

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

PRESENTADO POR:  
JARELIS BARRIOS SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS DE LA TECNOLOGÍA E INGENIERÍA  
PROGRAMA DE INGENIERÍA DE SISTEMAS  
CARTAGENA-BOLÍVAR  
2019

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

PRESENTADO POR:  
JARELIS BARRIOS SANABRIA

PASO 11 - PRUEBA DE HABILIDADES PRÁCTICAS CCNA  
TRABAJO FINAL

TUTOR:  
GIOVANNI ALBERTO BRACHO  
GRUPO\_203092\_20

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS DE LA TECNOLOGÍA E INGENIERÍA  
PROGRAMA DE INGENIERÍA DE SISTEMAS  
CARTAGENA – BOLÍVAR  
2019

## TABLA DE CONTENIDO

	Pág.
Índice de Ilustraciones .....	5
Índice de Tablas.....	6
Introducción .....	7
Objetivos.....	8
OBJETIVO GENERAL .....	8
Objetivos Especificos.....	8
Descripción general de la prueba de habilidades.....	9
Escenario 1 .....	9
1. Configuración del enrutamiento .....	12
2. Tabla de Enrutamiento .....	15
3. Deshabilitar la propagación del protocolo RIP .....	17
4. Verificación del protocolo RIP.....	18
5. Configurar encapsulamiento y autenticación PPP .....	19
6. Configuración de PAT.....	21
7. Configuración del servicio DHCP.....	25
Escenario 2.....	28
1. Configurar el direccionamiento IP.....	29
2. Configurar el protocolo de enrutamiento OSPFv2 .....	32
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches .....	37
4. En el Switch 3 deshabilitar DNS lookup.....	39
5. Asignar direcciones IP a los Switches acorde a los lineamientos.....	40
6. Desactivar todas las interfaces .....	40
7. Implement DHCP and NAT for IPv4 .....	40
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40 .....	40
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40.....	40

10.	Configurar NAT en R2 .....	41
11.	Configurar al menos dos listas de acceso de tipo estándar .....	41
12.	Configurar al menos dos listas de acceso de tipo extendido .....	42
13.	Verificar procesos de comunicación y redireccionamiento de tráfico.....	42
	CONCLUSIONES .....	44
	BIBLIOGRAFIA.....	45

## ÍNDICE DE ILUSTRACIONES

Ilustración 1 Tipología de Red I .....	9
Ilustración 2 Tipología de Red II .....	10
Ilustración 3 Ping de PC0 a PC1.....	15
Ilustración 4 Ping de PC1 a PC0.....	16
Ilustración 5 Ping de PC2 a PC3.....	16
Ilustración 6 Comando Show ip route - Práctica en el Router de Medellín .....	18
Ilustración 7 Comando Show ip Protocol .....	19
Ilustración 8 Verificación de autenticación por PAP EN MEDELLIN1 Por Ping hacia ISP .....	20
Ilustración 9 Verificación de autenticación por CHAP EN BOGOTA1 Por Ping hacia ISP .....	21
Ilustración 10 Ping PC2 a ISP .....	23
Ilustración 11 Ping PC0 a ISP .....	24
Ilustración 12 Ping de PC2 a PC0.....	25
Ilustración 13 Verificación del servicio DHCP en funcionamiento en la red por PING. ....	27
Ilustración 14 Administración de red escenario 2-A .....	28
Ilustración 15 Administración de red escenario 2-B .....	29
Ilustración 16 R3 .....	31
Ilustración 17 Internet pc comand prompt .....	31
Ilustración 18 Configuración en R1 .....	33
Ilustración 19 Configuración en R2-A .....	34
Ilustración 20 Configuración en R2-B .....	34
Ilustración 21 Configuración en R3-A .....	35
Ilustración 22 Configuración en R3-B .....	36
Ilustración 23 Ping R2 a R1 .....	42
Ilustración 24 Traceroute R2 a R1 .....	43

## ÍNDICE DE TABLAS

Tabla 1 Interfaces Sin Necesidad a la Desactivación .....	17
Tabla 2 OSPFv2 área 0 .....	32
Tabla 3 Configuración en R1-A.....	40
Tabla 4 Configuración en R1-B.....	41

## INTRODUCCIÓN

En la realización de la presente evaluación denominada como “Prueba de Habilidades prácticas”, se proponen dos (2) escenarios como solución a las diversas pruebas y habilidades adquiridas a lo largo del curso de Diplomado de profundización CCNA CISCO, en torno a todo lo que tiene que ver con el modelamiento de fundamentos de Networking, modelo OSI y direccionamiento IP, configuración de sistemas de red soportados en VLANs y enrutamiento en soluciones de red.

Abarcando los temas indicados, previstos con anterioridad, bajo la sustentación de prácticas de laboratorio asociados en eventos virtuales y en entornos de simulación en la mayoría a la herramienta relacionada como Packet Tracer, apoyadas en la creación, diseño y configuración de topologías adscritas a dispositivos de comunicación, con el fin de orientar hacia el buen sentido de apropiación de conocimientos prácticos para así poder influenciarlos dentro del campo y entorno tanto personal como profesional, en lo que referencia al modelamiento de redes de telecomunicaciones

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Realizar y desarrollar los dos escenarios propuestos como prueba de habilidades practicas del Diplomado de Profundización CCNA demostrando todos los conocimientos adquiridos durante el proceso.

### **OBJETIVOS ESPECIFICOS:**

- Plantear y desarrollar de forma efectiva los dos escenarios propuestos en la actividad
- Investigar e implementar PAT en CISCO
- Investigar mas a fondo los temas manejados en el desarrollo de la actividad
- Aplicar todos los conocimientos adquiridos en el proceso del diplomado
- Implementar herramienta Packet Tracer en los ejercicios planteados
- Documentar el desarrollo de los dos escenarios



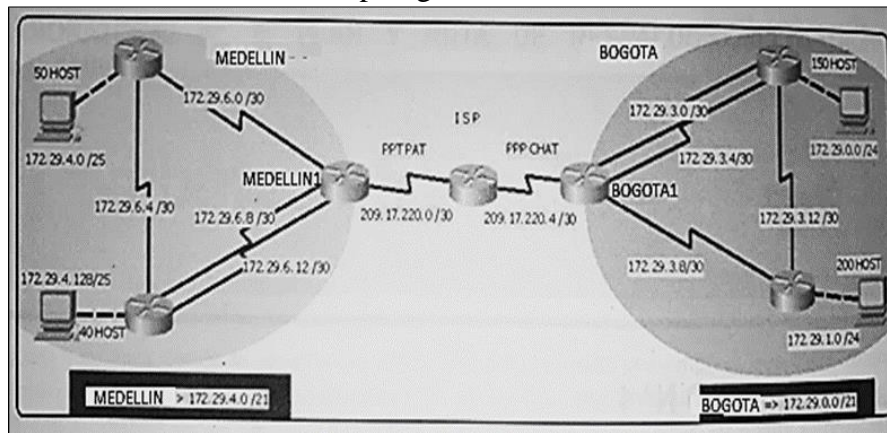
# DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES

## ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red

### Topología de red

Ilustración 1  
Tipología de Red I



Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

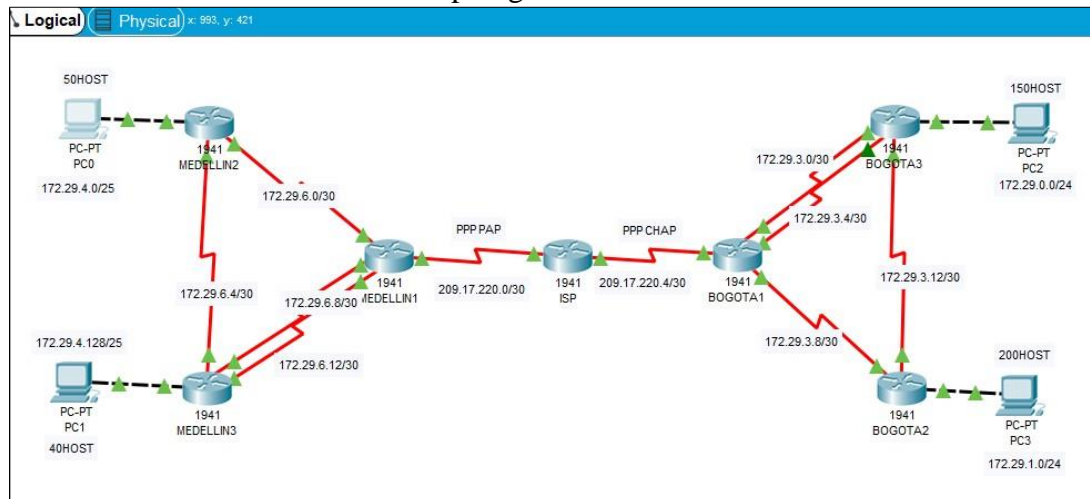
Debe configurar PPP en los enlaces hacia el ISP, con autenticación. Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

