# PRUEBA DE HABILIDADES PRACTICAS CCNA

RODRIGO DIAZ CHANTRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE SISTEMAS
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CALI – VALLE
2020

# PRUEBA DE HABILIDADES PRACTICAS CCNA

Diplomado de profundización Cisco (Informe final para optar por el titulo de Ingeniero de Sistemas)

TUTOR
HECTOR JULIÁN PARRA
MSC. DIRECCIÓN ESTRATÉGICA ESPECIALIDAD TELECOMUNICACIONES.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE SISTEMAS
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CALI – VALLE
2020

**Nota de Aceptación**

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cali – mayo 14 de 2020 – Fecha de Entrega Pendiente

Dedico este trabajo a cada todos los estudiantes de esta carrera tan fascinante, también a cada todos los instructores que siempre estuvieron prestos a dar su apoyo.

## AGRADECIMIENTOS

Primeramente, quiero dar gracias a Dios por permitirme llegar hasta esta instancia, también debo agradecer el apoyo incondicional de mis padres que han sido pieza clave en este proceso, también a mi hija y hermana que han sido una gran motivación para avanzar hasta donde me encuentro actualmente.

Por otra parte, quiero agradecer a la red de tutores de la universidad UNAD, quienes también han hecho posible mis avances con su dedicación y retroalimentación durante la carrera.

## TABLA DE CONTENIDO

## INDICE DE TABLAS

## TABLA DE ILUSTRACIONES

# GLOSARIO

**Router:** Dispositivo fisico (Hardware) que se encarga de enrutar el destino de cada paquete de datos dentro de una red informatica.

**Firewall:** Puede ser software y hardware que en escencia, bloquean los accesos no autorizados o permiten cierto trafico de red de acuerdo a la configuracion dada.

**Red WAN:** Es una topologia de red que permite unir dos o mas redes locales, aunque se encuentren en ubicaciones geograficas diferentes.

**DHCP:** Es un protocolo que asigna automaticamente direcciones IP a uno o varios hosts dentro de una red local.

**Ping:** es una utilidad que ayuda a diagnosticar si hay conexion entre el host origen y el host destino mediante un comando en el terminal o consola de comandos.

## RESUMEN

El desarrollo de la actividada a continuación tiene la finalidad de capacitar al profesional en la resolución de conflictos de conectividad o la generación de esquemas que permitan la misma, La universidad Nacional Abierta y a Distancia UNAD a través de su diplomado de profundización de redes de cisco y apoyándose en la academia virtual de cisco, pretenden ampliar estos conocimientos mediante el planteamiento de dos escenarios.

El primero tiene el objetivo de hacer entender como debe configurarse un dispositivo de red, aplicando controles de seguridad en los equipos de red y parametrizando los diferentes segmentos de red tanto de IPv4 como de IPv6, realizando configuraciones muy usadas en la actualidad como son el DHCP y la sincronización de relojes NTP para los equipos cliente.

En el segundo escenario se plantea la conectividad en una red de área abierta WAN donde se tienen dos sedes en diferentes ciudades y de acuerdo a la configuración aplicada, estas podrán conectarse o restringirse según sea el caso.



**PALABRAS CLAVE:** Configuración Redes WAN, Router DHCP, Topologias de red, Equipos Cisco.

# 1. INTRODUCCIÓN

En el presente documento se estará desarrollando un paso a paso de soluciones de conectividad de diferentes escenarios donde se requiere aplicar diferentes direccionamientos de red basado en topologías que cumplan con estándares reales de producción, generando habilidades practicas para el profesional.

## 1.1 ESCENARIO 1

Se requiere una configuración de la topología propuesta, esta debe poder establecer configuración entre dispositivios que usen los protocolos IPv4 e IPv6, por lo que los dispositivos deben soportar ambos protocolos, además de tener un direccionamiento adecuado y aplicar los controles de seguridad necesarios para reducir posibles suplantaciones o accesos no autorizados.

## 1.2 ESCENARIO 2

Es necesario establecer una red WAN en el esquema de una organización que cuenta con dos sedes ubicadas en distintas partes geográficamente, por lo que se deben tener en cuenta, aspectos de seguridad debido a que la conexión esta expuesta a internet y esto implica riesgos de seguridad, se necesita tener en cuenta la segmentación de red LAN y la configuración de las redes aceptadas para permitir el trafico de las mismas.

# 2. OBJETIVOS

## 2.1 OBJETIVO GENERAL

Adquirir conocimientos y destrezas dando solución a los diferentes esquemas o problemas de conectividad de red que se presentan a menudo en muchas organizaciones.

## 2.2 OBJETIVOS ESPECÍFICOS

- Configurar correctamente un esquema de red teniendo una topología base para establecer la conexión entre los hosts.
- Ampliar los conocimientos sobre el protocolo IPv6 que en poco tiempo será el protocolo a usar en las redes a nivel mundial dado el agotamiento de direcciones IPv4.
- Aplicar protocolos y controles de acceso en los dispositivos evitando el acceso no autorizado.
- Entender claramente la forma en que opera una red WAN y como plantear una topología de red para dos sedes en diferentes ubicaciones geográficas.

# 3. PLANTEAMIENTO DEL PROBLEMA

## 3.1 DEFINICIÓN DEL PROBLEMA

Configurar una red que requiere contar con varios protocolos como DHCP, NAT, NTP, además de la creación de VLANs para segmentar el trafico, se cuenta con la topología definida pero no se tiene aun la configuración realizada.

Interconectar dos sedes de una organización de acuerdo a la infraestructura ya establecida y teniendo en cuenta los parámetros y controles de seguridad.

## 3.2 JUSTIFICACIÓN

El desarrollo de este planteamiento consolidará los conocimientos adquiridos a lo largo de todas las unidades estudiadas, las habilidades recolectadas en este campo de la ingeniería son necesarias para todo profesional en ingeniería de sistemas porque el ingeniero debe tener la capacidad de dar soluciones de conectividad en las organizaciones, además de poder presentar de manera sencilla y entendible un documento gerencial con un proyecto de implementación de redes con todos sus controles.

## 4. ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

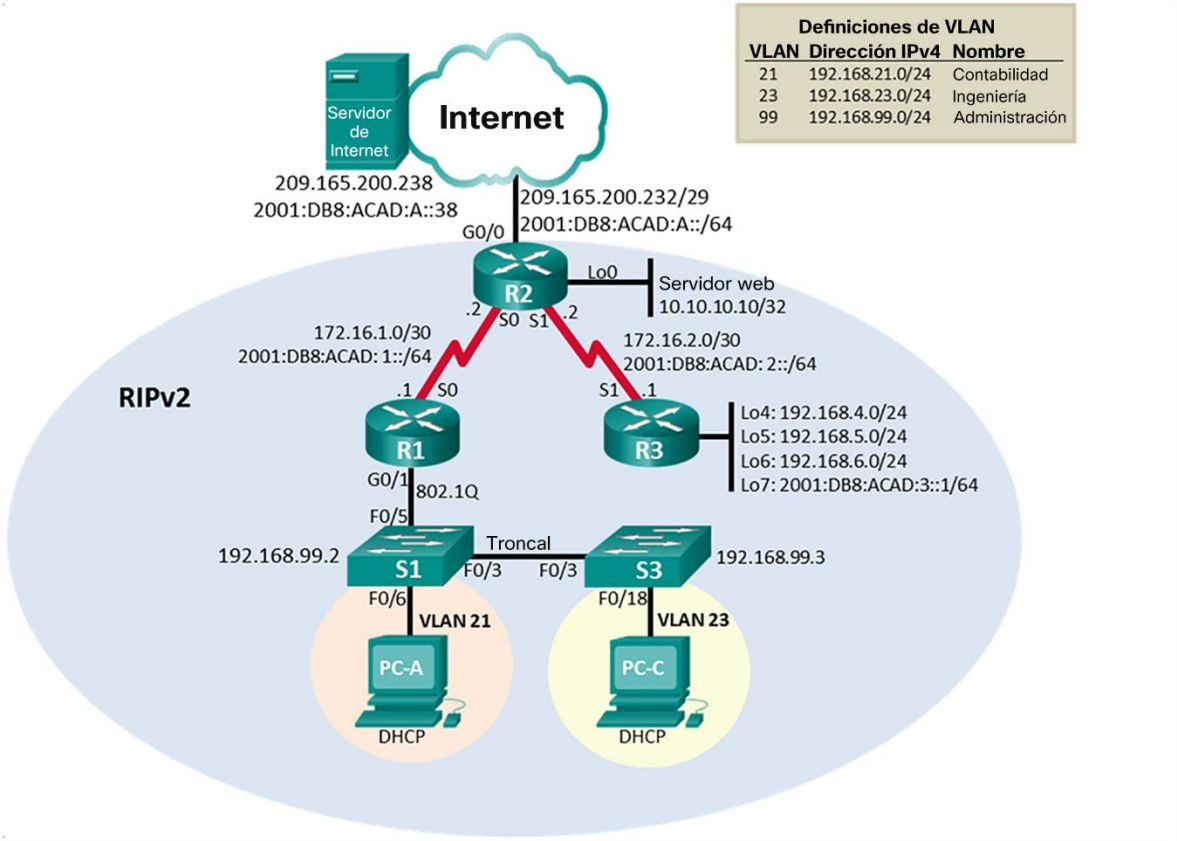


*Ilustración 1 Topologia Propuesta*

### Parte 1: Inicializar dispositivos

### Paso 1: Inicializar y volver a cargar los routers y los switches.

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

**Eliminar el archivo startup-config de todos los routers**

```
Router>ena
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
```

**Volver a cargar todos los routers**

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

Readonly ROMMON initialized

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

IOS Image Load Test
_____________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################
######## [OK]
```

**Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior**

```
Switch>ena
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

**Volver a cargar ambos switches**

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: 0009.7C9E.AD3D
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
############################################################################
######## [OK]

**Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches**

Switch>ena
Switch#show flash
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)

**Parte 2: Configurar los parámetros básicos de los dispositivos**

**Paso 1: Configurar la computadora de internet**

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

*Tabla 1 Parámetros Básicos*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:A::1 |

**Nota:** De acuerdo al cálculo realizado según la máscara de red, el Gateway 209.165.200.225 (Que se da en la tabla del documento) es incorrecto dado que para la red propuesta 209.165.200.232/29 solo admite 6 host y el primer host normalmente se usa como Gateway 209.165.200.233. El Gateway en IPv6 también tenía error debido a que el Gateway debe pertenecer a la misma subred, por lo tanto 2001:DB8:ACAD:2::1 es incorrecto.

**Paso 2: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

**Desactivar la búsqueda DNS**

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

**Nombre del router**

```
Router(config)#hostname R1
R1(config)#
```

**Contraseña de exec privilegiado cifrada**

R1(config)#enable secret class

**Contraseña de acceso a la consola**

R1(config)#line console 0
R1(config-line)#password cisco
**Contraseña de acceso Telnet**

R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco

**Cifrar las contraseñas de texto no cifrado**

R1(config-line)#login
R1(config-line)#service password-encryption

**Mensaje MOTD**

R1(config)#banner motd "Se prohibe el acceso no autorizado."

**Interfaz S0/0/0**

R1(config)#int s0/0/0
R1(config-if)#description connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

**Rutas predeterminadas**

R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0

**Paso 3: Configurar R2**

La configuración del R2 incluye las siguientes tareas:

**Desactivar la búsqueda DNS**

Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

**Nombre del router**

Router(config)#hostname R2

**Contraseña de exec privilegiado cifrada**

R2(config)#enable secret class

**Contraseña de acceso a la consola**

R2(config)#line console 0
R2(config-line)#password cisco

**Contraseña de acceso Telnet**

R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco

**Cifrar las contraseñas de texto no cifrado**

R2(config-line)#login
R2(config-line)#service password-encryption

**Habilitar el servidor HTTP**

R2(config-line)#ip http server

**Mensaje MOTD**

R2(config)#banner motd "Se prohibe el acceso no autorizado."

**Interfaz S0/0/0**

Se prohibe el acceso no autorizado.
User Access Verification
Password:
R2>ena
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#description connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

**Interfaz S0/0/1**

R2(config)#int s0/0/1
R2(config-if)#description connection to R3
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

**Interfaz G0/0 (simulación de Internet)**

R2(config)#int g0/0
R2(config-if)#description connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown

**Interfaz loopback 0 (servidor web simulado)**

R2(config-if)#description simulated Servidor Web
R2(config-if)#ip address 10.10.10.10 255.255.255.255

**Ruta predeterminada**

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0

**Paso 4: Configurar R3**

La configuración del R3 incluye las siguientes tareas:

**Desactivar la búsqueda DNS**

Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

**Nombre del router**

Router(config)#hostname R3
R3(config)#

**Contraseña de exec privilegiado cifrada**

R3(config)#enable secret class

**Contraseña de acceso a la consola**

R3(config)#line console 0
R3(config-line)#password cisco

**Contraseña de acceso Telnet**

R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco

**Cifrar las contraseñas de texto no cifrado**

R3(config-line)#login
R3(config-line)#service password-encryption

**Mensaje MOTD**

R3(config)#banner motd "Se prohibe el acceso no autorizado."

**Interfaz S0/0/1**

R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown

**Interfaz loopback 4**

R3(config-if)#int loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
ip address 192.168.4.1 255.255.255.0

**Interfaz loopback 5**

R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
ip address 192.168.5.1 255.255.255.0

**Interfaz loopback 6**

R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
ip address 192.168.6.1 255.255.255.0

**Interfaz loopback 7**

R3(config-if)#int loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
ipv6 address 2001:db8:acad:3::1/64

**Rutas predeterminadas**

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 s0/0/1

**Paso 5: Configurar S1**

La configuración del S1 incluye las siguientes tareas:

**Desactivar la búsqueda DNS**

Switch>ena
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup

**Nombre del switch**

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

**Contraseña de exec privilegiado cifrada**

S1(config)#enable secret class

**Contraseña de acceso a la consola**

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

**Contraseña de acceso Telnet**

```
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
```

**Cifrar las contraseñas de texto no cifrado**

```
S1(config-line)#login
S1(config-line)#service password-Encryption
```

**Mensaje MOTD**

```
S1(config)#banner motd "Se prohibe el acceso no autorizado."
```

**Paso 6: configurar el S3**

La configuración del S3 incluye las siguientes tareas:

**Desactivar la búsqueda DNS**

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

**Nombre del switch**

```
Switch(config)#hostname S3
S1(config)#
```

**Contraseña de exec privilegiado cifrada**

S3(config)#enable secret class

**Contraseña de acceso a la consola**

S3(config)#line console 0
S3(config-line)#password cisco

**Contraseña de acceso Telnet**

S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco

**Cifrar las contraseñas de texto no cifrado**

S3(config-line)#login
S3(config-line)#service password-Encryption

**Mensaje MOTD**

S3(config)#banner motd "Se prohibe el acceso no autorizado."

