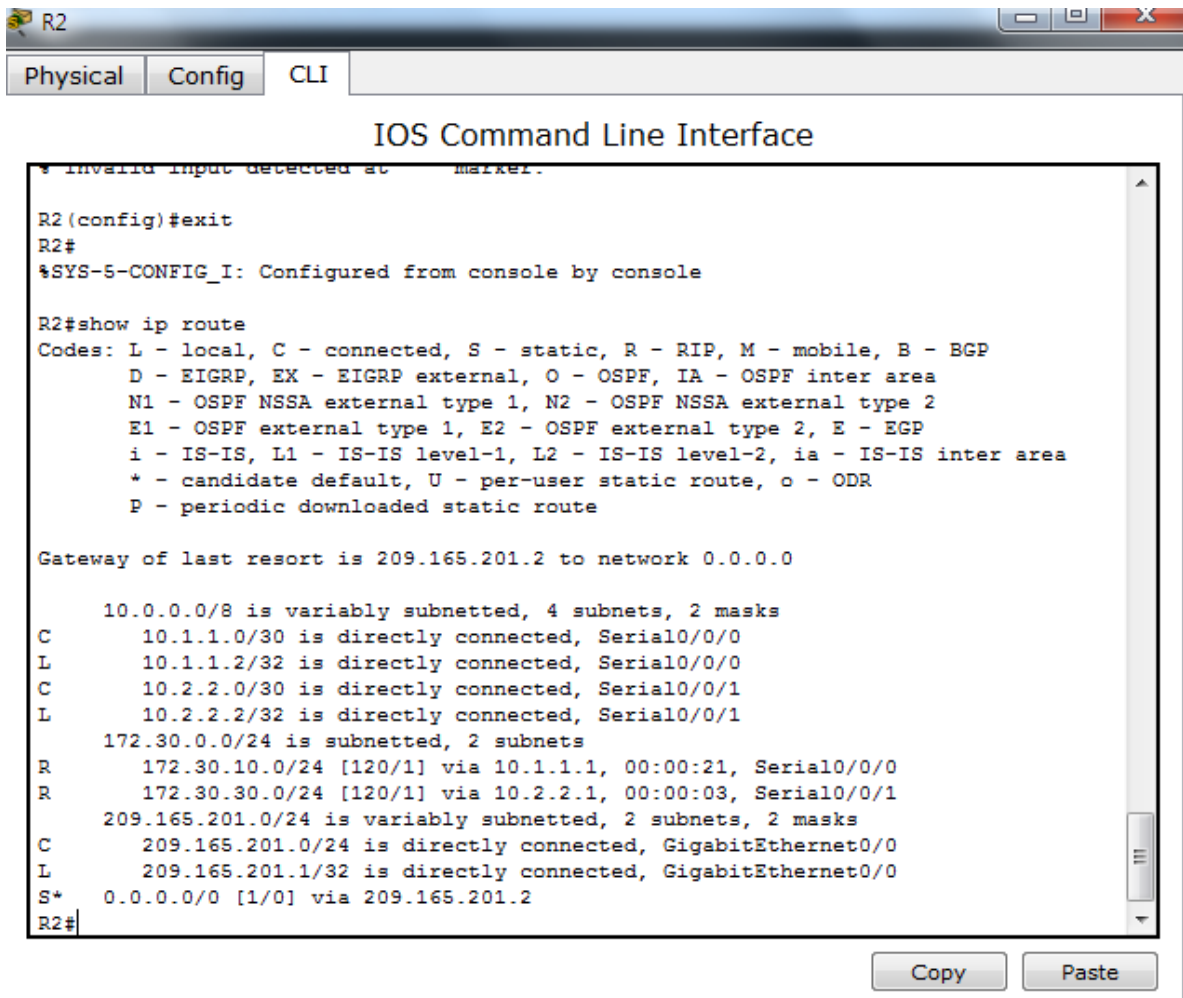
Gateway of last resort is 10.1.1.2 to network 0.0.0.0

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:16, Serial0/0/0
  172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.30.10.0/24 is directly connected, GigabitEthernet0/1
L 172.30.10.1/32 is directly connected, GigabitEthernet0/1
R 172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:16, Serial0/0/0
R1#
```

¿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?

Una puerta de enlace que conecta a internet y la ruta por defecto muestra en la tabla que esta prendida por rib.

- d. Consulte la tabla de routing en el R2.



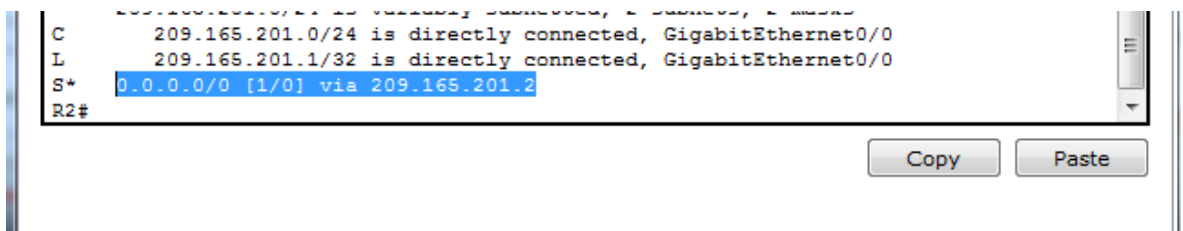
```
R2
Physical Config CLI
IOS Command Line Interface
* invalid input detected at ...
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is 209.165.201.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
    172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:03, Serial0/0/1
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
S*     0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

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

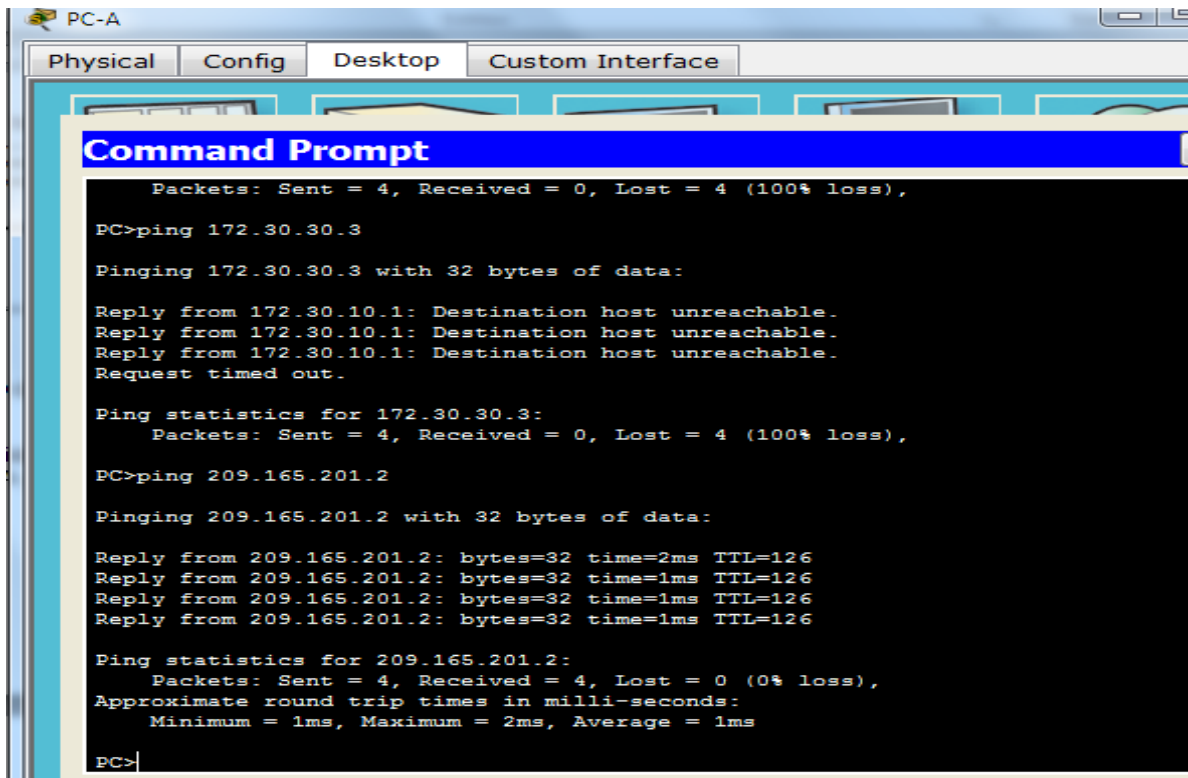


```
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
S*     0.0.0.0/0 [1/0] via 209.165.201.2
R2#
```

Paso 6. Verifique la conectividad.

- Simule el envío de tráfico a Internet haciendo ping de la PC-A y la PC-C a 209.165.201.2.
¿Tuvieron éxito los pings? Si

PC-A



The screenshot shows a Command Prompt window on PC-A. The window title is "PC-A" and it has tabs for "Physical", "Config", "Desktop", and "Custom Interface". The Command Prompt displays the following text:

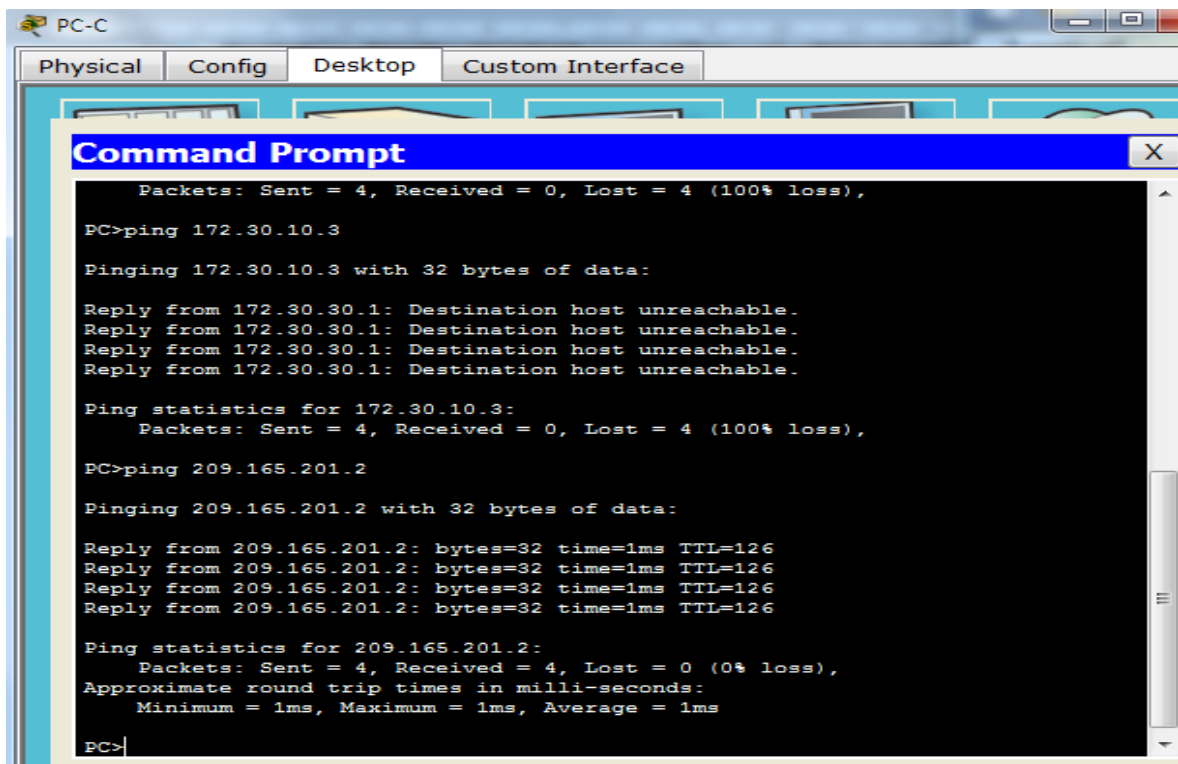
```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 172.30.30.3
Pinging 172.30.30.3 with 32 bytes of data:
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.
Request timed out.

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

PC>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

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

PC-C



The screenshot shows a Command Prompt window on PC-C. The window title is "PC-C" and it has tabs for "Physical", "Config", "Desktop", and "Custom Interface". The Command Prompt displays the following text:

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 172.30.10.3
Pinging 172.30.10.3 with 32 bytes of data:
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

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

PC>ping 209.165.201.2
Pinging 209.165.201.2 with 32 bytes of data:
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

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


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

¿Tuvieron éxito los pings? Si

PC-A

```
PC>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>
```

PC-C

```
PC>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=3ms TTL=125
Reply from 172.30.10.3: bytes=32 time=2ms TTL=125
Reply from 172.30.10.3: bytes=32 time=3ms TTL=125
Reply from 172.30.10.3: bytes=32 time=4ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms

PC>
```

Parte3: configurar IPv6 en los dispositivos

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

Paso 7. configurar los equipos host.

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

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 8. configurar IPv6 en los routers.

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

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

```
R1(config)#int g0/1
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#int s0/0
%Invalid interface type and number
R1(config)#int s0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:12::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#
```

```
Password:
Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:B::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#int S0/0/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:12::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#int S0/0/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:23::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#
```

Copy

Paste

```
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#int S0/0/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:23::3/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#
```

Copy

Paste

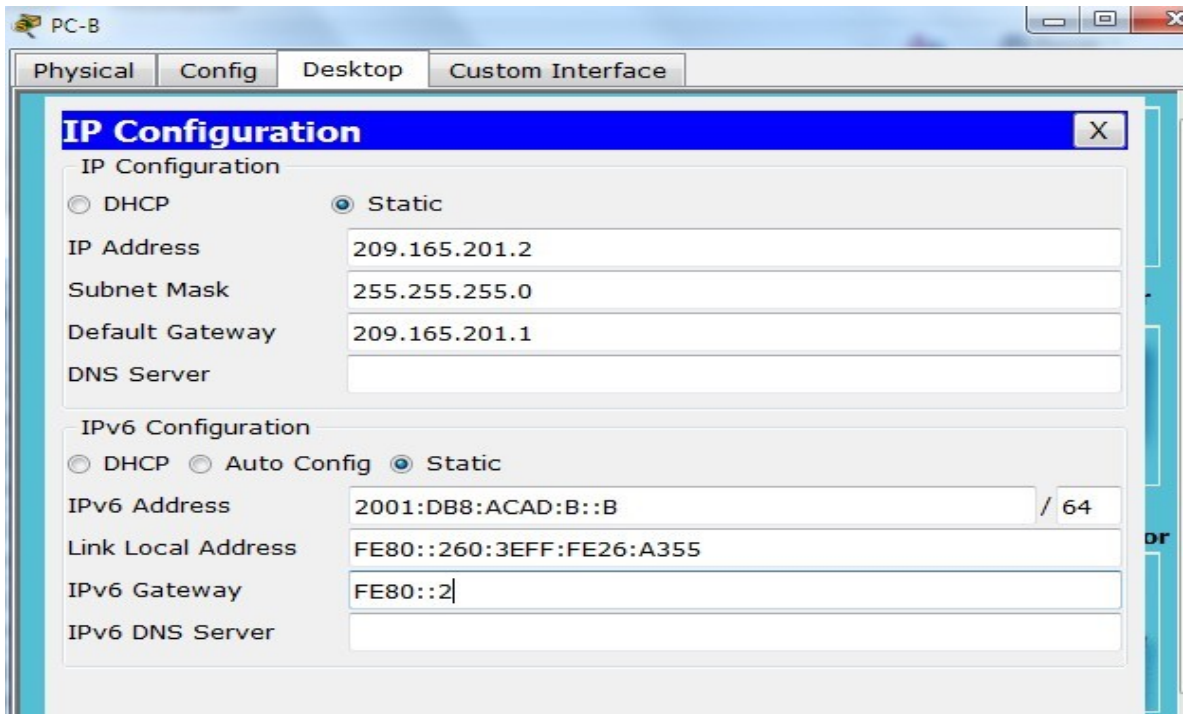
PC-A

The screenshot shows the 'IP Configuration' window for PC-A. The window has tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Config' tab is active, and the 'IP Configuration' window is open. It contains two sections: 'IP Configuration' and 'IPv6 Configuration'. In the 'IP Configuration' section, 'Static' is selected, and the fields are filled with IP Address: 172.30.10.3, Subnet Mask: 255.255.255.0, and Default Gateway: 172.30.10.1. In the 'IPv6 Configuration' section, 'Static' is selected, and the fields are filled with IPv6 Address: 2001:DB8:ACAD:A::A / 64, Link Local Address: FE80::20C:85FF:FEBC:239D, and IPv6 Gateway: FE80::1.

IP Configuration	
IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
IP Address	172.30.10.3
Subnet Mask	255.255.255.0
Default Gateway	172.30.10.1
DNS Server	

IPv6 Configuration	
IPv6 Configuration	<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static
IPv6 Address	2001:DB8:ACAD:A::A / 64
Link Local Address	FE80::20C:85FF:FEBC:239D
IPv6 Gateway	FE80::1
IPv6 DNS Server	

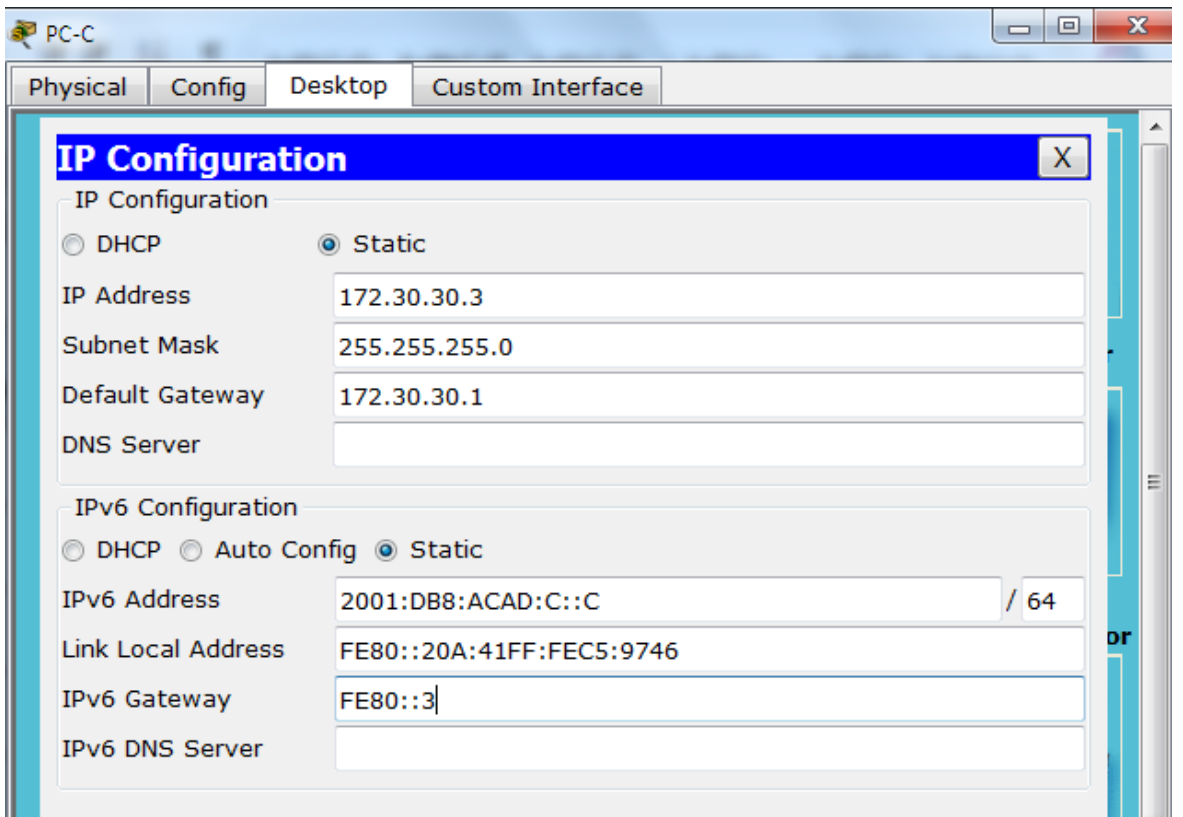
PC-B



The screenshot shows the IP Configuration window for PC-B. The window has tabs for Physical, Config, Desktop, and Custom Interface. The IP Configuration section is active, showing DHCP and Static options. The Static option is selected. The IP Address is 209.165.201.2, Subnet Mask is 255.255.255.0, and Default Gateway is 209.165.201.1. The IPv6 Configuration section is also active, showing DHCP, Auto Config, and Static options. The Static option is selected. The IPv6 Address is 2001:DB8:ACAD:B::B / 64, Link Local Address is FE80::260:3EFF:FE26:A355, and IPv6 Gateway is FE80::2.

IP Configuration		
IP Configuration		
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	
IP Address	209.165.201.2	
Subnet Mask	255.255.255.0	
Default Gateway	209.165.201.1	
DNS Server		
IPv6 Configuration		
<input type="radio"/> DHCP	<input type="radio"/> Auto Config	<input checked="" type="radio"/> Static
IPv6 Address	2001:DB8:ACAD:B::B	/ 64
Link Local Address	FE80::260:3EFF:FE26:A355	
IPv6 Gateway	FE80::2	
IPv6 DNS Server		

PC-C



The screenshot shows the IP Configuration window for PC-C. The window has tabs for Physical, Config, Desktop, and Custom Interface. The IP Configuration section is active, showing DHCP and Static options. The Static option is selected. The IP Address is 172.30.30.3, Subnet Mask is 255.255.255.0, and Default Gateway is 172.30.30.1. The IPv6 Configuration section is also active, showing DHCP, Auto Config, and Static options. The Static option is selected. The IPv6 Address is 2001:DB8:ACAD:C::C / 64, Link Local Address is FE80::20A:41FF:FEC5:9746, and IPv6 Gateway is FE80::3.

IP Configuration		
IP Configuration		
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	
IP Address	172.30.30.3	
Subnet Mask	255.255.255.0	
Default Gateway	172.30.30.1	
DNS Server		
IPv6 Configuration		
<input type="radio"/> DHCP	<input type="radio"/> Auto Config	<input checked="" type="radio"/> Static
IPv6 Address	2001:DB8:ACAD:C::C	/ 64
Link Local Address	FE80::20A:41FF:FEC5:9746	
IPv6 Gateway	FE80::3	
IPv6 DNS Server		

c. Habilite el routing IPv6 en cada router.

R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#
```

R2

```
R2(config)#ipv6 unicast-routing
R2(config)#
```

R3

```
R3(config)#ipv6 unicast-routing
R3(config)#
```

d. Introduzca el comando apropiado para verificar las direcciones IPv6 y el estado de enlace.

R1

```
R1#show ipv6 int brief
GigabitEthernet0/0      [administratively down/down]
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
Serial10/0/0            [up/up]
    FE80::1
    2001:DB8:ACAD:12::1
Serial10/0/1            [administratively down/down]
Vlan1                   [administratively down/down]
R1#
```

Copy

R2

```
R2#show ipv6 int brief
GigabitEthernet0/0      [up/up]
    FE80::2
    2001:DB8:ACAD:B::2
GigabitEthernet0/1      [administratively down/down]
Serial0/0/0             [up/up]
    FE80::2
    2001:DB8:ACAD:12::2
Serial0/0/1             [up/up]
    FE80::2
    2001:DB8:ACAD:23::2
Vlan1                   [administratively down/down]
R2#
```

Copy

Paste

R3

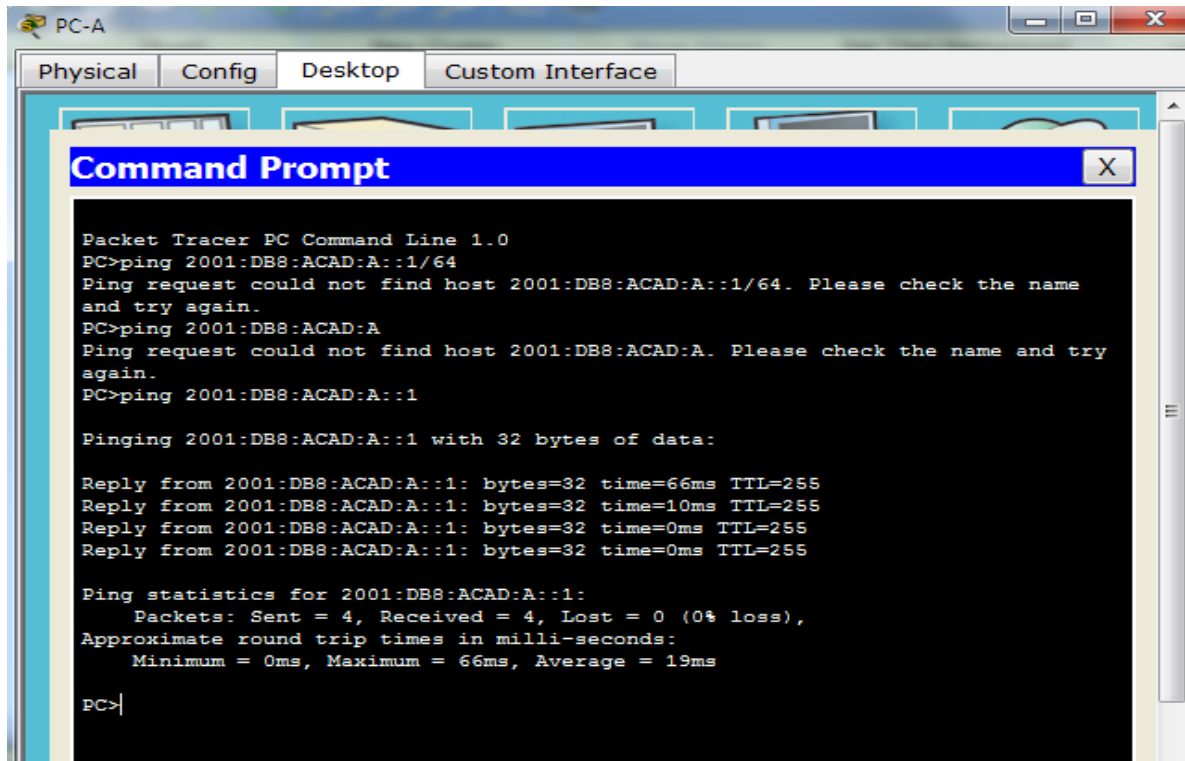
```
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

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

Escriba el comando en el espacio que se incluye a continuación. **show ipv6 int brief**

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

PC-A



The screenshot shows a Packet Tracer PC Command Line window for PC-A. The window title is "PC-A" and it has tabs for "Physical", "Config", "Desktop", and "Custom Interface". The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:A::1/64
Ping request could not find host 2001:DB8:ACAD:A::1/64. Please check the name
and try again.
PC>ping 2001:DB8:ACAD:A
Ping request could not find host 2001:DB8:ACAD:A. Please check the name and try
again.
PC>ping 2001:DB8:ACAD:A::1

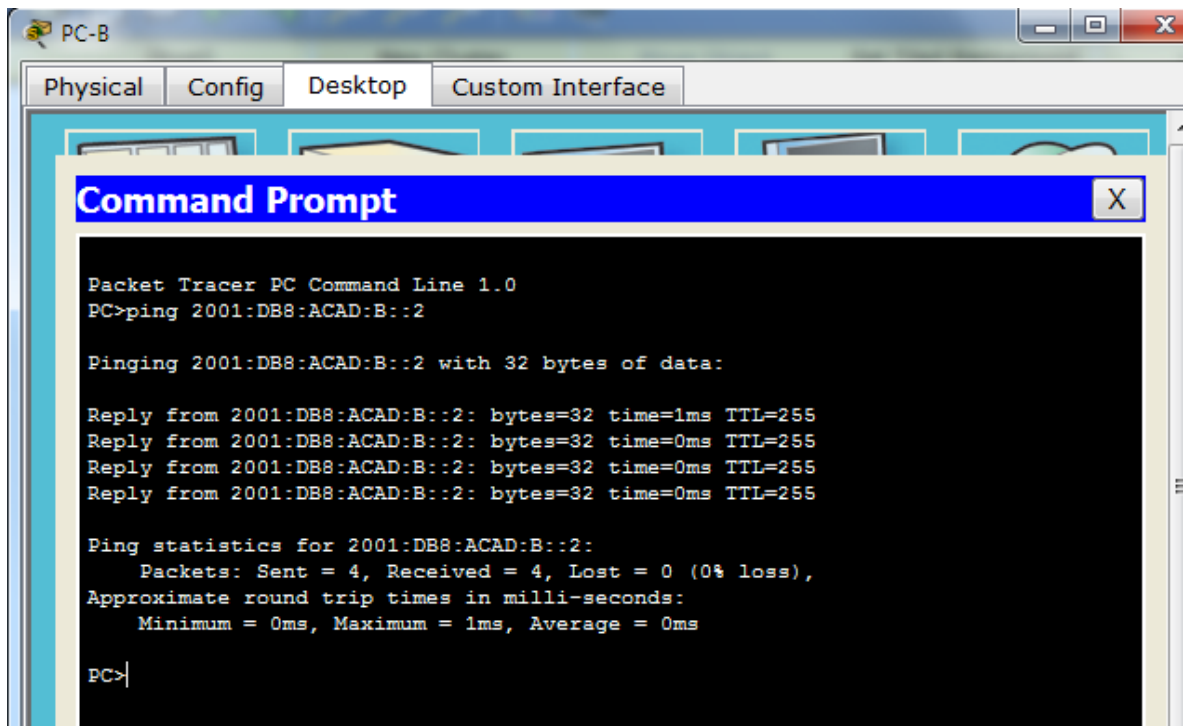
Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=66ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=10ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 66ms, Average = 19ms

PC>
```

PC-B



The screenshot shows a Packet Tracer PC Command Line window for PC-B. The window title is "PC-B" and it has tabs for "Physical", "Config", "Desktop", and "Custom Interface". The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:B::2

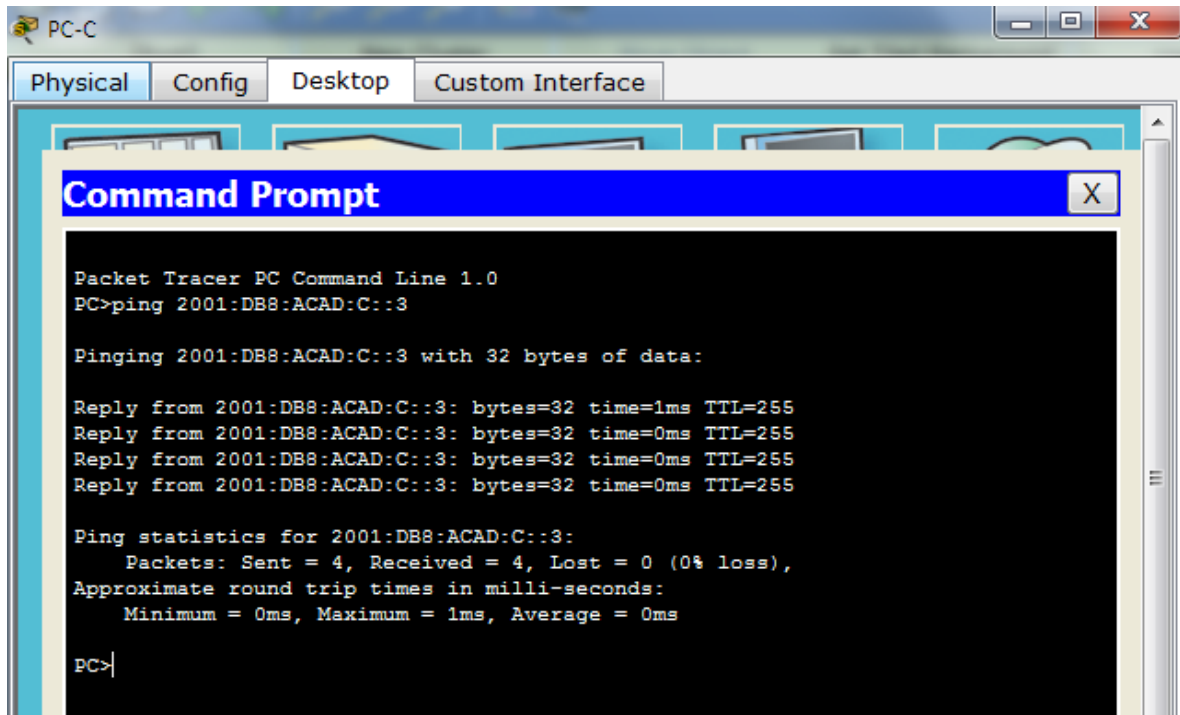
Pinging 2001:DB8:ACAD:B::2 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::2: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:B::2: bytes=32 time=0ms TTL=255

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

PC>
```

PC-C



```
PC-C
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 2001:DB8:ACAD:C::3

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

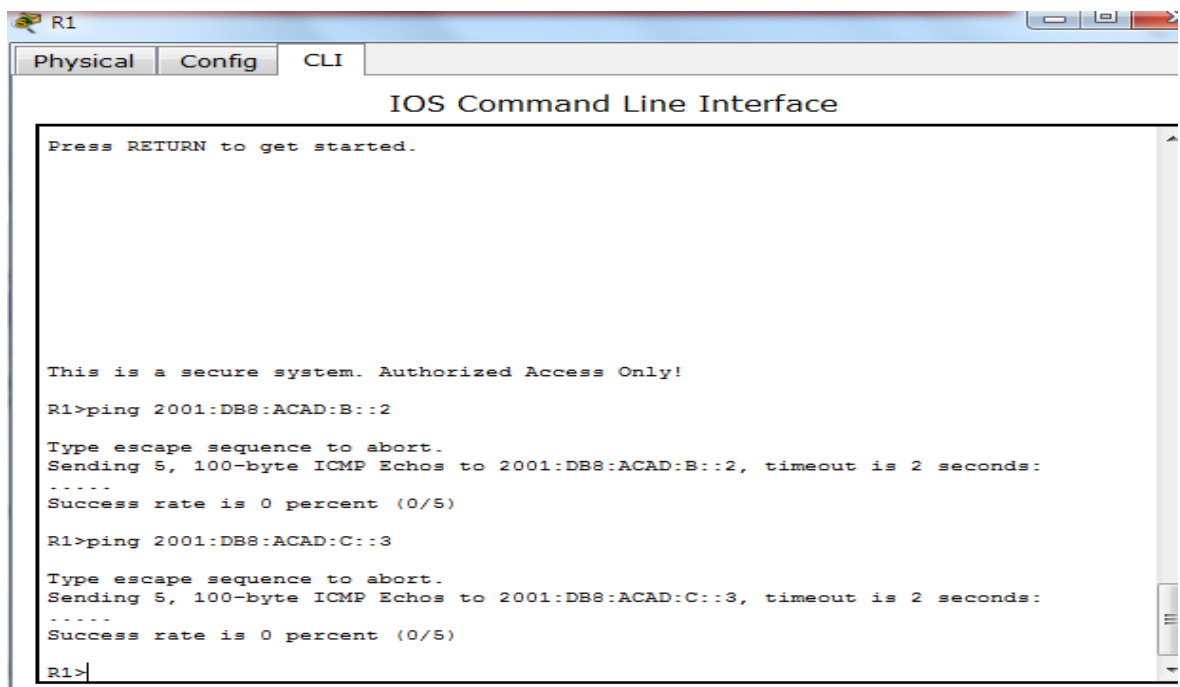
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:C::3: bytes=32 time=0ms TTL=255

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

PC>
```

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

R1



```
R1
Physical Config CLI

IOS Command Line Interface

Press RETURN to get started.

This is a secure system. Authorized Access Only!

R1>ping 2001:DB8:ACAD:B::2

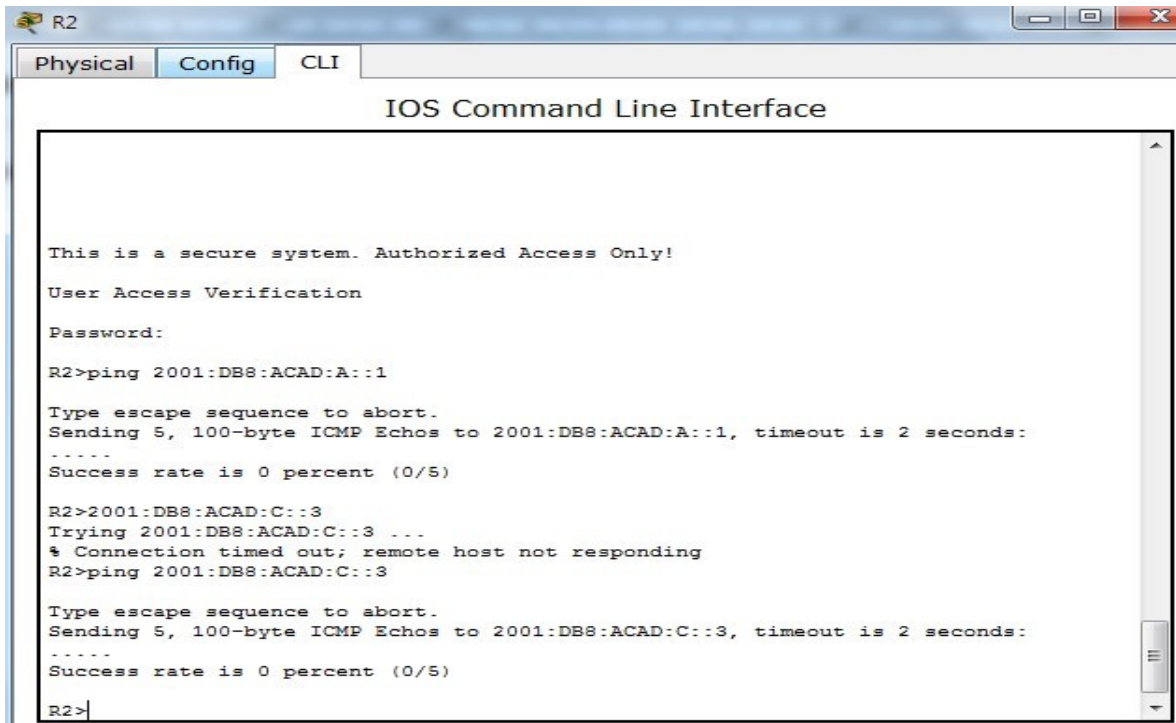
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1>ping 2001:DB8:ACAD:C::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1>
```


R2



```
R2
Physical Config CLI
IOS Command Line Interface

This is a secure system. Authorized Access Only!
User Access Verification
Password:
R2>ping 2001:DB8:ACAD:A::1

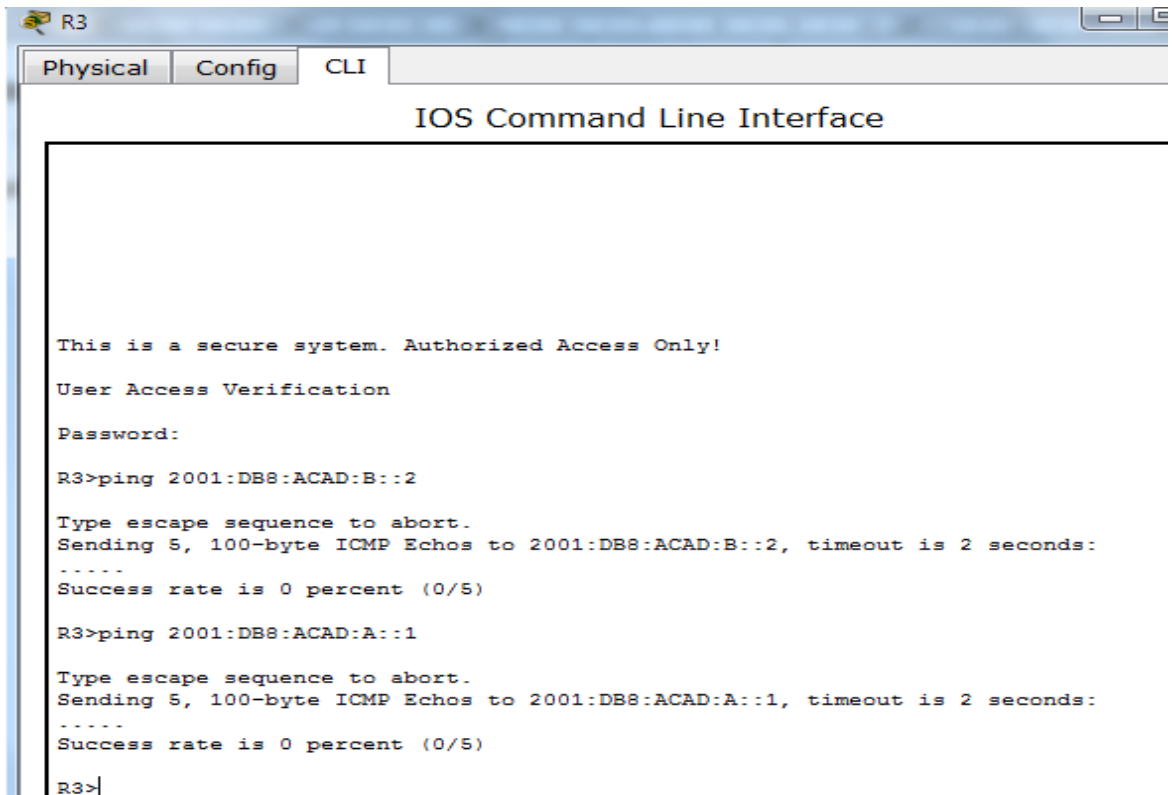
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:A::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R2>2001:DB8:ACAD:C::3
Trying 2001:DB8:ACAD:C::3 ...
% Connection timed out; remote host not responding
R2>ping 2001:DB8:ACAD:C::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R2>
```

R3



```
R3
Physical Config CLI
IOS Command Line Interface

This is a secure system. Authorized Access Only!
User Access Verification
Password:
R3>ping 2001:DB8:ACAD:B::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:B::2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R3>ping 2001:DB8:ACAD:A::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:A::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R3>
```

Parte 4: configurar y verificar el routing RIPng

Paso 1. Configurar el routing RIPng.

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

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

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#interface s0/0/0
R1(config-if)#ipv6 rip Test1 enable
R1(config-if)#
```

Copy

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

```
R2#configure terminal
Enter configuration commands, one per line. End with CN
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip test2 enable
R2(config-if)#
```

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

```
Password:
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#int s0/0/1
R3(config-if)#ipv6 rip Test3 enable
R3(config-if)#
```

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

R1

```
This is a secure system. Authorized Access Only!

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

R1#
```

R2

```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip test2"
  Interfaces:
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None

R2#
```

R3

```
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test3"
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/1
  Redistribution:
    None

R3#
```

¿En qué forma se indica RIPng en el resultado? *Por el nombre del proceso*

```

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

```

- e. Emita el comando `show ipv6 rip Test1`.

```
R1# show ipv6 rip Test1
```

```

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

R1#show ipv6 rip ?
  database  RIP local RIB
R1#show ipv6 rip database
RIP process "Test1" local RIB
  2001:DB8:ACAD:C::/64, metric 3, installed
    Serial0/0/0/FE80::2, expires in 175 sec
  2001:DB8:ACAD:12::/64, metric 2
    Serial0/0/0/FE80::2, expires in 175 sec
  2001:DB8:ACAD:23::/64, metric 2, installed
    Serial0/0/0/FE80::2, expires in 175 sec
R1#

```

¿Cuáles son las similitudes entre RIPv2 y RIPng?