### Desarrollo

Como trabajo inicial se debe realizar lo siguiente:

Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Ilustración 2  
Tipología de Red II



Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

A continuación se realiza la respectiva configuración básica de de los router en cada ciudad, configuración como habilitar la opción de encriptación para las contraseñas, asignación de los nombres de los router:

### Configuración Básica ISP

```
#Hostname: ISP
#Enable secret: itsasecret
#Password Line Console 0: cisco
#Password Line vty 0 15: cisco
#Service password-encryption
#Banner motd "Acceso solo al personal autorizado"
```

### Configuración Básica MEDELLIN1

```
# Hostname MEDELLIN
# Enable secret: itsasecret
```

```
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

### **Configuración Básica BOGOTA1**

```
# Hostname BOGOTA
# Enable secret: itsasecret
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

### **Configuración Básica MEDELLIN2**

```
#Hostname MEDELLIN2
# Enable secret: itsasecret
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

### **Configuración Básica BOGOTA2**

```
# Hostname BOGOTA2
# Enable secret: itsasecret
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

### **Configuración Básica MEDELLIN3**

```
# Hostname MEDELLIN3
# Enable secret: itsasecret
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

## **Configuración Básica BOGOTA3**

```
# Hostname BOGOTA3
# Enable secret: itsasecret
# Password Line Console 0: cisco
# Password Line vty 0 15: cisco
# Service password-encryption
# Banner motd "Acceso solo al personal autorizado"
```

### **1. Configuración del enrutamiento**

- a. Configurar el enrutamiento en la red usando el protocolo RIP versión 2, declare la red principal, desactive la sumarización automática.

A continuación, se implementa el protocolo RIP en su versión 2 de acuerdo al enunciado, además se desactiva la sumarización automática en ciertas interfaces:

## **Configuración RIPv2 en MEDELLIN1**

```
# Router rip
# Version 2
# No auto-summary
# Do show ip route connected
# Network 172.29.6.0
# Network 172.29.6.8
# Network 172.29.6.12
# Passive-interface s0/0/0 (WAN A ISP).
```

## **Configuración RIPv2 en BOGOTA1**

```
# Router rip
# Version 2
# No auto-summary
# Do show ip route connected # Network 172.29.3.0
# Network 172.29.3.4
# Network 172.29.3.8
# Passive-interface s0/0/0
```

## **Configuración RIPv2 en MEDELLIN2**

```
# Router rip
# Version 2
# No auto-summary
# Do show ip route connected
# Network 172.29.4.0
# Network 172.29.6.0
# Network 172.29.6.4
# Passive-interface g0/0
```

## **Configuración RIPv2 en BOGOTA2**

```
# Router rip
# Version 2
# No auto-summary
# Do show ip route connected
# Network 172.29.1.0
# Network 172.29.3.8
# Network 172.29.3.12
# Passive-interface s0/0/0
```

## **Configuración RIPv2 en MEDELLIN3**

```
# Router rip
# Version 2
# No auto-summary
# Do show ip route connected
# Network 172.29.4.128
# Network 172.29.6.4
# Network 172.29.6.8
# Network 172.29.6.12
# Passive-interface g0/0
```

## **Configuración RIPv2 en BOGOTA3**

```
# Router rip
# Version 2
# No auto-summary
```

```
# Do show ip route connected
# Network 172.29.0.0
# Network 172.29.3.0
# Network 172.29.3.4
# Network 172.29.3.12
# Passive-interface s0/0/0
```

- b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de RIP.

**Se asigna un ruta por defecto a cierto router según el enunciado:**

#### **Configuración MEDELLIN1 a ISP**

```
#Configure terminal
#Ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

#### **Configuración BOGOTA1 a ISP**

```
#Configure terminal
#Ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

- c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22.

**Se configura unas Rutas Estáticas del ISP con los router Bogotá y Medellín:**

```
#Ip route 172.29.4.0 255.255.252.0 209.17.220.2
#Ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

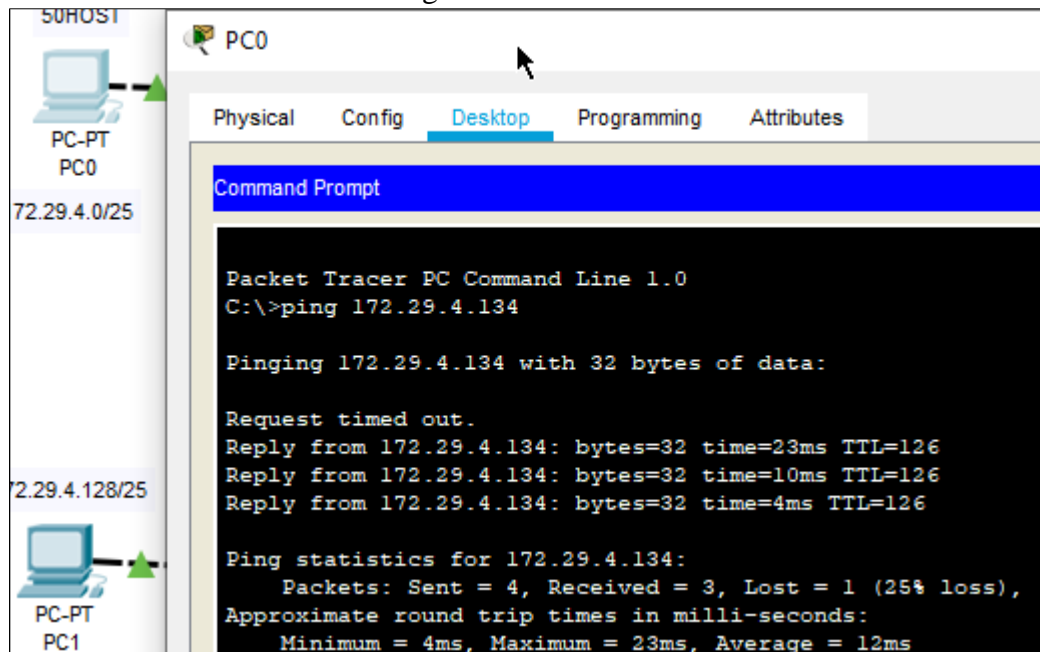
## 2. Tabla de Enrutamiento.