**Paso 7: Verificar la conectividad de la red**

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

*Tabla 2 Verificacion Conectividad*

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | *Ver Ilustración 2* |
| R2 | R3, S0/0/1 | 172.16.2.1 | *Ver Ilustración 3* |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | *Ver Ilustración 4* |

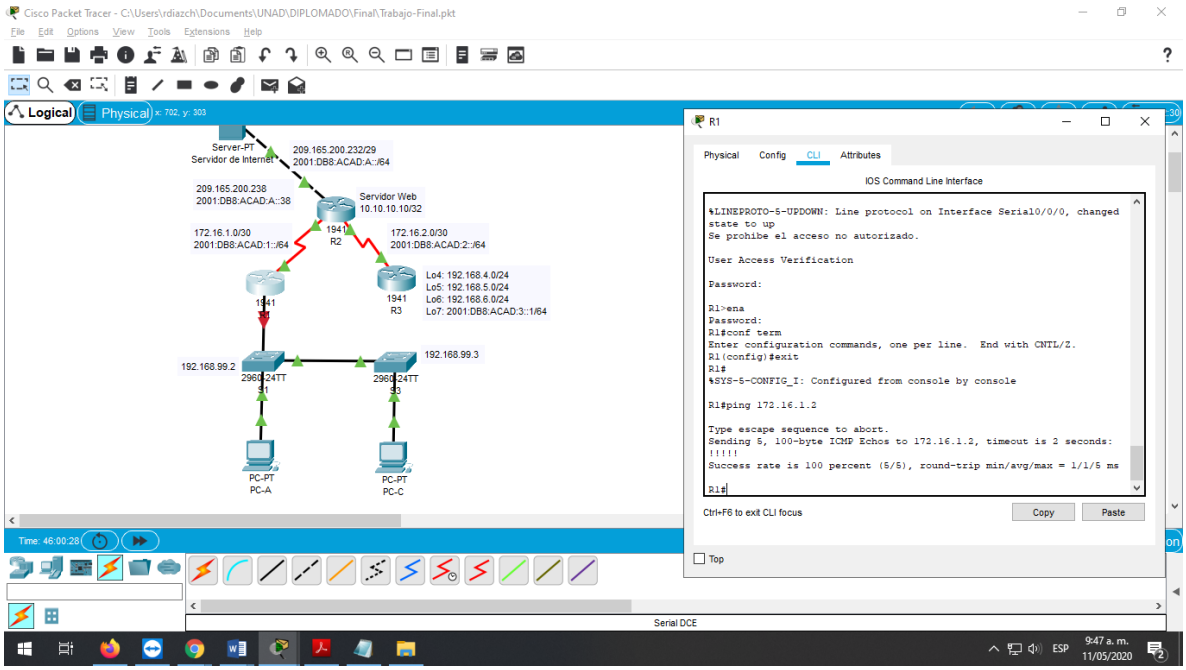

*Ilustración 2 Ping de R1 a R2*

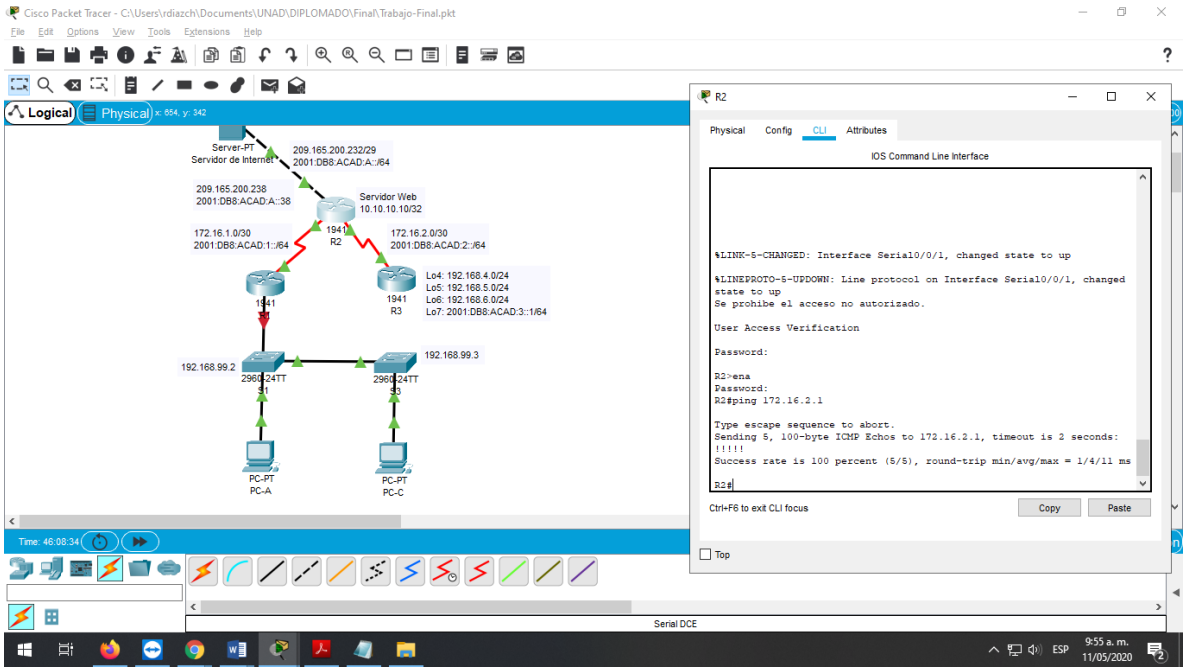


*Ilustración 3 Ping de R2 a R3*

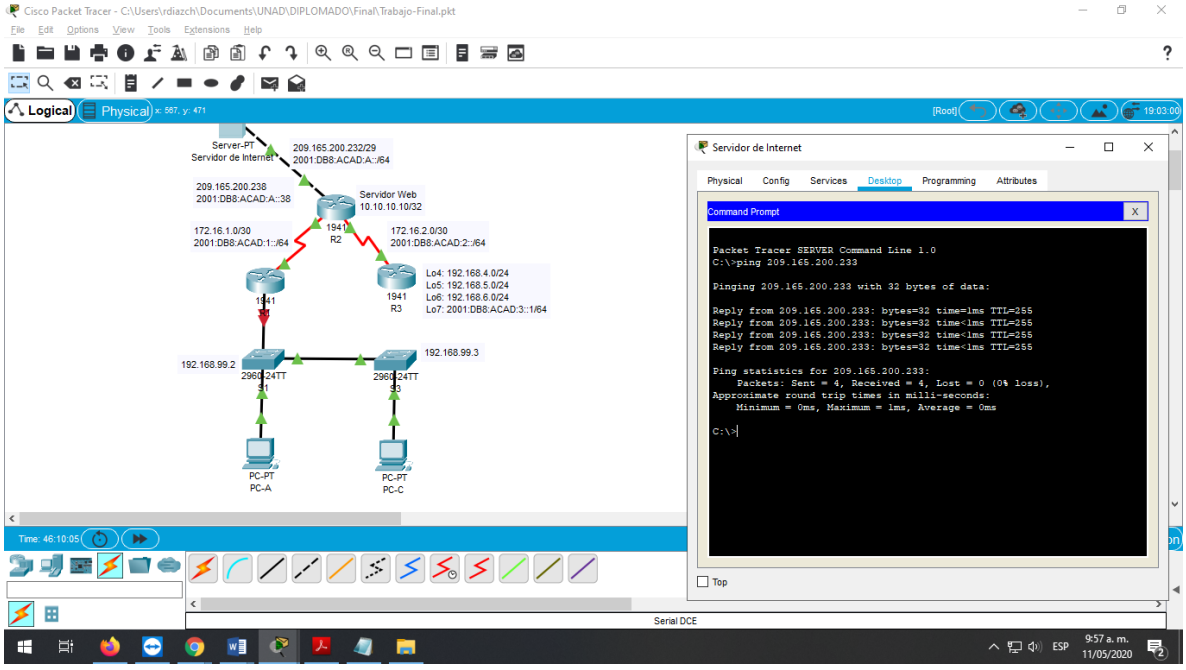


*Ilustración 4 Ping a R2*

**Parte 3: Configurar la seguridad del Switch, las VLAN y el routing entre VLAN**

**Paso 1: Configurar S1**

La configuración del S1 incluye las siguientes tareas:

**Crear la base de datos de VLAN**

```
S1>ena
Password:
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#
```

**Asignar la dirección IP de administración.**

```
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
```

**Asignar el gateway predeterminado**

```
S1(config)#ip default-gateway 192.168.99.1
```

**Forzar el enlace troncal en la interfaz F0/3**

```
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
switchport trunk native vlan 1
S1(config-if)#

**Forzar el enlace troncal en la interfaz F0/5**

S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#

**Configurar el resto de los puertos como puertos de acceso**

S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access

**Asignar F0/6 a la VLAN 21**

S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21

**Apagar todos los puertos sin usar**

S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#

**Paso 3: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

**Crear la base de datos de VLAN**

S3>ena
Password:
S3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23

S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion

**Asignar la dirección IP de administración**

S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown

**Asignar el gateway predeterminado.**

S3(config)#ip default-gateway 192.168.99.1

**Forzar el enlace troncal en la interfaz F0/3**

S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

**Configurar el resto de los puertos como puertos de acceso**

S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access

**Asignar F0/18 a la VLAN 21**

S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23

**Apagar todos los puertos sin usar**

S3(config-if)#int range f0/1-2, f0/4-17,f0/19-24, g0/1-2
S3(config-if-range)#shutdown

S3(config-if-range)#

**Paso 3: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

**Configurar la subinterfaz 802.1Q .21 en G0/1**

```
R1>ena
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
```

**Configurar la subinterfaz 802.1Q .23 en G0/1**

```
R1(config-subif)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
```

**Configurar la subinterfaz 802.1Q .99 en G0/1**

```
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

**Activar la interfaz G0/1**

```
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
```

**Paso 4: Verificar la conectividad de red**

Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

*Tabla 3 Verificacion Conectividad*

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | *Ver Ilustración 5* |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | *Ver Ilustración 6* |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | *Ver Ilustración 7* |
| S3 | R1, dirección VLAN 23 | | *Ver Ilustración 8* |

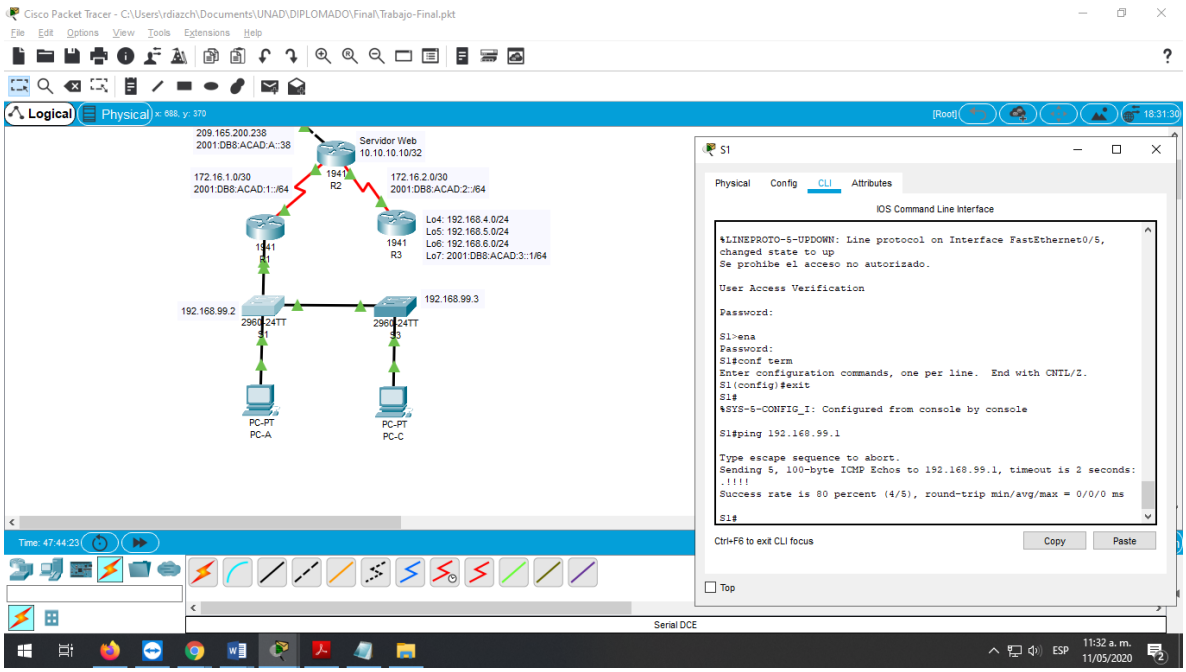


*Ilustración 5 Ping de S1 a R1 VLAN 99*

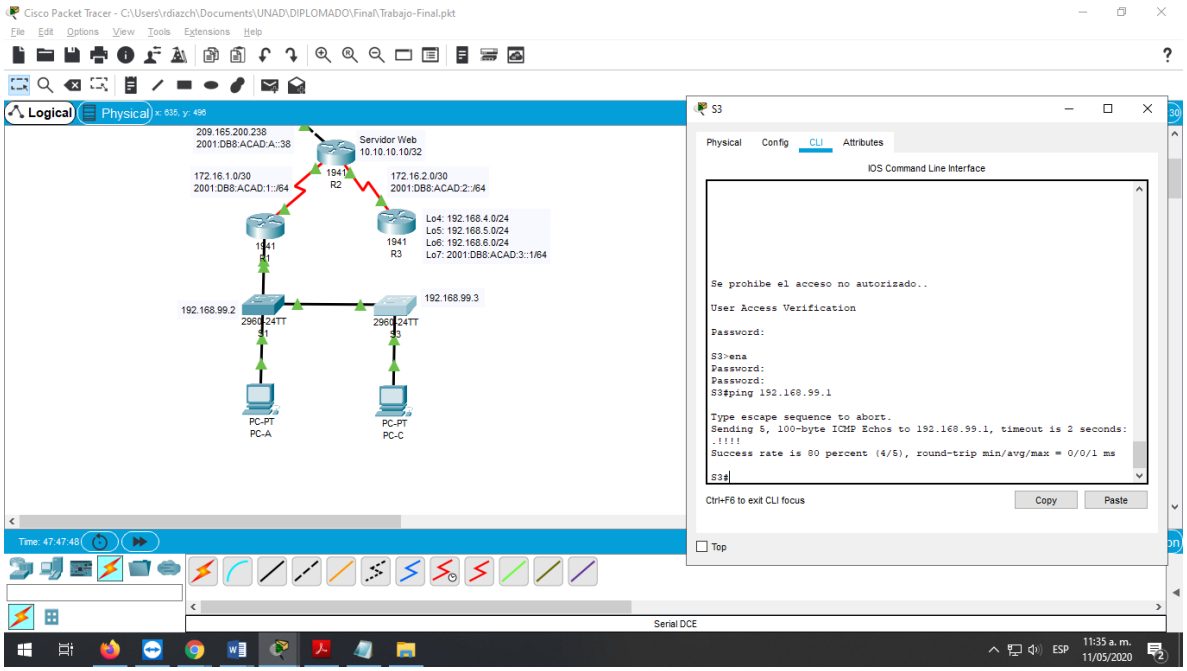


*Ilustración 6 Ping de S3 a R1 VLAN 99*

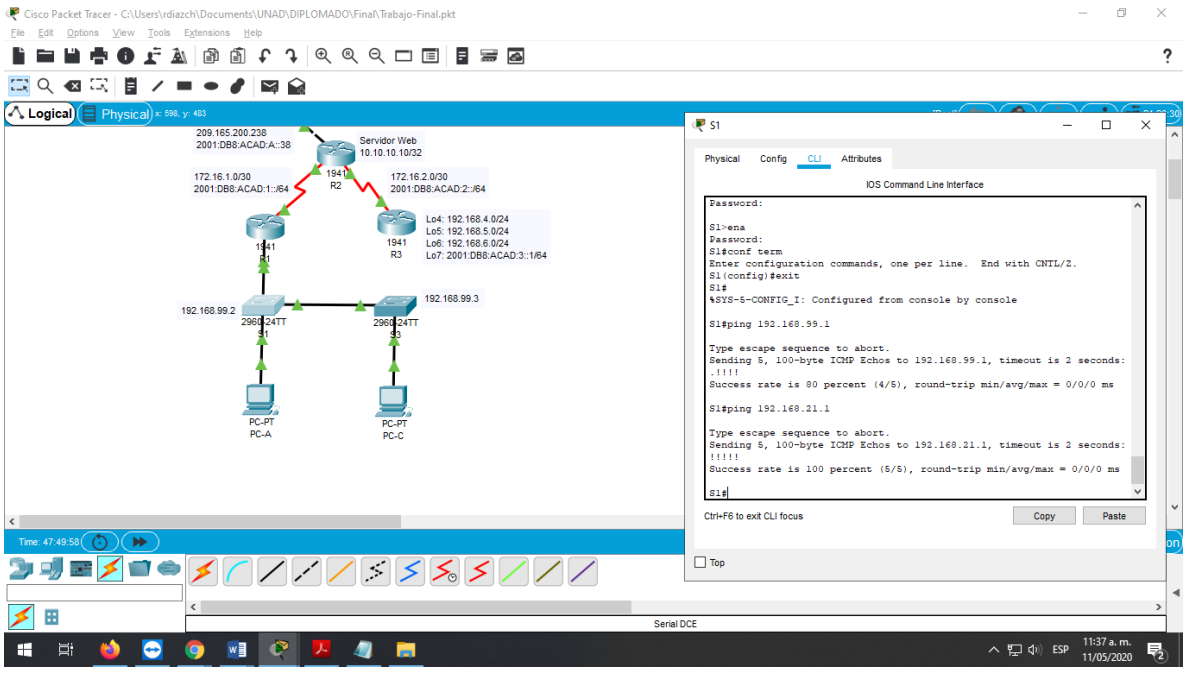


*Ilustración 7 Ping de S1 a R1 VLAN 21*

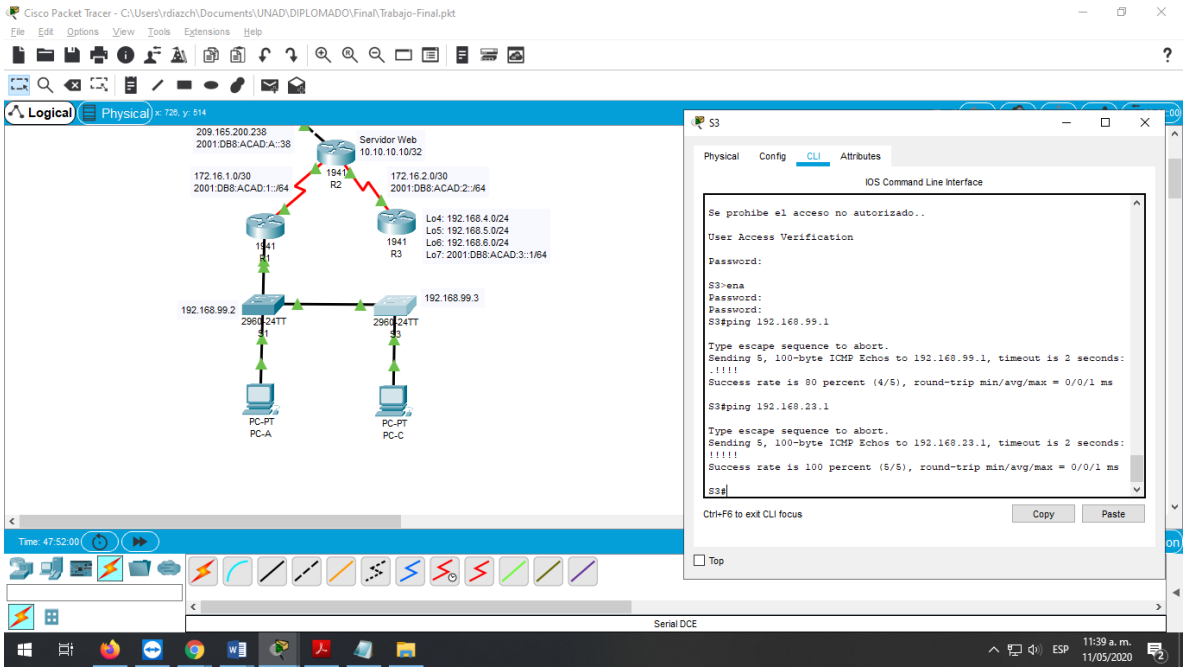


*Ilustración 8 Ping de S3 a R1 VLAN 23*

**Parte 4: Configurar el protocolo de Routing dinámico RIPv2**

**Paso 1: Configurar RIPv2 en el R1**

Las tareas de configuración para R1 incluyen las siguientes:

