PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JAIME ALFONSO OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JAIME ALFONSO OROZCO

Trabajo de la opción de grado para optar al título de Ingeniero de Sistemas

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES
Docente Ocasional

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
VALLEDUPAR, CESAR
2020

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE GRAFICAS

RESUMEN

La práctica se desarrolla en torno a dos escenarios, el primero a través de la configuración de una red pequeña aborda las temáticas de conectividad IPv4 e IPv6, se aplican los protocolos de: Seguridad de switches, routing entre VLAN, dinámico RIPv2, 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. El segundo escenario por intermedio de la configuración de una red distribuida en diferentes Ciudades permite la administracion de la red, configuración basica de parametros de los dispositivos, encapsulamiento y autenticación PPP, implementacion de protocolo OSPF, Configuración de PAP y Configuración de DHCP.

ABSTRACT

The practice is developed around two scenarios, the first through the configuration of a small network addresses the topics of IPv4 and IPv6 connectivity, the protocols of: Switch security, routing between VLANs, dynamic RIPv2, host configuration are controlled Dynamic (DHCP, Dynamic and Static Network Address Translation (NAT), Access Control Lists (ACL), and Server / Client Network Time Protocol (NTP). The second scenario through network configuration Distribution in different cities allows network administration, basic configuration of device parameters, PPP encapsulation and authentication, OSPF protocol implementation, PAP configuration and DHCP configuration.

GLOSARIO

DHCP: Protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor.

DNS: (Domain name system, sistema de nombre de dominio) Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio.

NAT: (Network address translation, traducción de direcciones de red) Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red**.**

PING: Comando utilizado para comprobar si una determinada interfaz de red, se encuentra activa.

RIP: (Routing Information Protocol, protocolo de información de enrutamiento) Un protocolo de puerta de enlace interno que enruta paquetes IPv4 y mantiene la tabla de enrutamiento de todos los hosts en la LAN.

Router: Es un dispositivo que administra el tráfico de datos que circula en una red de computadoras.

Switch: Es un dispositivo que permite la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

Tabla de enrutamiento: Tabla que contiene la información de enrutamiento para un paquete, que ayuda a determinar la mejor ruta de acceso para que el paquete llegue a destino.

Topología de red: Es el mapa físico o lógico de una red para intercambiar datos.

VLAN: (virtual local area network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

WLAN: siglas inglesas de Wireless Local Área Network, que es español significa Red de Área Local Inalámbrica.

INTRODUCCION

Mediante el desarrollo del presente trabajo se busca llevar a la práctica los conocimientos adquiridos durante el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), apoyado en la herramienta de Simulación PACKET TRACER.

Integrando los conocimientos y la práctica a través de la configuración de los dispositivos que conforman una topología de red, realizando el alistamiento, las configuraciones básicas y de seguridad, conexiones físicas entre equipos según los requerimientos de la red, implementando los protocolos de enrutamiento, encapsulamiento, listas de control ACL, routing entre VLAN, DHCP, direccionamiento dinámico y estático.

Con la certeza que el presente trabajo profundizará la experiencia como profesionales de Sistemas en un mundo en el que la Tecnología avanza a grandes pasos y el requerimiento de Seguridad en redes e información se hace cada vez más necesario.

OBJETIVOS

OBJETIVO GENERAL

Llevar a la práctica los Conocimientos y habilidades adquiridos en el diseño e implementación de soluciones integradas LAN / WAN.

OBJETIVOS ESPECÍFICOS

Diseñar la topología de red acorde a los requerimientos.

Configurar los dispositivos que integran la topología de red para que permitan la interconectividad.

Implementar los protocolos de enrutamiento, OPSFv2, NAT, RIP, encapsulamiento, listas de control ACL, routing entre VLAN, DHCP, direccionamiento dinámico y estático.

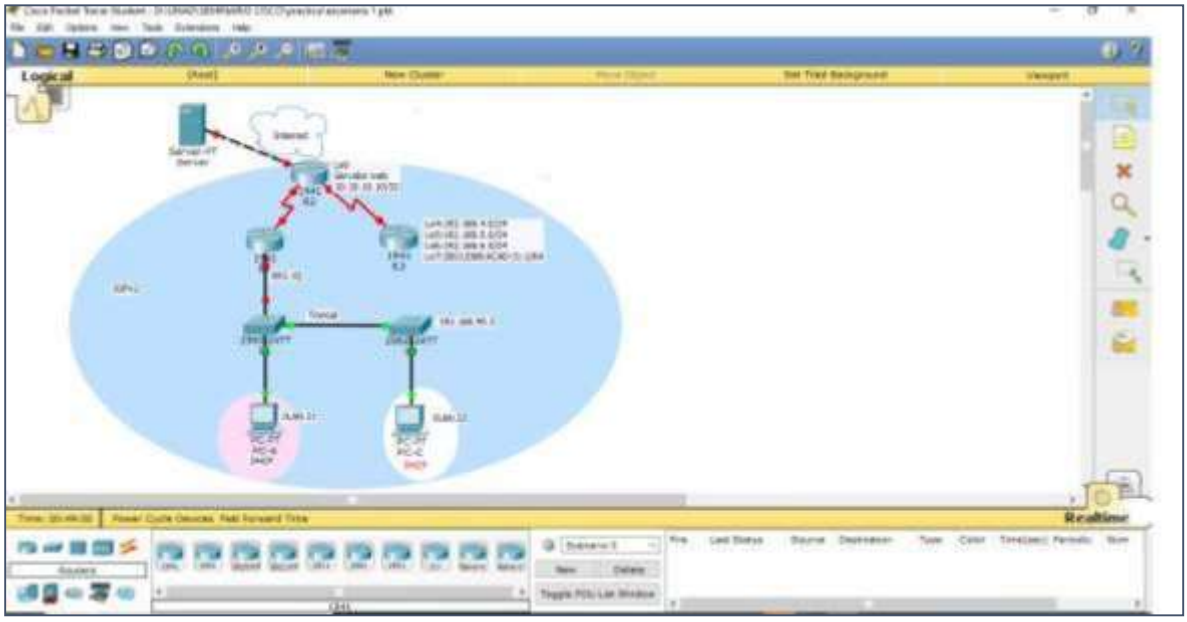
Ejecutar las políticas de seguridad en la configuración de los dispositivos.

1. DESARROLLO DEL ESCENARIO 1

1.1. Diseño de la Topología

Teniendo en cuenta los requerimientos del escenario propuesto, se realiza el diseño de la Topología en packet tracer, el cual debe admitir conectividad IPv4 e IPv6, la conexión física de los dispositivos preparados para realizar la configuración de seguridad de switches, routing entre VLAN, implementación de los protocolos de routing dinámico RIPv2, configuración de hosts dinámicos (DHCP) y el protocolo de tiempo de red (NTP) servidor/cliente, así como la implementación del protocolo de, la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL). En los router se agregan módulos con puerto serial adicional para permitir la conexión en los casos que se necesitan más de dos conexiones por cable serial.

Figura 3. Diseño de la red escenario 1 esquema en packet tracer



1.2. Inicialización de dispositivos

En cada uno de los router se borra la configuración inicial haciendo uso del comando erase startup-config para dejarlos listo para realizar las configuraciones planteadas en el escenario. Igualmente, eliminación del archivo startup-config de todos los switches y eliminación de la base de datos de VLAN anterior. Posteriormente se Cargan nuevamente los dispositivos con el comando reload.

Router>enable

Router#erase startup-config
Router#reload
Switch>enable
Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload

Verificación que la base de datos de VLAN no esté en la memoria flash en ambos switches
Switch>enable
Switch#show flash

Se evidencia que la base de datos de la VLAN fue borrada.
Directory of flash:/
1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
64016384 bytes total (59601463 bytes free)
Directory of flash:/
1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
64016384 bytes total (59601463 bytes free)

1.3. Configuración de los parámetros básicos de los dispositivos

1.3.1. Configuración de la computadora de Internet

En este paso, se realizan las siguientes tareas de configuración del servidor de Internet, basado en la siguiente tabla:

Tabla 1. Configuración del servidor de internet

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

Se ingresa a la configuración Física del Servidor y se establecen los parámetros anteriores. Se establecen los parámetros básicos de seguridad, nombres, desactivación la búsqueda DNS, contraseñas de acceso privilegiado, de consola y

telnet, se configura mensaje de prohibido de acceso no autorizado. Igualmente, de configuran los puertos seriales y las rutas predeterminadas.

1.3.2. Configuración del router R1

```
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd # UnAuthorized Access is prohibite!#

Configuración de los puertos seriales entre R1 y R2
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
R1(config-if)#exit

Configuración de ruta estática
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0
```

1.3.3. Configuración del router R2

```
Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
```

R2(config-line)#service password-encryption
R2(config)#banner motd # UnAuthorized Access is prohibite!#
R2(config)#ip http server (Comando invalido en packet tracer)

Configuración de los puertos seriales entre R2 y R1
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

Configuración de los puertos seriales entre R2 y R3
R2(config-if)#int s0/0/1
R2(config-if)#description connection to R3
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

Configuracion de los puertos entre R2 - Internet
R2(config-if)#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

Configuración ip loopback 0 Servidor Web
R2(config-if)#int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description simulated Web Server
R2(config-if)#exit

Configuración de ruta estática
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0

1.3.4. Configuración del router R3

Router>enable
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0

```
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd # UnAuthorized Access is prohibite!#

Configuración de los puertos seriales entre R3 y R2
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

Configuración ip del loopback 4
R3(config)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0

Configuración ip del loopback 5
R3(config-if)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0

Configuración ip del loopback 6
R3(config-if)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0

Configuración ip del loopback 7
R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit

Configuración de ruta estática
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
```

1.3.5. Configuración S1

```
Switch>enable
Switch#config t
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
```

```
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd # UnAuthorized Access is prohibite!#
S1(config)#
```

1.3.6. Configuración S3

```
Switch>enable
Switch#config t
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd # UnAuthorized Access is prohibite!#
```

1.4. . Verificación de la conectividad de la red

Basados en los siguientes requerimientos y haciendo uso del comando ping, se realiza la respectiva verificación de conectividad entre los dispositivos, arrojando como resultado satisfactorio.

Tabla 2. Parámetros para verificación de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