Las dos tienen la distancia de 120, usan la métrica y las autorizaciones las envían cada 30s.

- 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.

Show ipv6 route

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

```

R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:A::1/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:C::/64 [120/3]
    via FE80::2, Serial0/0/0, receive
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::1/128 [0/0]
    via Serial0/0/0, receive
R   2001:DB8:ACAD:23::/64 [120/2]
    via FE80::2, Serial0/0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#

```

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

```

R2>enable
Password:
R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0, receive
C   2001:DB8:ACAD:B::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:B::2/128 [0/0]
    via GigabitEthernet0/0, receive
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1, receive
C   2001:DB8:ACAD:12::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:12::2/128 [0/0]
    via Serial0/0/0, receive
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::2/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R2#

```

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

```

R3>enable
Password:
R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R   2001:DB8:ACAD:A::/64 [120/3]
    via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:C::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:C::3/128 [0/0]
    via GigabitEthernet0/1, receive
R   2001:DB8:ACAD:12::/64 [120/2]
    via FE80::2, Serial0/0/1, receive
C   2001:DB8:ACAD:23::/64 [0/0]
    via Serial0/0/1, directly connected
L   2001:DB8:ACAD:23::3/128 [0/0]
    via Serial0/0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R3#

```

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

```

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

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

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

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

PC>

```

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

```

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=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:C::C: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:ACAD:C::C:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 4ms

PC>

```

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

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

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

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

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

PC>
```

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

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

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

Reply from 2001:DB8:ACAD:A::A: bytes=32 time=3ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=12ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:ACAD:A::A: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:ACAD:A::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 4ms

PC>
```

¿Por qué algunos pings tuvieron éxito y otros no? No hay ruta que se notifique para la PCB

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

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

```
Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#
```

- 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>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:B::B
R2(config)#int s0/0/0
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#int s0/0/1
R2(config-if)#ipv6 rip Test2 default-information originate
R2(config-if)#
```

Paso 3. Verificar la configuración de enrutamiento.

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

R2# show ipv6 route

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

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


```

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

```

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

```

R1>enable
Password:
R1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C  2001:DB8:ACAD:A::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A::1/128 [0/0]
   via GigabitEthernet0/1, receive
R  2001:DB8:ACAD:C::/64 [120/3]
   via FE80::2, Serial0/0/0, receive
C  2001:DB8:ACAD:12::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:ACAD:12::1/128 [0/0]
   via Serial0/0/0, receive
R  2001:DB8:ACAD:23::/64 [120/2]
   via FE80::2, Serial0/0/0, receive
L  FF00::/8 [0/0]
   via Null0, receive
R1#

```

```

R3>enable
Password:
R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R 2001:DB8:ACAD:A::/64 [120/3]
  via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:C::/64 [0/0]
  via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:C::3/128 [0/0]
  via GigabitEthernet0/1, receive
R 2001:DB8:ACAD:12::/64 [120/2]
  via FE80::2, Serial0/0/1, receive
C 2001:DB8:ACAD:23::/64 [0/0]
  via Serial0/0/1, directly connected
L 2001:DB8:ACAD:23::3/128 [0/0]
  via Serial0/0/1, receive
L FF00::/8 [0/0]
  via Null0, receive
R3#

```

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

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

```

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

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

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

PC>

```

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

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

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

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

PC>
```

Reflexión

1. ¿Por qué desactivaría la sumarización automática para RIPv2? **Sería bueno para que los router no sumarize las rutas y así haya conectividad en redes discontinuas.**
2. En ambas situaciones, ¿en qué forma descubrieron la ruta a Internet el R1 y el R3? **Aprendieron con las actualizaciones de ripng donde fue configurada la ruta predeterminada R2**
3. ¿En qué se diferencian la configuración de RIPv2 y la de RIPng? **Se configura notificando las redes y el Ripng en las interfaces.**

8.2.4.5 LAB - CONFIGURING BASIC SINGLE-AREA OSPFV2

topologia

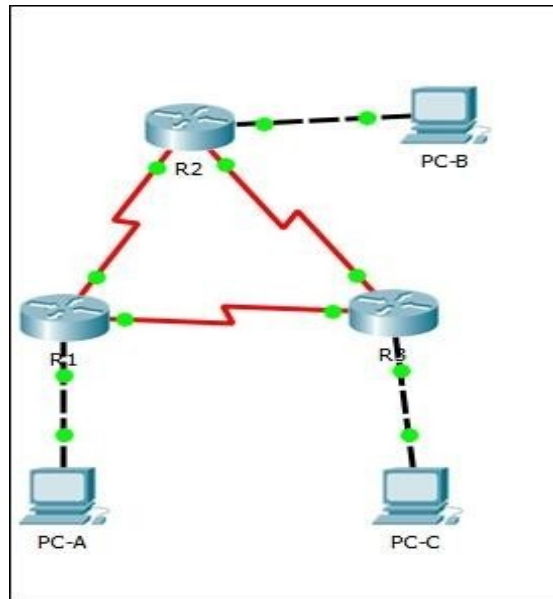


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPF

Parte 3: cambiar las asignaciones de ID del router

Parte 4: configurar interfaces OSPF pasivas

Parte 5: cambiar las métricas de OSPF

Información básica/situación

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

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

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

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

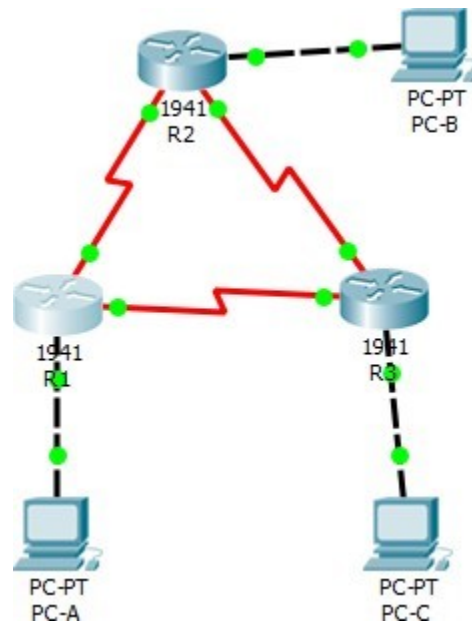
Recursos necesarios

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

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

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

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



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

Step 4: configurar los parámetros básicos para cada router.

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo como se muestra en la topología.
- Asigne **class** como la contraseña del modo EXEC privilegiado.
- Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- Configure un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
- Configure **logging synchronous** para la línea de consola.
- Configure la dirección IP que se indica en la tabla de direccionamiento para todas las interfaces.
- Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.

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

NOTA: SE REALIZA LA CONFIGURACION EN LOS TRES ROUTER DE ACUERDO A LA TABLA DE ENRUTAMIENTO

```
R1
Physical Config CLI Attributes
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#banner motd #Se prohíbe el acceso no autorizado!#
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#exit
R1#copy running-config startup-config
%SYS-5-CONFIG_I: Configured from console by console

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

TABLA DE ENRUTAMIENTO

```
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

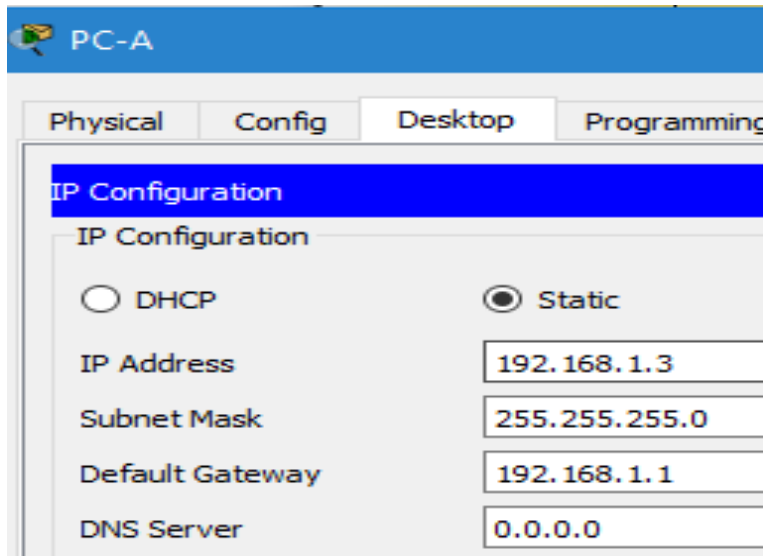
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 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

R1#
```

Step 5:

Step 6: configurar los equipos host.

NOTA: SE REALIZA LA RESPECTIVA CONFIGURACION EN LOS TRES PCS



Step 7: Probar la conectividad.

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

```
R1#ping 192.168.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/21/101 ms

R1#ping 192.168.13.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.13.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/7/31 ms

R1#
```

```
R2#
```

```
R2#ping 192.168.12.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/28 ms
```

```
R2#ping 192.168.23.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/30 ms
```

```
R2#
```

```
R3#ping 192.168.13.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/35 ms
```

Parte 2: Configurar y verificar el enrutamiento OSPF

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

Step 8: Configure el protocolo OSPF en R1.

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

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

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

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

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

Step 9: Configure OSPF en el R2 y el R3.

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

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/
R2(config)#router os
R2(config)#router ospf 1
R2(config-router)#net
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.12.0 0.0.0.3 area 0
00:47:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 192.168.2.0 0.0.0.3 area 0
R2(config-router)#network 192.168.23.0 0.0.0.3 area 0
R2(config-router)#
```

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router os
R3(config)#router ospf 1
R3(config-router)#net
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
R3(config-router)#network 192.168.13.0 0.0.0.3 area 0
00:50:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.13.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-router)#network 192.168.23.0 0.0.0.3 area 0
R3(config-router)#
00:51:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on
Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-router)#
```

Step 10: verificar los vecinos OSPF y la información de routing.

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

R1# **show ip ospf neighbor**

```
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
192.168.23.2     0     FULL/ -         00:00:34    192.168.13.2   Serial0/0/1
192.168.23.1     0     FULL/ -         00:00:36    192.168.12.2   Serial0/0/0
R1#
```

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

R1# **show ip route**

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

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O       192.168.2.0/24 [110/65] via 192.168.12.2, 00:05:42, Serial0/0/0
O       192.168.3.0/24 [110/65] via 192.168.13.2, 00:02:12, Serial0/0/1
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
    192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:02:02, Serial0/0/0
                    [110/128] via 192.168.13.2, 00:02:02, Serial0/0/1
```

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

Step 11: verificar la configuración del protocolo OSPF.

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

R1# **show ip protocols**

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.13.1          110          00:07:47
    192.168.23.1          110          00:07:36
    192.168.23.2          110          00:07:36
  Distance: (default is 110)
```

R1#

Step 12: verificar la información del proceso OSPF.

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

R1# **show ip ospf**

```

R1#show ip ospf
Routing Process "ospf 1" with ID 192.168.13.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
  Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm executed 7 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x00c59a
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

```

Step 13: 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

```

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

```

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

R1# show ip ospf interface

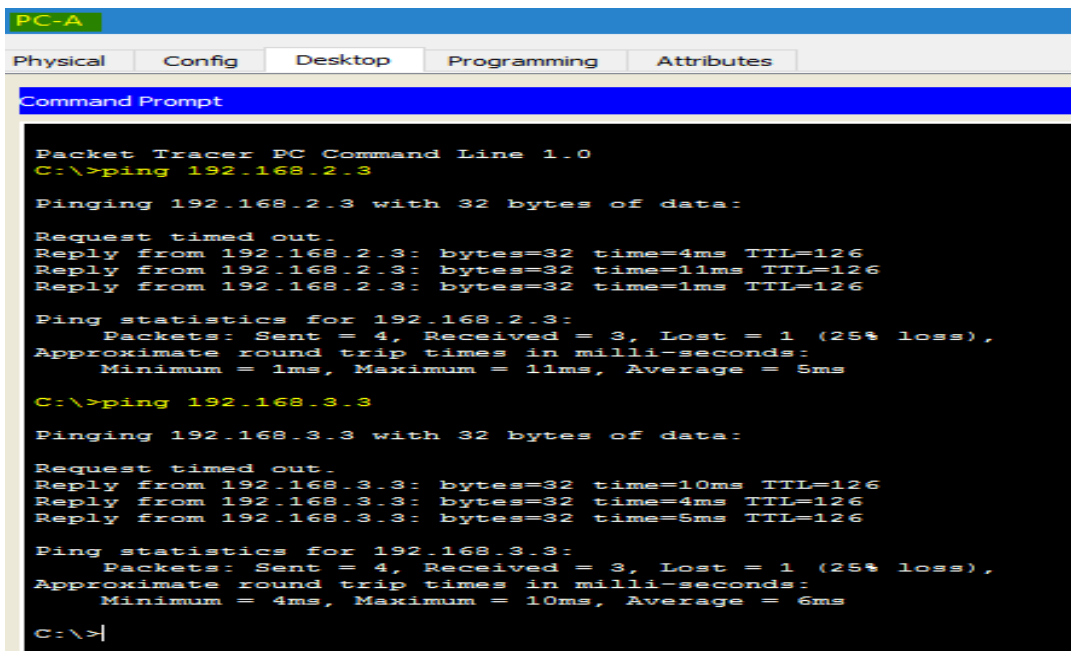
```
R1#show ip ospf interface
```

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

Step 14: Verificar la conectividad de extremo a extremo.

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

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



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.3: bytes=32 time=4ms TTL=126
Reply from 192.168.2.3: bytes=32 time=11ms 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 = 11ms, Average = 5ms
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=4ms TTL=126
Reply from 192.168.3.3: bytes=32 time=6ms TTL=126
Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 10ms, Average = 6ms
C:\>
```

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=14ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 7ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126
Reply from 192.168.3.3: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 9ms

C:\>|
```

```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=3ms TTL=126
Reply from 192.168.1.3: bytes=32 time=5ms TTL=126
Reply from 192.168.1.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=11ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>|
```

Parte 3: cambiar las asignaciones de ID del router

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

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

Dado que no se ha configurado ningún ID o interfaz de loopback en los tres routers, el ID de router para cada ruta se determina según la dirección IP más alta de cualquier interfaz activa. En la parte 3, cambiará la asignación de ID del router OSPF con direcciones de loopback. También usará el comando **router-id** para cambiar la ID del router.

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

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

- 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.

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

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

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

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

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

- 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.

NOTA: SE REALIZA EL PROCEDIMIENTO EN LOS TRES ROUTERS

```

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

Readonly ROMMON initialized

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

IOS Image Load Test

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

```

- e. Una vez que se haya completado el proceso de recarga del router, emita el comando **show ip protocols** para ver la nueva ID del router.

R1# show ip protocols

```

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:51
    2.2.2.2          110          00:00:51
    3.3.3.3          110          00:00:51
    192.168.13.1     110          00:01:23
    192.168.23.1     110          00:01:55
    192.168.23.2     110          00:04:38
  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

```
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/ -	00:00:35	192.168.12.2	Serial0/0/0

```
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**.

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

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

R1#
```

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

```
R1# show ip protocols
```

```

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1         110          00:18:36
    2.2.2.2         110          00:00:23
    3.3.3.3         110          00:00:23
    11.11.11.11    110          00:00:23
    192.168.13.1   110          00:49:08
    192.168.23.1   110          00:49:40
    192.168.23.2   110          00:52:23
  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
```

```

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/ -         00:00:31   192.168.12.2   Serial0/0/0
R1#

```

Part 2: 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 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 00:00:06
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
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
```

- 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 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, 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, 00:08:54, 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, 00:05:32, 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, 00:05:32, Serial0/0/1
           [110/128] via 192.168.12.1, 00:05:32, 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#
```

```

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, 00:10:15, Serial0/0/0
O       192.168.2.0/24 [110/65] via 192.168.23.1, 00:08:00, 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, 00:08:00, Serial0/0/1
           [110/128] via 192.168.13.1, 00:08:00, 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/ -	00:00:30	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

```

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)#pass
R2(config-router)#passive-interface def
R2(config-router)#passive-interface default
R2(config-router)#
01:02:39: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached

01:02:39: %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/ -	00:00:30	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 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**.
- f. En el R2, emita el comando **no passive-interface s0/0/0** 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 pas
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#
01:06:34: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#
```

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

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

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

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

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

- 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 pas
R2(config-router)#no passive-interface s0/0/1
R2(config-router)#
01:25:32: %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.

¿Qué interfaz usa el R3 para enrutarse a la red 192.168.2.0/24? *Serial0/0/1*

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

65

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

Parte 4: 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 3: 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 (connected)
  Hardware is CN Gigabit Ethernet, address is 0040.0bc7.6701 (bia
0040.0bc7.6701)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is
unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)

```

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#
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:26:20, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:40:09, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/128] via 192.168.13.2, 00:26:20, Serial0/0/1
                                [110/128] via 192.168.12.2, 00:26:20, 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 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 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
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
```

```
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 00:00:07
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 33.33.33.33
Suppress hello for 0 neighbor(s)
R1#
```

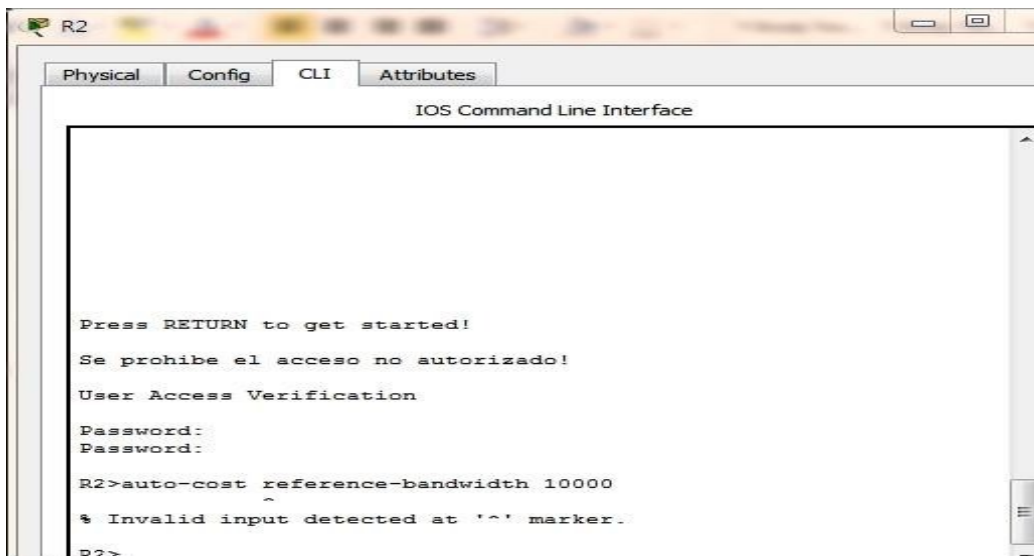
La suma de los costos de estas dos interfaces es el costo acumulado de la ruta a la red 192.168.3.0/24 en el R3 ($1 + 64 = 65$), como puede observarse en el resultado del comando **show ip route**.

- 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.

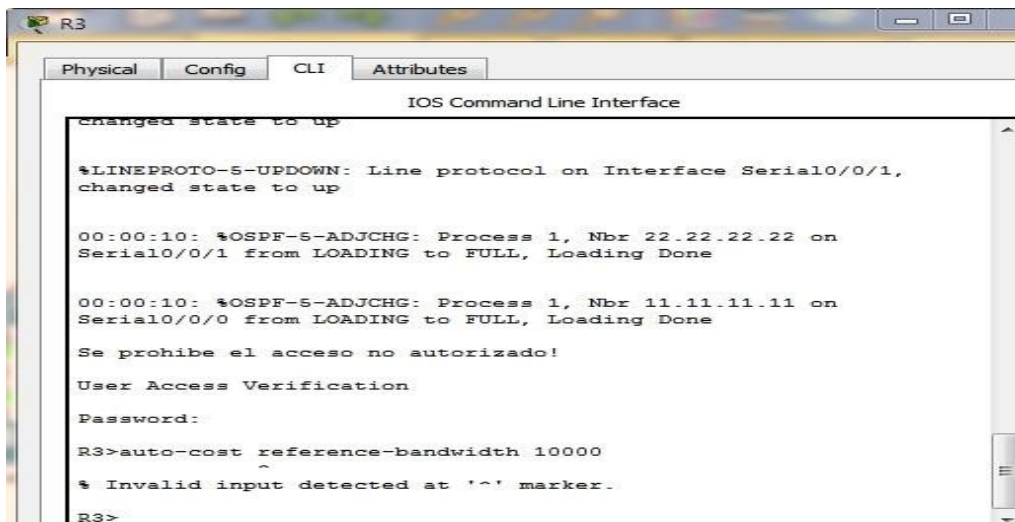
```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router os
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#
```

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



```
R2
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started!
Se prohíbe el acceso no autorizado!
User Access Verification
Password:
Password:
R2>auto-cost reference-bandwidth 10000
^
% Invalid input detected at '^' marker.
R2>
```



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

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

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 22.22.22.22 on
Serial0/0/1 from LOADING to FULL, Loading Done

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on
Serial0/0/0 from LOADING to FULL, Loading Done

Se prohíbe el acceso no autorizado!
User Access Verification
Password:
R3>auto-cost reference-bandwidth 10000
^
% Invalid input detected at '^' marker.
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
```

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).

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

```
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 100
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 33.33.33.33, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

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

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

```
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.13.1/30, Area 0
  Process ID 1, Router ID 11.11.11.11, Network Type POINT-TO-POINT, Cost: 6476
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  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#
```

- 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

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.

```
R1#show ip route ospf
O   192.168.2.0 [110/6576] via 192.168.12.2, 00:03:11, Serial0/0/0
O   192.168.3.0 [110/6576] via 192.168.13.2, 00:02:51, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/12952] via 192.168.13.2, 00:02:51, Serial0/0/1
        [110/12952] via 192.168.12.2, 00:02:51, Serial0/0/0

R1#
```

- 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?

Los equipos de la actualidad soportan velocidades en enlaces que son mayores a 100 Mb/s,

Step 4: cambiar el ancho de banda de una interfaz.

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

Nota: un concepto erróneo habitual es suponer que con el comando **bandwidth** se cambia el ancho de banda físico, o la velocidad, del enlace. El comando modifica la métrica de ancho

de banda que utiliza OSPF para calcular los costos de routing, pero no modifica el ancho de banda real (la velocidad) del enlace.

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

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

```
R1#show interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/0/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1158 kilobits/sec
  5 minute input rate 70 bits/sec, 0 packets/sec
  5 minute output rate 70 bits/sec, 0 packets/sec
    688 packets input, 48864 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
```

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

R1# **show ip route ospf**

```
R1#show ip route ospf
O    192.168.2.0 [110/65] via 192.168.12.2, 00:05:45, Serial0/0/0
O    192.168.3.0 [110/65] via 192.168.13.2, 00:04:59, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0 [110/128] via 192.168.13.2, 00:04:59, Serial0/0/1
    [110/128] via 192.168.12.2, 00:04:59, Serial0/0/0
```

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
```

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

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

```
R1#show ip route ospf
O   192.168.2.0 [110/129] via 192.168.13.2, 00:00:16, Serial0/0/1
O   192.168.3.0 [110/65] via 192.168.13.2, 00:06:37, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/128] via 192.168.13.2, 00:00:16, 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
% Invalid input detected at '^' marker.
R1#
```

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

- 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
O   192.168.2.0 [110/782] via 192.168.12.2, 00:00:20, Serial0/0/0
O   192.168.3.0 [110/782] via 192.168.13.2, 00:00:20, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/845] via 192.168.13.2, 00:00:20, Serial0/0/1
           [110/845] via 192.168.12.2, 00:00:20, Serial0/0/0
R1#
```

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

781+1=782 y 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
O   192.168.1.0 [110/65] via 192.168.13.1, 00:17:24, Serial0/0/0
O   192.168.2.0 [110/65] via 192.168.23.1, 00:17:24, Serial0/0/1
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/128] via 192.168.23.1, 00:10:57, Serial0/0/1

R3#
```

- i. Emita el comando **bandwidth 128** en todas las interfaces seriales restantes de la topología. ¿Cuál es el nuevo costo acumulado a la red 192.168.23.0/24 en el R1? ¿Por qué?

1562 781+781=1562

Step 5: 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
O   192.168.2.0 [110/782] via 192.168.12.2, 00:12:06, Serial0/0/0
O   192.168.3.0 [110/782] via 192.168.13.2, 00:12:06, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.13.2, 00:00:18, Serial0/0/1
        [110/1562] via 192.168.12.2, 00:00:18, Serial0/0/0

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
```

- 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
O   192.168.2.0 [110/782] via 192.168.12.2, 00:15:00, Serial0/0/0
O   192.168.3.0 [110/1563] via 192.168.12.2, 00:00:06, Serial0/0/0
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/1562] via 192.168.12.2, 00:00:06, 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.

781+781+1=1563 el cual es < 1565

8.3.3.6 LAB - CONFIGURING BASIC SINGLE-AREA OSPFV3

Topologia

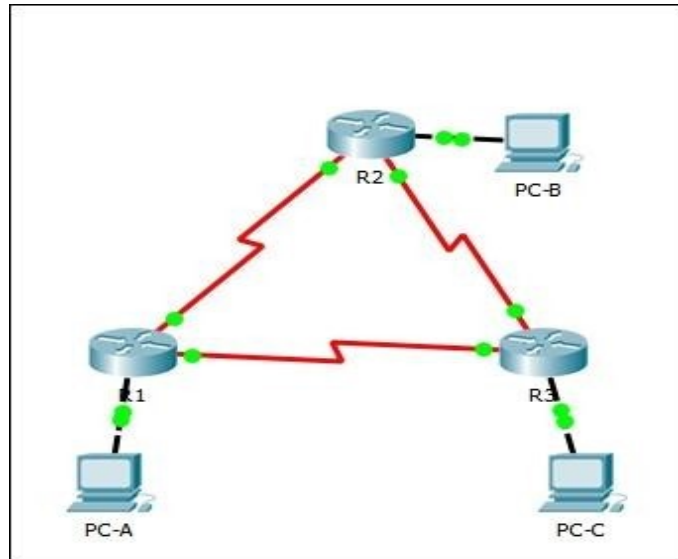


Tabla de direccionamiento

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

Objetivos

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

Parte 2: configurar y verificar el routing OSPFv3

Parte 3: configurar interfaces pasivas OSPFv3

Información básica/situación

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

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

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

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

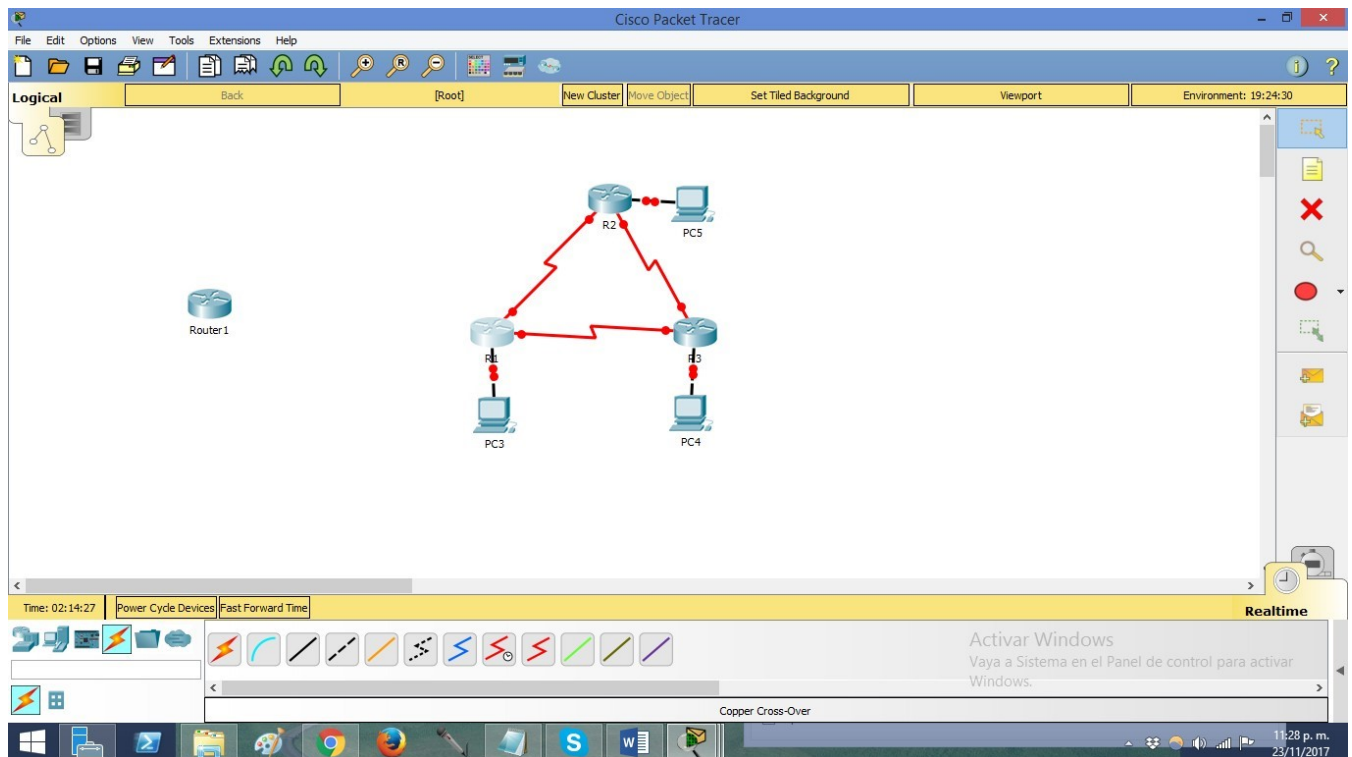
Recursos necesarios

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

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

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

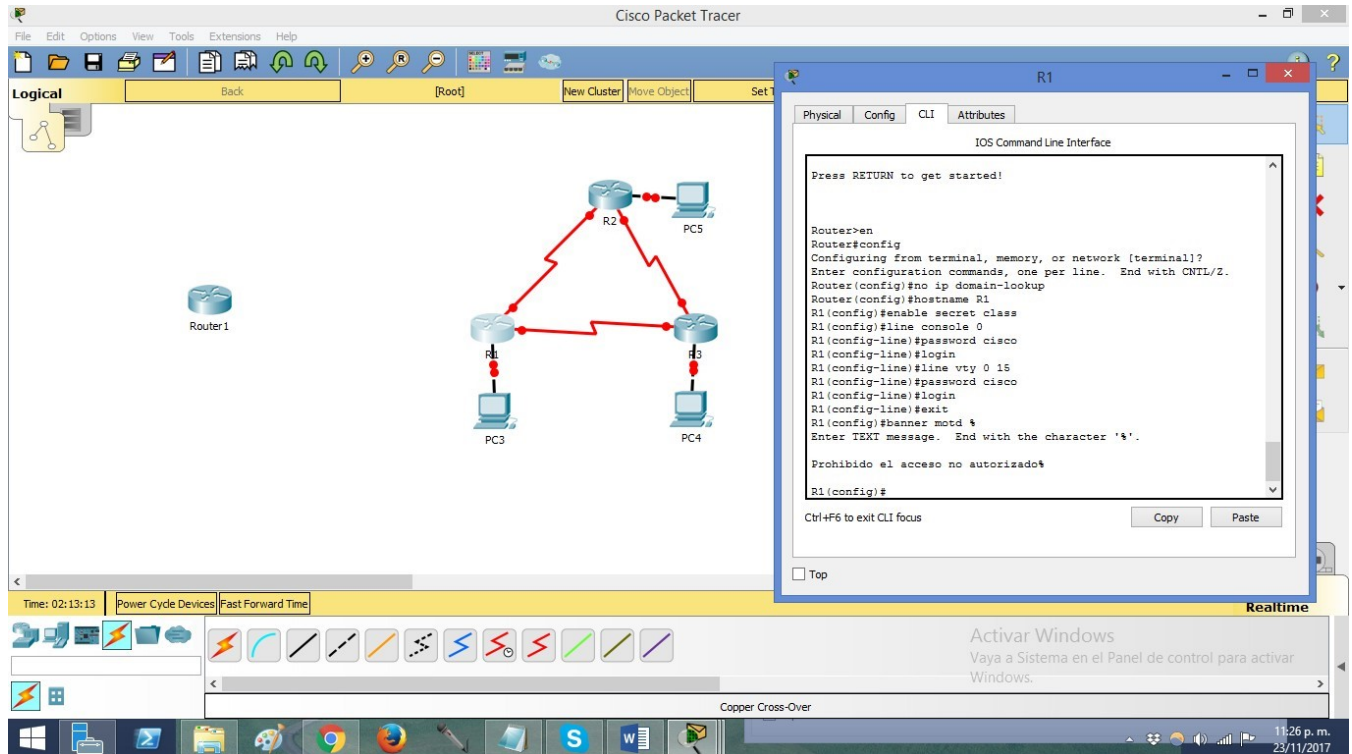
Step 6: realizar el cableado de red tal como se muestra en la topología.



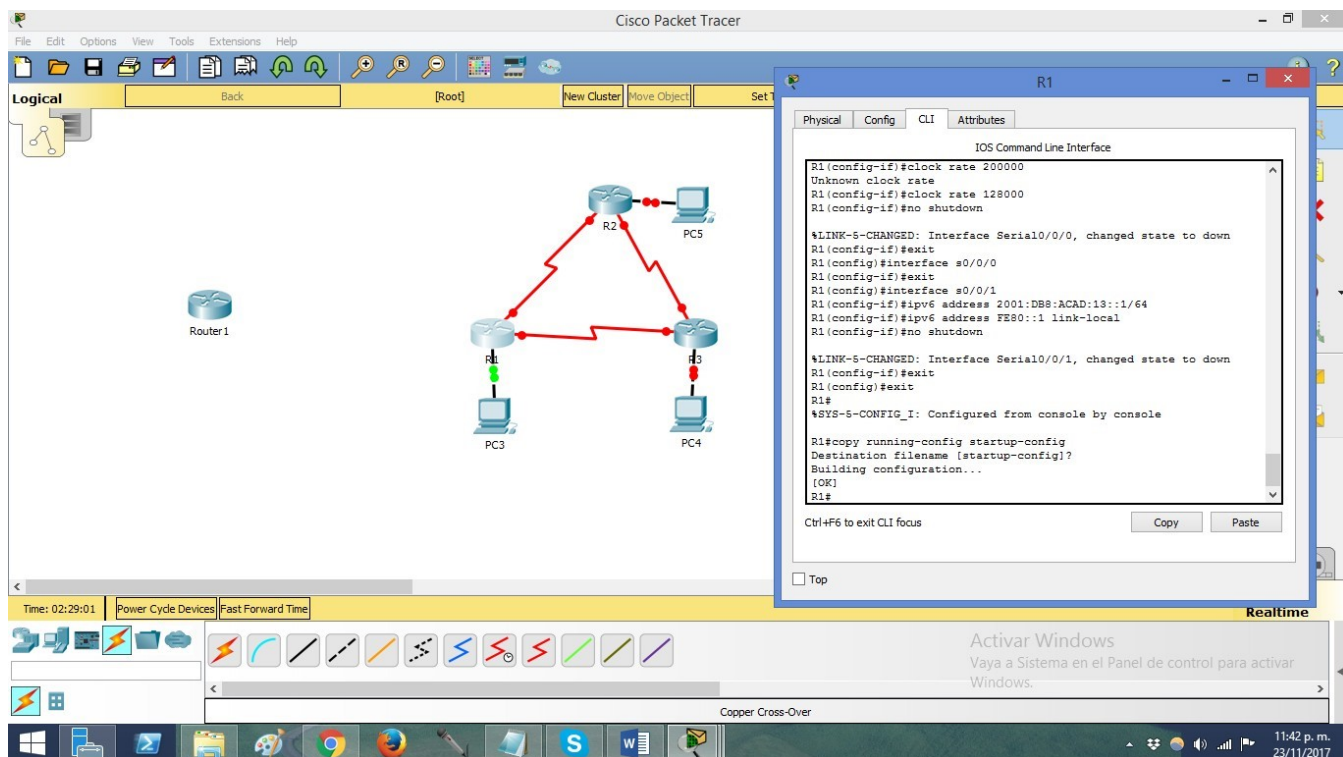
Step 7: inicializar y volver a cargar los routers según sea necesario.

Step 8: configurar los parámetros básicos para cada router.

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



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



Step 9: configurar los equipos host.

Step 10: 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.

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.

Step 11: asignar ID a los routers.

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

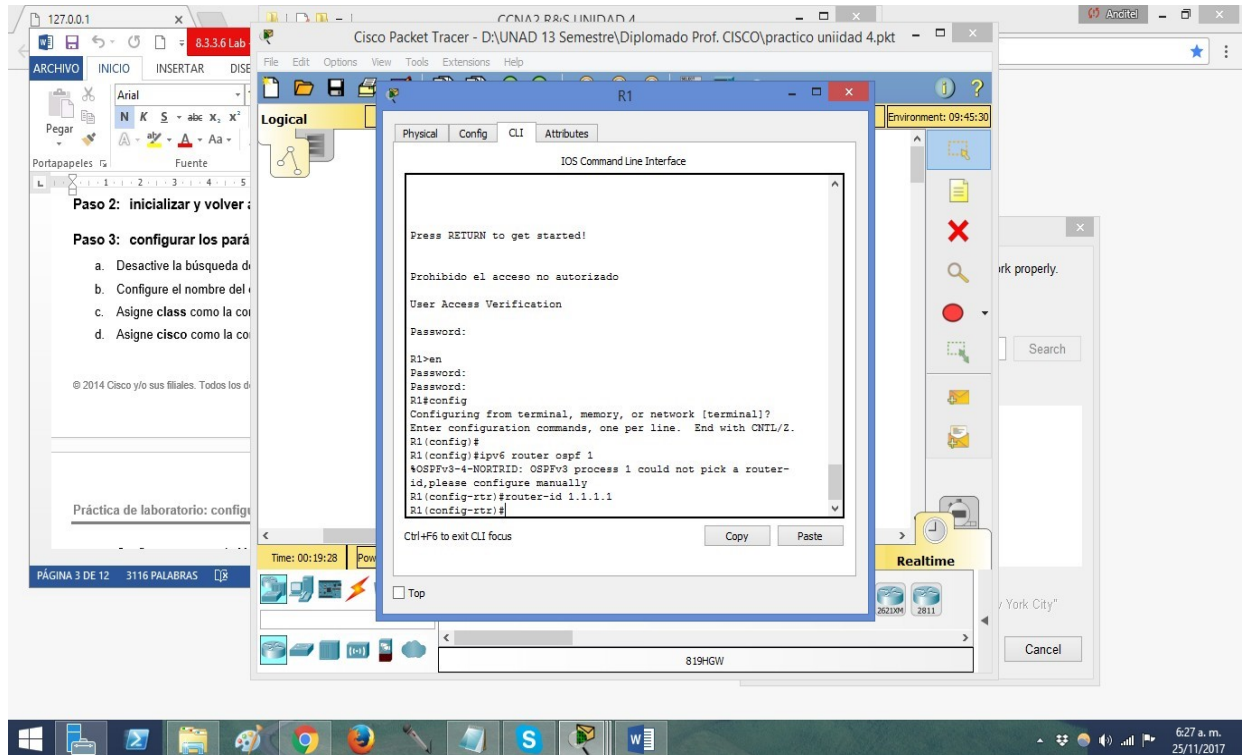
a. Emita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

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

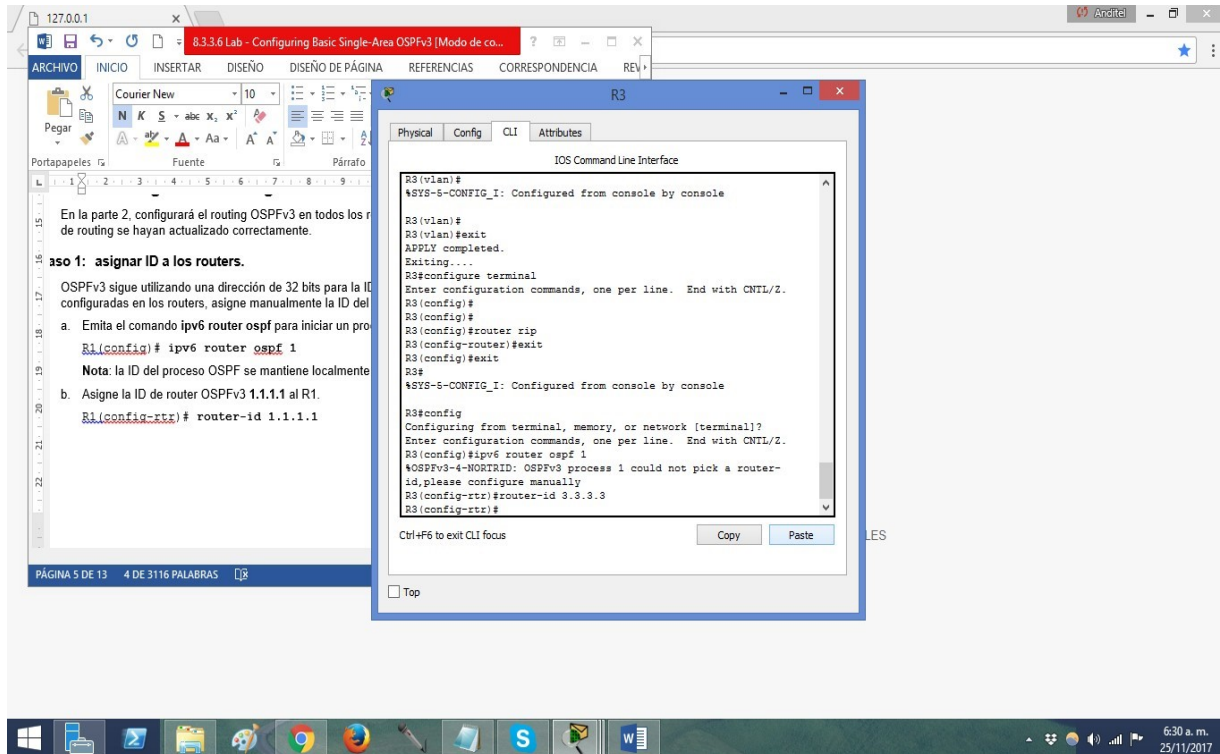
Nota: la ID del proceso OSPF se mantiene localmente y no tiene sentido para los otros routers de la red.