**Configurar RIP versión 2**

R1>ena
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2

**Anunciar las redes conectadas directamente**

R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

```
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
```

**Establecer todas las interfaces LAN como pasivas**

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
```

**Desactive la sumarización automática**

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

**Paso 2: Configurar RIPv2 en el R2**

La configuración del R2 incluye las siguientes tareas:

**Configurar RIP versión 2**

```
R2>ena
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
```

**Anunciar las redes conectadas directamente**

```
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
```

**Establecer todas las interfaces LAN (Loopback) como pasivas**

R2(config-router)#passive-interface loopback 0

**Desactive la sumarización automática**

R2(config-router)#no auto-summary

**Paso 3: Configurar RIPv2 en el R3**

La configuración del R3 incluye las siguientes tareas:

**Configurar RIP versión 2**

R3>ena
Password:
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2

**Anunciar las redes conectadas directamente**

R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0

**Establecer todas las interfaces LAN (Loopback) como pasivas**

R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6

**Desactive la sumarización automática**

R3(config-router)#no auto-summary

## Paso 4: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

**¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?**

R1#show ip protocols

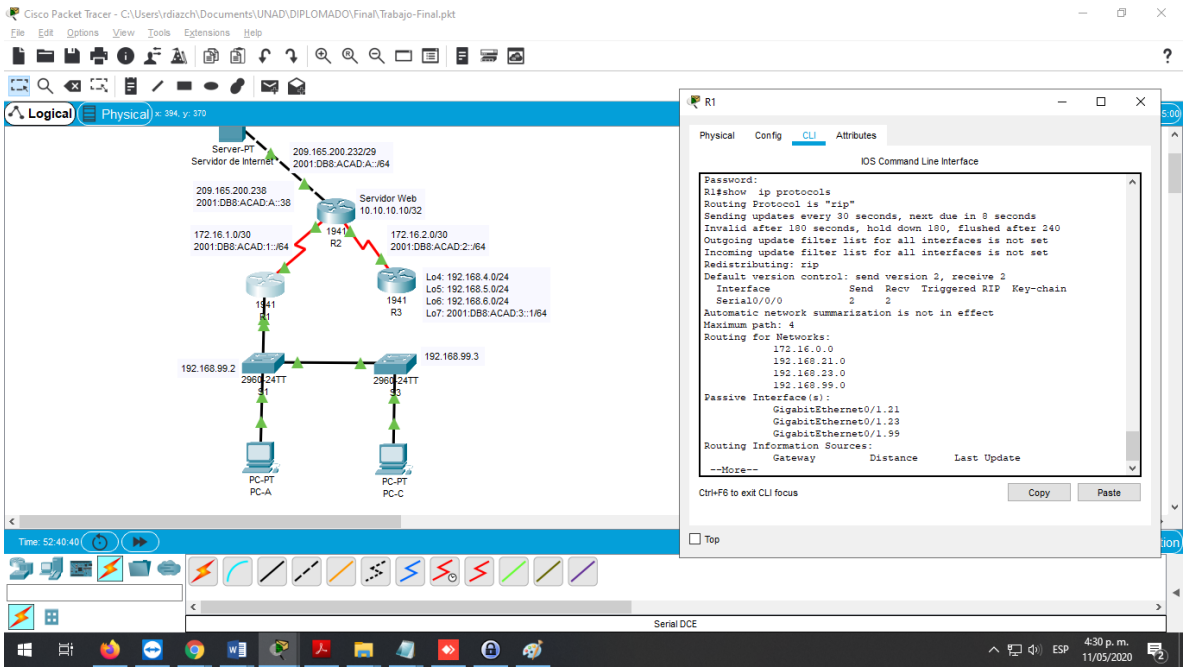


*Ilustración 9 show ip protocols R1*

**¿Qué comando muestra solo las rutas RIP?**

R1#show ip route rip

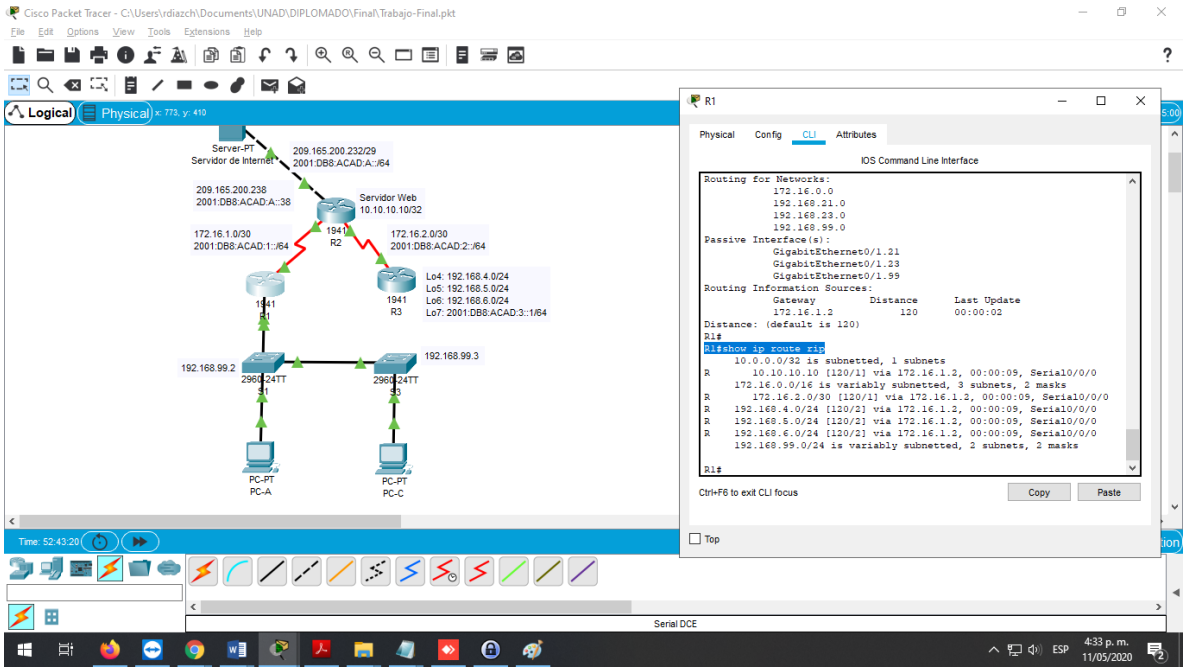


*Ilustración 10 show ip route rip*

## Parte 5: Implementar DHCP y NAT para IPv4

### Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

**Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas**

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

**Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas**

R1(config)#ip dhcp excluded-address 192.168.231.1 192.168.23.20

**Crear un pool de DHCP para la VLAN 21**

R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1

```
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

**Crear un pool de DHCP para la VLAN 23**

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

**Paso 2: Configurar la NAT estática y dinámica en el R2**

La configuración del R2 incluye las siguientes tareas:

**Crear una base de datos local con una cuenta de usuario**

```
R2>ena
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
```

**Habilitar el servicio del servidor HTTP**

El comando “ip http server” no es compatible con Packet Tracer.

**Configurar el servidor HTTP para utilizar la base de datos local para la autenticación**

El comando “ip http authentication local” no es compatible con Packet Tracer.

**Crear una NAT estática al servidor web**

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

**Asignar la interfaz interna y externa para la NAT estática**

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

**Configurar la NAT dinámica dentro de una ACL privada**

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

**Defina el pool de direcciones IP públicas utilizables.**

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

**Definir la traducción de NAT dinámica**

R2(config)#ip nat inside source list 1 pool INTERNET

**Paso 3: Verificar el protocolo DHCP y la NAT estática**

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

*Tabla 4 Verificacion DHCP y NAT*

| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | *Ver Ilustración 11* |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | *Ver Ilustración 12* |
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. | *Ver Ilustración 13* |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.233) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | *Ver Ilustración 14* |

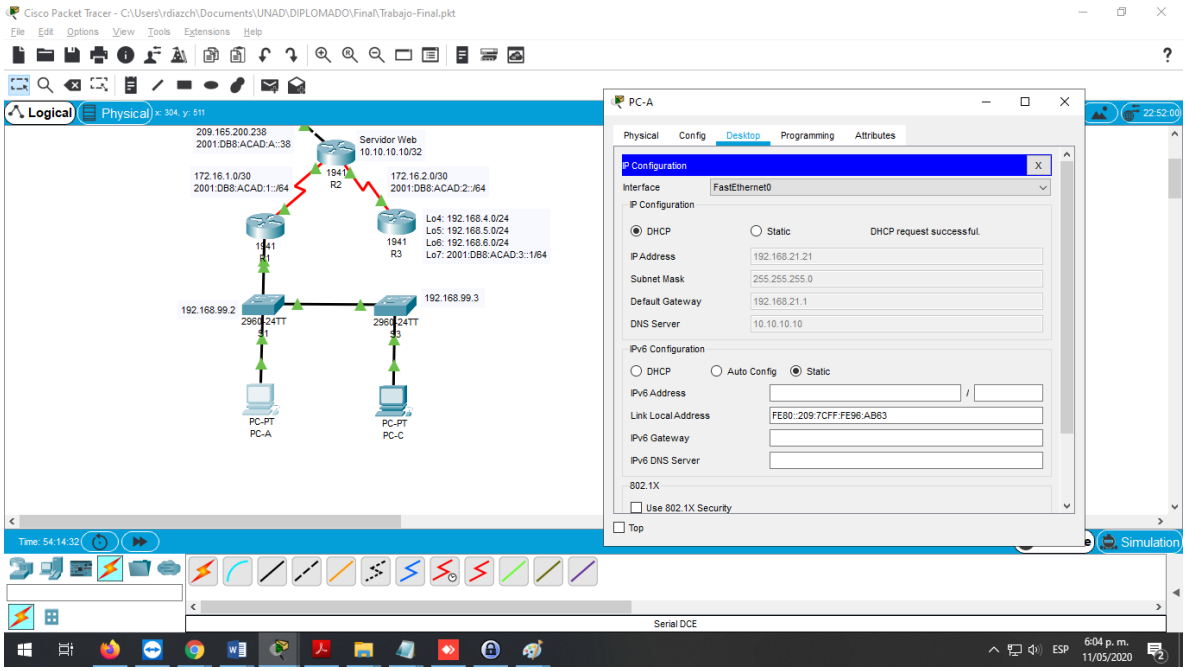


*Ilustración 11 DHCP en PC-A*

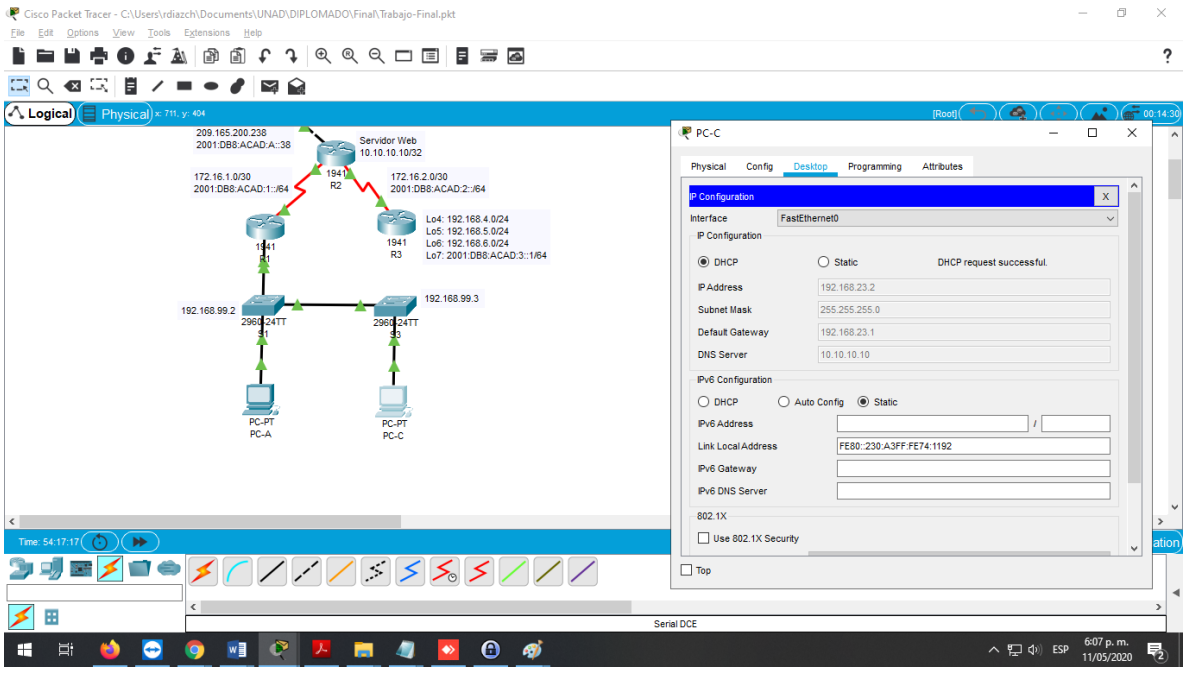


*Ilustración 12 DHCP en PC-C*

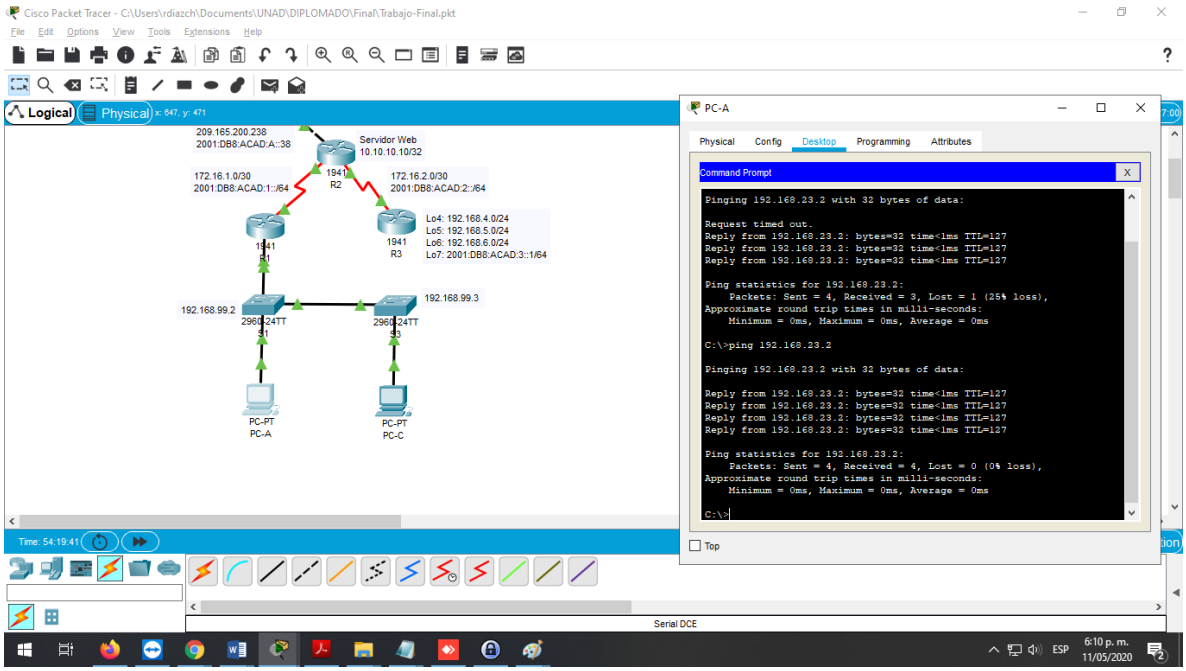


*Ilustración 13 Ping de PC-A a PC-C*

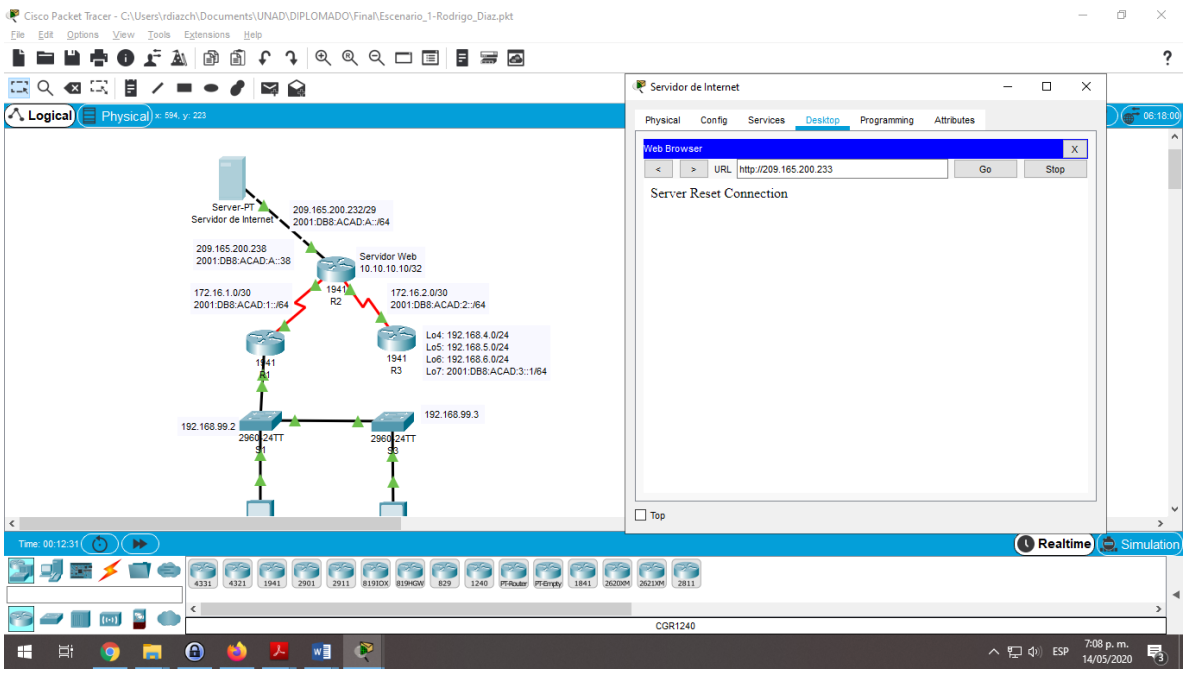


*Ilustración 14 Intento de acceso a servicio Web*

**Parte 6: Configurar NTP**

**Ajuste la fecha y hora en R2**

R2>ena
Password:
R2#
R2#clock set 9:00:00 5 march 2016
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.