Figura 2. Ping desde R1 a R2 S0/0/0

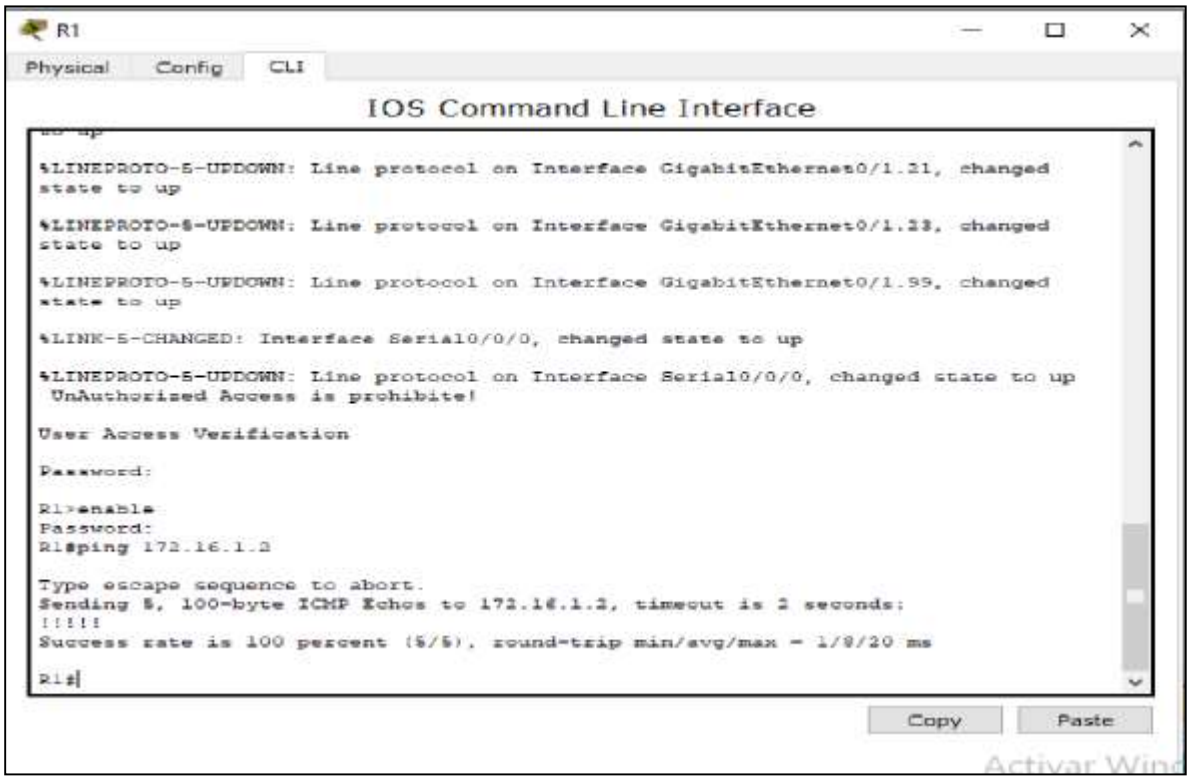


Figura 3. Ping desde R2 a R3 S0/0/1

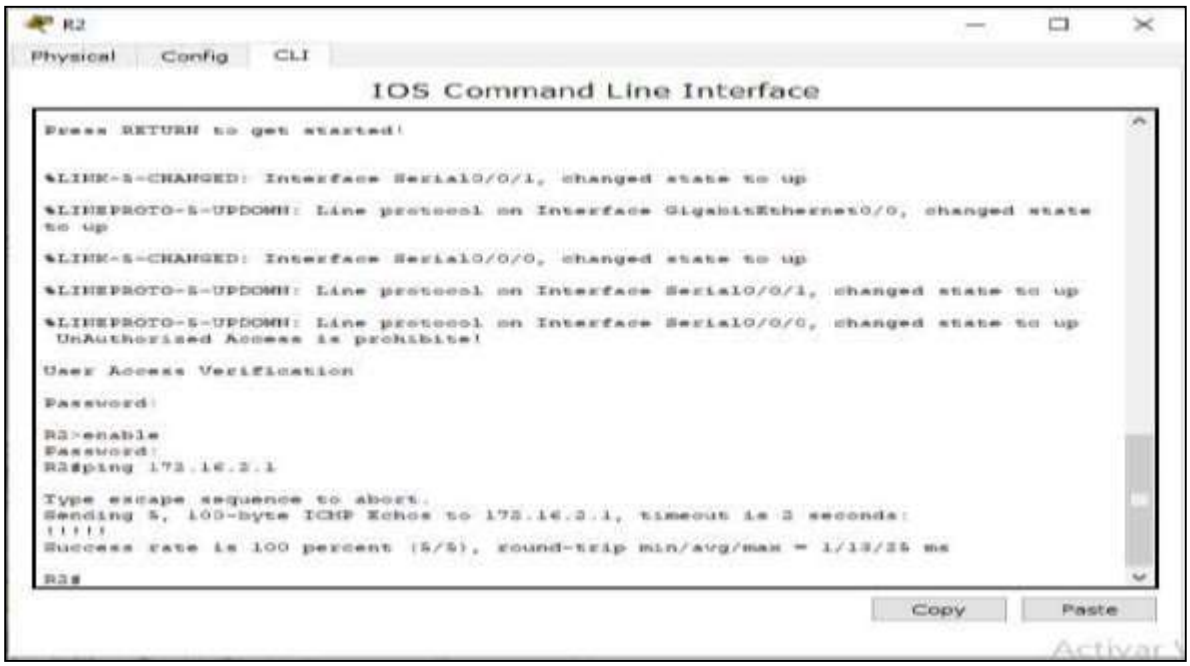
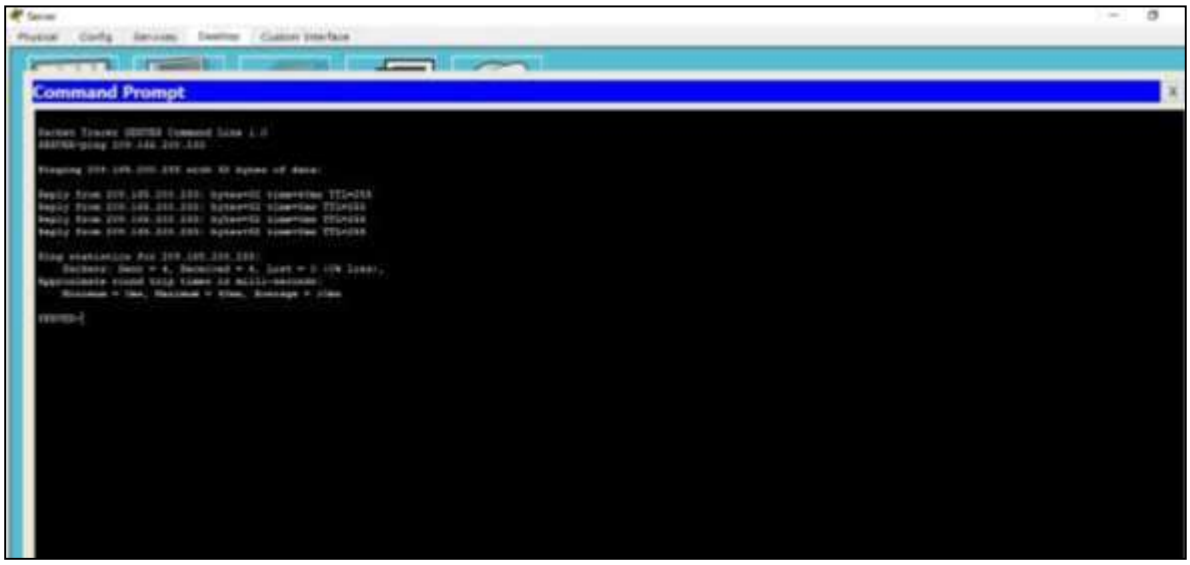


Figura 4. Ping desde el PC de Internet al Gateway Predeterminado



1.5. Configuración de la seguridad del switch, las VLAN y el routing entre VLAN

Se realiza la creación la base de datos de VLAN, Asignación de la dirección IP de administración, se asigna la primera dirección IPv4 de la subred como el gateway predeterminado y se configuran los puertos troncales.

1.5.1. Configuración S1

S1#config t
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-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#ip default-gateway 192.168.99.1

Configuración de los puertos troncales:

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1

S1(config-if-range)#switchport mode access

Configuración de los puertos de acceso y seguridad:
S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

1.5.2. Configuración S3

S3>enable
S3#config t
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
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

Configuración de los puertos de acceso y seguridad
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

1.5.3. Configuración R1

Asignación de la primera dirección disponible a la VLAN 21, LAN de Contabilidad
Configuración de la subinterfaz 802.1Q .21 en G0/1
R1>enable
R1#config t
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

Asignación de la primera dirección disponible a la VLAN 23, LAN de Ingeniería
Configuración de 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

Asignación de la primera dirección disponible a la VLAN 99, LAN de Administración
Configuración de la subinterfaz 802.1Q .99 en G0/1
R1(config-subif)#int g0/1.99
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

Activación de la interfaz G0/1
R1(config-subif)#int g0/1
R1(config-if)#no shutdown

1.5.4. Verificación de la conectividad de la red

A través del uso del comando ping se realiza prueba de la conectividad entre los switches y el R1, arrojando resultado satisfactorio.

Tabla 3. Parámetros verificación de conectividad switches y R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

Figura 5. Ping S1 a R1, dirección VLAN 99 y R1, dirección VLAN 21

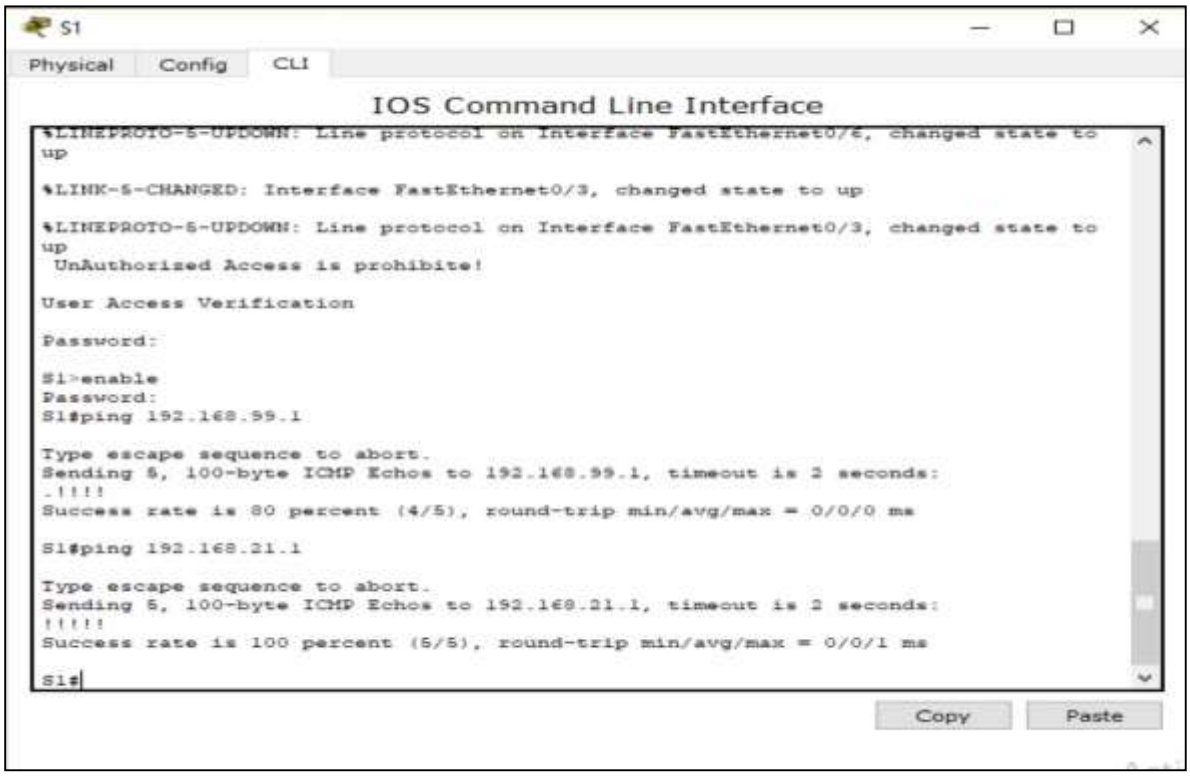
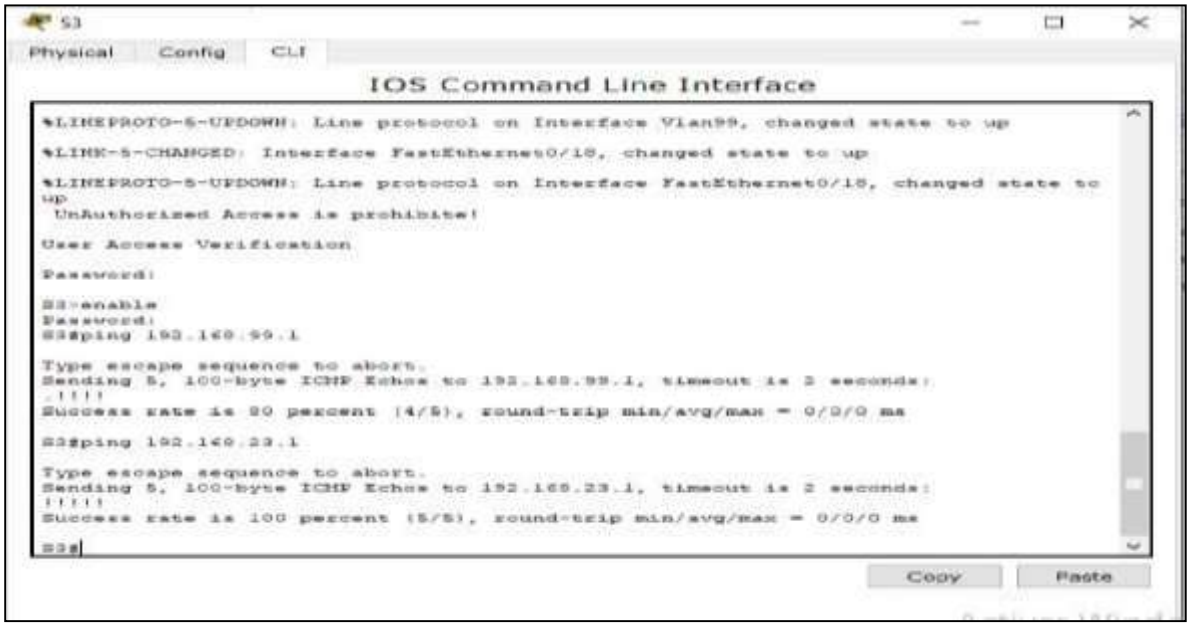


