

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS  
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JOSE GABRIEL RIBON ZARCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS  
INGENIERÍA DE SISTEMAS  
PUERTO COLOMBIA, ATLÁNTICO  
2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS  
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JOSE GABRIEL RIBON ZARCO

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

ASESOR  
GUSTAVO ADOLFO RODRIGUEZ  
DOCENTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS  
INGENIERÍA DE SISTEMAS  
PUERTO COLOMBIA, ATLÁNTICO  
2020

## TABLA DE CONTENIDOS

<b>RESUMEN</b> .....	8
<b>ABSTRACT</b> .....	10
<b>GLOSARIO</b> .....	11
<b>INTRODUCCIÓN</b> .....	12
<b>OBJETIVOS</b> .....	13
<b>1 DESARROLLO DEL ESCENARIO 1</b> .....	14
1.1 Inicializar dispositivos .....	15
1.1.1 Inicializar y volver a cargar los routers y los switches .....	15
1.2 Configurar los parámetros básicos de los dispositivos .....	15
1.2.1 Configurar la computadora de Internet.....	15
1.2.2 Configuración de R1.....	16
1.2.3 Configuración de R2.....	16
1.2.4 Configuración de R3.....	18
1.2.5 Configuración S1 .....	19
1.2.6 Configuración S3.....	20
1.2.7 Verificación de la conectividad de la red .....	20
1.3 Configuración de seguridad del Switch, las VLAN y el routing entre VLAN .....	22
1.3.1 Configuración S1 .....	22
1.3.2 Configuración S3.....	23
1.3.3 Configuración R1.....	24
1.3.4 Verificar la conectividad de la red.....	25
1.4 Configuración del protocolo de routing dinámico RIPv2 .....	28
1.4.1 Configuración RIPv2 en R1 .....	28
1.4.2 Configuración del protocolo RIPv2 en R2.....	28
1.4.3 Configuración del protocolo RIPv2 en R3.....	29
1.4.4 Verificación de la información de RIP.....	29
1.5 Implementación DHCP y NAT para IPv4 .....	33
1.5.1 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23	33
1.5.2 Configuración de la NAT estática y dinámica en el R2.....	33
1.5.3 Verificación del protocolo DHCP y la NAT estática .....	34

1.6	Configuración NTP .....	36
1.7	Configuración y verificación de las listas de control de acceso (ACL) .....	36
1.7.1	Restricción del acceso a las líneas VTY en el R2 .....	37
1.7.2	Verificación de las listas de control de acceso (ACL) .....	37
<b>2</b>	<b>DESARROLLO DEL ESCENARIO 2 .....</b>	<b>40</b>
2.1	Configuración del enrutamiento .....	48
2.1.1	Configuración de enrutamiento OSPF .....	48
2.1.2	Configuración de ruta ISP .....	51
2.2	Tabla de enrutamiento .....	51
2.3	Deshabilitar la propagación del protocolo OSPF .....	55
2.3.1	Deshabilitación propagación del protocolo OSPF en BOGOTA2 .....	56
2.3.2	Deshabilitación propagación del protocolo OSPF en BOGOTA3 .....	56
2.3.3	Deshabilitación propagación del protocolo OSPF en MEDELLIN2.....	56
2.3.4	Deshabilitación propagación del protocolo OSPF en MEDELLIN3.....	57
2.4	Verificación del Protocolo OSPF .....	57
2.5	Configuración de Encapsulamiento y Autenticación PPP.....	62
2.5.1	Enlace MEDELLÍN1 con ISP con autenticación PAP .....	62
2.5.2	Enlace BOGOTÁ1 con ISP con autenticación CHAP .....	63
2.6	Configuración de PAT.....	63
2.6.1	Configuración de NAT .....	63
2.6.2	Configuración de NAT en BOGOTÁ1 .....	65
2.7	Configuración del Servicio DHCP .....	68
2.7.1	Configuración servidor DHCP Medellín.....	68
2.7.2	Configuración de la red BOGOTA servidor DHCP .....	70
	<b>Anexo .....</b>	<b>72</b>
	<b>Conclusiones .....</b>	<b>73</b>
	<b>Bibliografía .....</b>	<b>74</b>

## LISTA DE TABLAS

Tabla 1. Verificación de conectividad.....	20
Tabla 2. Verificando la conectividad entre los switches y R1 .....	25
Tabla 3. Verificación de la información de RIP.....	29
Tabla 4. Comandos para verificación de ACL.....	37
Tabla 5. Interfaces que no requieren desactivación.....	56

## LISTA DE GRAFICAS

Figura 1.Topología de Red Escenario 1.....	14
Figura 2. Ping desde R1 a R2 S0/0/0.....	21
Figura 3. Ping desde R2 a R3 S0/0/1.....	21
Figura 4.Ping desde PC de Internet a Gateway Predeterminado.....	22
Figura 5.Ping desde S1 a R1 VLAN 99.....	26
Figura 6.Ping desde S3 a R1 VLAN 99.....	26
Figura 7. Ping desde S1 a R1 VLAN 21.....	27
Figura 8.Ping desde S3 a R1 VLAN 23.....	27
Figura 9. Verificación de comando show ip protocols.....	30
Figura 10.Verificación de comando show ip route rip.....	31
Figura 11. Verificación de Comando Show ip protocols en R3.....	31
Figura 12. Verificación de comando show ip protocols-Show ip route rip R2.....	32
Figura 13. Verificación de comando Show ip route rip en R3.....	32
Figura 14. Verificación de información de DHCP en PC-A.....	34
Figura 15. Verificación de información de DHCP en PC-C.....	35
Figura 16. Ping de PCA a PC-C.....	35
Figura 17.Accediendo al servidor web.....	36
Figura 18.Verificación de ACL en R2.....	38
Figura 19. Aplicación del comando show ip interface.....	39
Figura 20.Aplicación del comando show ip nat translations.....	39
Figura 21. Topología de red Escenario 2.....	40
Figura 22. Redes resumizadas.....	51
Figura 23. Tabla de enrutamiento ISP.....	52
Figura 24.Tabla de enrutamiento MEDELLIN1.....	52
Figura 25. Tabla de enrutamiento BOGOTA1.....	53
Figura 26. Tabla de enrutamiento BOGOTA2.....	53
Figura 27. Tabla de enrutamiento MEDELLIN2.....	54
Figura 28. Tabla de enrutamiento MEDELLIN 3.....	54
Figura 29. Tabla de enrutamiento BOGOTA3.....	55
Figura 30. Verificación de OSPF para MEDELLIN1.....	57
Figura 31. Verificación de OSPF para BOGOTA1.....	58
Figura 32. Verificación de OSPF para ISP.....	58
Figura 33. Verificación de OSPF para MEDELLIN1.....	59
Figura 34. Verificación de OSPF para BOGOTA1.....	60
Figura 35. Verificación de OSPF para MEDELLIN2.....	60
Figura 36. Verificación de OSPF para BOGOTA2.....	61
Figura 37. Verificación de OSPF para MEDELLIN3.....	61
Figura 38. Verificación de OSPF para BOGOTA3.....	62
Figura 39. Ping de PC1 a PC3.....	64

Figura 40. Evidencia de NO conexión de Extremo a Extremo .....	64
Figura 41. Configuración de PAT en MEDELLIN1 .....	65
Figura 42. Ping de PC3 a ISP posterior a NAT .....	66
Figura 43. Traducción de direcciones en BOGOTA1 .....	67
Figura 44. Ping de PC2 a ISP después de NAT .....	67
Figura 45. Habilitación de DHCP en la PC2.....	69
Figura 46. Habilitación DHCP en PC1 .....	70
Figura 47. Habilitación DHCP en PC3 .....	71
Figura 48. Habilitación DHCP en PC4 .....	71

## RESUMEN

Actualmente la importancia que representan las telecomunicaciones para toda organización ha hecho que se diseñen arquitecturas de red cada vez más fiables y seguras garantizando la interconectividad, así como la seguridad, disponibilidad y productividad, es por ello que como Profesionales de Tecnología se hace cada vez más necesario afianzar los conocimientos, comprender el óptimo funcionamiento de los dispositivos que intervienen en las arquitecturas de red, las políticas de seguridad y los diferentes protocolos que hacen posible la comunicación a gran escala de manera segura y óptima.

Apoyados en la herramienta de simulación PACKET TRACER, de CISCO Networking Academy, se lleva a la práctica los conocimientos a través del desarrollo de dos escenarios, en el escenario uno, se realiza la configuración de una red pequeña, que permite la conectividad IPv4 e IPv6, implementando 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 corresponde a la arquitectura de red de una Empresa que posee sucursales distribuidas en diferentes Ciudades, que requiere la administración de la red, configuración direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman



parte de la topología de red, encapsulamiento y autenticación PPP, implementación de protocolo OSPF, Configuración de PAP y Configuración de DHCP.

## ABSTRACT

Currently, the importance of telecommunications for the entire organization has led to the design of increasingly reliable and secure network architectures guaranteeing interconnectivity, as well as security, availability and productivity, which is why as Technology Professionals it is increasingly more it is necessary to strengthen the knowledge, understand the optimal functioning of the devices that intervene in the network architectures, the security policies and the different protocols that make possible the communication on a large scale in a safe and optimal way.

Supported by the simulation tool PACKET TRACER, from CISCO Networking Academy, the knowledge is put into practice through the development of two scenarios, in scenario one, the configuration of a small network is carried out, which allows IPv4 and IPv6 connectivity , implementation of protocols for: Switch security, routing between VLANs, dynamic RIPv2, configuration of dynamic hosts (DHCP, dynamic and static network address translation (NAT), access control lists (ACL) and the protocol of Network time (NTP) server / client The second scenario corresponds to the network architecture of a Company that has branches distributed in different Cities, which requires network administration, IP address configuration, routing protocols and other aspects that They are part of the network topology, PPP encapsulation and authentication, OSPF protocol implementation, PAP configuration and DHCP configuration.

## GLOSARIO

**RIP:** Es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados.

**OSPF:** camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

**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.

**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.

## INTRODUCCIÓN

Teniendo en cuenta que uno de los factores más importantes en el diseño de una red es brindar seguridad y confianza. Esta seguridad se basa en el modelo de red construido, en los parámetros establecidos en cada uno de los dispositivos interconectados, permitiendo la comunicación necesaria y denegando la no requerida, filtrando el tráfico de red a través del enrutamiento seguro y aprovechando al máximo los recursos de la infraestructura tecnológica.

La Finalidad del presente trabajo es afianzar los conocimientos adquiridos durante el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), estos conocimientos son llevados a la práctica mediante la herramienta de Simulación PACKET TRACER haciendo posible incorporar las temáticas aprendidas en la configuración de los dispositivos de red, alistamiento, configuración de seguridad, conexiones físicas entre equipos e implementando los diferentes protocolos de enrutamiento: RIPV2, DHCP y listas de control ACL.

## OBJETIVOS

### OBJETIVO GENERAL

Utilizar herramientas de Simulación para el desarrollo de escenarios que permitan poner en práctica los conocimientos y habilidades adquiridos en el diseño e implementación de soluciones integradas LAN / WAN.

### OBJETIVOS ESPECÍFICOS

- Realizar el diseño de la topología de red según los escenarios propuestos.
- Configurar los dispositivos que conforman la topología de red para lograr la interconectividad entre los mismos.
- Implementar los protocolos routing dinámico RIPv2, de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.
- Implementar políticas de seguridad en los dispositivos.
- Realizar análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.
- Identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS.

## DESARROLLO DEL ESCENARIO 1

### Topología de Red.

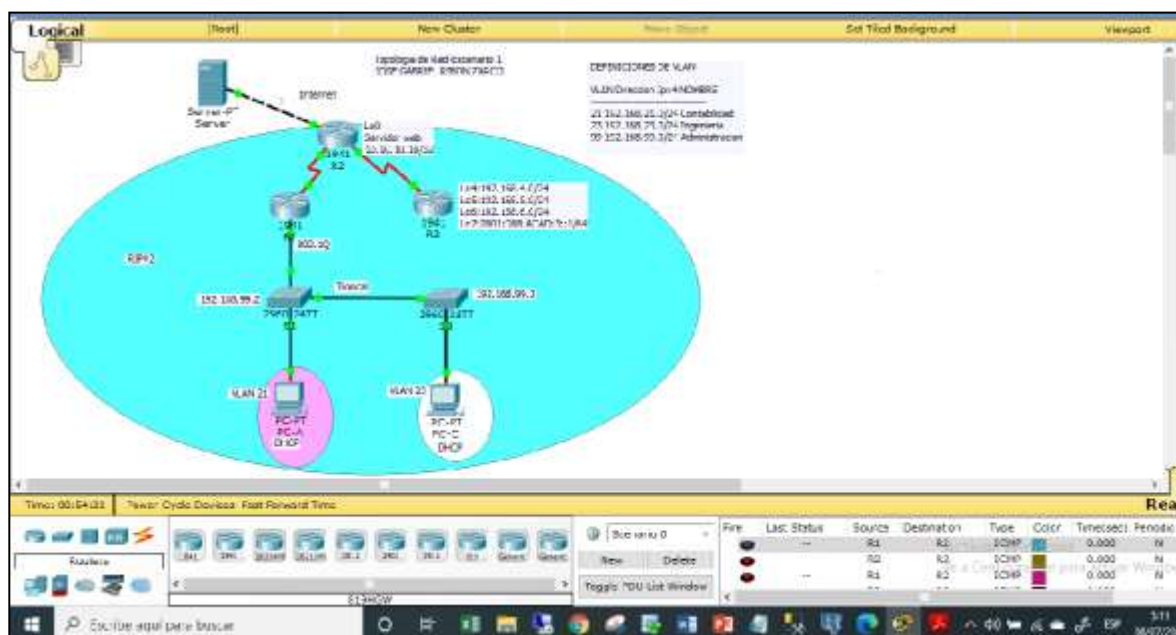
Basado en el escenario propuesto se procede a realizar el Diseño de la Topología de una pequeña red en la herramienta packet tracer, diseño que de acuerdo a los requerimientos solicitados en el escenario debe permitir la conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

Para el Diseño de la Topología de red, se requirió el uso de los siguientes dispositivos:

- 3 routers tipo 1941, conectados mediante cable serial DCE.
- 1 servidor Server-PT, conectado al router 2 mediante cable cruzado.
- 2 Switches Tipo 2960
- 2 PC conectados mediante cable directo a los Switches

En cada uno de los router se adicionan módulos para puertos seriales adicionales acorde al requerimiento de red.

Figura 1. Topología de Red Escenario 1



Diseño propio

## 1.1 Inicializar dispositivos

### 1.1.1 Inicializar y volver a cargar los routers y los switches

Se procede a inicializar los dispositivos a través de la ejecución del comando **erase startup-config** en cada uno de los routers para dar inicio a la configuración propuesta en el escenario 1. Así mismo en los Switches se ejecuta el mismo comando y adicional se elimina la base de datos de la VLAN a través del comando **delete vlan.dat**, realizando la respectiva verificación en cada uno de los switches que la base de datos de VLAN no se encuentre en la memoria flash. Posteriormente se ejecuta el comando reload para cargar los dispositivos.

```
Router>enable
Router#erase startup-config
Router#reload
Switch>enable
Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload
Switch>enable
Switch#show flash
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)
```

## 1.2 Configurar los parámetros básicos de los dispositivos

### 1.2.1 Configurar la computadora de Internet

Se ingresa a la configuración física del servidor de internet y se establecen los parámetros de acuerdo a las siguientes especificaciones:

- 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

### 1.2.2 Configuración de R1

Se realiza la configuración básica de seguridad, se asignan el nombre de acuerdo a la topología (R1) se desactiva la búsqueda DNS, se asigna la contraseña de acceso privilegiado: class, de consola y telnet: cisco, se crea el mensaje de acceso no autorizado para garantizar la seguridad en el dispositivo.

A continuación, se describen los comandos que permiten establecer las políticas de configuración básica de seguridad.

```
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!#
```

Se establece el direccionamiento IPv4 e IPv6, la frecuencia de reloj y se activa la interfaz. Así mismo se procede a configurar los puertos seriales y las rutas predeterminadas.

### 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
```

### 1.2.3 Configuración de R2



Se realiza la configuración básica de seguridad, se asignan el nombre de acuerdo a la topología (R2) se desactiva la búsqueda DNS, se asigna la contraseña de acceso privilegiado: class, de consola y telnet: cisco, se crea el mensaje de acceso no autorizado para garantizar la seguridad en el dispositivo.

A continuación, se describen los comandos que permiten establecer las políticas de configuración básica de seguridad.

```
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 prohibited!#
```

Se solicita habilitar el servidor HTTP, pero este comando no es aceptado por packet tracer

```
R2(config)#ip http server (Comando no aceptado por packet tracer)
```

Se establece el direccionamiento IPv4 e IPv6, la frecuencia de reloj y se activa la interfaz. Así mismo se procede a configurar los puertos seriales y las rutas predeterminadas.

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
```

Configuración 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
```

Se establece la dirección IPv4 para Interfaz loopback 0 (servidor web simulado)

```
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
```

#### 1.2.4 Configuración de R3

Se realiza la configuración básica de seguridad, se asignan el nombre de acuerdo a la topología (R3) se desactiva la búsqueda DNS, se asigna la contraseña de acceso privilegiado: class, de consola y telnet: cisco, se crea el mensaje de acceso no autorizado para garantizar la seguridad en el dispositivo.

A continuación, se describen los comandos que permiten establecer las políticas de configuración básica de seguridad.

```
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!#
```

Se establece el direccionamiento IPv4 e IPv6, la frecuencia de reloj y se activa la interfaz. Así mismo se procede a configurar los puertos seriales y las rutas predeterminadas.

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
```

Se establecen las direcciones ipv4 para las Interfaces loopback 4,5 y 6 utilizando las primeras direcciones disponibles en cada subred

```
R3(config)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
```

Se establece la dirección ipv6 para la Interfaz loopback 7 utilizando la primera dirección disponible en la subred

```
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
```

### 1.2.5 Configuración S1

Se realizan las configuraciones básicas de seguridad, se asignan el nombre de acuerdo a la topología (S1), se desactiva la búsqueda DNS, se asignan las contraseñas de acceso privilegiado: class, de consola y telnet: cisco, se crea el mensaje de acceso no autorizado.

```
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!#

```

### 1.2.6 Configuración S3

Se realizan las configuraciones básicas de seguridad, se asignan el nombre de acuerdo a la topología (S3), se desactiva la búsqueda DNS, se asignan las contraseñas de acceso privilegiado: class, de consola y telnet: cisco, se crea el mensaje de acceso no autorizado.

```

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!#

```

### 1.2.7 Verificación de la conectividad de la red

Haciendo uso del comando **ping** se procede a verificar la conectividad de la red, según los requerimientos y resultados descritos en la siguiente tabla.

Tabla 1.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

```
R1
Physical Config CLI
IOS Command Line Interface
no up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.22, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.25, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Unauthorized Access is prohibited!
User Access Verification
Password:
R1>enable
Password:
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/27 ms
R1#
```

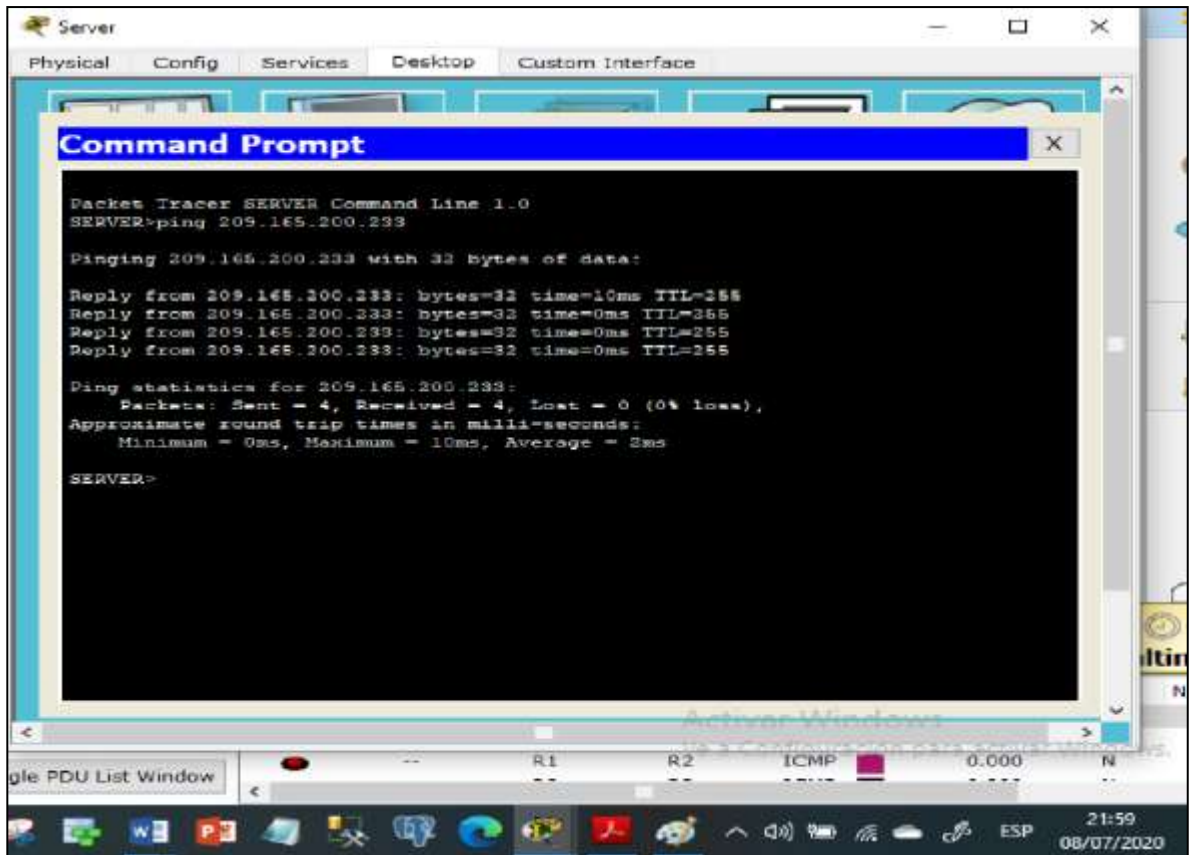
Diseño Propio

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

```
R2
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Unauthorized Access is prohibited!
User Access Verification
Password:
R2>enable
Password:
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms
R2#
```

Diseño Propio

Figura 4. Ping desde PC de Internet a Gateway Predeterminado



Diseño Propio

### 1.3 Configuración de seguridad del Switch, las VLAN y el routing entre VLAN

#### 1.3.1 Configuración S1

Teniendo en cuenta la tabla de equivalencias de VLAN propuesta para la topología de red, se procede a realizar la creación y nombramiento de cada una de las VLAN que se indican en el escenario.

```
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
```

Se Procede con la asignación de la dirección IP de administración, configurando la primera dirección IPv4 de la subred como el gateway predeterminado.

```
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 y finalmente apagar todos los puertos sin usar.

```
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
```

### 1.3.2 Configuración S3

Creación y nombramiento de cada una de las VLAN, según la tabla de equivalencias de la Topología.

```
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
```

Asignación de la dirección IP a la VLAN de administración

```
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
```

Asignación de la primera dirección IP en la subred como gateway predeterminado.

```
S3(config)#ip default-gateway 192.168.99.1
```

Configuración de la red VLAN 1 como VLAN nativa

```
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, apagando todos los puertos sin usar.

```
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
```

### 1.3.3 Configuración R1

Las siguientes tareas se configuran en R1:

Configuración de la subinterfaz 802.1Q .21 en G0/1, asignando la primera dirección disponible a la VLAN 21, LAN de Contabilidad, configuración de la subinterfaz 802.1Q .23 en G0/1, asignando la primera dirección disponible a la VLAN 23, LAN de Ingeniería, configuración de la subinterfaz 802.1Q .99 en G0/1 asignando la primera dirección disponible a la VLAN 99, LAN de Administración y finalmente se activa la interfaz 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
```



```

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

```

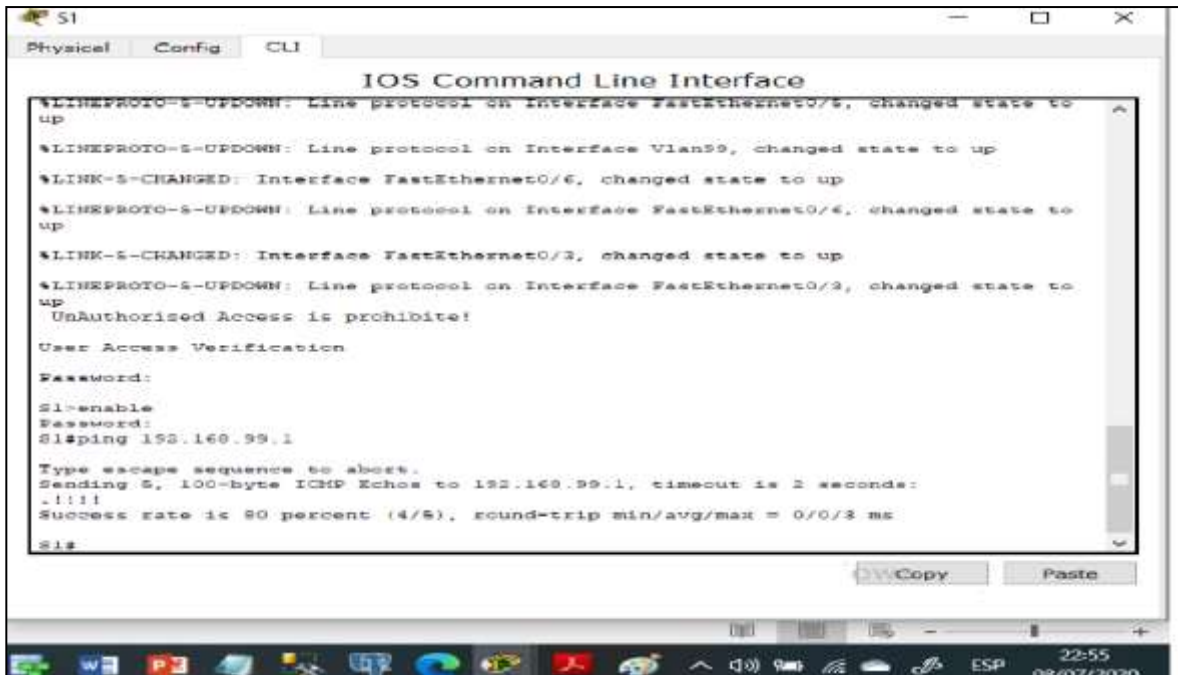
#### 1.3.4 Verificar la conectividad de la red

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

Tabla 2.Verificando la conectividad entre los 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 desde S1 a R1 VLAN 99



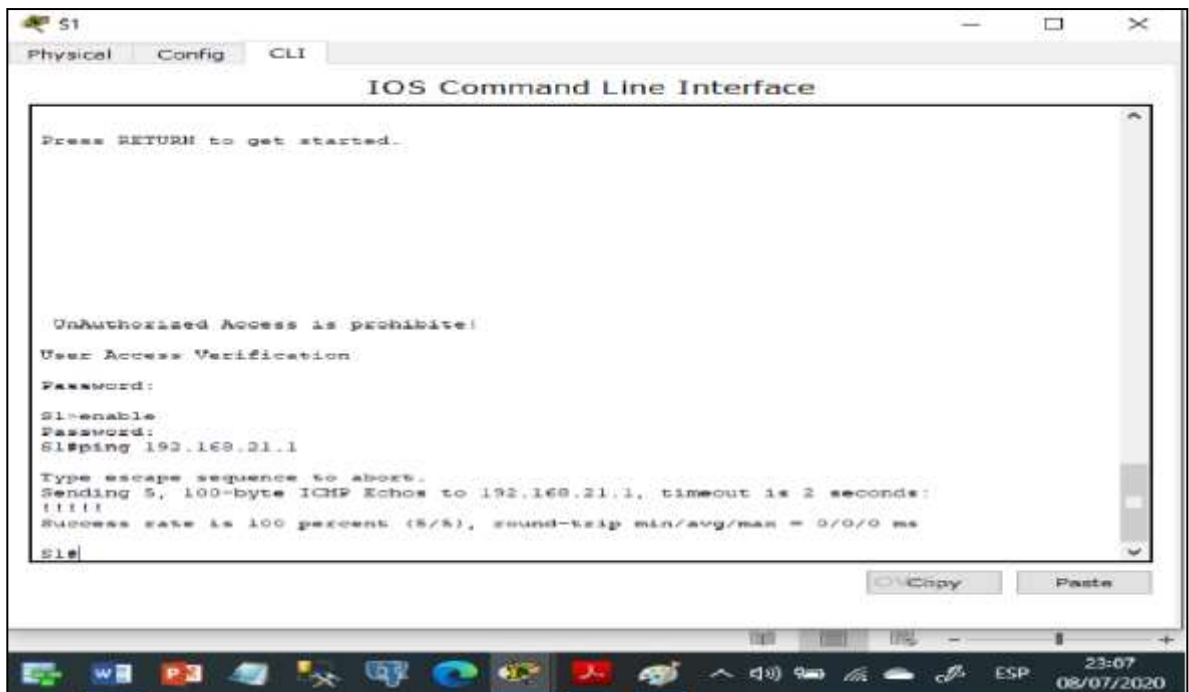
Diseño Propio

Figura 6. Ping desde S3 a R1 VLAN 99



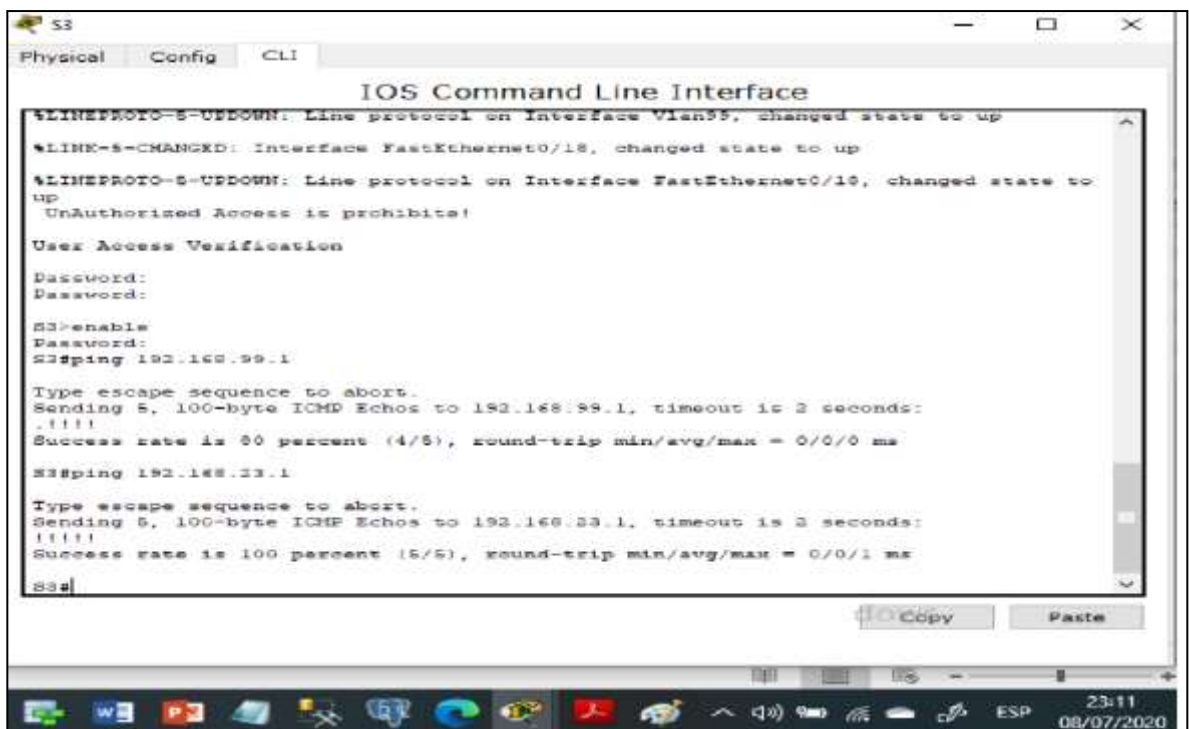
Diseño Propio

Figura 7. Ping desde S1 a R1 VLAN 21



Diseño Propio

Figura 8. Ping desde S3 a R1 VLAN 23



Diseño Propio

## 1.4 Configuración del protocolo de routing dinámico RIPv2

### 1.4.1 Configuración RIPv2 en R1