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

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



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



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

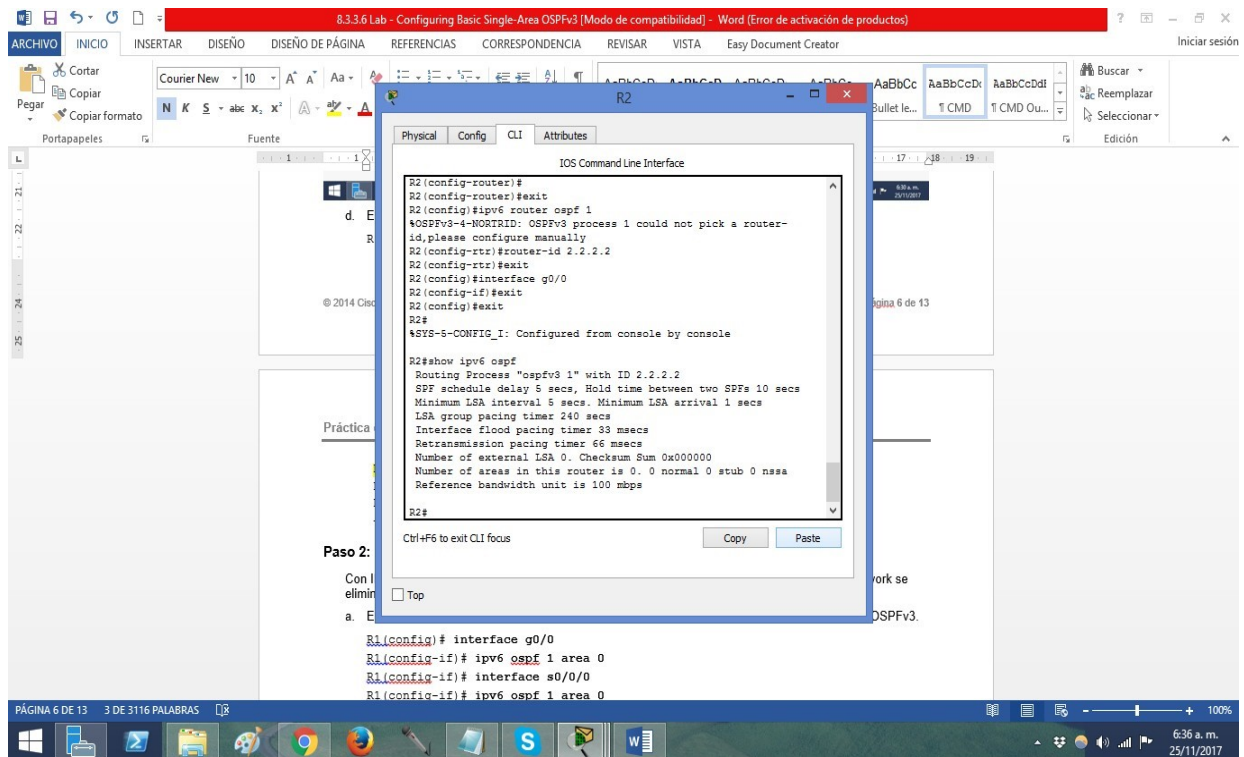
R2# **show ipv6 ospf**

Routing Process "ospfv3 1" with ID 2.2.2.2

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

Router is not originating router-LSAs with maximum metric

<Output Omitted>



Step 12: configurar OSPFv6 en el R1.

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

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

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

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

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

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

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

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

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

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

```
R1#
```

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

R1#

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

Step 13: verificar vecinos de OSPFv3.

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

R1# **show ipv6 ospf neighbor**

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

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

The screenshot shows a document titled "8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3" with the following content:

Paso 3: verificar vecinos de OSPFv3.
Emita el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

```
R1# show ipv6 ospf neighbor
```

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

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

Paso 4: verificar la configuración del protocolo OSPFv3.
El comando **show ipv6 protocols** es una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

```
R1# show ipv6 protocols
```

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"

The terminal window shows the following output:

```
R1# show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID
2.2.2.2	0	FULL/ -	00:00:30	3
3.3.3.3	0	FULL/ -	00:00:38	3

Step 14: verificar la configuración del protocolo OSPFv3.

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

R1# **show ipv6 protocols**

IPv6 Routing Protocol is "connected"

IPv6 Routing Protocol is "ND"

IPv6 Routing Protocol is "**ospf 1**"

Router ID 1.1.1.1

Number of areas: 1 normal, 0 stub, 0 nssa

Interfaces (**Area 0**):

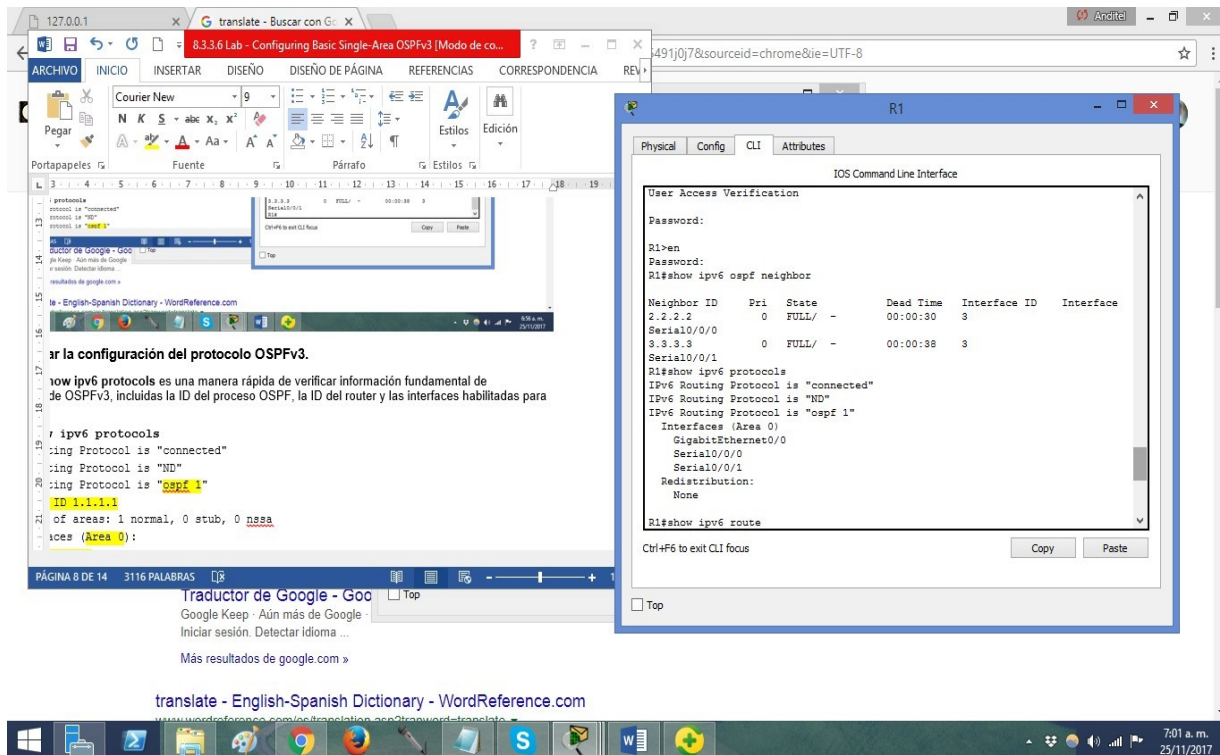
Serial0/0/1

Serial0/0/0

GigabitEthernet0/0

Redistribution:

None



The screenshot displays a Windows desktop environment. In the foreground, a Microsoft Word document is open, showing the text from the previous blocks. In the background, a terminal window titled 'R1' is open, displaying the output of the 'show ipv6 protocols' command. The terminal output is as follows:

```
IOS Command Line Interface

User Access Verification

Password:
R1>en
Password:
R1#show ipv6 ospf neighbor

Neighbor ID  Pri  State           Dead Time   Interface ID  Interface
2.2.2.2      0  FULL/-        00:00:30    3
3.3.3.3      0  FULL/-        00:00:38    3

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

R1#show ipv6 route

Ctrl+H to exit CLI focus
```


Step 15: verificar las interfaces OSPFv3.

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

R1# **show ipv6 ospf interface**

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

Link Local Address FE80::1, Interface ID 7

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

Network Type POINT_TO_POINT, Cost: 64 Transmit

Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:05

Graceful restart helper support enabled

Index 1/3/3, flood queue length 0

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

Last flood scan length is 1, maximum is 1

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 3.3.3.3

Suppress hello for 0 neighbor(s)

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

Link Local Address FE80::1, Interface ID 6

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

Network Type POINT_TO_POINT, Cost: 64 Transmit

Delay is 1 sec, State POINT_TO_POINT

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

Hello due in 00:00:00

Graceful restart helper support enabled

Index 1/2/2, flood queue length 0

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

Last flood scan length is 1, maximum is 2

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

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 2.2.2.2

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

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

No backup designated router on this network

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

Hello due in 00:00:03

Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

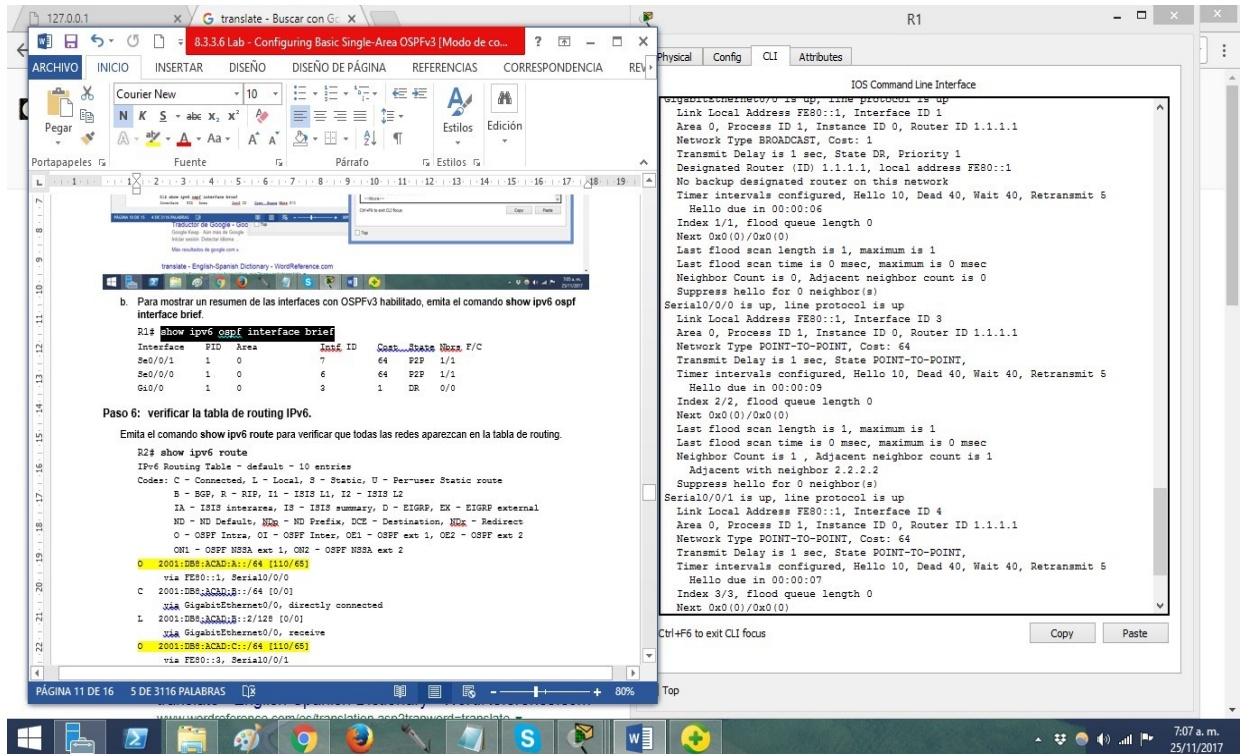
Next 0x0(0)/0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

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

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)



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

R1# show ipv6 ospf interface brief

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

Step 16: verificar la tabla de routing IPv6.

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

R2# show ipv6 route

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

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

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:B::/64 [0/0]

via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:B::2/128 [0/0]

via GigabitEthernet0/0, receive

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1

C 2001:DB8:ACAD:12::/64 [0/0]

via Serial0/0/0, directly connected

L 2001:DB8:ACAD:12::2/128 [0/0]

via Serial0/0/0, receive

O 2001:DB8:ACAD:13::/64 [110/128]

via FE80::3, Serial0/0/1

via FE80::1, Serial0/0/0

C 2001:DB8:ACAD:23::/64 [0/0]

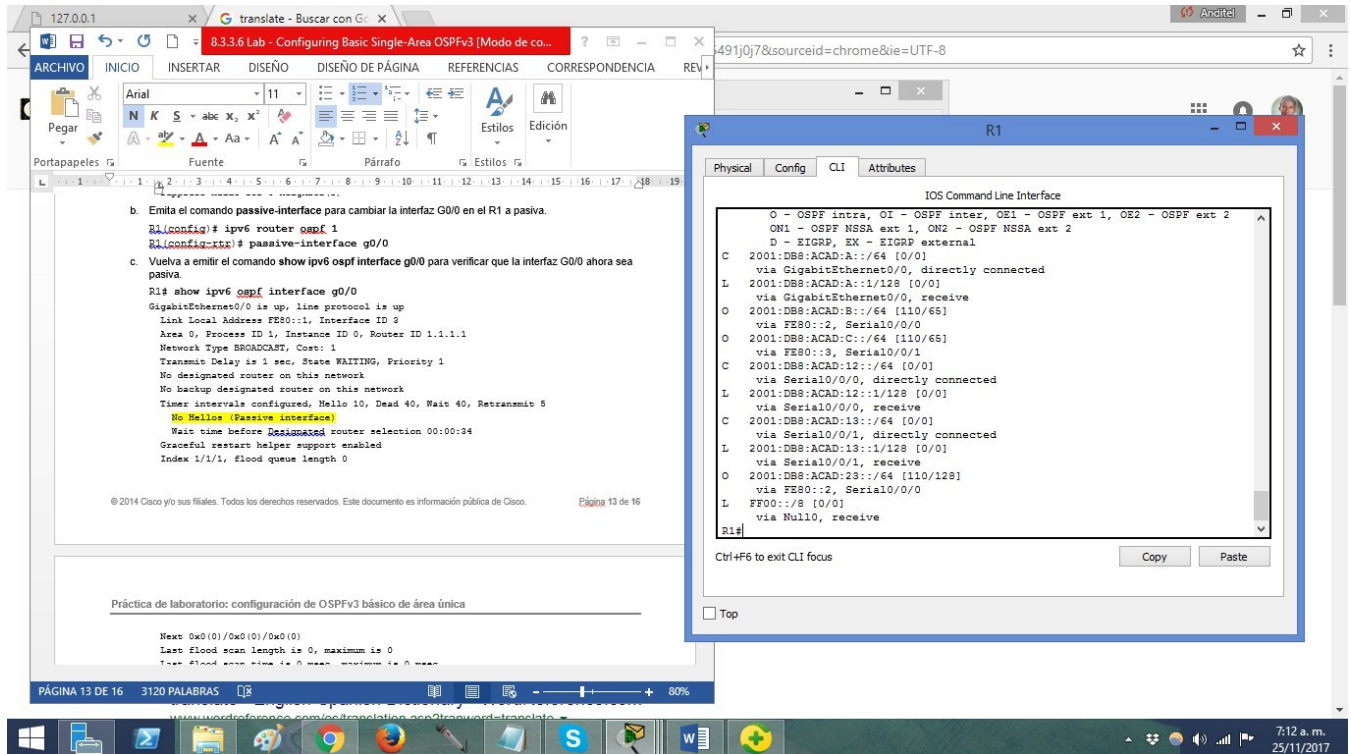
via Serial0/0/1, directly connected

L 2001:DB8:ACAD:23::2/128 [0/0]

via Serial0/0/1, receive

L FF00::/8 [0/0]

via Null0, receive



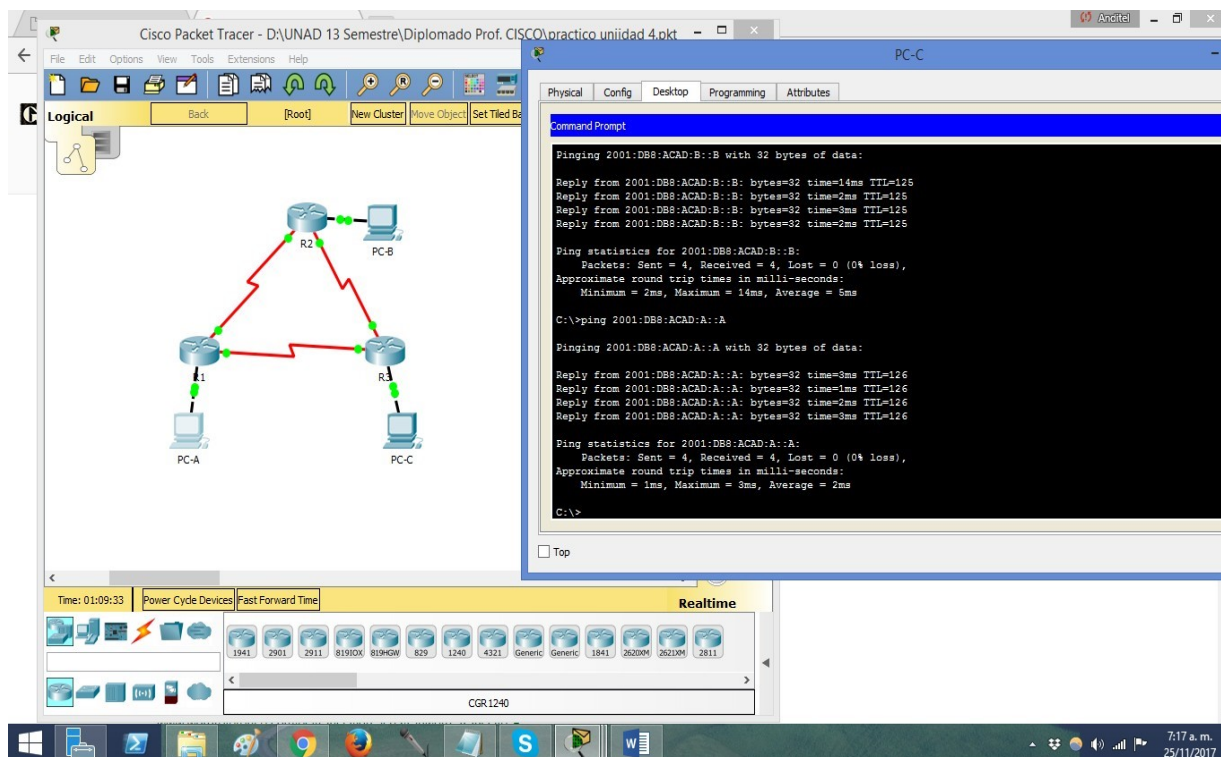
¿Qué comando utilizaría para ver solamente las rutas OSPF en la tabla de routing?

_____ **show** **ipv6** **route**

Step 17: Verificar la conectividad de extremo a extremo.

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

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



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.

Step 18: configurar una interfaz pasiva.

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

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

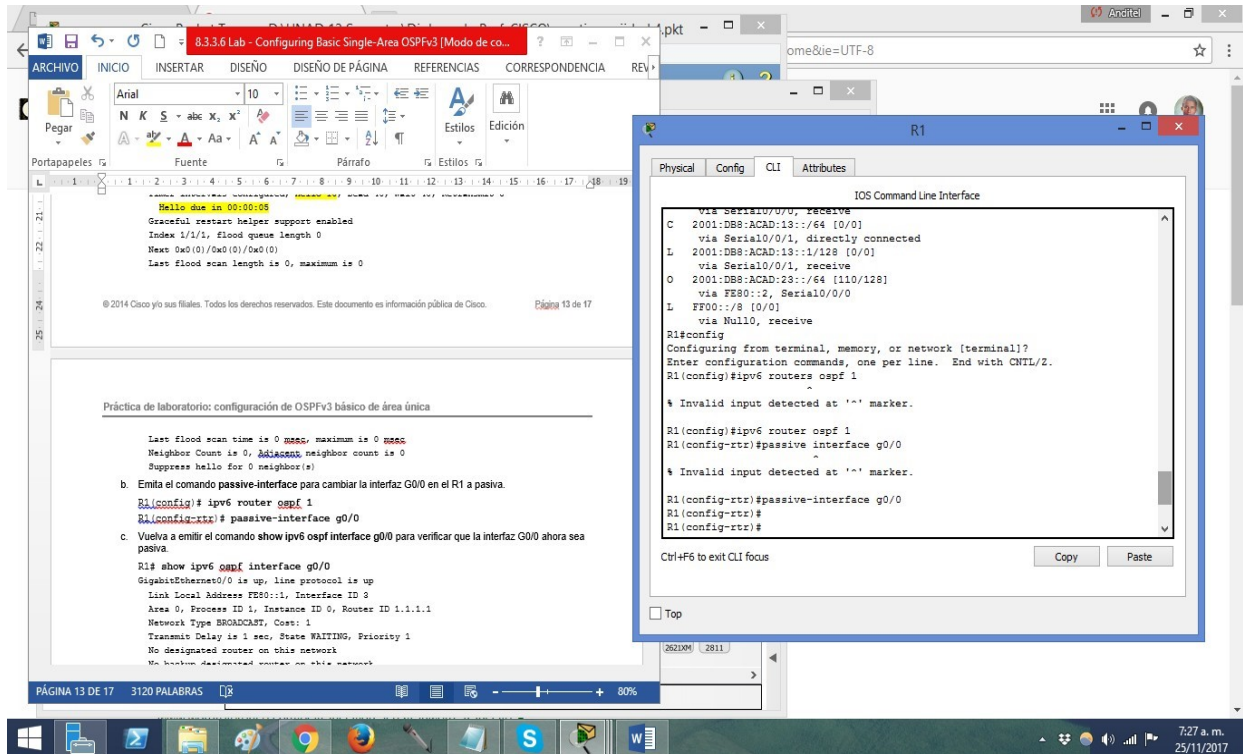
```
GigabitEthernet0/0 is up, line protocol is up
```

Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, local address FE80::1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

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

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

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



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

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

GigabitEthernet0/0 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3

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

Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State WAITING, Priority 1

No designated router on this network

No backup designated router on this network

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

No Hellos (Passive interface)

Wait time before Designated router selection 00:00:34

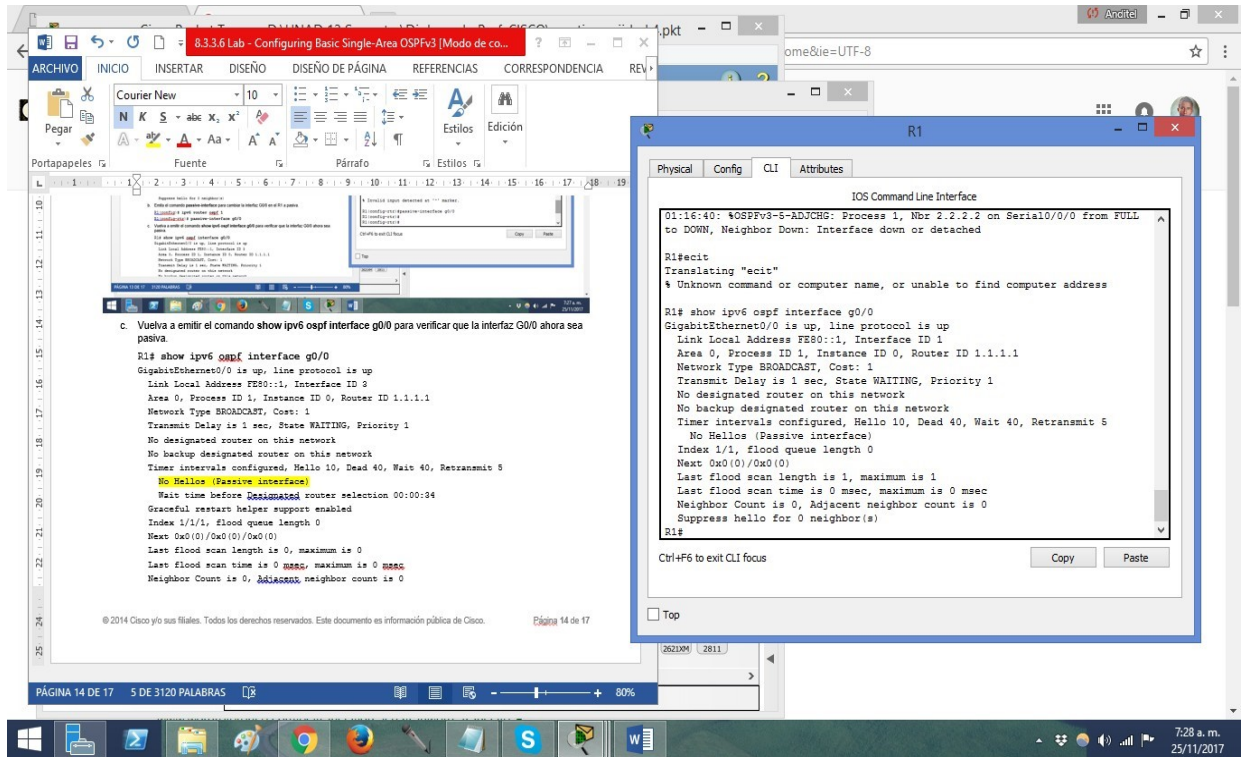
Graceful restart helper support enabled

Index 1/1/1, flood queue length 0

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

Last flood scan length is 0, maximum is 0

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



- 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 - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2

IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

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

O 2001:DB8:ACAD:A::/64 [110/65]

via FE80::1, Serial0/0/0

O 2001:DB8:ACAD:C::/64 [110/65]

via FE80::3, Serial0/0/1
O 2001:DB8:ACAD:13::/64 [110/128]
via FE80::3, Serial0/0/1
via FE80::1, Serial0/0/0

Step 19: establecer la interfaz pasiva como la interfaz predeterminada en el router.

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

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

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

```
R1# show ipv6 ospf neighbor
```

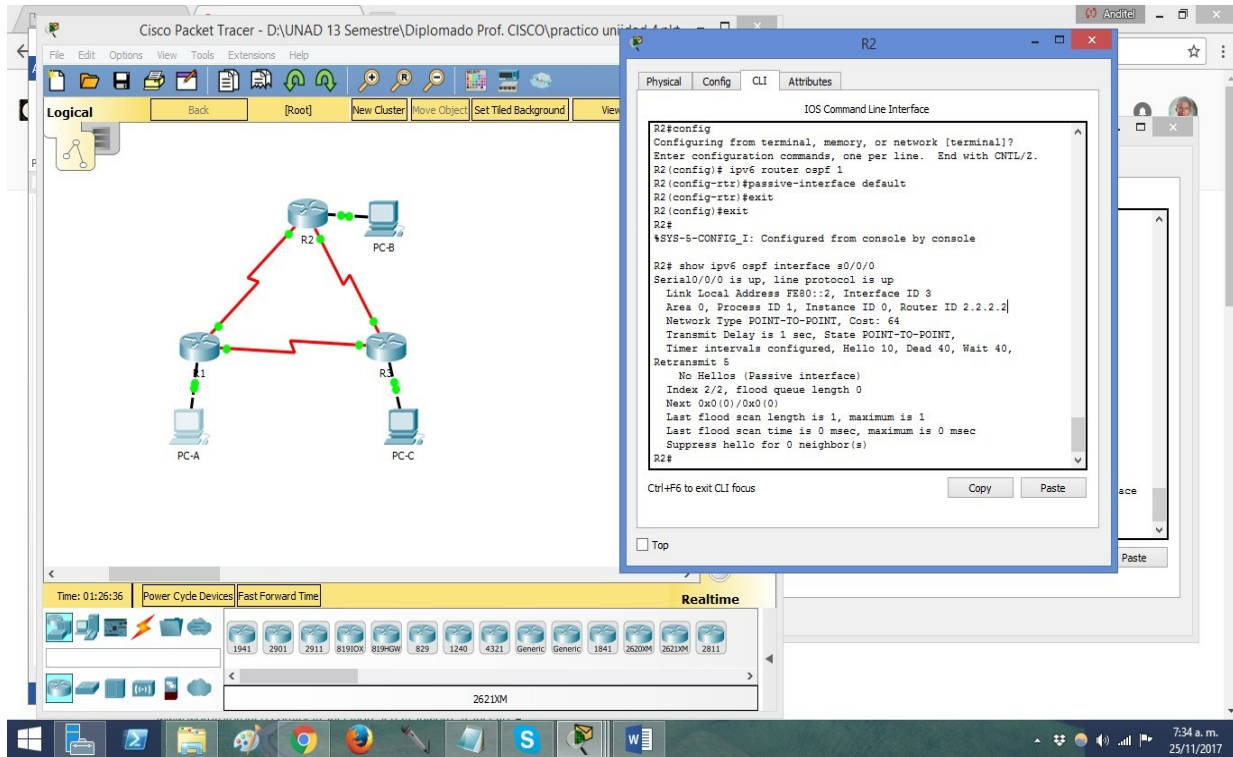
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

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

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

```
R2# show ipv6 ospf interface s0/0/0  
Serial0/0/0 is up, line protocol is up  
Link Local Address FE80::2, Interface ID 6  
Area 0, Process ID 1, Instance ID 0, Router ID 2.2.2.2  
Network Type POINT_TO_POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT_TO_POINT  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
No Hellos (Passive interface)  
Graceful restart helper support enabled  
Index 1/2/2, flood queue length 0  
Next 0x0(0)/0x0(0)/0x0(0)  
Last flood scan length is 2, maximum is 3
```


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



- d. Si todas las interfaces OSPFv3 en el R2 son pasivas, no se anuncia ninguna información de routing. Si este es el caso, el R1 y el R3 ya no deberían tener una ruta a la red 2001:DB8:ACAD:B::/64. Esto se puede verificar mediante el comando **show ipv6 route**.
- e. Ejecute el comando **no passive-interface** para cambiar S0/0/1 en el R2 a fin de que envíe y reciba actualizaciones de routing OSPFv3. Después de introducir este comando, aparece un mensaje informativo que explica que se estableció una adyacencia de vecino con el R3.
- ```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# no passive-interface s0/0/1
*Apr 8 19:21:57.939: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1
from LOADING to FULL, Loading Done
```
- f. Vuelva a emitir los comandos **show ipv6 route** y **show ipv6 ospf neighbor** en el R1 y el R3, y busque una ruta a la red 2001:DB8:ACAD:B::/64.

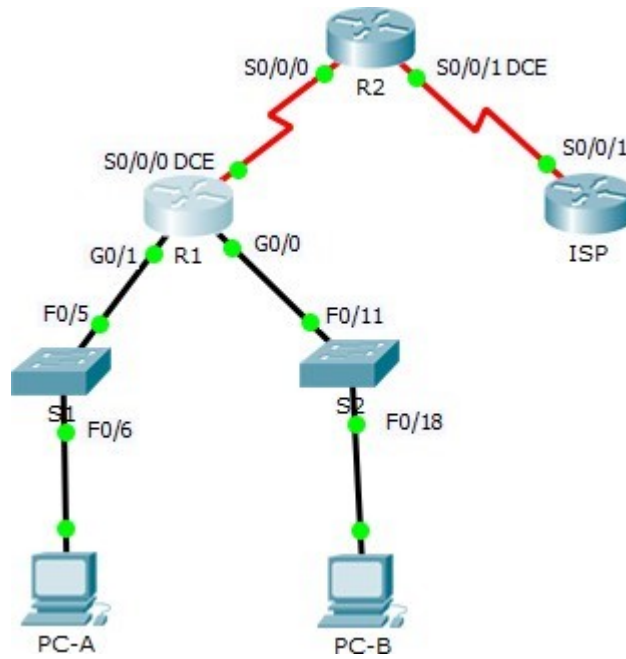
**Tabla de resumen de interfaces del router**

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

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

### 10.1.2.4 LAB - CONFIGURING BASIC DHCPV4 ON A ROUTER.

#### Topología



#### Tabla de direccionamiento

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

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

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

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

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

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

- a. Desactive la búsqueda DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.
- e. Configure **logging synchronous** para evitar que los mensajes de consola interrumpan la entrada de comandos.
- f. Configure las direcciones IP para todas las interfaces de los routers de acuerdo con la tabla de direccionamiento.

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line s0/0/0
^
% Invalid input detected at '^' marker.

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

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

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

R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip add 209.165.200.226 255.255.255.224
R2(config-if)#no shut

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

```
ISP>en
ISP#int s0/0/1
^
% Invalid input detected at '^' marker.

ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/1
ISP(config-if)#ip add 209.165.200.225 255.255.255.224
ISP(config-if)#no shut

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

ISP(config-if)#
```

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

```
Serial0/0/0: incorrect IP address assignment
R1(config-if)#ip add ip 192.168.2.253 255.255.255.252
 ^
% Invalid input detected at '^' marker.

R1(config-if)#int s0/0/0
R1(config-if)#clock rate 12800
Unknown clock rate
R1(config-if)#clock rate 128000
R1(config-if)#ip add 192.168.2.253 255.255.255.252
R1(config-if)#no shut

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

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

R1(config-if)#
```

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

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

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

R2(config-if)#int s0/0/1
R2(config-if)#clock rate 128000
R2(config-if)#ip add 209.165.200.226 255.255.255.224
R2(config-if)#no shut

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

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

R2(config-if)#
```

- h. Configure EIGRP for R1.

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

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

```
R2(config)# router eigrp
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
```

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

```
ISP#config 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

```

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

#### **Step 4: verificar la conectividad de red entre los routers.**

Si algún ping entre los routers falla, corrija los errores antes de continuar con el siguiente paso.

Use los comandos **show ip route** y **show ip interface brief** para detectar posibles problemas.

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

## **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.

#### **Step 6: 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(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

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, ya que el router se encuentra en otra red y no puede pasar el dominio de broadcast por lo tanto no puede pasar el router 1

### **Step 7: configurar el R1 como agente de retransmisión DHCP.**

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

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

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
```

```
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

**Step 8: 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.

- A la PC- A se le asigno la siguiente dirección IP 192.168.1.10 mascara 255.255.255. 0
- A la PC- B se le asigno la siguiente dirección IP 192.168.0.10 mascara 255.255.255. 0

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?

- Según la configuración se excluyó las siguientes direcciones IP 192.168.1.1 - 192.168.1.9, por consiguiente la primera dirección que PC-A puede arrendar es la 192.168.1.10
- Según la configuración se excluyó las siguientes direcciones IP 192.168.0.1 - 192.168.0.9, por consiguiente la primera dirección que PC-B puede arrendar es la 192.168.0.10

**Step 9: 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?

```
Password:
R2#show ip dhcp binding
IP address Client-ID/
 Hardware address Lease expiration Type
192.168.1.10 0040.0B54.782B -- Automatic
192.168.0.10 0030.A3A8.B6AB -- Automatic
```



- b. En el R2, introduzca el comando **show ip dhcp server statistics** para ver la actividad de mensajes y las estadísticas del pool de DHCP.  
¿Cuántos tipos de mensajes DHCP se indican en el resultado?  
No esta implementado en packet tracer
- c. En el R2, introduzca el comando **show ip dhcp pool** para ver la configuración del pool de DHCP.  
En el resultado del comando **show ip dhcp pool**, ¿a qué hace referencia el índice actual (Current index)?  
No esta implementado en packet tracer
- d. En el R2, introduzca el comando **show run | section dhcp** para ver la configuración DHCP en la configuración en ejecución.
- 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.

**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

**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

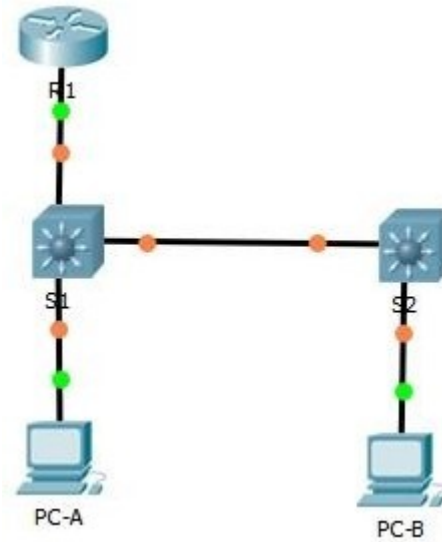
### **Reflexión**

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

Uno de los beneficios de DHCP es que facilita la administración de las direcciones IP, las ventajas de usar agentes de retransmisión de DHCP en lugar de varios routers que funcionen como servidores de DHCP es que consiente en que los router se dediquen a su función de rutear sin afectar su hardware, además permiten una fácil administración de las redes.

## 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      | 209.165.200.225 | 255.255.255.224   |
| S1          | VLAN 1   | 192.168.1.1     | 255.255.255.0     |
|             | VLAN 2   | 192.168.2.1     | 255.255.255.0     |

### Objetivos

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

**Parte 2: cambiar la preferencia de SDM**

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

**Parte 3: configurar DHCPv4**

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

#### **Parte 4: configurar DHCP para varias VLAN**

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

#### **Parte 5: habilitar el routing IP**

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

### **Información básica/situación**

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

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

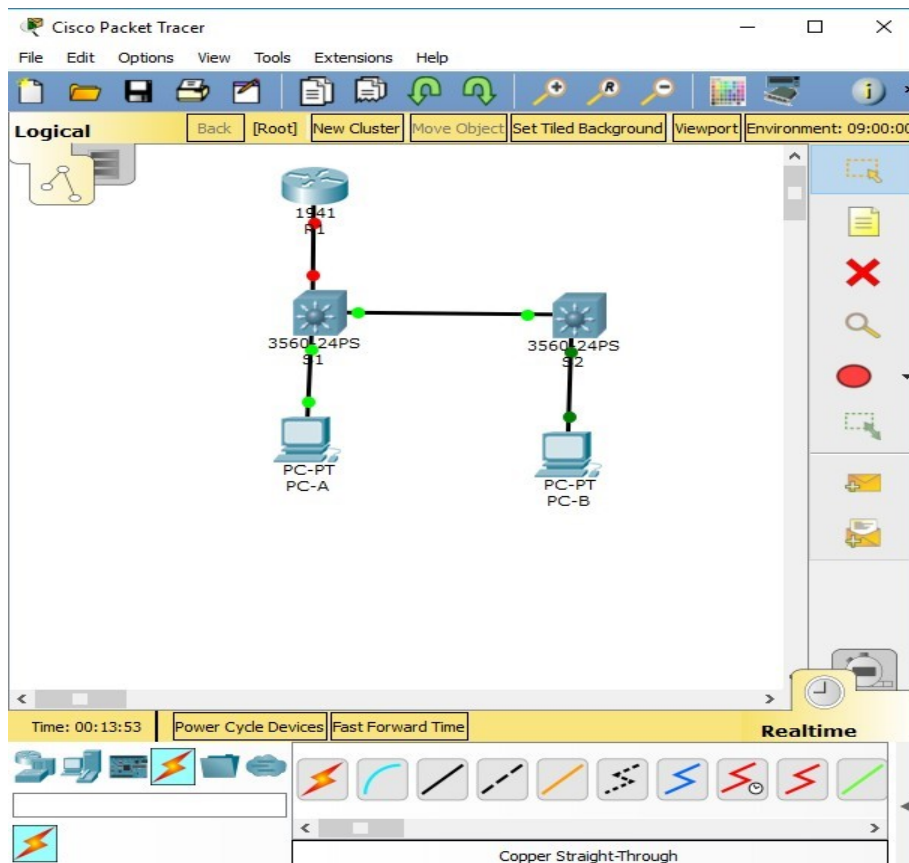
**Nota:** los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se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

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

### Recursos necesarios

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

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



Realizar el cableado de red tal como se muestra en la topología.  
Inicializar y volver a cargar los routers y switches.