**Configure R2 como un maestro NTP**

R2(config)#ntp master 5
R2(config)#

**Configure R1 para actualizaciones de calendario periódicas con hora NTP**

R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar

**Verifique la configuración de NTP en R1**

R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
show ntp associations
address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 6 16 7 2.00 726181534747.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#

**Parte 7: Configurar y verificar las listas de control de acceso (ACL)**

**Paso 1: Restringir el acceso a las líneas VTY en el R2**

**Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2**

R2(config)# ip access-list standard ADMIN-MGT

R2(config-std-nacl)#permit host 172.16.1.1

**Aplicar la ACL con nombre a las líneas VTY**

R2(config-line)#access-class ADMIN-MGT in

**Permitir acceso por Telnet a las líneas de VTY**

R2(config-line)#transport input telnet

**Verificar que la ACL funcione como se espera**

Se prohibe el acceso no autorizado.
User Access Verification
Password:
R1>ena
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado.
User Access Verification
Password:
R2>

Se prohibe el acceso no autorizado.
User Access Verification
Password:
R3>ena
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#

**Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

**Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció**

R2#show access-list

```
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
```

**Restablecer los contadores de una lista de acceso**

```
R2#clear ip access-list counters
                 ^
% Invalid input detected at '^' marker.
```

**No soportado por Packet Tracer**

**¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?**

```
R2#show ip interface
```

**¿Con qué comando se muestran las traducciones NAT?**

```
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
R2#
```

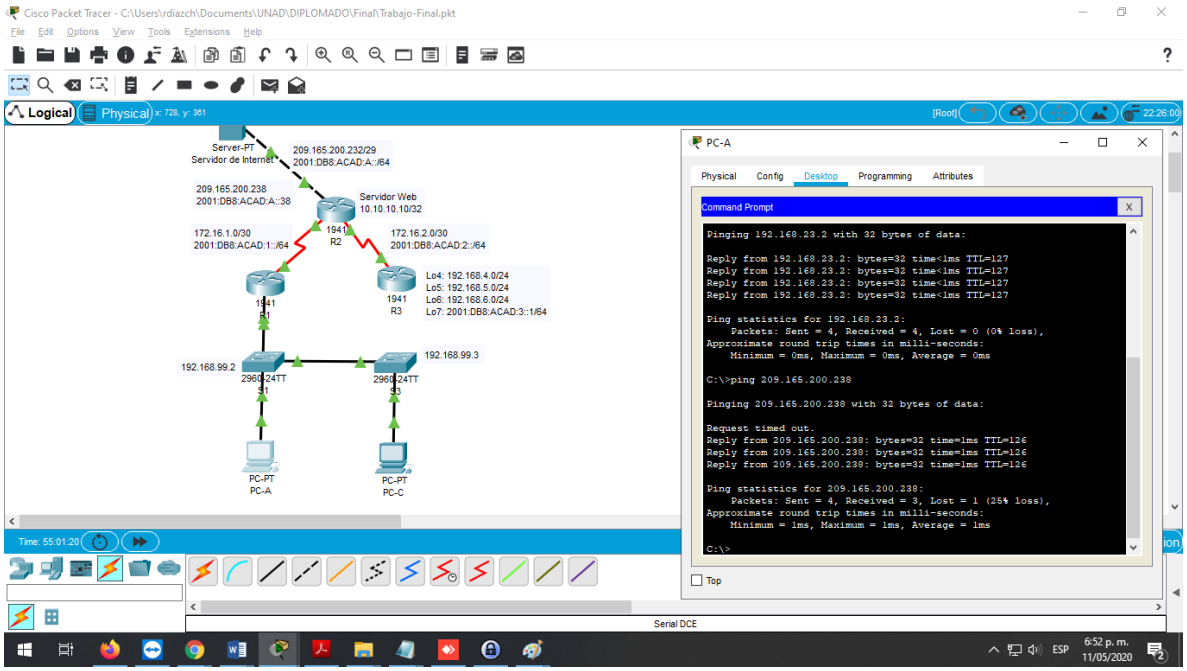


*Ilustración 15 Ping de PC-A a PC-C y Servidor de Internet*

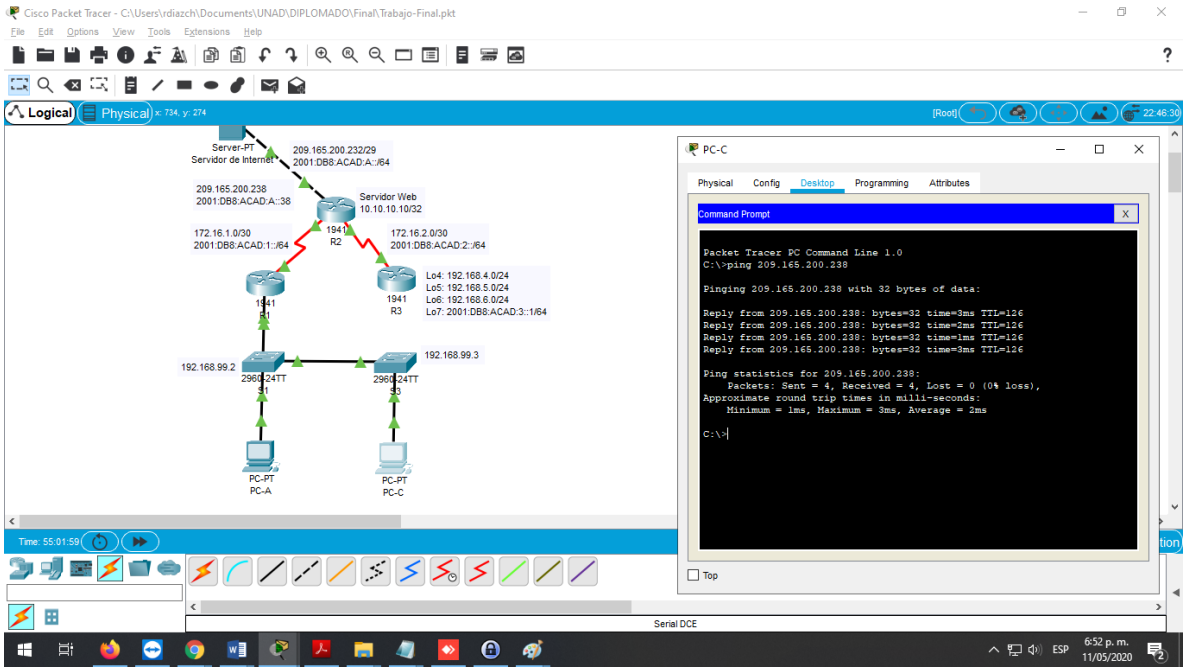


*Ilustración 16 Ping de PC-C a Servidor de Internet*

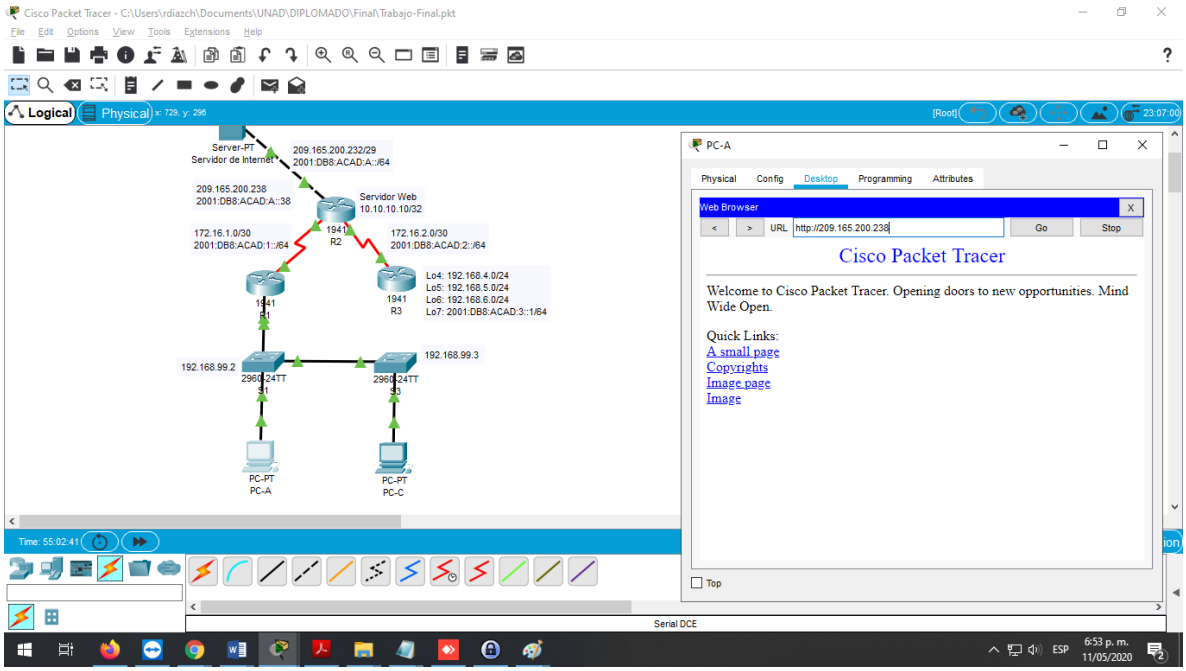


*Ilustración 17 Acceso a HTTP Web Service desde PC-A*

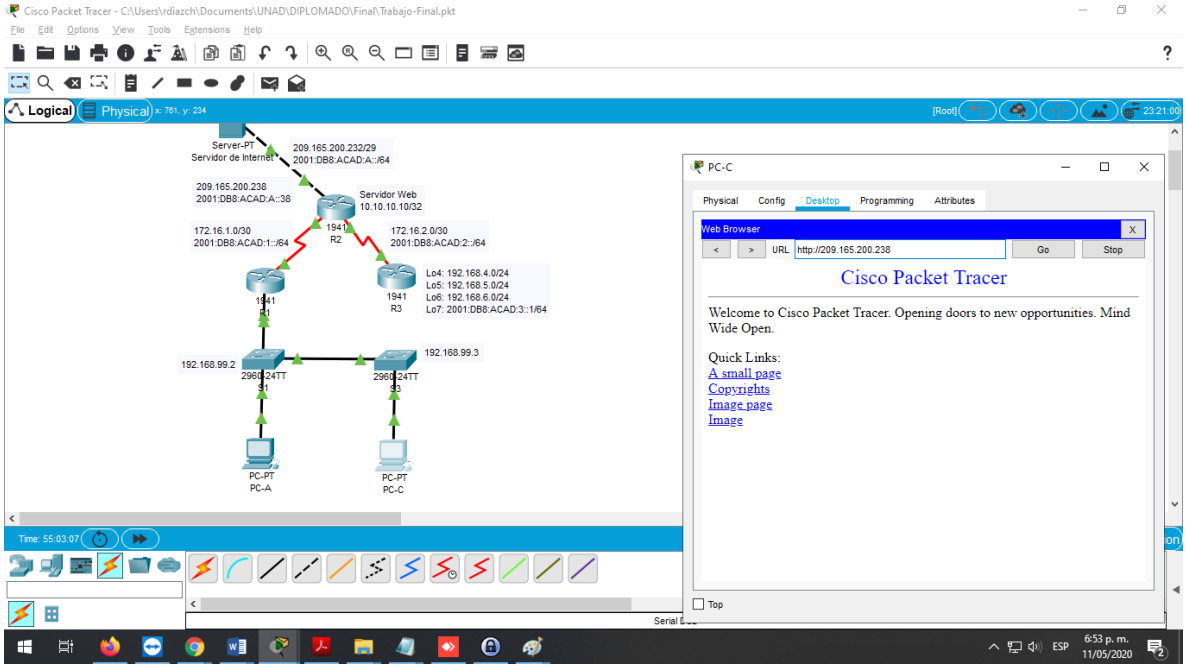


*Ilustración 18 Acceso a HTTP Web Service desde PC-C*

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.235:1025192.168.21.21:1025 209.165.200.238:80
209.165.200.238:80
tcp 209.165.200.236:1025192.168.23.2:1025 209.165.200.238:80
209.165.200.238:80
**¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?**

R2#clear ip nat translation *
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
R2#

## 5. ESCENARIO 2

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

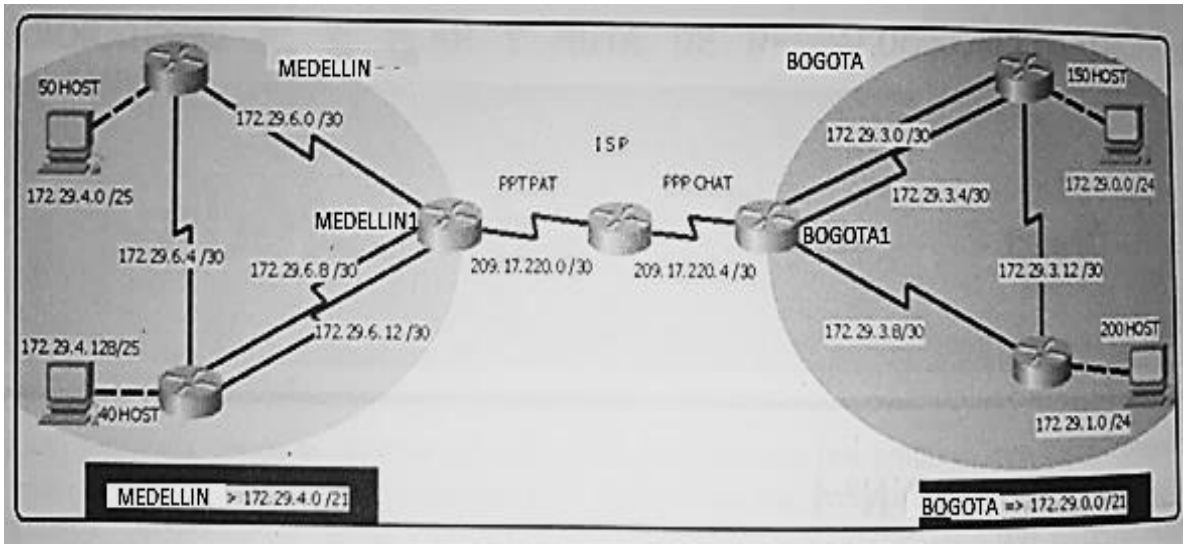


*Ilustración 19 Escenario 2*

Este escenario plantea el uso de OSPF 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 las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

```
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd "Se prohibe el acceso no autorizado."
ISP(config)#
```

```
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota1
Bogota1(config)#enable secret class
Bogota1(config)#line console 0
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#line vty 0 15
Bogota1(config-line)#password cisco
Bogota1(config-line)#login
Bogota1(config-line)#service password-encryption
Bogota1(config-line)# banner motd "Se prohibe el acceso no autorizado."
```

```
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota2
Bogota2(config)#enable secret class
Bogota2(config)#line console 0
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#line vty 0 15
```

```
Bogota2(config-line)#password cisco
Bogota2(config-line)#login
Bogota2(config-line)#service password-encryption
Bogota2(config)#banner motd "Se prohibe el acceso no autorizado."
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota3
Bogota3(config)#enable secret class
Bogota3(config)#line console 0
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#line vty 0 15
Bogota3(config-line)#password cisco
Bogota3(config-line)#login
Bogota3(config-line)#service password-encryption
Bogota3(config)#banner motd "Se prohibe el acceso no autorizado."

Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin1
Medellin1(config)#enable secret class
Medellin1(config)#line console 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#service password-encryption
Medellin1(config)#banner motd "Se prohibe el acceso no autorizado."

Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin2
Medellin2(config)#enable secret class
Medellin2(config)#line console 0
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#line vty 0 15
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#service password-encryption
```

Medellin2(config)#banner motd "Se prohibe el acceso no autorizado."

Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin3
Medellin3(config)#enable secret class
Medellin3(config)#line console 0
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#line vty 0 15
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#service password-encryption
Medellin3(config)#banner motd "Se prohibe el acceso no autorizado."

- Realizar la conexión física de los equipos con base en la topología de red

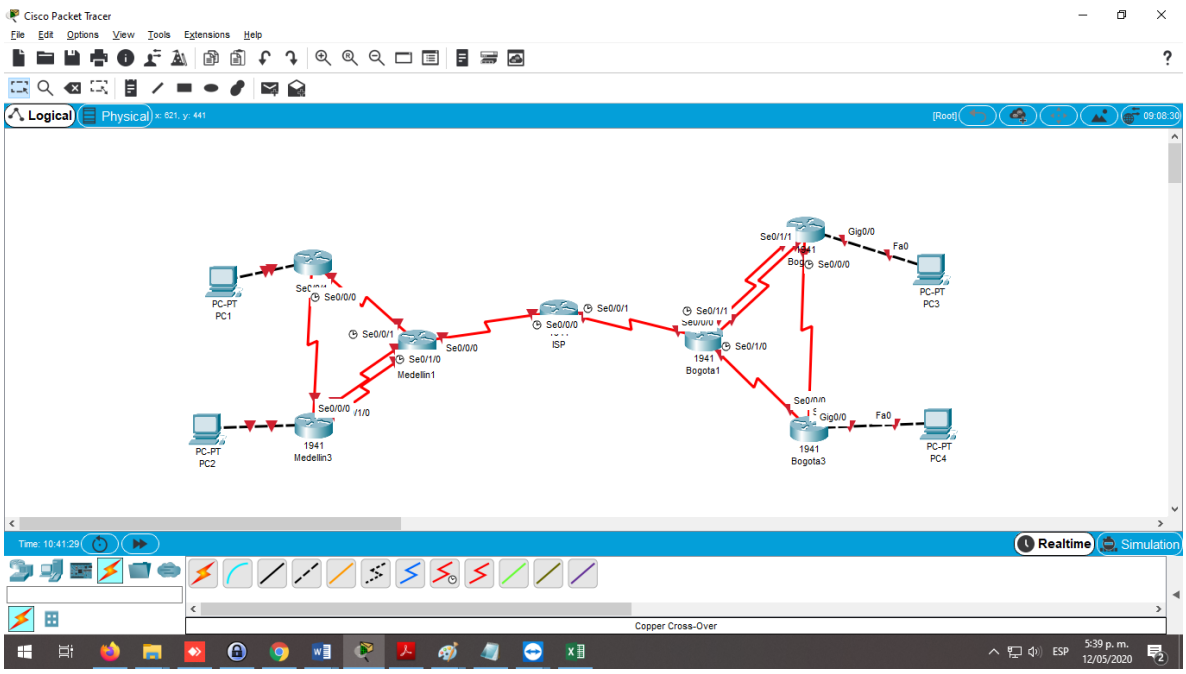


*Ilustración 20 Esquema sin Configurar*

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

*Tabla 5 Enrutamiento Escenario 2*

| Dispositivo | Interfaz | Dirección IP | Mascara | Wildcard | Gateway |
|---|---|---|---|---|---|
| ISP | S0/0/1 | 209.17.220.5 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/0 | 209.17.220.1 | 255.255.255.252 | 0.0.0.3 | |
| Bogota1 | S0/0/0 | 209.17.220.6 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/1 | 172.29.3.1 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/1 | 172.29.3.5 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/0 | 172.29.3.9 | 255.255.255.252 | 0.0.0.3 | |
| Bogota2 | S0/0/1 | 172.29.3.2 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/1 | 172.29.3.6 | 255.255.255.252 | 0.0.0.3 | |
| | G0/0 | 172.29.0.1 | 255.255.255.0 | 0.0.0.255 | |
| | S0/0/0 | 172.29.3.13 | 255.255.255.252 | 0.0.0.3 | |
| Bogota3 | S0/0/0 | 172.29.3.10 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/1 | 172.29.3.14 | 255.255.255.252 | 0.0.0.3 | |
| | G0/0 | 172.29.1.1 | 255.255.255.0 | 0.0.0.255 | |
| Medellin1 | S0/0/0 | 209.17.220.2 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/0 | 172.29.6.13 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/1 | 172.29.6.9 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/1 | 172.29.6.1 | 255.255.255.252 | 0.0.0.3 | |
| Medellin2 | S0/0/1 | 172.29.6.2 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/0 | 172.29.6.5 | 255.255.255.252 | 0.0.0.3 | |
| | G0/0 | 172.29.4.1 | 255.255.255.128 | 0.0.0.127 | |
| Medellin3 | S0/1/0 | 172.29.6.14 | 255.255.255.252 | 0.0.0.3 | |
| | S0/1/1 | 172.29.6.10 | 255.255.255.252 | 0.0.0.3 | |
| | S0/0/0 | 172.29.6.6 | 255.255.255.252 | 0.0.0.3 | |
| | G0/0 | 172.29.4.129 | 255.255.255.128 | 0.0.0.127 | |
| PC1 | Fa0 | DHCP | 255.255.255.128 | 0.0.0.127 | 172.29.4.1 |
| PC2 | Fa0 | DHCP | 255.255.255.128 | 0.0.0.127 | 172.29.4.129 |
| PC3 | Fa0 | DHCP | 255.255.255.0 | 0.0.0.255 | 172.29.0.1 |
| PC4 | Fa0 | DHCP | 255.255.255.0 | 0.0.0.255 | 172.29.1.1 |

**Router ISP**

ISP>ena
Password:
ISP#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**ISP(config)#int s0/0/1**
ISP(config-if)#description connection to Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
This command applies only to DCE interfaces
ISP(config-if)#no shutdown
**ISP(config)#int s0/0/0**
ISP(config-if)#description connection to Medellin1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

**Routers Bogotá**

Bogota1>ena
Password:
Bogota1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**Bogota1(config)#int s0/0/0**
Bogota1(config-if)#description connection to ISP
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
**Bogota1(config)#int s0/1**/1
Bogota1(config-if)#description connection to Bogota2
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
**Bogota1(config-if)#int s0/0/1**
Bogota1(config-if)#description connection to Bogota2
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
**Bogota1(config-if)#int s0/1/0**
Bogota1(config-if)#description connection to Bogota3
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown

**Bogota2(config)#int s0/0/1**
Bogota2(config-if)#description connection Bogota1
Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota2(config-if)#no shutdown
%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
**Bogota2(config-if)#int s0/1/1**
Bogota2(config-if)#description connection to Bogota1
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
**Bogota2(config-if)#int s0/0/0**
Bogota2(config-if)#description connection to Bogota3
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#no shutdown
**Bogota2(config)#int g0/0**
Bogota2(config-if)#description connection to PC3
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown

Bogota3>ena
Password:
Bogota3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**Bogota3(config)#int s0/0/0**
Bogota3(config-if)#description connection to Bogota1
Bogota3(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota3(config-if)#clock rate 128000
This command applies only to DCE interfaces
Bogota3(config-if)#no shutdown
%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
**Bogota3(config-if)#int s0/0/1**
Bogota3(config-if)#description connection to Bogota2
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#clock rate 128000
This command applies only to DCE interfaces
Bogota3(config-if)#no shutdown
%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

**Bogota3(config)#int g0/0**
Bogota3(config-if)#description connection to PC4
Bogota3(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota3(config-if)#no shutdown

**Routers Medellín**

Medellin1>ena
Password:
Medellin1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**Medellin1(config)#int s0/0/0**
Medellin1(config-if)#description connection to ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#no shutdown
**Medellin1(config)#int s0/1/0**
Medellin1(config-if)#description connection to Medellin3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
**Medellin1(config-if)#int s0/1/1**
Medellin1(config-if)#description connection to Medellin3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
**Medellin1(config-if)#int s0/0/1**
Medellin1(config-if)#description connection to Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown

Medellin2>ena
Password:
Medellin2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**Medellin2(config)#int s0/0/1**
Medellin2(config-if)#description connection to Medellin1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#no shutdown
%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
**Medellin2(config-if)#int s0/0/0**
Medellin2(config-if)#description connection to Medellin3

Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
**Medellin2(config-if)# int g0/0**
Medellin2(config-if)#description connection to PC1
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown

Medellin3>ena
Password:
Medellin3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
**Medellin3(config)#int s0/1/0**
Medellin3(config-if)#description connection to Medellin1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
**Medellin3(config-if)#int s0/1/1**
Medellin3(config-if)#description connection to Medellin1
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
**Medellin3(config-if)#int s0/0/0**
Medellin3(config-if)#description connection to Medellin2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
%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
**Medellin3(config-if)#int g0/0**
Medellin3(config-if)#description connection to PC2
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

**Parte 1: Configuración del enrutamiento**

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

**Routers Bogotá**

```
Bogota1>ena
Password:
Bogota1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config-router)#router ospf 1
Bogota1(config-router)#router-id 1.1.1.1
Bogota1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/1/0
C 209.17.220.4/30 is directly connected, Serial0/0/0
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#network 209.17.220.4 0.0.0.3 area 0
Bogota1(config-router)#exit

Bogota2>ena
Password:
Password:
Bogota2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router ospf 1
Bogota2(config-router)#router-id 2.2.2.2
Bogota2(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.12/30 is directly connected, Serial0/0/0
Bogota2(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#exit

Bogota3>ena
Password:
Bogota3#conf term
```

Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router ospf 1
Bogota3(config-router)#router-id 3.3.3.3
Bogota3(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
Bogota3(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#exit

**Routers Medellín**

Medellin1>ena
Password:
Medellin1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 4.4.4.4
Medellin1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
C 209.17.220.0/30 is directly connected, Serial0/0/0
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#exit

Medellin2>ena
Password:
Medellin2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#router ospf 1
Medellin2(config-router)#router-id 5.5.5.5
Medellin2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0

Medellin2(config-router)#exit

Medellin3>ena
Password:
Medellin3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router ospf 1
Medellin3(config-router)#router-id 6.6.6.6
Medellin3(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/1/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#exit

**Router ISP**

ISP>ena
Password:
Password:
ISP#conf term
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config-router)#router-id 7.7.7.7
ISP(config-router)#do show ip route connected
C 209.17.220.0/30 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#exit

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 OSPF.

Bogota1>ena
Password:
Password:
Password:

```
Bogota1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota1(config)#router ospf 1
Bogota1(config-router)#default-information originate
Bogota1(config-router)#exit

Medellin1>ena
Password:
Medellin1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin1(config)#router ospf 1
Medellin1(config-router)#default-information originate
Medellin1(config-router)#exit
```