- a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

### Pruebas de conectividad (mediante PING)

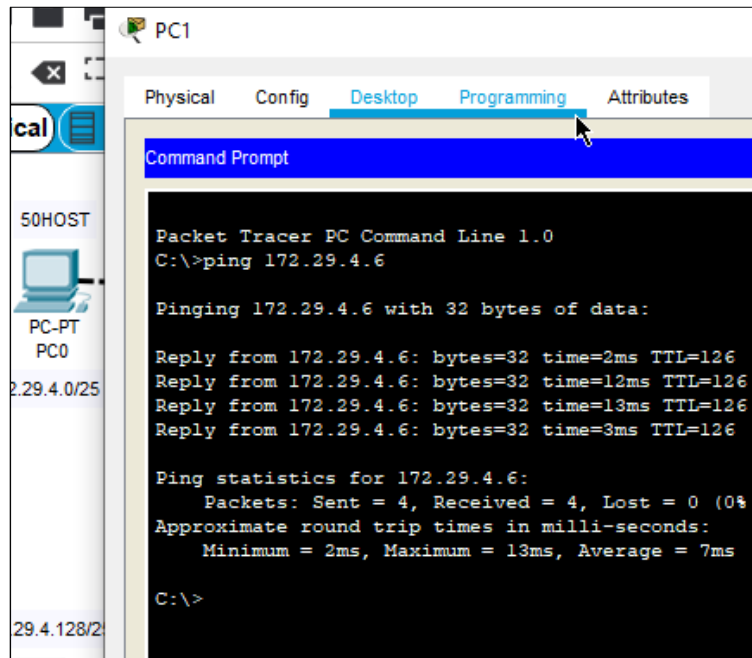
#### Ping de PC0 a PC1

Ilustración 3  
Ping de PC0 a PC1



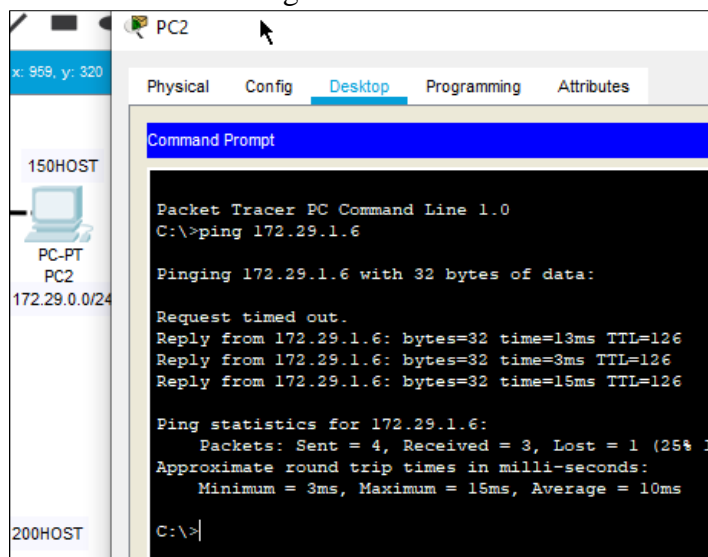
#### Ping de PC1 a PC0

Ilustración 4  
Ping de PC1 a PC0



Ping de PC2 a PC3

Ilustración 5  
Ping de PC2 a PC3





- b. Verificar el balanceo de carga que presentan los routers.
- c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
- d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.
- e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

### 3. Deshabilitar la propagación del protocolo RIP.

- a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo RIP, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 1  
Interfaces Sin Necesidad a la Desactivación

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

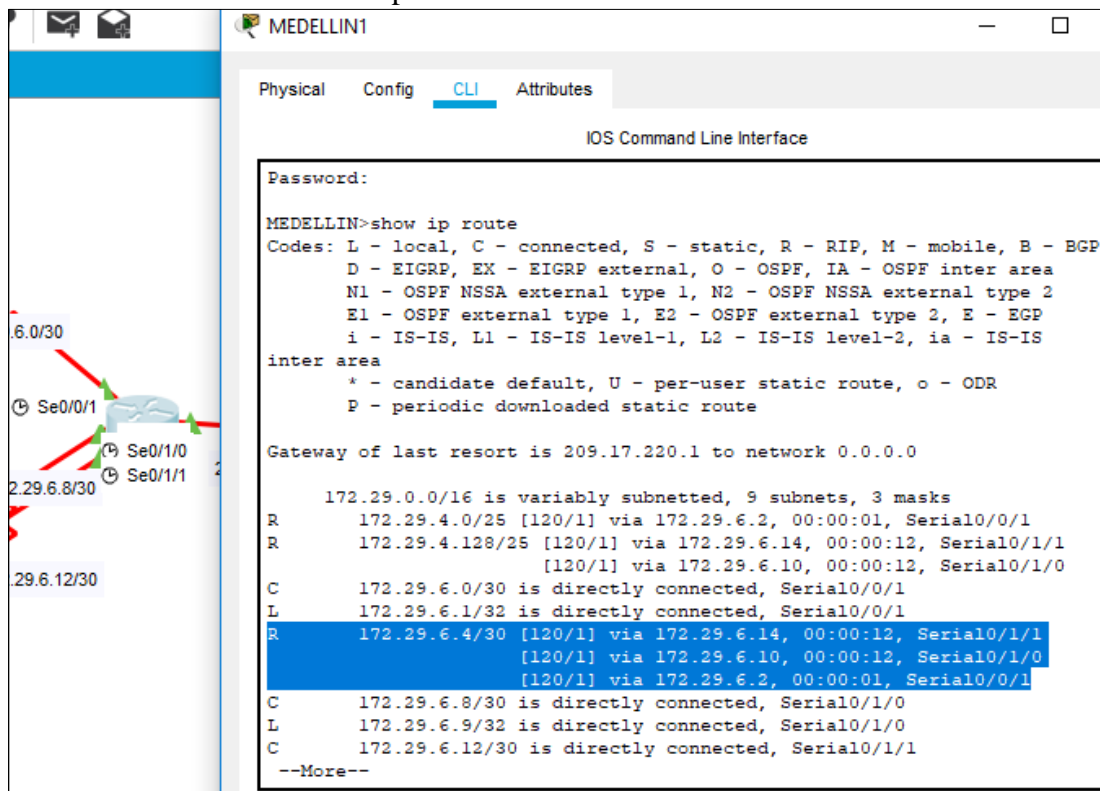
La Deshabilitación de la propagación del protocolo RIP ya se realizó en el punto anterior gracias al comando `Passive-interface` aplicado en la interfaz que señala este enunciado.

#### 4. Verificación del protocolo RIP.

- a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos.
- b. Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Se verifican gracias al comando **show ip route** en este caso se realiza la práctica en el Router de MEDELLIN1:

Ilustración 6  
Comando Show ip route - Práctica en el Router de Medellín



```
MEDELLIN1
Physical Config CLI Attributes
IOS Command Line Interface
Password:
MEDELLIN>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 209.17.220.1 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R   172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:01, Serial0/0/1
R   172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:12, Serial0/1/1
   [120/1] via 172.29.6.10, 00:00:12, Serial0/1/0
C   172.29.6.0/30 is directly connected, Serial0/0/1
L   172.29.6.1/32 is directly connected, Serial0/0/1
R   172.29.6.4/30 [120/1] via 172.29.6.14, 00:00:12, Serial0/1/1
   [120/1] via 172.29.6.10, 00:00:12, Serial0/1/0
   [120/1] via 172.29.6.2, 00:00:01, Serial0/0/1
C   172.29.6.8/30 is directly connected, Serial0/1/0
L   172.29.6.9/32 is directly connected, Serial0/1/0
C   172.29.6.12/30 is directly connected, Serial0/1/1
--More--
```

Por medio del comando **Show ip protocol** para verificar la configuración en RIP, el cual observamos que nos muestra la información de ruteo, las interfaces pasivas y más.

## Ilustración 7 Comando Show ip Protocol

```
MEDELLIN1
Physical Config CLI Attributes
IOS Command Line Interface

MEDELLIN>
MEDELLIN>
MEDELLIN>show ip protocol
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 20 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
  Serial0/0/1          2    2
  Serial0/1/0          2    2
  Serial0/1/1          2    2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.29.0.0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway            Distance    Last Update
  172.29.6.2           120        00:00:17
  172.29.6.14          120        00:00:29
  172.29.6.10          120        00:00:29
  Distance: (default is 120)
```

### 5. Configurar encapsulamiento y autenticación PPP.

- a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

Se realizó la siguiente configuración entre el ISP y MEDELLIN1:

#### Autenticación PPP PAP EN ISP

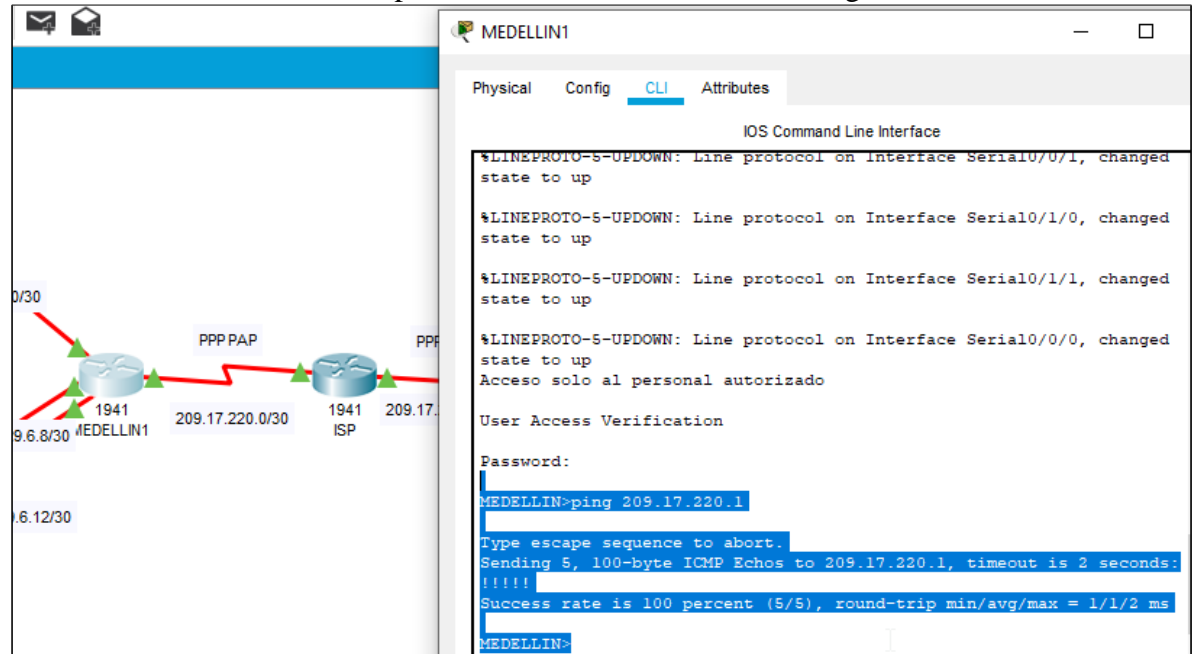
```
# Username MEDELLIN password cisco
# Interface s0/0/0
# Encapsulation ppp
# Ppp authentication pap
# Ppp pap sent-username ISP password cisco
```