Figura 6. Ping S3 a R1, dirección VLAN 99 y R1, dirección VLAN 23



1.6. Configuración del protocolo de routing dinámico RIPv2

En cada uno de los router se realiza la configuración del Protocolo RIPv2, se asignan las redes directamente conectadas, se establecen todas las interfaces LAN como pasivas y se desactiva la sumarización automática

1.6.1. Configuración RIPv2 en el R1

Configuración del protocolo RIPv2 en el R1
R1>enable
R1#config t
R1(config)#router rip
R1(config-router)#version 2

Determinando todas las redes IPv4 directamente conectadas
R1(config-router)#do show ip route connected
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

Estableciendo 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

Desactivando la sumarización automática
R1(config-router)#no auto-summary

1.6.2. Configuración RIPv2 en el R2

Configuración del protocolo RIPv2 en el R2
R2>enable
R2#config t
R2(config)#router rip
R2(config-router)#version 2

Determinando todas las redes IPv4 directamente conectadas Omitiendo la red G0/0.
R2(config-router)#do show ip route connected
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0

Estableciendo la interface loopback 0 como pasiva
R2(config-router)#passive-interface loopback 0

Desactivando la sumarización automática
R2(config-router)#no auto-summary

1.6.3. Configuración RIPv3 en el R2

Configuración del protocolo RIPv2 en el R3

R3>enable
R3#config t
R3(config)#router rip
R3(config-router)#version 2

Determinando todas las redes IPv4 directamente conectadas
R3(config-router)#do show ip route connected
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

Estableciendo todas las interfaces loopback como pasivas

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

Desactivando la sumarización automática

R3(config-router)#no auto-summary

1.7. Verificación de la información de RIP

En la siguiente tabla se describen los comandos utilizados para verificar el correcto funcionamiento del protocolo RIP

Tabla 4. Comandos para la verificación de la información de RIP

Pregunta	Respuesta
¿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?	show ip protocols

¿Qué comando muestra solo las rutas RIP?	show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show | run section router rip

1.8. Implementación DHCP y NAT para IPv4

Se realiza la reserva de direcciones para las VLAN, se crea un pool de DHCP para las VLAN 21 y VLAN 23 y Configurar de la NAT estática y dinámica.

1.8.1. Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

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

```
R1>enable
R1#config t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

Creación de 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 (Packet tracer no soporta este commando)
```

Creación de un pool de DHCP para la VLAN 23.

```
R1(dhcp-config)#ip dhcp pool ENGNR
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 (Packet tracer no soporta este comando)
```

1.8.2. Configurar la NAT estática y dinámica en el R2

Creación de una base de datos local con una cuenta de usuario y Habilitación del servicio del servidor HTTP y creación de una NAT estática al servidor web.

```
R2>enable
R2#config t
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server (Packet tracer no soporta este comando)
R2(config)#ip http authentication local (Packet tracer no soporta este comando)
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

```
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
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
```

Definición del pool de las direcciones Ip públicas.

```
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

1.9. Verificación del protocolo DHCP y la NAT estática

Se realiza la verificación en el PC-A y en el PC-C que haya adquirido la IP del servidor DHCP, obteniendo resultados satisfactorios.

Tabla 5. Verificación del protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Satisfactorio
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Packet tracert No soporta este procedimiento, porque, no soporto el comando Ip HTTP server en R2 para Activar el Servidor web, pero al ingresar desde una red real se puede ingresar con el usuario y contraseña.

Figura 7. PC-A con información de ip del servidor de DHCP

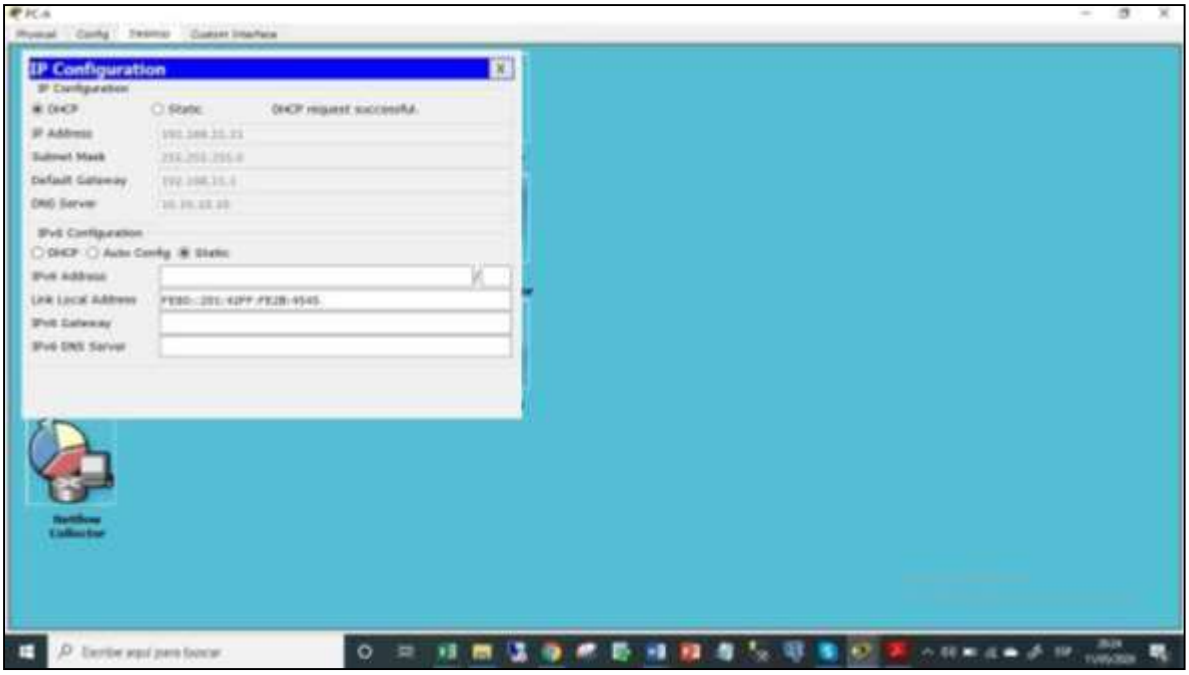


Figura 8. PC-C con información de ip del servidor de DHCP

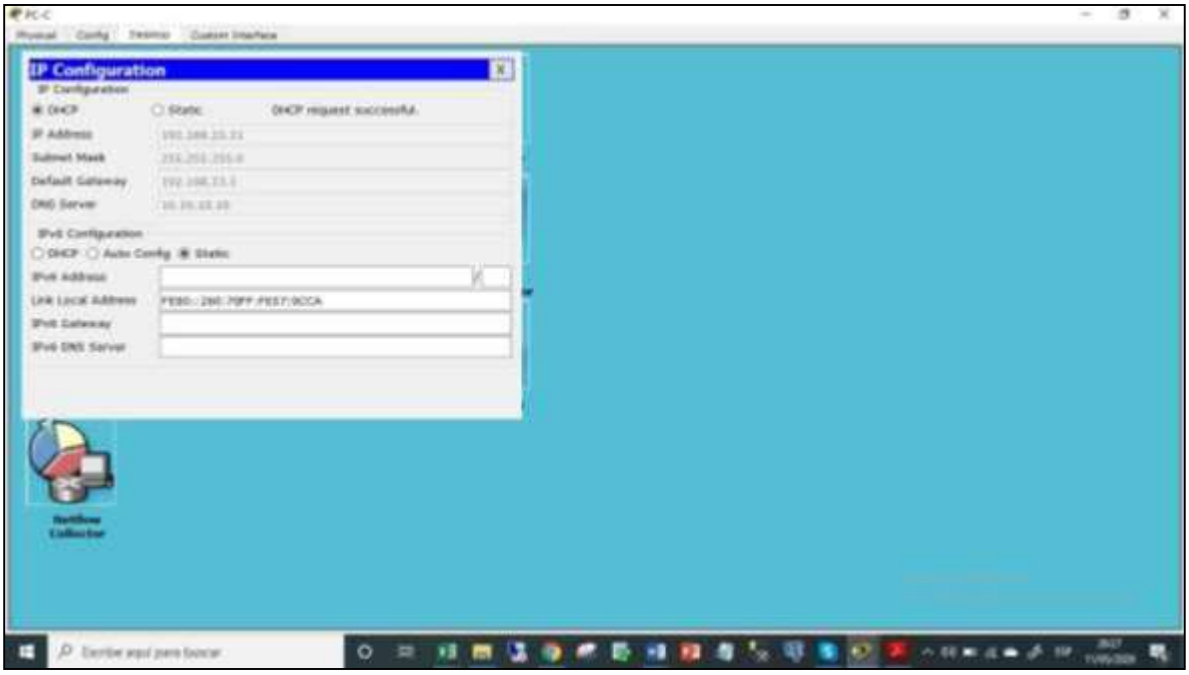
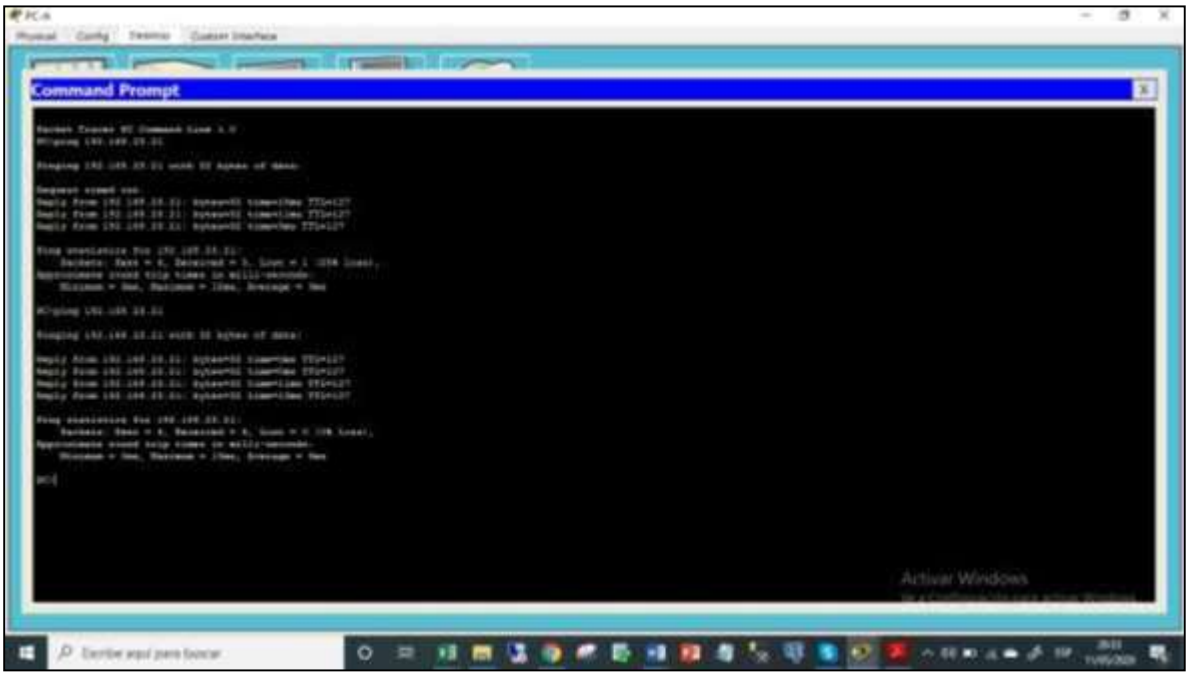


Figura 9. Ping PC-A a PC-C



1.10. Configuración de NTP

Ajustando la fecha y hora en R2.
R2>enable
R2#clock set 21:08:00 11 may 2020
R2#config t
R2(config)#ntp master 5(Packet tracer no soporta este comando)

Configuración de R1 como un cliente NTP.
R1>enable
R1#config t
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#end
R1#show ntp associations(Packet tracer no soporta este comando)

1.11. Configuración y verificación de las listas de control de acceso (ACL)

Configuración de una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, aplicación de ACL con nombre a las líneas VTY.

