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

PASO 11 - PRUEBA DE HABILIDADES PRÁCTICAS CCNA
TRABAJO FINAL

PRESENTADO POR:
MICHAEL SMITH SANDOVAL

TUTOR:
GERARDO GRANADOS ACUÑA
GRUPO_203092_28

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS DE LA TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
CEAD – MEDELLIN

2019

TABLA DE CONTENIDO

Pág.

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:

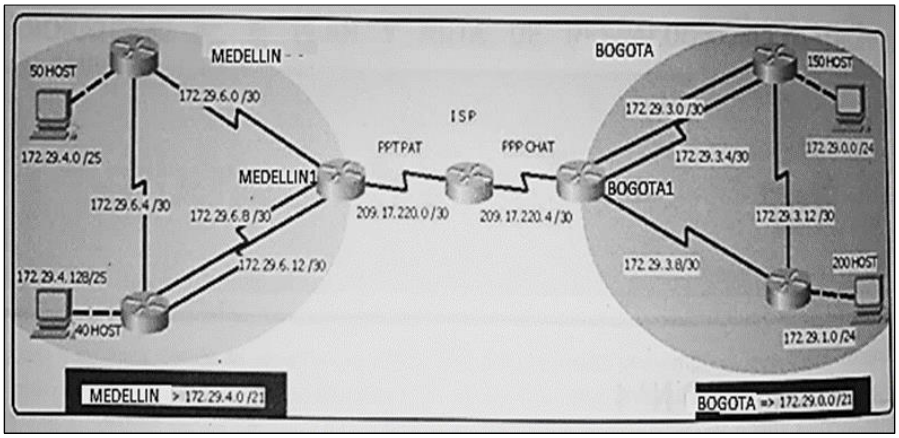
- Plantear y desarrollar de forma efectiva los dos escenarios propuestos en la actividad
- Investigar e implementar PAT en CISCO
- Investigar mas a fondo los temas manejados en el desarrollo de la actividad
- Aplicar todos los conocimientos adquiridos en el proceso del diplomado
- Implementar herramienta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

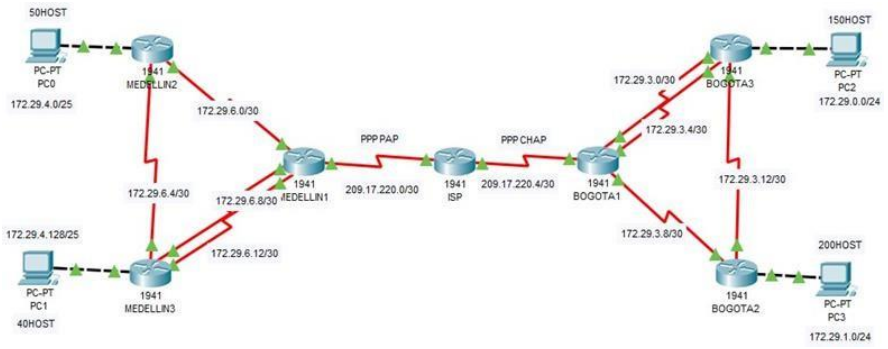


Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.
Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada 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 fisica de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.



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, configuracion 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 sumarizan las subredes de cada uno a /22.

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

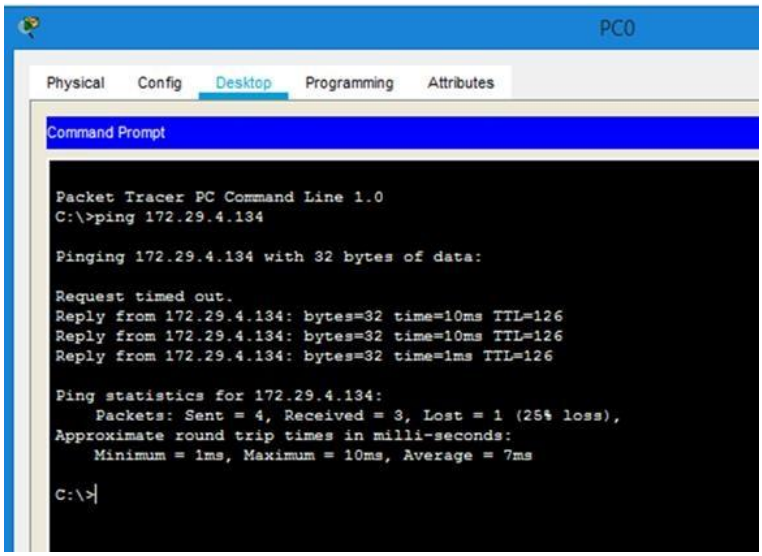
#Ip route 172.29.4.0 255.255.252.0 209.17.220.2
#Ip route 172.29.0.0 255.255.252.0 209.17.220.6

2. **Tabla de Enrutamiento**.