Configurar los parámetros básicos en los dispositivos.

- f. Asigne los nombres de dispositivos como se muestra en la topología.
- g. Desactive la búsqueda del DNS.
- h. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.
- i. Configure las direcciones IP en las interfaces G0/1 y Lo0 del R1, según la tabla de direccionamiento.

The screenshot shows the configuration of Router R1 in Cisco Packet Tracer. The CLI window displays the following commands and output:

```
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

Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shut
Router(config-if)#
Router(config-if)#
```

The network diagram shows Router R1 (3560-24PS) connected to PC-A (PC-PT) and PC-B (PC-PT). The environment is set to 12:30:00.

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

The screenshot shows the configuration of Switch S1 in Cisco Packet Tracer. The CLI window displays the following commands and output:

```
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)#
```

The network diagram shows Switch S1 (3560-24PS) connected to PC-A (PC-PT) and PC-B (PC-PT). The environment is set to 05:00:00.

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

## Parte 2: cambiar la preferencia de SDM

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

### Paso 10: mostrar la preferencia de SDM en el S1.

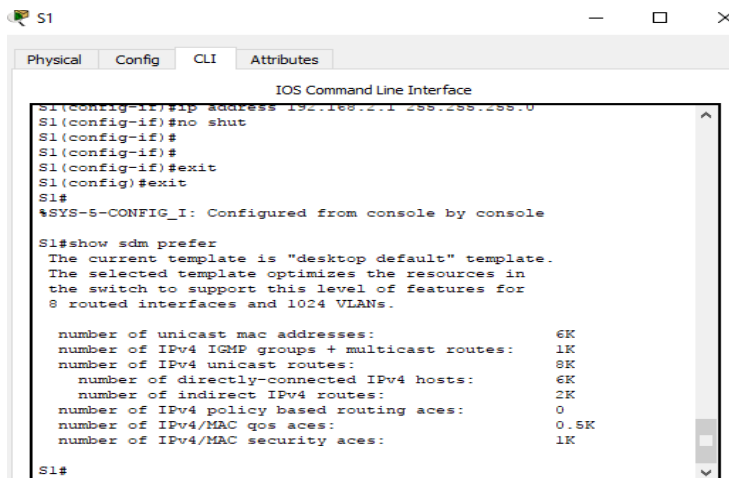
En el S1, emita el comando **show sdm prefer** en modo EXEC privilegiado. Si no se cambió la plantilla predeterminada de fábrica, debería seguir siendo **default**. La plantilla **default** no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será **dual-ipv4-and-ipv6 default**.

```
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
```



```
IOS Command Line Interface
S1(config-if)#ip address 192.168.2.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#
S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 6K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 8K
 number of directly-connected IPv4 hosts: 6K
 number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K
S1#
```

¿Cuál es la plantilla actual?

*RTA// “Desktop default”*

**Paso 11: cambiar la preferencia de SDM en el S1.**

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

S1(config)# **sdm prefer lanbase-routing**

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

¿Qué plantilla estará disponible después de la recarga?

*RTA// “lanbase-routing”*

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

S1# **reload**

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm]

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

**Paso 12: 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

The screenshot shows a terminal window titled 'S1' with tabs for Physical, Config, CLI, and Attributes. The CLI window displays the following text:

```

IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#sdm prefer lanbase-routing
^
% Invalid input detected at '^' marker.

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

S1#show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 6K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 8K
 number of directly-connected IPv4 hosts: 6K
 number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K

S1#

```

At the bottom of the terminal window, there are 'Copy' and 'Paste' buttons.

### Parte 3: configurar DHCPv4

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

### Paso 13: configurar DHCP para la VLAN 1.

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

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

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

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

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

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

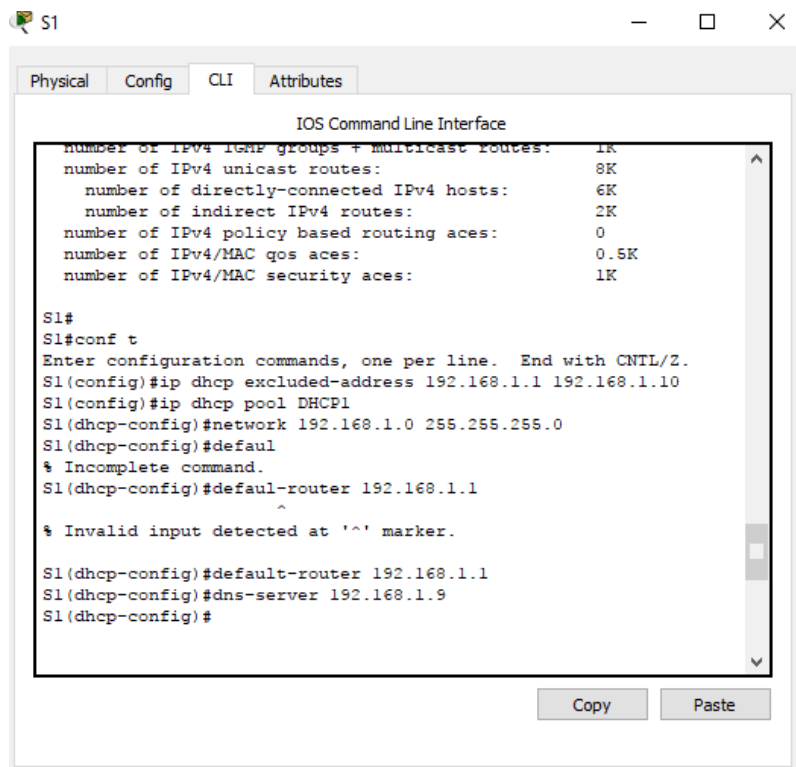
- d. Asigne el gateway predeterminado como 192.168.1.1. En el espacio proporcionado, escriba el comando que utilizó.

```
RTA// 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.

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

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



```
S1
IOS Command Line Interface
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 8K
 number of directly-connected IPv4 hosts: 6K
 number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K

S1#
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)#ip dhcp pool DHCP1
S1(dhcp-config)#network 192.168.1.0 255.255.255.0
S1(dhcp-config)#default
% Incomplete command.
S1(dhcp-config)#default-router 192.168.1.1
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#default-router 192.168.1.1
S1(dhcp-config)#dns-server 192.168.1.9
S1(dhcp-config)#
```

#### Paso 14: 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

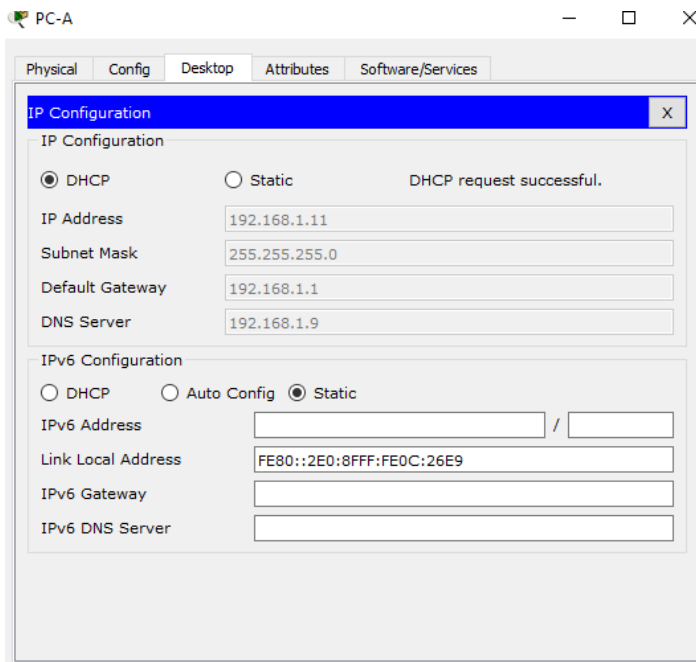
Gateway predeterminado: 192.168.1.1

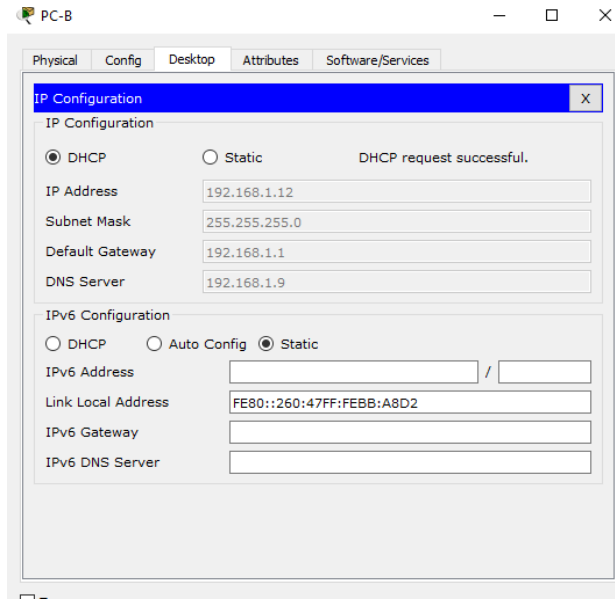
Para la PC-B, incluya lo siguiente:

Dirección IP: 192.168.1.12

Máscara de subred: 255.255.255.0

Gateway predeterminado: 192.168.1.9





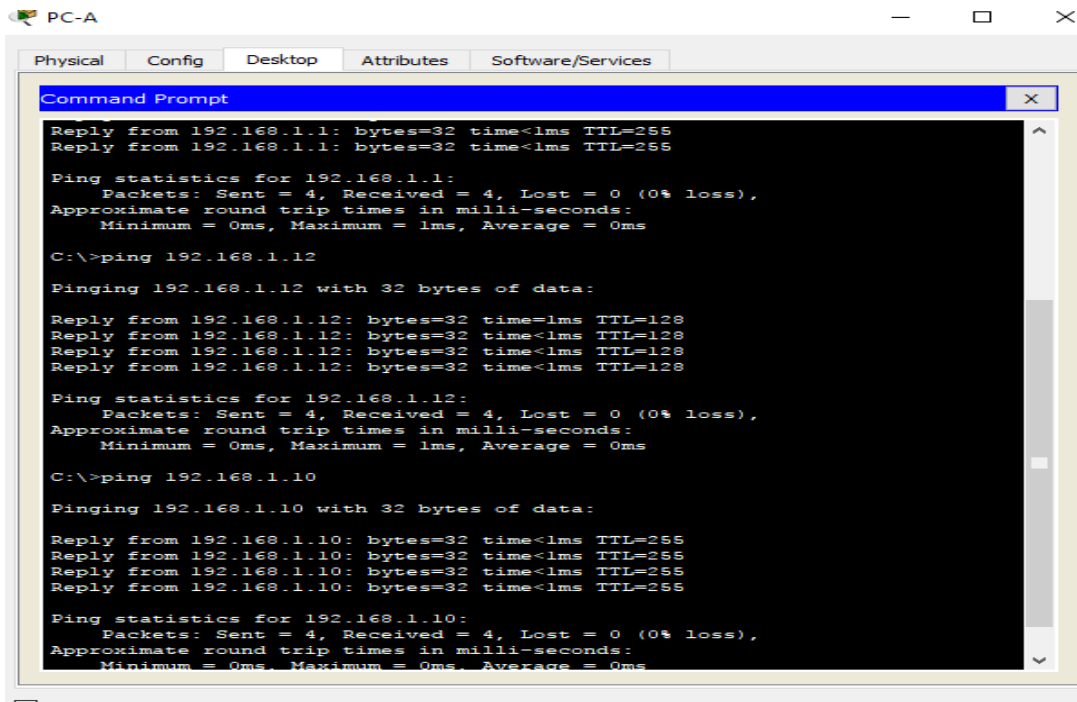
b. Pruebe la conectividad haciendo ping de la PC-A al gateway predeterminado, la PC-B y el R1.

¿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.



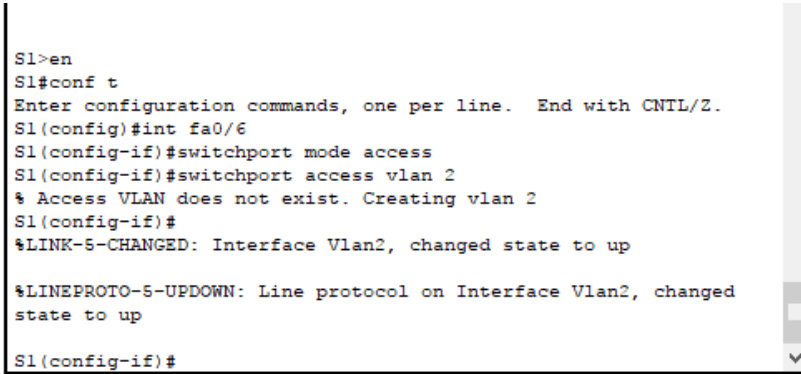
## Parte 4: configurar DHCPv4 para varias VLAN

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

### Paso 15: 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.

```
RTA// S1(config)#int fa0/6
 S1(config-if)#switchport mode access
 S1(config-if)#switchport access vlan 2
```



```
S1>en
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed
state to up
S1(config-if)#
```

Copy Paste

### Paso 16: configurar DHCPv4 para la VLAN 2.

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

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

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

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

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

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

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

*RTA// S1(dhcp-config)#default-router 192.168.2.1*

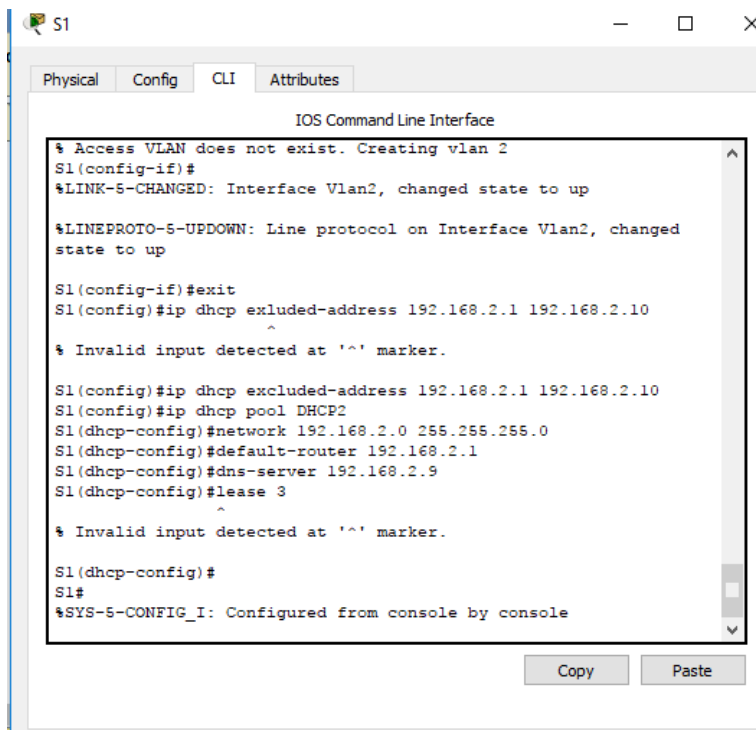
- e. Asigne el servidor DNS como 192.168.2.9. En el espacio proporcionado, escriba el comando que utilizó.

*RTA// 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.

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

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



```
% Access VLAN does not exist. Creating vlan 2
S1(config-if)#
%LINK-S-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-S-UPDOWN: Line protocol on Interface Vlan2, changed
state to up

S1(config-if)#exit
S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
^
% Invalid input detected at '^' marker.

S1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)#ip dhcp pool DHCP2
S1(dhcp-config)#network 192.168.2.0 255.255.255.0
S1(dhcp-config)#default-router 192.168.2.1
S1(dhcp-config)#dns-server 192.168.2.9
S1(dhcp-config)#lease 3
^
% Invalid input detected at '^' marker.

S1(dhcp-config)#
S1#
%SYS-S-CONFIG_I: Configured from console by console
```

### Paso 17: 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?

***RTA// La puerta de enlace de la PC-A esta en la misma red por lo tanto el ping es satisfactorio y el otro no.***

---

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

¿Qué resultado arrojó este comando?

***RTA// No hay una puerta de enlace que ha sido establecida y no hay una tabla de ruteo en el switch***

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

Host Gateway Last Use Total Uses
Interface

ICMP redirect cache is empty

S1#
```

Copy Paste

## Parte 5: habilitar el routing IP

En la parte 5, habilitará el routing IP en el switch, que permitirá la comunicación entre VLAN.

Para que todas las redes se comuniquen, se deben implementar rutas estáticas en el S1 y el R1.

### Paso 18: 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?

***RTA// El switch esta enrutando los paquetes de todas las 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?

**RTA//** El switche exhibe una tabla de ruteo mostrando las vlans directamente conectadas.

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

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

**RTA//** El router muestra dos redes directamente conectadas, pero no tienen una entrada para la red dos.

- 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?

**RTA//** Para que se dé la comunicación se debe las rutas deben ser agregadas en la tabla de ruteo.

### **Paso 19: 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.

**RTA//** S1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.10

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

**RTA//** 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?

**RTA//** Es el Gateway como último recurso



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

¿Cómo está representada la ruta estática?

*RTA// Está representada la ruta estática 192.168.2.0 conectada a la g0/1*

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

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

### **Reflexión**

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

RTA// Si las direcciones estáticas se excluyeron antes de que se creara el grupo DHCPv4, existe una ventana de tiempo en la que las direcciones excluidas podrían distribuirse dinámicamente

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

RTA// El interruptor asignará configuraciones de IP basadas en la asignación de VLAN del puerto al que está conectado el host

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

RTA// El interruptor puede funcionar como un servidor DHCP y puede realizar rutas estáticas e inter-VLAN

### **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

### 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.

### 10.2.3.5 LAB - CONFIGURING STATELESS AND STATEFUL DHCPV6

Topología

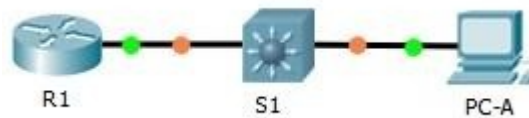


Tabla de direccionamiento

| 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      |

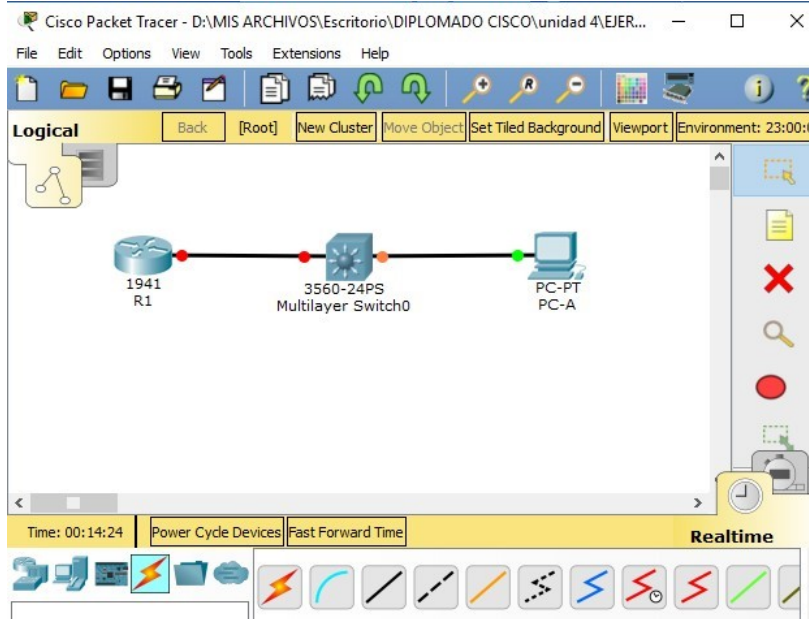
#### Objetivos

**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.

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

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

**Step 20: realizar el cableado de red tal como se muestra en la topología.**

**Step 21: inicializar y volver a cargar el router y el switch según sea necesario.**

**Step 22: Configurar R1**

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

**Step 23: configurar el S1.**

- Desactive la búsqueda del DNS.
- Configure el nombre del dispositivo.
- Cifre las contraseñas de texto no cifrado.
- Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

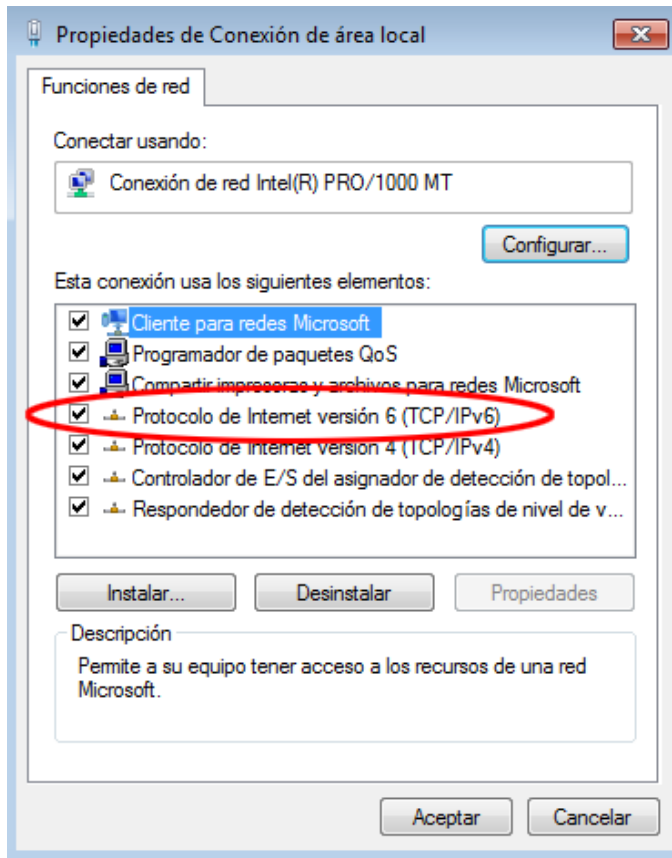
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

## Parte 2: configurar la red para SLAAC

### Step 24:

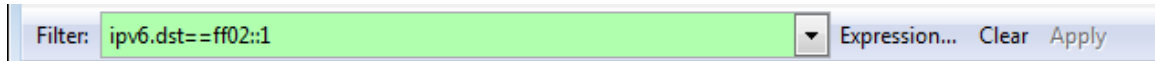
### Step 25: preparar la PC-A.

- 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.



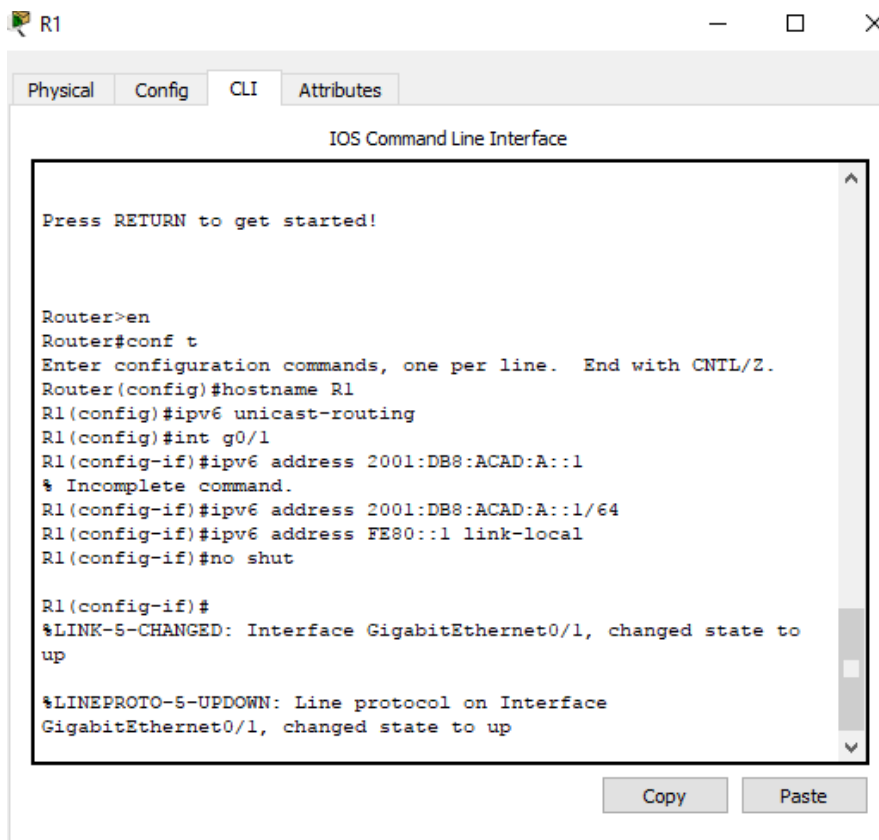
- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de

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 26: 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.



### Step 27: 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.

The screenshot shows a network device CLI window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The output of the command `R1#show ipv6 interface g0/1` is shown in a scrollable text area. The output indicates that IPv6 is enabled on GigabitEthernet0/1 with a link-local address of FE80::1. It also shows global unicast addresses: 2001:DB8:ACAD:A::1 (subnet 2001:DB8:ACAD:A::/64) and FF02::1. The interface MTU is 1500 bytes, and various ICMP and ND settings are listed. The prompt `R1#` is visible at the bottom of the text area. Below the text area are "Copy" and "Paste" buttons.

```
%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
 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
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
```

### Step 28: 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
```

### Step 29: 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)

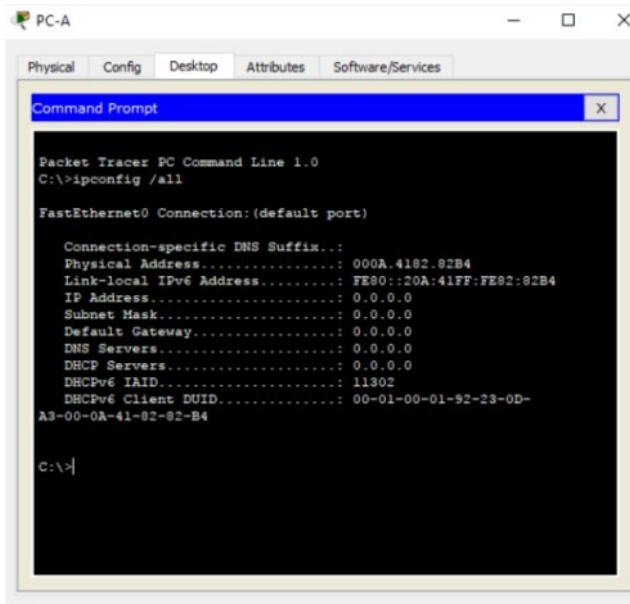
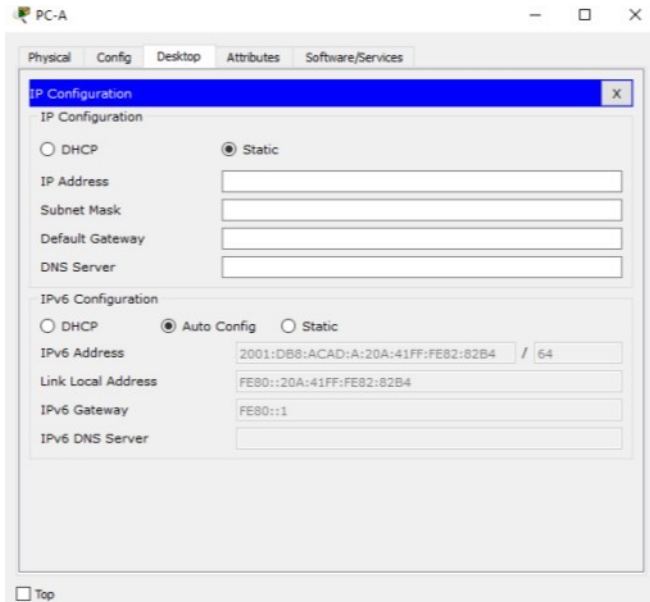
ND NS retransmit interval is 1000 milliseconds

Default router is FE80::1 on Vlan1

**Step 30: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-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.

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



- 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.

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

| No.  | Time       | Source  | Destination | Protocol | Length | Info                                        |
|------|------------|---------|-------------|----------|--------|---------------------------------------------|
| 3346 | 3013.20590 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 3518 | 3972.07973 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 3673 | 4130.43155 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 3840 | 4284.68370 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 3989 | 4435.87602 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |

Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), 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 version 6
  - Type: Router Advertisement (134)
  - Code: 0
  - Checksum: 0x1816 [correct]
  - Cur hop limit: 64
  - Flags: 0x00
    - 0... .. = Managed address configuration: Not set
    - .0... .. = Other configuration: Not set
    - ..0... .. = Home Agent: Not set
    - ...0... = Prf (Default Router Preference): Medium (0)
    - ....0.. = Proxy: Not set
    - ....0. = Reserved: 0
  - Router lifetime (s): 1800
  - Reachable time (ms): 0
  - Retrans timer (ms): 0
  - ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
  - ICMPv6 Option (MTU : 1500)
  - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
    - Type: Prefix information (3)
    - Length: 4 (32 bytes)
    - Prefix Length: 64
    - Flag: 0xc0
    - Valid Lifetime: 2592000
    - Preferred Lifetime: 604800
    - Reserved
    - Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

### Parte 3: configurar la red para DHCPv6 sin estado

#### Step 31: 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.

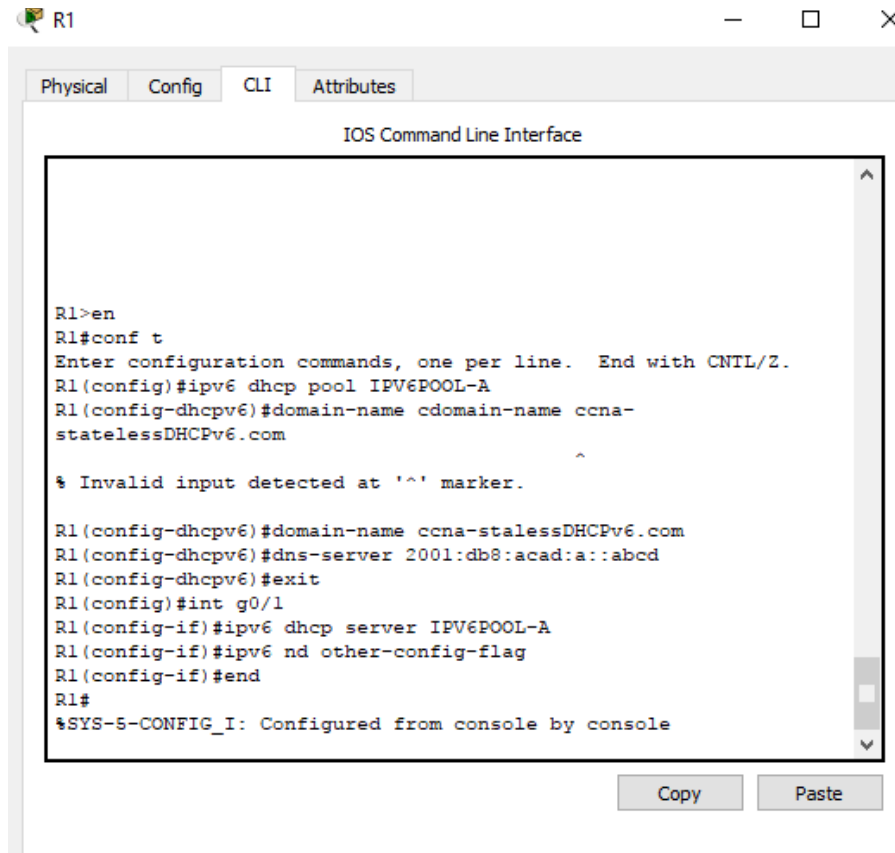
```
R1(config)# interface g0/1
```

```
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
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#domain-name cdomain-name ccna-
statelessDHCPv6.com
^
% Invalid input detected at '^' marker.

R1(config-dhcpv6)#domain-name ccna-stalessDHCPv6.com
R1(config-dhcpv6)#dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)#exit
R1(config)#int g0/1
R1(config-if)#ipv6 dhcp server IPV6POOL-A
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

**Step 32: 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
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#
```

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.

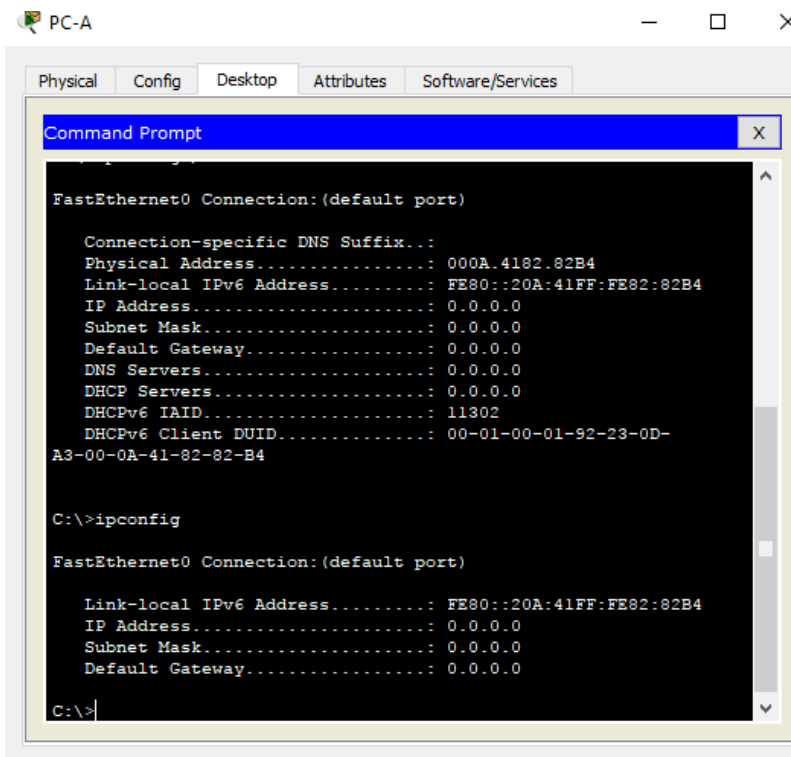
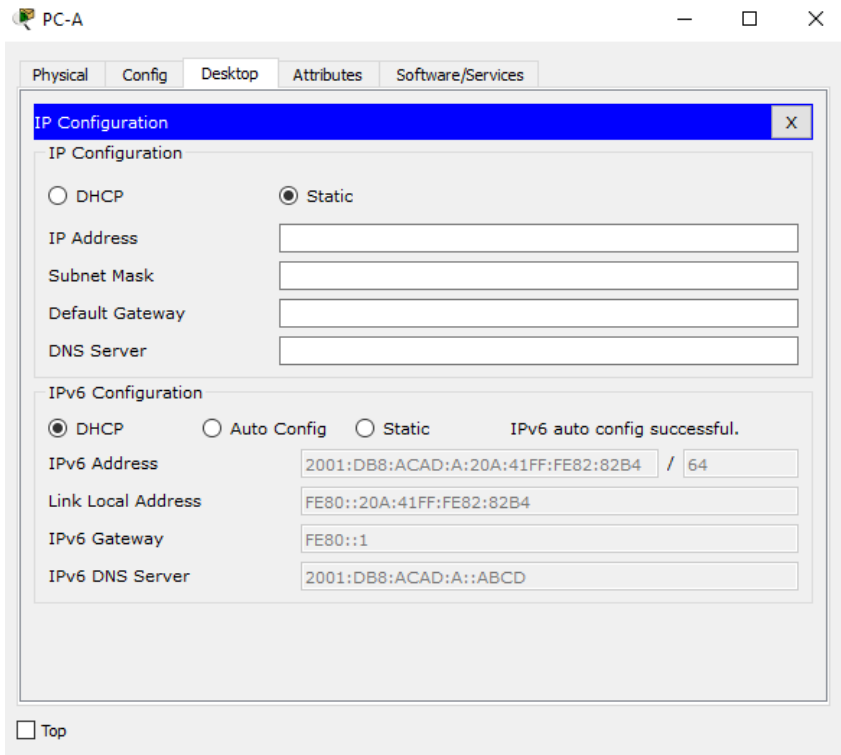
### Step 33: ver los cambios realizados en la red en la PC-A.

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

```
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
Descripción : Conexión de red Intel(R) PRO/1000
MT
Dirección física. : 00-0C-29-E3-23-17
DHCP habilitado : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>
Dirección IPv4. : 192.168.96.139<Preferido>
Máscara de subred : 255.255.255.0
Puerta de enlace predeterminada : fe80::1%11
IAID DHCPv6 : 234884137
DUID de cliente DHCPv6. : 00-01-00-01-19-A7-DD-BE-00-0C-29-03-17
Servidores DNS. : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. : habilitado

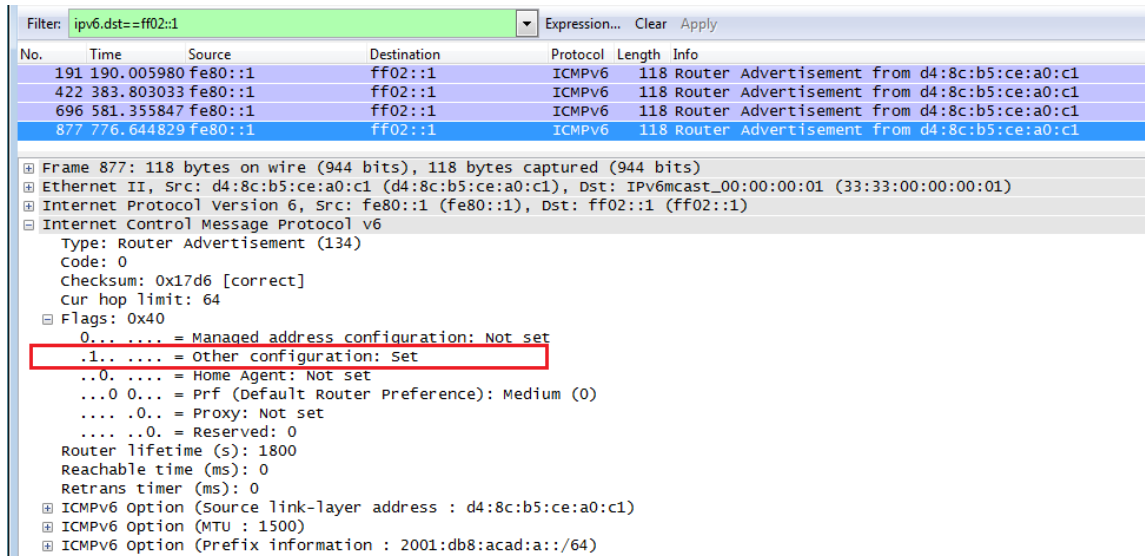
Adaptador de túnel isatap.localdomain:
Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
Descripción : Adaptador ISATAP de Microsoft
Dirección física. : 00-00-00-00-00-00-00-E0
DHCP habilitado : no
Configuración automática habilitada .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





### Step 34: 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.



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

| No. | Time       | Source  | Destination | Protocol | Length | Info                                        |
|-----|------------|---------|-------------|----------|--------|---------------------------------------------|
| 191 | 190.005980 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 422 | 383.803033 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 696 | 581.355847 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 877 | 776.644829 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), 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: 0x17d6 [correct]
  - cur hop limit: 64
  - Flags: 0x40
    - 0... .. = Managed address configuration: Not 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
  - Reachable time (ms): 0
  - Retrans timer (ms): 0
  - ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
  - ICMPv6 Option (MTU : 1500)
  - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)

### Step 35: 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
```

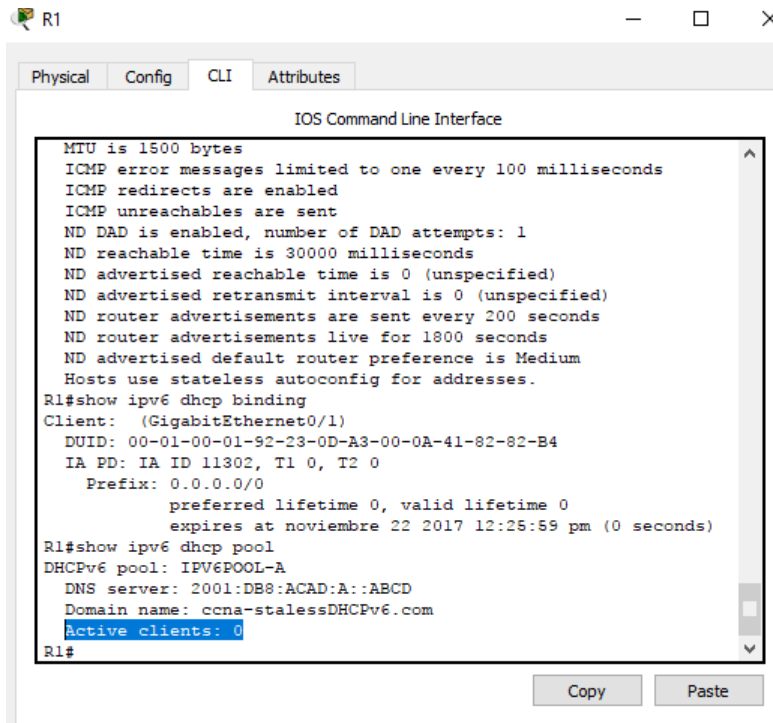
```
R1# show ipv6 dhcp pool
```

```
DHCPv6 pool: IPV6POOL-A
```

```
DNS server: 2001:DB8:ACAD:A::ABCD
```

```
Domain name: ccna-statelessDHCPv6.com
```

```
Active clients: 0
```



The screenshot shows a Cisco IOS CLI window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The output of the command `R1#show ipv6 dhcp binding` is shown, including details for a client on GigabitEthernet0/1, such as DUID, IA PD, and prefix. Below this, the output of `R1#show ipv6 dhcp pool` is displayed, showing the DHCPv6 pool name "IPV6POOL-A", DNS server, domain name, and active clients count (0). The prompt `R1#` is visible at the bottom of the terminal window.

```
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#show ipv6 dhcp binding
Client: (GigabitEthernet0/1)
DUID: 00-01-00-01-92-23-0D-A3-00-0A-41-82-82-B4
IA PD: IA ID 11302, T1 0, T2 0
Prefix: 0.0.0.0/0
 preferred lifetime 0, valid lifetime 0
 expires at noviembre 22 2017 12:25:59 pm (0 seconds)
R1#show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-stalessDHCPv6.com
Active clients: 0
R1#
```

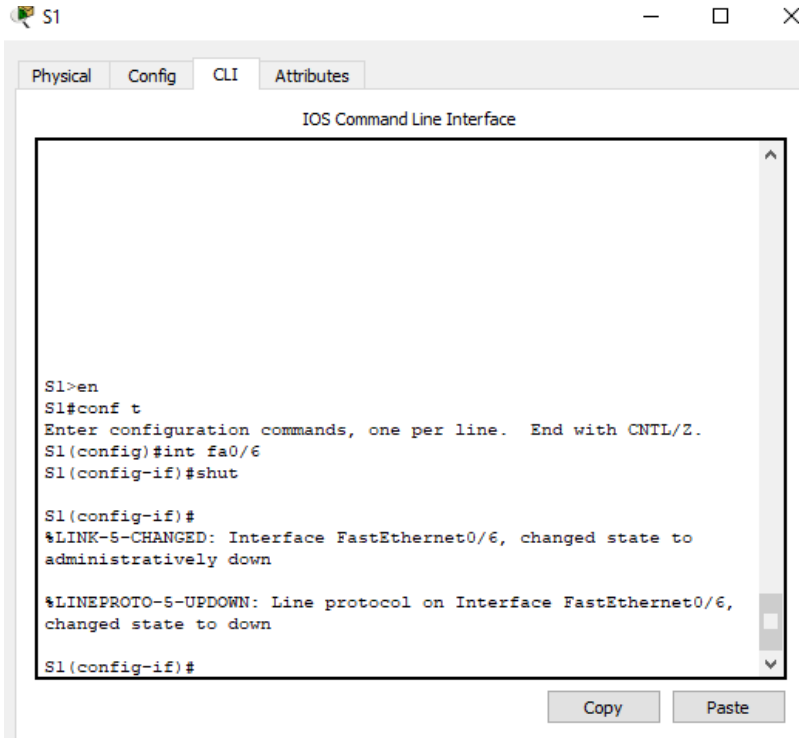
**Step 36: restablecer la configuración de red IPv6 de la PC-A.**

- 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**



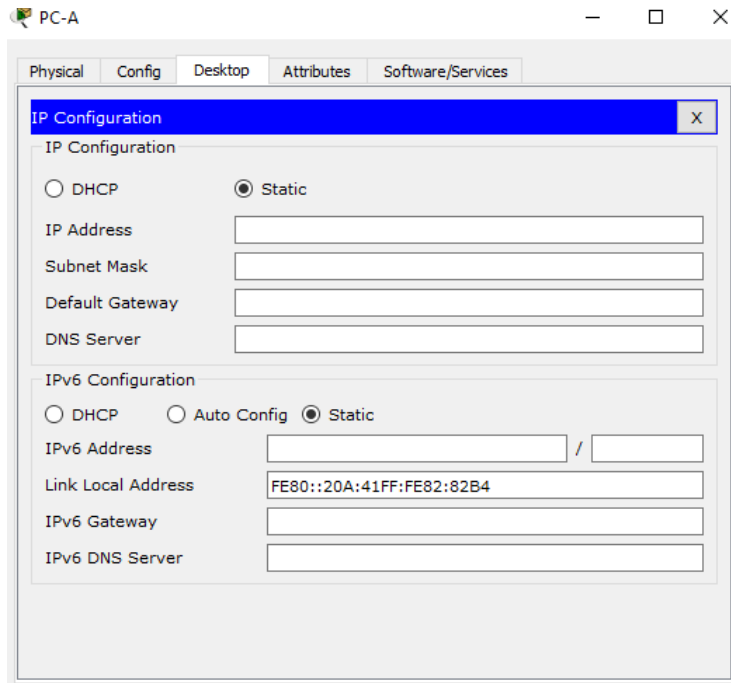
```
S1>en
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int fa0/6
S1(config-if)#shut

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

S1(config-if)#
```

- 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.

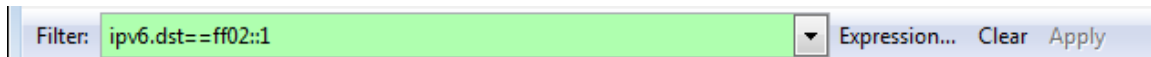


- 2) Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

## Parte 4: configurar la red para DHCPv6 con estado

### Step 37: preparar la PC-A.

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



### Step 38: cambiar el pool de DHCPv6 en el R1.

- a. Agregue el prefijo de red al pool.  

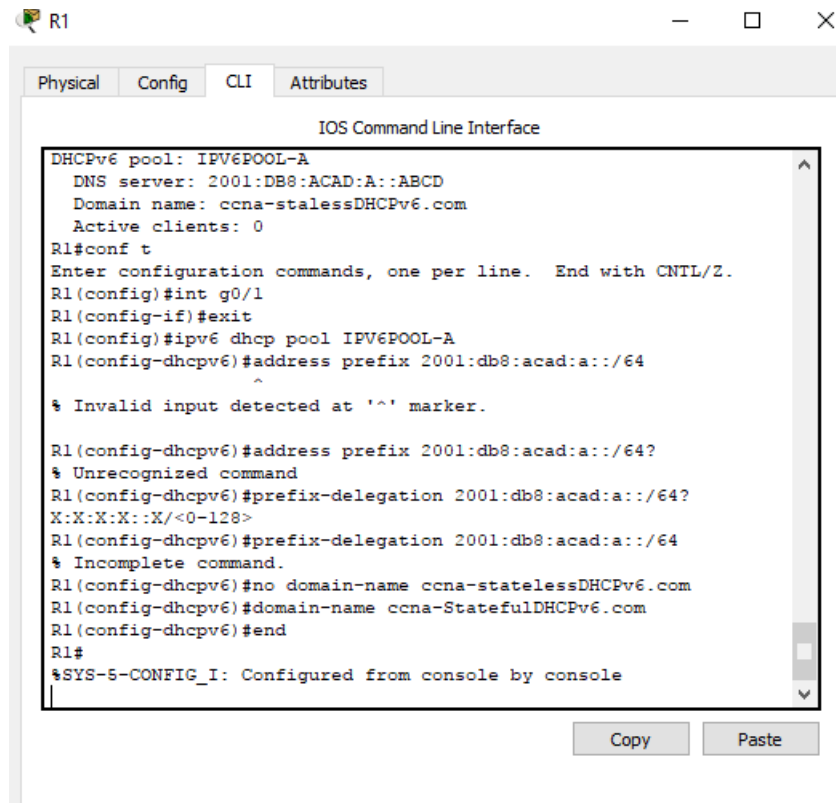
```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```
- b. Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

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

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

```
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
```

```
R1(config-dhcpv6)# end
```



```
R1
IOS Command Line Interface
DHCPv6 pool: IPV6POOL-A
 DNS server: 2001:DB8:ACAD:A::ABCD
 Domain name: ccna-stalessDHCPv6.com
 Active clients: 0
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#exit
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64?
% Unrecognized command
R1(config-dhcpv6)#prefix-delegation 2001:db8:acad:a::/64?
X:X:X:X::X/<0-128>
R1(config-dhcpv6)#prefix-delegation 2001:db8:acad:a::/64
% Incomplete command.
R1(config-dhcpv6)#no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)#domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

c. Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
```

```
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
R1(config)#int g0/1
R1(config-if)#exit
R1(config)#ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64
^
% Invalid input detected at '^' marker.

R1(config-dhcpv6)#address prefix 2001:db8:acad:a::/64?
% Unrecognized command
R1(config-dhcpv6)#prefix-delegation 2001:db8:acad:a::/64?
X:X:X:X:X/<0-128>
R1(config-dhcpv6)#prefix-delegation 2001:db8:acad:a::/64
% Incomplete command.
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

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

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

```
R1# debug ipv6 dhcp detail
```

```
IPv6 DHCP debugging is on (detailed)
```

```
DHCPv6 pool: IPV6POOL-A
 DNS server: 2001:DB8:ACAD:A::ABCD
 Domain name: ccna-StatefulDHCPv6.com
 Active clients: 0
R1#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R1#
```

**Step 39: 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

Physical Config CLI Attributes

IOS Command Line Interface

```
R1(config)#int g0/1
R1(config-if)#shut

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 shut

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

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

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

R1#
```

Copy Paste



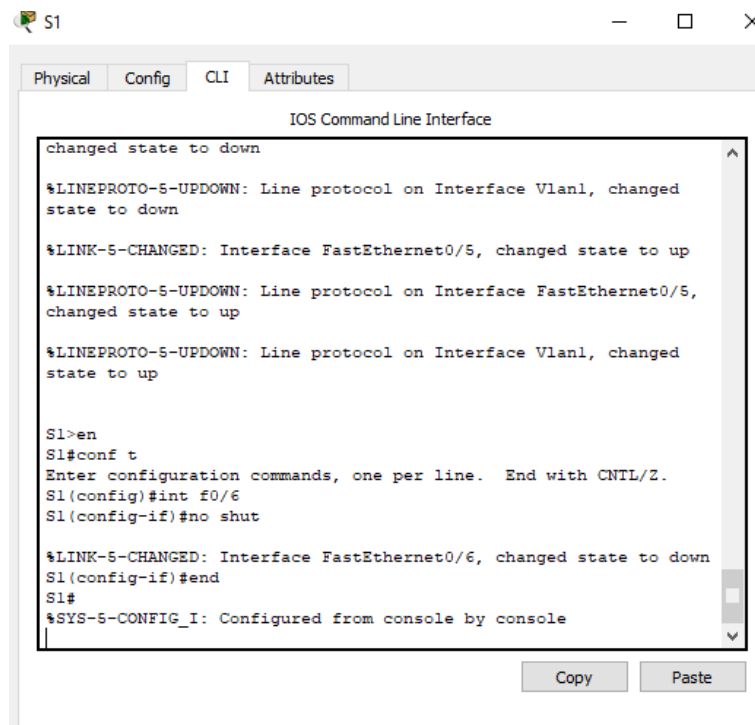
#### Step 40: habilitar la interfaz F0/6 en el S1.

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
```



#### Step 41: 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)

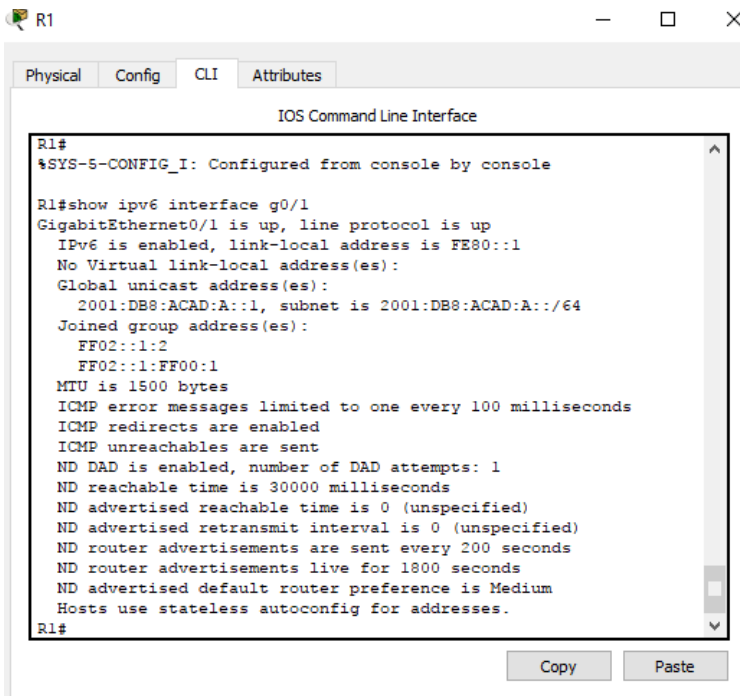
ND router advertisements are sent every 200 seconds

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.



The screenshot shows a terminal window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The active tab is "CLI", displaying the "IOS Command Line Interface". The output of the command "R1#show ipv6 interface g0/1" is as follows:

```
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#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

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.

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
```

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

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

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

```
DUID: 0001000117F6723D000C298D5444
```

```
Username : unassigned
```

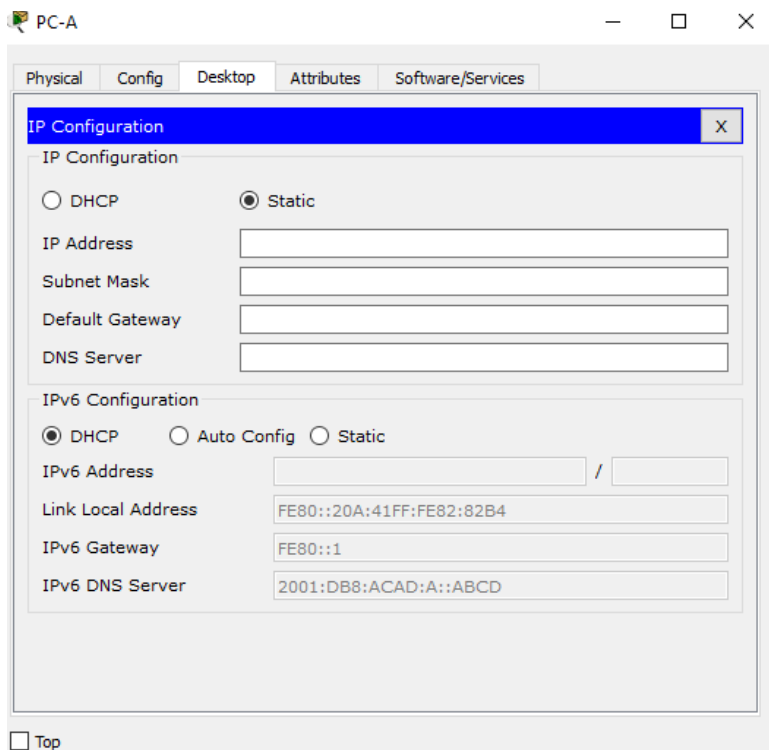
```
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
```

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

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

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

```
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . . : ccna-StatefulDHCPv6.com
Descripción : Conexión de red Intel(R) PRO/1000
MT
Dirección física. : 00-0C-29-E3-23-17
DHCP habilitado : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
Concesión obtenida. : jueves, 05 de septiembre de 2013
La concesión expira : jueves, 05 de septiembre de 2013
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 **undebug all** en el R1 para detener la depuración de DHCPv6.

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

R1# **u all**

Se ha desactivado toda depuración posible

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)
```

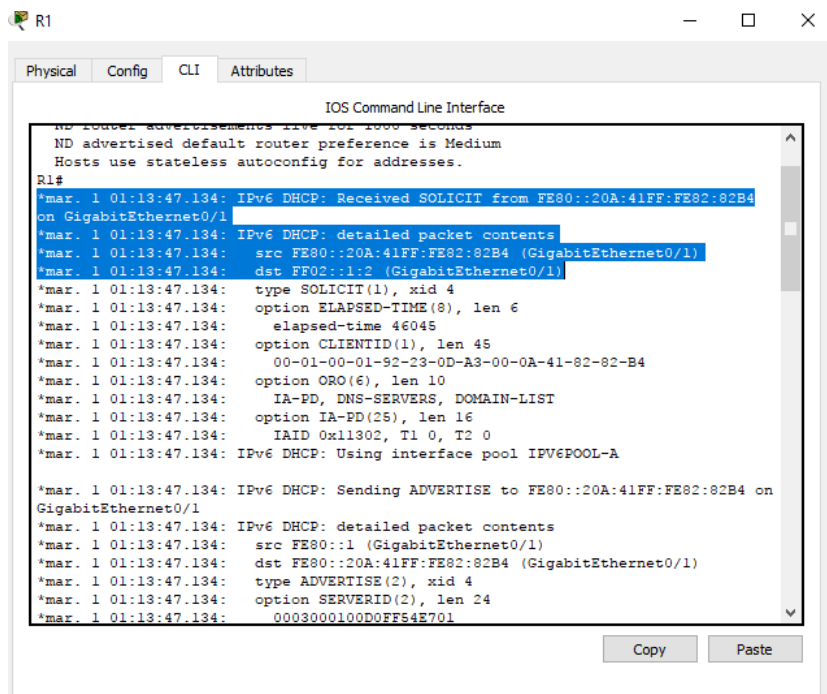
```
*Mar 5 16:42:39.775: dst FF02::1:2
```

```
*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
Physical Config CLI Attributes
IOS Command Line Interface
ND router advertisements live for 1000 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
R1#
*Mar 1 01:13:47.134: IPv6 DHCP: Received SOLICIT from FE80::20A:41FF:FE82:82B4
on GigabitEthernet0/1
*Mar 1 01:13:47.134: IPv6 DHCP: detailed packet contents
*Mar 1 01:13:47.134: src FE80::20A:41FF:FE82:82B4 (GigabitEthernet0/1)
*Mar 1 01:13:47.134: dst FF02::1:2 (GigabitEthernet0/1)
*Mar 1 01:13:47.134: type SOLICIT(1), xid 4
*Mar 1 01:13:47.134: option ELAPSED-TIME(8), len 6
*Mar 1 01:13:47.134: elapsed-time 46045
*Mar 1 01:13:47.134: option CLIENTID(1), len 45
*Mar 1 01:13:47.134: 00-01-00-01-92-23-0D-A3-00-0A-41-82-82-B4
*Mar 1 01:13:47.134: option ORO(6), len 10
*Mar 1 01:13:47.134: IA-PD, DNS-SERVERS, DOMAIN-LIST
*Mar 1 01:13:47.134: option IA-PD(25), len 16
*Mar 1 01:13:47.134: IAID 0x11302, T1 0, T2 0
*Mar 1 01:13:47.134: IPv6 DHCP: Using interface pool IPV6POOL-A
*Mar 1 01:13:47.134: IPv6 DHCP: Sending ADVERTISE to FE80::20A:41FF:FE82:82B4 on
GigabitEthernet0/1
*Mar 1 01:13:47.134: IPv6 DHCP: detailed packet contents
*Mar 1 01:13:47.134: src FE80::1 (GigabitEthernet0/1)
*Mar 1 01:13:47.134: dst FE80::20A:41FF:FE82:82B4 (GigabitEthernet0/1)
*Mar 1 01:13:47.134: type ADVERTISE(2), xid 4
*Mar 1 01:13:47.134: option SERVERID(2), len 24
*Mar 1 01:13:47.134: 0003000100D0FF54E701
```

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
```

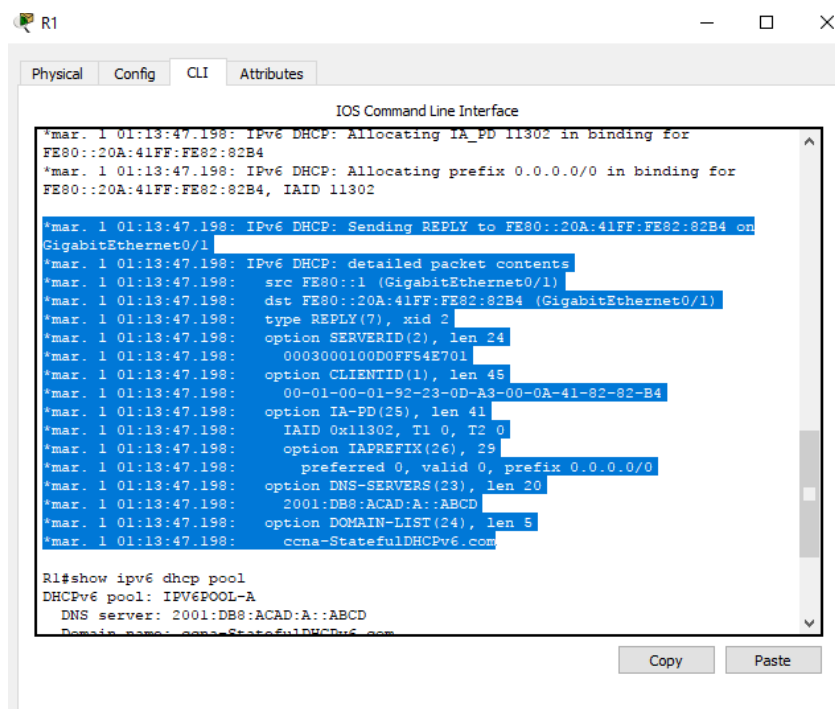
```
*Mar 5 16:42:39.779: src FE80::1
```

```
*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

```



## Step 42: verificar DHCPv6 con estado en la PC-A.

- Detenga la captura de Wireshark en la PC-A.

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

Filter: `ipv6.dst==ff02::1`

| 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 ... = 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.

Filter: `dhcpv6`

| No. | Time       | Source                       | Destination                  | Protocol | Length | Info                                                      |
|-----|------------|------------------------------|------------------------------|----------|--------|-----------------------------------------------------------|
| 250 | 443.078236 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c298d5444   |
| 267 | 475.083284 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c298d5444   |
| 425 | 656.281211 | fe80::d428:7de2:997ff02::1:2 | ff02::1:2                    | DHCPv6   | 146    | Solicit XID: 0xc86c32 CID: 0001000117f6723d000c298d5444   |
| 429 | 656.282249 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Advertise XID: 0xc86c32 CID: 0001000117f6723d000c298d5444 |
| 460 | 657.292018 | fe80::d428:7de2:997ff02::1:2 | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 188    | Request XID: 0xc86c32 CID: 0001000117f6723d000c298d5444   |
| 462 | 657.292638 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Reply XID: 0xc86c32 CID: 0001000117f6723d000c298d5444     |

Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware\_be:6c:89 (00:50:56:be:6c:89)

Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)

User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)

DHCPv6

- Message type: Reply (7)
- Transaction ID: 0xc86c32
- Server Identifier: 00030001fc994775c3e0
- Client Identifier: 0001000117f6723d000c298d5444
- Identity Association for Non-temporary Address
  - Option: Identity Association for Non-temporary Address (3)
    - Length: 40
    - Value: 0e000c290000a8c000010e000005001820010db8acad000a...
    - IAID: 0e000c29
    - T1: 43200
    - T2: 69120
    - IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce
  - DNS recursive name server
    - Option: DNS recursive name server (23)
    - Length: 16
    - Value: 20010db8acad000a000000000000abcd
    - DNS servers address: 2001:db8:acad:a:abcd
  - Domain Search List
    - Option: Domain Search List (24)
    - Length: 25
    - Value: 1363636e612d537461746566756c44484350763603636f6d...
    - DNS Domain Search List
    - Domain: ccna-StatefulDHCPv6.com

## 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?

*RTA// DHCPv6 usa más recursos de memoria. Las respuestas serán vagas, pero DHCPv6 con estado requiere que el enrutador almacene información de estado dinámico sobre los clientes de DHCPv6. Los clientes DHCPv6 sin estado no usan el servidor DHCP para obtener información de dirección, por lo que esta información no necesita ser almacenada.*

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

*RTA// Cisco recomienda DHCPv6 sin estado al implementar e implementar redes IPv6 sin un Cisco Network Registrar.*

### Tabla de resumen de interfaces del router

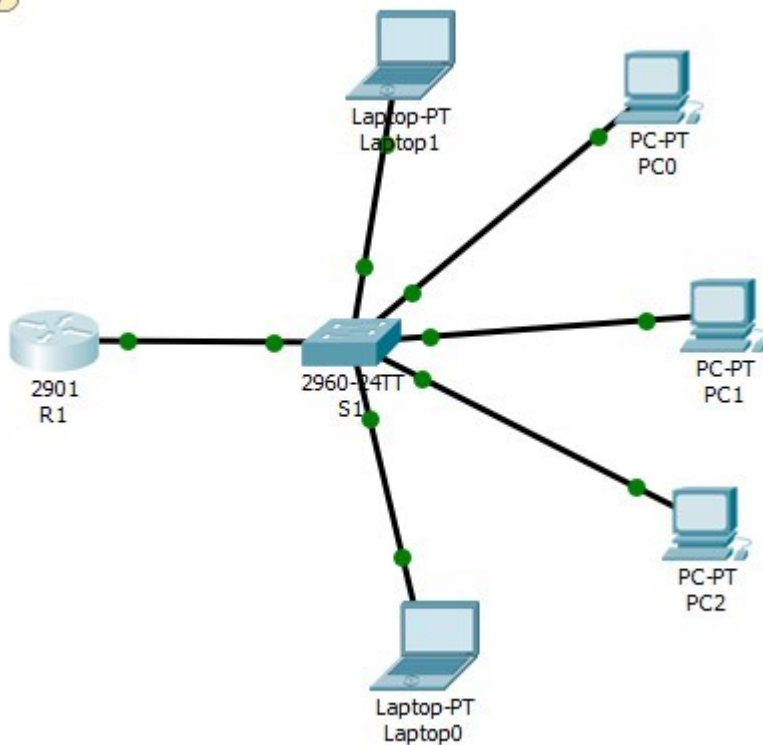
| Resumen de interfaces del router |                             |                             |                       |                       |
|----------------------------------|-----------------------------|-----------------------------|-----------------------|-----------------------|
| Modelo de 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.

#### Topología



#### IdT y DHCP

##### Objetivo

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

##### Situación

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

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

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

- Configure un router Cisco 1941 (o un dispositivo ISR que pueda admitir un servidor de DHCP) para las direcciones IPv4 o IPv6 de DHCP.

- Piense en cinco dispositivos de su hogar en los que desee recibir direcciones IP desde el servicio DHCP del router. Configure las terminales para solicitar direcciones DHCP del servidor de DHCP.
- Muestre los resultados que validen que cada terminal garantiza una dirección IP del servidor. Utilice un programa de captura de pantalla para guardar la información del resultado o emplee el comando de la tecla **ImprPant**.

```

R1>ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

R1>ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/11 ms

R1>ping 192.168.1.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.13, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1>ping 192.168.1.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.15, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1>ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1>|

```

## 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?  
R/ Para tener una red de menor coste

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

- ✚ El uso de IPv6 que tendrá más de direcciones y no quedarse sin espacio si se convierten en una gran empresa.
- ✚ IPv6 es fundamentalmente dinámico y que hace que sea más fácil de configurar.
- ✚ Puede crear la seguridad de que con ella no podría obtener con un router básico.
- ✚ Se conecta fácilmente con otros dispositivos, como ordenadores portátiles y teléfonos celulares
- ✚ Permite un mejor control sobre sus recursos

## 11.2.2.6 LAB - CONFIGURING DYNAMIC AND STATIC NAT

Topología

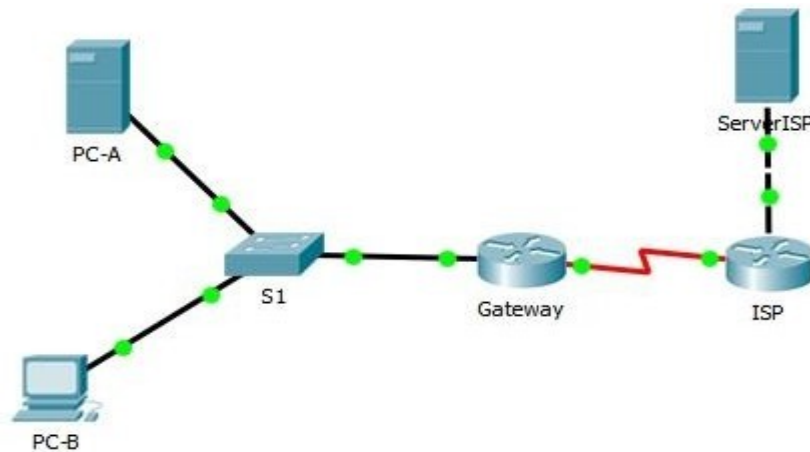


Tabla de direccionamiento

| 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                    |
|                          | G0/0         | 192.31.7.1     | 255.255.255.0     | N/A                    |
| SERVER ISP               | G0/0         | 192.31.7.1     | 255.255.255.0     | 192.31.7.1             |
| PC-A (servidor simulado) | NIC          | 192.168.1.20   | 255.255.255.0     | 192.168.1.1            |
| PC-B                     | NIC          | 192.168.1.21   | 255.255.255.0     | 192.168.1.1            |

### Objetivos

**Parte 1: armar la red y verificar la conectividad**

**Parte 2: configurar y verificar la NAT estática**

**Parte 3: configurar y verificar la NAT dinámica**

### Información básica/situación

La traducción de direcciones de red (NAT) es el proceso en el que un dispositivo de red, como un router Cisco, asigna una dirección pública a los dispositivos host dentro de una red

privada. El motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada.

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

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

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

### **Recursos necesarios**

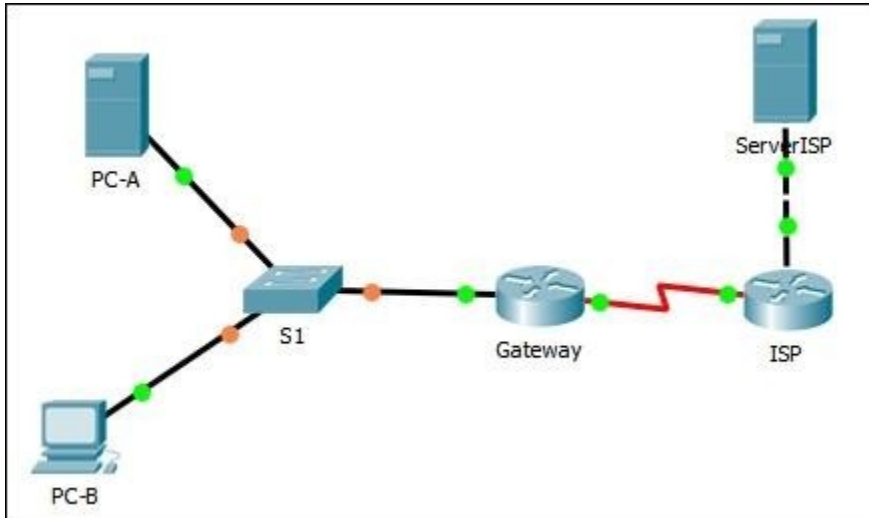
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

## **Parte 1: armar la red y verificar la conectividad**

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

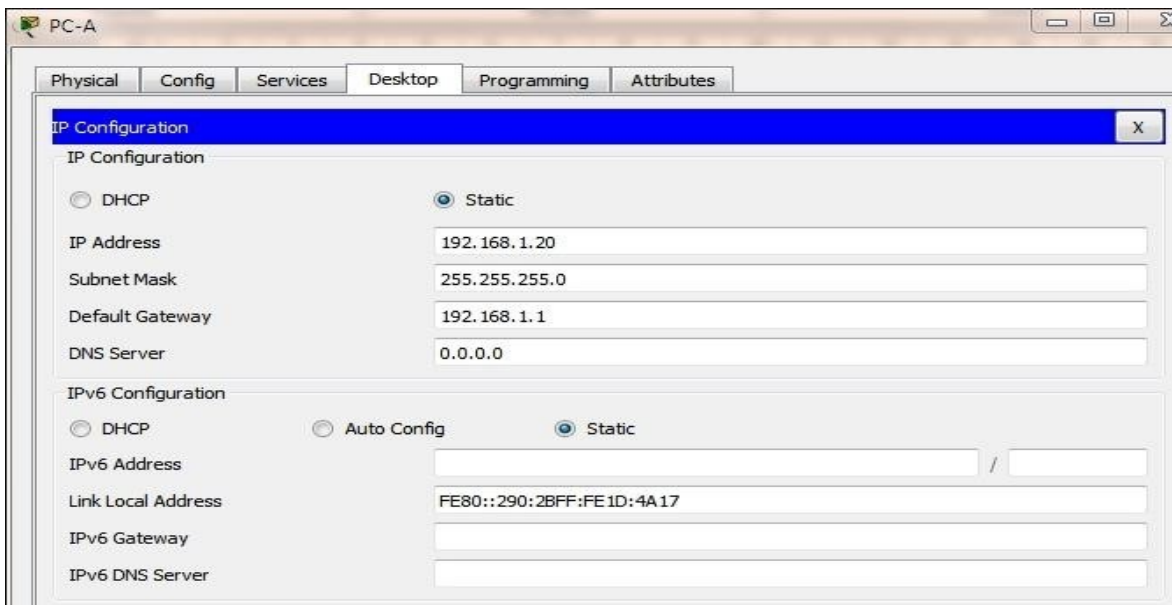
**Step 43: realizar el cableado de red tal como se muestra en la topología.**

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

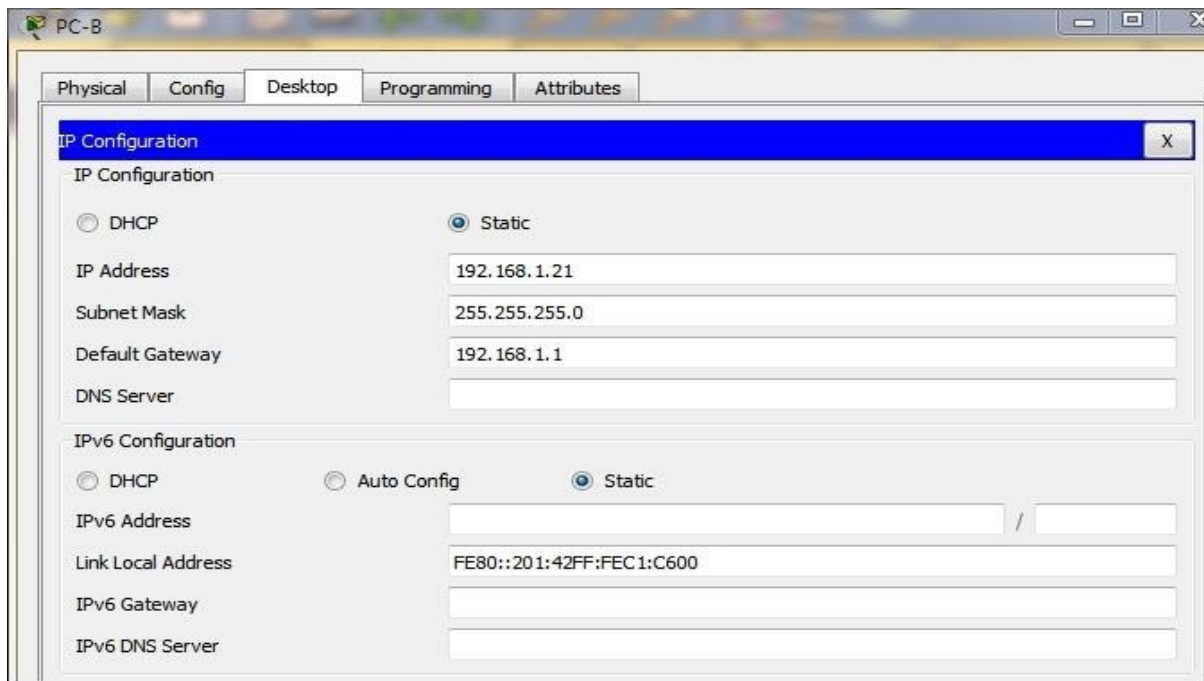


**Step 44: configurar los equipos host.**

**PC-A**



## PC-B



**Step 45: inicializar y volver a cargar los routers y los switches según sea necesario.**

**Step 46: 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 **1280000** para las interfaces seriales 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 47: crear un servidor web simulado en el ISP.**

- Cree un usuario local denominado **webuser** con la contraseña cifrada **webpass**.  
ISP(config)# **username webuser privilege 15 secret webpass**
- Habilite el servicio del servidor HTTP en el ISP.  
ISP(config)# **ip http server**
- Configure el servicio HTTP para utilizar la base de datos local.

ISP(config)# ip http authentication local

**Step 48: configurar el routing estático.**

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

ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18

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

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

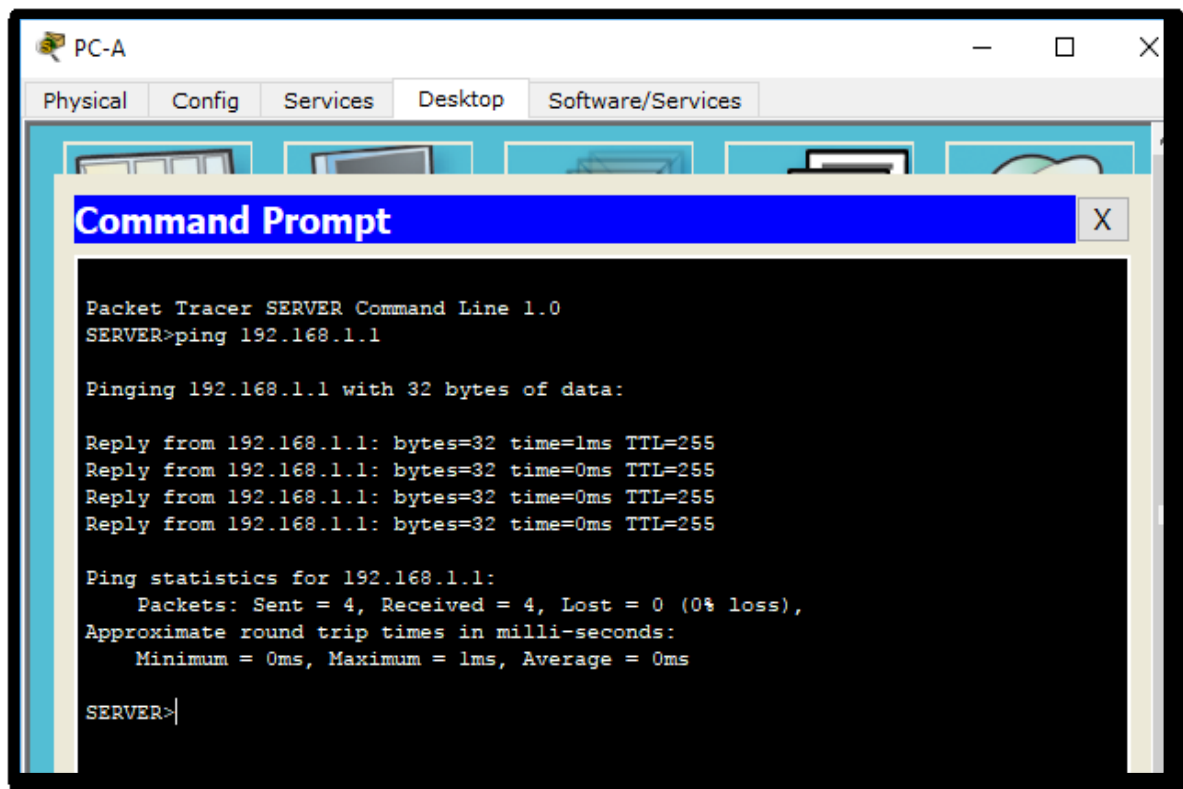
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

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

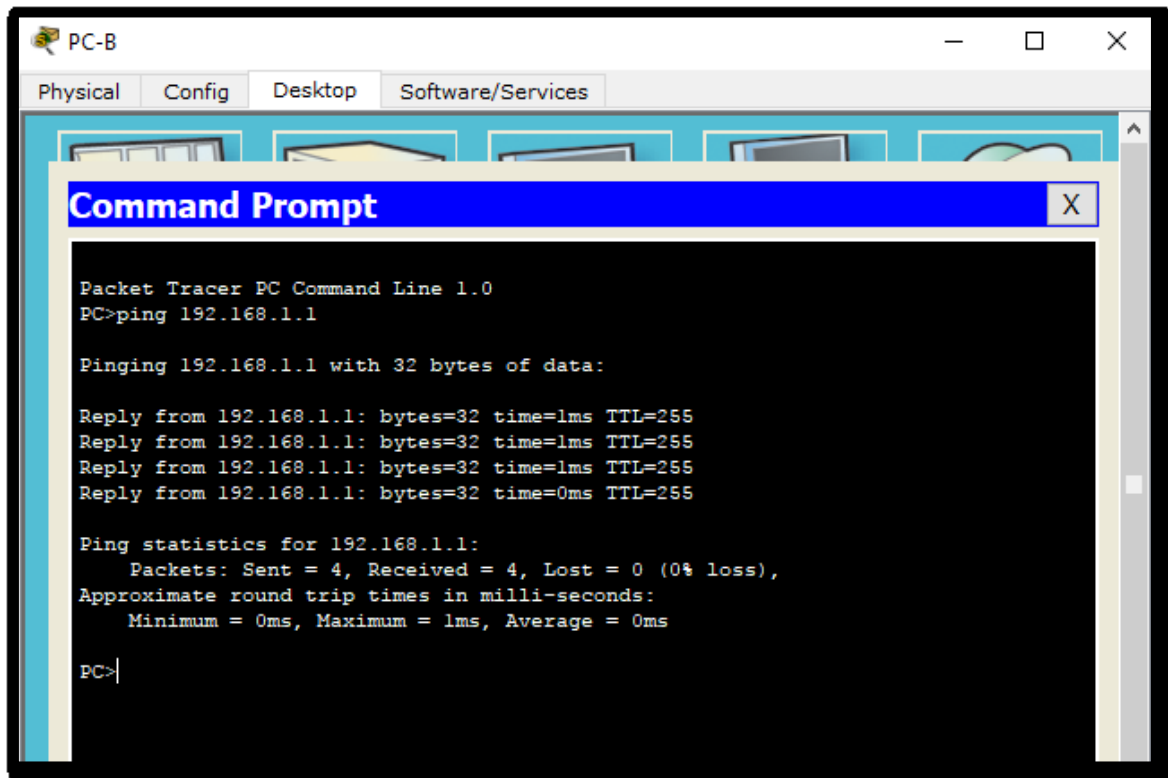
**Step 49: Guardar la configuración en ejecución en la configuración de inicio.**

**Step 50: Verificar la conectividad de la red**

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.







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

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

Gateway of last resort is 209.165.201.17 to network 0.0.0.0

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

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

Gateway of last resort is not set

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

**Parte 2: configurar y verificar la NAT estática.**

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

**Step 51: configurar una asignación estática.**

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

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

```
Gateway>enable
Gateway#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20
209.165.200.225
Gateway(config)#
```

**Step 52: Especifique las interfaces.**

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

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

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

**Step 53: probar la configuración.**

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

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

```
Gateway#
Gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
Gateway(config)#interface g0/1
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface s0/0/1
Gateway(config-if)#ip nat outside
Gateway(config-if)#exit
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway#
```

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

192.168.1.20 = 209.165.200.225

¿Quién asigna la dirección global interna? El route y el proveedor de internet.

¿Quién asigna la dirección local interna? Los administradores de red.

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

```

SERVER>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.

Ping statistics for 192.31.7.1:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

```

C:\>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.
Reply from 209.165.201.17: Destination host unreachable.

Ping statistics for 192.31.7.2:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

**Gateway# show ip nat translations**

```

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

```

```

Gateway>enable
Gateway#show ip nat translations
Pro Inside global Inside local Outside local
Outside global
--- 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? **10**

```

icmp 209.165.200.225:10 192.168.1.20:10 192.31.7.2:10
icmp 209.165.200.225:11 192.168.1.20:11 192.31.7.2:11
icmp 209.165.200.225:12 192.168.1.20:12 192.31.7.2:12
icmp 209.165.200.225:13 192.168.1.20:13 192.31.7.2:13
icmp 209.165.200.225:14 192.168.1.20:14 192.31.7.2:14

```

**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? **7**

¿Cuáles son los números de puerto que se usaron?

Global/local interno: \_\_\_\_\_

Global/local externo: \_\_\_\_\_

- d. Debido a que se configuró NAT estática para la PC-A, verifique que el ping del ISP a la dirección pública de NAT estática de la PC-A (209.165.200.225) se realice correctamente.
- e. En el router Gateway, muestre la tabla de NAT para verificar la traducción.

Gateway# **show ip nat translations**

```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225 192.168.1.20 --- ---
```

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

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

Gateway# **show ip nat statistics**

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

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

```
Outside interfaces:
```

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

CEF Translated packets: 39, CEF Punted packets: 0

Expired translations: 3

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

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

### Parte 3: configurar y verificar la NAT dinámica

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

#### Step 54: 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 55: 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 56: 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 57: 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 58: 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 59: 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 = \_\_\_\_\_

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? \_\_\_\_\_

- 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? \_\_\_\_\_

¿Qué números de puerto se usaron?

Interno: \_\_\_\_\_

Externo: \_\_\_\_\_

¿Qué número de puerto bien conocido y qué servicio se usaron? \_\_\_\_\_

- 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

App1 doors: 0

Normal doors: 0

Queued Packets: 0

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

### Step 60: 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?

---

---

2. ¿Cuáles son las limitaciones de NAT?

---

---

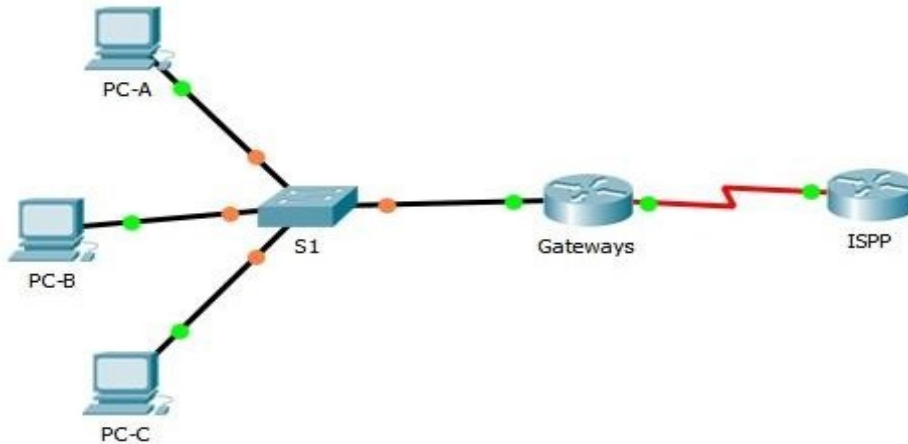
**Tabla de resumen de interfaces del router**

| <b>Resumen de interfaces del router</b> |                             |                                |                           |                              |
|-----------------------------------------|-----------------------------|--------------------------------|---------------------------|------------------------------|
| <b>Modelo de router</b>                 | <b>Interfaz Ethernet #1</b> | <b>Interfaz Ethernet n.º 2</b> | <b>Interfaz serial #1</b> | <b>Interfaz serial n.º 2</b> |
| 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.

#### topologia



#### Tabla de direccionamiento

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

#### Recursos necesarios

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

## Parte 1: armar la red y verificar la conectividad

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

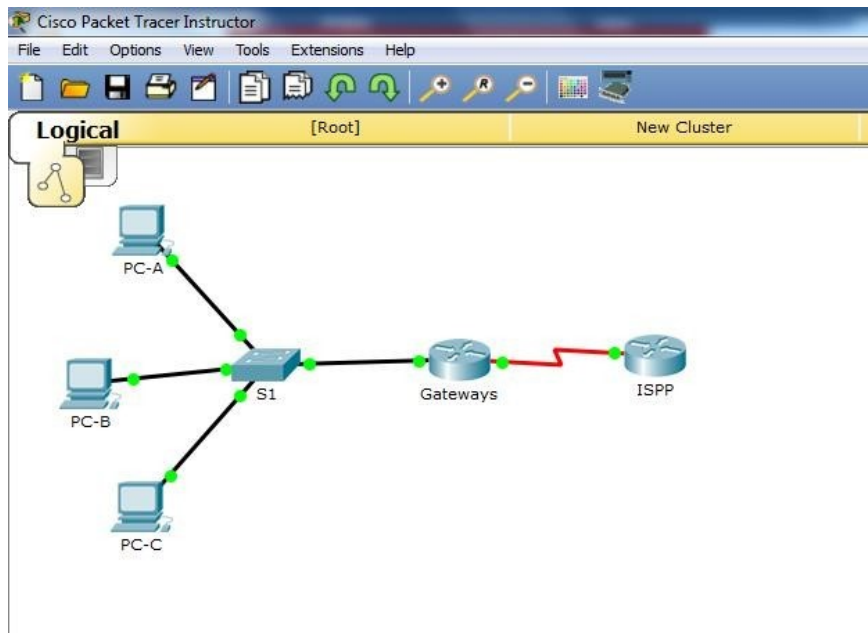
**Step 61: realizar el cableado de red tal como se muestra en la topología.**

**Step 62: configurar los equipos host.**

**Step 63: inicializar y volver a cargar los routers y los switches.**

**Step 64: configurar los parámetros básicos para cada router.**

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



```
Gateway
Physical Config CLI

IOS Command Line Interface

DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#interface 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)#interface s0/0/1
Gateway(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway(config-if)#no shutdown

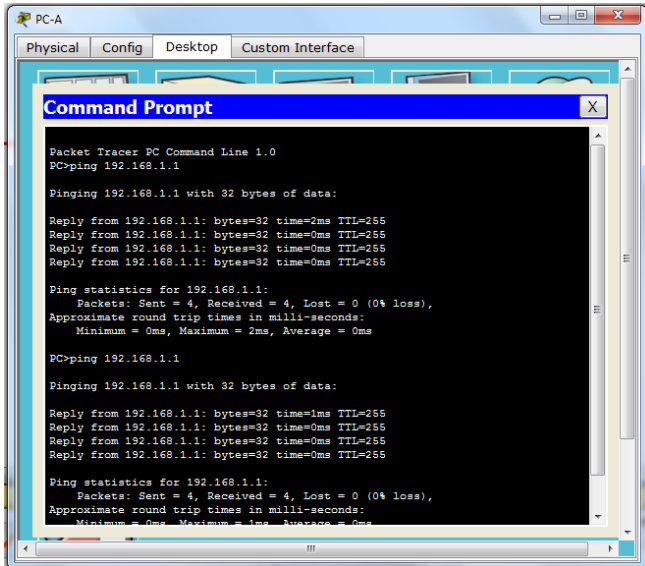
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Gateway(config-if)#
```

### Step 65: configurar el routing estático.

- a. Cree una ruta estática desde el router ISP hasta el router Gateway.  
ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**
- b. Cree una ruta predeterminada del router Gateway al router ISP.  
Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

### Step 66: Verificar la conectividad de la red

- a. Desde los equipos host, haga ping a la interfaz G0/1 en el router Gateway. Resuelva los problemas si los pings fallan.
- b. Verifique que las rutas estáticas estén bien configuradas en ambos routers.



## Parte 2: configurar y verificar el conjunto de NAT con sobrecarga

En la parte 2, configurará el router Gateway para que traduzca las direcciones IP de la red 192.168.1.0/24 a una de las seis direcciones utilizables del rango 209.165.200.224/29.

**Step 67: 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 68: 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 69: 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 70: 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 71: verificar la configuración del conjunto de NAT con sobrecarga.**

- a. Desde cada equipo host, haga ping a la dirección 192.31.7.1 del router ISP.
- b. Muestre las estadísticas de NAT en el router Gateway.

Gateway# **show ip nat statistics**

```
Gateway#
Gateway#show ip nat translations
Gateway#
Gateway#show ip nat statistics
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 14 Misses: 18
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 12
 pool public_access: netmask 255.255.255.248
 start 209.165.200.225 end 209.165.200.230
 type generic, total addresses 6 , allocated 1 (16%), misses 0
Gateway#
```

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 3

pool public\_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

type generic, total addresses 6, allocated 1 (16%), misses 0



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

- c. Muestre las NAT en el router Gateway.

Gateway# **show ip nat translations**

| Pro  | Inside global     | Inside local   | Outside local | Outside global |
|------|-------------------|----------------|---------------|----------------|
| icmp | 209.165.200.225:0 | 192.168.1.20:1 | 192.31.7.1:1  | 192.31.7.1:0   |
| icmp | 209.165.200.225:1 | 192.168.1.21:1 | 192.31.7.1:1  | 192.31.7.1:1   |
| icmp | 209.165.200.225:2 | 192.168.1.22:1 | 192.31.7.1:1  | 192.31.7.1:2   |

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

¿Cuántas direcciones IP locales internas se indican en el resultado de muestra anterior? **3 direcciones**

¿Cuántas direcciones IP globales internas se indican? **una**

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

**12 puertos para 12 paquetes**

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

El ping falla porque la configuración NAT no deja que ISP las conozca por la ip original sin por las que deja ver NAT.

### **Parte 3: configurar y verificar PAT**

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

**Step 72: borrar las NAT y las estadísticas en el router Gateway.**

**Step 73: verificar la configuración para NAT.**

- a. Verifique que se hayan borrado las estadísticas.
- b. Verifique que las interfaces externa e interna estén configuradas para NAT.
- c. Verifique que la ACL aún esté configurada para NAT.

¿Qué comando usó para confirmar los resultados de los pasos a al c? **Show ip nat statistic**

**Step 74: 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 75: eliminar la traducción NAT de la lista de origen interna al conjunto externo.**

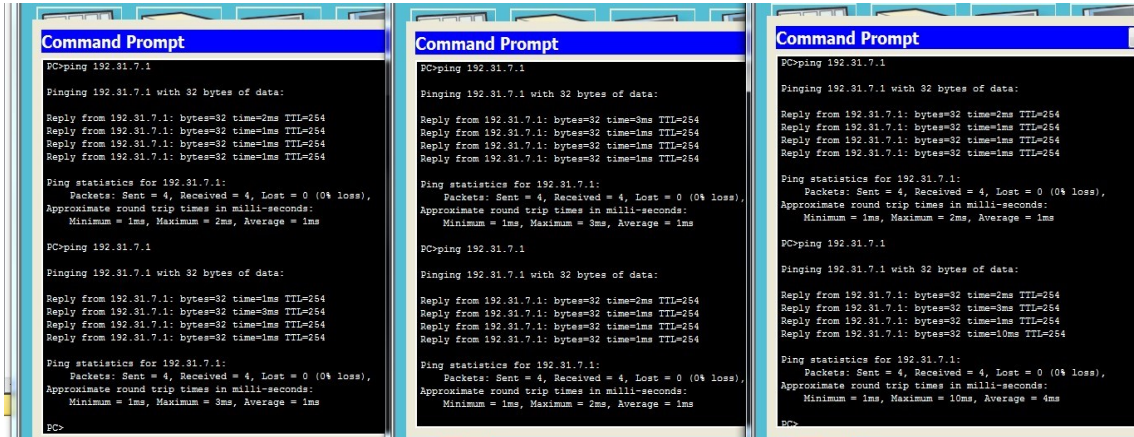
```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

**Step 76: asociar la lista de origen a la interfaz externa.**

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

**Step 77: probar la configuración PAT.**

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



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

Gateway# **show ip nat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

c. Muestre las traducciones NAT en el Gateway.

Gateway# **show ip nat translations**

Pro Inside global    Inside local    Outside local    Outside global

icmp 209.165.201.18:3 192.168.1.20:1 192.31.7.1:1 192.31.7.1:3

```
icmp 209.165.201.18:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.201.18:4 192.168.1.22:1 192.31.7.1:1 192.31.7.1:4
```

```

Gateway

Physical Config CLI

IOS Command Line Interface

Gateway(config)#no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
Gateway(config)#ip nat inside source list 1 interface serial 0/0/1 overload
Gateway(config)#
Gateway(config)#exit
Gateway#
$SYS-S-CONFIG_I: Configured from console by console

Gateway#show ip nat statistic
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 26 Misses: 30
Expired translations: 26
Dynamic mappings:
Gateway#show ip nat statistic
Total translations: 12 (0 static, 12 dynamic, 12 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 38 Misses: 42
Expired translations: 26
Dynamic mappings:
Gateway#show ip nat translations
Gateway#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.201.18:1024 192.168.1.22:15 192.31.7.1:15 192.31.7.1:1024
icmp 209.165.201.18:1025 192.168.1.22:16 192.31.7.1:16 192.31.7.1:1025
icmp 209.165.201.18:13 192.168.1.21:13 192.31.7.1:13 192.31.7.1:13
icmp 209.165.201.18:14 192.168.1.21:14 192.31.7.1:14 192.31.7.1:14
icmp 209.165.201.18:15 192.168.1.21:15 192.31.7.1:15 192.31.7.1:15
icmp 209.165.201.18:16 192.168.1.21:16 192.31.7.1:16 192.31.7.1:16
icmp 209.165.201.18:17 192.168.1.22:17 192.31.7.1:17 192.31.7.1:17
icmp 209.165.201.18:18 192.168.1.22:18 192.31.7.1:18 192.31.7.1:18
icmp 209.165.201.18:24 192.168.1.20:24 192.31.7.1:24 192.31.7.1:24
icmp 209.165.201.18:25 192.168.1.20:25 192.31.7.1:25 192.31.7.1:25
icmp 209.165.201.18:26 192.168.1.20:26 192.31.7.1:26 192.31.7.1:26
icmp 209.165.201.18:27 192.168.1.20:27 192.31.7.1:27 192.31.7.1:27

```

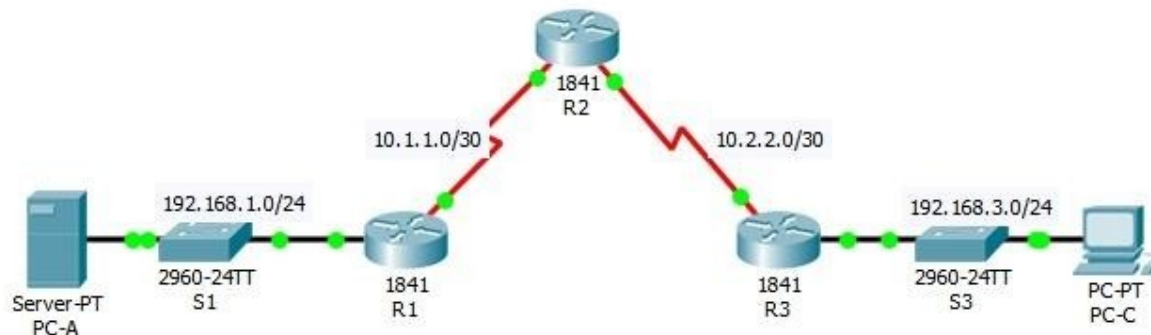
## Reflexión

¿Qué ventajas tiene la PAT? Al usar una ip publica en este caso se ahorran muchas direcciones IP publicas, pues usando los distintos puertos para diferenciar los paquetes, la seguridad también se incrementa.

## EJERCICIOS TEORICO PRACTICOS

### 4.4.1.2 PACKET TRACER - CONFIGURE IP ACLS TO MITIGATE ATTACKS

## Topologia



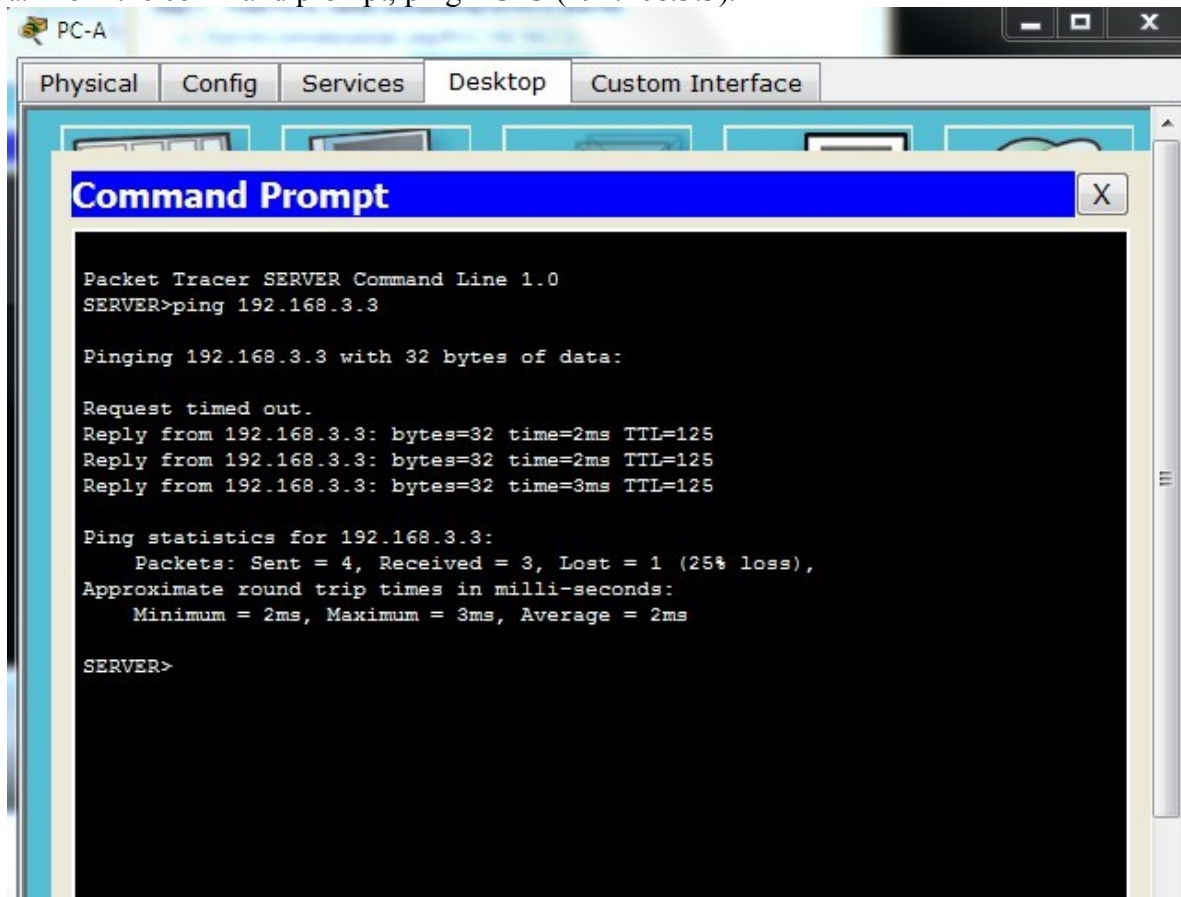
| Device | Interface    | IP Address  | Subnet Mask     | Default Gateway | Switch Port |
|--------|--------------|-------------|-----------------|-----------------|-------------|
| R1     | Fa0/1        | 192.168.1.1 | 255.255.255.0   | N/A             | S1 Fa0/5    |
|        | S0/0/0 (DCE) | 10.1.1.1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

### Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

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

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



```
PC-A
Physical Config Services Desktop Custom Interface
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

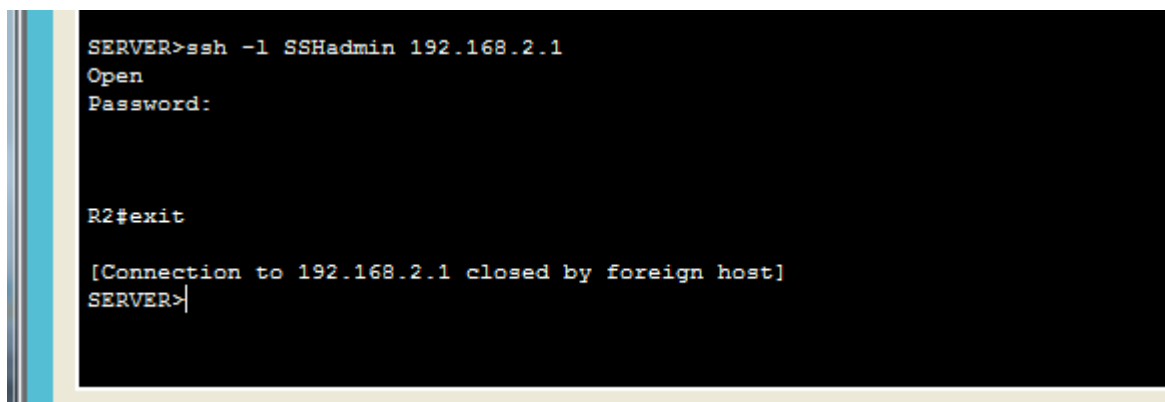
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.3:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 2ms, Maximum = 3ms, Average = 2ms

SERVER>
```

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

**PC> ssh -l SSHadmin 192.168.2.1**



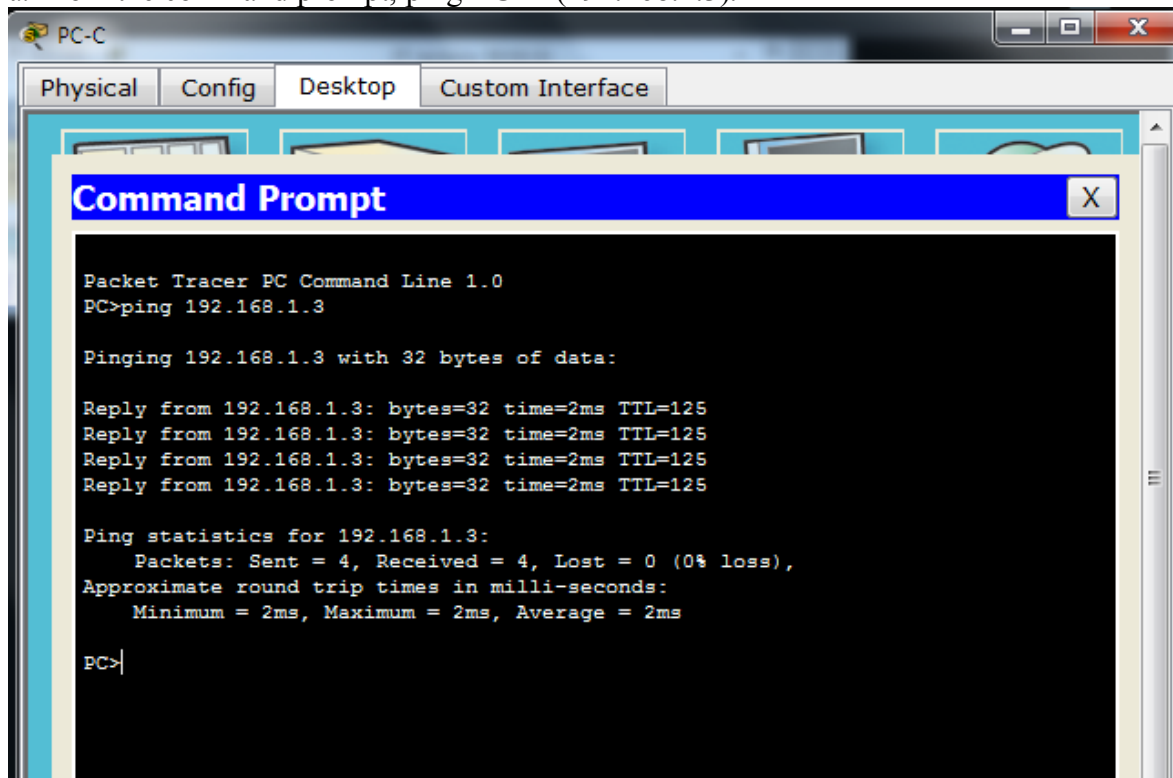
```
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#exit

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

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

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



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

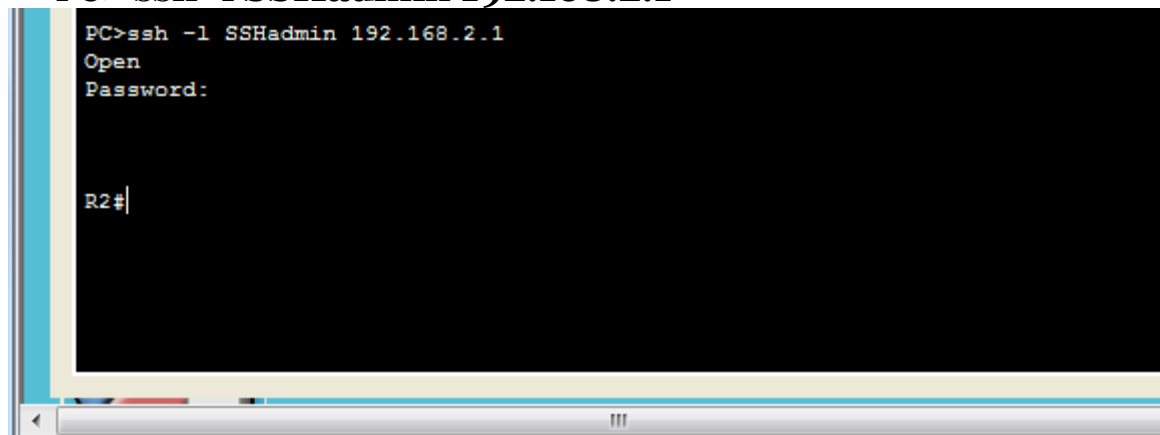
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

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 = 2ms, Average = 2ms

PC>
```

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

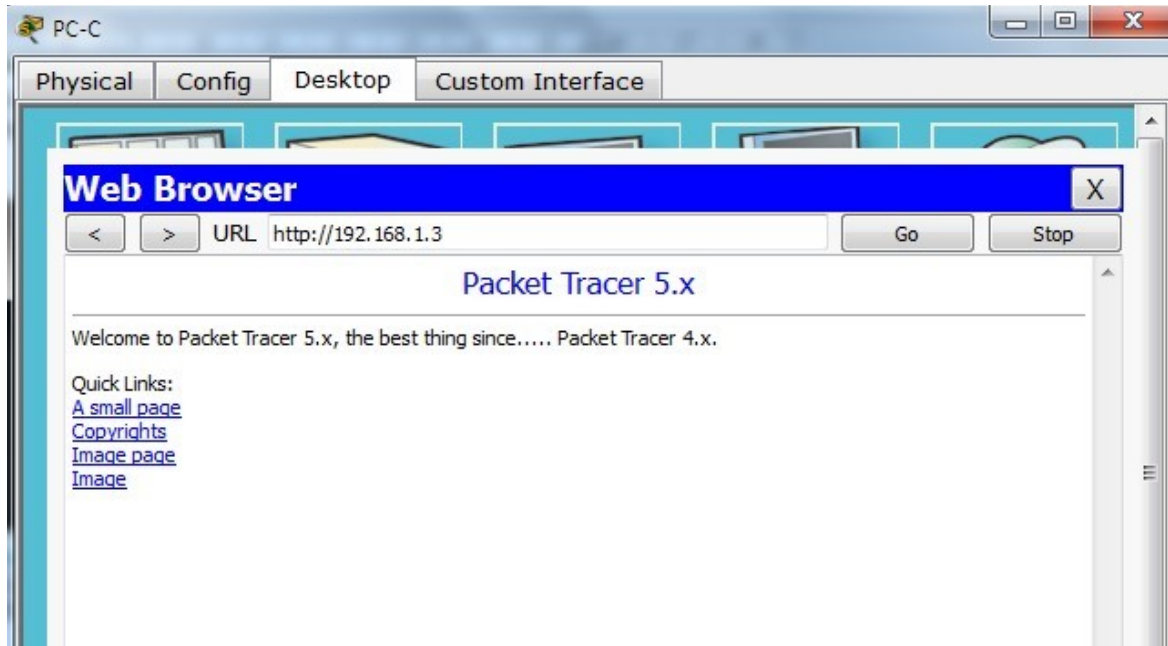
**PC> ssh -l SSHadmin 192.168.2.1**



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

R2#
```

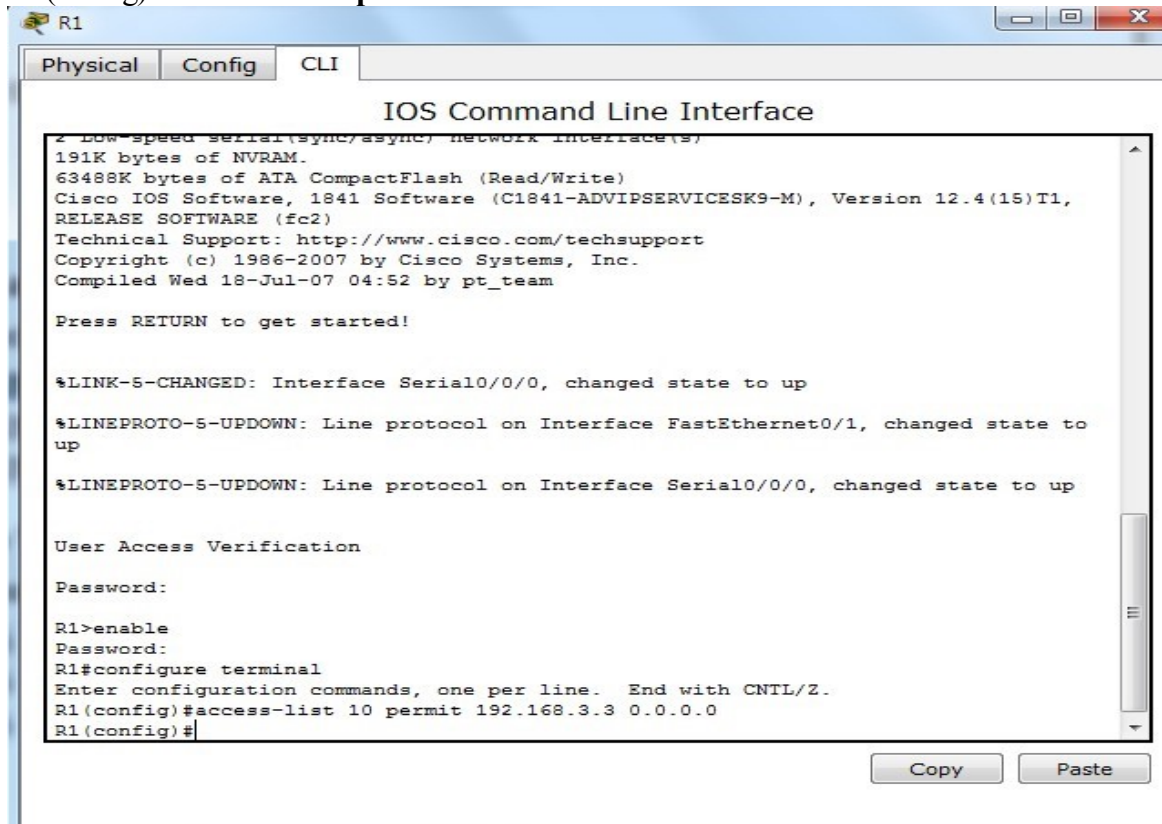
c. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser when done.



## Part 2: Secure Access to Routers

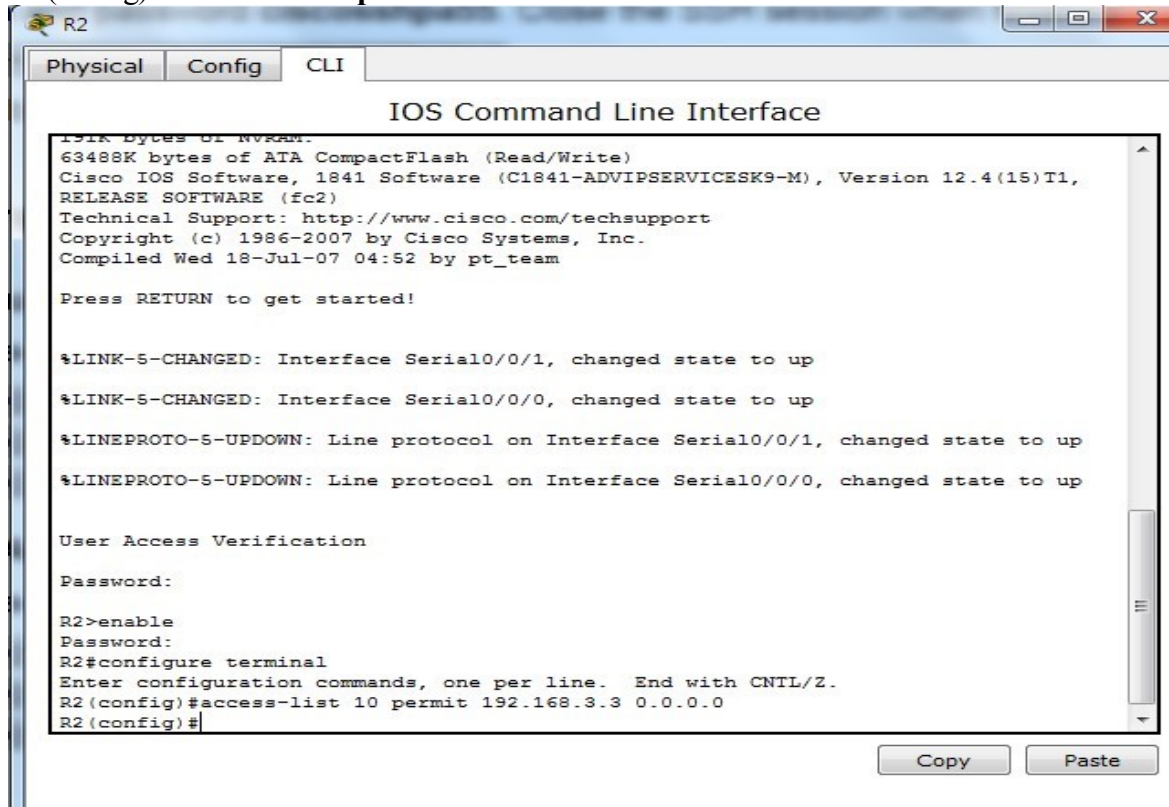
**Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.** Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

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





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



The screenshot shows the CLI of router R2. The interface is titled "IOS Command Line Interface". The output shows the following sequence of events:

```
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
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

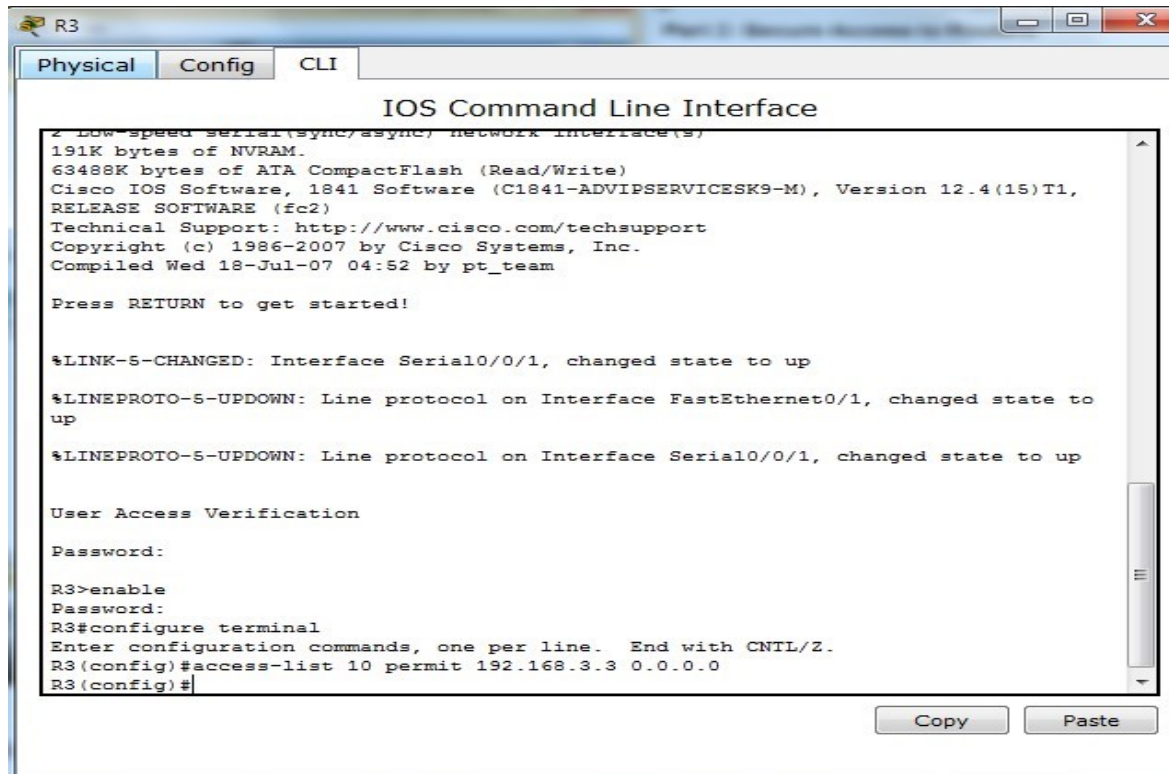
User Access Verification

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 0.0.0.0
R2(config)#
```

Buttons for "Copy" and "Paste" are visible at the bottom right of the terminal window.

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



The screenshot shows the CLI of router R3. The interface is titled "IOS Command Line Interface". The output shows the following sequence of events:

```
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
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:

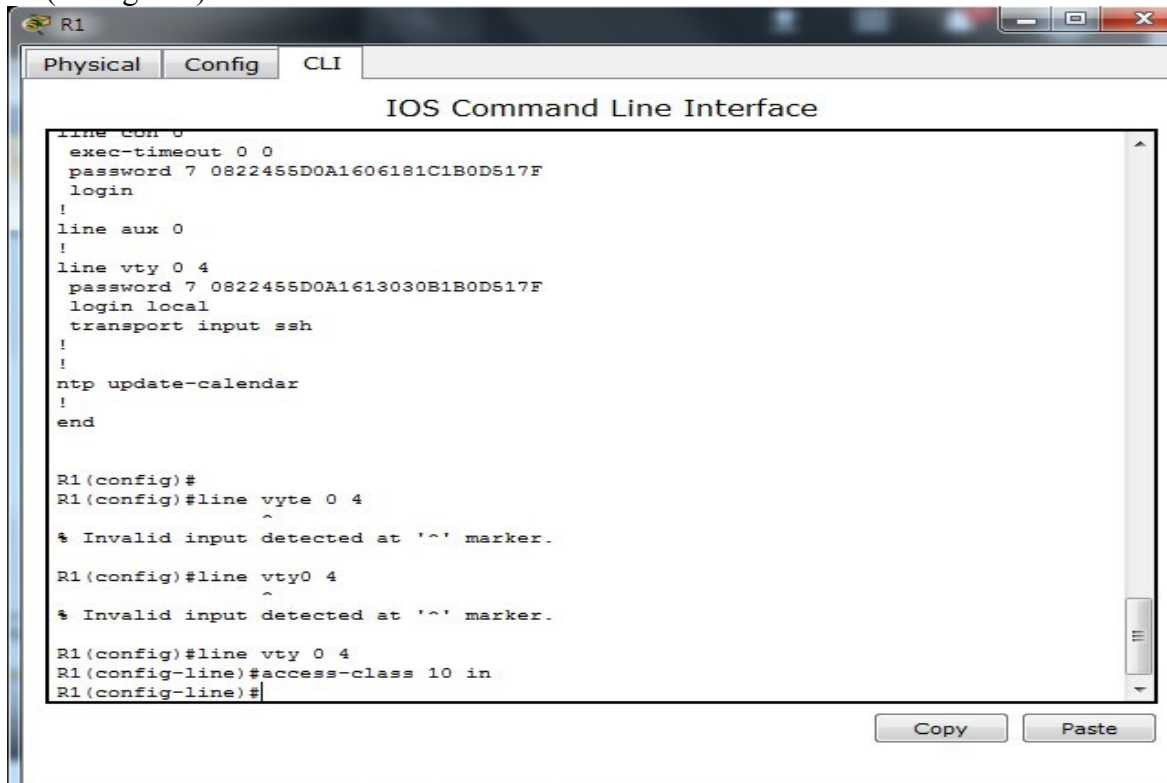
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)#
```

Buttons for "Copy" and "Paste" are visible at the bottom right of the terminal window.