## Autenticación PPP PAP EN MEDELLIN1

```
# Username ISP password cisco
# Interface s0/0/0
# Encapsulation ppp
# Ppp authentication pap
# Ppp pap sent-username MEDELLIN password cisco
```

Ilustración 8

Verificación de autenticación por PAP EN MEDELLIN1 Por Ping hacia ISP



b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Se realizó la siguiente configuración entre el ISP y BOGOTA1:

## Configuración de autenticación CHAP

### Autenticación PPP CHAP EN ISP

```
# Username BOGOTA password cisco
# Interface s0/0/1
# Encapsulation ppp
# Ppp authentication chap
```

## Autenticación PPP CHAP EN BOGOTA1

```
# Username ISP password cisco
# Interface s0/0/0
# Encapsulation ppp
# Ppp authentication chap
```

Ilustración 9

Verificación de autenticación por CHAP EN BOGOTA1 Por Ping hacia ISP

The image shows a network topology on the left and a CLI terminal window on the right. The topology features two routers: '1941 ISP' and '1941 BOGOTA1'. They are connected via a link labeled 'PPP CHAP' with the IP address '209.17.220.4/30'. The terminal window, titled 'BOGOTA1', shows the following output:

```
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
Acceso solo al personal autorizado

User Access Verification

Password:
BOGOTA>ping 209.17.220.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/20 ms
BOGOTA>
```

## 6. Configuración de PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

- c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Se realiza la siguiente configuración: Se activa el NAT en Bogota 1 y Medellin1 logrando indicar cuales son las interfaces de salida y entrada, además de la configuración listas por overload:

### **Configuración de NAT en los siguientes router:**

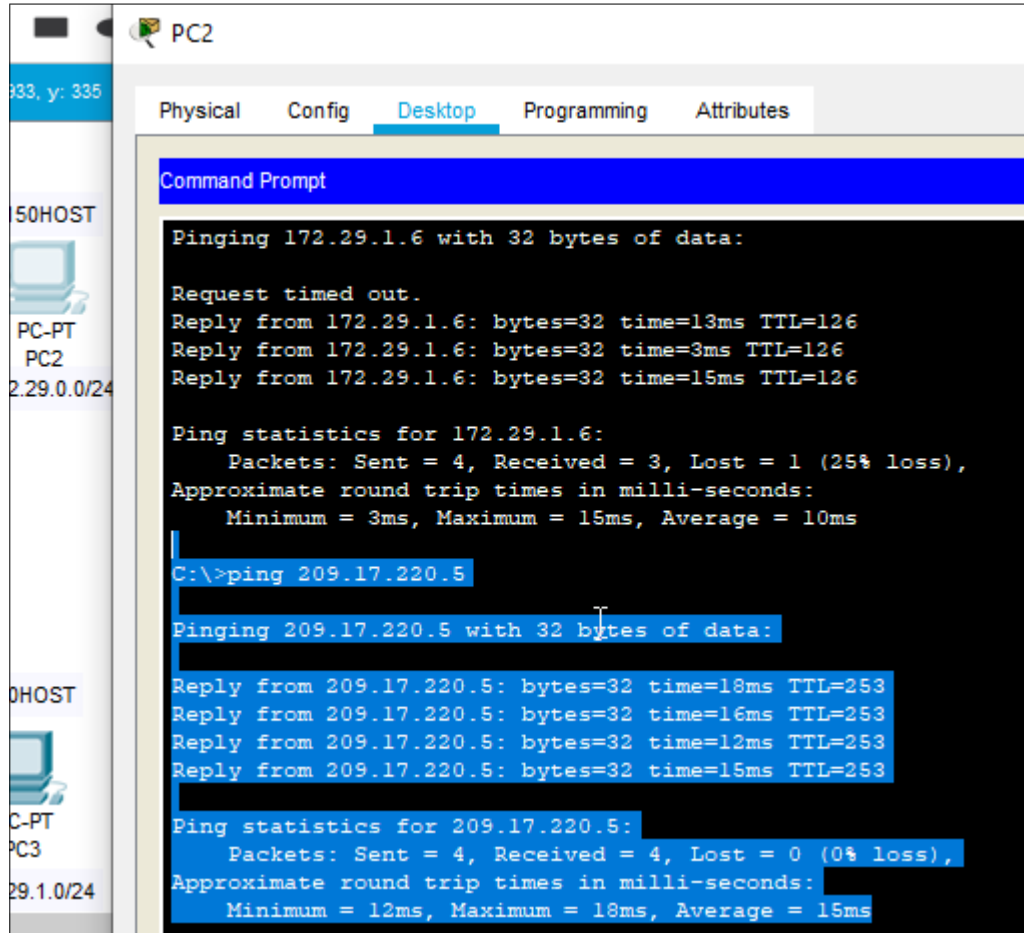
#### **NAT en MEDELLIN1**

```
# Configure terminal
# Ip nat inside source list 1 interface s0/0/0 overload
# Access-list 1 permit 172.29.4.0 0.0.3.255
# Int s0/0/0
# Ip nat outside
# Int s0/0/1
# Ip nat inside
# Int s0/1/0
# Ip nat inside
# Int s0/1/1
# Ip nat inside
```

#### **NAT en BOGOTA1**

```
# Configure terminal
# Ip nat inside source list 1 interface s0/0/0 overload
# Access-list 1 permit 172.29.0.0 0.0.3.255
# Int s0/0/0
# Ip nat outside
# Int s0/0/1
# Ip nat inside
# Int s0/1/0
# Ip nat inside
# Int s0/1/1
# Ip nat inside
```

Ilustración 10  
Ping PC2 a ISP



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 172.29.1.6 with 32 bytes of data:
Request timed out.
Reply from 172.29.1.6: bytes=32 time=13ms TTL=126
Reply from 172.29.1.6: bytes=32 time=3ms TTL=126
Reply from 172.29.1.6: bytes=32 time=15ms TTL=126