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

```
ISP>ena
Password:
ISP#conf te
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

**Parte 2: Tabla de Enrutamiento**

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

## Router ISP

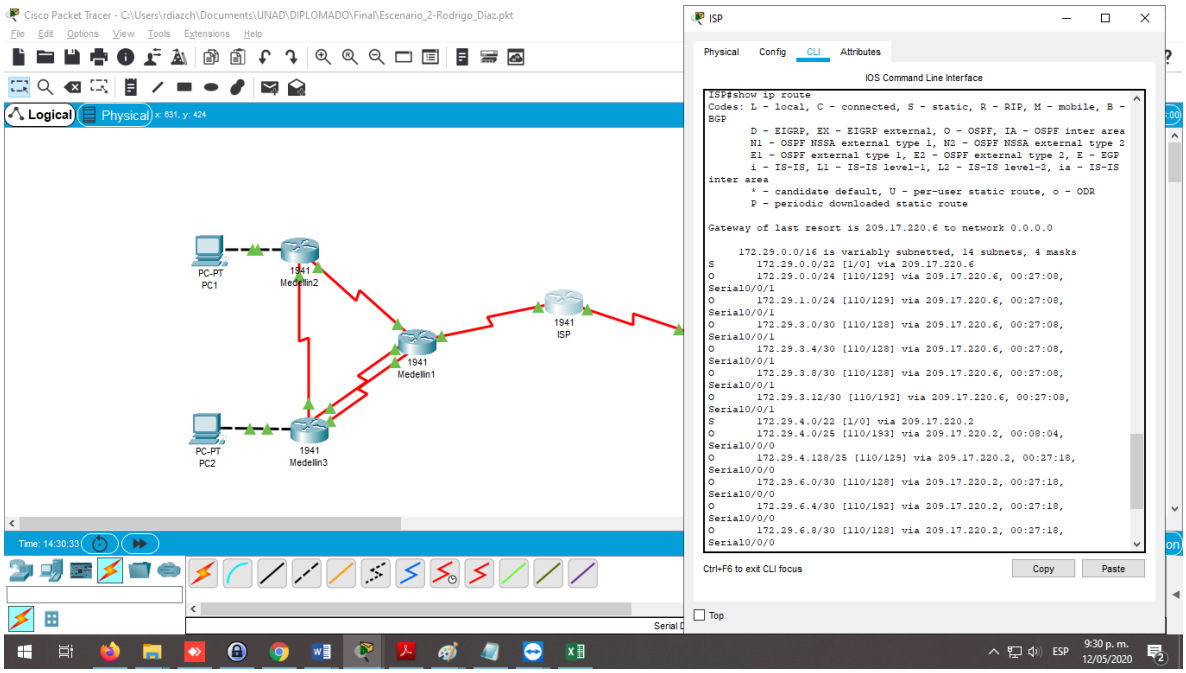


*Ilustración 21 show ip route en ISP*

## Router Bogota1

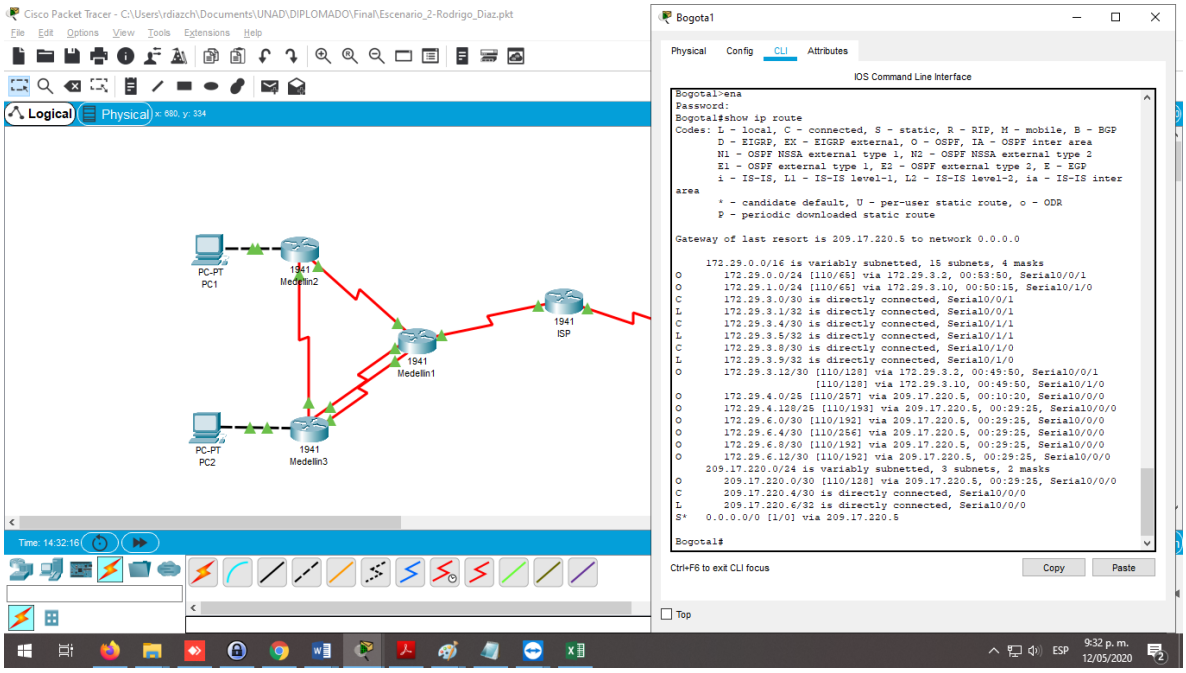


*Ilustración 22 show ip route en Bogota1*

## Router Bogota2

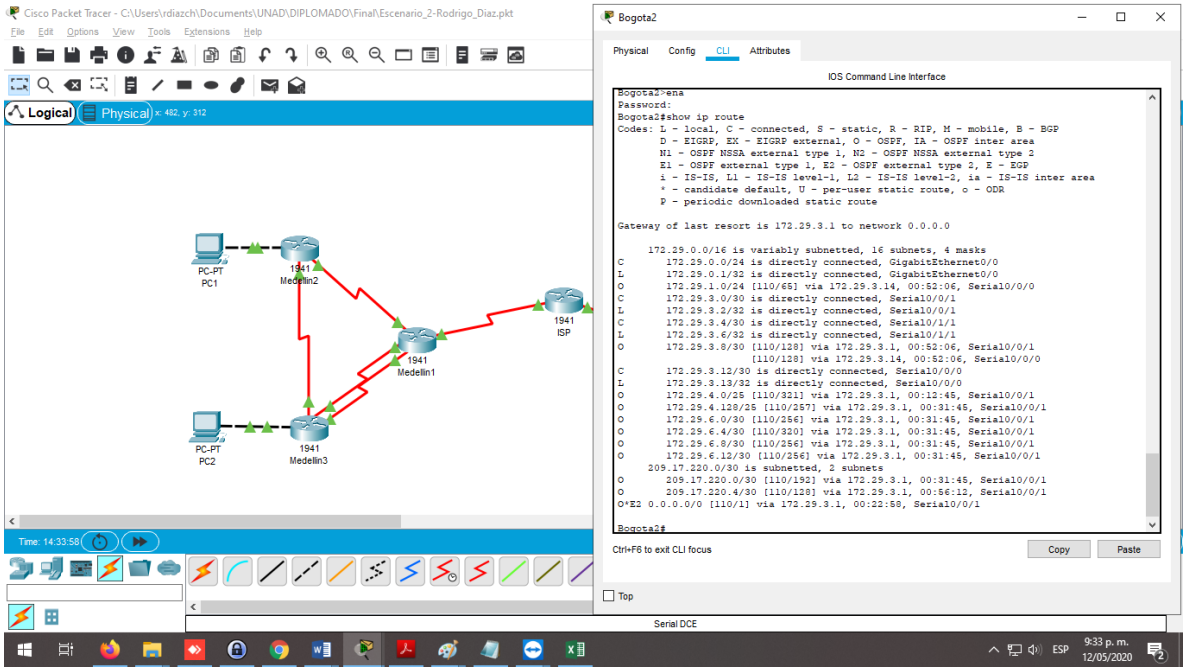


*Ilustración 23 show ip route en Bogota2*

## Router Bogota3

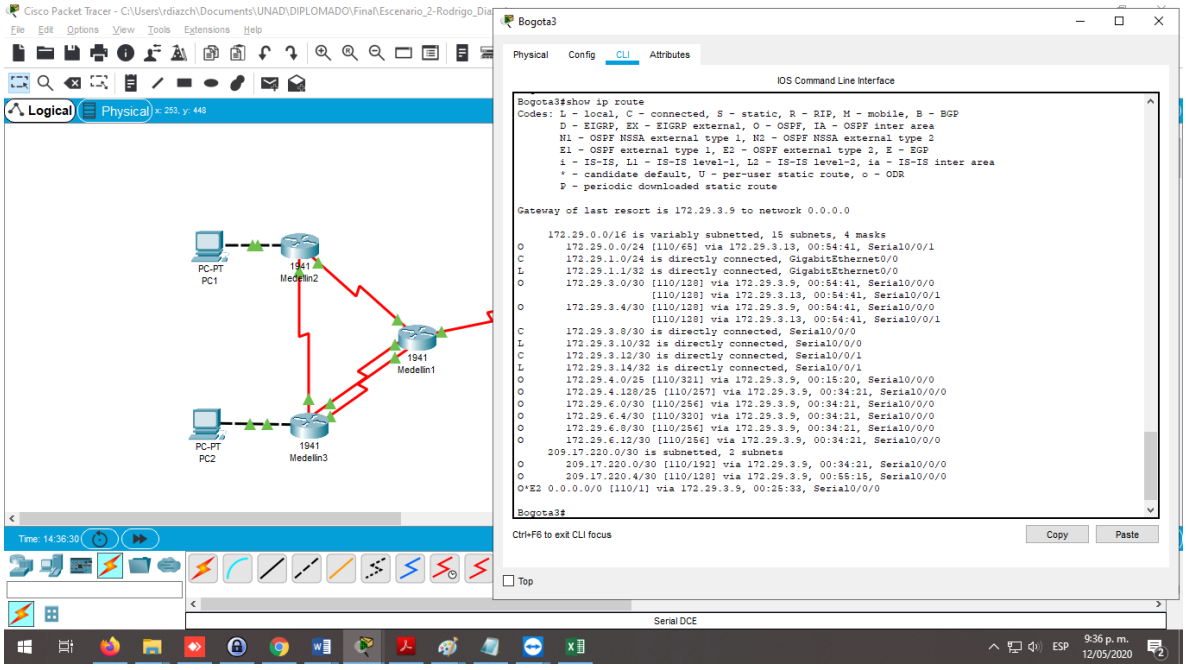


*Ilustración 24 show ip route en Bogota3*

## Router Medellin1

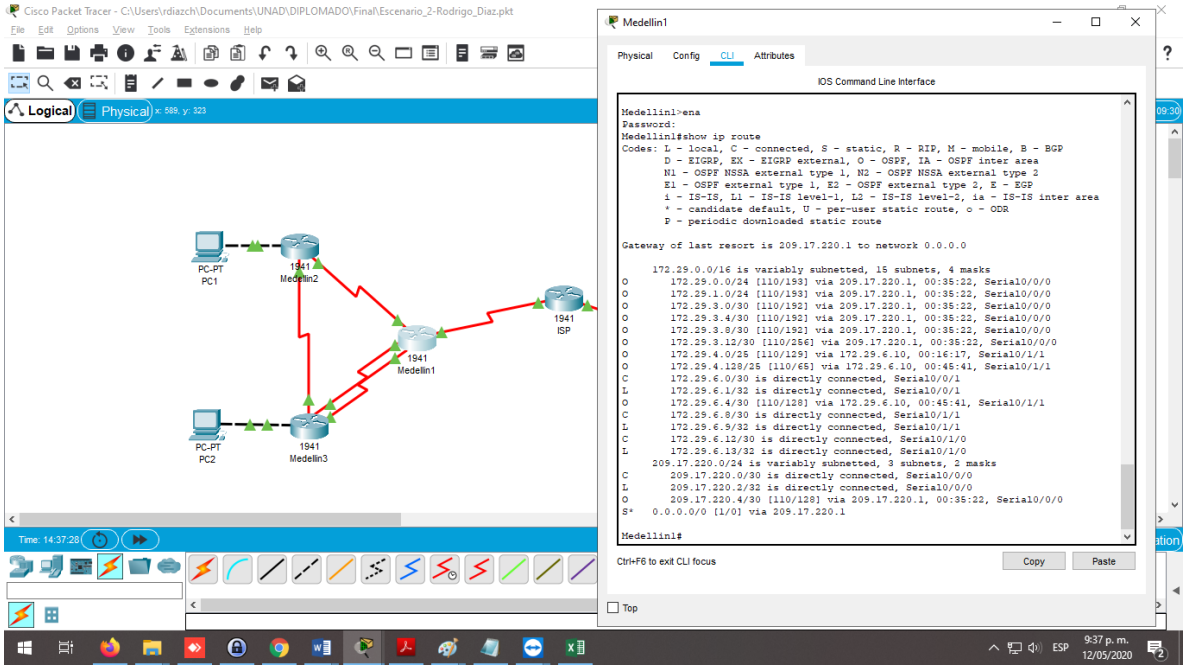


*Ilustración 25 show ip route en Medellin1*

## Router Medellin2

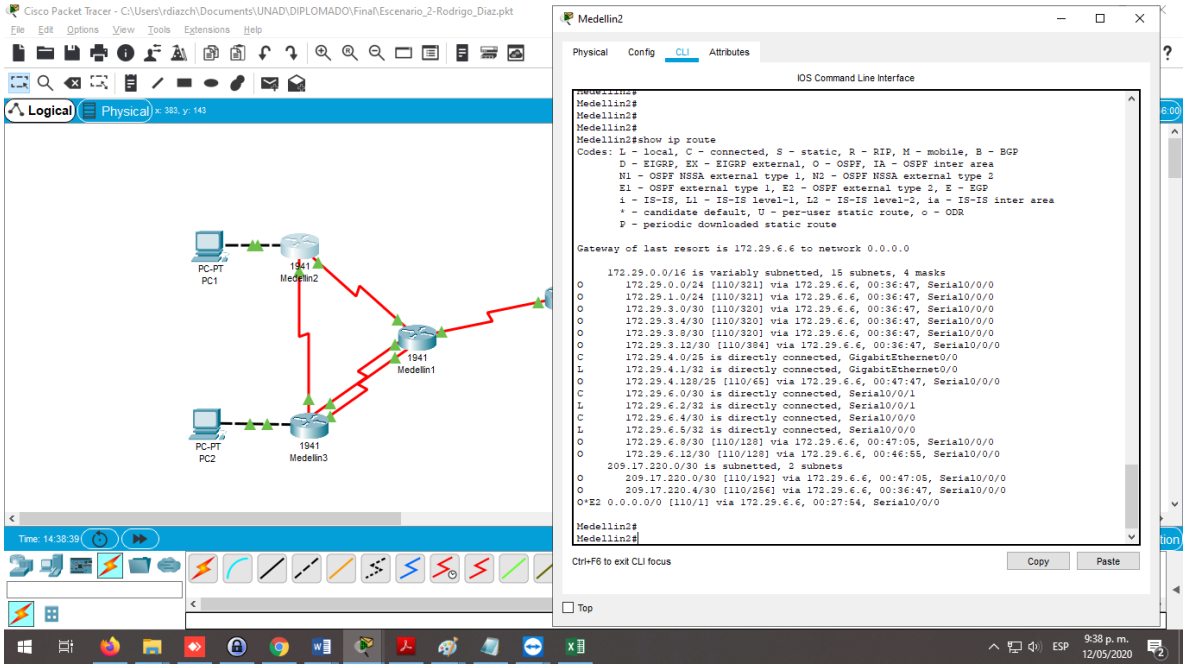


*Ilustración 26 show ip route en Medellin2*

## Router Medellin3

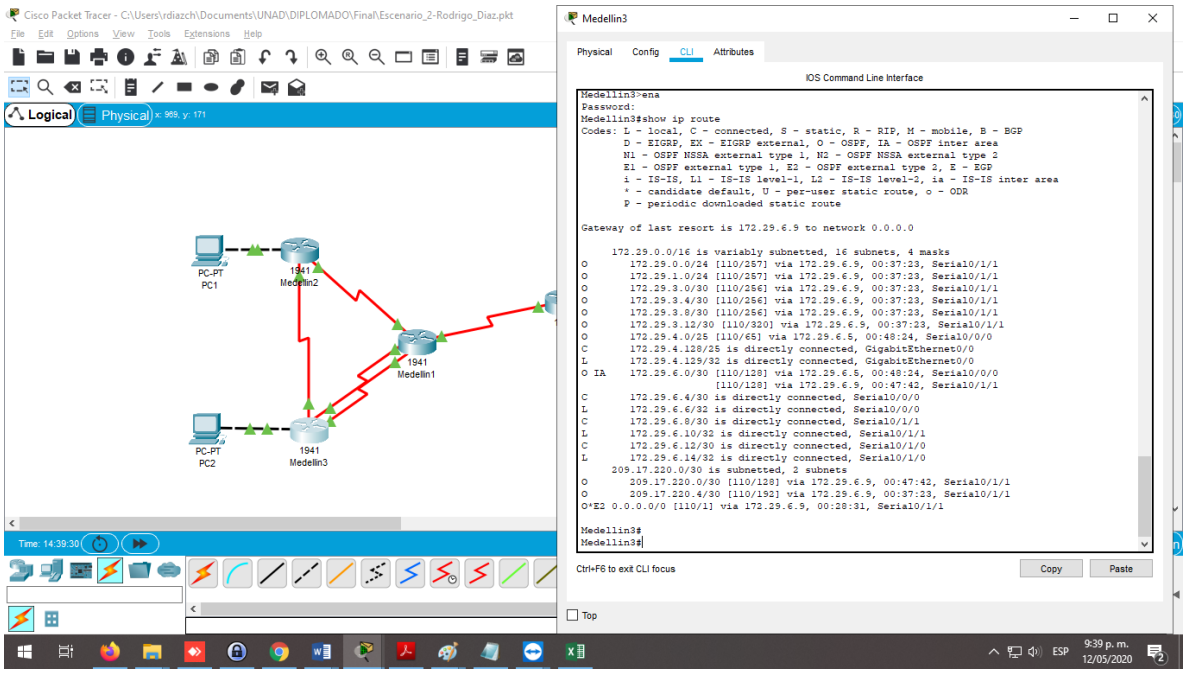


*Ilustración 27 show ip route en Medellin3*

## Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

*Tabla 6 Deshabilitar OSPF*

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

```
Bogota1>ena
Password:
Bogota1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#router ospf 1
Bogota1(config-router)#passive-interface s0/0/0
Bogota1(config-router)#
15:49:06: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

Bogota2>ena
Password:
Bogota2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router ospf 1
Bogota2(config-router)#passive-interface s0/1/0
Bogota2(config-router)#passive-interface g0/0
Bogota2(config-router)#exit

Bogota3>ena
Password:
Bogota3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#router ospf 1
Bogota3(config-router)#passive-interface g0/0
Bogota3(config-router)#exit



Medellin1>ena
Password:
Medellin1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface s0/0/0
Medellin1(config-router)#
15:52:57: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached

Medellin2>ena
Password:
Medellin2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Medellin2(config)#router ospf 1
Medellin2(config-router)#passive-interface g0/0
Medellin2(config-router)#exit