1.11.1 Restricción del acceso a las líneas VTY en el R2

```
R2>enable
R2#config t
R2(config)#ip access-list standar ADMIN-MGT
R2(config-std-nacl)#
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open UnAuthorized Access is prohibite!
User Access Verification
Password:
R2>
R3>enable
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
```

1.11.2 . Introducción de comandos para verificación de las ACL.

Evidenciándose la incorporación de las listas permitidas en cada uno de los router.

Tabla 6. Comandos para verificación de ACL

Descripción del comando	Entrada del estudiante (comando)
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(Packet tracer no soporta este comando)
¿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?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025209.165.200.238:1025

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * R2#show ip nat translation Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- ---

Figura 4. Ping a la computadora de Internet desde la PC-A

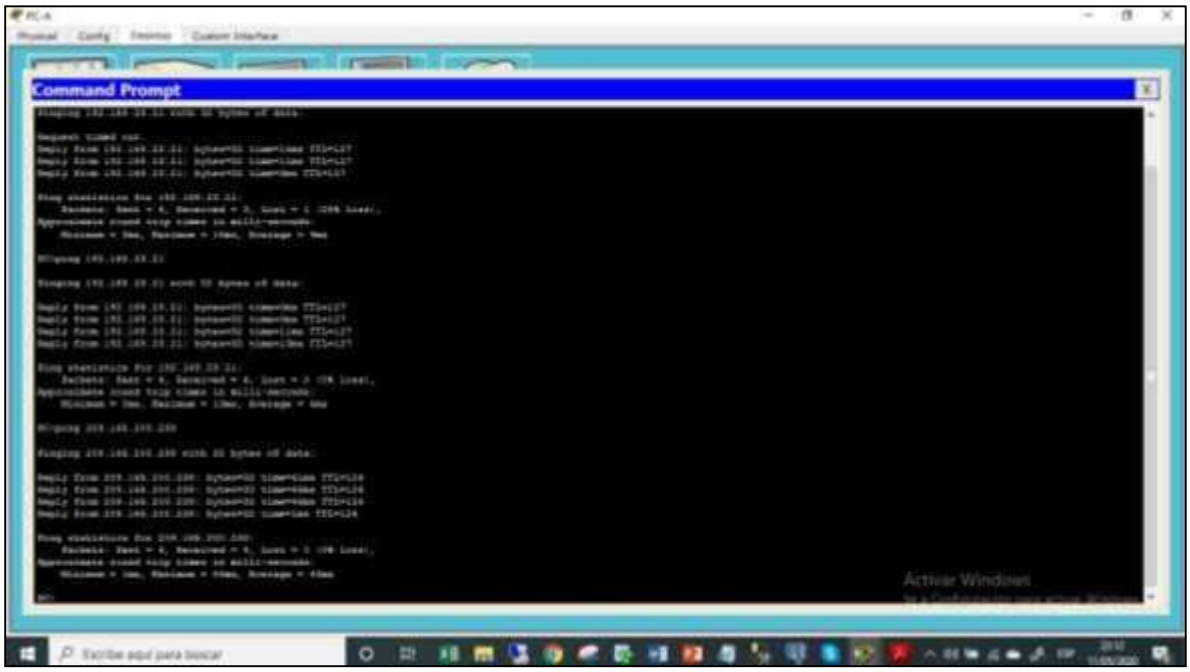
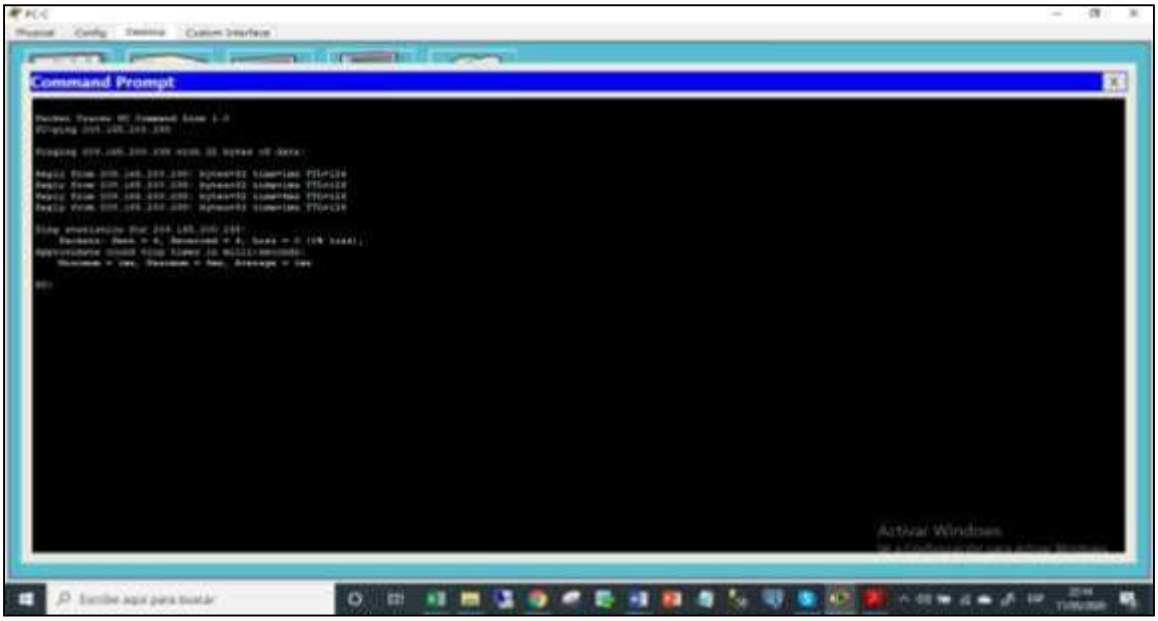


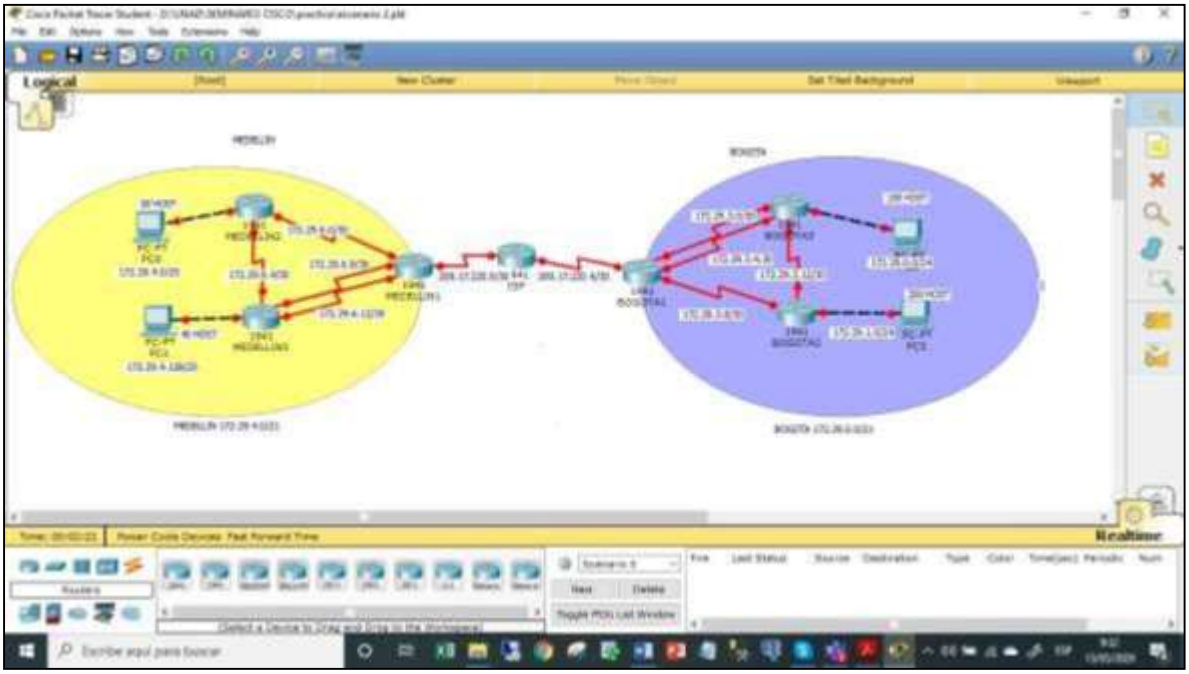
Figura 5. Ping a la computadora de Internet desde la PC-C



2. DESARROLLO DE ESCENARIO 2

Se realiza el Diseño de la Topología de la red en packet tracer acorde al planteamiento del escenario 2, el cual corresponde a una red distribuida en las Ciudades de Bogotá y Medellín, se realiza la conexión física de los dispositivos, preparados para realizar la configuración de acuerdo a los parámetros establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red. En los router se adicionaron módulos con puerto serial adicional para permitir la conexión en los casos que se necesitan más de dos conexiones por cable serial.

Figura 12. Diseño de la red escenario 2 esquema en packet tracer



2.1. Configuración del enrutamiento

Realización de las rutinas de diagnóstico para dejar los equipos listos para su configuración (asignación nombres de equipos, asignar claves de seguridad, etc). Desactivación de la búsqueda DNS, contraseñas de acceso privilegiado, de consola y telnet, se configura mensaje de prohibido de acceso no autorizado. Igualmente se configuran los puertos seriales y las rutas predeterminadas.

2.1.1. Configuración del Router ISP

Router>enable
Router#config t

```
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#banner motd # UnAuthorized Access is prohibite!#
ISP(config)#ip domain-name cisco.com
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
```

Configuración de la interfaz s0/0/0

```
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#description connection to MEDELLIN1
ISP(config-if)#no shutdown
ISP(config-if)#exit
```

Configuración de la interfaz s0/0/1

```
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
ISP(config-if)#no shutdown
ISP(config-if)#exit
```

2.1.2. Configuración del Router MEDELLIN1

```
Router>enable
Router#config t
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#banner motd # UnAuthorized Access is prohibite!#
MEDELLIN1(config)#ip domain-name cisco.com
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
```

Configuración de la interfaz s0/0/0

```
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-if)#exit
```

Configuración de la interfaz s0/0/1

```
MEDELLIN1(config)#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
MEDELLIN1(config-if)#exit
```

Configuración de la interfaz s0/1/0

```
MEDELLIN1(config)#int s0/1/0
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)#exit
```

Configuración de la interfaz s0/1/1

```
MEDELLIN1(config)#int s0/1/1
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)#exit
```

2.1.3. Configuración del Router MEDELLIN2

```
Router>enable
Router#config t
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#banner motd # UnAuthorized Access is prohibite!#
```

MEDELLIN2(config)#ip domain-name cisco.com
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

Configuración de la interfaz s0/0/0
MEDELLIN2(config)#int s0/0/0
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
MEDELLIN2(config-if)#exit

Configuración de la interfaz s0/0/1
MEDELLIN2(config)#int s0/0/1
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)#exit

Configuración de la interfaz g0/0
MEDELLIN2(config)#int g0/0
MEDELLIN2(config-if)#description to PC2
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#exit

2.1.4. Configuración del Router MEDELLIN3

Router>enable
Router#config t
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#banner motd # UnAuthorized Access is prohibite!#
MEDELLIN3(config)#ip domain-name cisco.com
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
```

Configuración de la interfaz s0/0/0

```
MEDELLIN3(config)#int s0/0/0
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)#exit
```

Configuración de la interfaz s0/0/1

```
MEDELLIN3(config)#int s0/0/1
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)#exit
```

Configuración de la interfaz s0/1/0

```
MEDELLIN3(config)#int s0/1/0
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
MEDELLIN3(config-if)#exit
```

Configuración de la interfaz g0/0

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#description connection to PC1
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#exit
```

2.1.5. Configuración del Router BOGOTA1

```
Router>enable
Router#config t
Router(config)#hostname BOGOTA1
BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#enable secret class
BOGOTA1(config)#banner motd # UnAuthorized Access is prohibite!#
BOGOTA1(config)#ip domain-name cisco.com
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
```

Configuración de la interfaz s0/0/0

```
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)#no shutdown
BOGOTA1(config-if)#exit
```

Configuración de la interfaz s0/0/1

```
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#description connection to BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
```

Configuración de la interfaz s0/1/0

```
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#description connection to BOGOTA3
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)#exit
```

Configuración de la interfaz s0/1/1

```
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#description connection to BOGOTA3
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)#exit
```

2.1.6. Configuración del Router BOGOTA2

```
Router>enable
Router#config t
Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#enable secret class
```

BOGOTA2(config)#banner motd # UnAuthorized Access is prohibite!#
BOGOTA2(config)#ip domain-name cisco.com
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

Configuración de la interfaz s0/0/0

BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#description connection to BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit

Configuración de la interfaz s0/0/1

BOGOTA2(config)#int s0/0/1
BOGOTA2(config-if)#description connection to BOGOTA3
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit

Configuración de la interfaz g0/0

BOGOTA2(config)#int g0/0
BOGOTA2(config-if)#description connection to PC4
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit

2.1.7. Configuración del Router BOGOTA3

Router>enable
Router#config t
Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#banner motd # UnAuthorized Access is prohibite!#
BOGOTA3(config)#ip domain-name cisco.com
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
```

Configuración de la interfaz s0/0/0

```
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#description connection to BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
```

Configuración de la interfaz s0/0/1

```
BOGOTA3(config)#int s0/0/1
BOGOTA3(config-if)#description connection to BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
```

Configuración de la interfaz s0/1/0

```
BOGOTA3(config)#int s0/1/0
BOGOTA3(config-if)#description connection to BOGOTA2
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
```

Configuración de la interfaz g0/0

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#description connection to PC3
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#exit
```

2.1.8. Configuración de enrutamiento OSPF

Configuración de enrutamiento de ruta por defecto hacia el ISP y redistribución dentro de las publicaciones de OSPF.

Configuración ruta estática predeterminada red de MEDELLIN1:

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router rip
MEDELLIN1(config-router)#default-information originate
```

Configuración ruta estática predeterminada red de BOGOTA1:

```
BOGOTA1>enable
BOGOTA1#config t
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router rip
BOGOTA1(config-router)#default-information originate
```

2.1.9. Sumarización de las redes

Se realiza la sumarización de redes para verificar cual es la ruta estatica que va a ser dirigida desde el router ISP hacia cada red interna de Bogotá y Medellín.

Figura 13. Sumarización de las redes

		RED SUMARIZADA																	
		128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1		
172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0		172.29.4.0/25
172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0		172.29.4.128/25
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0		172.29.6.4/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0		172.29.6.8/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0		172.29.6.12/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0		172.29.6.0/30
172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	SUMARIZACION RED MEDELLIN	172.29.4.0/22
																			RED BOGOTA1
		128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1		
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		172.29.0.0/24
172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0		172.29.1.0/24
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0		172.29.3.12/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0		172.29.3.8/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0		172.29.3.0/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0		172.29.3.4/30
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	SUMARIZACION RED BOGOTA	172.29.0.0/22

2.1.10 Configuración de ruta estática

Dirigida hacia cada red interna de Bogotá y Medellín

```
ISP>enable
ISP#config t
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
```

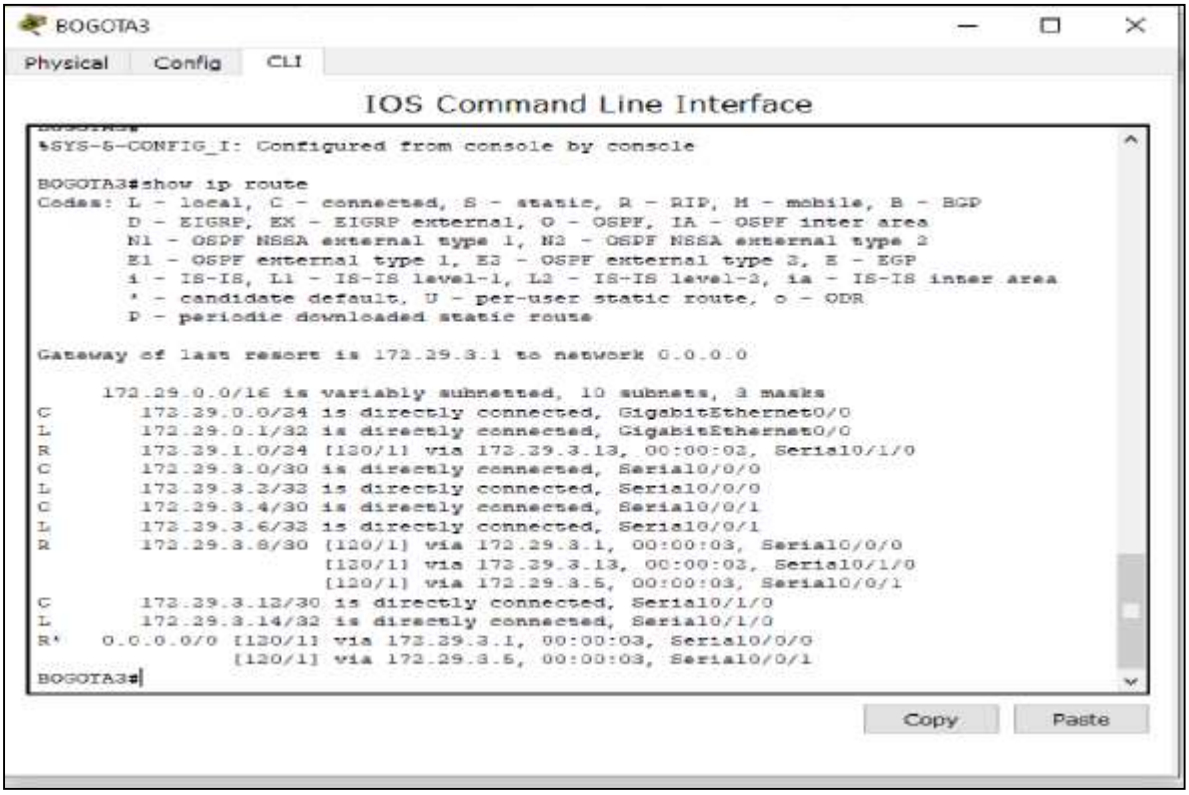
2.2. Tabla de enrutamiento.

Verificación de la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas. Verificación del balanceo de carga que presentan los routers.

El balanceo de carga se hace en los router que tienen dos seriales para conectarse a un mismo router. Se evidencia un equilibrio de carga en las rutas.

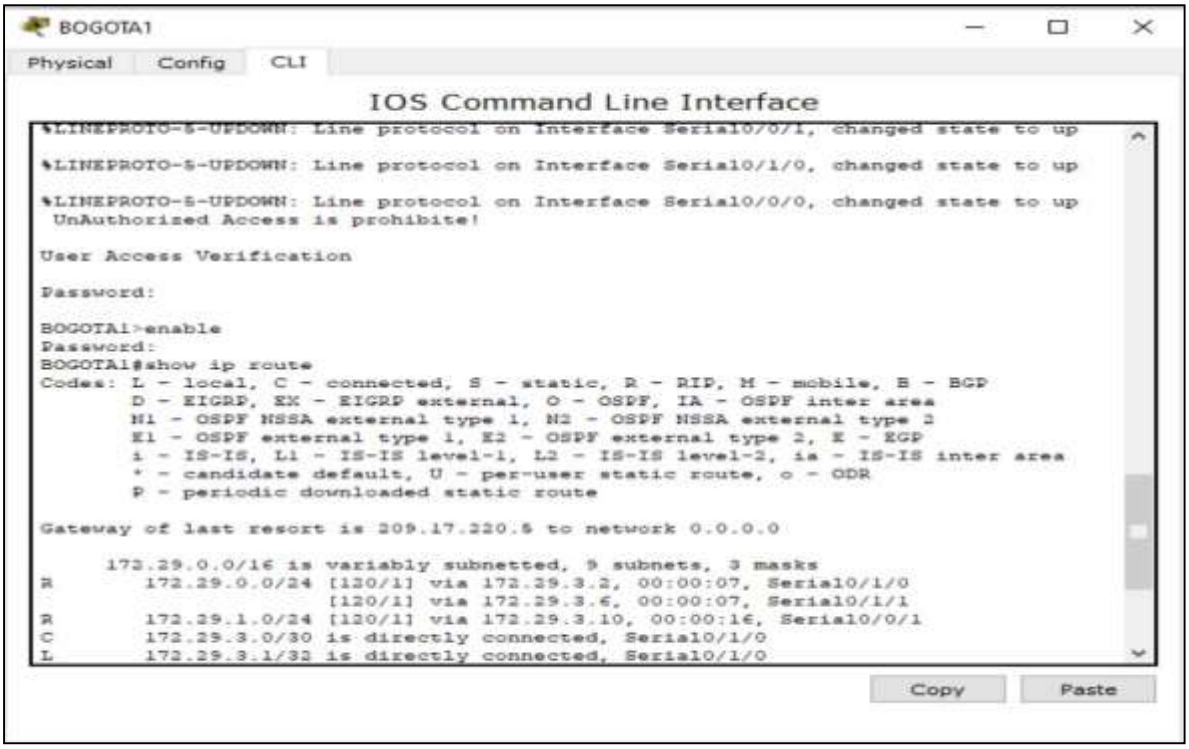
BOGOTA3>enable
BOGOTA3#config t
BOGOTA3#show ip route

Figura 14. Tabla de enrutamiento BOGOTA3



BOGOTA1>enable
BOGOTA1#show ip route

Figura 15. Tabla de enrutamiento BOGOTA1



2.3. Deshabilitar la propagación del protocolo OSPF

Con el objetivo de no propagar las publicaciones por interfaces que no sean requeridas, se procede a deshabilitar la propagación del protocolo OSPF y dejar activas solo las interfaces requeridas, según requerimientos descritos en la siguiente tabla:

Tabla 7. Iinterfaces 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

2.3.1. Notificación de las redes para RIP version 2 Router MEDELLIN1

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#router rip
MEDELLIN1(config-router)#version 2
MEDELLIN1(config-router)#no auto-summary
MEDELLIN1(config-router)#do show ip route connected
MEDELLIN1(config-router)#network 172.29.6.0
MEDELLIN1(config-router)#network 172.29.6.8
MEDELLIN1(config-router)#network 172.29.6.12
MEDELLIN1(config-router)#passive-interface Serial0/0/0
```

2.3.2. Notificación de las redes para RIP version 2 Router MEDELLIN2

```
MEDELLIN2>enable
MEDELLIN2#config t
MEDELLIN2(config)#router rip
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#no auto-summary
MEDELLIN2(config-router)#do show ip route connected
MEDELLIN2(config-router)#network 172.29.4.0
MEDELLIN2(config-router)#network 172.29.6.0
MEDELLIN2(config-router)#network 172.29.6.4
MEDELLIN2(config-router)#passive-interface g0/0
```

2.3.3. Notificación de las redes para RIP version 2 Router MEDELLIN3

```
MEDELLIN3>enable
MEDELLIN3#config t
MEDELLIN3(config)#router rip
MEDELLIN3(config-router)#version 2
MEDELLIN3(config-router)#no auto-summary
MEDELLIN3(config-router)#do show ip route connected
MEDELLIN3(config-router)#network 172.29.4.128
MEDELLIN3(config-router)#network 172.29.6.4
MEDELLIN3(config-router)#network 172.29.6.8
MEDELLIN3(config-router)#network 172.29.6.12
MEDELLIN3(config-router)#passive-interface g0/0
```

2.3.4. Notificación de las redes para RIP version 2 Router BOGOTA1

```
BOGOTA1>enable
```

```
BOGOTA1#config t
BOGOTA1(config)#router rip
BOGOTA1(config-router)#version 2
BOGOTA1(config-router)#no auto-summary
BOGOTA1(config-router)#do show ip route connected
BOGOTA1(config-router)#network 172.29.3.0
BOGOTA1(config-router)#network 172.29.3.4
BOGOTA1(config-router)#network 172.29.3.8
BOGOTA1(config-router)#passive-interface Serial0/0/0
```

2.3.5. Notificación de las redes para RIP version 2 Router BOGOTA2

```
BOGOTA2>enable
BOGOTA2#config t
BOGOTA2(config)#router rip
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#no auto-summary
BOGOTA2(config-router)#do show ip route connected
BOGOTA2(config-router)#network 172.29.1.0
BOGOTA2(config-router)#network 172.29.3.8
BOGOTA2(config-router)#network 172.29.3.12
BOGOTA2(config-router)#passive-interface g0/0
```

2.3.6. Notificación de las redes para RIP version 2 Router BOGOTA3

```
BOGOTA3>enable
BOGOTA3#config t
BOGOTA3(config)#router rip
BOGOTA3(config-router)#version 2
BOGOTA3(config-router)#no auto-summary
BOGOTA3(config-router)#do show ip route connected
BOGOTA3(config-router)#network 172.29.0.0
BOGOTA3(config-router)#network 172.29.3.0
BOGOTA3(config-router)#network 172.29.3.4
BOGOTA3(config-router)#network 172.29.3.12
BOGOTA3(config-router)#passive-interface g0/0
```

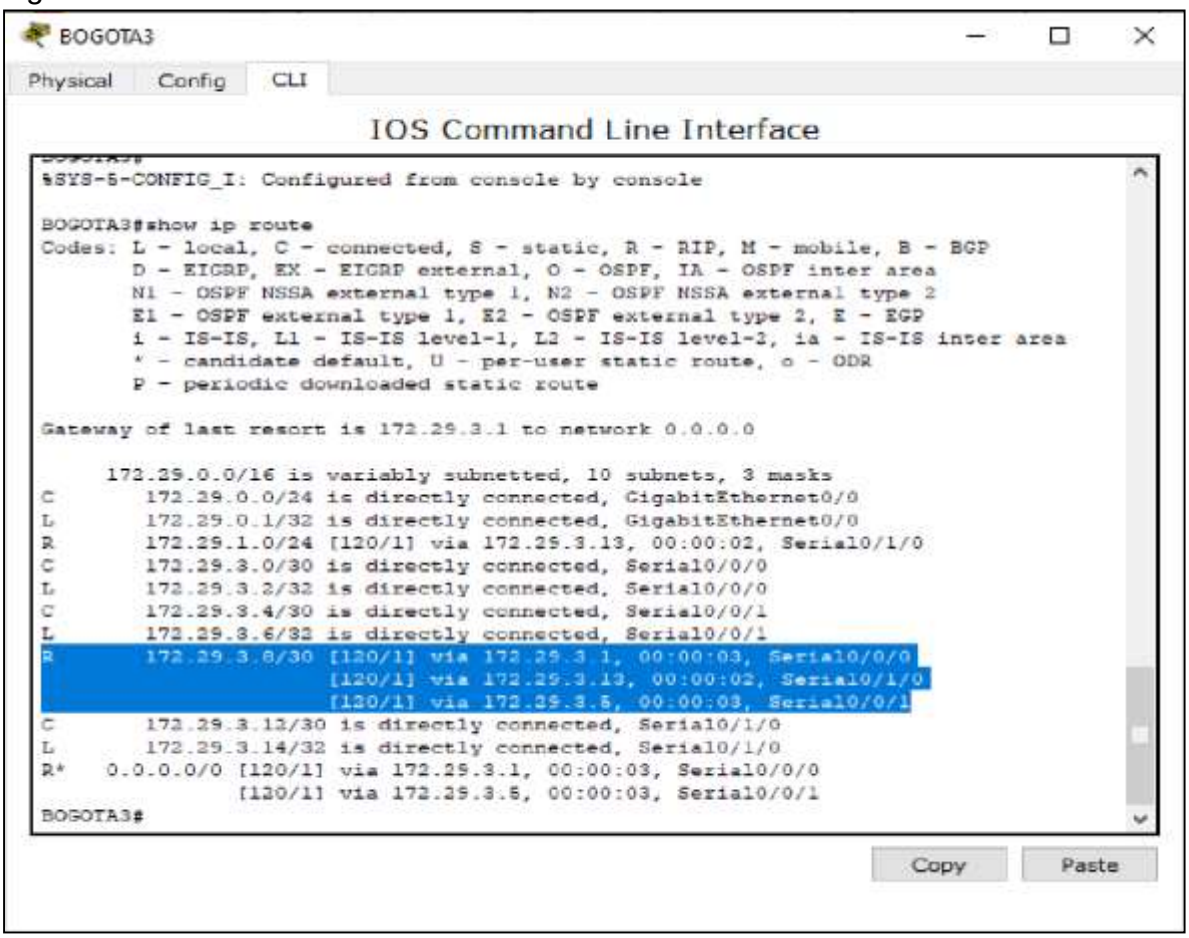
2.4. Verificación del Protocolo OSPF.

Se verifica a través del comando show ip route y se documenta las evidencias de enrutamiento configuradas en los routers, igualmente las interfaces pasivas para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

2.4.1. Visualización de las rutas redundantes en el router BOGOTA3

BOGOTA3#show ip route

Figura 16. Visualización de las rutas redundantes en el router BOGOTA3



2.4.2. Visualización de las rutas redundantes en el router MEDELLIN3

MEDELLIN3>enable
MEDELLIN3#show ip route

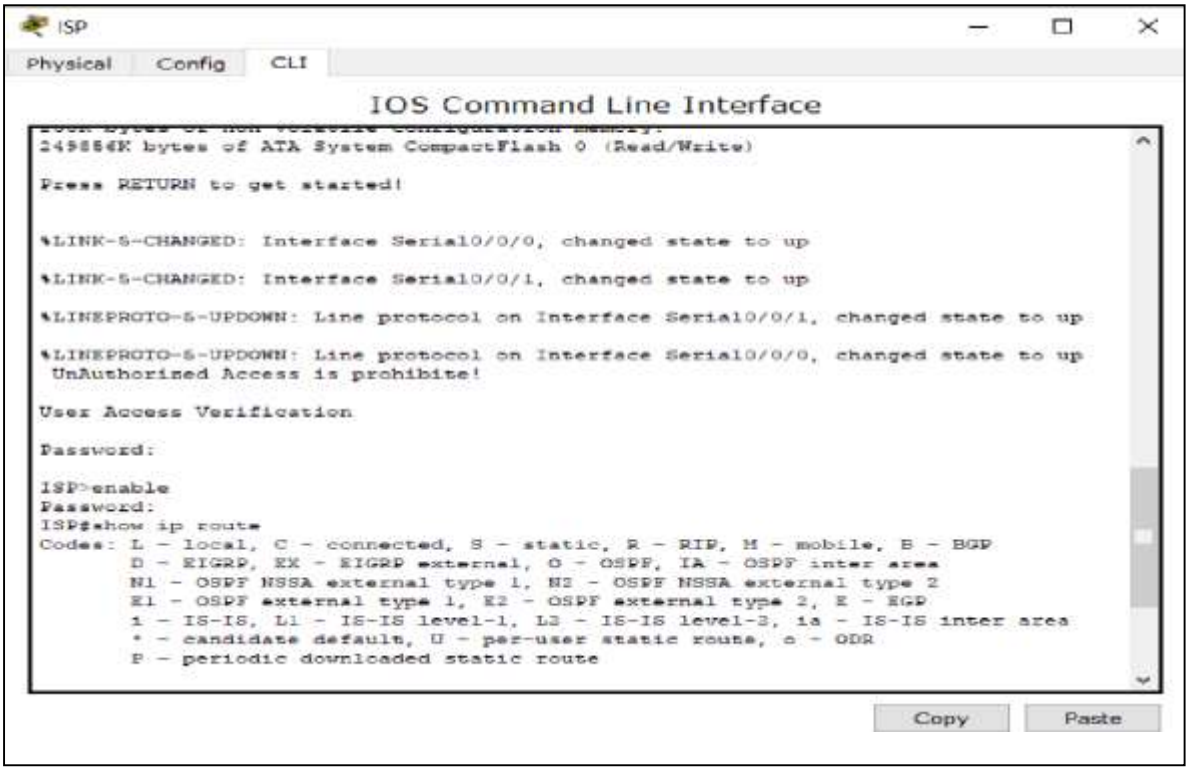
Figura 17. Visualización de las rutas redundantes en el router MEDELLIN3

2.4.3. Verificación de router ISP

solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

ISP>enable
ISP#show ip route

Figura 18. Verificación de rutas estáticas adicionales en router ISP



2.5. Configuración de Encapsulamiento y Autenticación PPP

2.5.1. Configuración del enlace Medellín1 con ISP con autenticación PAP

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
```

```
ISP>enable
ISP#config t
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
```

2.5.2. Configuración del enlace Bogotá1 con ISP con autenticación CHAP

```
BOGOTA1>enable
BOGOTA1#config t
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap

ISP>enable
ISP#config t
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

2.6. Configuración de PAT

2.6.1. Configuración de NAT

Se realiza la configuración de NAT en el router Medellín1 y en el en el router Bogotá1 teniendo en cuenta los requerimientos de la red, 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.

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
```

Figura 19. Verificación de no comunicación de extremo a extremo

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
●	Failed	PC4	PC2	ICMP		0.000	N
●	Failed	PC1	PC3	ICMP		0.000	N
●	Successful	PC2	ISP	ICMP		0.000	N

Figura 20. Ping de PC2 a ISP

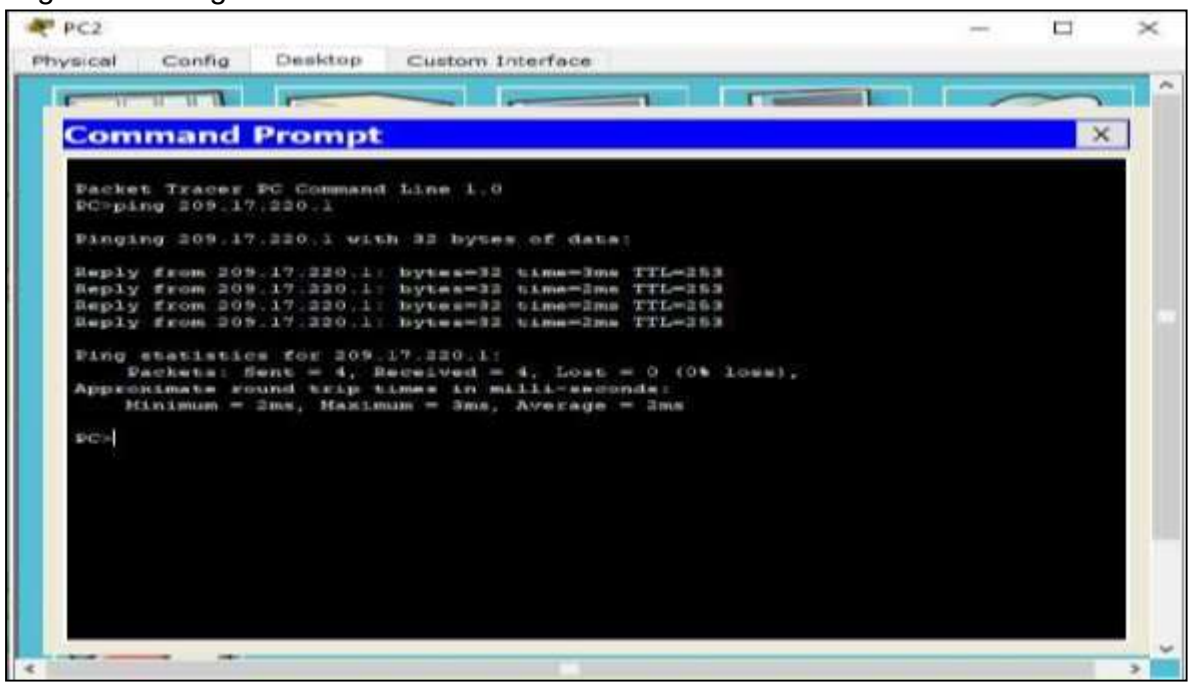
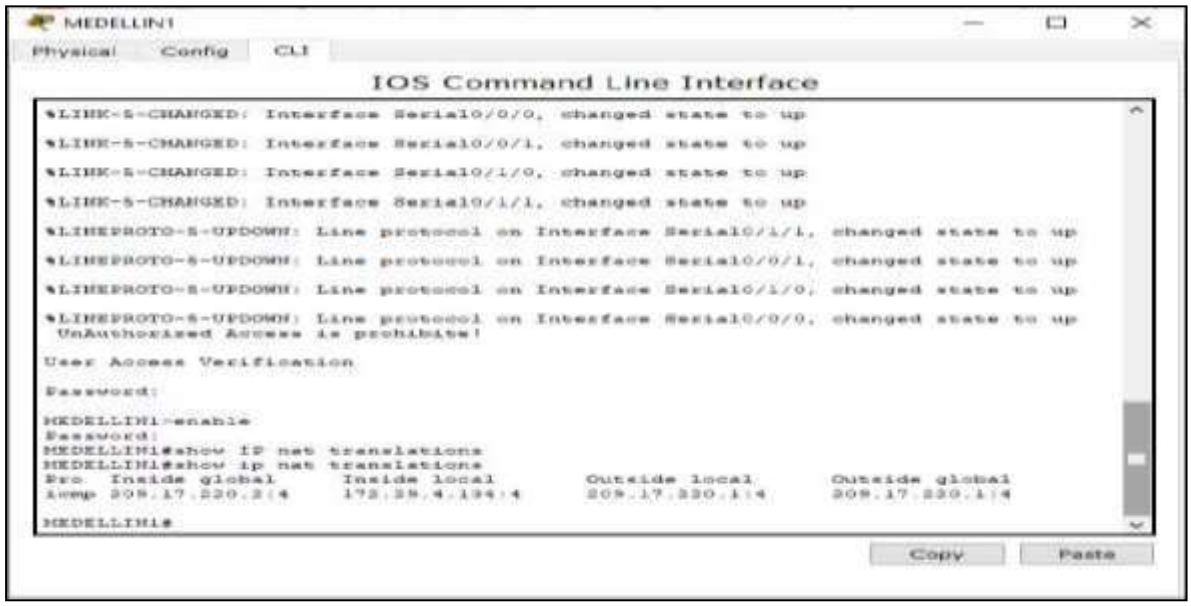


Figura 21. Verificación de configuración de PAT en MEDELLIN1

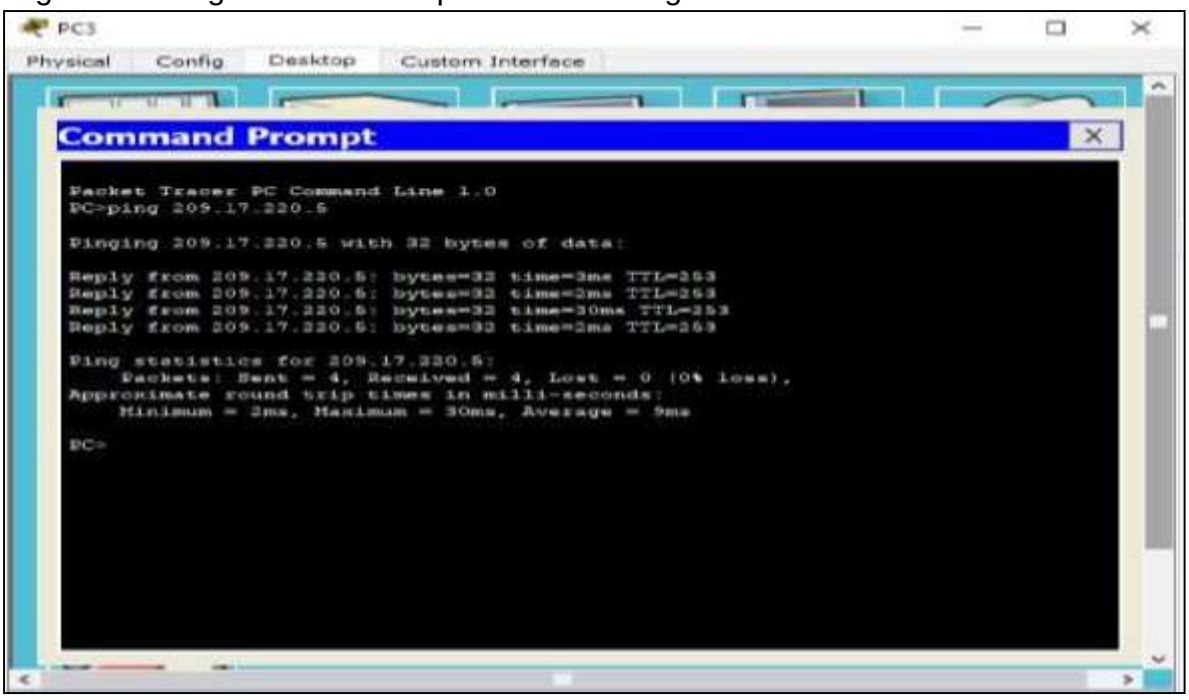


2.6.2. Configuración de NAT en el router Bogotá1

Se procede a configurar el NAT en el router Bogotá1. Comprobando que la traducción de direcciones indica las interfaces de entrada y de salida.

```
BOGOTA1>enable
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
```

Figura 22. Ping de PC3 a ISP posterior a configuración de NAT



2.6.2.1. Comprobación de traducción de direcciones

A través del comando Show IP NAT translations se comprueba que la traducción de direcciones se realizó efectivamente, indicando las interfaces de entrada y de salida.

Figura 23. Comprobación de traducción de direcciones en BOGOTA 1

Figura 24. ping de PC3 A ISP posterior a configuración de NAT

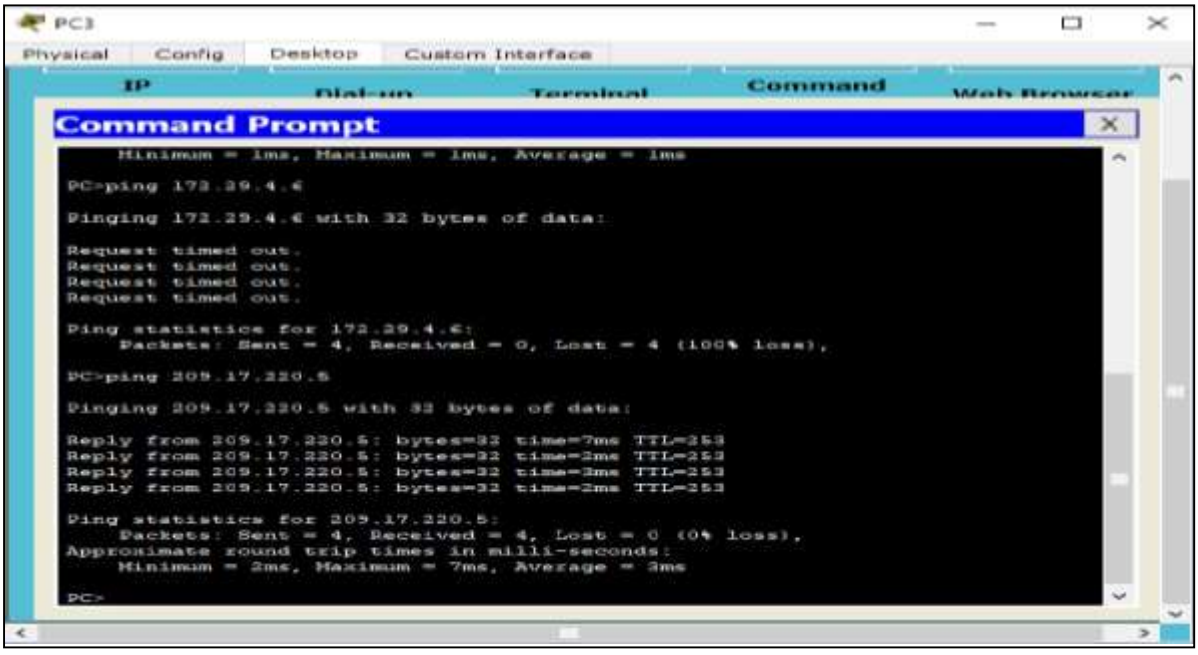
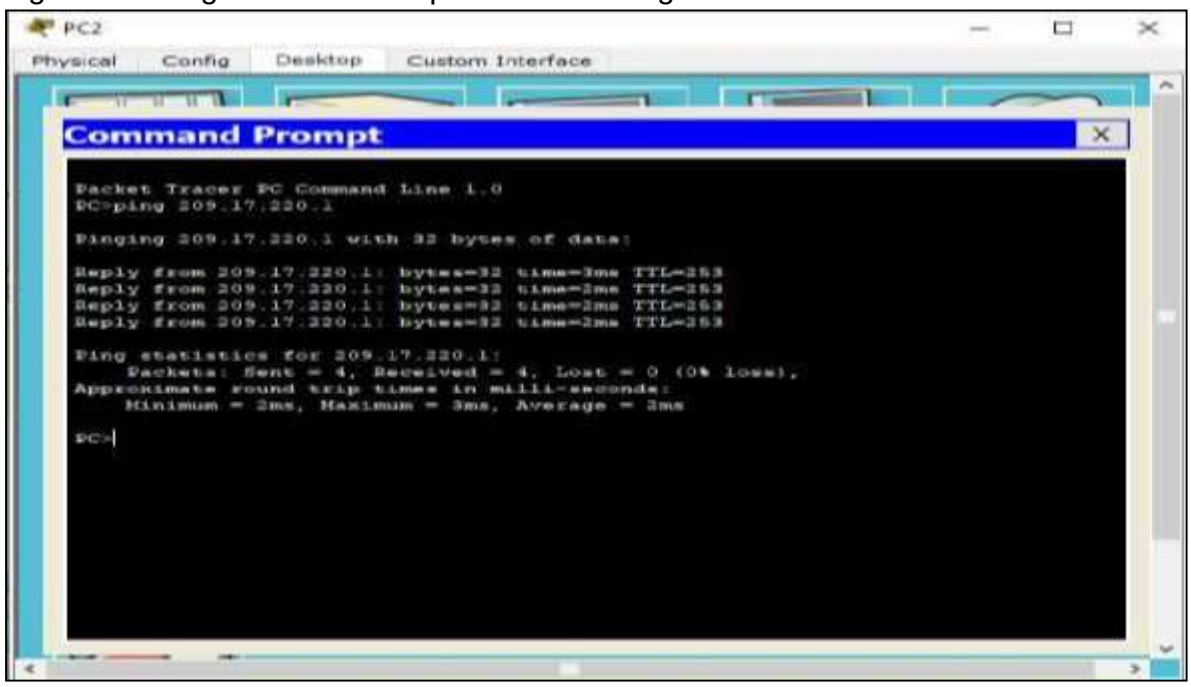


Figura 25. Ping de PC2 a ISP posterior a configuración de NAT



2.7. Configuración del Servicio DHCP

Se realiza la configuración del servicio DHCP en la red Medellín2 y Medellin3, según requerimiento de red el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN. Adicionalmente se configura el router Medellín3 para habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Igualmente se realiza la configuración la red Bogotá2 y Bogotá3 habilitando el router Bogota2 como servidor DHCP para ambas redes LAN. Así mismo se configura el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

2.7.1. Configuración del servidor DHCP red Medellín

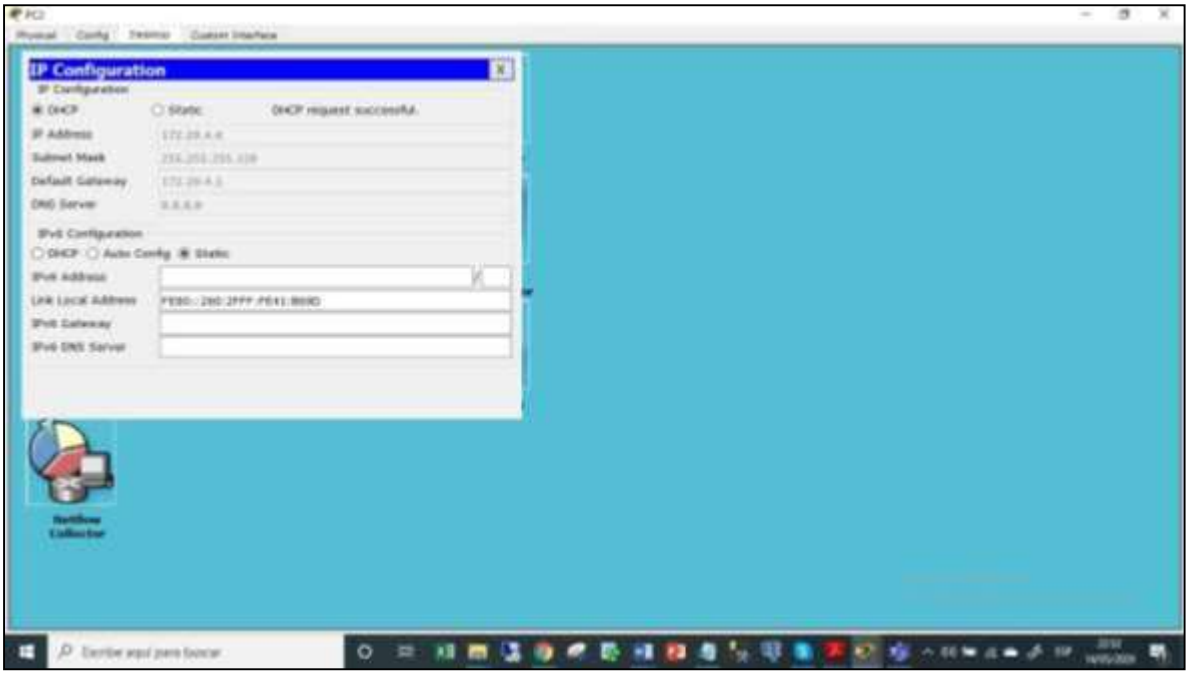
Configuración de la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

MEDELLIN2>enable
MEDELLIN2#config t

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MED2
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 pool MED3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
```

No obstante, para que PC2 reciba la dirección, se debe habilitar directamente DHCP en la PC2

Figura 26. Habilitación directa de DHCP en la PC2



2.7.1.2. Configuración de router MEDELLIN3 para habilitación de broadcast a MEDELLIN2

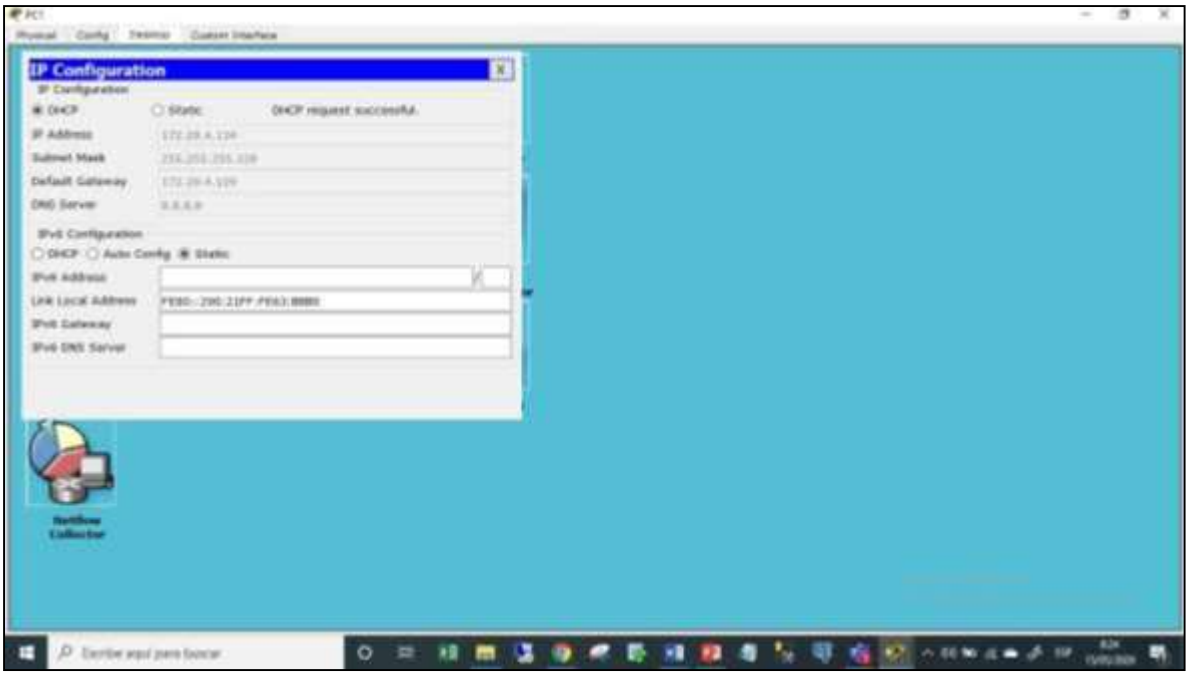
Adicionalmente para que la PC1 pueda conectarse en MEDELLIN3, se debe crear un redireccionamiento para que MEDELLIN2, se conecte con DHCP

```
MEDELLIN3>enable
MEDELLIN3#config t
```

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

Igualmente, para que PC1 reciba la dirección, se debe habilitar directamente DHCP en la PC1.

Figura 27. Habilitación directa de DHCP en la PC1



2.7.2. Configuración de la red Bogotá para el servidor DHCP

Configuración de la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes LAN.

```
BOGOTA2>enable
BOGOTA2#conf t
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp pool BOG2
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)#ip dhcp pool BOG3
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

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

```
BOGOTA3>enable
BOGOTA3#config t
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```

Figura 28. Habilitación directa DHCP en la PC3

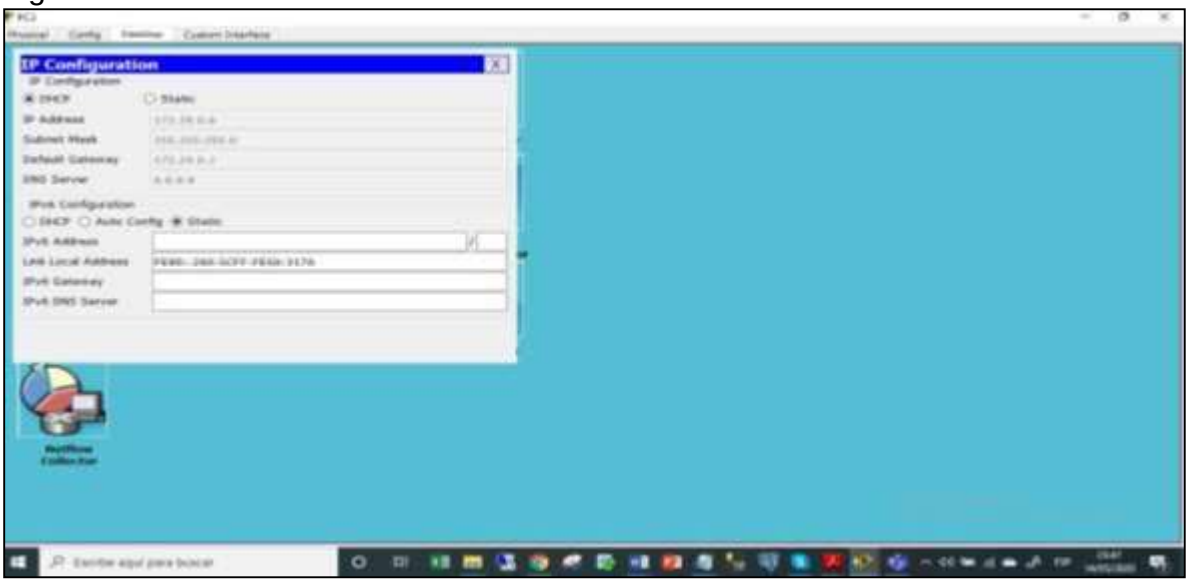
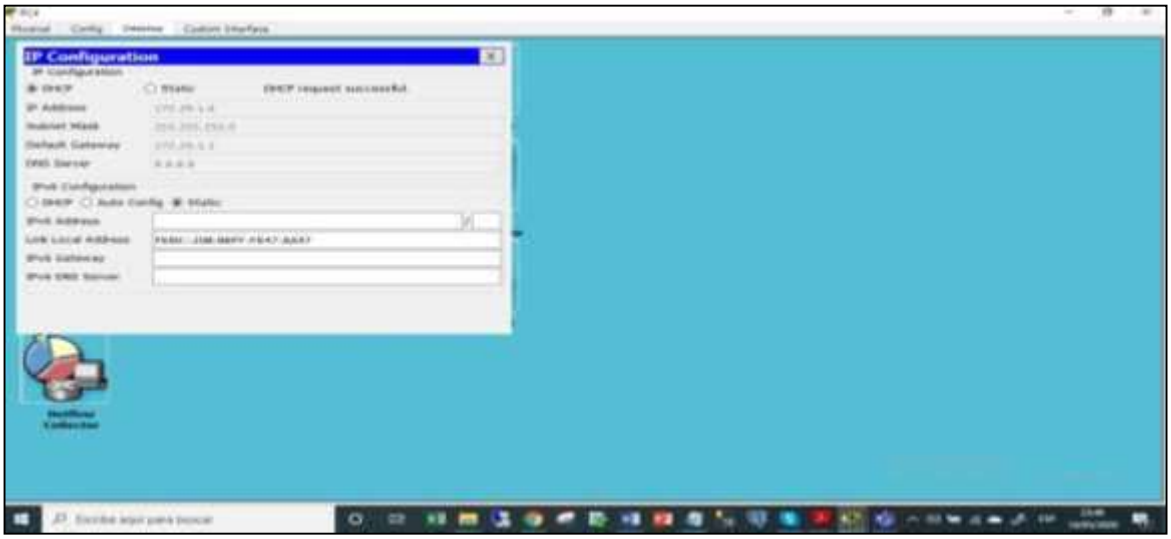


Figura 29. Habilitación directa DHCP en la PC4



CONCLUSIONES

Una adecuada configuración en el diseño de la topología de red, permite garantizar la seguridad, la disponibilidad y la confidencialidad en el tráfico de datos, es por ello que es necesario implementar los protocolos de seguridad y comunicación óptimos que logren contribuir con los pilares fundamentales en la arquitectura tecnológica y minimicen los riesgos y vulnerabilidades.

Es importante destacar que a través del servidor DHCP es posible asignar direcciones IP dinámicas a los dispositivos que están dentro de la red.

Con la implementación de las listas de acceso(ACL), es posible que los router logren identificar y filtrar el tráfico de red, controlando el flujo de paquetes que entran y salen.

Implementar los políticas y protocolos de Seguridad y control de las redes, hacen posible cumplir con los estándares requeridos de confiabilidad y disponibilidad para preservar los sistemas de información.

En el diseño de una topología de red es fundamental determinar a cuáles dispositivos se les puede permitir la comunicación y el tipo de tráfico a ser intercambiado, denegando el tráfico no requerido y autorizando el necesario.

Como Profesionales de Tecnología se hace necesario la formación y capacitación permanente en herramientas y lineamientos que permitan cada vez más fortalecer los Sistemas, la infraestructura tecnológica y por ende la información de las Organizaciones.

BIBLIOGRAFIA

CISCO. CCNA Exploration. Conceptos y protocolos de enrutamiento. Cuarta version. México. CISCO NETWORKING ACADEMY, 2011.

DI TOMMASO, Leandro. “configuración de VLANS con CISCO: Micro Ways” {En línea}. {6 agosto de 2009} disponible en: (https://www.mikroways.net/2009/08/05/configuracion-de-vlans-con-cisco/)

LÓPEZ BULLA, Ricardo. “Enrutamiento y configuración de redes: Fundación Universitaria del Área Andina” {En línea}. {10 septiembre de 2018} disponible en: (https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACI%C3%93N%20DE%20REDES.pdf?sequence=1&isAllowed=y)

ORACLE. “Glosario de términos de redes” {En línea}. {1 julio de 2014} disponible en: https://docs.oracle.com/cd/E56339_01/html/E53820/gnchw.html

PRIETO FERNANDEZ, Raúl. “Enrutamiento dinámico OSPF con Packet Tracer: My Blog” {En línea}. {20 agosto de 2016} disponible en: (https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer)

SIGNIFICADOS. "Significados.com” {En línea}. {22 mayo de 2016} disponible en: https://www.significados.com/switch/