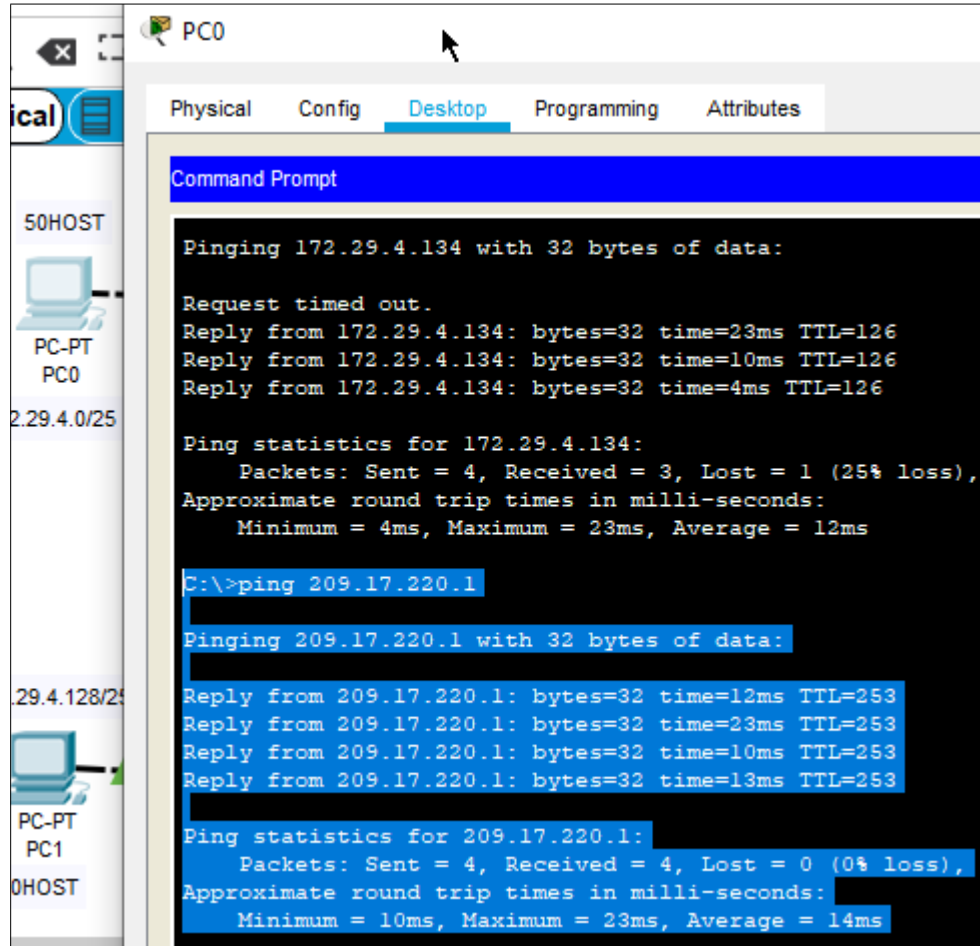
Ping statistics for 172.29.1.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 15ms, Average = 10ms

C:\>ping 209.17.220.5
Pinging 209.17.220.5 with 32 bytes of data:
Reply from 209.17.220.5: bytes=32 time=18ms TTL=253
Reply from 209.17.220.5: bytes=32 time=16ms TTL=253
Reply from 209.17.220.5: bytes=32 time=12ms TTL=253
Reply from 209.17.220.5: bytes=32 time=15ms TTL=253

Ping statistics for 209.17.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 18ms, Average = 15ms
```

Ping satisfactorio

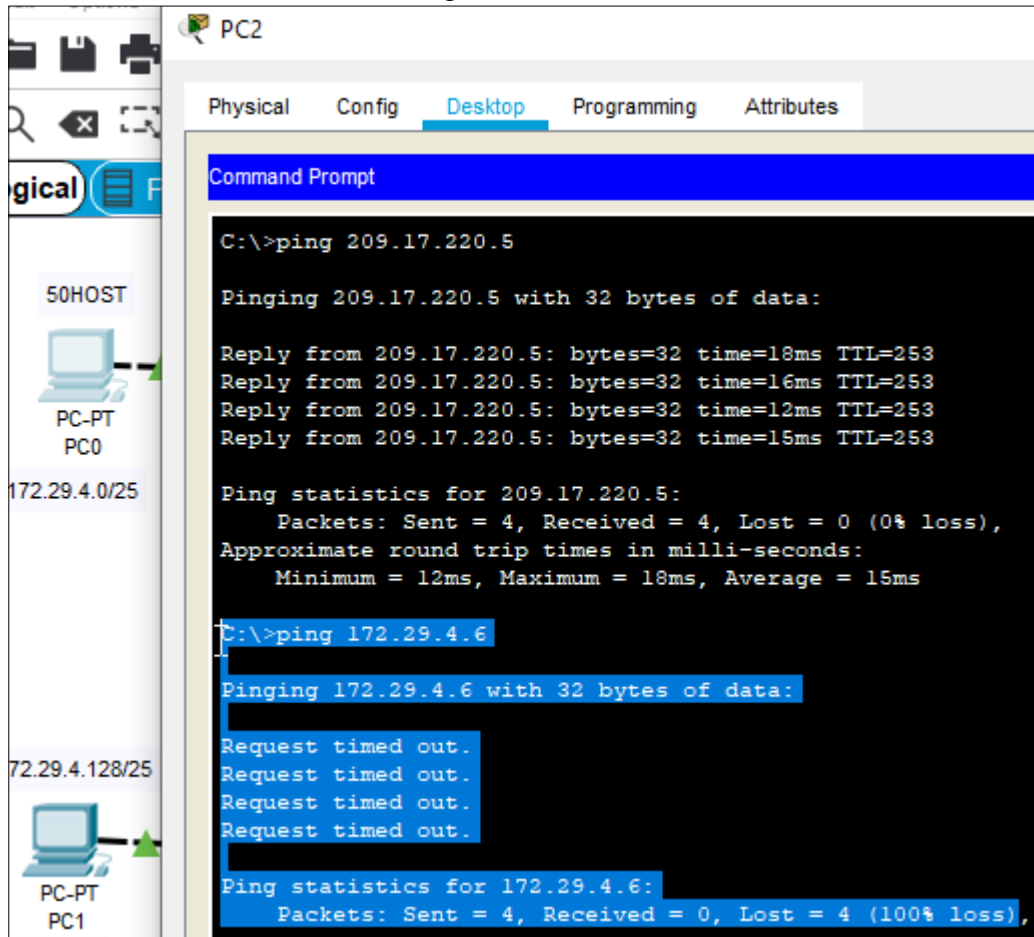
Ilustración 11  
Ping PC0 a ISP



Ping satisfactorio



Ilustración 12  
Ping de PC2 a PC0



Ping fallido, porque NAT lo bloquea.

## 7. Configuración del servicio DHCP.

- Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
- El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
- Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
- Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Se realiza la configuración DHCP en los router Medellin2, 3 y Bogota2, 3.

### **Iniciamos la configuración DHCP EN MEDELLIN 2:**

```
# Ip dhcp excluded-address 172.29.4.1 172.29.4.5
# Ip dhcp excluded-address 172.29.4.129 172.29.4.133
# Ip dhcp pool MED2
# Network 172.29.4.0 255.255.255.128
#Default-router 172.29.4.1
#Dns-server 8.8.8.8
# Ip dhcp pool MED3
# Network 172.29.4.128 255.255.255.128
#Default-router 172.29.4.129
# Dns-server 8.8.8.8
```

### **Configuración DHCP EN MEDELLIN3**

```
# Configure terminal
# Interface g0/0
# Ip helper-address 172.29.6.5
```

### **Configuración DHCP EN BOGOTA2**