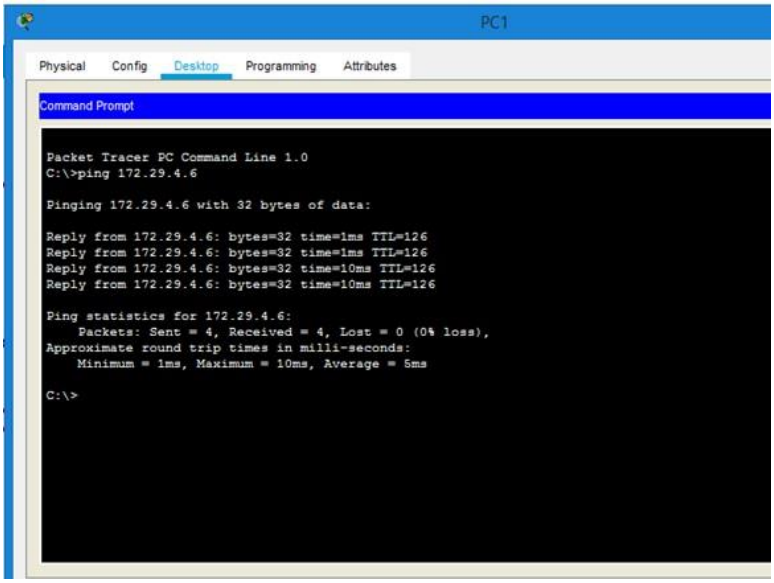
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Pruebas de conectividad (mediante PING)

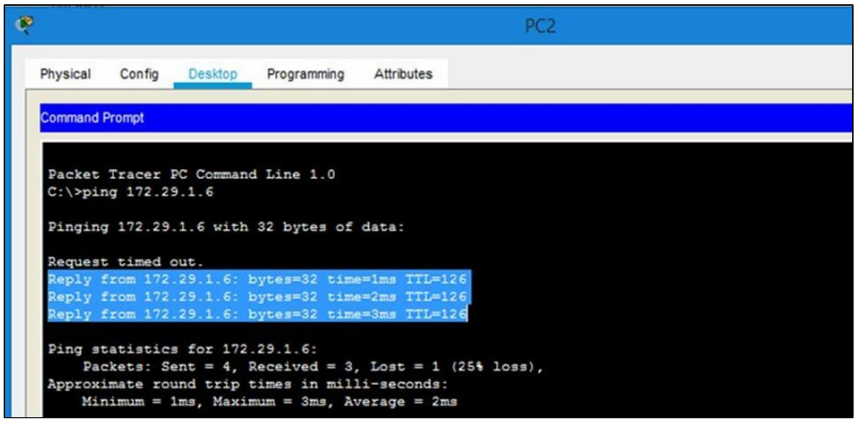
Ping de PC0 a PC1



Ping de PC1 a PC0



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.

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

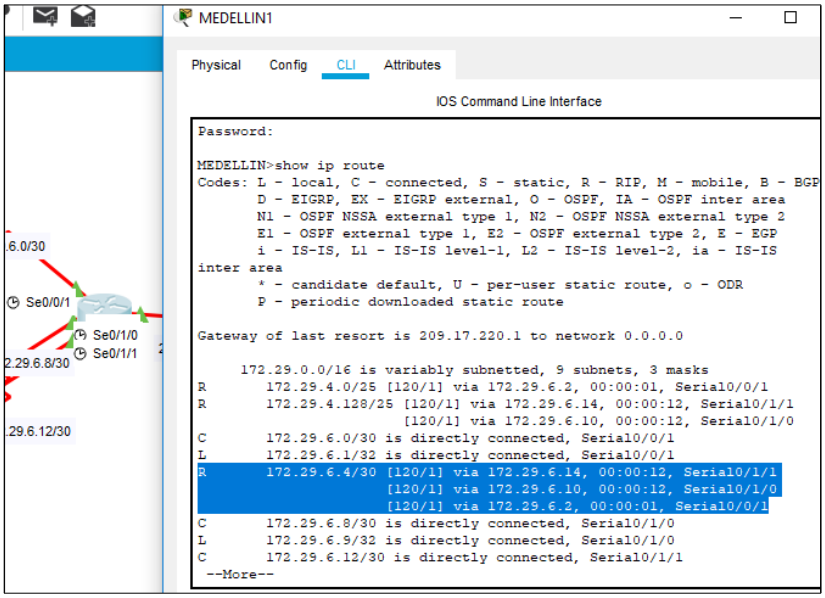
La Deshabilitacion de la propagación del protocolo RIP ya se realizó en el punto anterior gracias al comando Passive-interface aplicado en la interfaz que señala este enunciado.

4. Verificación del protocolo RIP.

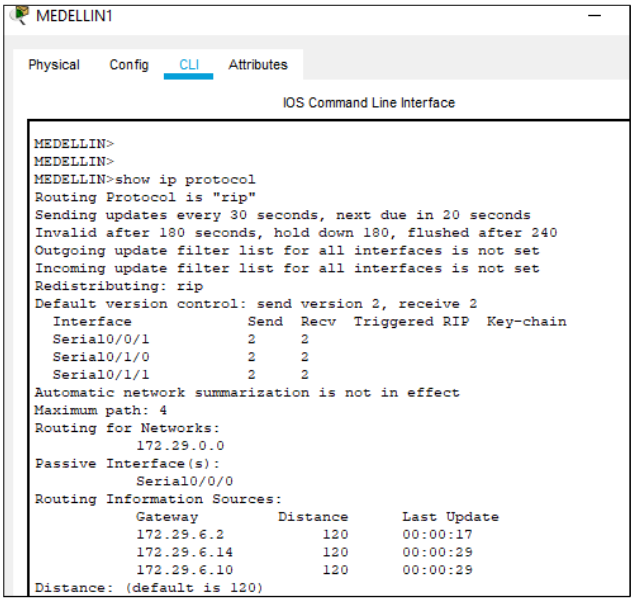
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos.

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:



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.



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

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

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:

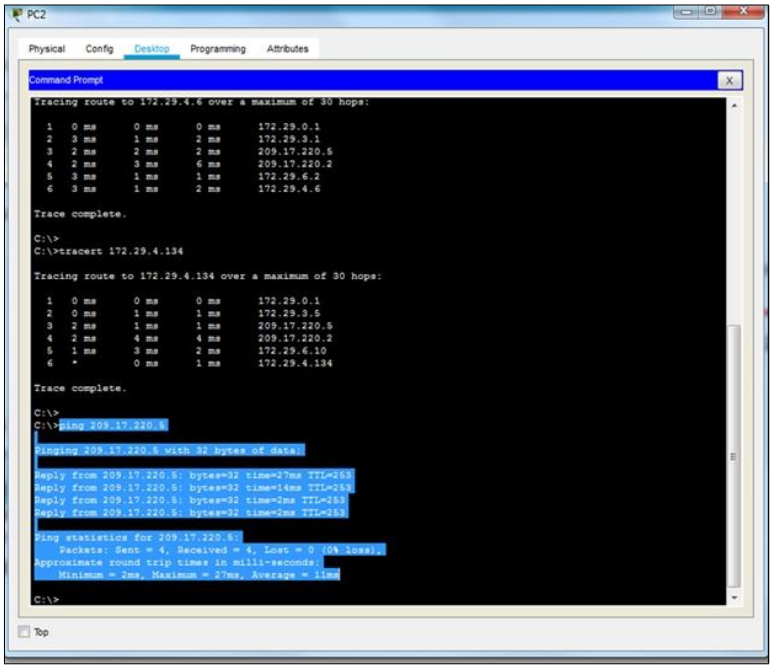
NAT en MEDELLIN1

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 s0/01
Ip nat inside
Int s0/1/0
Ip nat inside
Int s0/1/1
Ip nat inside

NAT en BOGOTA1

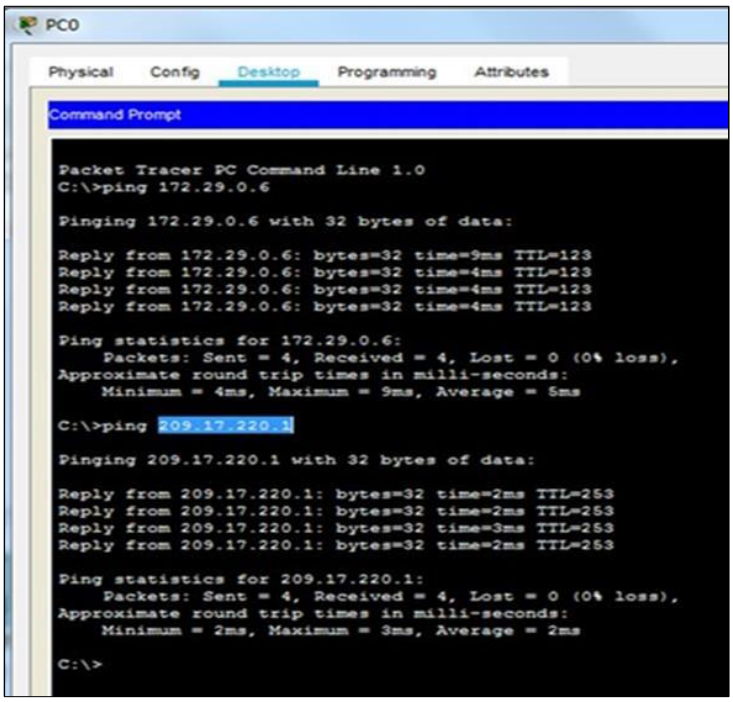
Configure terminal
Ip nat inside source list 1 interface s0/0/0 overload
Access-list 1 permit 172.29.0.0 0.0.3.255
Int s0/0/0
Ip nat outside
Int s0/0/1
Ip nat inside
Int s0/1/0
Ip nat inside
Int s0/1/1
Ip nat inside

Ping PC2 a ISP



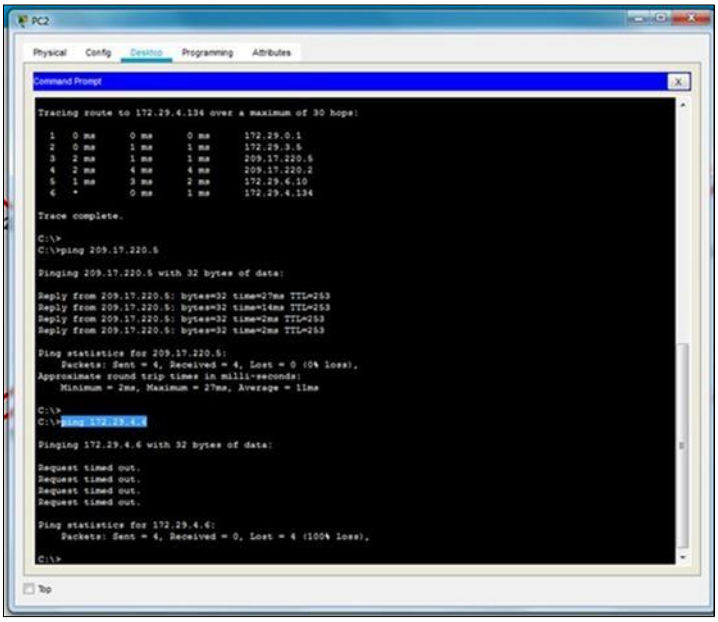
Ping satisfactorio

Ping PC0 a ISP



Ping satisfactorio

Ping de PC2 a PC0



Ping fallido, porque NAT lo bloquea.

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

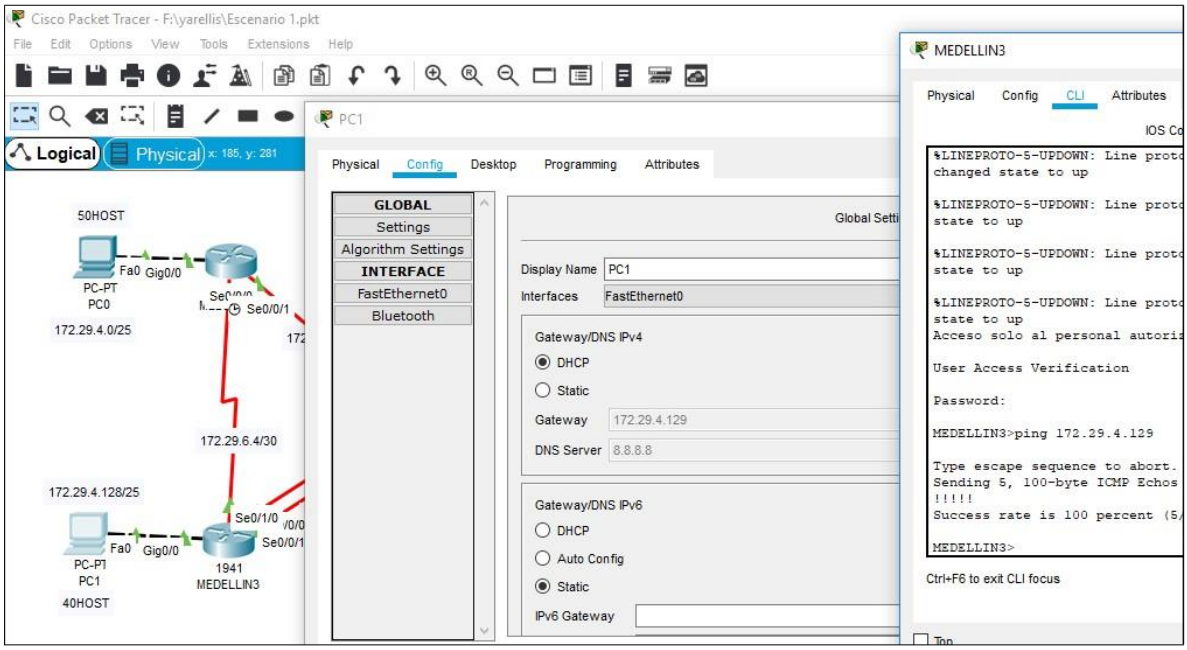
Ip dhcp excluded-address 172.29.1.1 172.29.1.5
Ip dhcp excluded-address 172.29.0.1 172.29.0.5
Ip dhcp pool BOG2
Network 172.29.1.0 255.255.255.0
Default-router 172.29.1.1
Dns-server 8.8.8.8
Ip dhcp pool BOG3
Network 172.29.0.0 255.255.255.0
Default-router 172.29.0.1
Default-router 172.29.0.1

Configuración DHCP EN BOGOTA3

Configure terminal
Interface g0/0
Ip helper-address 172.29.3.13

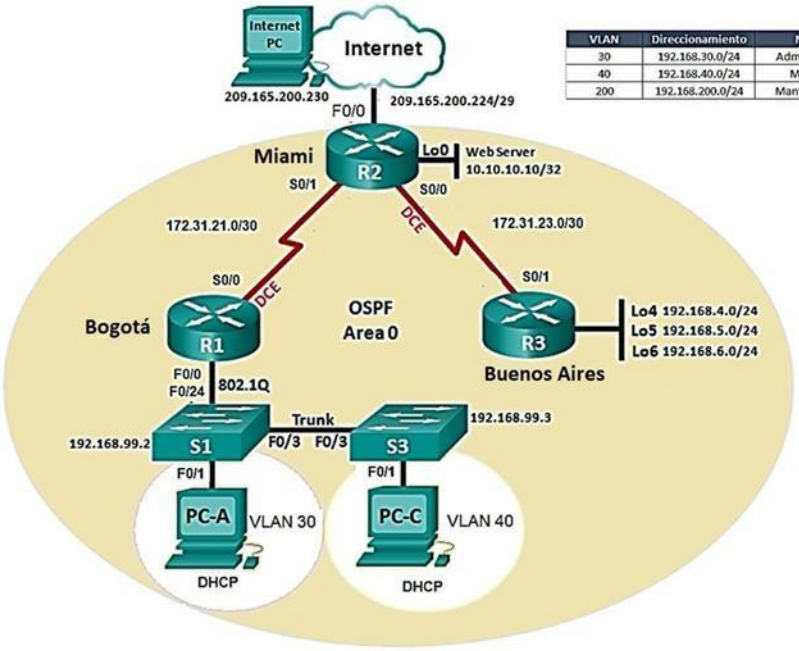
Verificación del servicio DHCP en funcionamiento en la red por PING.

Verificación del servicio DHCP en funcionamiento en PC1, gracias al servicio de DCHP en el router MEDELLIN3, le asigno la ip 172.29.4.129 al equipo PC1, el cual se verifica total acceso al equipo por medio de un ping fue exitoso.


Cisco Packet Tracer - F:\yarellis\Escenario 1.pkt
File Edit Options View Tools Extensions Help
Logical
Physical
50HOST
PC-PT
PC0
Fa0
Gig0/0
Se0/0/1
172.29.4.0/25
172.29.6.4/30
172.29.4.128/25
Se0/1/0
Se0/0/1
PC-PT
PC1
40HOST
1941
MEDELLIN3
PC1
Physical Config Desktop Programming Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Display Name PC1
Interfaces FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Gateway 172.29.4.129
DNS Server 8.8.8.8
Gateway/DNS IPv6
DHCP
Auto Config
Static
IPv6 Gateway
MEDELLIN3
Physical Config CLI Attributes
%LINEPROTO-5-UPDOWN: Line proto
changed state to up
%LINEPROTO-5-UPDOWN: Line proto
state to up
%LINEPROTO-5-UPDOWN: Line proto
state to up
%LINEPROTO-5-UPDOWN: Line proto
state to up
Acceso solo al personal autori
User Access Verification
Password:
MEDELLIN3>ping 172.29.4.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos
!!!!!
Success rate is 100 percent (5
MEDELLIN3>
Ctrl+F6 to exit CLI focus

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.



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

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

R1

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

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

R3

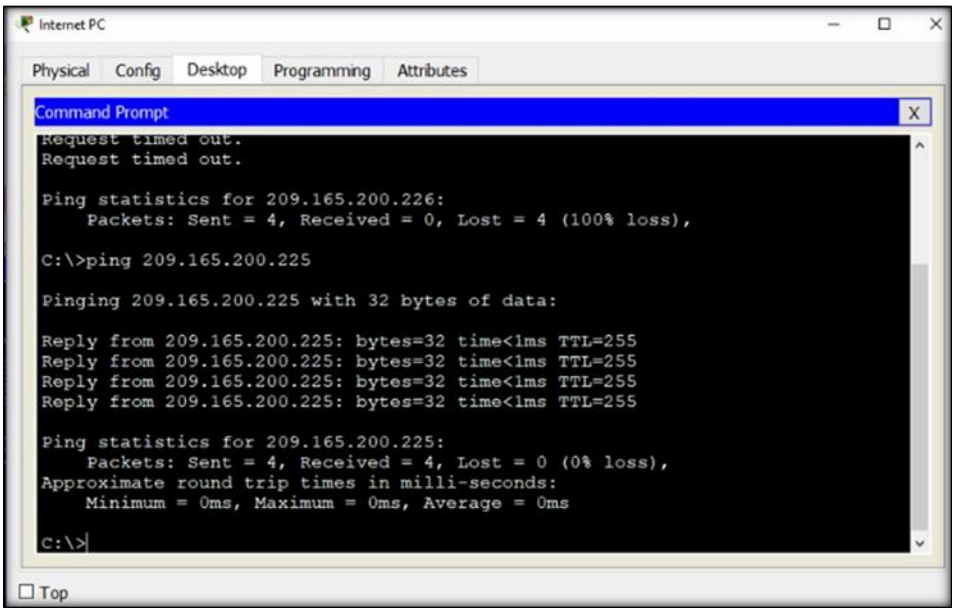
#hostname R3 #interface serial 0/0/0
#ip address 172.31.23.2 255.255.255.252
#clock rate 12800 Unknown clock rate #no shut
#no shutdown #interface loopback 4
#ip address 192.168.4.1 255.255.255.0
#no shutdown
interface loopback 5
#ip address 192.168.5.1 255.255.255.0
#no shutdown
interface loopback 6
#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

R3

```
R3#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 1/4/18 ms

R3#
```



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

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.

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

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
5.5.5.5           0   FULL/  -        00:00:34    172.31.21.2
Serial0/0/0
R1#
```

```
#bandwidth 256
#ip ospf cot 9500
```

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

```
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 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 5 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x00da9e
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
8.8.8.8           0   FULL/  -        00:00:38    172.31.23.2
Serial0/0/0
1.1.1.1           0   FULL/  -        00:00:31    172.31.21.1
Serial0/0/1
R2#
```

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

```
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 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 4
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x008f2e
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
5.5.5.5           0   FULL/  -        00:00:39    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.

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

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

S3

#hostname S3
#vlan 30
#name Administracion
#vlan 40
#name Mercadeo
#vlan 200
#name Mantenimiento
#in
#interface vlan 99
#ip ad
% Incomplete command.
#ip ad
#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
5. Asignar direcciones IP a los Switches acorde a los lineamientos.
6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

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.

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

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

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

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

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

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.

R1

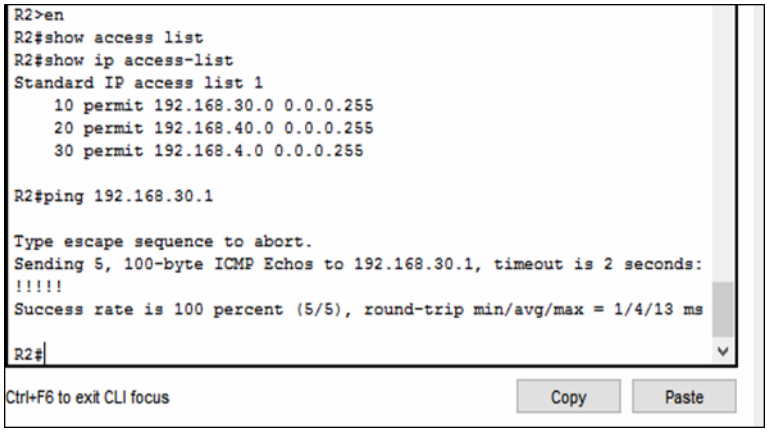
#access-list 1 permit 192.168.30.0 0.0.0.255
#access-list 1 permit 192.168.40.0 0.0.0.255
#access-list 1 permit 192.168.4.0 0.0.0.255
#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

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.

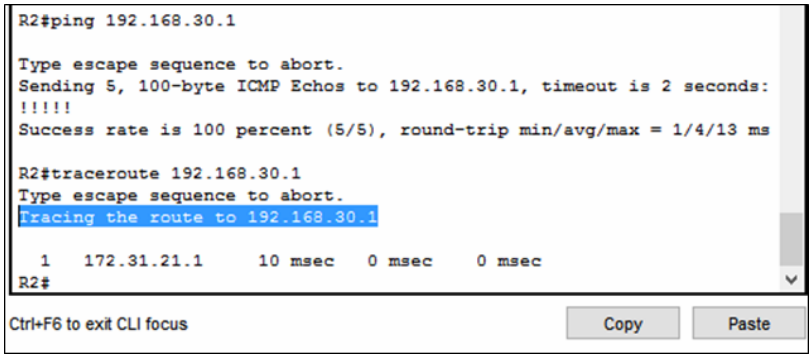
#ip nat inside source list 1 pool INTERNET

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

Ping R2 a R1



Traceroute R2 a R1



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, P. (18 de Agosto de 2010). *http://www.redescisco.net*. Obtenido de http://www.redescisco.net/sitio/2010/08/18/implementando-nat-en-routers-cisco/

COLOMES, P. (30 de Agosto de 2013). *https://es.slideshare.net*. Obtenido de https://es.slideshare.net/pcolomes/implementacin-de-natpat-en-routers-cisco

CRIS. (12 de JUNIO de 2019). *https://support.cloudflare.com*. Obtenido de https://support.cloudflare.com/hc/es-es/articles/200169336--C%C3%B3mo-puedo-ejecutar-un-traceroute-

DI TOMMASO, L. (6 de JUNIO de 2010). *https://www.mikroways.net*. Obtenido de https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/

DUARTE, E. (18 de JUNIO de 2014). *http://blog.capacityacademy.com*. Obtenido de http://blog.capacityacademy.com/2014/06/18/cisco-ccna-como-configurar-nat-overload-en-cisco-router/

https://todopacketracer.com. (18 de 10 de 2011). Obtenido de Configuración de VLANs: https://todopacketracer.com/2011/10/18/configuracion-de-vlans/

Microsoft Windows Server. (30 de NOVIEMBRE de 2018). *https://support.microsoft.com*. Obtenido de https://support.microsoft.com/es-co/help/314868/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows

OSPF DESIGN GUIDE. (10 de Agosto de 2005). *https://www.cisco.com*. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

UNAD. (2014). *https://cisco.com*. Obtenido de Principios de Enrutamiento [OVA]: https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD. (5 de Junio de 2014). *https://cisco.com*. Obtenido de Configuración de Switches y Router [OVA]: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD. (2014). *https://www.cisco.com*. Obtenido de PING y TRACER como estrategia en procesos de Networking [OVA]: https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

WALTON, A. (2019). *https://ccnadesdecero.es*. Obtenido de https://ccnadesdecero.es/configuracion-pat-nat-sobrecarga/