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

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

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



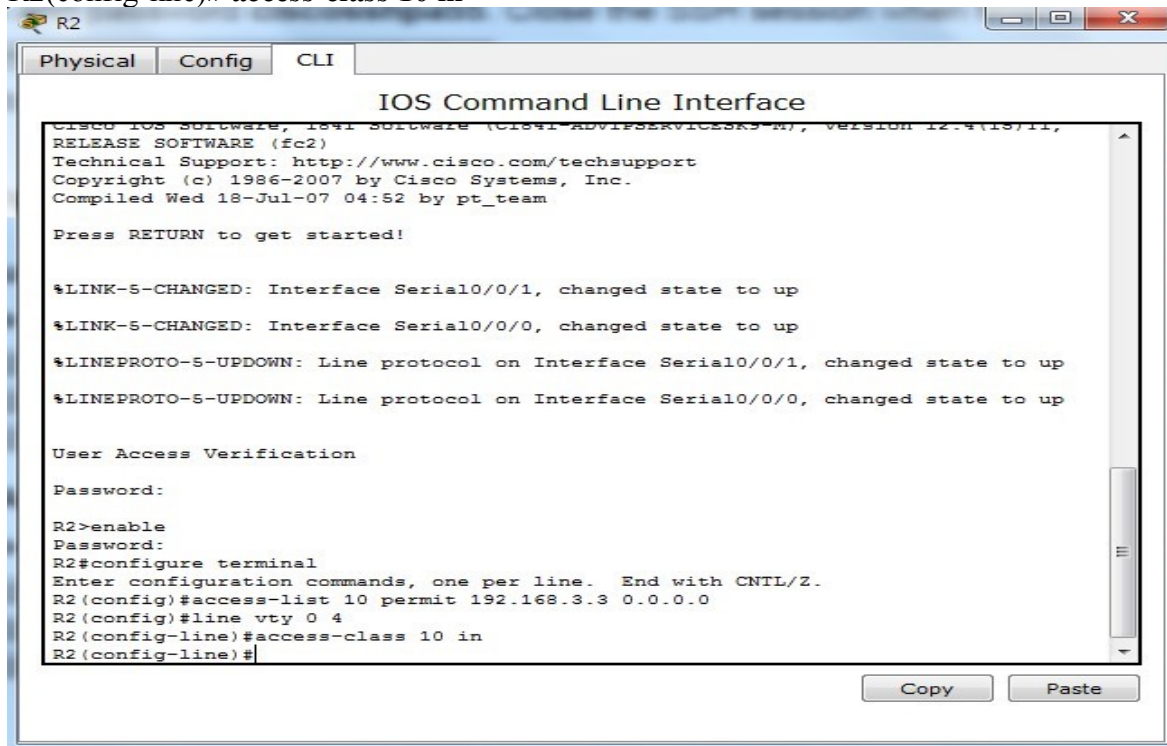
```
R1
Physical Config CLI
IOS Command Line Interface
line con 0
exec-timeout 0 0
password 7 0822455D0A1606181C1B0D517F
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A1613030B1B0D517F
login local
transport input ssh
!
!
ntp update-calendar
!
end

R1(config)#
R1(config)#line vty 0 4
^
% Invalid input detected at '^' marker.

R1(config)#line vty0 4
^
% Invalid input detected at '^' marker.

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

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



```
R2
Physical Config CLI
IOS Command Line Interface
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(13)11,
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 0.0.0.0
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#
```

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

```
63456K Bytes of NVRAM CompactFlash (read/write)
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 0.0.0.0
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#
```

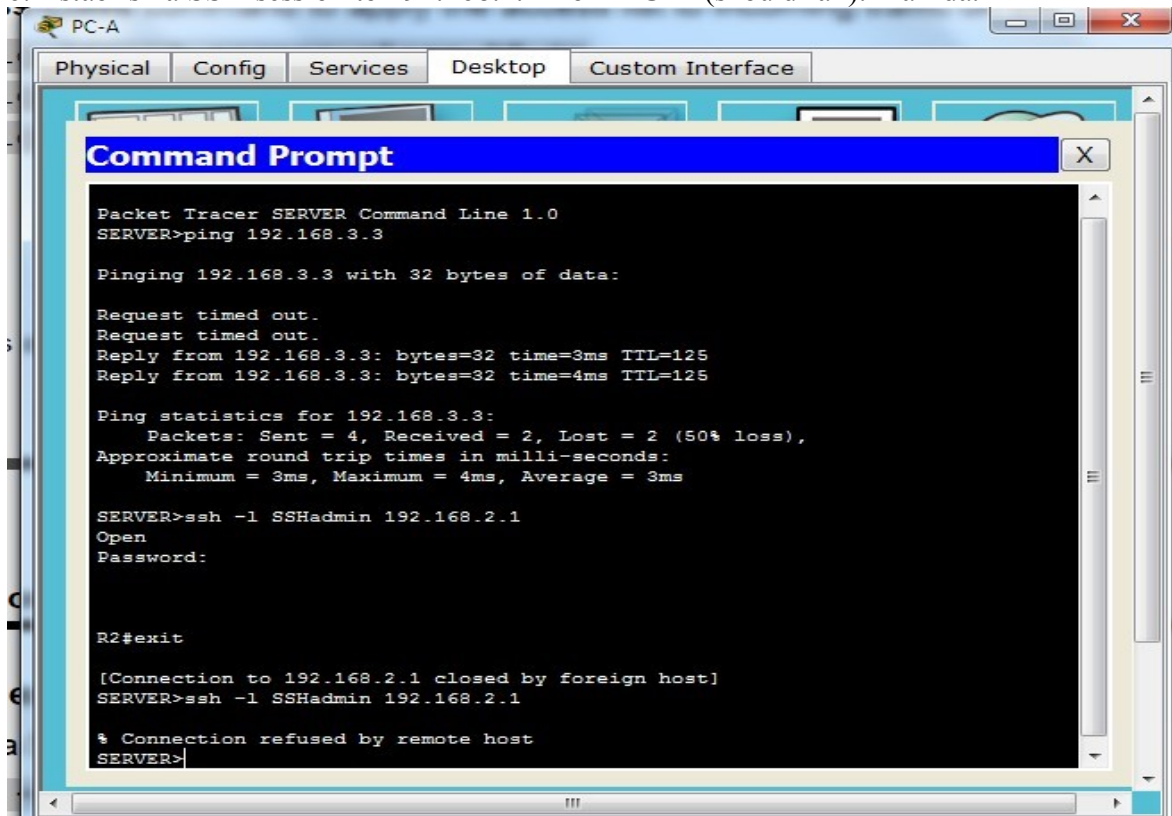
### Step 3: Verify exclusive access from management station PC-C.

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

PC> ssh -l SSHAdmin 192.168.2.1

```
[Connection to 192.168.2.1 closed by foreign host]
PC>
PC>ssh -l sshadmin 192.168.2.1
Open
Password:
Password:
Password:
[Connection to 192.168.2.1 closed by foreign host]
PC>
PC>ssh -l SSHAdmin 192.168.2.1
Open
Password:
R2#
```

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

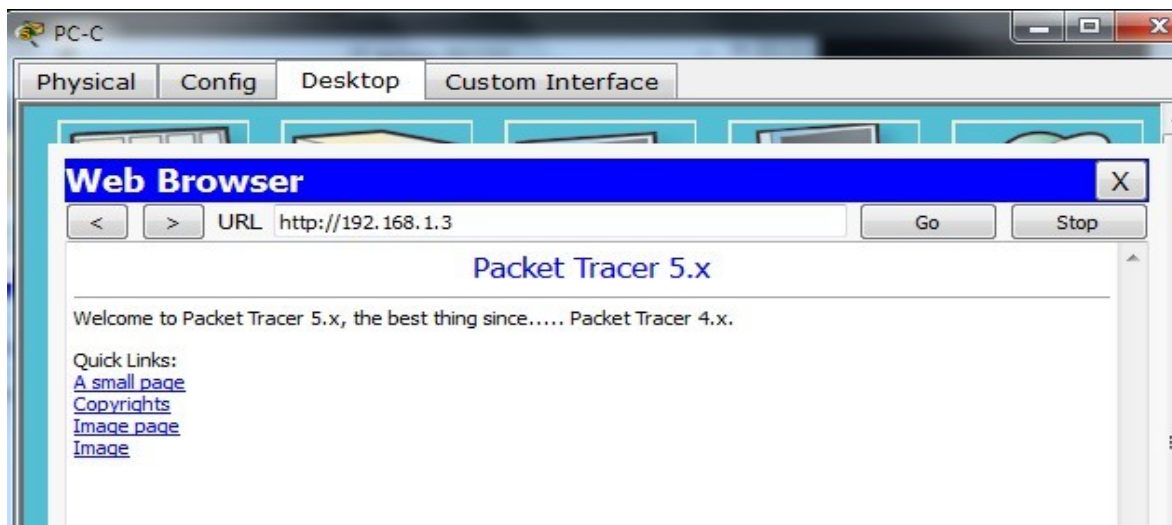


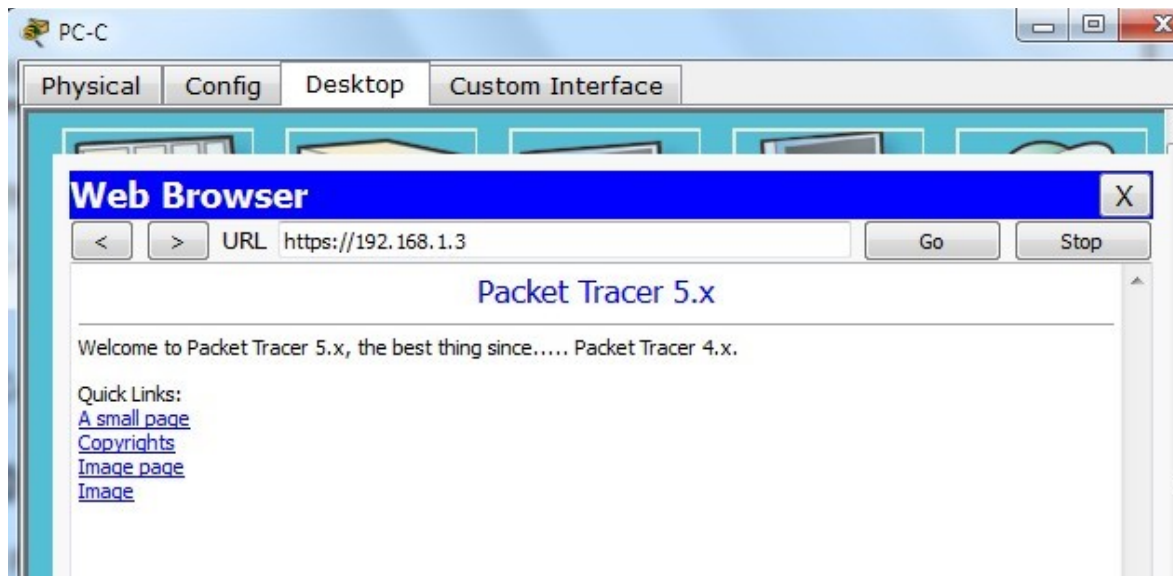
### Part 3: Create a Numbered IP ACL 120 on R1

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

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

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





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

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

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



R1

Physical Config CLI

### IOS Command Line Interface

```
!
line vty 0 4
 password 7 0822455D0A1613030B1B0D517F
 login local
 transport input ssh
!
!
ntp update-calendar
!
end

R1(config)#
R1(config)#line vty 0 4
^
% Invalid input detected at '^' marker.

R1(config)#line vty0 4
^
% Invalid input detected at '^' marker.

R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#
```

Copy Paste

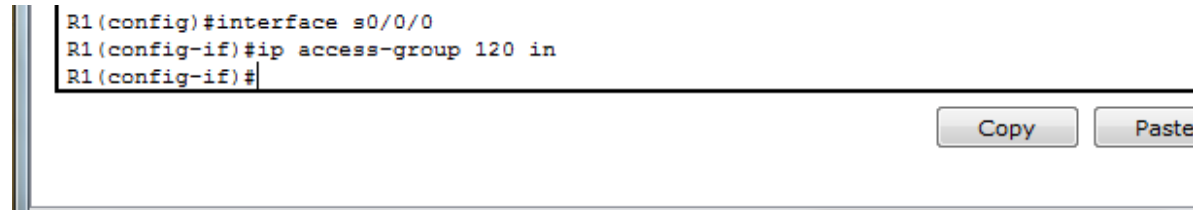
### Step 3: Apply the ACL to interface S0/0/0.

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

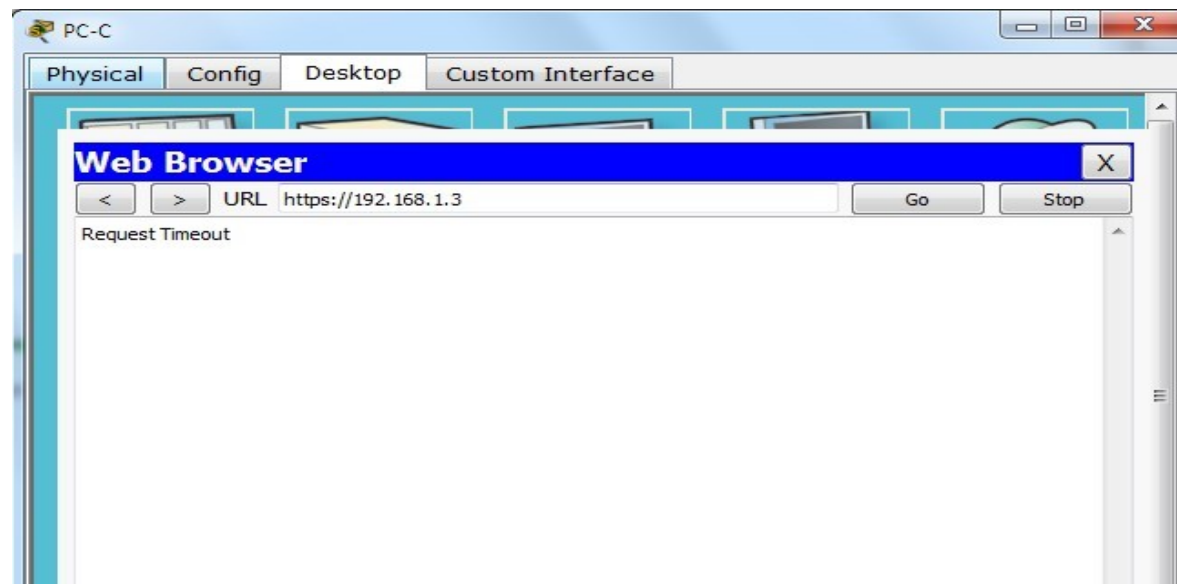
```
R1(config)# interface s0/0/0
```

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

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



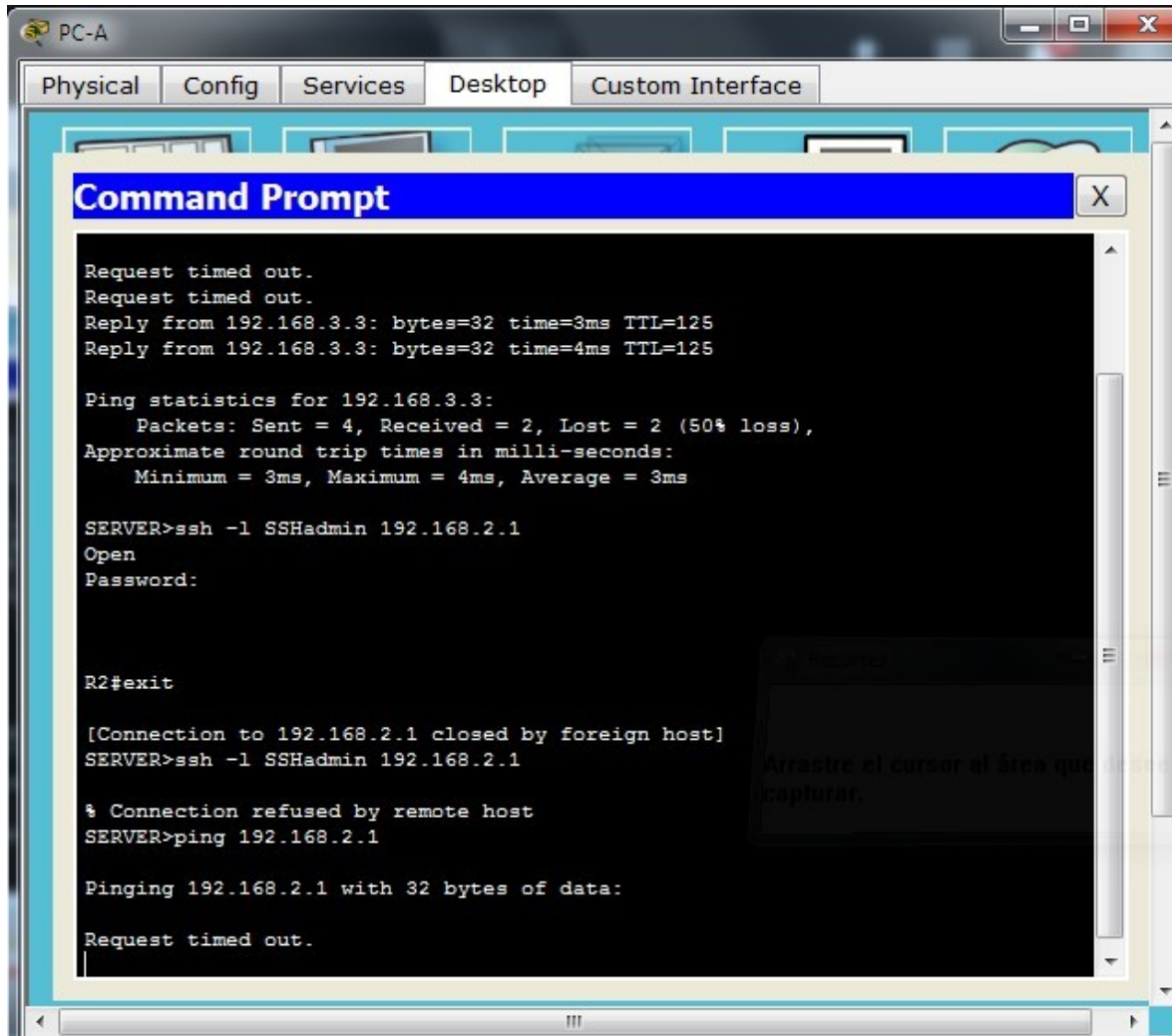
### Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser



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

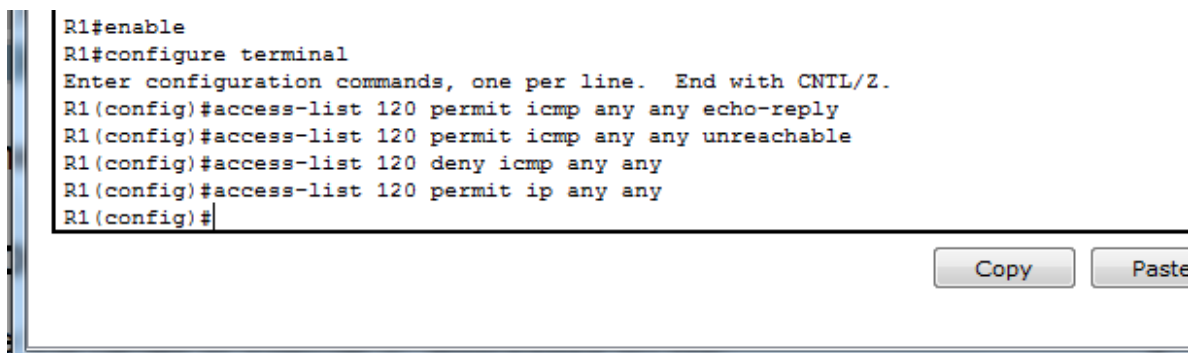
Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

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



**Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.**  
Use the **access-list** command to create a numbered IP ACL.

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



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



```
PC-A
Physical Config Services Desktop Custom Interface
Command Prompt
% Connection refused by remote host
SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

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

SERVER>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=2ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms

SERVER>
```

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

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

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

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

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

```
R3(config-line)#exit
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 Fa0/1.

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

```
R3(config)# interface fa0/1
```

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

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

Copy

Paste

## 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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#
```

Copy

Paste

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

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

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

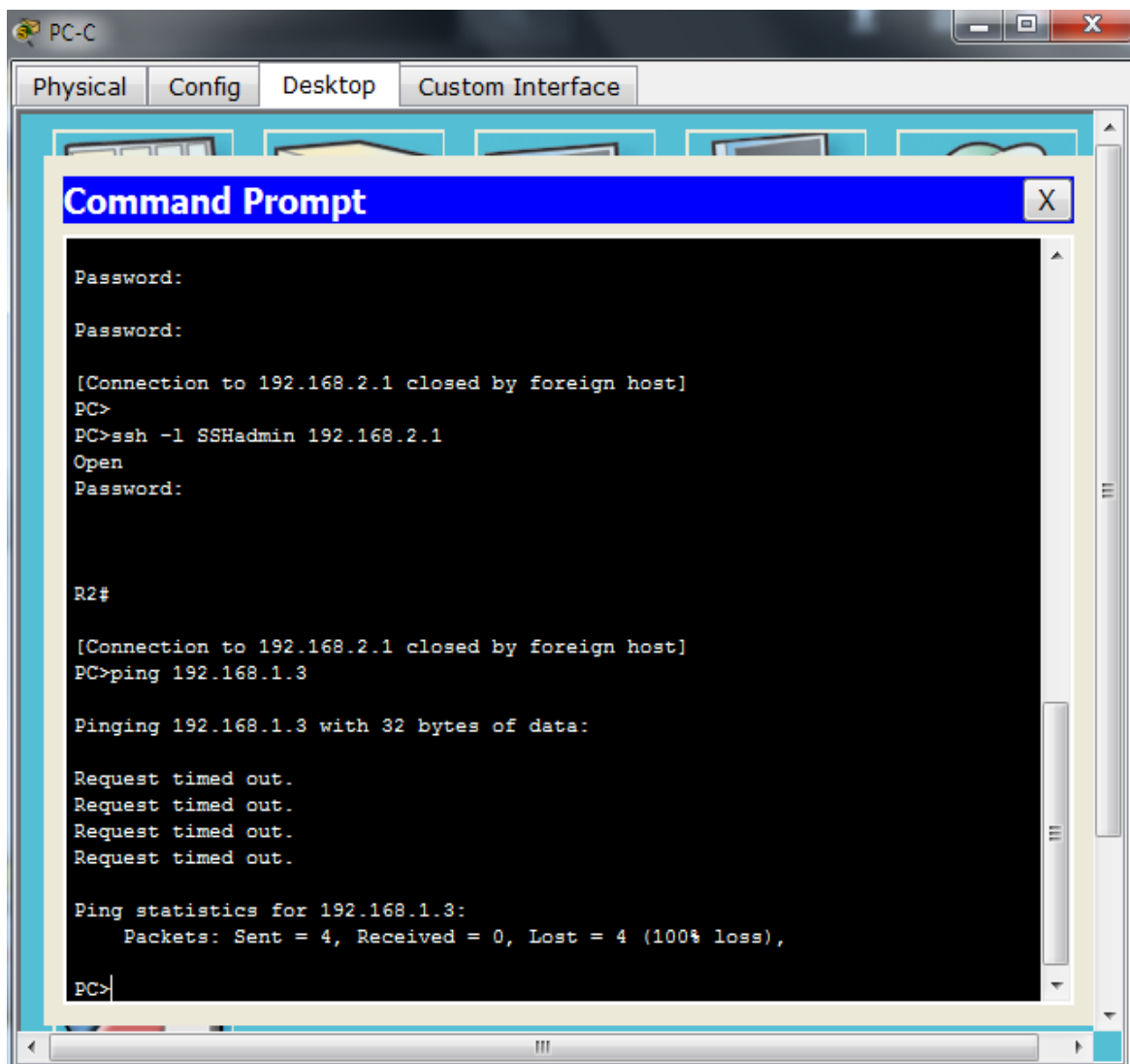
```
R3(config)#interface s0/0/1
R3(config-if)#ip access-group 100 in
R3(config-if)#exit
R3(config)#
```

Copy

Paste

### 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.



# Activity Results

Time Elapsed: 01:19:34

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Congratulations on completing this activity!

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

| Assessment Items | Status  | Points | Component(s) |
|------------------|---------|--------|--------------|
| Network          |         |        |              |
| R1               |         |        |              |
| ACL              |         |        |              |
| 10               | Correct | 1      | ACL          |
| 120              | Correct | 1      | ACL          |
| Ports            |         |        |              |
| Serial0/0/0      | Correct | 0      | Other        |
| Access-grou...   | Correct | 0      | ACL          |
| VTY Lines        |         |        |              |
| VTY Line 0       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 1       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 2       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 3       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 4       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| R2               |         |        |              |
| ACL              |         |        |              |
| 10               | Correct | 0      | ACL          |
| 120              | Correct | 1      | ACL          |
| VTY Lines        |         |        |              |
| VTY Line 0       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 1       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 2       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 3       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 4       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| R3               |         |        |              |
| ACL              |         |        |              |
| 10               | Correct | 1      | ACL          |
| 100              | Correct | 1      | ACL          |
| 110              | Correct | 1      | ACL          |
| Ports            |         |        |              |
| FastEthernet0/1  | Correct | 0      | Other        |
| Access-grou...   | Correct | 1      | ACL          |
| VTY Lines        |         |        |              |
| VTY Line 0       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 1       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 2       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 3       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |
| VTY Line 4       | Correct | 0      | Other        |
| Access Cont...   | Correct | 1      | ACL          |

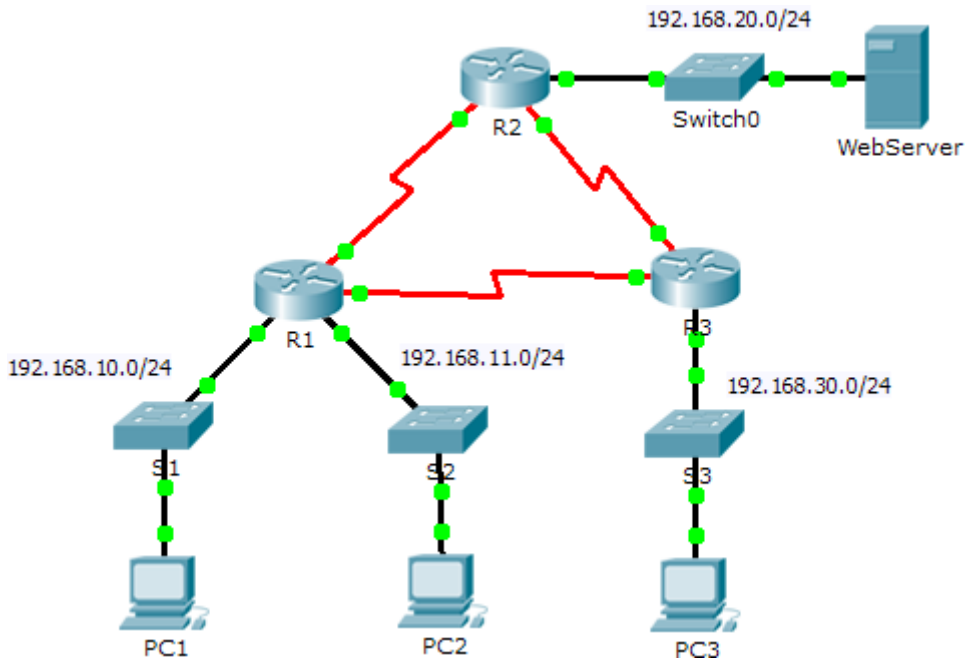
Score : 23/23

Item Count : 23/23

| Component | Items/Total | Score |
|-----------|-------------|-------|
| ACL       | 23/23       | 23/23 |

## 9.2.1.10 - CONFIGURING STANDARD ACLS

### Topology



### Addressing Table

| Device | Interface | IP Address   | Subnet Mask     | Default Gateway |
|--------|-----------|--------------|-----------------|-----------------|
| R1     | F0/0      | 192.168.10.1 | 255.255.255.0   | N/A             |
|        | F0/1      | 192.168.11.1 | 255.255.255.0   | N/A             |
|        | S0/0/0    | 10.1.1.1     | 255.255.255.252 | N/A             |
|        | S0/0/1    | 10.3.3.1     | 255.255.255.252 | N/A             |
| R2     | F0/0      | 192.168.20.1 | 255.255.255.0   | N/A             |
|        | S0/0/0    | 10.1.1.2     | 255.255.255.252 | N/A             |
|        | S0/0/1    | 10.2.2.1     | 255.255.255.252 | N/A             |
| R3     | F0/0      | 192.168.30.1 | 255.255.255.0   | N/A             |
|        | S0/0/0    | 10.3.3.2     | 255.255.255.252 | N/A             |
|        | S0/0/1    | 10.2.2.2     | 255.255.255.252 | N/A             |

|           |     |                |               |              |
|-----------|-----|----------------|---------------|--------------|
| PC1       | NIC | 192.168.10.10  | 255.255.255.0 | 192.168.10.1 |
| PC2       | NIC | 192.168.11.10  | 255.255.255.0 | 192.168.11.1 |
| PC3       | NIC | 192.168.30.10  | 255.255.255.0 | 192.168.30.1 |
| WebServer | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |

## Objectives

### Part 1: Plan an ACL Implementation

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

## Background / Scenario

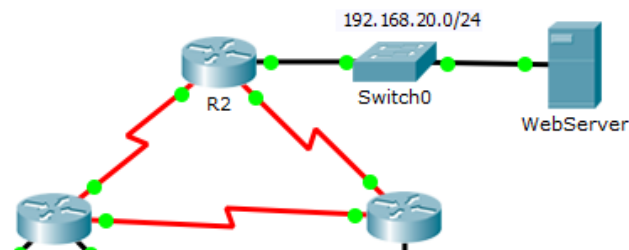
Standard access control lists (ACLs) are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the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

## Part 1: Plan an ACL Implementation

### Step 1: Investigate the current network configuration.

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

#### *Ping PSc y Dispositivos*



| re | Last Status | Source | Destination | Type | Color  | Time(sec) | Periodic | Num | Edit   | Delete   |
|----|-------------|--------|-------------|------|--------|-----------|----------|-----|--------|----------|
|    | Successful  | PC1    | PC2         | ICMP | Blue   | 0.000     | N        | 0   | (edit) | (delete) |
|    | Successful  | PC1    | PC3         | ICMP | Red    | 0.000     | N        | 1   | (edit) | (delete) |
|    | Successful  | PC2    | PC3         | ICMP | Green  | 0.000     | N        | 2   | (edit) | (delete) |
|    | Successful  | PC3    | PC1         | ICMP | Purple | 0.000     | N        | 3   | (edit) | (delete) |
|    | Successful  | PC2    | WebServer   | ICMP | Yellow | 0.000     | N        | 4   | (edit) | (delete) |

### 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 192.168.30/24 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#configure terminal
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 GigabitEthernet0/0
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(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
```

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

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

```
R2#show ip int 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
```

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

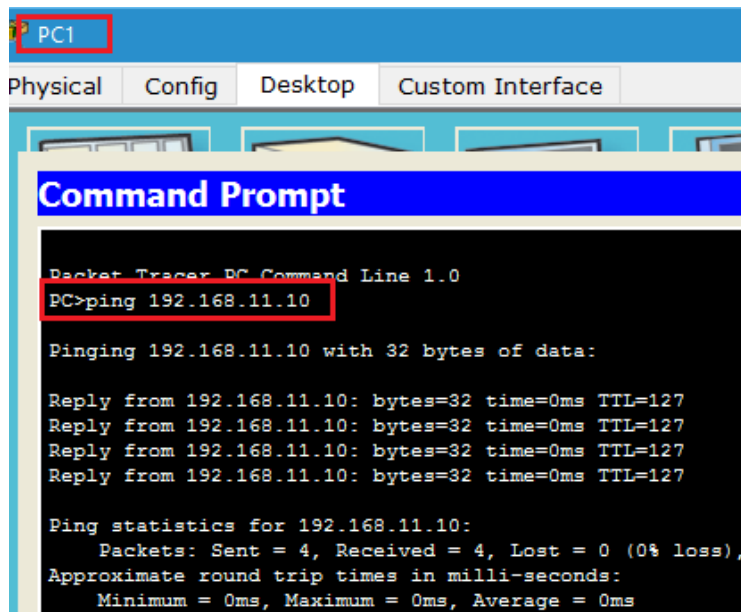
```
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
```



```
R3#show ip int 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
```

- 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.



- A ping from 192.168.10.10 to 192.168.20.254 succeeds.

PC1

Physical Config Desktop Custom Interface

### Command Prompt

```
PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

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

Ping statistics for 192.168.20.254:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

- A ping from 192.168.11.10 to 192.168.20.254 fails.

PC2

Physical Config Desktop Custom Interface

### Command Prompt

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

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 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.

PC1

Physical Config Desktop Custom Interface

### Command Prompt

```
PC>
PC>ping 192.168.30.10
Pinging 192.168.30.10 with 32 bytes of data:
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Ping statistics for 192.168.30.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- A ping from 192.168.11.10 to 192.168.30.10 succeeds.

PC2

Physical Config Desktop Custom Interface

### Command Prompt

```
PC>
PC>ping 192.168.30.10
Pinging 192.168.30.10 with 32 bytes of data:
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.30.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

- A ping from 192.168.30.10 to 192.168.20.254 succeeds.

The screenshot shows the Packet Tracer PC Command Line interface for PC3. The command prompt is `PC>ping 192.168.20.254`. The output shows four successful replies from 192.168.20.254 with 32 bytes of data, a time of 1ms, and a TTL of 126. The ping statistics for 192.168.20.254 are: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 7ms, Average = 2ms.

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=7ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.254:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 7ms, Average = 2ms

```

Conclusiones:

- Las listas de control de acceso permiten Limitar el tráfico de red y mejorar el rendimiento de la misma.
- Proporcionan un nivel básico de seguridad para el acceso a la red.
- Ayudan a establecer qué tipo de tráfico se envía o se bloquea en las interfaces del router.

## Activity Results

Time Elapsed: 01:07:14

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All

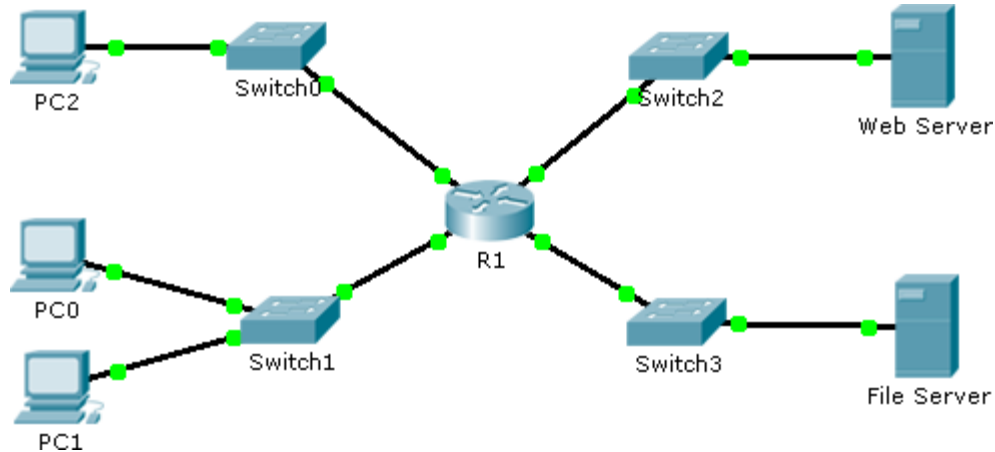
| Assessment Items   | Status  | Points |
|--------------------|---------|--------|
| Network            |         |        |
| R2                 |         |        |
| ACL                | Correct | 25     |
| Ports              |         | 0      |
| GigabitEthernet0/0 |         | 0      |
| Access-group ...   | Correct | 25     |
| R3                 |         |        |
| ACL                | Correct | 25     |
| Ports              |         | 0      |
| GigabitEthernet0/0 |         | 0      |
| Access-group ...   | Correct | 25     |

| Component                        | Items/Total | Score   |
|----------------------------------|-------------|---------|
| IPv4 Standard ACL Implementation | 4/4         | 100/100 |

Score : 100/100  
Item Count : 4/4

## 9.2.1.11 PACKETTRACER - CONFIGURING NAMED STANDARD ACLS

### Topology



### Addressing Table

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

### Objectives

**Part 1: Configure and Apply a Named Standard ACL**

**Part 2: Verify the ACL Implementation**

## Background / Scenario

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

### Part 1: Configure and Apply a Named Standard ACL

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

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

### Step 2: Configure a named standard ACL.

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

```
R1(config)# ip access-list standard File_Server_Restrictions
```

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

```
R1(config-std-nacl)# deny any
```

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router R1 connected to four switches (Switch0, Switch1, Switch2, Switch3). Switch0 and Switch1 are connected to PC2, PC0, and PC1. Switch2 is connected to a Web Server, and Switch3 is connected to a File Server. The bottom right pane shows the CLI for R1 with the following configuration:

```
R1>en
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1 (config)# ip access-list Restricciones de Servidor_de
Archivo_estndares
^
$ Invalid input detected at '^' marker.

R1 (config)# ip acceso-listar Restricciones de Servidor_de
Archivo_estndares
^
$ Invalid input detected at '^' marker.

R1 (config)# ip acceso-list standard
^
$ Invalid input detected at '^' marker.

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)#
```

Below the CLI, a table shows the interface configuration for R1:

| Interface | IP Address    | Subnet Mask   | Other Info |
|-----------|---------------|---------------|------------|
| 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        |

The bottom status bar indicates "Time Elapsed: 00:11:57" and "Completion: 80/100".

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

### Step 3: Apply the named ACL.

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

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

- b. Save the configuration.

The screenshot displays the Cisco Packet Tracer interface. On the left, a network topology is shown with a central router R1 connected to four switches (Switch0, Switch1, Switch2, Switch3). Switch0 and Switch1 are connected to PC2, PC0, and PC1 respectively. Switch2 and Switch3 are connected to a Web Server and a File Server respectively. The main window shows the CLI for R1 with the following configuration:

```
R1(config)# ip access-list standard
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)# int f0/1
R1(config-if)# ip access-group File_Server_Restrictions out
R1(config-if)# end
R1#
*SYS-5-CONFIG_I: Configured from console by console
R1#show access-list
R1#show access-list
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 deny any
R1#
```

Below the CLI window, a 'Realtime' section shows a table of traffic:

| Last Status | Source | Destination |
|-------------|--------|-------------|
| Successful  | PC1    | File Server |
| Successful  | PC0    | File Server |
| Successful  | PC2    | File Server |

At the bottom right, a 'Part 2: Verify the ACL Implementation' section contains the following text:

**Part 2: Verify the ACL Implementation**  
**Step 1: Verify the ACL configuration and application to the interface.**  
Use the **show access-lists** command to verify the ACL configuration. Use the **show run** or **show ip interface fastethernet 0/1** command to verify that the ACL is applied correctly to the interface.

### Part 2: Verify the ACL Implementation

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

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



The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router R1 connected to four switches (Switch0, Switch1, Switch2, Switch3). Switch0 is connected to PC2, Switch1 to PC0 and PC1, Switch2 to a Web Server, and Switch3 to a File Server. On the right, the CLI window for R1 shows the following output:

```

R1#show access-list
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.200.4
 20 deny any

R1#show ip int f0/1
FastEthernet0/1 is up, line protocol is up (connected)
 Internet address is 192.168.200.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is File_Server_Restrictions
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP 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

```

Below the CLI window, a task card titled "Step 1: Verify the ACL configuration and application to the interface." provides instructions: "Use the show access-lists command to verify the ACL configuration. Use the show run or show ip interface fastEthernet 0/1 command to verify that the".

Step 2: Verify that the ACL is working properly.

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

The screenshot shows a "PT Activity" window with the following content:

**Part 1: Configure and Apply a Named Standard ACL**

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

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

**Step 2: Configure a named standard ACL.**

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

```

R1(config)# ip access-list standard

```

At the bottom, the window shows "Tiempo Restante: 00:31:10", "Completion: 100/100", and buttons for "Arriba", "Verificar Resultados", "Reiniciar Actividad", and navigation arrows.



# Resultados de la Actividad

Tiempo Restante: 00:31:50

Felicitaciones Guest! Usted completó la actividad.

Retroalimentación General   **Objetos de Evaluación**   Pruebas de Conectividad

Expand/Collapse All

| Objetos de Evaluación      | Estado   | Puntos |
|----------------------------|----------|--------|
| Red                        |          |        |
| R1                         |          |        |
| Lista de Control de Acceso |          | 0      |
| File_Server_Restric...     | Correcto | 80     |
| Puertos                    |          | 0      |
| FastEthernet0/1            |          | 0      |
| Access-group Out           | Correcto | 20     |

Score : 100/100

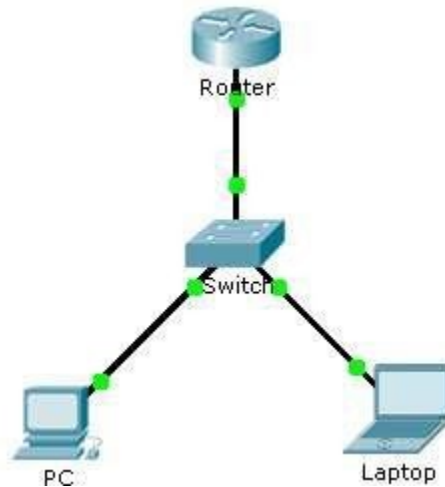
Item Count : 2/2

| Componente                       | Items/Total | Score   |
|----------------------------------|-------------|---------|
| IPv4 Standard ACL Implementation | 2/2         | 100/100 |

Cerrar

### 9.2.3.3 PACKET TRACER - CONFIGURING AN ACL ON VTY LINES

Topologia



#### Addressing Table

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

#### Objectives

**Part 1: Configure and Apply an ACL to VTY Lines**

**Part 2: Verify the ACL Implementation**

#### Background

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

## Part 1: Configure and Apply an ACL to VTY Lines

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

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

### Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on Router.

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

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

The screenshot shows a Packet Tracer activity window on the left and a router CLI window on the right. The activity window contains the following text:

**Part 1: Configure and Apply an ACL to VTY Lines**  
**Part 2: Verify the ACL Implementation**

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

**Part 1: Configure and Apply an ACL to VTY Lines**

**Step 1: Verify Telnet access before the ACL is configured.**  
Both computers should be able to Telnet to the Router. The password is **cisco**.

**Step 2: Configure a numbered standard ACL.**  
Configure the following numbered ACL on Router.  

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

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

**Step 3: Place a named standard ACL on the router.**  
Access to the Router interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of Router, enter line configuration mode for lines 0 – 4 and use the **access-class** command to apply the ACL to all the VTY lines:

The router CLI window shows the following output:

```
IOS Command Line Interface
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 263952K/8192K
bytes of memory
Processor board ID JAD06190MT2 (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

!LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

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

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

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

```
Router(config)# line vty 0 15
```

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

PT Activity: 00:19:50

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

**Step 2: Configure a numbered standard ACL.**  
 Configure the following numbered ACL on Router.  
 Router(config)# access-list 99 permit host 10.0.0.1

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

**Step 3: Place a named standard ACL on the router.**  
 Access to the Router interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of Router, enter line configuration mode for lines 0 – 4 and use the access-class command to apply the ACL to all the VTY lines:  
 Router(config)# line vty 0 15  
 Router(config-line)# access-class 99 in

**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.

**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.

Time Elapsed: 00:19:50      Completion: 100/100

Router

Physical   Config   CLI   Attributes

IOS Command Line Interface

```
M360 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

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

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy   Paste

PC

Lower Cycle Devices

Top

(Select a Device to Ping and Ping to the Workspaces)

## 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.

#### 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.

##### 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.

Time Elapsed: 00:22:16      Completion: 100/100

Router

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

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

Router#
```

Copy   Paste

Top

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

### Step 2: Configure a numbered standard ACL.

Configure the following numbered ACL on Router.

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

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

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

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

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

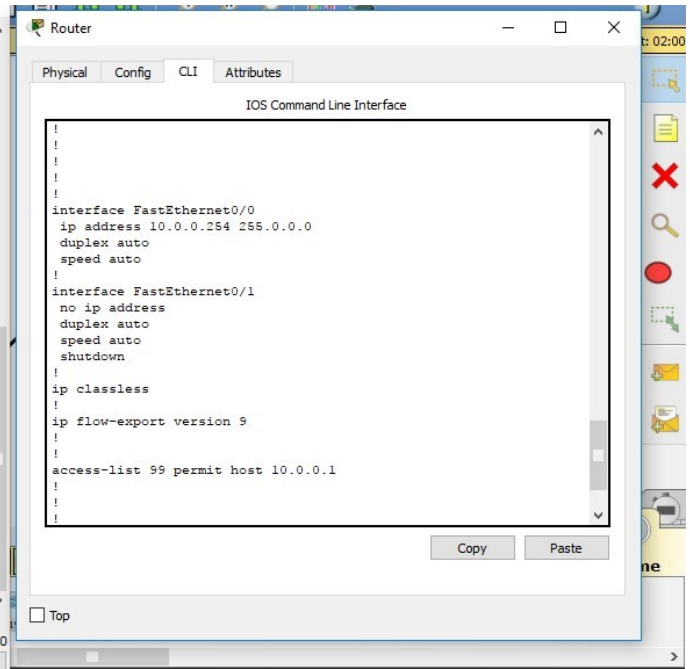
## Part 2: Verify the ACL Implementation

### 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.

### Step 2: Verify that the ACL is working properly.

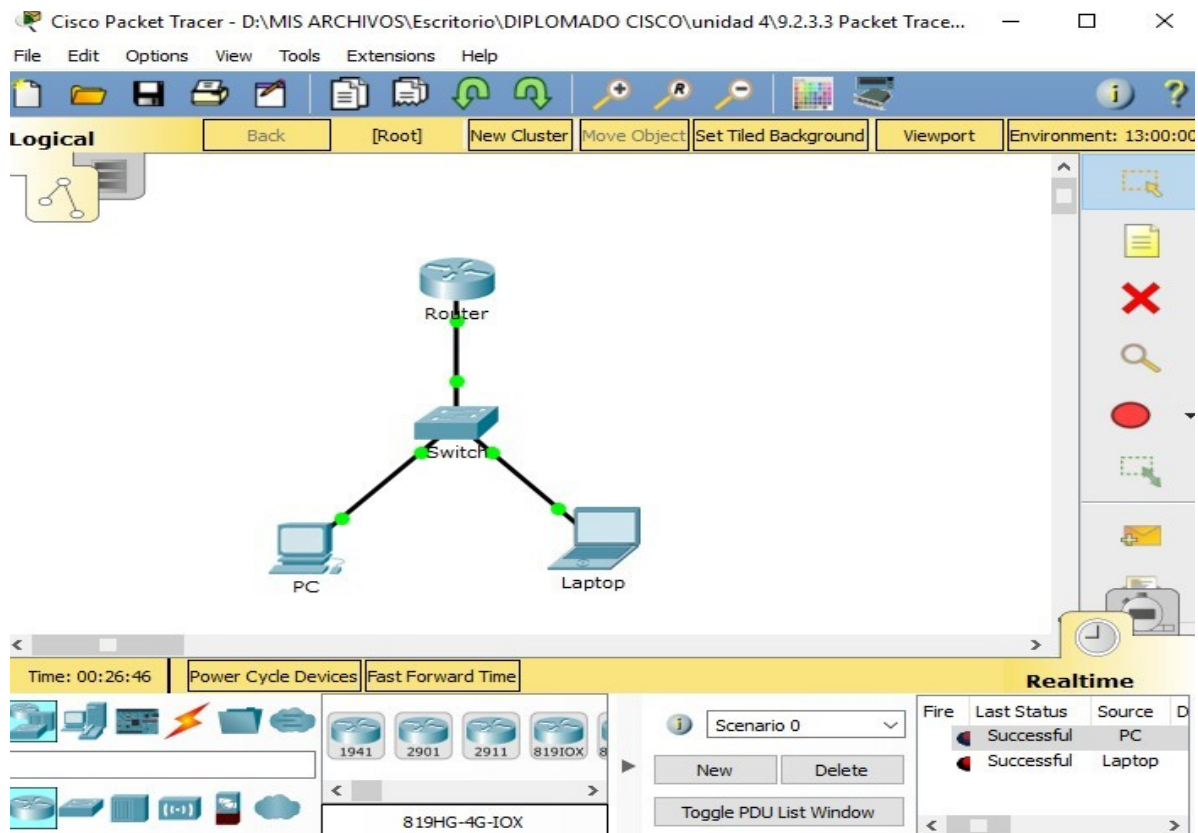
Both computers should be able to ping the Router, but only PC should be able to Telnet to it.



```
Router
Physical Config CLI Attributes
IOS Command Line Interface
!
!
!
!
interface FastEthernet0/0
ip address 10.0.0.254 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 99 permit host 10.0.0.1
!
!
!
Copy Paste
```

## 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.



Cisco Packet Tracer - D:\MIS ARCHIVOS\Escritorio\DIPLOMADO CISCO\unidad 4\9.2.3.3 Packet Trace...

File Edit Options View Tools Extensions Help

Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Environment: 13:00:00

Router

Switch

PC Laptop

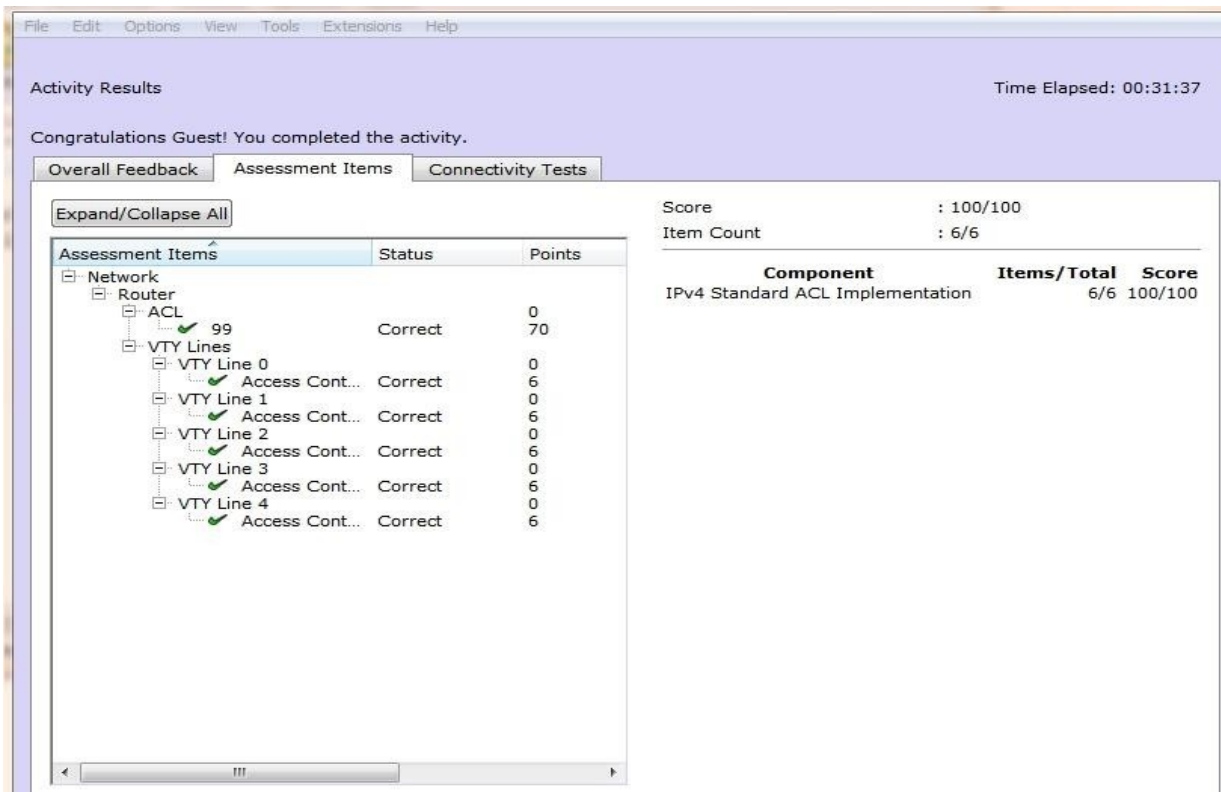
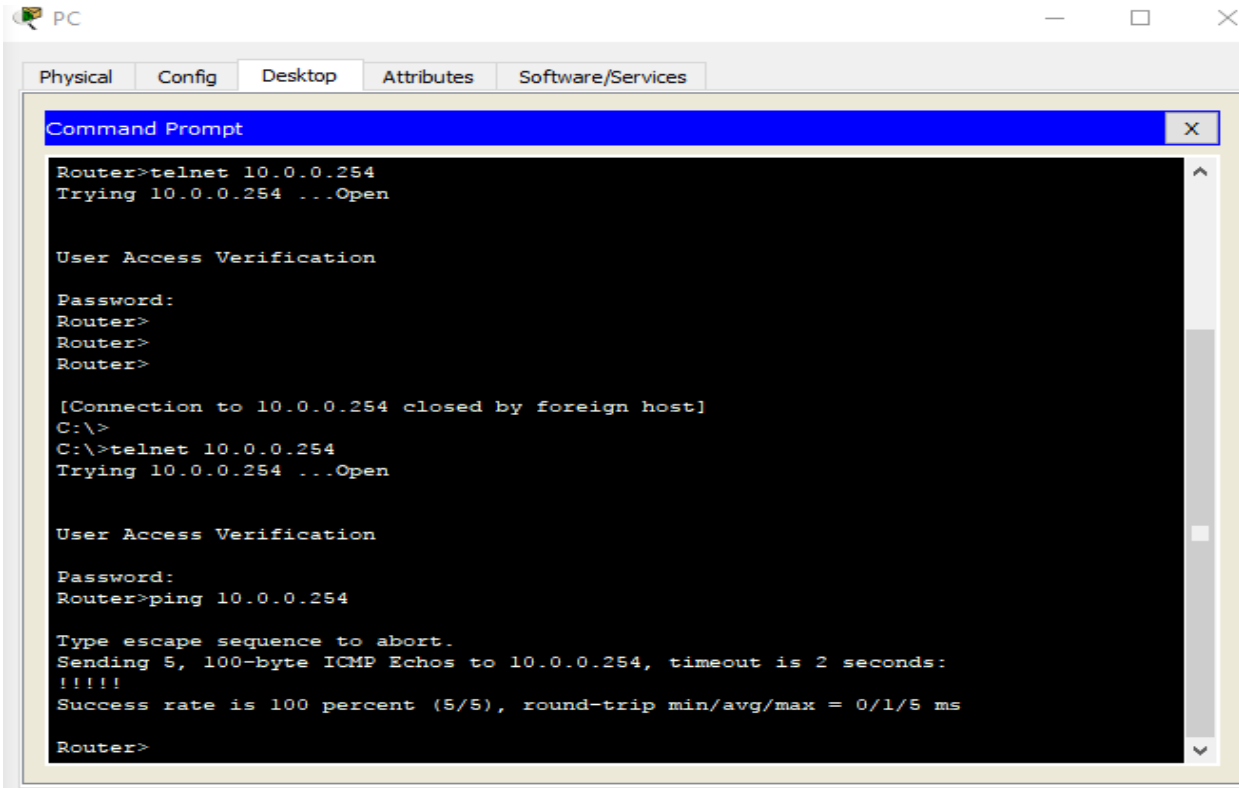
Time: 00:26:46 Power Cycle Devices Fast Forward Time

Scenario 0

New Delete

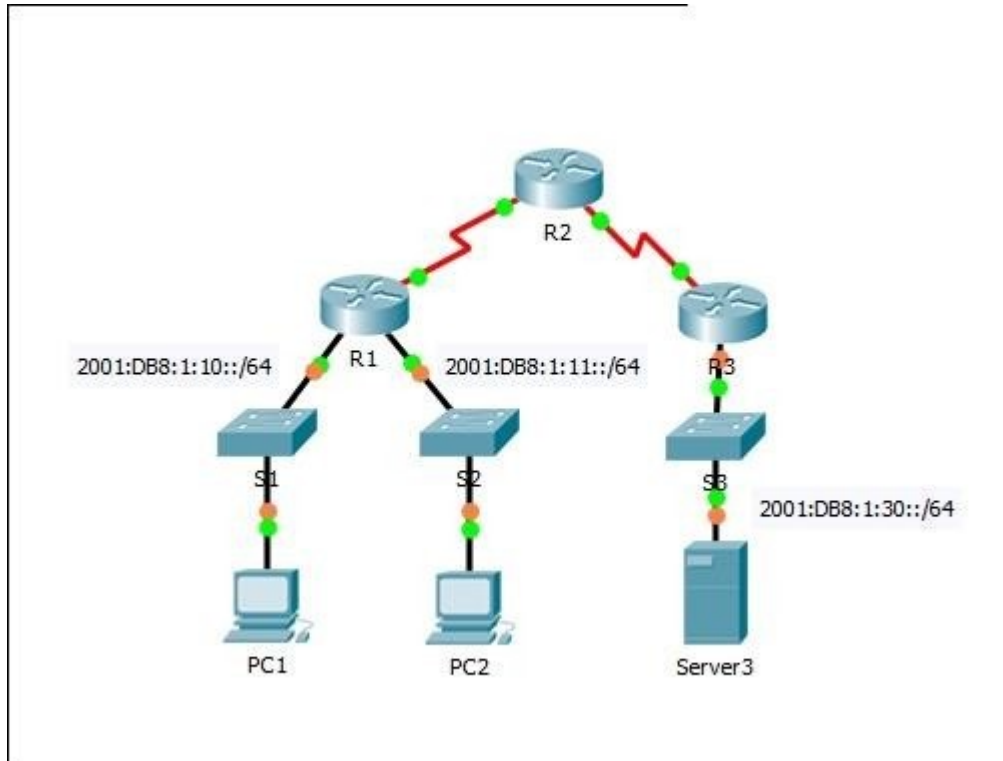
Toggle PDU List Window

| Fire | Last Status | Source | D |
|------|-------------|--------|---|
|      | Successful  | PC     |   |
|      | Successful  | Laptop |   |



## 9.5.2.6 PACKET TRACER - CONFIGURING IPV6 ACLS

### Topology



### Addressing Table

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

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

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

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

Configure an ACL named **BLOCK\_HTTP** on **R1** with the following statements.

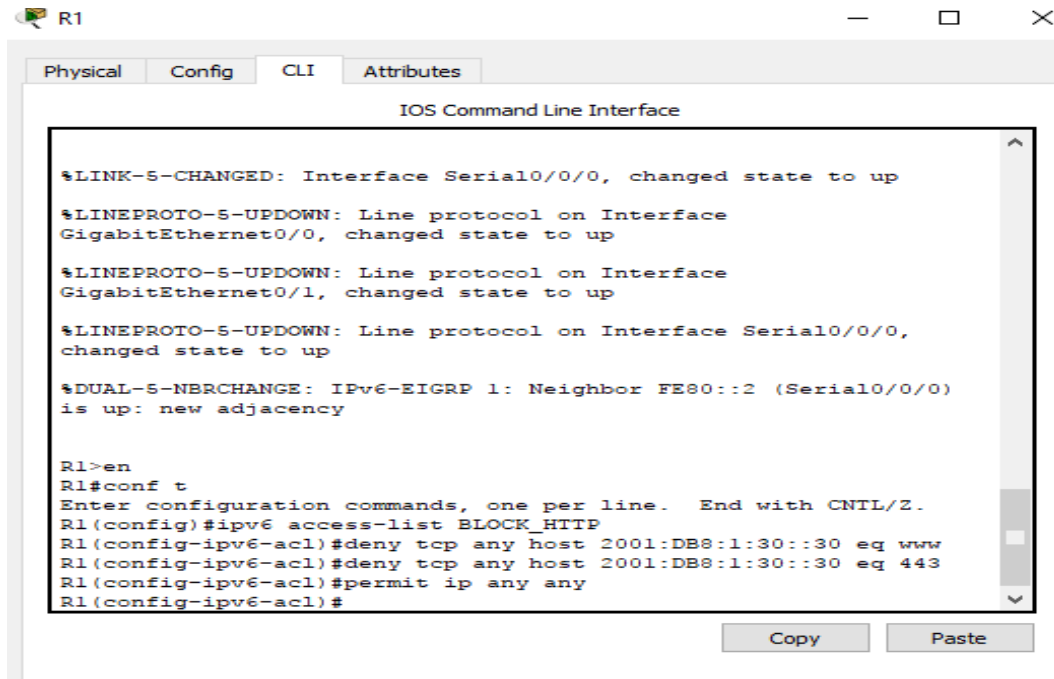
- Block HTTP and HTTPS traffic from reaching **Server3**.



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

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

- b. Allow all other IPv6 traffic to pass.



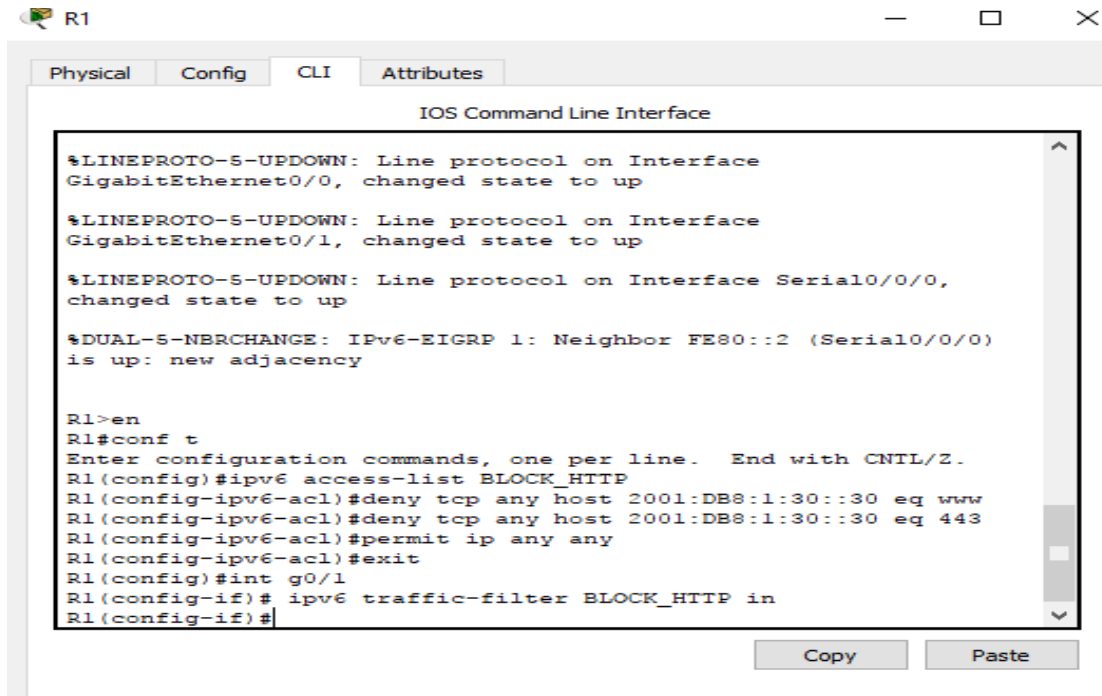
The screenshot shows a terminal window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows several system messages indicating interface state changes for Serial0/0/0 and GigabitEthernet0/0 and 0/1. The user then enters the command "R1>en" to enter enable mode, followed by "R1#conf t" to enter configuration mode. The user configures an IPv6 access list named "BLOCK\_HTTP" with the following commands: "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", and "R1(config-ipv6-acl)#permit ip any any". The terminal ends with "R1(config-ipv6-acl)#".

## 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-if)# ipv6 traffic-filter BLOCK_HTTP in
```

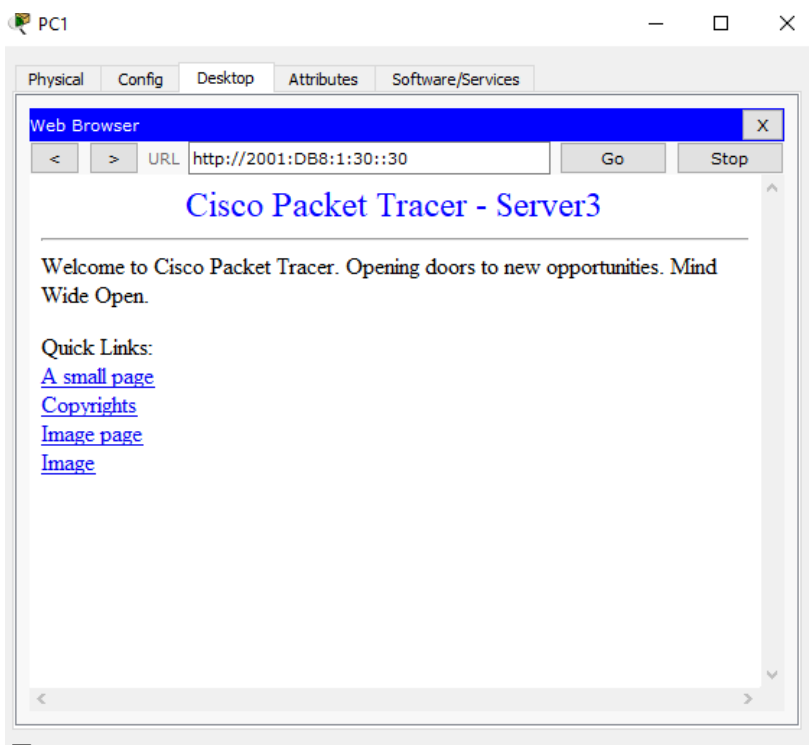




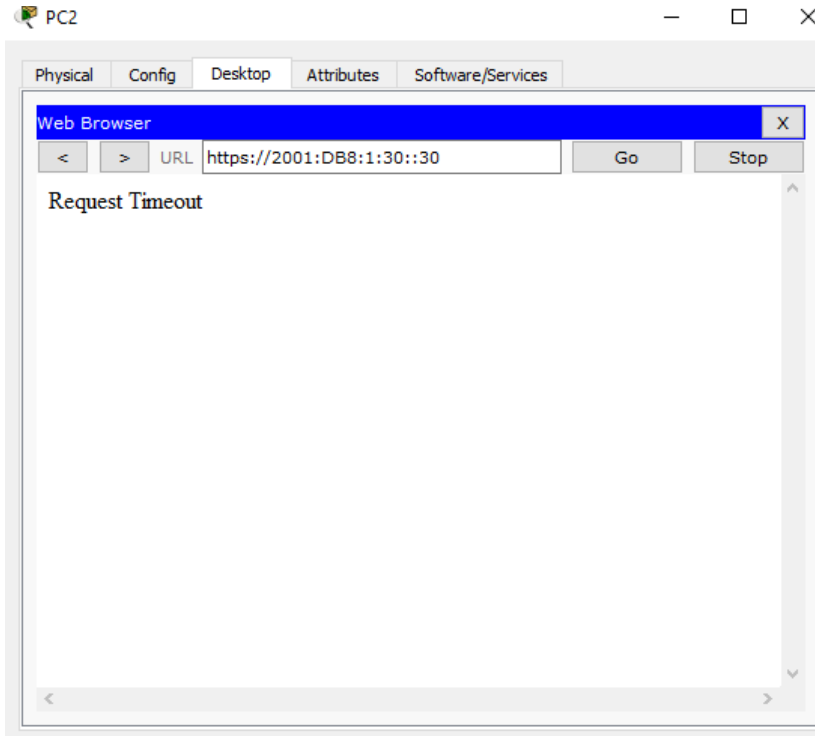
### Step 3: Verify the ACL implementation.

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

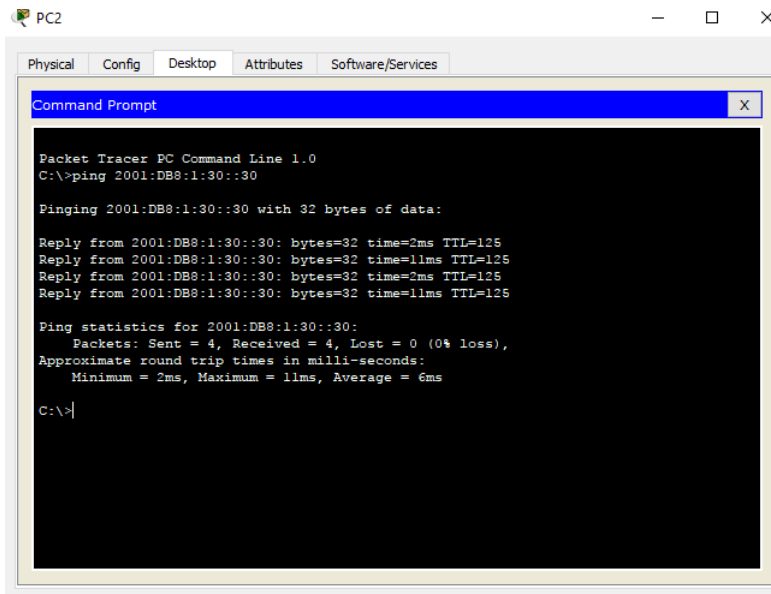
- Open the web browser of PC1 to <http://2001:DB8:1:30::30> or <https://2001:DB8:1:30::30>. The website should appear.



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



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



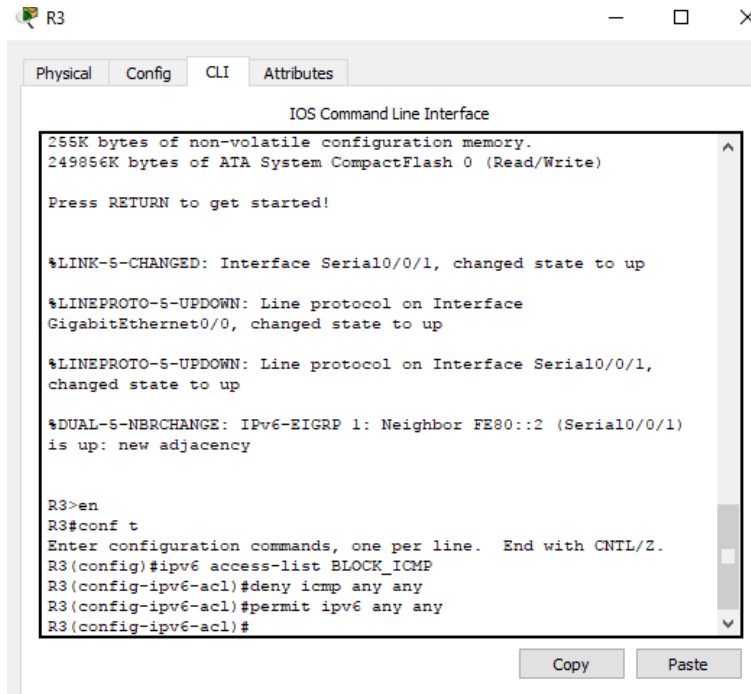
## Part 2: Configure, Apply, and Verify a Second IPv6 ACL

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.
- b. Allow all other IPv6 traffic to pass.



```
R3
IOS Command Line Interface
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

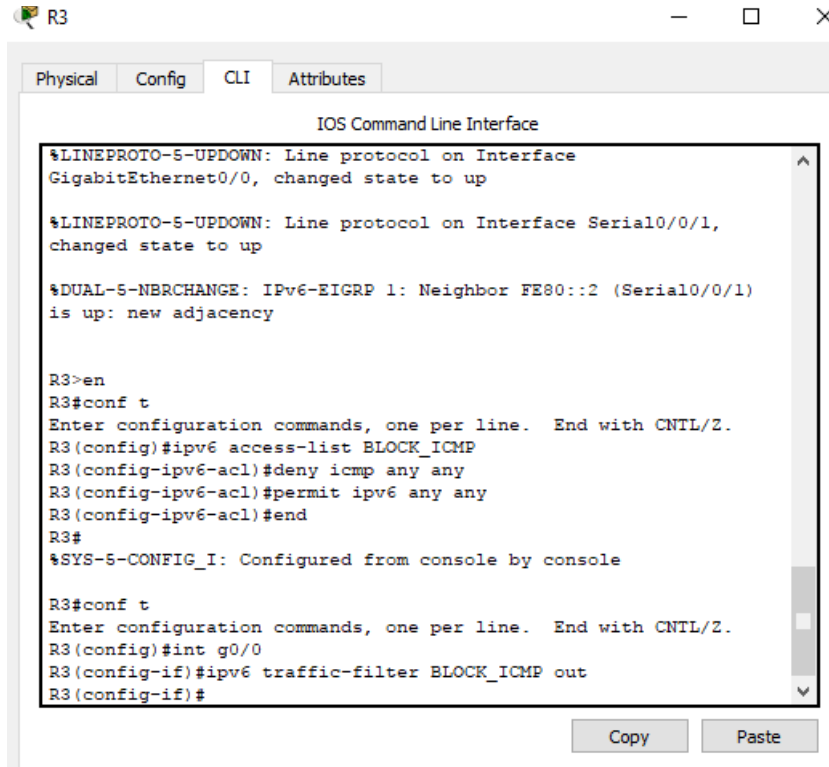
Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/1)
is up: new adjacency

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)#
```

## 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

Physical Config CLI Attributes

IOS Command Line Interface

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

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

%DUAL-5-NBRCHANGE: IPv6-EIGRP 1: Neighbor FE80::2 (Serial0/0/1)
is up: new adjacency

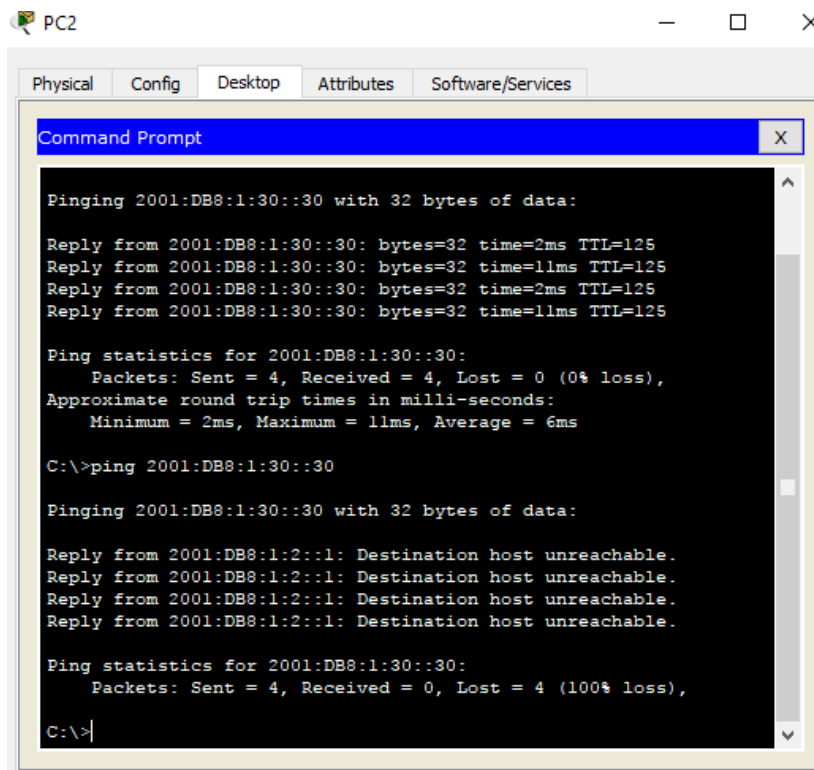
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
R3(config-if)#
```

Copy Paste

### Step 3: Verify that the proper access list functions.

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



PC2

Physical Config Desktop Attributes Software/Services

Command Prompt

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

Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=11ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>ping 2001:DB8:1:30::30

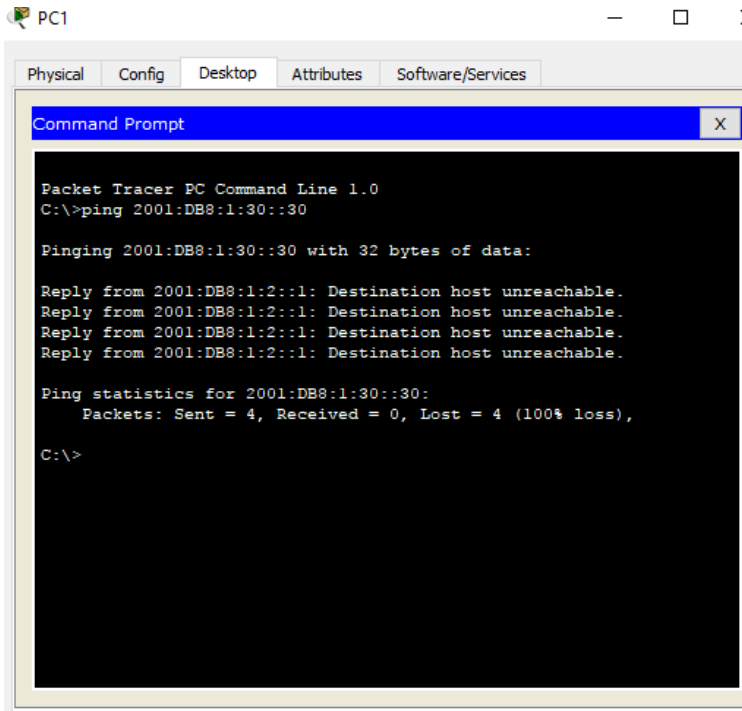
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

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.

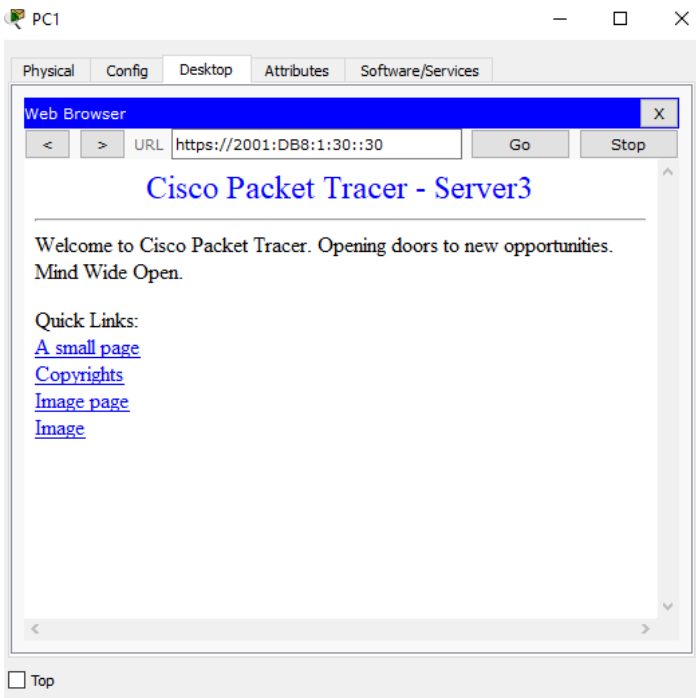
Ping statistics for 2001:DB8:1:30::30:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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



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



**RESULTADO// 100/100**

Activity Results Time Elapsed: 01:06:44

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All

| Assessment Items   |                         | Sta |
|--------------------|-------------------------|-----|
| Network            |                         |     |
| R1                 |                         |     |
| ACLV6              | ✓ BLOCK_HTTP            | Cor |
| Ports              |                         |     |
| GigabitEthernet0/1 | ✓ IPv6 Traffic Filte... | Cor |
| R3                 |                         |     |
| ACLV6              | ✓ BLOCK_ICMP            | Cor |
| Ports              |                         |     |
| GigabitEthernet0/0 | ✓ IPv6 Traffic Filte... | Cor |

| Component               | Items/Total | Score   |
|-------------------------|-------------|---------|
| IPv6 ACL Implementation | 4/4         | 100/100 |

< [ ] >

Close



## CONCLUSIONES

Podemos concluir que cuando se desarrolla las practicas conocemos que los routers utilizan protocolos de routing dinámico, lo cual consiste en el intercambio de información de routing por lo tanto logra, detección de redes remotas, mantenimiento de información de routing, uso de la mejor ruta hacia las redes de destino, pero con capacidad para encontrar una mejor ruta nueva si la ruta actual no está disponible.

OSPF es un protocolo de routing de estado de enlace sin clase, se indica en la tabla de routing con el código de origen de ruta O, se habilita con el comando `router ospf id-proceso` del modo de configuración global, no necesita coincidir con otros routers OSPF para establecer adyacencias con esos vecinos.

Para que los routers establezcan una adyacencia, sus intervalos de saludo, intervalos muertos, tipos de red y máscaras de subred deben coincidir. Con el comando `show ip ospf neighbors` verificamos las adyacencias OSPF.

El comando `show ip protocols` se utiliza para verificar la información importante de configuración OSPF, incluidas la ID del proceso OSPF, la ID del router y las redes que anuncia el router.

Las ACL extendidas filtran paquetes según varios atributos, como el tipo de protocolo, la dirección IPv4 de origen o de destino y los puertos de origen o de destino, teniendo en cuenta que para la colocación de una ACL extendida es colocarla lo más cerca posible del origen.

En cuanto a DHCP en redes, se establece cuando todos los dispositivos de red se asigna una única dirección IP de forma estática, para permitir la comunicación, pero para ser más eficiente y con menos carga de trabajo para los administradores se hace la configuración dinámica, mediante el uso de DHCPv4 o DHCPv6 según los requerimientos de versión de IP.

NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones. NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al proveedor de internet (ISP.)



## RECOMENDACIONES

- Es necesario saber y conocer a fondo el tema de las conexiones de redes, debido a que si se realiza una conexión de datos incorrecta a ningún momento se va a poder establecer contacto entre las mismas, causando una pérdida de tiempo, dinero, etc.
- Tanto el emulador como la simulación de la red deben estar bien instalados, configurados, además de digitar bien los comandos, para que se ejecuten correctamente, cumplan las funciones programadas, de esta manera la red rendirá y cumplirá cada paso de la programación correspondiente sin ningún problema.

## REFERENCIAS BIBLIOGRÁFICAS.

- CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>
- CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>
- CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>
- CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado De <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>
- CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>
- CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>
- CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>
- CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>
- CISCO. (2014). Soluciones de Red. Fundamentos de Networking.