```
# Ip dhcp excluded-address 172.29.1.1 172.29.1.5
# Ip dhcp excluded-address 172.29.0.1 172.29.0.5
# Ip dhcp pool BOG2
# Network 172.29.1.0 255.255.255.0
# Default-router 172.29.1.1
# Dns-server 8.8.8.8
# Ip dhcp pool BOG3
# Network 172.29.0.0 255.255.255.0
# Default-router 172.29.0.1
# Default-router 172.29.0.1
```

### **Configuración DHCP EN BOGOTA3**

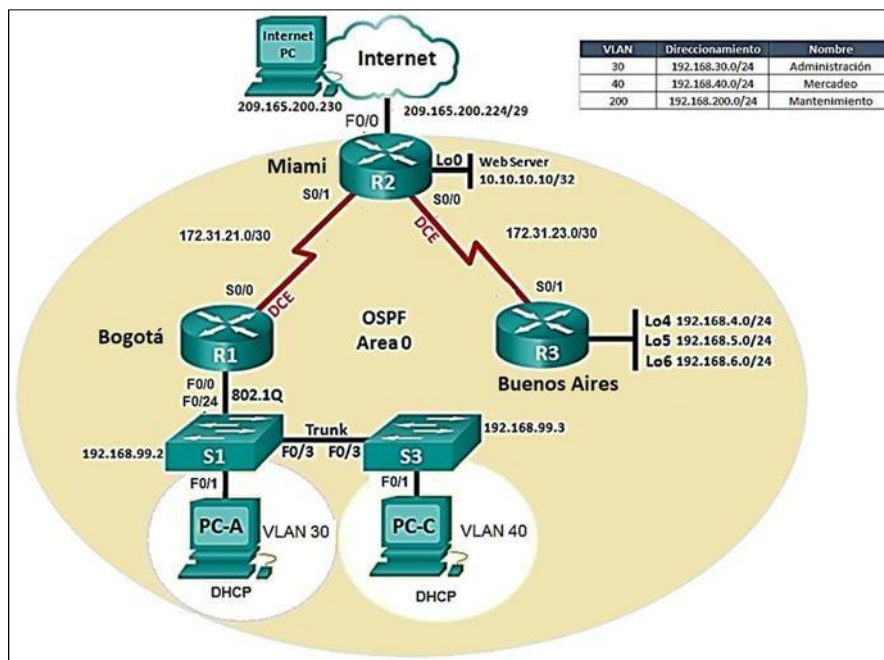
```
# Configure terminal
# Interface g0/0
# Ip helper-address 172.29.3.13
```



## ESCENARIO 2

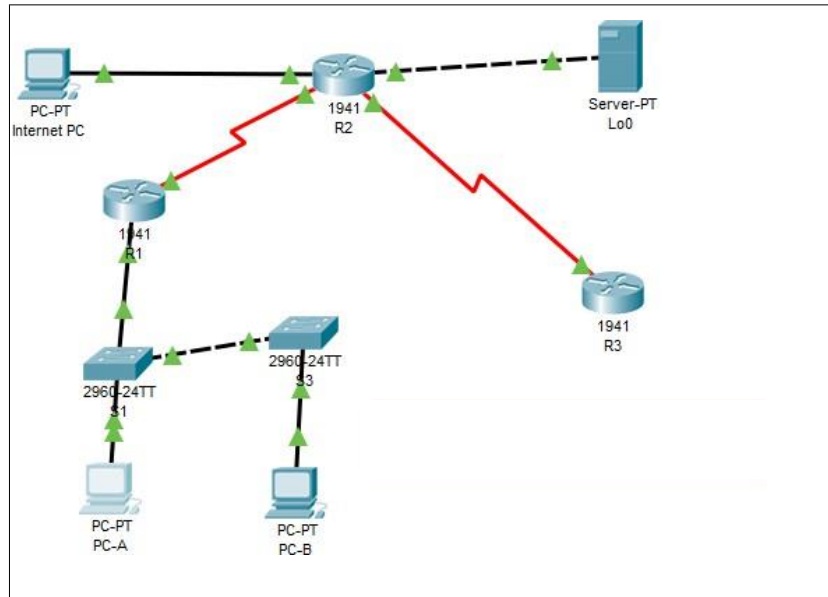
Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Ilustración 14  
Administración de red escenario 2-A



Se realiza la configuración de Red de la siguiente forma en el Packet Tracer donde se utilizaron los dispositivos adecuados para realizar los puntos de acuerdo al enunciado dado:

Ilustración 15  
Administración de red escenario 2-B



1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

### Configuración en Router R1

```
#hostname R1
#interface serial 0/0/0
#ip Address 172.31.21.1 255.255.255.252
#clock rate 12800
#no shutdown
```

### Configuración en R2

```
#hostname R2
#interface serial 0/0/1
#ip address 172.31.21.2 255.255.255.252
#no shutdown
#interface serial 0/0/0
#ip adr
#ip adres #ip ad
#ip address 172.31.23.1 255.255.255.252
#clock rate 12800 Unknown clock rate #no shutdown
```

```
#interface serial 0/0/1
#ip ad
#ip address 172.31.21.2 255.255.255.252
#no shutdown #interfa
#interface serial 0/0/0
#ip address 172.31.23.1 255.255.255.252
#clock rate 12800 Unknown clock rate #no shutdown
#interface gigabitEthernet 0/0
#ip address 209.165.200.225 255.255.255.248
#no shutdown
#interface gigabit Ethernet 0/0
#ip address 209.165.200.225 255.255.255.248
#no shutdown
#interface GigabitEthernet 0/1
#ip address 10.10.10.1 255.255.255.0
```

### **Configuración en R3**

```
#hostname R3 #interface serial 0/0/0
#ip address 172.31.23.2 255.255.255.252
#clock rate 12800 Unknown clock rate #no shut
#no shutdown #interface loopback 4
#ip address 192.168.4.1 255.255.255.0
#no shutdown
# interface loopback 5
#ip address 192.168.5.1 255.255.255.0
#no shutdown
# interface loopback 6
#ip address 192.168.6.1 255.255.255.0
#no shutdown
Web Ip estatica 10.10.10.10 255.255.255.0
Getway 10.10.10.1
```

Ilustración 16  
R3

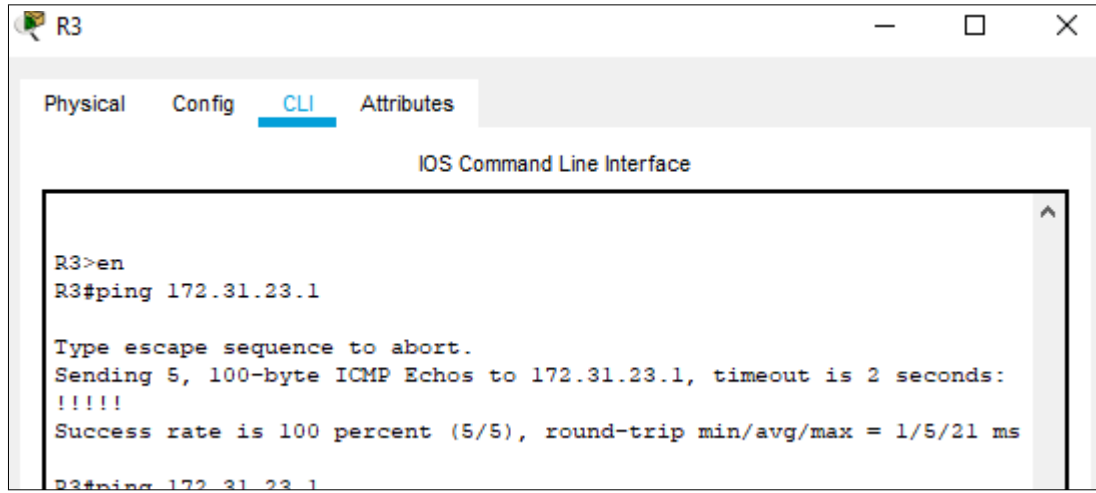
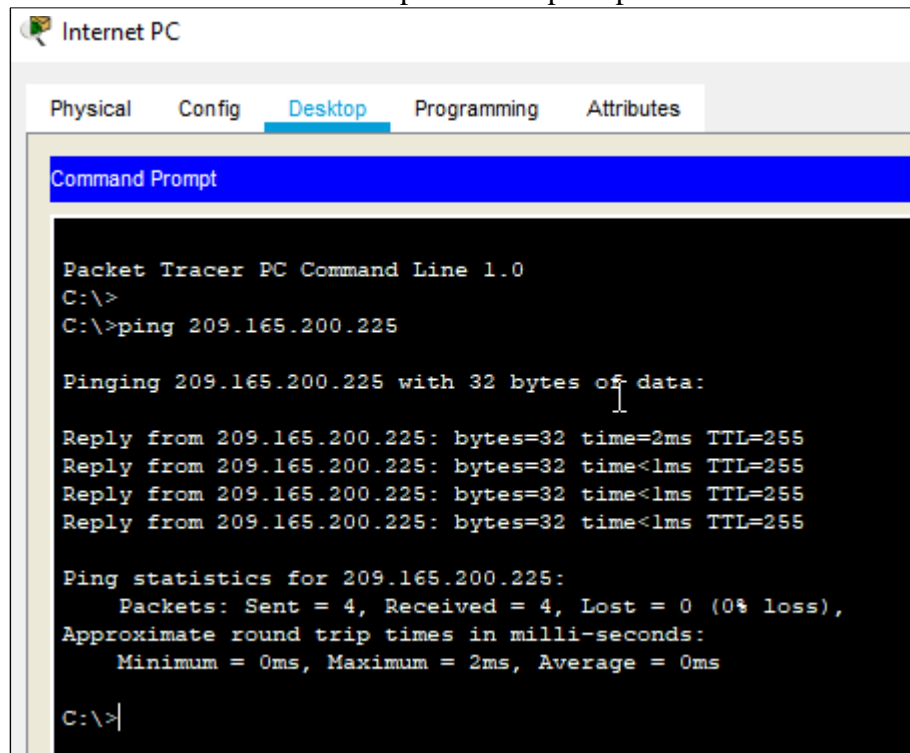


Ilustración 17  
Internet pc comand prompt



2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

Tabla 2  
OSPFv2 área 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

### Configuración en R1

```
#router ospf 1
#router-id 1.1.1.1
#network 172.31.21.0 0.0.0.3 area 0
#network 192.168.30.0 0.0.0.255 area 0
#network 192.168.40.0 0.0.0.255 area 0
#network 192.168.200.0 0.0.0.255 area 0
#passive-interface g0/1.30
#passive-interface g0/1.40
#passive-interface g0/1.200
#int s0/0/0
#band #bandwidth 256
#ip ospf cost 9500
```



## Ilustración 18 Configuración en R1



The screenshot shows the CLI interface of a Cisco router named R1. The 'CLI' tab is selected. The output of the command 'show ip ospf neighbor' is displayed, showing a single neighbor with ID 5.5.5.5 on interface Serial10/0/0. The state is FULL/-. The dead time is 00:00:34. The address is 172.31.23.0.

```
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
R1#show ip ospf neighbor  
  
Neighbor ID      Pri   State           Dead Time   Add  
Interface  
5.5.5.5          0    FULL/ -         00:00:34   172  
Serial10/0/0
```

## Configuración en R2

```
#router ospf 1  
#router ospf 1  
#router-id 5.5.5.5  
#network 172.31.21.0 0.0.0.3 area 0  
#network 172.31.23.0 0.0.0.3 area 0  
#network 10.10.10.0 0.0.0.255 area 0  
#pas  
#passive-interface g0/1  
#int s0/0/0  
#bandwidth 256  
#int s0/0/1  
#bandwidth 256  
#int s0/0/0  
#ip ospf cost 9500
```

Ilustración 19  
Configuración en R2-A

The screenshot shows the CLI of router R2. The 'CLI' tab is selected. The command 'show ip ospf' has been executed, displaying the following output:

```

R2>en
R2#show ip ospf
Routing Process "ospf 1" with ID 5.5.5.5
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 sec
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 2
    Area has no authentication
    SPF algorithm executed 3 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0x01b16b
    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
  
```

Ilustración 20  
Configuración en R2-B

The screenshot shows the CLI of router R2. The 'CLI' tab is selected. The command 'show ip ospf neighbor' has been executed, displaying the following output:

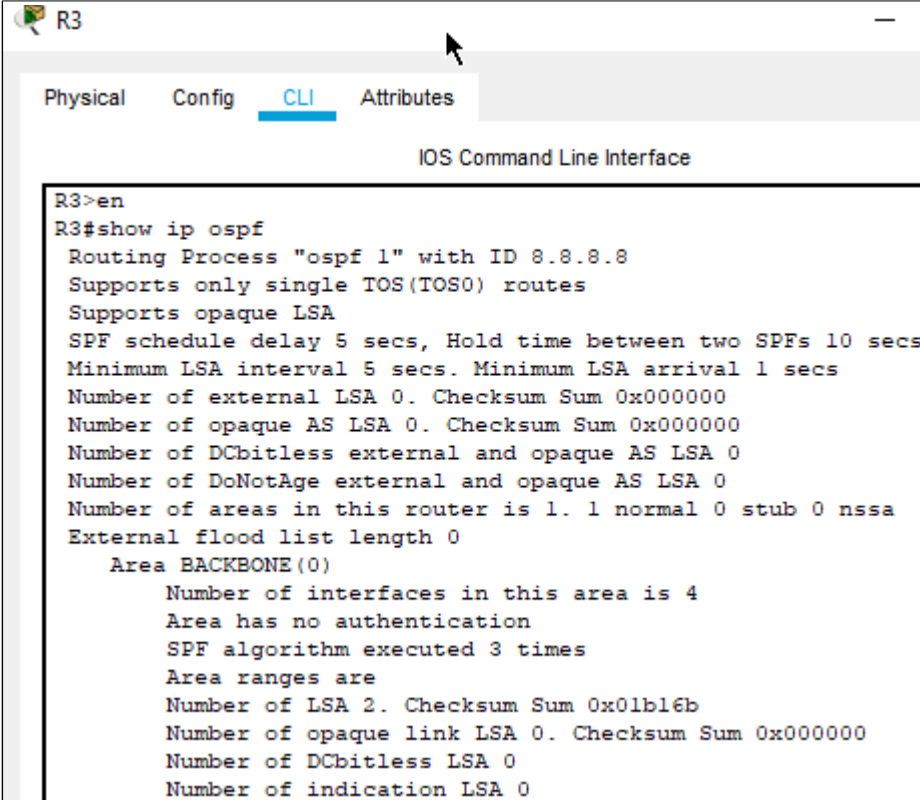
```

R2#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address
Interface
8.8.8.8          0    FULL/ -         00:00:30   172.31.23.2
Serial0/0/0
  
```

## Configuración en R3

```
#router ospf 1
#router-id 8.8.8.8
#network 172.31.23.0 0.0.0.3 area 0
#network 192.168.4.0 0.0.3.255 area 0
#passive-interface lo4
#passive-interface lo5 #passive-interface lo6
#exit
#int s0/0/1
#bandwidth 256
```

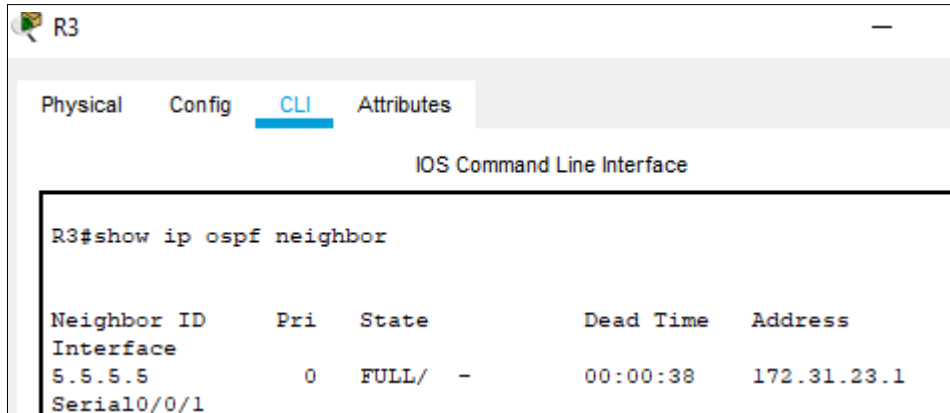
Ilustración 21  
Configuración en R3-A



The screenshot shows a terminal window titled 'R3' with a tabbed interface. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show ip ospf' in enable mode. The output shows the configuration of the OSPF process 'ospf 1' with ID 8.8.8.8, including details about supported LSAs, SPF schedule, and the configuration of Area BACKBONE(0) with 4 interfaces.

```
R3>en
R3#show ip ospf
Routing Process "ospf 1" with ID 8.8.8.8
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 4
    Area has no authentication
    SPF algorithm executed 3 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0x01b16b
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
```

Ilustración 22  
Configuración en R3-B



The screenshot shows the CLI interface of a Cisco router named R3. The 'CLI' tab is selected. The command 'show ip ospf neighbor' has been executed, resulting in the following output:

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
5.5.5.5	0	FULL/ -	00:00:38	172.31.23.1
Serial0/0/1				

3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

### **Configuración en R1**

```
#int g0/1.30
#description accoun
#description administracion lan
#encapsulation dot1q 30
#ip ad
#ip address 192.168.30.1 255.255.255.0
#int g0/1.40
#description mercadeo lan
#encapsulation dot1q 40
#ip address 192.168.40.1 255.255.255.0
#int g0/1.200
#description mantenimiento lan
#encapsulation dot1q 200
#ip address 192.168.200.1 255.255.255.0
#interface g0/1
#no shut
#no shutdown
```

### **Configuración en S1**

```
#host s1 vlan 20
#name administracion
#vlan 40
#name mercadeo
#vlan 200
#name mantenimiento
#exit
#interface vlan 99
#ip address 192.168.99.2 255.255.255.0
#no shutdown
#exit
#ip default-gateway 192.168.99.1
#interface f
#interface fastethernet 0/3
#switchport mode trunk
#sw
#switchport t
```

```

#switchport trunk n
#switchport trunk native vlan 1
#int ran
#INT RAN ?
#interface range fa0/1.2, fa0/4-24, g
#interface range fa0/1.2, fa0/4-24, gigabitethernet 0/1-2
#interface range not validated - command rejected
#interface range fa0/1-2, fa0/4-24, gigabitethernet 0/1-2
#switchport mode access
#exit
#interface fa0/1
#switchport mode access
#switchport access vlan 30
#interface range fa0/1-2, fa0/4-24, gigabitethernet 0/1-2
#switchport mode access
#no shut
#no shutdown
#exit
#end
#interface f
#interface fastEthernet 0/3
#switchport mode t
#switchport mode trunk

```

### **Configuración en S3**

```

#hostname S3
#vlan 30
#name Administracion
#vlan 40
#name Mercadeo
#vlan 200
#name Mantenimiento
#in
#interface vlan 99
#ip address 192.168.99.3 255.255.255.0
#no shut
#no shu
#no shutdown #exit
#ip def
#ip default-gateway 192.168.99.1
#interface fa0/3
#sw #switchport m
#switchport mode t

```

```

#switchport mode trunk
#sw
#switchport tr
#switchport trunk n
#switchport trunk native vlan 1
#interface fa0/3
#int
#r
#ran
#interface r
#interface range fa0/1-2, fa0/4-24, g
#interface range fa0/1-2, fa0/4-24, gigabitEthernet 0/1-2
#switch
#switchport mo
#switchport mode ac
#switchport mode access
#exit
#int
#interface f
#interface fastEthernet 0/1
#sw
#switchport m
#switchport mode a
#switchport mode access
#sw
#switchport ac
#switchport access vlan 40
#no shu
#no shutdown
#exit

```

#### 4. En el Switch 3 deshabilitar DNS lookup

En el Switch R3 usamos el siguiente comando para deshabilitar el DNS lookup

```

#en
#conf t
#no ip domain-lookup
#Exit

```

5. Asignar direcciones IP a los Switches acorde a los lineamientos.

Se asignaron las ip de todos los Switch acorde al enunciado utilizando el comando "ip address" el cual ya está ejecutado en los puntos anteriores.

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Las interfaces innecesarias en los router también se desactivaron en los puntos anteriores utilizando el comando "Passive-interface"

### Configuración en S1

```
#int range fa0/1-2, fa0/4, fa0/7-23, g0/1-2
#shutdown
```

7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

### Configuración en R1

```
#ip dhcp excluded-address 192.168.30.1 192.168.30.30
#ip dhcp excluded-address 192.168.40.1 192.168.40.30
```

Tabla 3  
Configuración en R1-A

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
-----------------------------------	--

### Configuración en R1

```
#ip dhcp pool ADMINISTRACION
#dns-server 10.10.10.11
#default-router 192.168.30.1
#network 192.168.30.0 255.255.255.0
```



Tabla 4  
Configuración en R1-B

Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
-----------------------------------	--

### Configuración en R1

```
#ip dhcp pool MERCADEO
#dns-server 10.10.10.11
#default-router 192.168.40.1
#network 192.168.40.0 255.255.255.0
```

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet

### Configuración en R2

```
#user webuser privilege 15 secret cisco12345
#ip nat inside source static 10.10.10.10 209.168.200.229
#user webuser privilege 15 secret cisco12345
#ip nat inside source static 10.10.10.10 209.168.200.229
#interface gigabitEthernet 0/0
#ip nat outside
#int g0/1
#ip nat inside
#exit
```

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

### Configuración en R1

```
#access-list 1 permit 192.168.30.0 0.0.0.255
#access-list 1 permit 192.168.40.0 0.0.0.255
#access-list 1 permit 192.168.4.0 0.0.0.255
#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
```

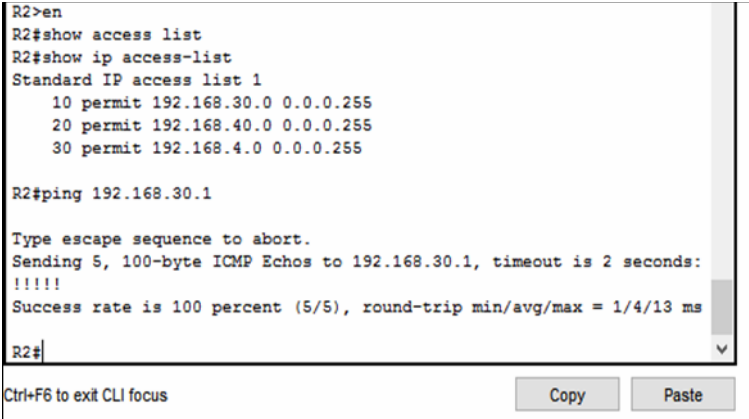
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
#ip nat inside source list 1 pool INTERNET
```

13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Ping R2 a R1

Ilustración 23  
Ping R2 a R1



```
R2>en
R2#show access list
R2#show ip access-list
Standard IP access list 1
 10 permit 192.168.30.0 0.0.0.255
 20 permit 192.168.40.0 0.0.0.255
 30 permit 192.168.4.0 0.0.0.255

R2#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms

R2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Traceroute R2 a R1

Ilustración 24  
Traceroute R2 a R1

```
R2#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms

R2#traceroute 192.168.30.1
Type escape sequence to abort.
Tracing the route to 192.168.30.1
 0  172.31.21.1    10 msec  0 msec   0 msec
R2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

## CONCLUSIONES

En la realización y respectiva solución de la actividad propuesta, se ejecutaron a cabalidad los 2 escenarios propuestos como prueba hacia todos los temas abarcados durante el presente diplomado de profundización CCNA CISCO, y a la vez, se escatimaron refuerzos sobre lo aprendido dentro de las diversas fases correspondientes, tales como configuración de RIPv2, NAT, configuraciones básicas en dispositivos dentro de una topología LAN, configuración de VLANs, entorno DHCP, direccionamiento dinámico y estático, pruebas de conectividad, entre otros.

Se procedió a sustentar todos y cada uno de los pasos y procesos requeridos para la realización de la actividad, tales como validación de comandos y capturas de pantalla.

La prueba de habilidades prácticas desarrollada se presenta como una gran oportunidad para definir futuros procesos de apropiación y configuración de dispositivos dentro de una topología LAN, en un ambiente real hacia optimizaciones de tipo profesional.

## BIBLIOGRAFIA

- COLOMES, PAOLO. 2010.** <http://www.redescisco.net>. [En línea] 18 de Agosto de 2010. <http://www.redescisco.net/sitio/2010/08/18/implementando-nat-en-routers-cisco/>.
- . **2013.** <https://es.slideshare.net>. [En línea] 30 de Agosto de 2013. <https://es.slideshare.net/pcolomes/implementacin-de-natpat-en-routers-cisco>.
- CRIS. 2019.** <https://support.cloudflare.com>. [En línea] 12 de JUNIO de 2019. <https://support.cloudflare.com/hc/es-es/articles/200169336--C%C3%B3mo-puedo-ejecutar-un-traceroute->.
- DI TOMMASO, LEANDRO. 2010.** <https://www.mikroways.net>. [En línea] 6 de JUNIO de 2010. <https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/>.
- DUARTE, EUGENIO. 2014.** <http://blog.capacityacademy.com>. [En línea] 18 de JUNIO de 2014. <http://blog.capacityacademy.com/2014/06/18/cisco-ccna-como-configurar-nat-overload-en-cisco-router/>.
- 2011.** <https://todopacketracer.com>. *Configuración de VLANs*. [En línea] 18 de 10 de 2011. <https://todopacketracer.com/2011/10/18/configuracion-de-vlans/>.
- Microsoft Windows Server. 2018.** <https://support.microsoft.com>. [En línea] 30 de NOVIEMBRE de 2018. <https://support.microsoft.com/es-co/help/314868/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows>.
- OSPF DESIGN GUIDE. 2005.** <https://www.cisco.com>. [En línea] 10 de Agosto de 2005. <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>.
- UNAD. 2014.** <https://cisco.com>. *Principios de Enrutamiento [OVA]*. [En línea] 2014. [https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm).
- . **2014.** <https://cisco.com>. *Configuración de Switches y Router [OVA]*. [En línea] 5 de Junio de 2014. <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>.
- . **2014.** <https://www.cisco.com>. *PING y TRACER como estrategia en procesos de Networking [OVA]*. [En línea] 2014. <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>.
- WALTON, ALEX. 2019.** <https://ccnadesdecero.es>. [En línea] 2019. <https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/>.
- . **2019.** <https://ccnadesdecero.es>. [En línea] 2019. <https://ccnadesdecero.es/configuracion-nat-estatica/>.