Medellin3>ena
Password:
Medellin3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#router ospf 1
Medellin3(config-router)#passive-interface s0/0/1
Medellin3(config-router)#passive-interface g0/0
Medellin3(config-router)#exit
```

**Parte 4: Verificación del protocolo OSPF.**

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 OSPF y las interfaces que participan de la publicación entre otros datos.

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

**Router Bogota1**

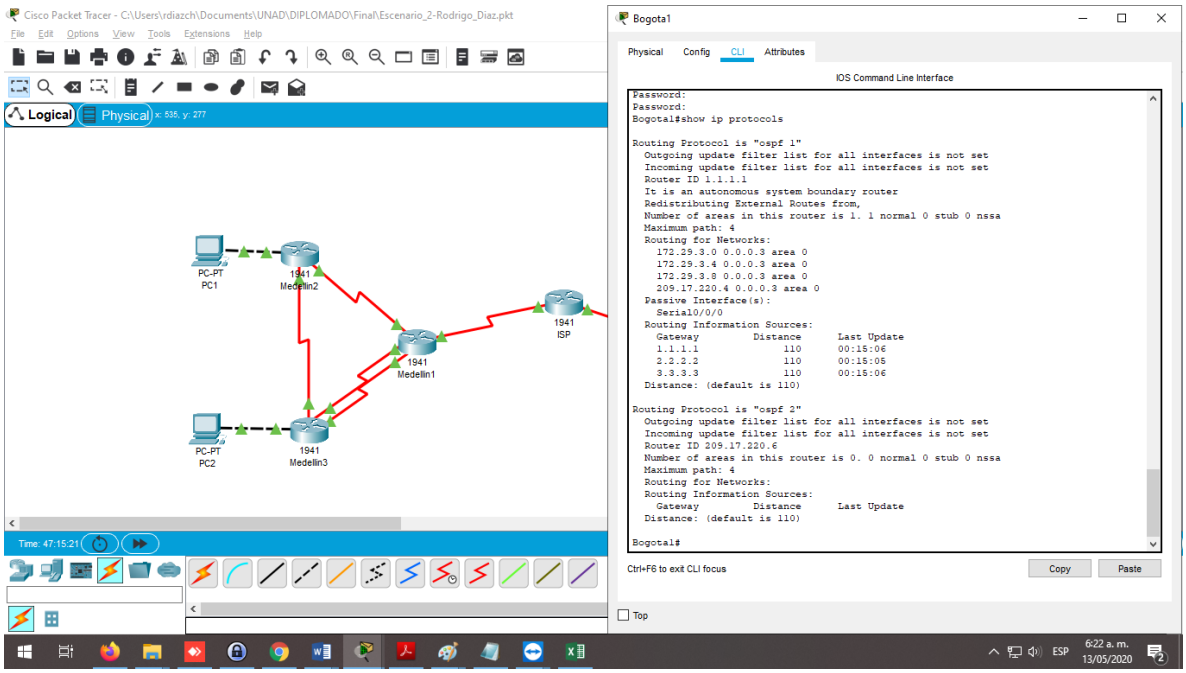


*Ilustración 28 show ip protocols en Bogota1*

## Router Bogota2

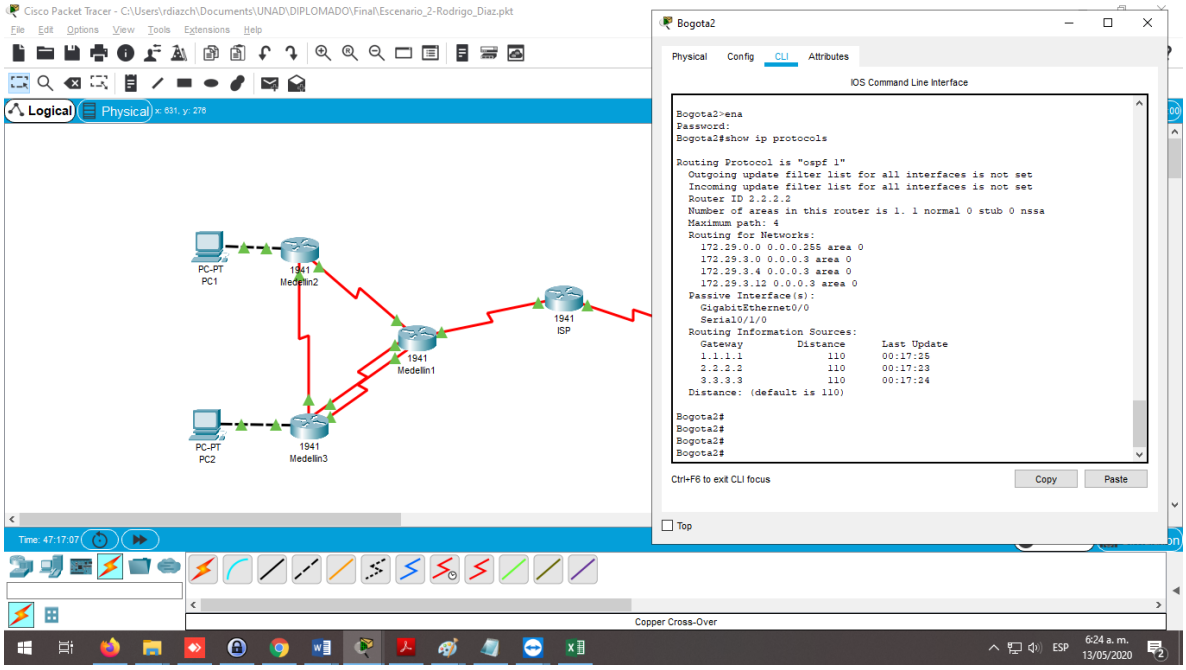


*Ilustración 29 show ip protocols en Bogota2*

## Router Bogota3

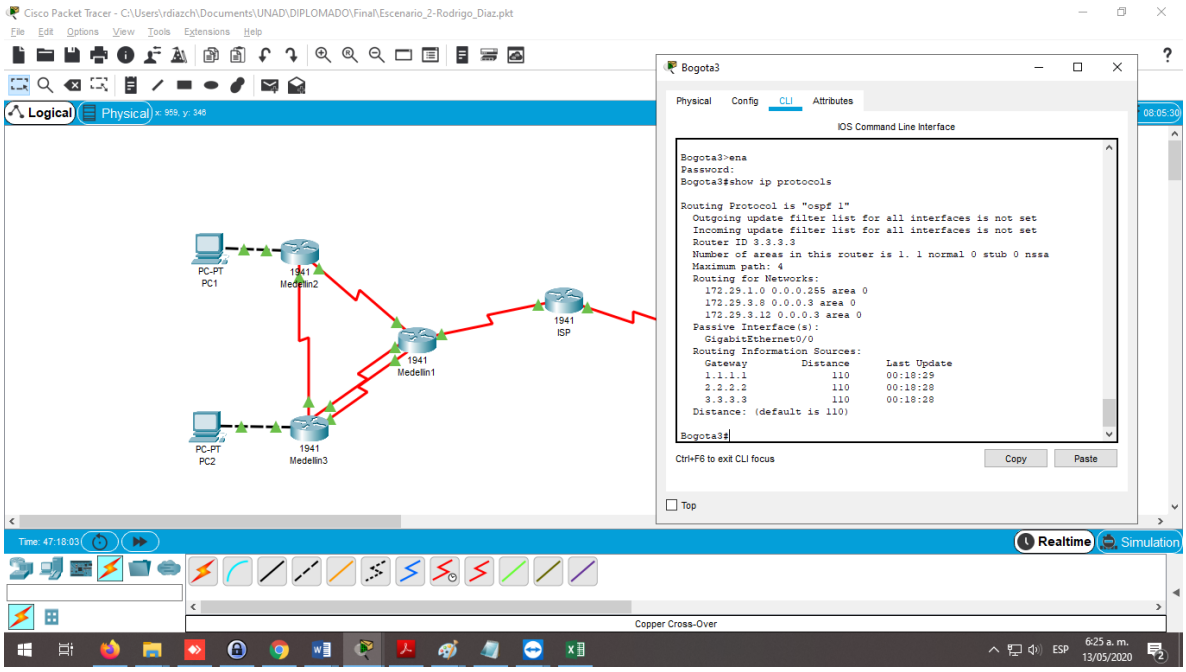


*Ilustración 30 show ip protocols en Bogota3*

## Router Medellin1

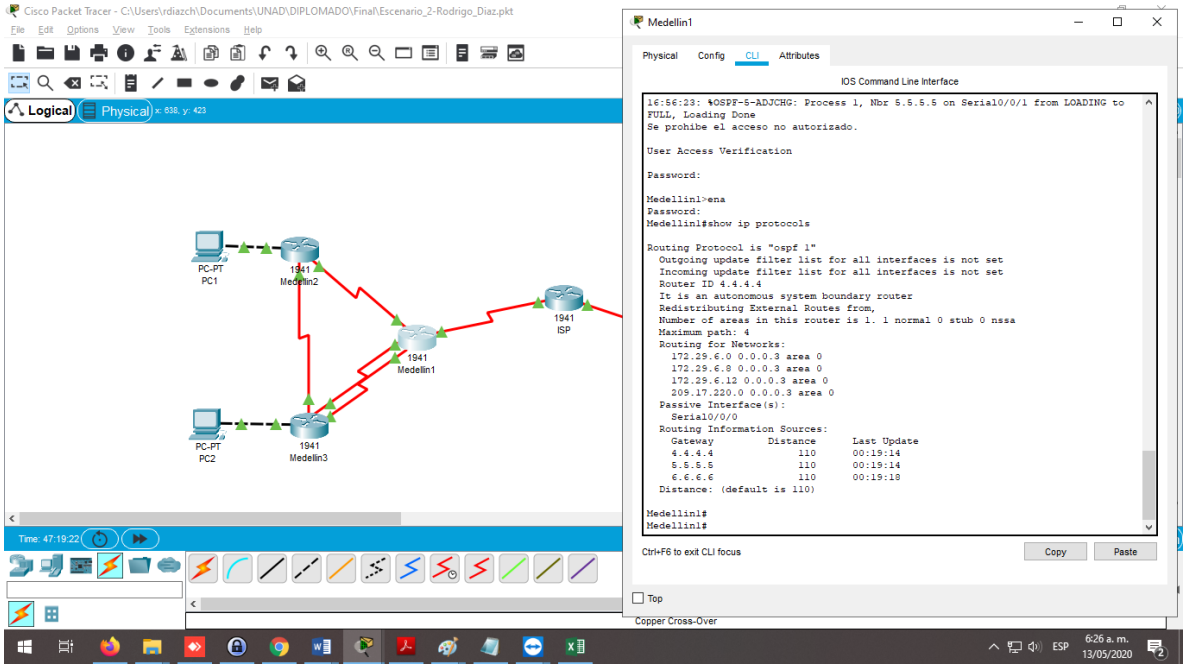


*Ilustración 31 show ip protocols en Medellin1*

## Router Medellin2

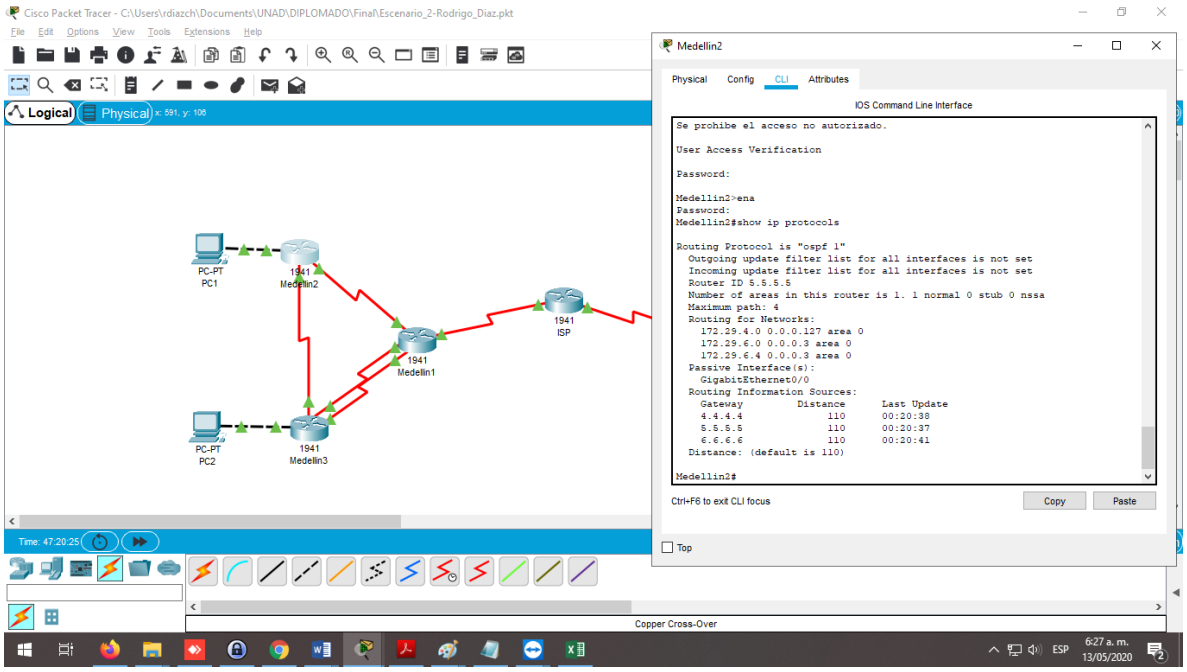


*Ilustración 32 show ip protocols en Medellin2*

## Router Medellin3

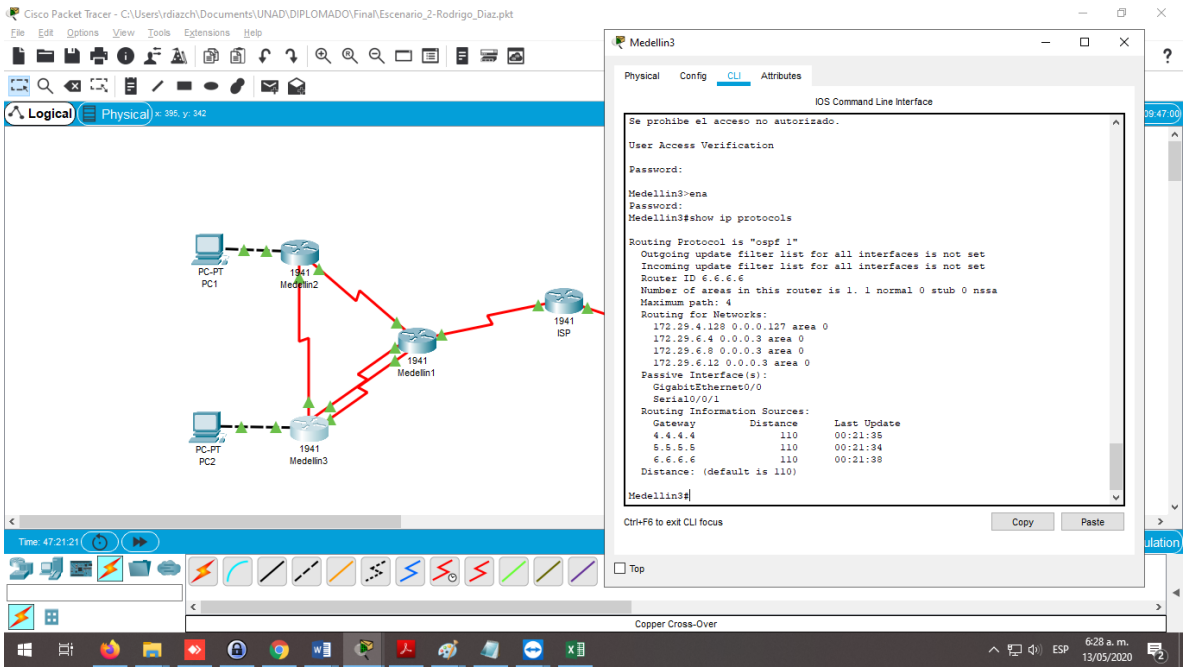


*Ilustración 33 show ip protocols en Medellin3*

**Router ISP**

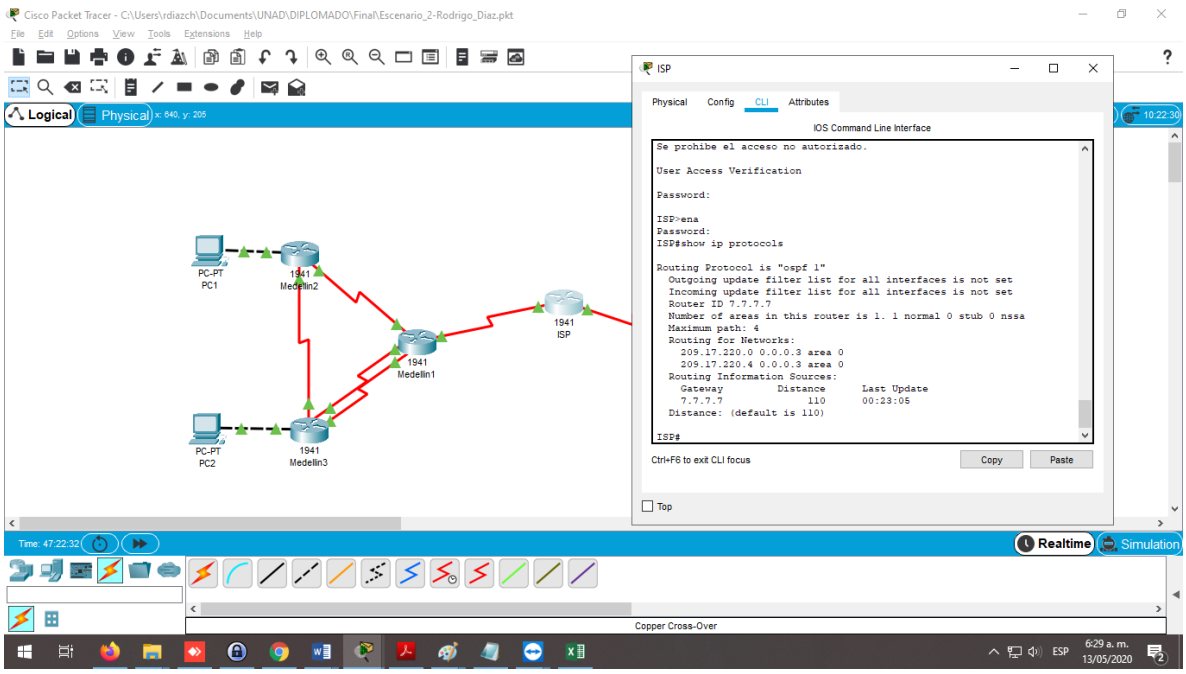


*Ilustración 34 show ip protocols en ISP*

**Parte 5: Configurar encapsulamiento y autenticación PPP.**

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

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

Medellin1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#interface Serial 0/0/0
Medellin1(config-if)#encapsulation ppp
Medellin1(config-if)#%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#username ISP secret cisco
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username MEDELLIN password cisco

```
Medellin1(config-if)#exit

Bogota1>ena
Password:
Bogota1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#interface Serial 0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#username ISP secret cisco
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#exit

ISP>ena
Password:
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface Serial0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#interface Serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to down
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/0/0
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
ISP(config)#
```

**Parte 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 0/0/0 del router Medellín1, cómo diferente puerto.