```
R1>enable
R1#config t
R1(config)#router rip
R1(config-router)#version 2
```

Determinando 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 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
```

### 1.4.2 Configuración del protocolo RIPv2 en R2

Configuración del protocolo RIPv2 en R2

```
R2>enable
R2#config t
R2(config)#router rip
R2(config-router)#version 2
```

Determinando 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
```

### 1.4.3 Configuración del protocolo RIPv2 en R3

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

Determinando 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 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
```

### 1.4.4 Verificación de la información de RIP

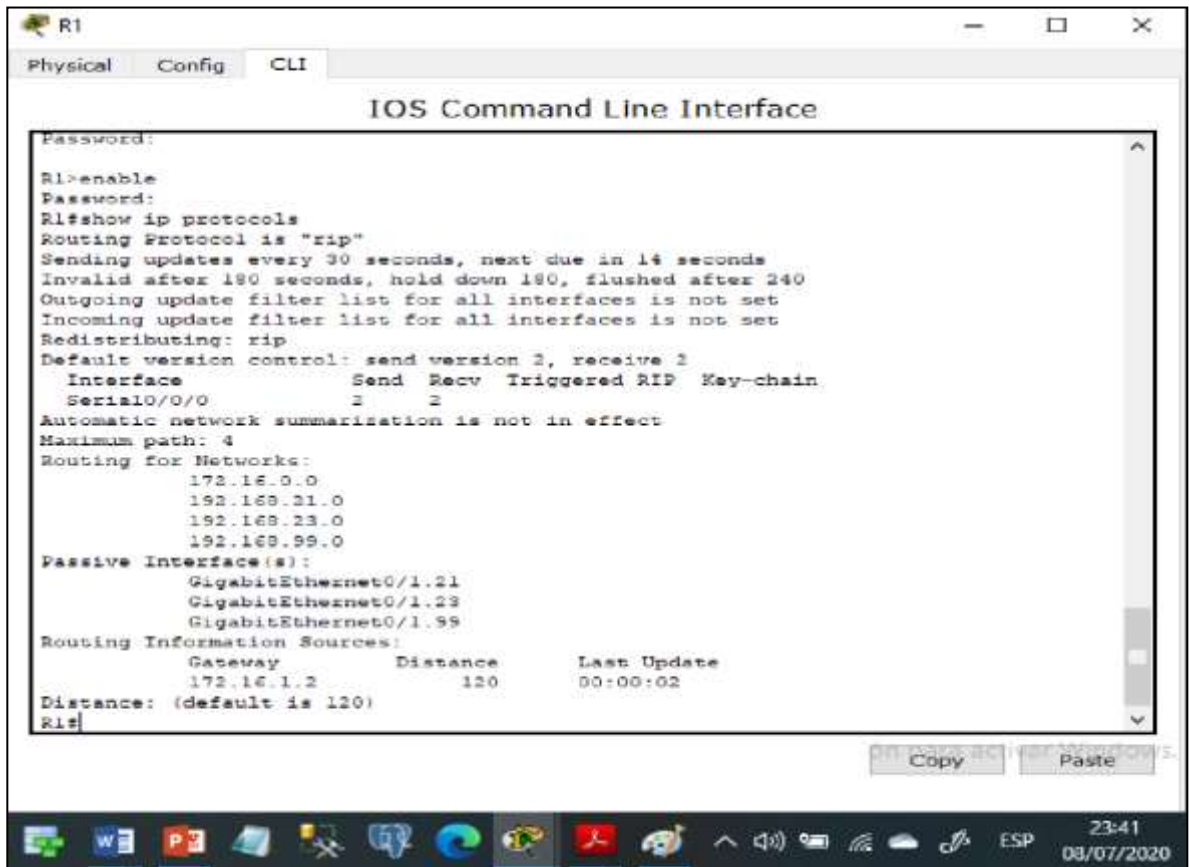
Para la verificación de la información del Protocolo RIP se utilizan los comandos: show ip protocols, show ip route rip y Show | run section router rip, descritos en la siguiente tabla:

Tabla 3. Verificación de la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso	show ip protocols

RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	
¿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

Figura 9. Verificación de comando show ip protocols



Diseño Propio

Figura 10. Verificación de comando show ip route rip

```
IOS Command Line Interface
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
Interface      Send Recv Triggers RIP Key-chain
Serial0/0/0    2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.16.0.0
 192.168.21.0
 192.168.23.0
 192.168.99.0
Passive Interface(s):
 GigabitEthernet0/1.21
 GigabitEthernet0/1.23
 GigabitEthernet0/1.25
Routing Information Sources:
 Gateway      Distance    Last Update
 172.16.1.2   120         00:00:02
Distance: (default is 120)
R1#show ip route rip
10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10 [120/1] via 172.16.1.2, 00:00:15, Serial0/0/0
R   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R   172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:15, Serial0/0/0
R   192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:15, Serial0/0/0
R   192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:15, Serial0/0/0
R   192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:15, Serial0/0/0
R   192.168.25.0/24 is variably subnetted, 2 subnets, 2 masks
```

Diseño Propio

Figura 11. Verificación de Comando Show ip protocols en R3

```
IOS Command Line Interface
Password:
R3#enable
Password:
R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
Interface      Send Recv Triggers RIP Key-chain
Serial0/0/1    2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.16.0.0
 192.168.4.0
 192.168.5.0
 192.168.6.0
Passive Interface(s):
 Loopback4
 Loopback5
 Loopback6
Routing Information Sources:
 Gateway      Distance    Last Update
 172.16.2.2   120         00:00:24
R3#
```

Diseño Propio



Figura 12. Verificación de comando show ip protocols-Show ip route rip R2

```

R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 27 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 3, receive 2
Interface          Send Recv Triggered RIP Key-chain
Serial0/0/0         2      2
Serial0/0/1         2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.16.0.0
Passive Interface(s):
  Loopback0
Routing Information Sources:
  Gateway         Distance      Last Update
  172.16.2.1      120           00:00:04
  172.16.1.1      120           00:00:02
Distance: (default is 120)
R2#show ip route rip
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R   192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:20, Serial0/0/1
R   192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:20, Serial0/0/1
R   192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:20, Serial0/0/1
R   192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:18, Serial0/0/0, ...
  
```

Diseño Propio

Figura 13. Verificación de comando Show ip route rip en R3

```

R3#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R3#show ip route rip
  10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10 [120/1] via 172.16.2.2, 00:00:24, Serial0/0/1
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R   172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:24, Serial0/0/1
R   192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R   192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:24, Serial0/0/1
R   192.168.22.0/24 [120/2] via 172.16.2.2, 00:00:24, Serial0/0/1
R   192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:24, Serial0/0/1
  
```

Diseño Propio



## 1.5 Implementación DHCP y NAT para IPv4

### 1.5.1 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

Dentro de las tareas de configuración en R1 se realiza la reserva de direcciones para las VLAN, se crea el pool de DHCP para las VLAN 21 y VLAN 23 y se configurara la NAT estática y dinámica.

Reserva de 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 (Comando invalido en Packet tracer)
```

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 (Comando invalido en Packet tracer)
```

### 1.5.2 Configuración de la NAT estática y dinámica en el R2

Se procede a Crear la base de datos local con una cuenta de usuario y Habilitar el servicio del servidor HTTP y crear la NAT estática al servidor web.

```
R2>enable
R2#config t
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server (Comando invalido en Packet tracer)
R2(config)#ip http authentication local (Comando invalido en Packet tracer)
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
```

```

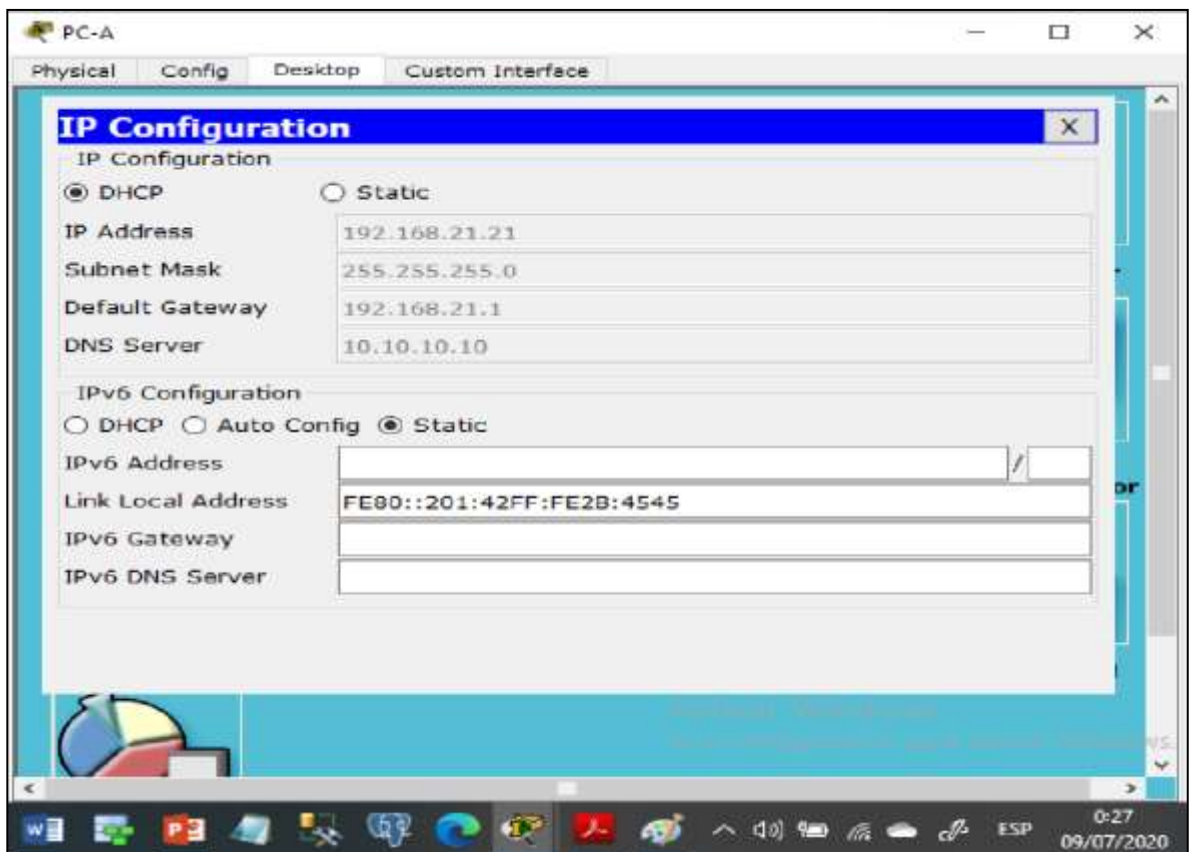
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
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

```

### 1.5.3 Verificación del protocolo DHCP y la NAT estática

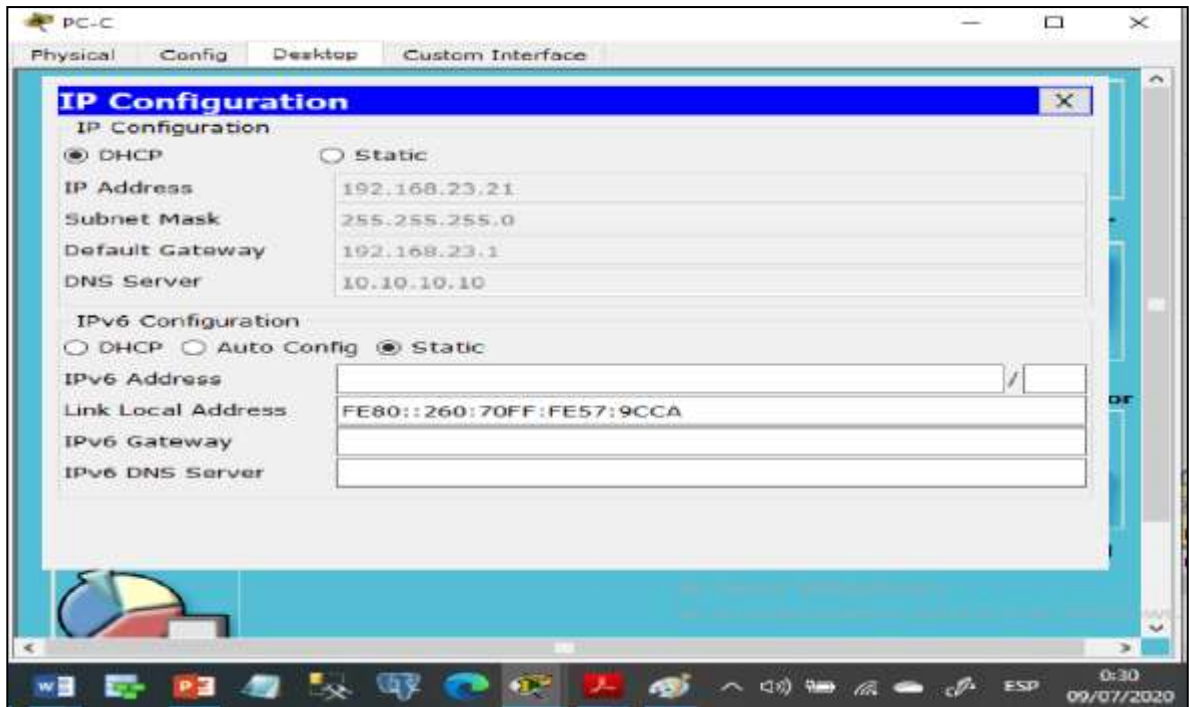
En el PC-A y en el PC-C se realiza la verificación que haya adquirido la IP del servidor DHCP, con resultados satisfactorios.

Figura 14. Verificación de información de DHCP en PC-A



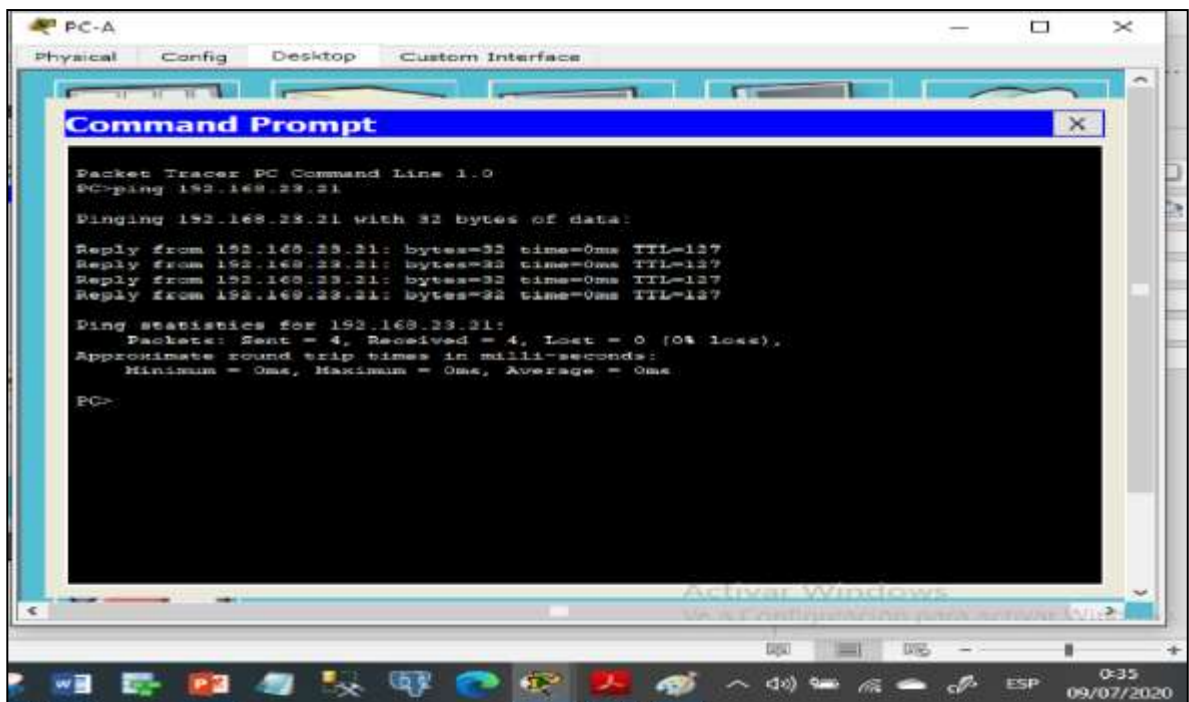
Diseño Propio

Figura 15. Verificación de información de DHCP en PC-C



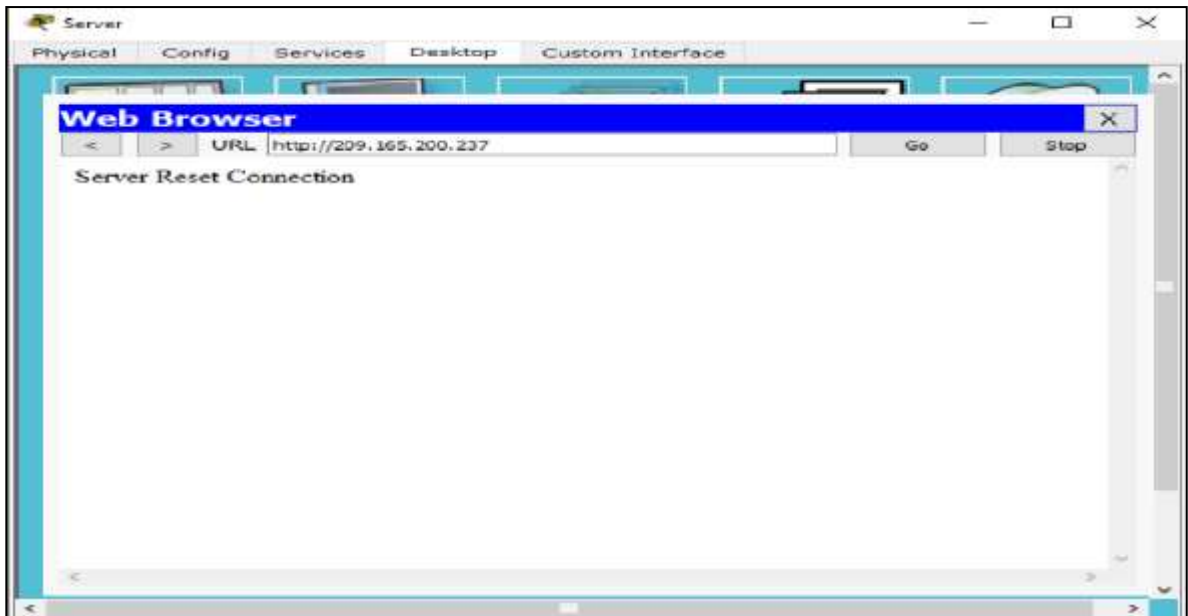
Diseño Propio

Figura 16. Ping de PCA a PC-C



Diseño Propio

Figura 17. Accediendo al servidor web



Diseño Propio

Desde Packet tracer no es posible realizar este procedimiento, porque, no soporto el comando Ip HTTP server en R2 para activar el Servidor web.

## 1.6 Configuración NTP

Ajustando la fecha y hora en R2

```
R2>enable
R2#clock set 20:02:00 7 jun 2020
R2#config t
R2(config)#ntp master 5(Comando invalido en Packet tracer)
```

Configurando 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
```

Verificando la configuración de NTP en R1

```
R1#show ntp associations(Comando invalido en Packet tracer)
```

## 1.7 Configuración y verificación de las listas de control de acceso (ACL)

### 1.7.1 Restricción del acceso a las líneas VTY en el R2

Configurando la lista de acceso con nombre para permitir que solo R1 establezca conexión Telnet con R2 y aplicación de ACL con nombre a las líneas VTY.

```
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
R1#telnet 172.16.1.2
R3>enable
R3#telnet 172.16.1.2
```

### 1.7.2 Verificación de las listas de control de acceso (ACL)

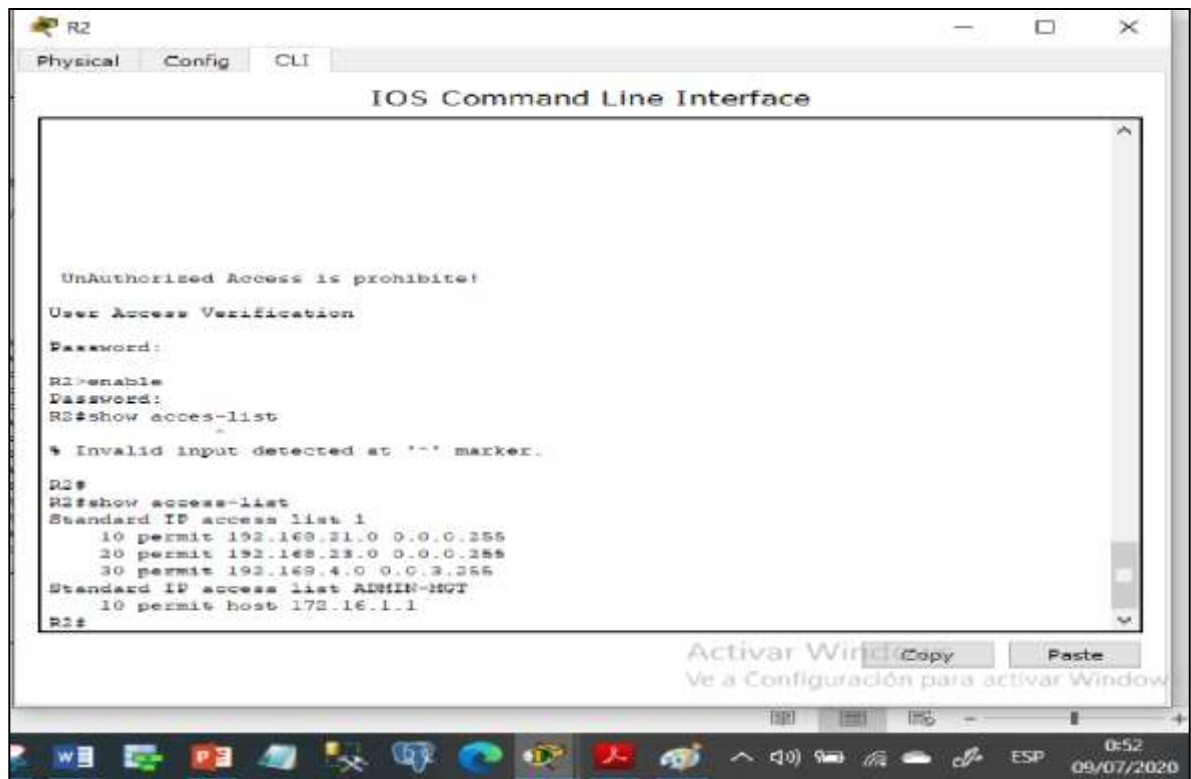
En la Siguiete tabla se muestran los comandos utilizados para la verificación de las listas permitidas en cada uno de los router.

Tabla 4. 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 R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters(Comando invalido en Packet tracer)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * R2#show ip nat translation

Figura 18.Verificación de ACL en R2



Diseño Propio

Figura 19. Aplicación del comando show ip interface



Diseño Propio

Figura 20. Aplicación del comando show ip nat translations



Diseño Propio



## DESARROLLO DEL ESCENARIO 2

### Topología de Red

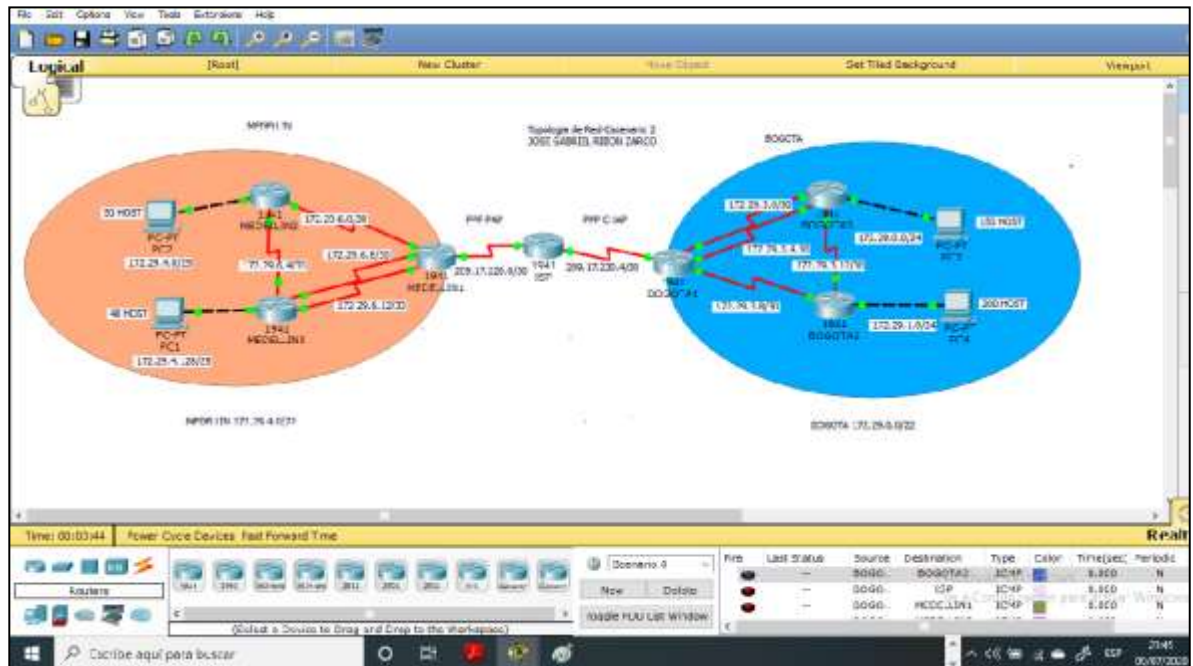
Se procede a realizar el Diseño de la Topología de red en la herramienta de simulación packet tracer, basado en el planteamiento del escenario 2, correspondiente a una Empresa que posee sucursales distribuidas en las ciudades de Bogotá y Medellín.

Para el Diseño de la Topología de red, se requirió el uso de los siguientes dispositivos:

- 7 routers tipo 1941, conectados mediante cable serial DCE.
- 4 PCS (2 por cada Ciudad), conectados a los router mediante cable cruzado (Cooper Cross-Over).

Se da inicio con la ubicación y la conexión física de los dispositivos, según escenario presentado, listos para realizar la configuración de acuerdo a los lineamientos establecidos, en este escenario se debe implementar el protocolo de enrutamiento OSPF con rutas por defecto distribuidas, asimismo, habilitar el encapsulamiento PPP y su autenticación. De acuerdo a los requerimientos en los router se adicionaron módulos con puerto serial para permitir la conexión en los casos que sea necesario.

Figura 21. Topología de red Escenario 2



Diseño Propio



Se procede a realizar las configuraciones básicas de cada uno de los routers (asignación nombres de equipos, asignación de claves de seguridad, etc). desactivación de la búsqueda DNS, contraseñas de acceso privilegiado, de consola y telnet, configuración de mensaje de prohibido de acceso no autorizado. Así mismo se configuran los puertos seriales para permitir la conectividad entre los diferentes dispositivos y las rutas predeterminadas, según Topología de red.

Las siguientes configuraciones permiten establecer la seguridad de la arquitectura de red.

### 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 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 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 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 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 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 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
```

Se procede a realizar las configuraciones de las interfaces seriales, asignando el direccionamiento IP, determinando la mascara de red y la velocidad de envio de datos, para establecer la conectividad entre los diferentes dispositivos.

#### Configuración de interfaces seriales del Router ISP

##### 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
```

#### Configuración de interfaces seriales del Router MEDELLIN1

##### 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
```

Configuración de interfaces seriales del Router MEDELLIN2

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
```

Configuración de interfaces seriales del Router MEDELLIN3

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
```

Configuración de interfaces seriales del Router BOGOTA1

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
```

Configuración de interfaces seriales del Router BOGOTA2

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
```

Configuración de interfaces seriales del Router BOGOTA3

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 Configuración del enrutamiento

### 2.1.1 Configuración de enrutamiento OSPF

Según requerimiento del escenario, se procede a realizar la configuración de enrutamiento a través del protocolo OSPF versión 2, para lo cual se identifican las conexiones directas en cada uno de los routers para declarar la red principal, así mismo se desactiva la sumarización automática.

Configuración OSPF en el Router MEDELLIN1

```
MEDELLIN1>enable
MEDELLIN1#config t
```



```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN1(config-router)#exit
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#no auto-summary
```

#### Configuración OSPF en el Router MEDELLIN2

```
MEDELLIN2>enable
MEDELLIN2#config t
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 1
MEDELLIN2(config-router)#default-information originate
MEDELLIN2(config-router)#no auto-summary
```

#### Configuración OSPF en el Router MEDELLIN3

```
MEDELLIN3>enable
MEDELLIN3#config t
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 1
MEDELLIN3(config-router)#default-information originate
MEDELLIN3(config-router)#no auto-summary
```

#### Configuración OSPF en el Router BOGOTA1

```
BOGOTA1>enable
BOGOTA1#config t
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA1(config-router)#exit
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#no auto-summary
```

## Configuración OSPF en el Router BOGOTA2

```
BOGOTA2>enable
BOGOTA2#config t
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 1
BOGOTA2(config-router)#default-information originate
BOGOTA2(config-router)#no auto-summary
```

## Configuración OSPF en el Router BOGOTA3

```
BOGOTA3>enable
BOGOTA3#config t
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 1
BOGOTA3(config-router)#default-information originate
BOGOTA3(config-router)#no auto-summary
```

En los routers Bogota1 y Medellín1 se agrega a su configuración de enrutamiento una ruta por defecto hacia el ISP y así mismo redistribuirla dentro de las publicaciones de OSPF.

```
MEDELLIN1>enable
MEDELLIN1#config t
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#exit
```

```
BOGOTA1>enable
BOGOTA1#config t
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 1
```

```

BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#exit

```

### 2.1.2 Configuración de ruta ISP

Teniendo en cuenta que el router ISP tiene comunicación directa con MEDELLIN1 y BOGOTA1, se configura una ruta estática dirigida hacia cada red interna de estos routers, para lo cual es necesario sumarizar las subredes de cada uno a /22.

```

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

```

Figura 22. Redes sumarizadas

		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	0	1	0	0	172.29.6.8/30
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	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	172.29.4.0/22	
RED BOGOTA1																		
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	0	1	1	0	172.29.3.12/30
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	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	0	1	0	172.29.3.4/30
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	172.29.0.0/22	

Diseño propio

### 2.2 Tabla de enrutamiento

Se verifica a través del comando show ip route la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas. Igualmente, por intermedio de estos comandos se puede observar el balanceo de carga de los routers.

Figura 23. Tabla de enrutamiento ISP

```

IOS Command Line Interface

User Access Verification

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

Gateway of last resort is not set

S    172.29.0.0/22 is subnetted, 2 subnets
S    172.29.0.0/22 [11/0] via 209.17.220.6
S    172.29.4.0/22 [11/0] via 209.17.220.3
C    209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C    209.17.220.0/30 is directly connected, Serial0/0/0
L    209.17.220.1/32 is directly connected, Serial0/0/0
C    209.17.220.2/32 is directly connected, Serial0/0/0
C    209.17.220.4/30 is directly connected, Serial0/0/1
L    209.17.220.5/32 is directly connected, Serial0/0/1
C    209.17.220.6/32 is directly connected, Serial0/0/1
ISP#
  
```

Diseño propio

Figura 24. Tabla de enrutamiento MEDELLIN1

```

MEDELLIN1 IOS Command Line Interface

MEDELLIN1>enable
Password:
MEDELLIN1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 209.17.220.1 to network 0.0.0.0

O    172.29.0.0/16 is variably subnetted, 9 subnets, 2 masks
O    172.29.4.0/25 [110/65] via 172.29.6.3, 01:01:16, Serial0/0/1
O    172.29.4.128/25 [110/65] via 172.29.6.10, 01:19:21, Serial0/1/0
C    172.29.6.0/30 is directly connected, Serial0/0/1
L    172.29.6.1/32 is directly connected, Serial0/0/1
O    172.29.6.4/30 [110/136] via 172.29.6.3, 01:30:44, Serial0/0/1
    [110/136] via 172.29.6.10, 01:20:44, Serial0/1/0
C    172.29.6.8/30 is directly connected, Serial0/1/0
L    172.29.6.9/32 is directly connected, Serial0/1/0
C    172.29.6.12/30 is directly connected, Serial0/1/1
L    172.29.6.13/32 is directly connected, Serial0/1/1
C    209.17.220.0/24 is variably subnetted, 3 subnets, 3 masks
C    209.17.220.0/30 is directly connected, Serial0/0/0
C    209.17.220.1/32 is directly connected, Serial0/0/0
L    209.17.220.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.1
MEDELLIN1#
  
```

Diseño propio

Figura 25. Tabla de enrutamiento BOGOTA1

```

BOGOTA1#enable
Password:
BOGOTA1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 209.17.220.5 to network 0.0.0.0

O    172.29.0.0/16 is variably subnetted, 5 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.3, 00:59:23, Serial0/1/0
O    172.29.1.0/24 [110/65] via 172.29.2.10, 01:05:42, Serial0/0/1
C    172.29.2.0/30 is directly connected, Serial0/1/0
L    172.29.3.1/32 is directly connected, Serial0/1/0
C    172.29.3.4/30 is directly connected, Serial0/1/1
L    172.29.3.5/32 is directly connected, Serial0/1/1
C    172.29.3.8/30 is directly connected, Serial0/0/1
L    172.29.3.9/32 is directly connected, Serial0/0/1
O    172.29.3.12/30 [110/128] via 172.29.3.2, 00:59:50, Serial0/1/0
    [110/128] via 172.29.3.10, 00:59:50, Serial0/0/1
C    209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C    209.17.220.4/30 is directly connected, Serial0/0/0
C    209.17.220.5/32 is directly connected, Serial0/0/0
L    209.17.220.6/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.17.220.5
BOGOTA1#
    
```

Diseño propio

Figura 26. Tabla de enrutamiento BOGOTA2

```

BOGOTA2#enable
Password:
BOGOTA2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 172.29.3.14 to network 0.0.0.0

O    172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.14, 01:04:57, Serial0/0/1
C    172.29.1.0/24 is directly connected, GigabitEthernet0/0
L    172.29.1.1/32 is directly connected, GigabitEthernet0/0
O    172.29.3.0/30 [110/128] via 172.29.3.5, 01:05:21, Serial0/0/0
    [110/128] via 172.29.3.14, 01:05:21, Serial0/0/1
O    172.29.3.4/30 [110/128] via 172.29.3.9, 01:05:21, Serial0/0/0
    [110/128] via 172.29.3.14, 01:05:21, Serial0/0/1
C    172.29.3.8/30 is directly connected, Serial0/0/0
L    172.29.3.10/32 is directly connected, Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
L    172.29.3.13/32 is directly connected, Serial0/0/1
O    209.17.220.0/20 is subnetted, 1 subnets
O    209.17.220.4/20 [110/128] via 172.29.3.9, 00:40:26, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.14, 01:04:42, Serial0/0/1
    [110/1] via 172.29.3.9, 00:38:32, Serial0/0/0
BOGOTA2#
    
```

Diseño propio



Figura 27. Tabla de enrutamiento MEDELLIN2

```

MEDELLIN2#enable
Password:
MEDELLIN2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        F - periodic downloaded static route

Gateway of last resort is 172.29.6.6 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/28 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
O       172.29.4.128/25 [110/65] via 172.29.6.6, 01:40:26, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.2/32 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.5/32 is directly connected, Serial0/0/1
O       172.29.6.8/30 [110/128] via 172.29.6.1, 01:41:56, Serial0/0/0
        [110/128] via 172.29.6.6, 01:41:56, Serial0/0/1
O       172.29.6.12/30 [110/128] via 172.29.6.1, 01:41:12, Serial0/0/0
        [110/128] via 172.29.6.6, 01:41:12, Serial0/0/1
O       209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.0/30 [110/120] via 172.29.6.1, 00:56:14, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.4, 01:40:07, Serial0/0/1
        [110/1] via 172.29.6.1, 00:52:37, Serial0/0/0
MEDELLIN2#
    
```

Diseño propio  
Figura 28. Tabla de enrutamiento MEDELLIN 3

```

MEDELLIN3#enable
Password:
MEDELLIN3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        D - periodic downloaded static route

Gateway of last resort is 172.29.6.5 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O       172.29.4.0/25 [110/65] via 172.29.6.5, 01:48:09, Serial0/1/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/120] via 172.29.6.5, 01:46:49, Serial0/1/0
        [110/120] via 172.29.6.5, 01:46:49, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/1/0
L       172.29.6.6/32 is directly connected, Serial0/1/0
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/0/1
L       172.29.6.14/32 is directly connected, Serial0/0/1
O       209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.0/30 [110/120] via 172.29.6.9, 01:01:04, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.5, 01:48:09, Serial0/1/0
        [110/1] via 172.29.6.5, 00:57:26, Serial0/0/0
MEDELLIN3#
    
```

Diseño propio

Figura 29. Tabla de enrutamiento BOGOTA3



Diseño propio

Se evidencia en el router ISP las rutas estáticas adicionales a las directamente conectadas.

En los routers Bogotá1 y Medellín1, se puede evidenciar cierta similitud teniendo en cuenta su ubicación, los dos enlaces de conexión y la ruta por defecto.

El balanceo de carga se produce en los router que tienen dos enlaces para conectarse a un mismo router, optimizando los recursos de la red de forma eficiente generando un equilibrio de carga en las rutas.

En los routers Medellín2 y Bogotá2, se evidencian redes conectadas directamente y recibidas mediante OSPF.

### 2.3 Deshabilitar la propagación del protocolo OSPF

Para implementar una mayor seguridad en la red, se deshabilita la propagación del protocolo OSPF en las interfaces que no sean necesarias y de esta forma evitar las publicaciones por interfaces que no sean requeridas y dejar activas solo las interfaces requeridas, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 5. Interfaces que no requieren desactivación

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

### 2.3.1 Deshabilitación propagación del protocolo OSPF en BOGOTA2

```

BOGOTA2>enable
BOGOTA2#config t
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#end
BOGOTA2#wr
    
```

### 2.3.2 Deshabilitación propagación del protocolo OSPF en BOGOTA3

```

BOGOTA3>enable
BOGOTA3#config t
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#end
BOGOTA3#wr
    
```

### 2.3.3 Deshabilitación propagación del protocolo OSPF en MEDELLIN2

```

MEDELLIN2>enable
MEDELLIN2#config t
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#end
MEDELLIN2#wr
    
```



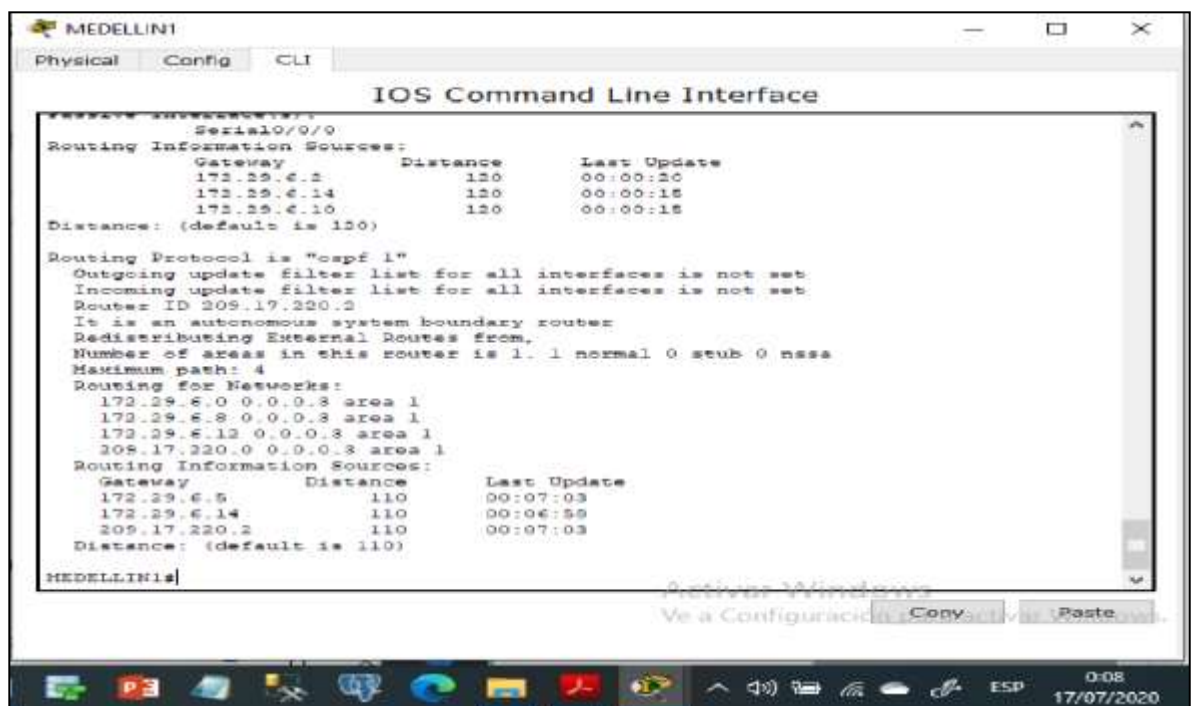
### 2.3.4 Deshabilitación propagación del protocolo OSPF en MEDELLIN3

```
MEDELLIN3>enable
MEDELLIN3#config t
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#end
MEDELLIN3#wr
```

### 2.4 Verificación del Protocolo OSPF

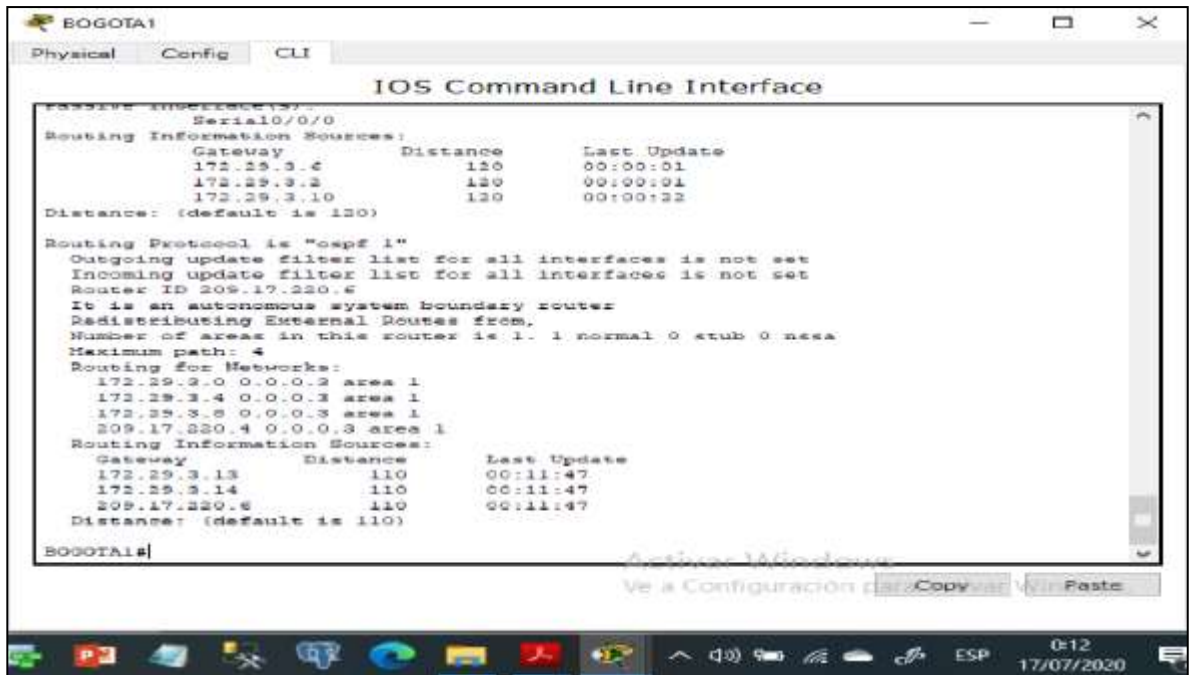
haciendo uso del comando “show ip protocols” se procede a verificar las interfaces pasivas, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura 30. Verificación de OSPF para MEDELLIN1



Diseño propio

Figura 31. Verificación de OSPF para BOGOTA1



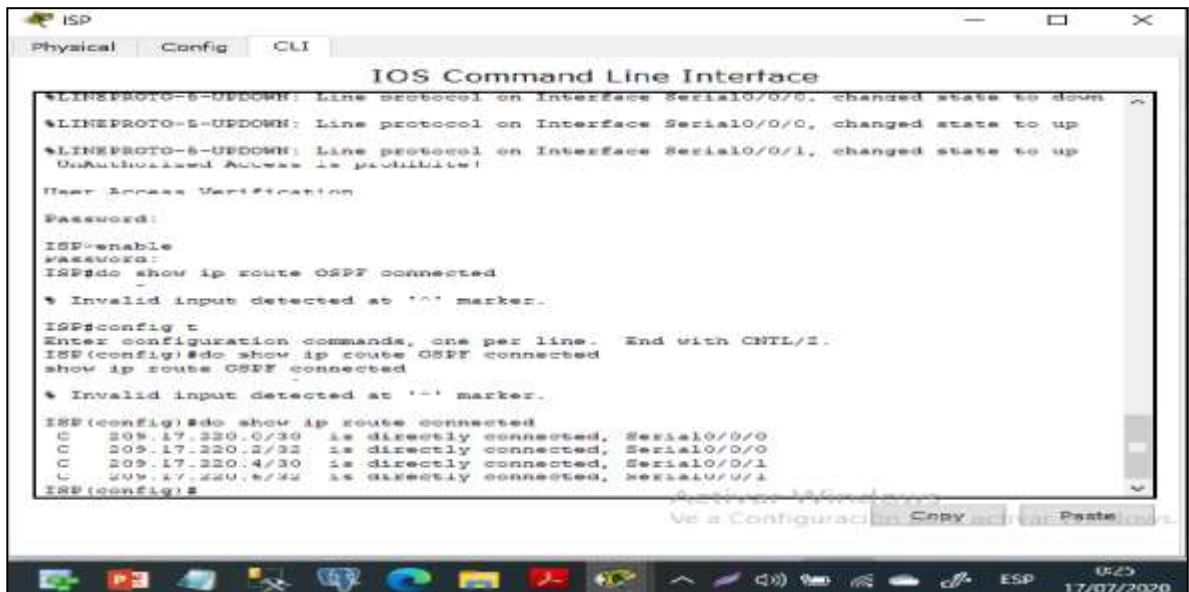
```
BOGOTA1#
Physical Config CLI
IOS Command Line Interface
Passive Interface(s):
Serial0/0/0
Routing Information Sources:
  Gateway         Distance      Last Update
  172.29.3.6       120           00:00:01
  172.29.3.2       120           00:00:01
  172.29.3.10      120           00:00:22
Distance: (default is 120)

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.8
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13      110           00:11:47
    172.29.3.14      110           00:11:47
    209.17.220.6     110           00:11:47
Distance: (default is 110)
BOGOTA1#
```

Diseño propio

Utilizando el comando “do show ip route OSPF” se procede con la verificación de la base de datos de OSPF para ISP, MEDELLIN1, MEDELLIN2, MEDELLIN3, BOGOTA1, BOGOTA2 Y BOGOTA3.

Figura 32. Verificación de OSPF para ISP



```
ISP#
Physical Config CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Unauthorized Access is prohibited!

User Access Verification

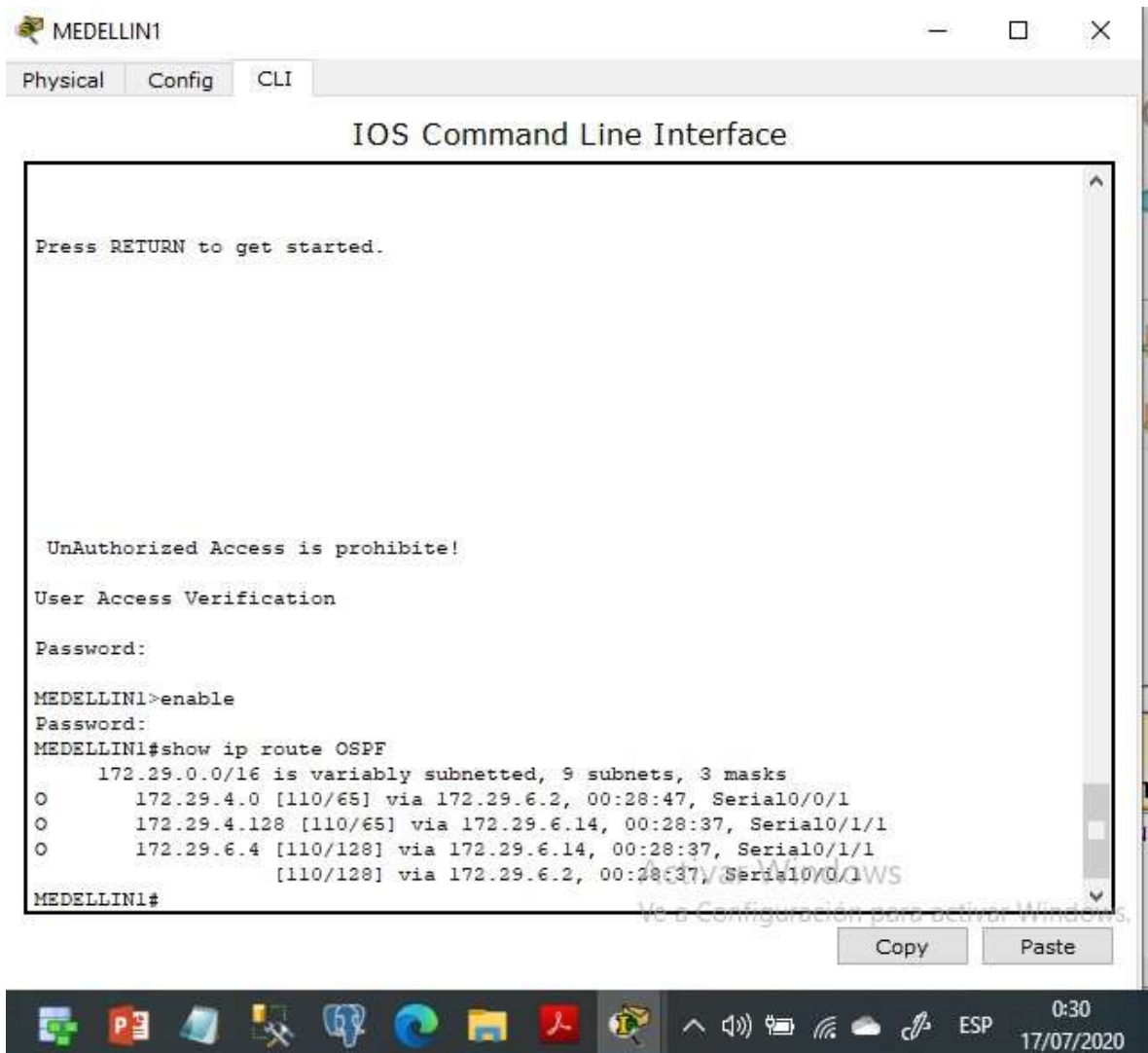
Password:
ISP#enable
Password:
ISP#do show ip route OSPF connected
% Invalid input detected at '^' marker.

ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#do show ip route OSPF connected
show ip route OSPF connected
% Invalid input detected at '^' marker.

ISP(config)#do show ip route connected
C 209.17.220.0/30 is directly connected, Serial0/0/0
C 209.17.220.2/32 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
C 209.17.220.8/32 is directly connected, Serial0/0/1
ISP(config)#
```

Diseño propio

Figura 33. Verificación de OSPF para MEDELLIN1



Diseño propio

Figura 34. Verificación de OSPF para BOGOTA1



```
BOGOTA1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

UnAuthorized Access is prohibite!
User Access Verification
Password:
BOGOTA1>enable
Password:
BOGOTA1#show ip route OSPF
 172.29.0.0/16 is variably subnetted, 5 subnets, 3 masks
O   172.29.0.0 [110/65] via 172.29.3.6, 00:31:45, Serial0/1/1
O   172.29.1.0 [110/65] via 172.29.3.10, 00:31:45, Serial0/0/1
O   172.29.3.12 [110/120] via 172.29.3.6, 00:31:45, Serial0/1/1
O   172.29.3.12 [110/120] via 172.29.3.10, 00:31:45, Serial0/0/1
BOGOTA1#
```

Diseño propio

Figura 35. Verificación de OSPF para MEDELLIN2

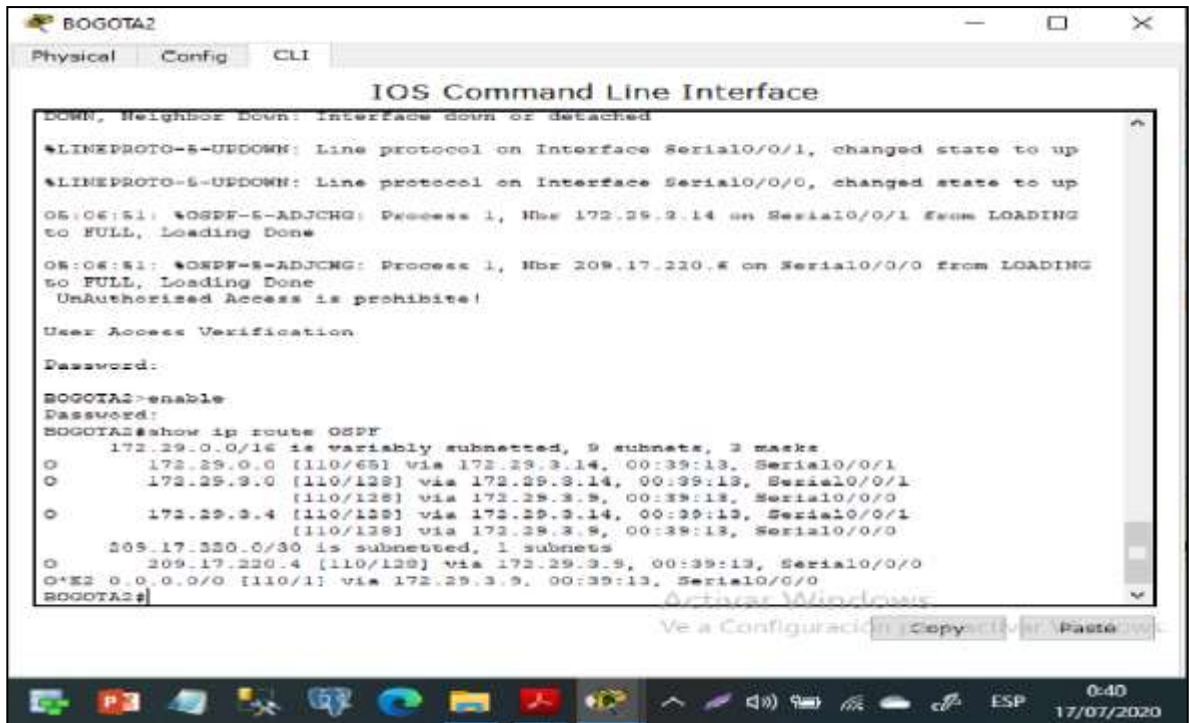


```
MEDELLIN2
Physical Config CLI
IOS Command Line Interface

UnAuthorized Access is prohibite!
User Access Verification
Password:
MEDELLIN2>enable
Password:
MEDELLIN2#show ip route OSPF
 172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O   172.29.4.128 [110/65] via 172.29.6.6, 00:36:58, Serial0/0/1
O   172.29.6.8 [110/128] via 172.29.6.6, 00:36:58, Serial0/0/1
O   172.29.6.8 [110/128] via 172.29.6.1, 00:36:58, Serial0/0/0
O   172.29.6.12 [110/128] via 172.29.6.6, 00:36:58, Serial0/0/1
O   172.29.6.12 [110/120] via 172.29.6.1, 00:36:58, Serial0/0/0
209.17.220.0/30 is subnetted, 1 subnets
O   209.17.220.0 [110/128] via 172.29.6.1, 00:36:08, Serial0/0/0
O*E3 0.0.0.0/0 [110/1] via 172.29.6.1, 00:36:08, Serial0/0/0
MEDELLIN2#
```

Diseño propio

Figura 36. Verificación de OSPF para BOGOTA2



Diseño propio

Figura 37. Verificación de OSPF para MEDELLIN3



Diseño propio



Figura 38. Verificación de OSPF para BOGOTA3



Diseño propio

## 2.5 Configuración de Encapsulamiento y Autenticación PPP

Se realiza la configuración de encapsulamiento según la Topología, MEDELLIN1 con ISP autenticación PAP, BOGOTÁ1 con ISP se debe configurar con autenticación CHAP.

### 2.5.1 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 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
```

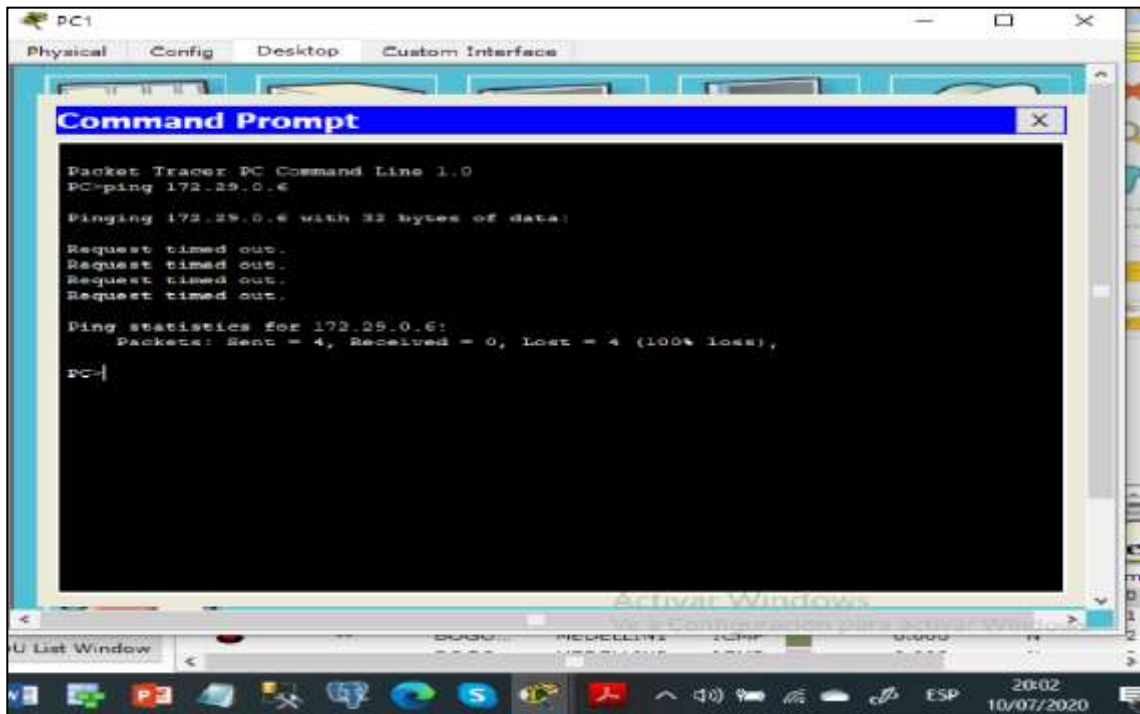
## 2.6 Configuración de PAT

### 2.6.1 Configuración de NAT

Según los lineamientos de la red, en los router MEDELLÍN1 y BOGOTÁ1, se realiza configuración NAT, una vez realizada esta configuración 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 39. Ping de PC1 a PC3



Diseño propio  
Figura 40. Evidencia de NO conexión de Extremo a Extremo

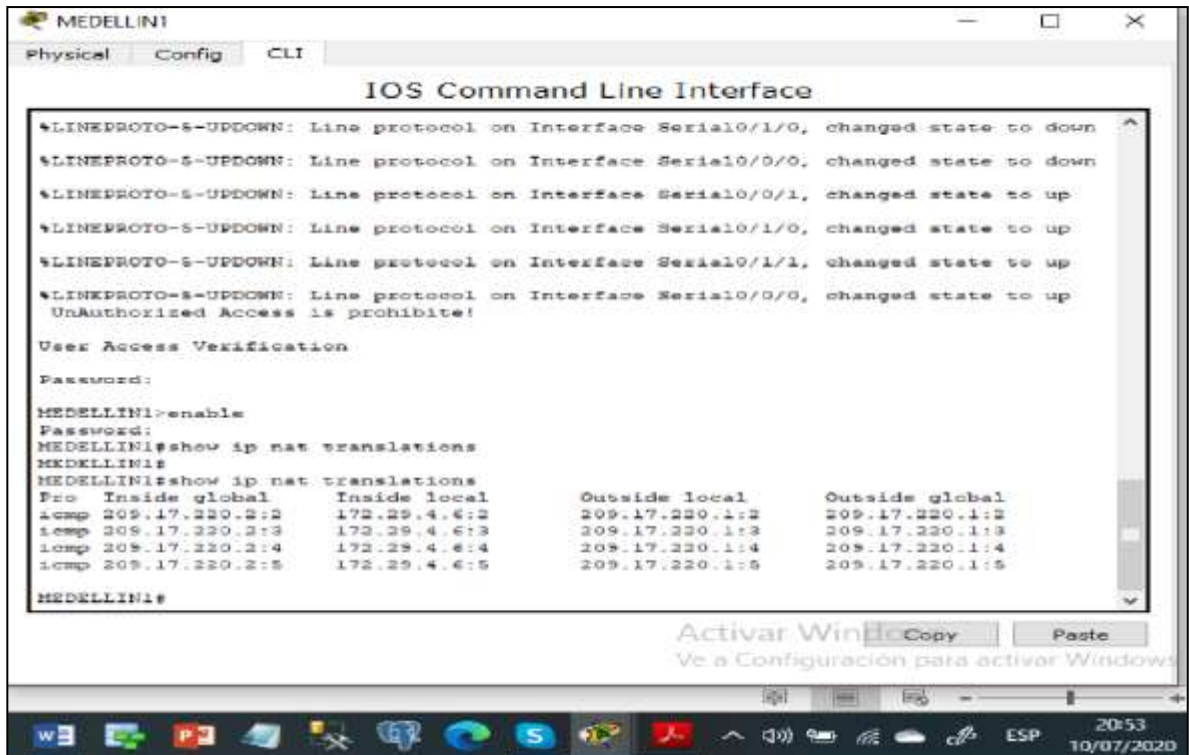
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	P
●	Failed	PC4	PC1	ICMP	Green	0.000	
●	Failed	PC2	PC3	ICMP	Blue	0.000	
●	Successful	PC4	ISP	ICMP	Dark Green	0.000	

Diseño propio

Al realizar ping de los equipos que están en cada extremo se evidencia que no hay comunicación de extremo a extremo acorde a los requisitos del escenario. Se realiza la verificación de la configuración NAT con el comando show ip nat translations.



Figura 41. Configuración de PAT en MEDELLIN1



Diseño propio

## 2.6.2 Configuración de NAT en BOGOTÁ1

Se realiza la configuración de NAT BOGOTA1.

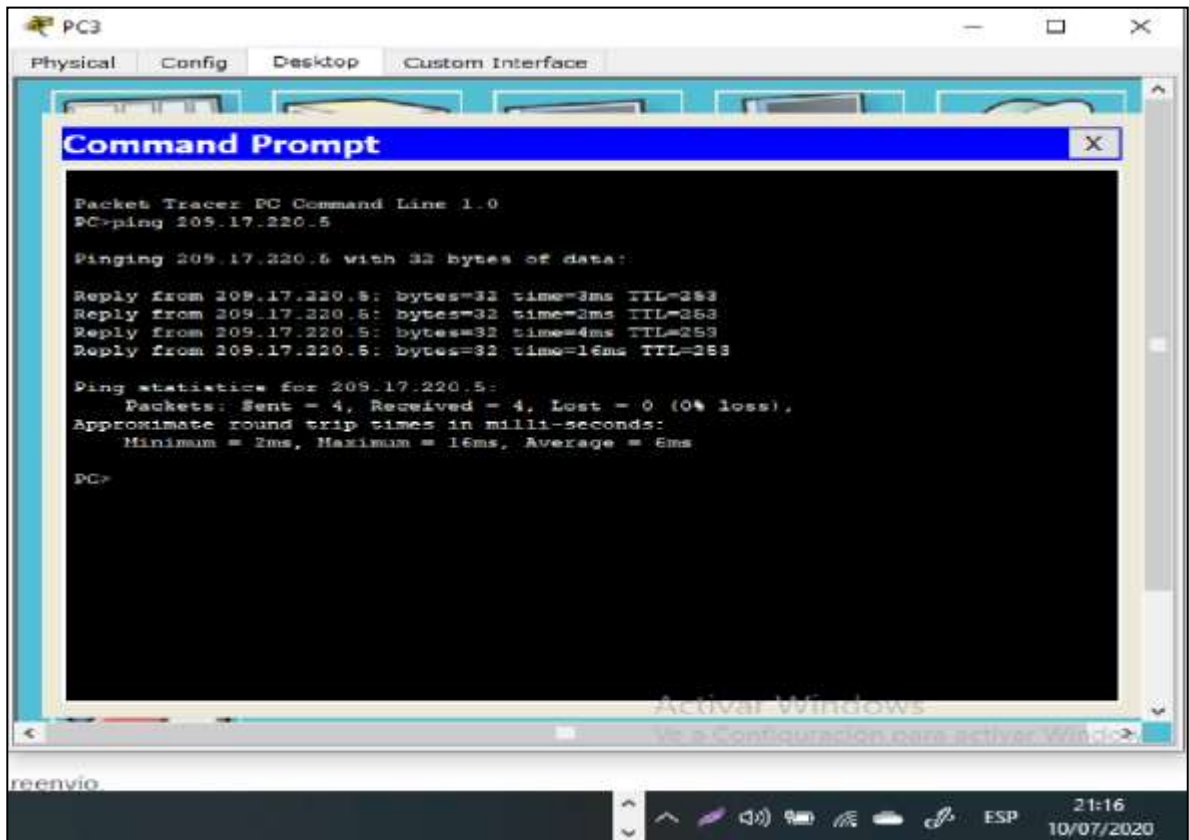
```

BOGOTA1>enable
BOGOTA1#config t
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

```

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

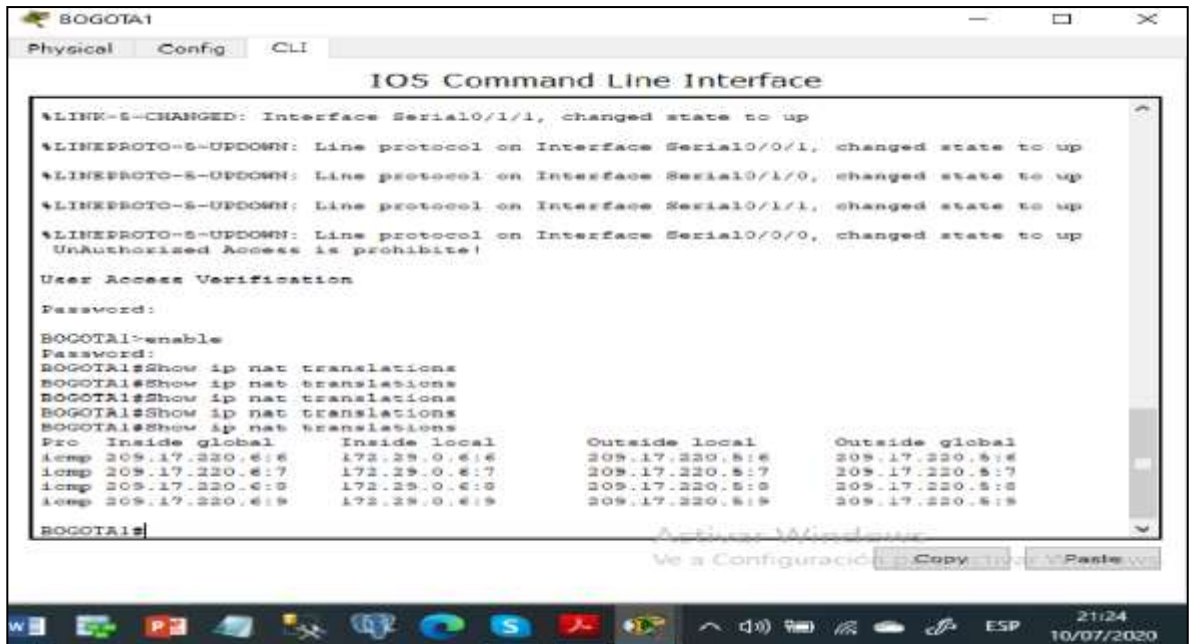
Figura 42. Ping de PC3 a ISP posterior a NAT



Diseño propio

Se realiza la verificación de la configuración NAT con el comando show ip nat translations. Verificando las interfaces de entrada y de salida.

Figura 43. Traducción de direcciones en BOGOTA1



```
BOGOTA1
Physical Config CLI
IOS Command Line Interface

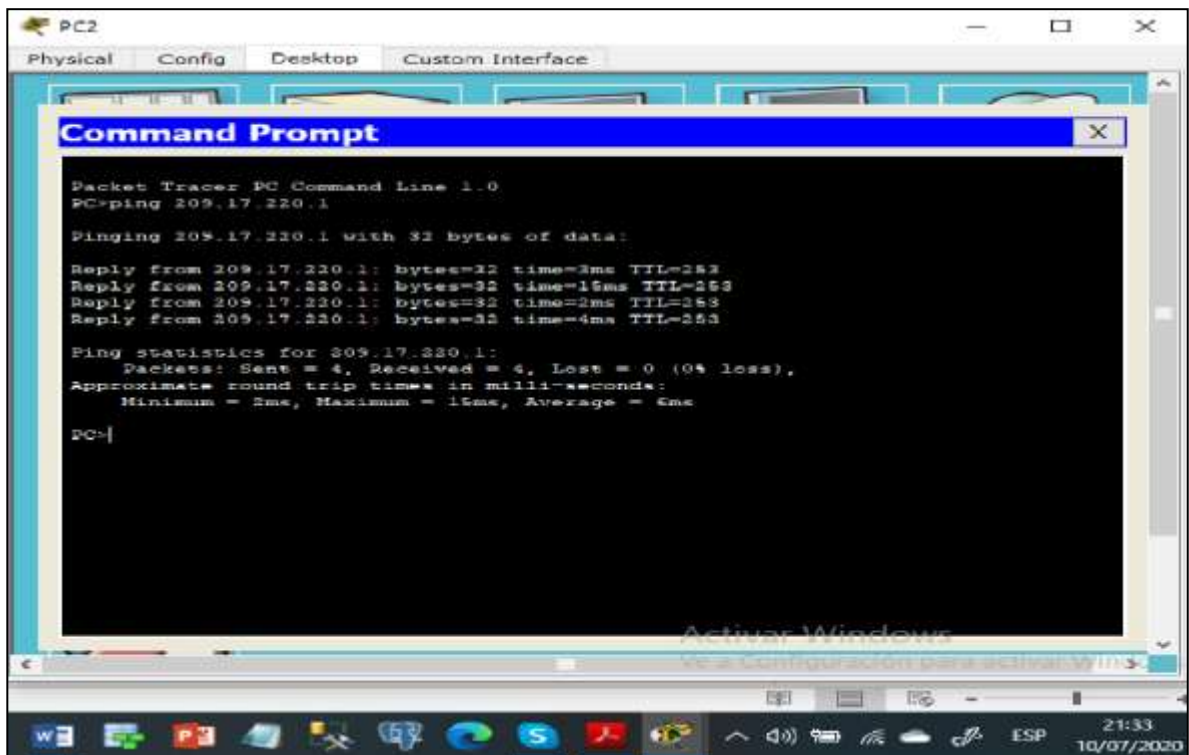
%LINK-3-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Unauthorized Access is prohibited!

User Access Verification

Password:
BOGOTA1>enable
BOGOTA1#show ip nat translations
BOGOTA1#show ip nat translations
BOGOTA1#show ip nat translations
BOGOTA1#show ip nat translations
BOGOTA1#show ip nat translations
Pro  Inside global      Inside local      Outside local    Outside global
icmp 209.17.220.6:6      172.29.0.6:6     209.17.220.6:6  209.17.220.6:6
icmp 209.17.220.6:7      172.29.0.6:7     209.17.220.6:7  209.17.220.6:7
icmp 209.17.220.6:8      172.29.0.6:8     209.17.220.6:8  209.17.220.6:8
icmp 209.17.220.6:9      172.29.0.6:9     209.17.220.6:9  209.17.220.6:9
BOGOTA1#
```

Diseño propio

Figura 44. Ping de PC2 a ISP después de NAT



```
PC2
Physical Config Desktop Custom Interface
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 209.17.220.1

Pinging 209.17.220.1 with 32 bytes of data:

Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=15ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=4ms TTL=253

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 15ms, Average = 6ms

PC>
```

Diseño propio

## 2.7 Configuración del Servicio DHCP

Se procede a la configuración del servicio DHCP en la red Medellín2 y Medellín3, configurando el router Medellín 2 como servidor DHCP para ambas redes LAN. Igualmente El router Medellín3 debe habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

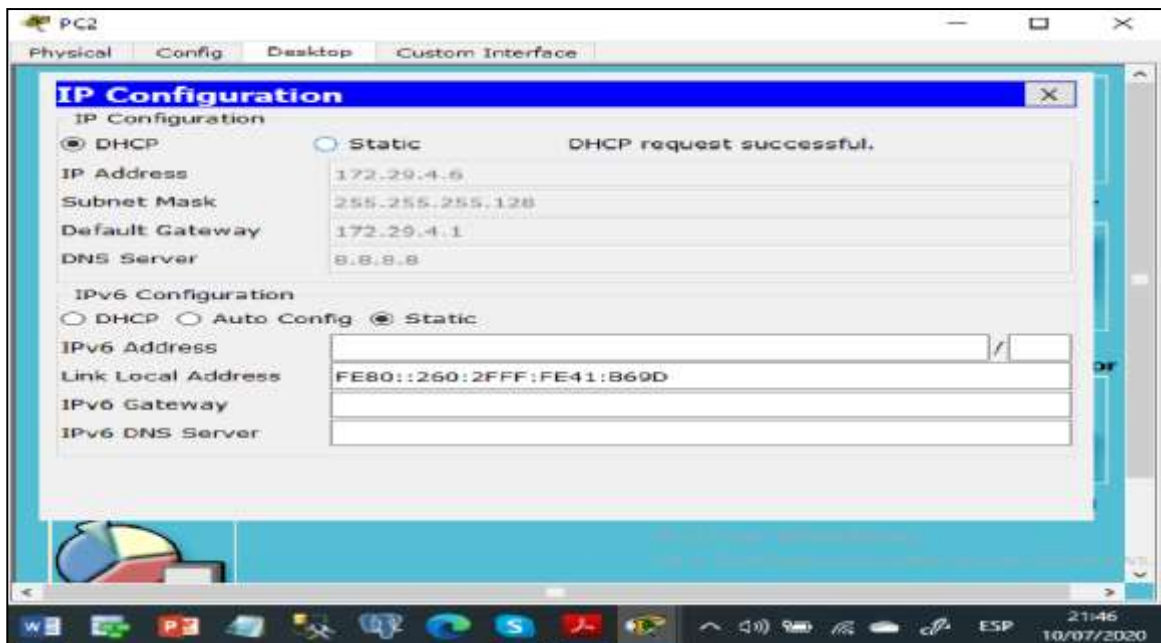
De igual forma se procede a configurar la red Bogota2 y Bogota3, configurando el router Bogota2 como servidor DHCP para ambas redes LAN. Igualmente el router Bogotá1 debe habilitar el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

### 2.7.1 Configuración servidor DHCP Medellín

```
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
```

Para que PC2 reciba la dirección, se debe habilitar directamente DHCP en la PC2

Figura 45. Habilitación de DHCP en la PC2



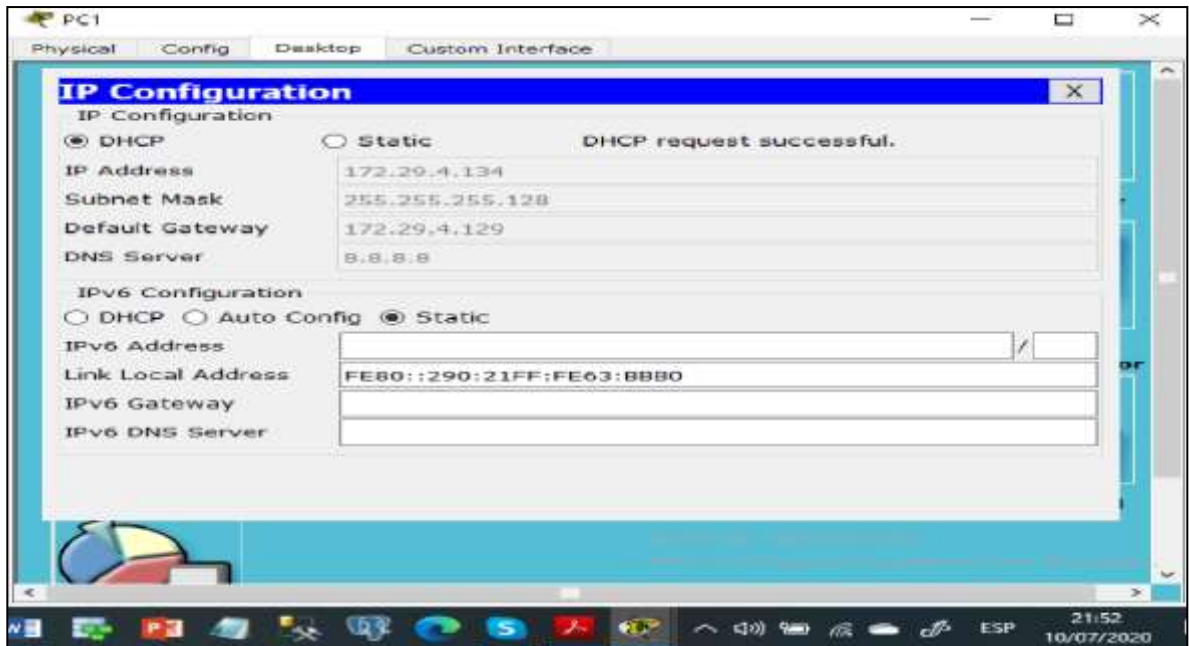
Diseño propio

Para lograr que la PC1 pueda conectarse en MEDELLIN3, se debe configurar 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
```

Para que PC1 reciba la dirección, se debe habilitar DHCP en la PC1.

Figura 46. Habilitación DHCP en PC1



Diseño propio

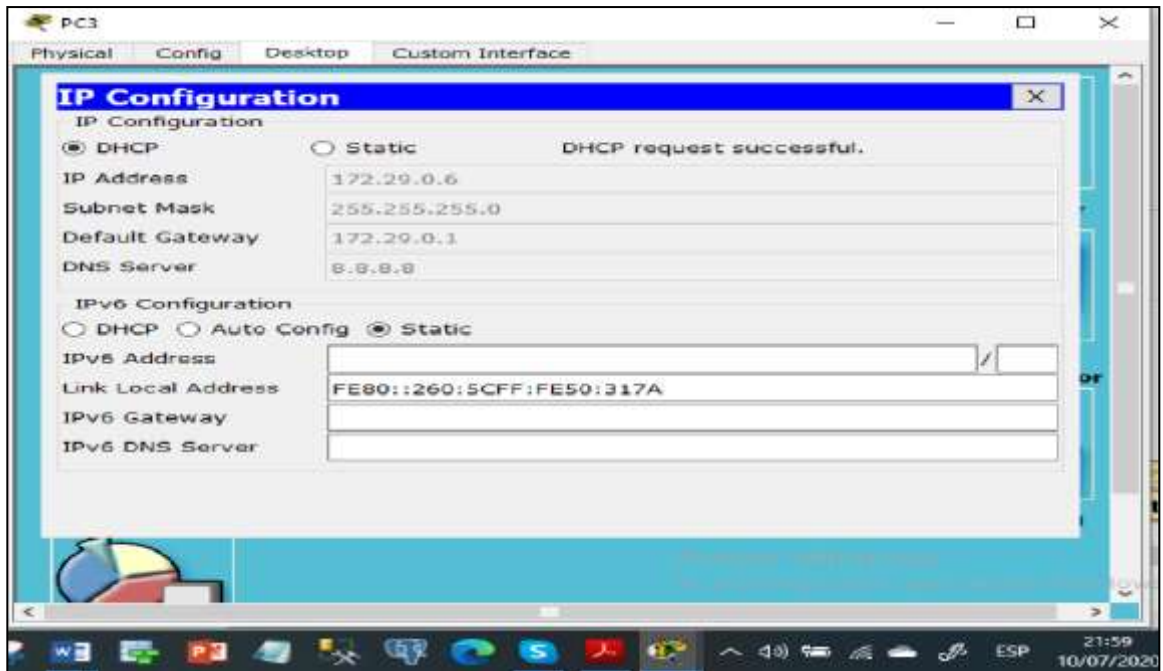
### 2.7.2 Configuración de la red BOGOTA servidor DHCP

```
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
```

Configuración del router Bogota3 habilitando el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

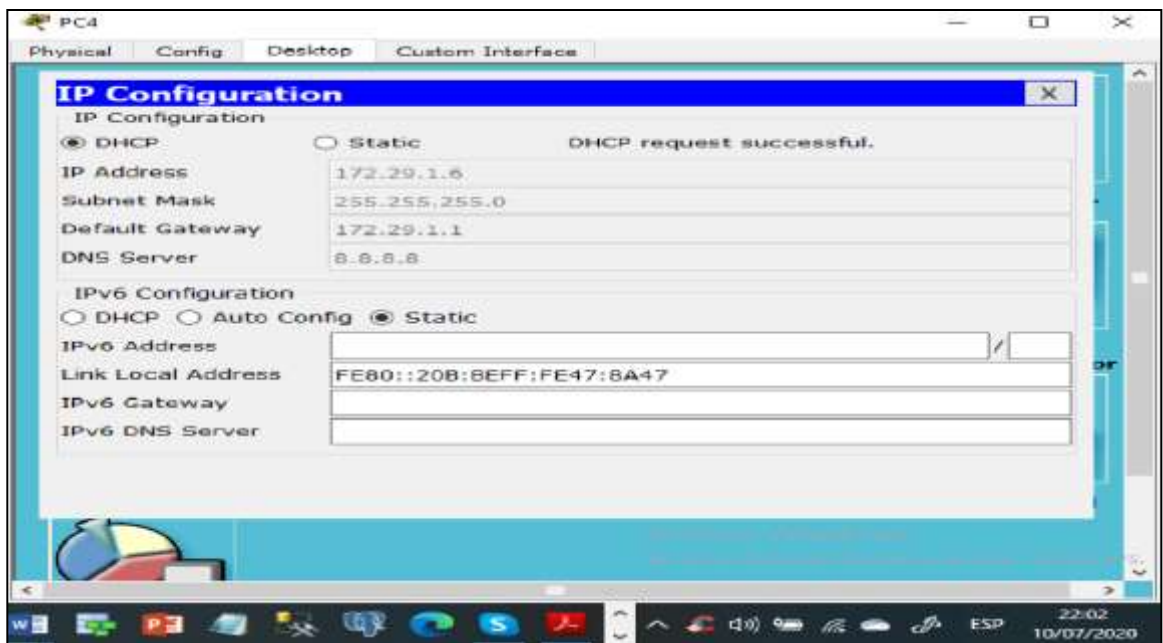
```
BOGOTA3>enable
BOGOTA3#config t
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```

Figura 47. Habilitación DHCP en PC3



Diseño propio

Figura 48. Habilitación DHCP en PC4



Diseño propio



## ANEXO

Link de ejercicios.

<https://1drv.ms/u/s!AgwO84dCHufvg08hhHjBzh9uf4NW?e=edPmlB>



## CONCLUSIONES

En el diseño de una red es importante la implementación de los protocolos de enrutamiento que permitan definir las políticas de seguridad, determinar la comunicación entre los dispositivos de la red es fundamental para garantizar estándares de calidad que permitan preservar la seguridad, confiabilidad y disponibilidad de los datos que circulan a través de la red.

En un entorno de red es posible identificar y controlar el tráfico de red, gracias a la implementación de las listas de acceso(ACL), controlando los paquetes que viajan a través de la misma.

El protocolo de enrutamiento OSPF permite recalcular las rutas para determinar cuáles son los caminos más cortos en una red para llegar al destino.

Las configuraciones básicas de una topología de red, permiten identificar los dispositivos, asegurar la comunicación, habilitar las interfaces y establecer las políticas de seguridad.

Los protocolos de enrutamiento estáticos, resultan muy útiles para pequeñas redes, dado que requieren la intervención del administrador de forma permanente, mientras que los protocolos de enrutamiento dinámico que permiten establecer nuevas rutas en la medida que la red cambia, dado que los routers automáticamente pueden modificar sus tablas de enrutamiento.

## BIBLIOGRAFÍA

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

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%20CONFIGURACION%20DE%20REDES.pdf?sequence=1&isAllowed=y>)

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-dinamicoospf-con-packet-tracer>)

PRIETO FERNANDEZ, Raúl. "Enrutamiento entre VLANS con Packet Tracer: My Blog" {En línea}. {12 junio de 2019} disponible en: (<https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-entre-vlans-con-packet-tracer>)

RAMOS GATA, Jose Ramón. "Vlan: Ragasys Sistemas" {En línea}. {30 junio de 2020} disponible en: (<https://blog.ragasys.es/tag/vlan>)

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