```
Se prohibe el acceso no autorizado.
User Access Verification
Password:
Medellin1>ena
Password:
Medellin1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin1(config)#ip access-list standard HOST
Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
Medellin1(config-std-nacl)#exit
Medellin1(config)#ip nat inside source list HOST interface s0/1/1 overload
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#exit
Medellin1(config)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#int s0/1/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Medellin1#show ip nat translation
Medellin1#
```

**Ping Medellin1 a Medellin2 y Medellin3**

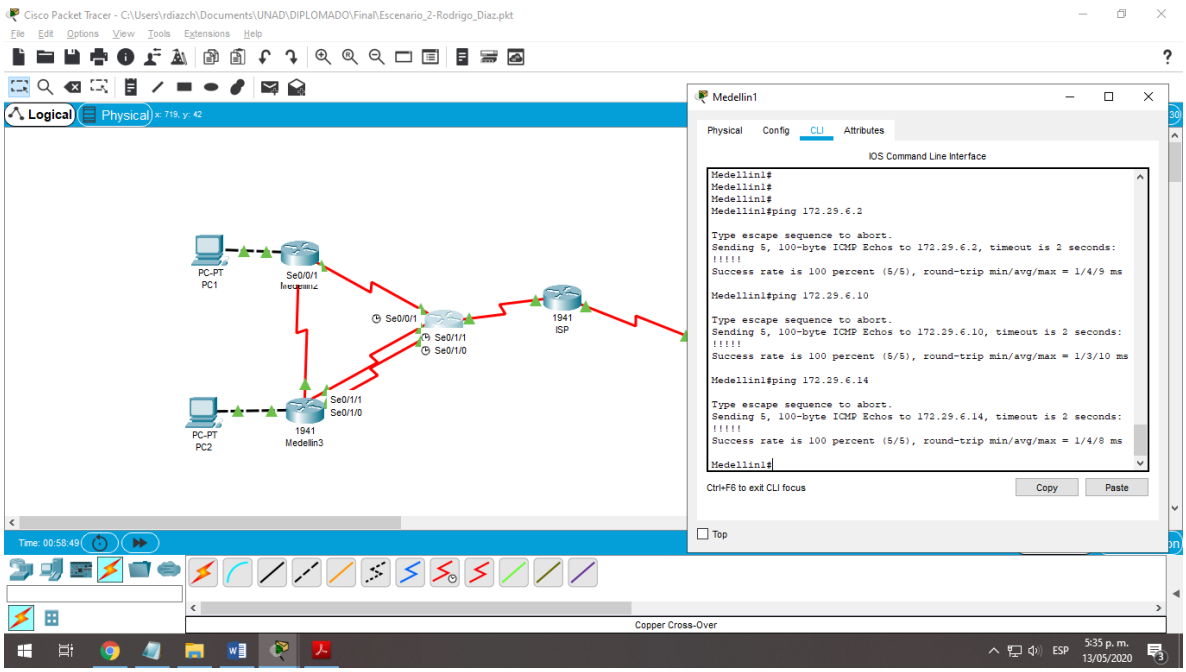


*Ilustración 35 Ping Sede Medellin*

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 prohibe el acceso no autorizado.
User Access Verification
Password:
Bogota1>ena
Password:
Bogota1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#ip access-list standard HOST
Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
Bogota1(config-std-nacl)#exit
Bogota1(config)#ip nat inside source list HOST interface s0/0/0 overload
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#int s0/0/1

```
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#exit
Bogota1#
%SYS-5-CONFIG_I: Configured from console by console
Bogota1#show ip nat translation
```

**Ping Router Bogota2 y Bogota 3**

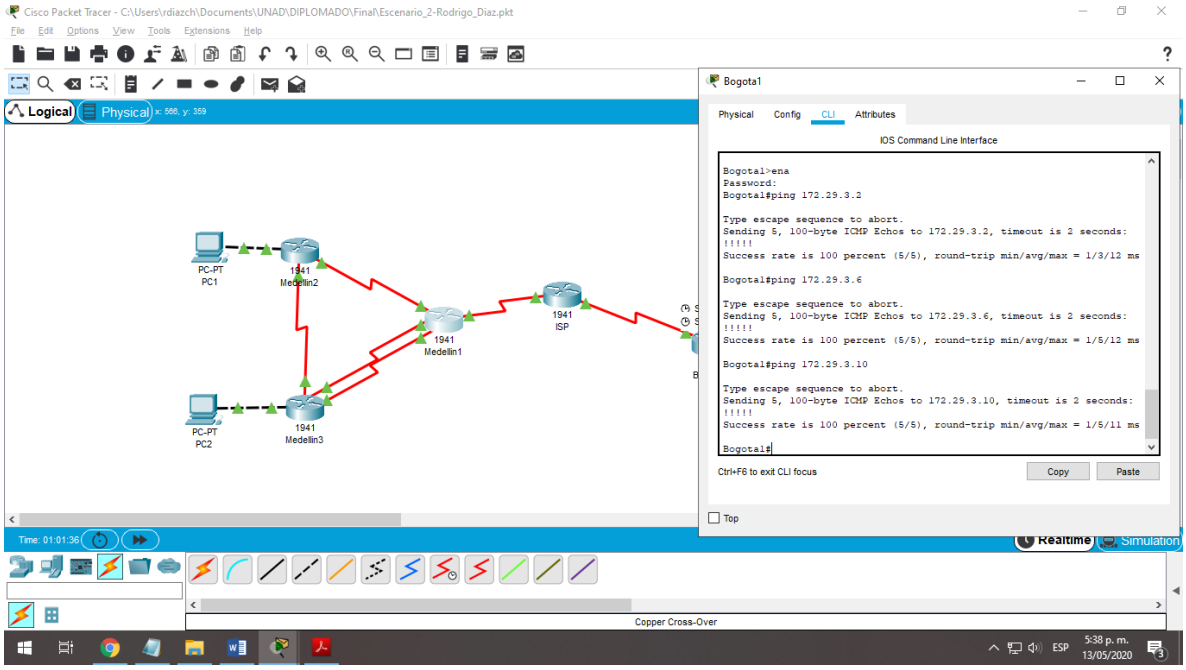


*Ilustración 36 Ping Sede Bogota*

**Parte 7: Configuración del servicio DHCP**

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

```
Se prohibe el acceso no autorizado.
User Access Verification
Password:
Medellin2>ena
Password:
Medellin2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Medellin2(config)#ip dhcp excluded-address 172.29.4.1
Medellin2(config)#ip dhcp pool MEDELLIN2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.1
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp excluded-address 172.29.4.129
Medellin2(config)#ip dhcp pool MEDELLIN3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
```

Es necesario crear una ruta en Medellin3 para que las peticiones de los clientes DHCP puedan llegar al router Medellin2, esto lo hacemos con el comando “ip-helper”:

```
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#exit
```

## Peticion DHCP para el PC1

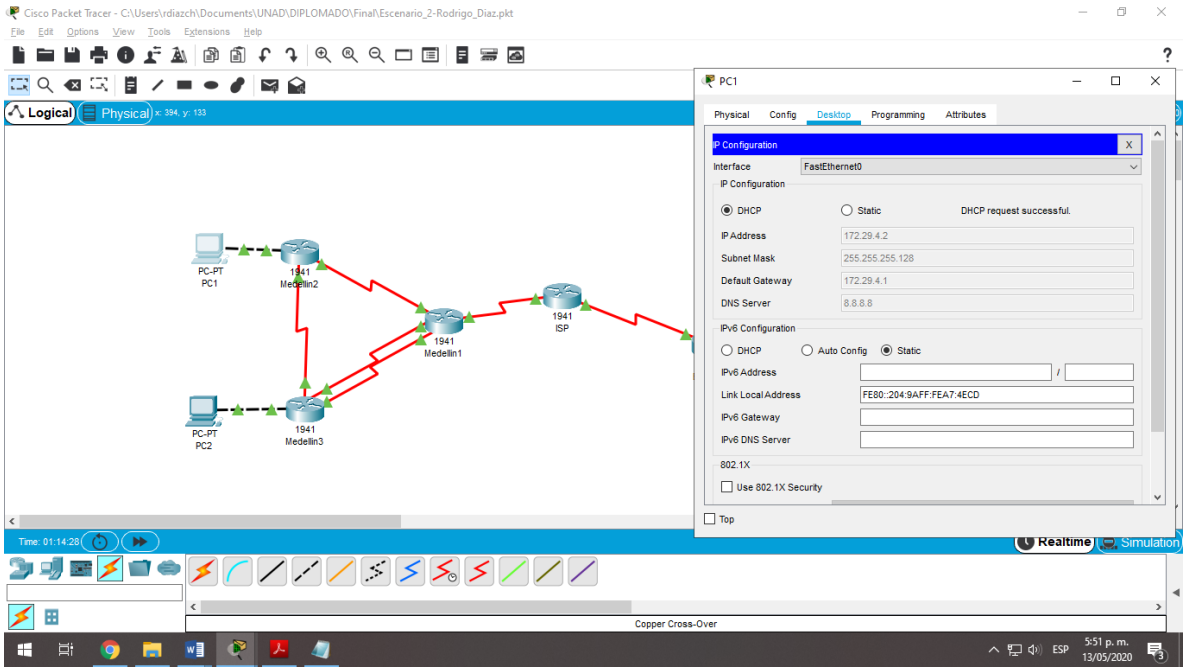


*Ilustración 37 Peticion DHCP en PC1*

## Peticion DHCP para el PC2

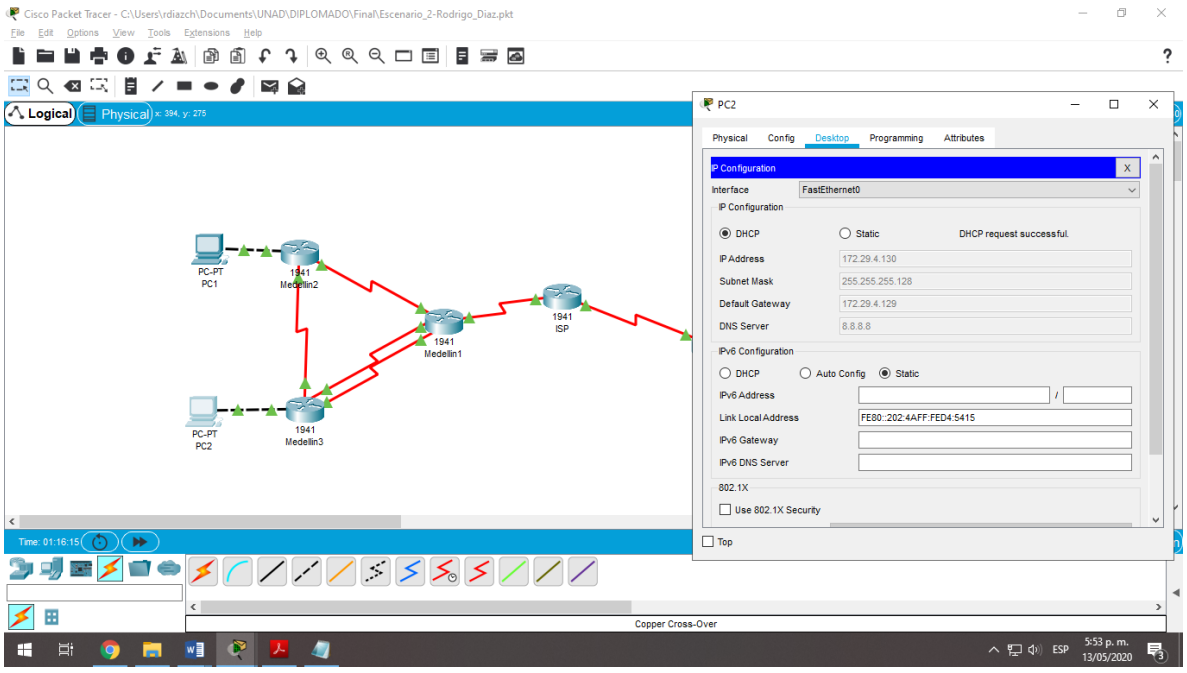


*Ilustración 38 Peticion DHCP en PC2*

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
Bogota2(config)#ip dhcp excluded-address 172.29.0.1
Bogota2(config)#ip dhcp pool BOGOTA2
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
Bogota2(config)#ip dhcp excluded-address 172.29.1.1
Bogota2(config)#ip dhcp pool BOGOTA3
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
```

Para este caso también debemos apoyarnos del comando “ip-helper” para que las peticiones DHCP que lleguen al router Bogota3 sigan su ruta hacia Bogota2 que es el servidor DHCP:

```
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config-if)#exit
```

## Peticion DHCP para el PC3

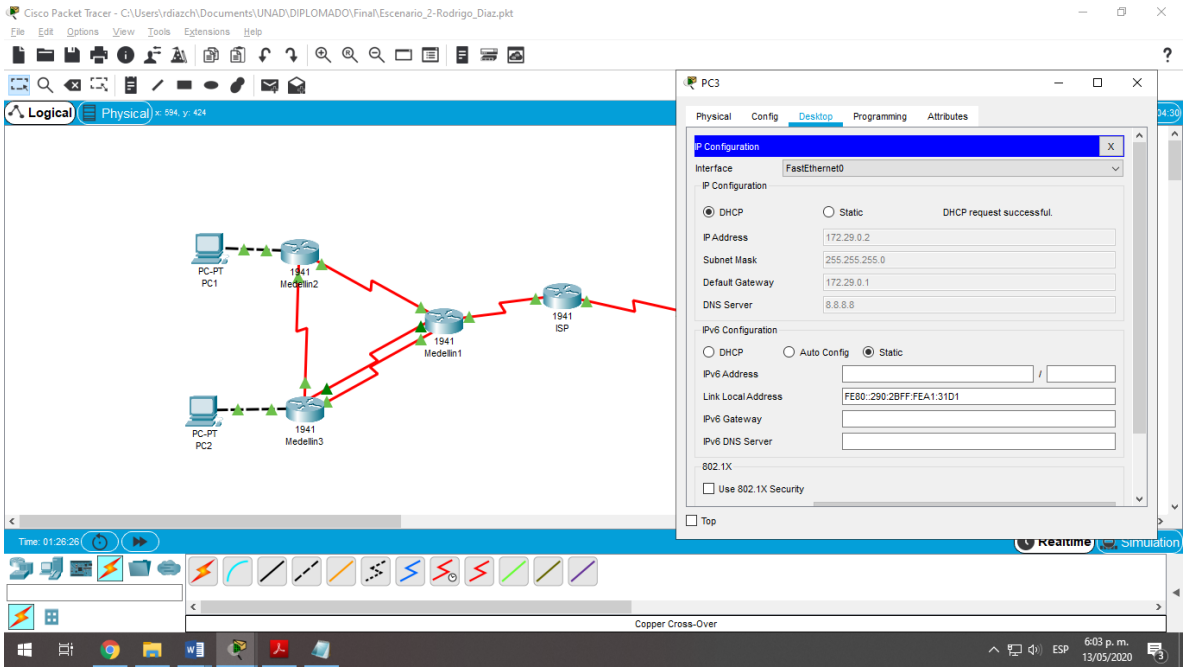


*Ilustración 39 Peticion DHCP en PC3*

## Peticion DHCP para el PC4

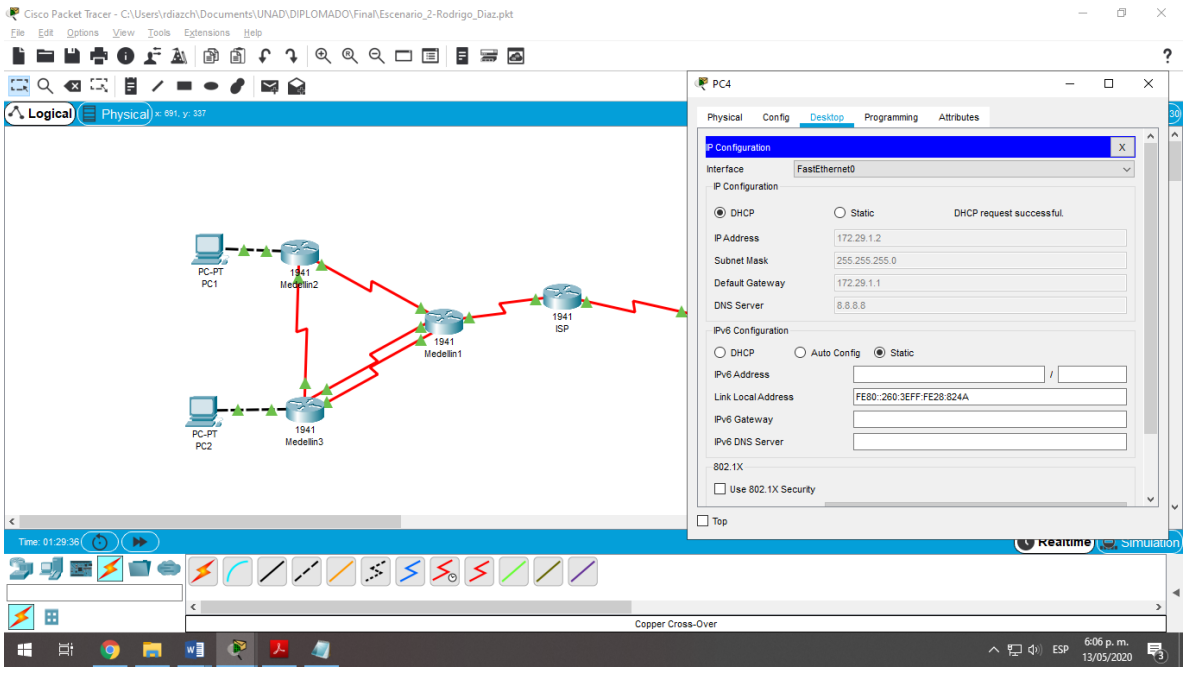


*Ilustración 40 Peticion DHCP en PC4*

## CONCLUSIONES

Con el escenario 1 pudimos aprender a parametrizar los Switch administrables para asignarlos a diferentes VLANs y desactivar los que no se requieren, también se establecieron los privilegios para ejecución de comandos en los dispositivos de red y se realizaron todas las pruebas de conectividad para corroborar la funcionalidad adecuada de los hosts.

En el segundo escenario pudimos establecer la conexión entre las dos sedes partiendo de los direccionamientos adecuados, aunque también se usaron configuraciones parecidas al primer escenario, se tuvieron q aplicar mecanismos como NAT para lograr establecer dicha comunicación entre sedes, algo que se aplica también en los tuneles VPN que actualmente son lo mas usado en las organizaciones por los niveles de seguridad que proporcionan.

## REFERENCIAS BIBLIOGRAFICAS


CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC