.SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

DIANA MARCELA SILVA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
PITALITO - HUILA
2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

DIANA MARCELA SILVA TORRES

TRABAJO ESCRITO PARA OPTAR POR EL TÍTULO DE:
INGENIERÍA DE SISTEMAS

TUTOR
HÉCTOR JULIÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
PITALITO - HUILA
2020

DEDICATORIA Y AGRADECIMIENTOS

Agradezco primero a Dios por haberme dado una familia maravillosa, la cual ha creído en mí siempre, dándome ejemplo de superación, humildad y sacrificio; enseñándome a valorar todo lo que tengo. A ellos les dedico el presente trabajo, porque han fomentado en mí el deseo de superación y de triunfo en la vida, lo que ha contribuido a la consecución de este logro. Espero siempre contar con su valioso e incondicional apoyo.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

GLOSARIO

VLAN: Procedimiento para establecer redes lógicas de una forma independiente dentro de una misma red física.

CONECTIVIDAD: Es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.

OSPF: Protocolo de enrutamiento desarrollado para redes IP de tipo enlace /estado.

DHCP: Protocolo de configuración dinámica de host de tipo cliente /servidor en el que el servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

NAT: Protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.

DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.

PROTOCOLOS DE ENRUTAMIENTO: conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.

TOPOLOGÍA LÓGICA: es la forma que utilizan los hosts para comunicarse a través de una red.

DIRECCIÓN IP: es un direccionamiento utilizado para identificar un dispositivo en la red.

PING: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.
ENCAPSULAMIENTO: es el proceso en el que los datos que se encuentran dispuestos para ser enviados a través de una red se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red

TOPOLOGÍA FÍSICA: disposición de cada uno de los dispositivos o hardware dentro de una red.

RESUMEN

Para el desarrollo de este trabajo se realizó el planteamiento de dos escenarios cada uno con una topología diferente, donde encontramos una descripción detallada la cual nos ayudó para la configuración mediante fireware CISCO IOS de cada uno de los dispositivos utilizados para su simulación en el software Packet Tracer, permitiendo comprobar su conectividad.

En el primer escenario se nos pide configurar una red pequeña con conexión IPv4 e IPv6, proporcionando seguridad en cada uno de los dispositivos routers y switches, utilizando protocolo DHCP, NTP Servidor/Cliente, redes dinámicas y estáticas (NAT), listas de control de acceso (ACL).

En el segundo escenario se debe configurar e interconectar cada uno de los dispositivos que la conforman según los protocolos de enrutamiento OSPF, habilitar el encapsulamiento PPP y autenticación, comprobando la conectividad de los dispositivos entre sí.

1. INTRODUCCIÓN

En este documento podrá encontrar el desarrollo de la prueba de habilidades correspondiente al Diplomado de Profundización CCNA; en la cual se abordarán cada una de las temáticas relacionadas con el núcleo problémico del curso, el cual tiene como objetivo principal el aprendizaje y adquisición de habilidades en fundamentos de redes por parte del estudiante que le permitan diseñar una red empresarial eficaz y escalable, en la cual posea las capacidades para realizar la instalación, configuración, supervisión y solución a cualquier problema que se pueda presentar con los equipos que conforman la infraestructura de la red.

La prueba de habilidades consiste en la configuración de dos redes, cada una perteneciente a un escenario de diferente magnitud, en los cuales se deben realizar las labores de verificación de la conectividad de la red a partir de la ejecución de los comandos correspondientes, la configuración de cada dispositivo de acuerdo con las indicaciones para el desarrollo de la prueba, la introducción de los niveles de seguridad establecidos que permitan mantener la integridad de la red y protegerla de cualquier amenaza y, finalmente, una vez se cumpla con los estándares de configuración de la topología de la red, se debe evidenciar su funcionalidad y verificar que todos los elementos de su infraestructura tengan conectividad.

Para el escenario número uno, se configuro una red pequeña que admitiera conectividad IPv4 e IPv6; además, fue necesario agregar seguridad de switches, routing entre VLAN, protocolo de routing dinámico RIPv2, protocolo de configuración de hosts dinámicos (DHCP), 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. Una vez adoptadas estas medidas, se realizó la evaluación y registro de la red mediante los comandos comunes de CLI. Por otra parte, para el escenario número dos, se llevó a cabo la configuración de una red de una empresa con sucursales en la ciudad de Bogotá y en la ciudad de Medellín; en este escenario, fue necesario el uso del protocolo de enrutamiento OSPF debido a que las rutas se encuentran por defecto redistribuidas y, la habilitación y autenticación del encapsulamiento PPP.

En la implementación de cada uno de los escenarios propuestos para el desarrollo de la prueba de habilidades, fue necesario hacer uso de la versión 7.2.2 del software para simulación de redes Packet Tracer de la academia CISCO; el cual permite llevar a cabo tanto el análisis y experimentación de la respuesta de la topología física de la red, como la configuración de cada uno de los dispositivos que la componen.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar la prueba de habilidades del diplomado de profundización CCNA, a partir del análisis y configuración de la red propuesta tanto para el escenario número uno como para el escenario número dos, teniendo en cuenta la fundamentación teórica y práctica adquirida en cuanto al diseño e implementación de la topología lógica y física de una red.

2.2 OBJETIVOS ESPECÍFICOS

- Documentar paso a paso el procedimiento realizado para llevar a cabo la solución de la prueba de habilidades a partir de la implementación de la red propuesta para los escenarios uno y dos.

- Analizar cada uno de los elementos que componen la topología de la red, con el fin de llevar a cabo de manera exitosa la configuración de cada uno de sus dispositivos para garantizar seguridad y conectividad óptima en la red.

- Mostrar los conocimientos y habilidades adquiridas en la implementación e interconexión de topologías de red a partir del manejo del software Packet Tracer de la academia CISCO.

3 PLANTEAMIENTO Y SOLUCION DE LOS ESCENARIOS

En este informe se tienen dos escenarios cada uno con sus especificaciones para analizarlos, configurarlos y verificar su funcionalidad de acuerdo con las indicaciones dadas, por eso se debe tener muy encuenta los comandos y dispositivos que se utilizaran en el software Packet Tracer de Cisco, para darle un buen funcionamiento a las simulaciones.

3.1. ESCENARIO 1

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

Topología

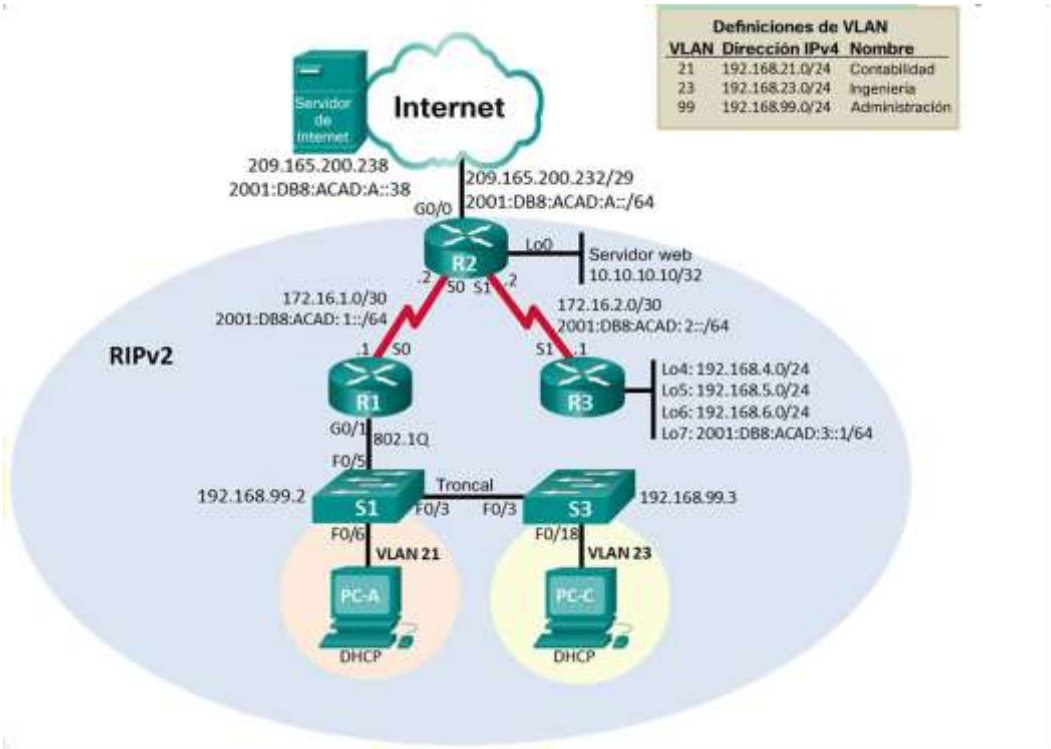


Figure 1Topologia Escenario 1

Parte 1: Inicializar dispositivos

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

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

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

a. Eliminamos el archivo startup-config de los routers con el comando:

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

b. Volvemos a cargar los routers con el comando:

```
Router>enable
Router#reload
Proceed with reload? [confirm]
```

c. Eliminamos el archivo startup-config de todos los switches con el comando:

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
```

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#

Eliminamos la base de datos de VLAN anterior con el comando:

Switch>enable

Switch#delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

%Error deleting flash:/vlan.dat (No such file or directory)

d. Volvemos a cargar los switches con el comando:

Switch>enable

Switch#reload

Proceed witch reload? [confirm]

e. Verificamos que la base de datos de VLAN no esté en la memoria flash en ambos switches con el comando:

Switch>enable

Switch#show flash

Directory of flash:/

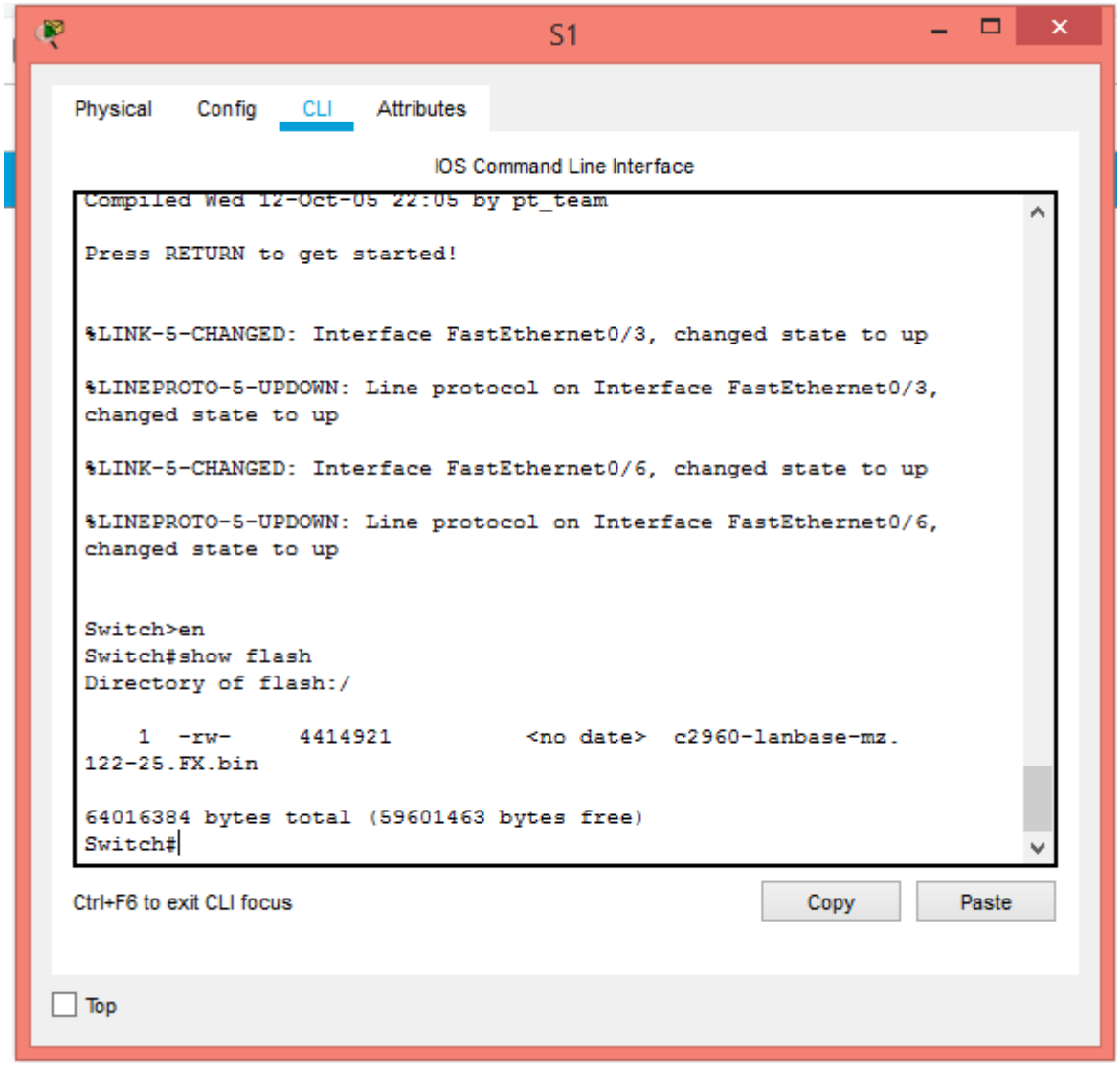


Figure 2 Verificación base de datos VLAN

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Configuramos la computadora segun los datos dados en la topología

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.229
Máscara de subred para IPv4	255.2552.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 1. Configuracion de la PC de Internet

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

a. Desactivamos la búsqueda DNS con el comando:

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#
```

b. Colocamos nombre al router con el comando:

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#
```

c. Colocamos una contraseña de EXEC Privilegiado cifrada con el comando:

```
R1>enable
R1#configure terminal
R1(config)#enable secret Class
R1(config)#
```

d. Colocamos una contraseña de acceso a la consola con el comando:

```
R1>enable
R1#configure terminal
R1(config)#line console 0
R1(config-line)#password Cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

e. Colocamos una contraseña de acceso Telenet con el comando:

```
R1>enable
R1#configure terminal
R1(config)#line vty 0 15
R1(config-line)#password Cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

f. Ciframos las contraseñas de texto no cifrado con el comando:

```
R1>enable
R1#configure terminal
R1(config)#service password-encryption
R1(config)#
```

g. Colocamos un Mensaje MOTD con el comando:

```
R1>enable
R1#configure terminal
R1(config)#banner motd #Se prohíbe el acceso no autorizado#
R1(config)#
```

h. Establecemos la descripción de la interface S0/0/0, dirección IPv4, IPv6, frecuencia de reloj en128000 y activacion con los comando:

```
R1>enable
R1#configure terminal
R1(config)#interface serial 0/0/0
R1(config-if)#description interfaz DCE conectada a el 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
```

i. Configuramos rutas predeterminadas con el comando:

```
R1>enable
R1#configure terminal
R1(config)#interface s0/0/0
R1(config-if)#ip route 0.0.0.0 0.0.0.0 se0/0/0
R1(config-if)#ipv6 route ::/0 se0/0/0
```

R1(config)#exit
R1(config)#

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración R2 incluye las siguientes tareas:

a. Desactivamos la búsqueda DNS con el comando:

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#exit

b. Colocamos nombre al router con el comando:

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#exit

c. Colocamos una contraseña de EXEC Privilegiado cifrada con el comando:

R2>enable
R2#configure terminal
R2(config)#enable secret Class
R2(config)#

d. Colocamos una contraseña de acceso a la consola con el comando:

```
R2>enable
R2#configure terminal
R2(config)#line console 0
R2(config-line)#password Cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

e. Colocamos una contraseña de acceso Telenet con el comando:

```
R2>enable
R2#configure terminal
R2(config)#line vty 0 15
R2(config-line)#password Cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

f. Ciframos las contraseñas de texto no cifrado con el comando:

```
R2>enable
R2#configure terminal
R2(config)#service password-encryption
R2(config)#
```

g. Habilitamos el servidor HTTP con el comando:

R2(config)#ip http server
R2(config)#ip http authentication local
Nota: El programa no deja ejecutar el comando.

h. Colocamos un Mensaje MOTD con el comando:

R2>enable
R2#configure terminal
R2(config)#banner motd #Se prohíbe el acceso no autorizado#
R2(config)#

i. Establecemos la descripción de las interfaces, dirección IPv4, IPv6, frecuencia de reloj en128000 y activacion con los comando:

- **S0/0/0**

R2>enable
R2#configure terminal
R2(config)#interface serial 0/0/0
R2(config-if)#description interfaz conectada a el 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

- **S0/0/1**

R2>enable

R2#configure terminal

R2(config)#interface serial 0/0/1

R2(config-if)#description interfaz DCE conectada a R3

R2(config-if)#ip address 172.16.2.1 255.255.255.252

R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64

R2(config-if)#clock rate 128000

R2(config-if)#no shutdown

- **G0/0 (Simulación de internet)**

R2>enable

R2#configure terminal

R2(config)#interface g0/0

R2(config-if)#description interface de simulación de internet

R2(config-if)#ip address 209.165.200.225 255.255.255.252

R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64

R2(config-if)#no shutdown

- **Interfaz loopback0 (servidor web simulado)**

R2>enable

R2#configure terminal

R2(config)#interface loopback 0

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255

R2(config-if)#exit

R2(config-if)#

j. Configuramos rutas predeterminadas con el comando:

```
R2>enable
R2#configure terminal
R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config-if)#ipv6 route ::/0 g0/0
R2(config)#exit
R2(config)#
```

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

a. Desactivamos la búsqueda DNS con el comando:

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#
```

b. Colocamos nombre al router con el comando:

```
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#
```

c. Colocamos una contraseña de EXEC Privilegiado cifrada con el comando:

```
R3>enable
R3#configure terminal
R3(config)#enable secret Class
R3(config)#
```

d. Colocamos una contraseña de acceso a la consola con el comando:

```
R3>enable
R3#configure terminal
R3(config)#line console 0
```

```
R3(config-line)#password Cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#
```

e. Colocamos una contraseña de acceso Telenet con el comando:

```
R3>enable
R3#configure terminal
R3(config)#line vty 0 15
R3(config-line)#password Cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#
```

f. Ciframos las contraseñas de texto no cifrado con el comando:

```
R3>enable
R3#configure terminal
R3(config)#service password-encryption
R3(config)#
```

g. Colocamos un Mensaje MOTD con el comando:

```
R3>enable
R3#configure terminal
R3(config)#banner motd #Se prohíbe el acceso no autorizado#
R3(config)#
```

i. Establecemos la descripción de las interfaces, dirección IPv4, IPv6, frecuencia de reloj en128000 y activacion con los comando:

- **S0/0/1**

```
R3>enable
R3#configure terminal
R3(config)#interface serial 0/0/1
R3(config-if)#description interfaz conectada a R2
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R3(config-if)#no shutdown
```

- **Interfaz loopback4**

```
R3>enable
R3#configure terminal
R3(config)#interface loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.224
R3(config-if)#no shutdown
R3(config-if)# exit
R3(config)#
```

- **Interfaz loopback5**

```
R3>enable
R3#configure terminal
R3(config)#interface loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.224
```

R3(config-if)#no shutdown
R3(config-if)# exit
R3(config)#

- **Interfaz loopback6**

R3>enable
R3#configure terminal
R3(config)#interface loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.224
R3(config-if)#no shutdown
R3(config-if)# exit
R3(config)#

- **Interfaz loopback7**

R3>enable
R3#configure terminal
R3(config)#interface loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#no shutdown
R3(config-if)# exit
R3(config)#

j. Configuramos rutas predeterminadas con el comando:

R3>enable
R3#configure terminal

```
R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config-if)#ipv6 route ::/0 s0/0/1
R3(config)#exit
R3(config)#
```

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

a. Desactivamos la búsqueda DNS con el comando:

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#
```

b. Colocamos nombre al Switch con el comando:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#
```

c. Colocamos una contraseña de EXEC Privilegiado cifrada con el comando:

```
S1>enable
S1#configure terminal
S1(config)#enable secret Class
S1(config)#
```

d. Colocamos una contraseña de acceso a la consola con el comando:

```
S1>enable
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password Cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

e. Colocamos una contraseña de acceso Telenet con el comando:

```
S1>enable
S1#configure terminal
S1(config)#line vty 0 15
S1(config-line)#password Cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

f. Ciframos las contraseñas de texto no cifrado con el comando:

```
S1>enable
S1#configure terminal
S1(config)#service password-encryption
S1(config)#
```

g. Colocamos un Mensaje MOTD con el comando:

```
S1>enable
S1#configure terminal
S1(config)#banner motd #Se prohíbe el acceso no autorizado#
S1(config)#
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

a. Desactivamos la búsqueda DNS con el comando:

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#
```

b. Colocamos nombre al Switch con el comando:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S3
S3(config)#
```

c. Colocamos una contraseña de EXEC Privilegiado cifrada con el comando:

```
S3>enable
S3#configure terminal
S3(config)#enable secret Class
S3(config)#
```

d. Colocamos una contraseña de acceso a la consola con el comando:

```
S3>enable
S3#configure terminal
S3(config)#line console 0
S3(config-line)#password Cisco
S3(config-line)#login
S3(config-line)#exit
```

S3(config)#

e. Colocamos una contraseña de acceso Telenet con el comando:

S3>enable
S3#configure terminal
S3(config)#line vty 0 15
S3(config-line)#password Cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#

f. Ciframos las contraseñas de texto no cifrado con el comando:

S3>enable
S3#configure terminal
S3(config)#service password-encryption
S3(config)#

g. Colocamos un Mensaje MOTD con el comando:

S3>enable
S3#configure terminal
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#

Paso 7: Verificar la conectividad de la red

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

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

a. Probaremos la conectividad desde R1 hacia R2, S0/0/0 por medio de la IP 172.16.1.2

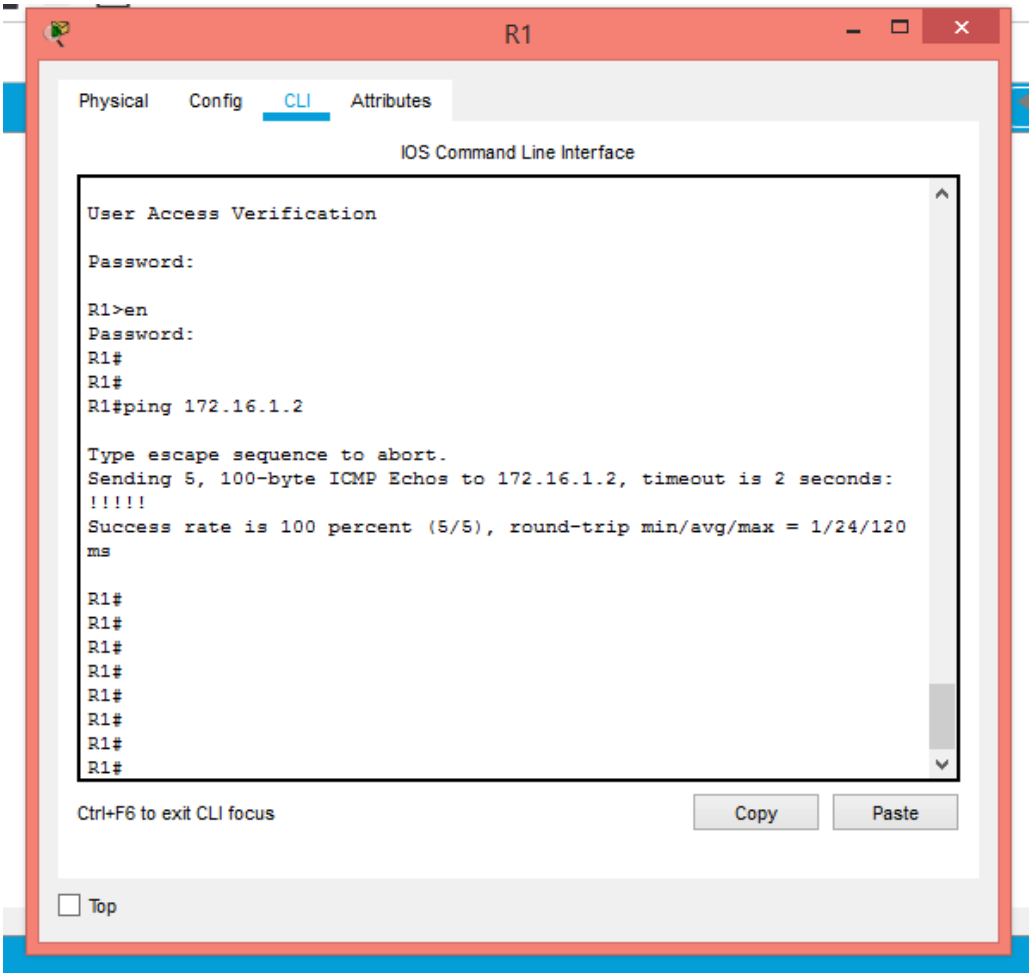


Figure 3 Comprobación conectividad de R1 a R2

b. Probaremos la conectividad desde R2 hacia R3, S0/0/1 por medio de la IP 172.16.2.2

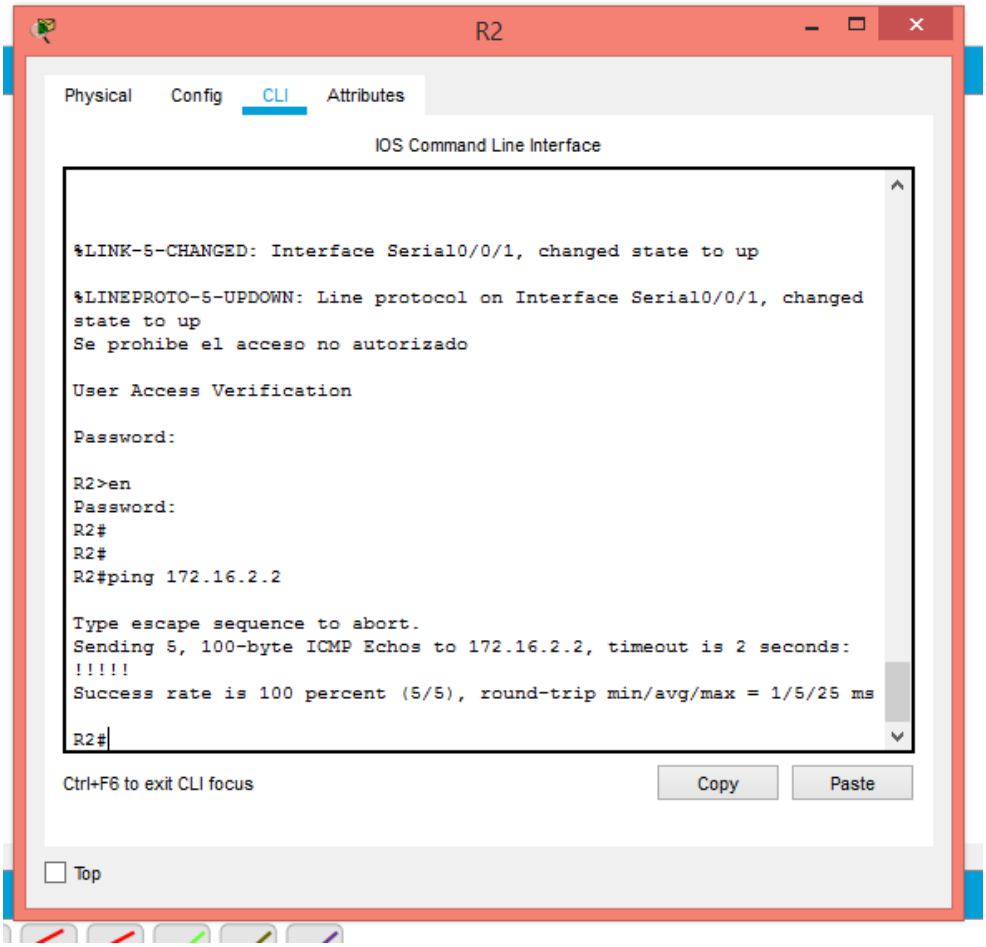


Figure 4 Comprobación conectividad R2 a R3

c. Probaremos la conectividad desde PC de Internet hacia el Gateway predeterminado por medio de la IP 209.165.200.225

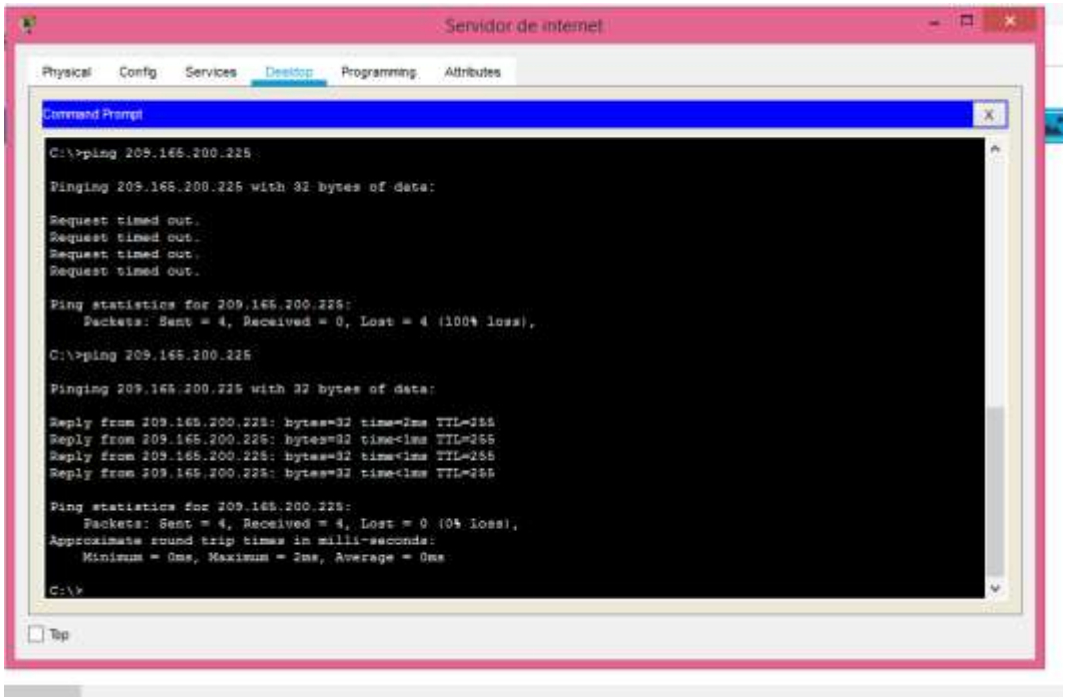


Figure 5 Comprobación conectividad PC Internet a Gateway Predeterminado

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

a. Crearemos y daremos nombre a las VLAN

```
S1>enable
S1#configure terminal
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
```

```
S1(config-vlan)#exit
S1>enable
S1#configure terminal
S1(config)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#exit
S1>enable
S1#configure terminal
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
```

b. Asignamos la IPv4 a la VLAN de administración.

```
S1>enable
S1#configure terminal
S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

c. Asignaremos la primera dirección IPv4 como gateway predeterminado.

```
S1>enable
S1#configure terminal
S1(config)#ip default-gateway 192.168.99.1
S1(config)#
```

d. Forzaremos el enlace troncal en la interfaz F0/3, utilizando la red VLAN1 como VLAN native

```
S1>enable
S1#configure terminal
```

S1(config)#interface f0/3

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#

e. Forzaremos el enlace troncal en la interfaz F0/5, utilizando la red VLAN1 como VLAN native

S1>enable

S1#configure terminal

S1(config)#interface f0/5

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#

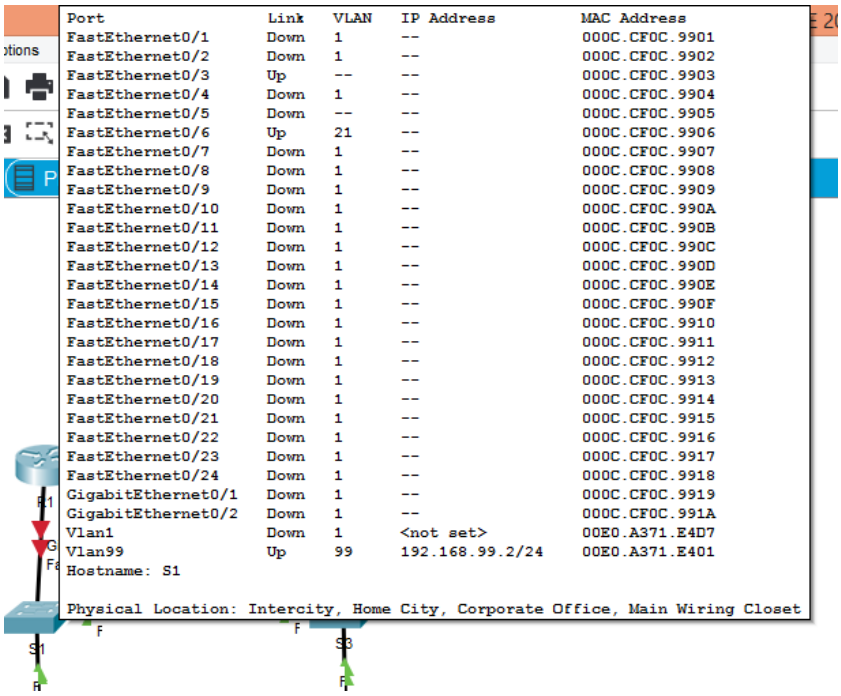
f. Configuraremos los demas puertos como puertos de acceso

S1>enable
S1#configure terminal
S1(config)#interface range fa0/1, fa0/2, fa0/4, fa0/6-24, g0/1, g0/2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit

g. Asignaremos la interface F0/6 a la VLAN 21

S1>enable
S1#configure terminal
S1(config)#interface fa0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit

h. Apagar todos los puertos sin usar



Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	000C.CF0C.9901
FastEthernet0/2	Down	1	--	000C.CF0C.9902
FastEthernet0/3	Up	--	--	000C.CF0C.9903
FastEthernet0/4	Down	1	--	000C.CF0C.9904
FastEthernet0/5	Down	--	--	000C.CF0C.9905
FastEthernet0/6	Up	21	--	000C.CF0C.9906
FastEthernet0/7	Down	1	--	000C.CF0C.9907
FastEthernet0/8	Down	1	--	000C.CF0C.9908
FastEthernet0/9	Down	1	--	000C.CF0C.9909
FastEthernet0/10	Down	1	--	000C.CF0C.990A
FastEthernet0/11	Down	1	--	000C.CF0C.990B
FastEthernet0/12	Down	1	--	000C.CF0C.990C
FastEthernet0/13	Down	1	--	000C.CF0C.990D
FastEthernet0/14	Down	1	--	000C.CF0C.990E
FastEthernet0/15	Down	1	--	000C.CF0C.990F
FastEthernet0/16	Down	1	--	000C.CF0C.9910
FastEthernet0/17	Down	1	--	000C.CF0C.9911
FastEthernet0/18	Down	1	--	000C.CF0C.9912
FastEthernet0/19	Down	1	--	000C.CF0C.9913
FastEthernet0/20	Down	1	--	000C.CF0C.9914
FastEthernet0/21	Down	1	--	000C.CF0C.9915
FastEthernet0/22	Down	1	--	000C.CF0C.9916
FastEthernet0/23	Down	1	--	000C.CF0C.9917
FastEthernet0/24	Down	1	--	000C.CF0C.9918
GigabitEthernet0/1	Down	1	--	000C.CF0C.9919
GigabitEthernet0/2	Down	1	--	000C.CF0C.991A
Vlan1	Down	1	<not set>	00E0.A371.E4D7
Vlan99	Up	99	192.168.99.2/24	00E0.A371.E401

Hostname: S1

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Figure 6 Puertos apagados de S1

Nota: Los puertos por defecto se encuentran apagados.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

a. Crearemos y daremos nombre a las VLAN

```
S3>enable
S3#configure terminal
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#exit
S3>enable
S3#configure terminal
S3(config)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#exit
```

```
S3>enable
S3#configure terminal
S3(config)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
```

b. Asignamos la IPv4 a la VLAN de administración.

```
S3>enable
S3#configure terminal
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

c. Asignaremos la primera dirección IPv4 como gateway predeterminado.

```
S3>enable
S3#configure terminal
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
```

d. Forzaremos el enlace troncal en la interfaz F0/3, utilizando la red VLAN1 como VLAN native

```
S3>enable
S3#configure terminal
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#
```

e. Configuraremos los demas puertos como puertos de acceso

```
S3>enable
S3#configure terminal
S3(config)#interface range fa0/1-2, fa0/4-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

f. Asignaremos la interface F0/18 a la VLAN 21

```
S3>enable
S3#configure terminal
S3(config)#interface fa0/18
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
```

g. Apagar todos los puertos sin usar

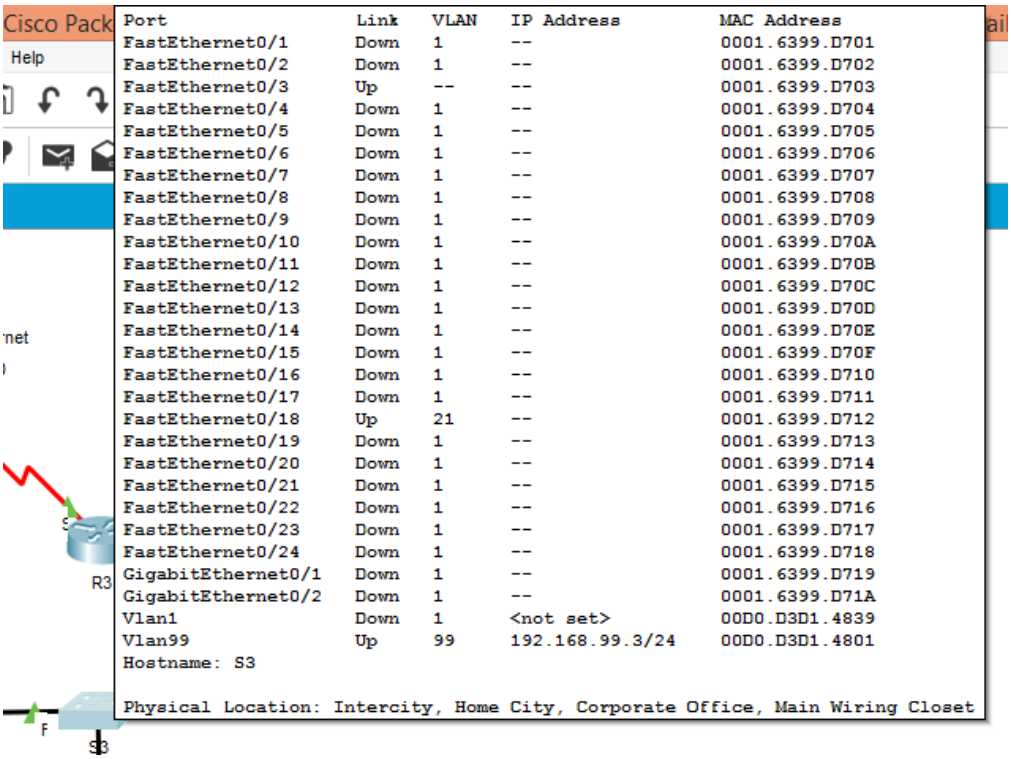


Figure 7 Puertos Apagados S3

Nota: Los puertos por defecto se encuentran apagados.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

a. Configuraremos la subinterfaz 802.1Q .21 en la interface G0/1

```
R1>enable
R1#configure terminal
R1(config)#interface g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```

b. Configuraremos la subinterfaz 802.1Q .23 en la interface G0/1

```
R1>enable
R1#configure terminal
R1(config)#interface g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```

c. Configuraremos la subinterfaz 802.1Q .99 en la interface G0/1

```
R1>enable
R1#configure terminal
R1(config)#interface g0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```

d. Activaremos la interfaz G0/1

```
R1>enable
R1#configure terminal
R1(config)#interface g0/1
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

a. Probaremos la conectividad desde S1 hacia R1, dirección VLAN 99 por medio de la IP 192.168.99.1

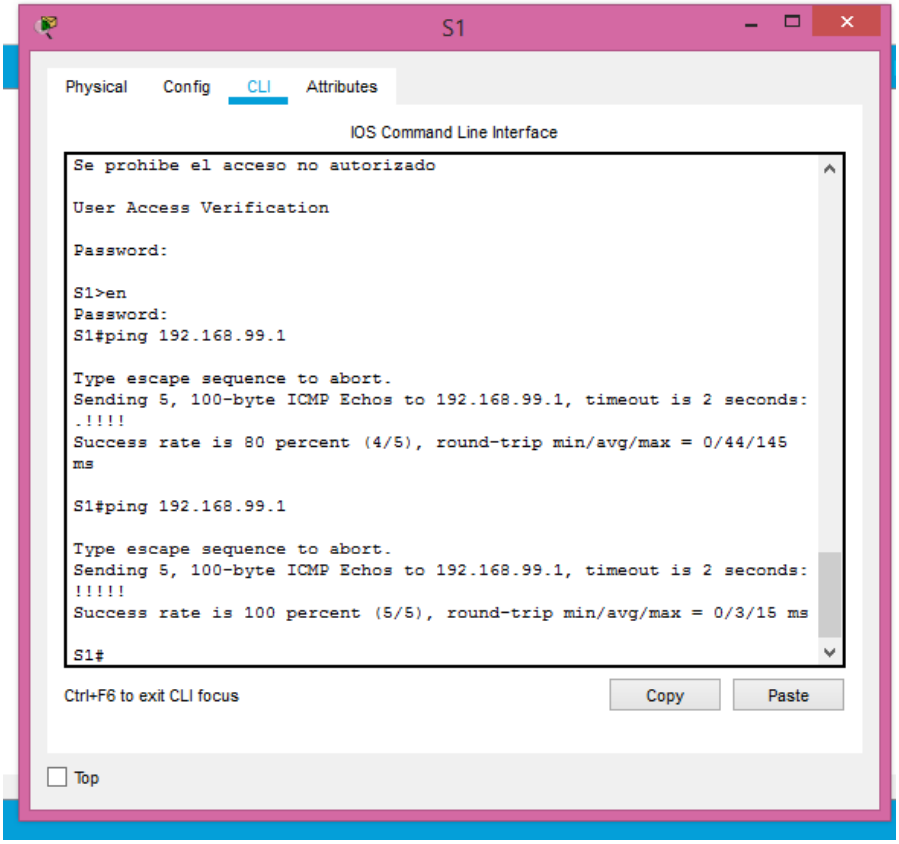


Figure 8 Comprobación conectividad S1 a R1

b. Probaremos la conectividad desde S3 hacia R1, dirección VLAN 99 por medio de la IP 192.168.99.1

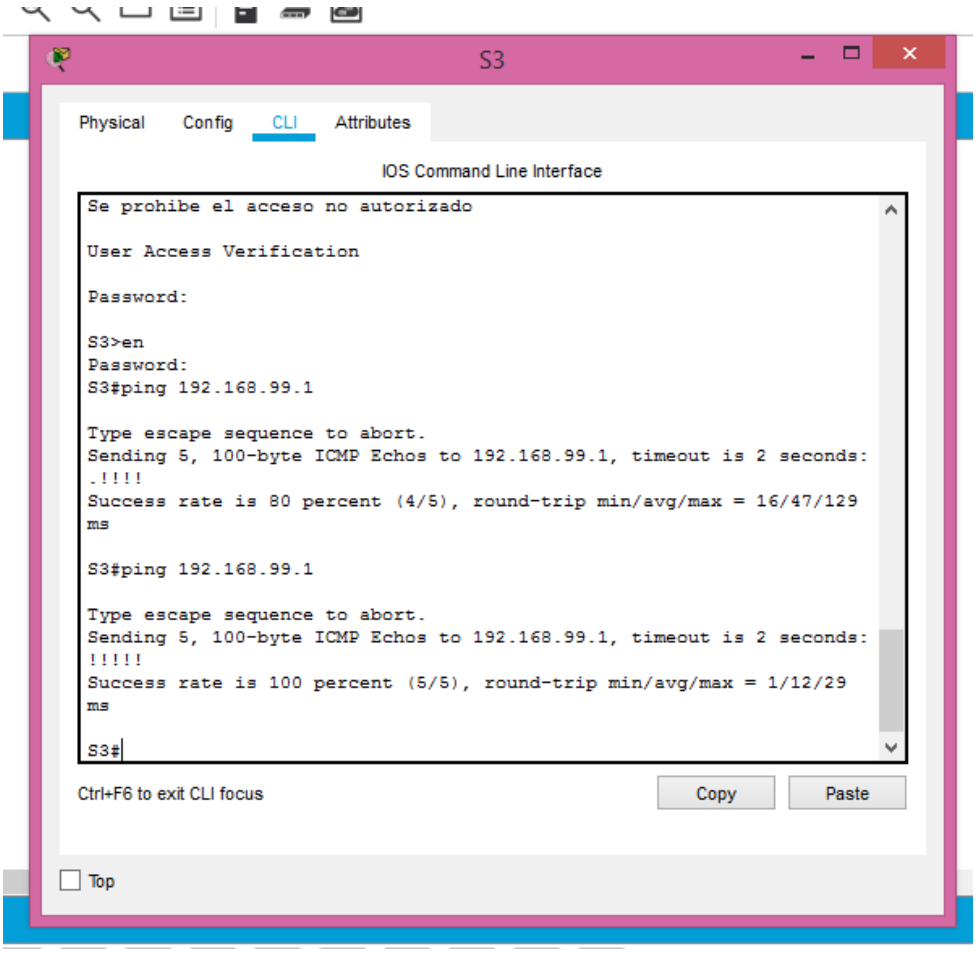


Figure 9 Comprobación conectividad S3 a R1

c. Probaremos la conectividad desde S1 hacia R1, dirección VLAN 21 por medio de la IP 192.168.21.1

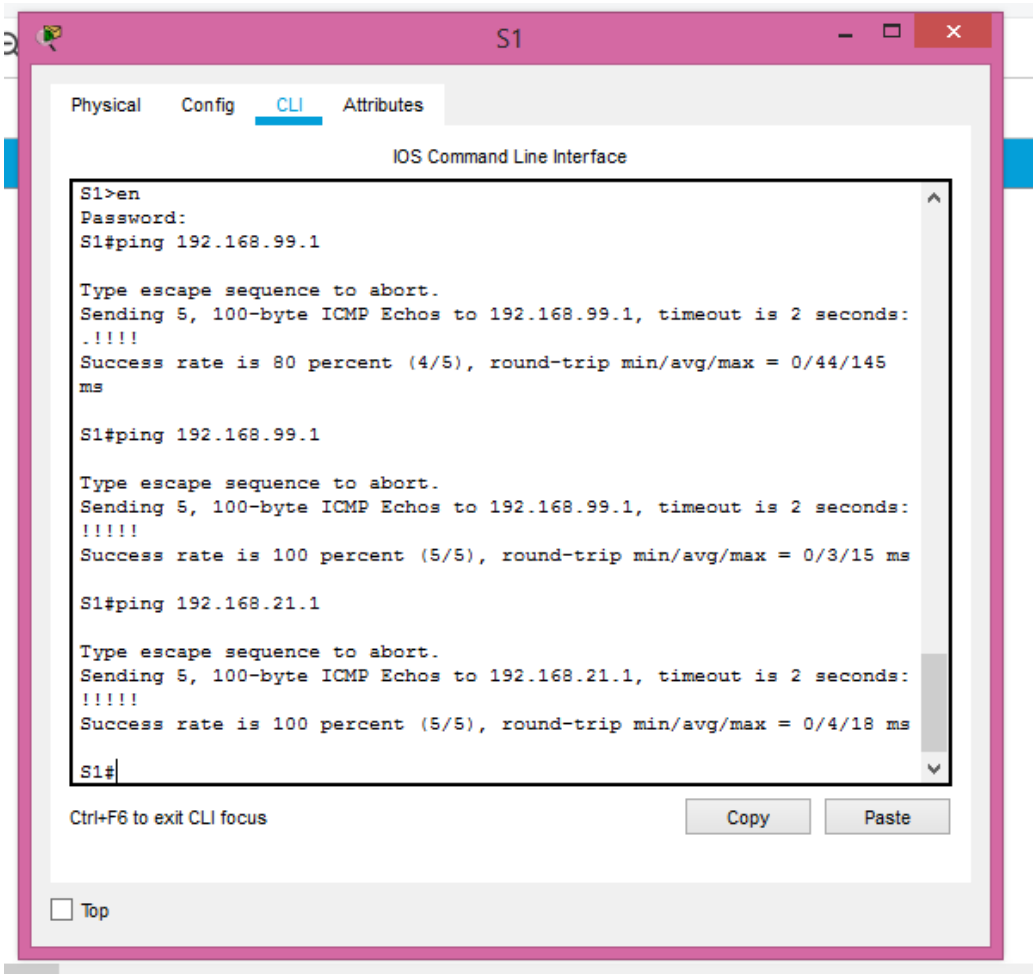


Figure 10 Comprobacion conectividad S1 a R1

d. Probaremos la conectividad desde S3 hacia R1, dirección VLAN 23 por medio de la IP 192.168.23.1

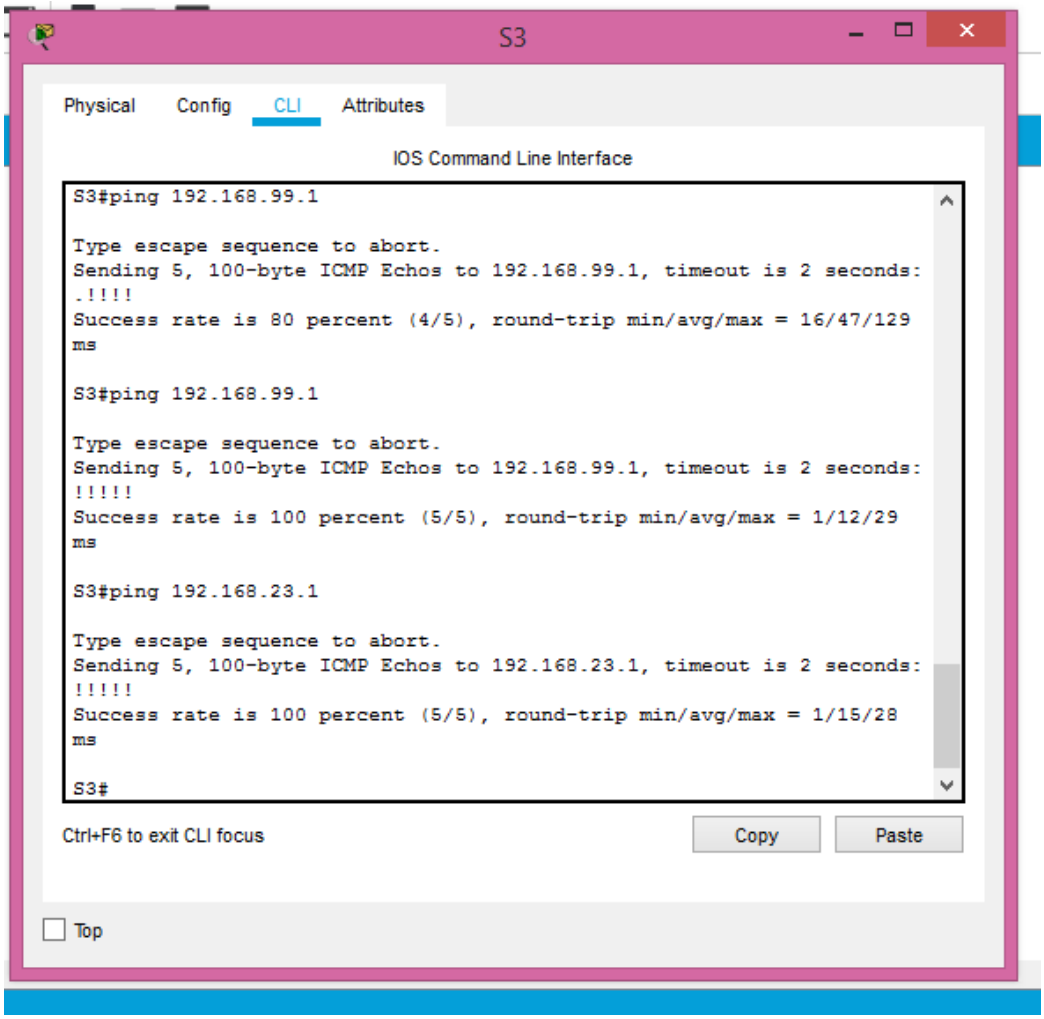


Figure 11 Comprobación conectividad S3 a R1

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Configuraremos el RIP version 2 en R1 anunciando las redes conectadas directamente, estableciendo interfaces LAN como pasivas y desactivando la sumarizacion automatica.

R1>enable

R1#configure terminal

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 172.16.1.0

R1(config-router)#network 192.168.99.0

R1(config-router)#network 192.168.23.0

R1(config-router)#network 192.168.21.0

R1(config-router)#passive-interface g0/0

R1(config-router)#passive-interface g0/1

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

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

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

R1(config-router)#no auto-summary

R1(config-router)#exit

R1(config)#exit

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Configuraremos el RIP version 2 en R2 anunciando las redes conectadas directamente, estableciendo interfaz LAN como pasivas y desactivando la sumarizacion automatica.

R2>enable

R2#configure terminal

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 172.16.1.0

R2(config-router)#network 172.16.2.0

R2(config-router)#network 10.10.10.0

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

R2(config-router)#no auto-summary

R2(config-router)#exit

R2(config)#

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:
Configuraremos el RIP version 2 en R3 anunciando las redes conectadas directamente, estableciendo interfaces LAN como pasivas y desactivando la sumarizacion automatica.

R3>enable

R3#configure terminal

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)#network 172.16.2.0

R3(config-router)#network 172.16.4.0

R3(config-router)#network 172.16.5.0

R3(config-router)#network 172.16.6.0

R3(config-router)#passive-interface loopback4

R3(config-router)#passive-interface loopback5

R3(config-router)#passive-interface loopback6

R3(config-router)#no auto-summary

R3(config-router)#exit

R3(config)#

Paso 4: Verificar la información de RIP

Verificaremos que RIP esté funcionando Como se espera. Introduciendo el comando de CLI adecuado para obtener la siguiente información:

a. ¿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?

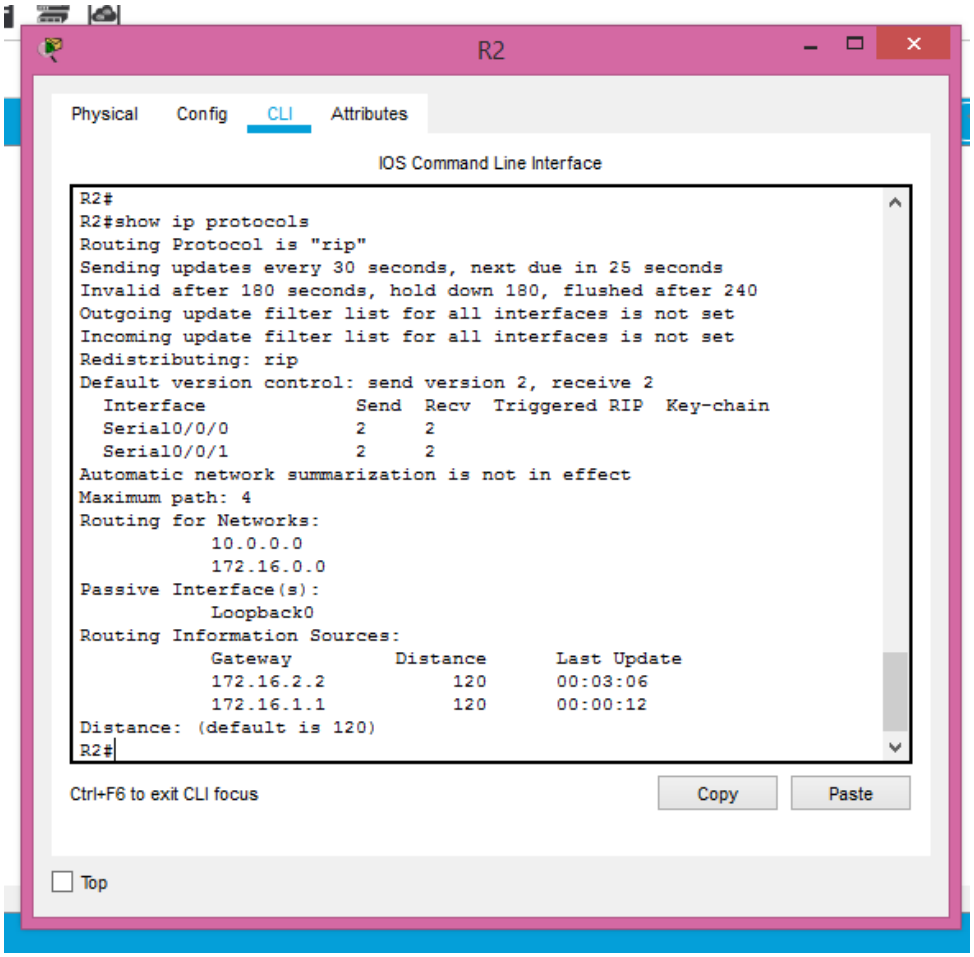


Figure 12 ID proceso RIP, ID Router, Redes Routing, Interfaces Pasivas

b. ¿Qué comando muestra solo las rutas RIP?

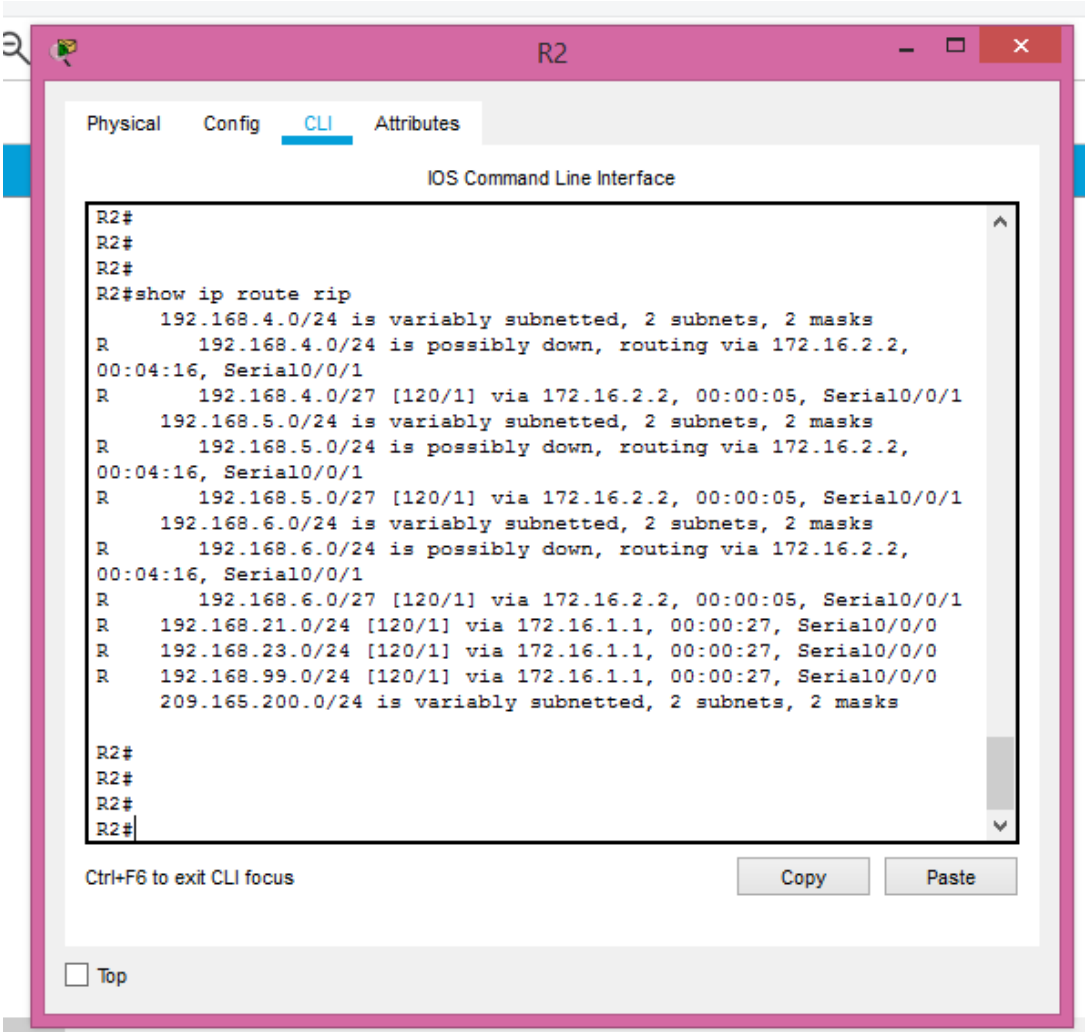


Figure 13 Rutas RIP

c. ¿Qué comando muestra la sección de RIP de la configuración en ejecución?

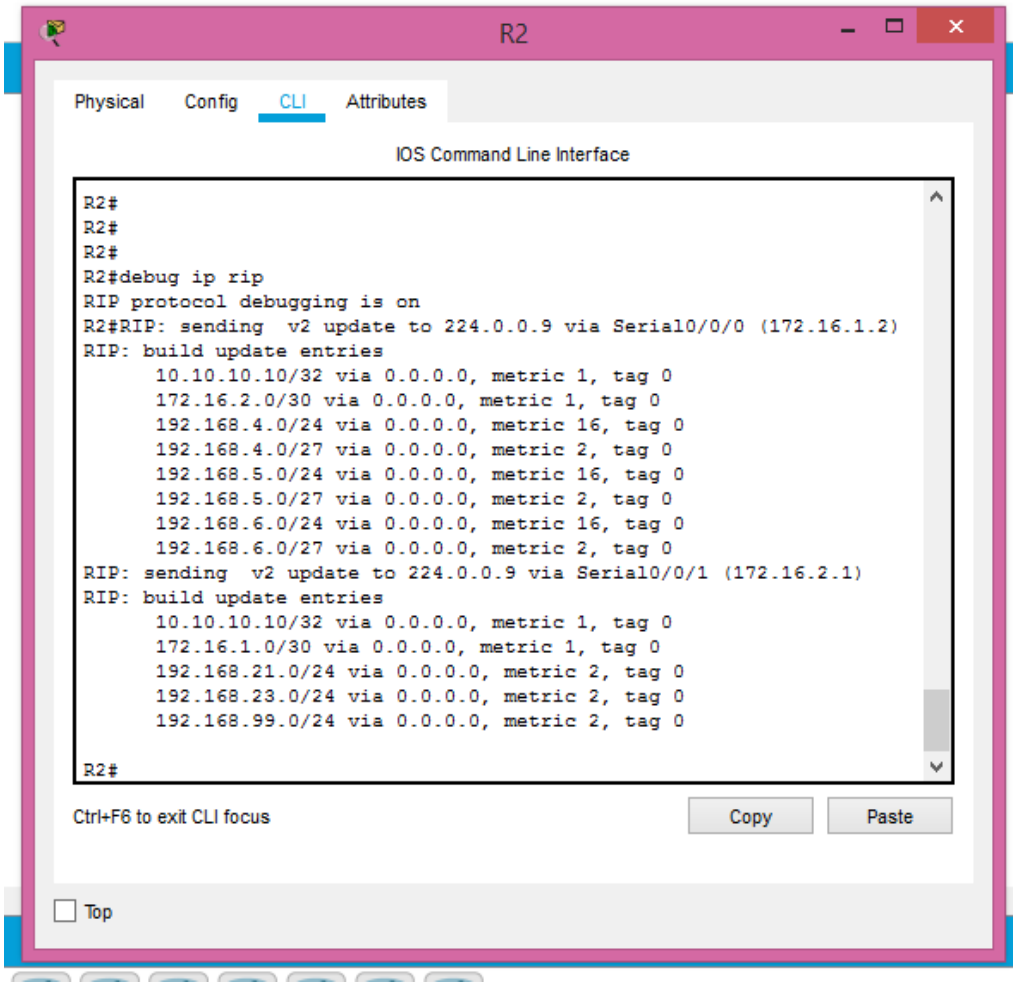


Figure 14 Seccion RIP configuracion en ejecución

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

a. Reservamos las primeras 20 direcciones IP en la VLAN 21 y 23 para configuraciones estáticas

R1>enable

```
R1#configure terminal
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.1.20
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
```

b. Creamos un pool de DHCP para la VLAN 21

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#
```

c. Creamos un pool de DHCP para la VLAN 23

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#
```

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

La configuración del R2 incluye las siguientes tareas:

a. Crearemos una base de datos local con una cuenta de usuario

```
R2>enable
R2#configure terminal
R2(config)#username webuser privilege 15 password cisco12345
R2(config)#line vty 0 15
R2(config-line)#login local
R2(config-line)#exit
```

b. Habilitaremos y configuraremos el servidor HTTP

```
R2(config)#ip http server
R2(config)#ip http authentication local
```

Nota: El programa no deja ejecutar el comando

c. Crearemos una NAT estática al servidor web y asignaremos la interfaz interna y externa

```
R2>enable
R2#configure terminal
R2(config)#ip nat inside source static 192.168.21.0 209.165.200.229
R2(config)#ip nat inside source static 192.168.23.0 209.165.200.229
R2(config)#
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
```

d. Configuraremos la NAT dinámica dentro de una ACL privada

```
R2>enable
R2#configure terminal
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 192.168.0.0 0.0.7.255
```

e. Definiremos el pool de direcciones IP públicas utilizables

```
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.0
```

f. Definiremos la traducción de NAT dinámica

```
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#interface s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

a. Verificamos que la PC-A haya adquirido información de IP del servidor de DHCP

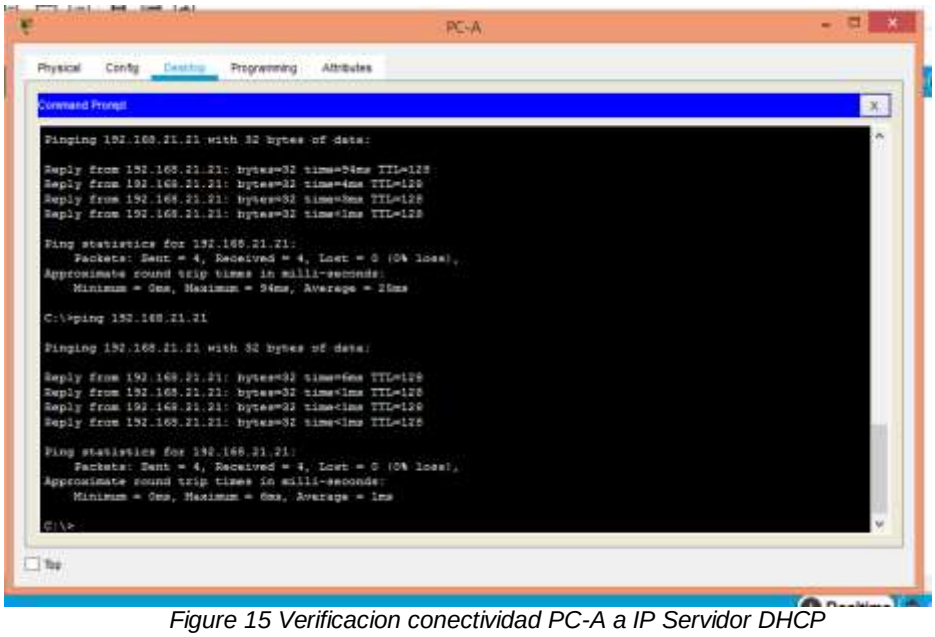


Figure 15 Verificacion conectividad PC-A a IP Servidor DHCP

b. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

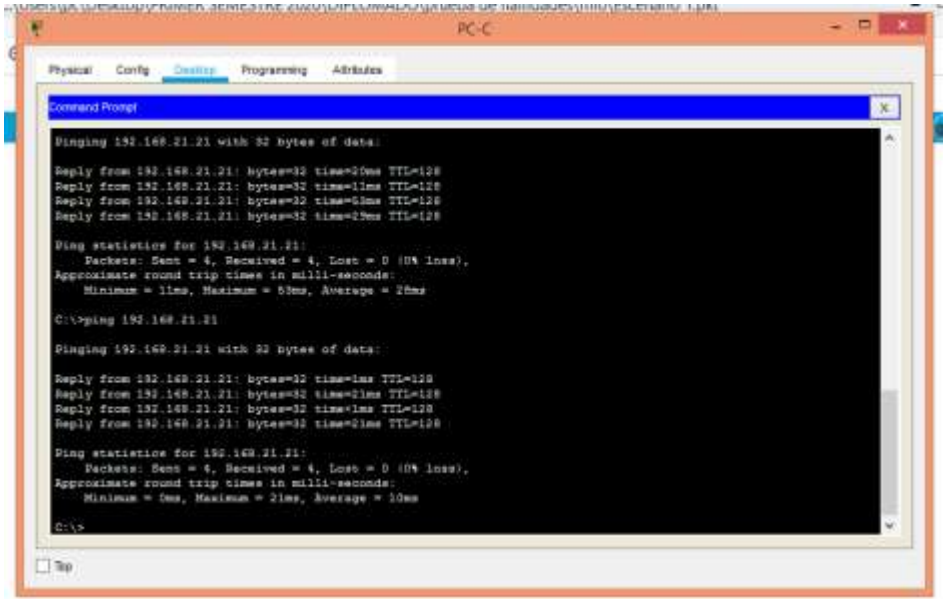


Figure 16 Verificacion conectividad PC-C a IP Servidor DHCP

c. Verificar que la PC-A pueda hacer ping a la PC-C

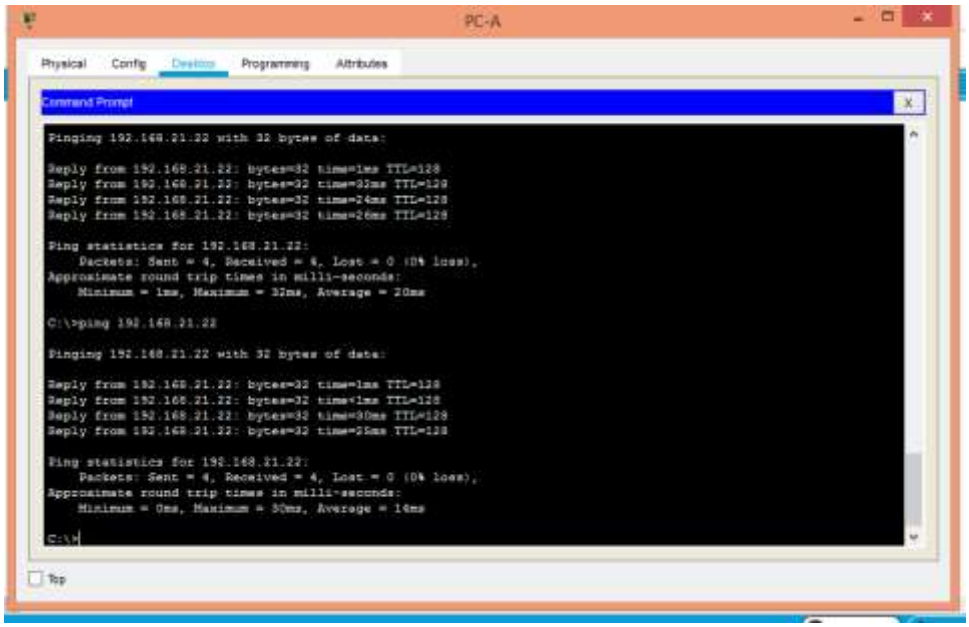


Figure 17 Verificacion conectividad PC-A a PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.

d. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

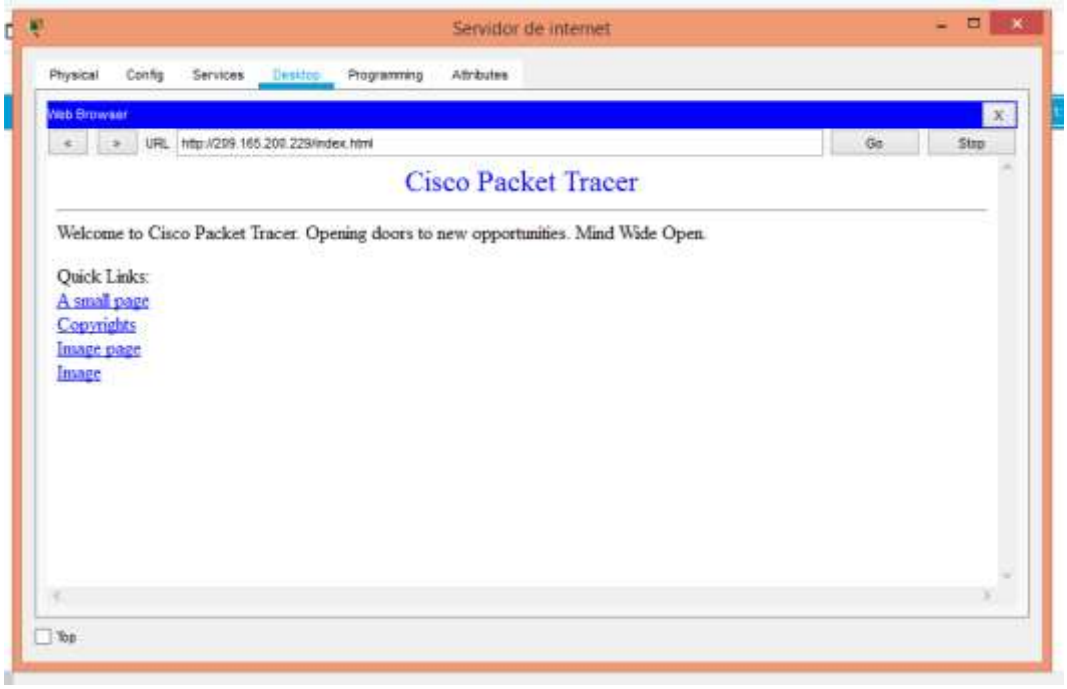


Figure 18 Acceder al Servidor Web

Parte 6: Configurar NTP

a. Ajustamos la fecha y hora en R2, configuramos R2 como un maestro NTP

```
R2>enable
R2#clock set 09:00 15 may 2020
R2#configure terminal
R2(config)#ntp master 5
R2(config)#exit
```

b. Configuramos R1 como cliente NTP y actualizaciones de calendario periódicas con hora NTP

```
R1>enable
R1#configure terminal
```

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

c. Verificamos la configuración NTP en R1 con el comando **show ntp status**

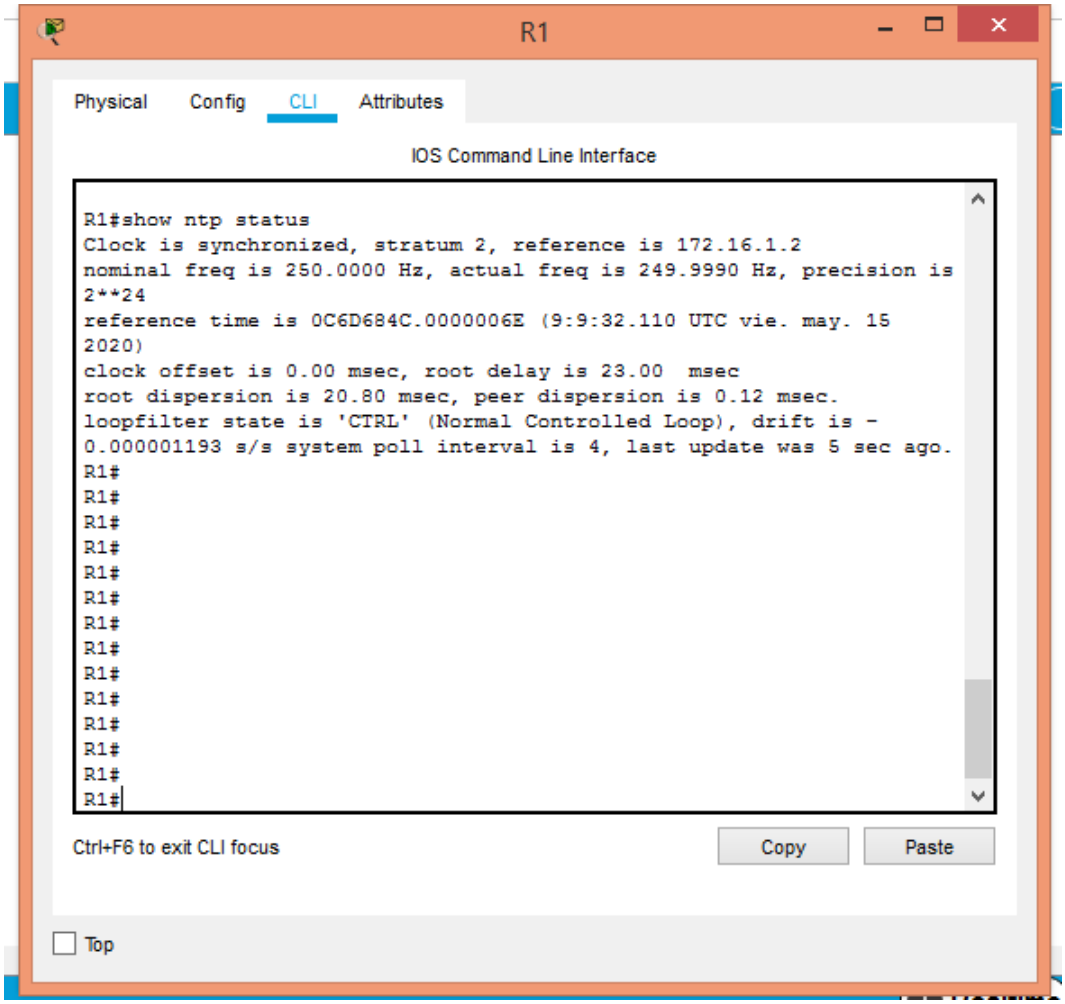


Figure 19 Verificar configuracion NTP en R1

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

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

a. Configuramos la lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

```
R2>enable
R2#configure terminal
R2(config)#ip access-list standar ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#deny any
R2(config-std-nacl)#exit
```

b. Aplicamos la ACL con nombre a las líneas VTY, permitimos el acceso por telnet a las líneas VTY

```
R2>enable
R2#configure terminal
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
```

c. Verificamos que la ACL funcione como se espera

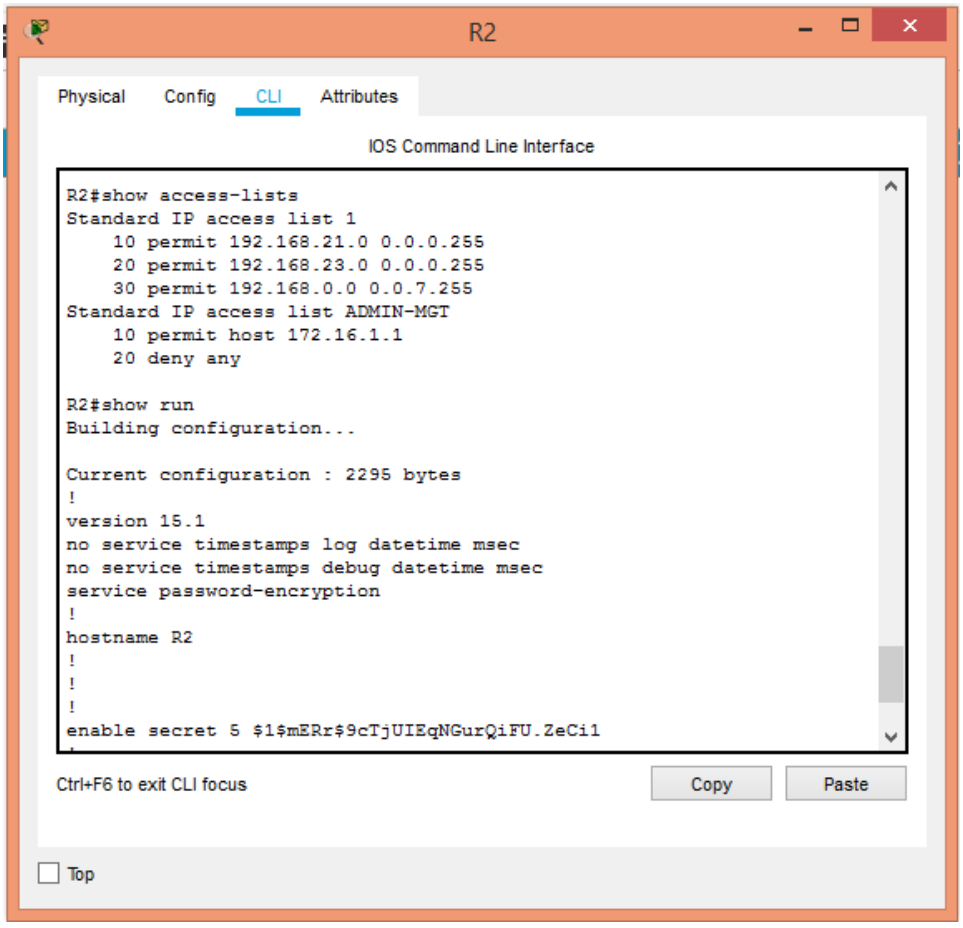


Figure 20 Funcionamiento de la ACL

Paso 1: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

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

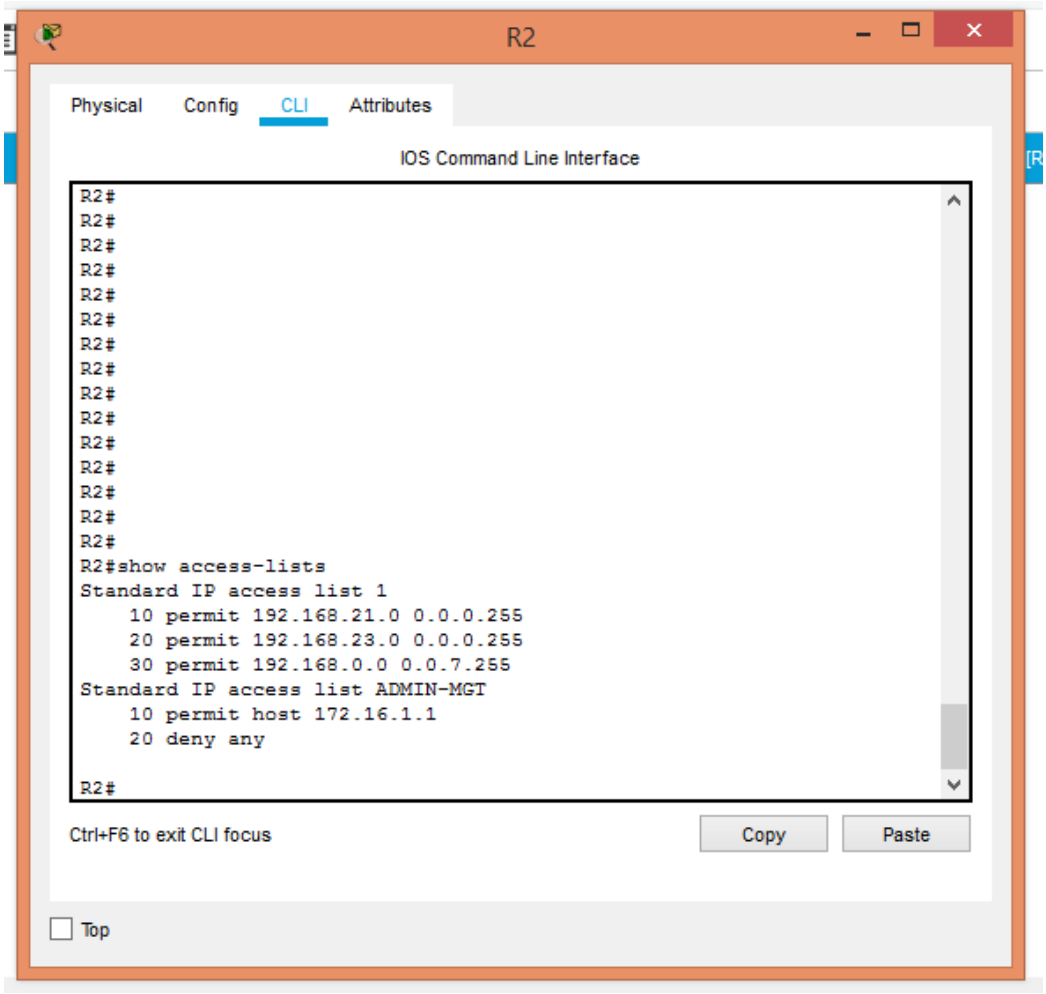


Figure 21 Coincidencias Recibidas

b. Restablecer los contadores de una lista de acceso

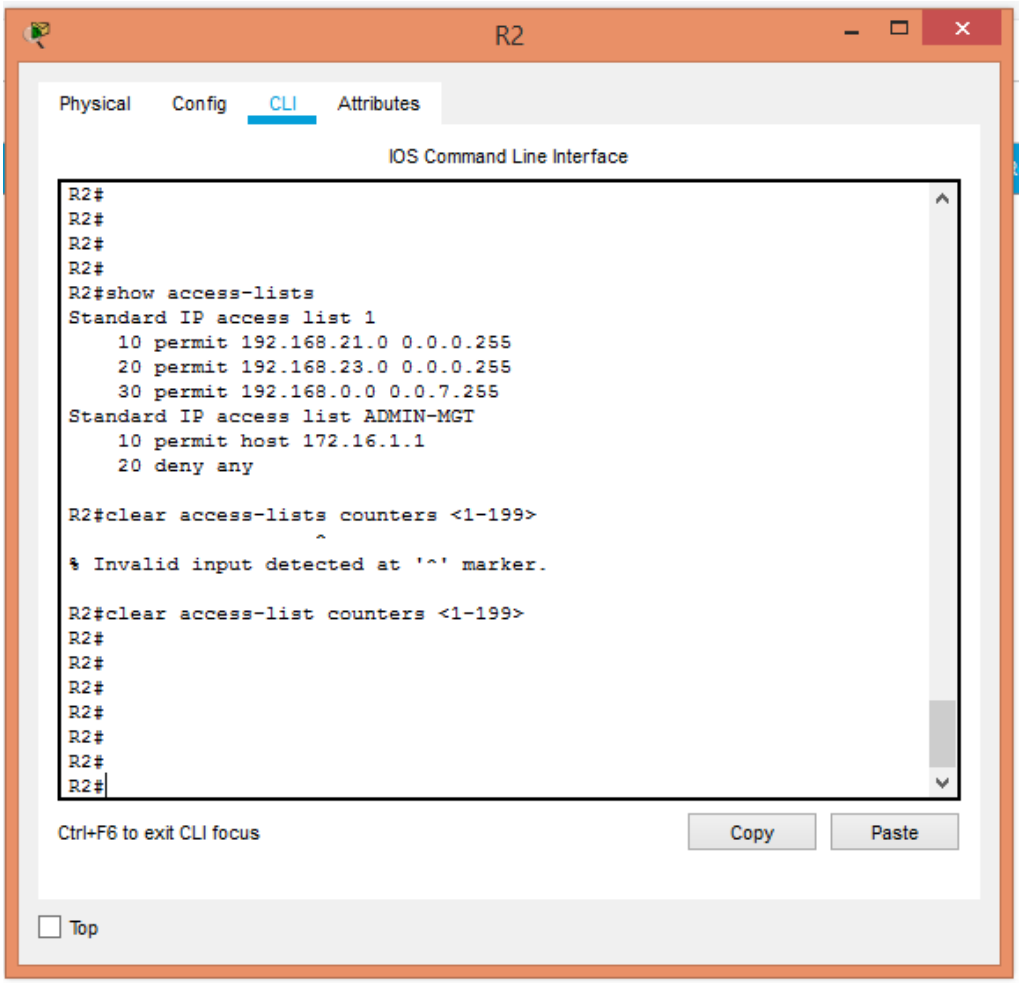


Figure 22 Restablecimiento de contadores

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

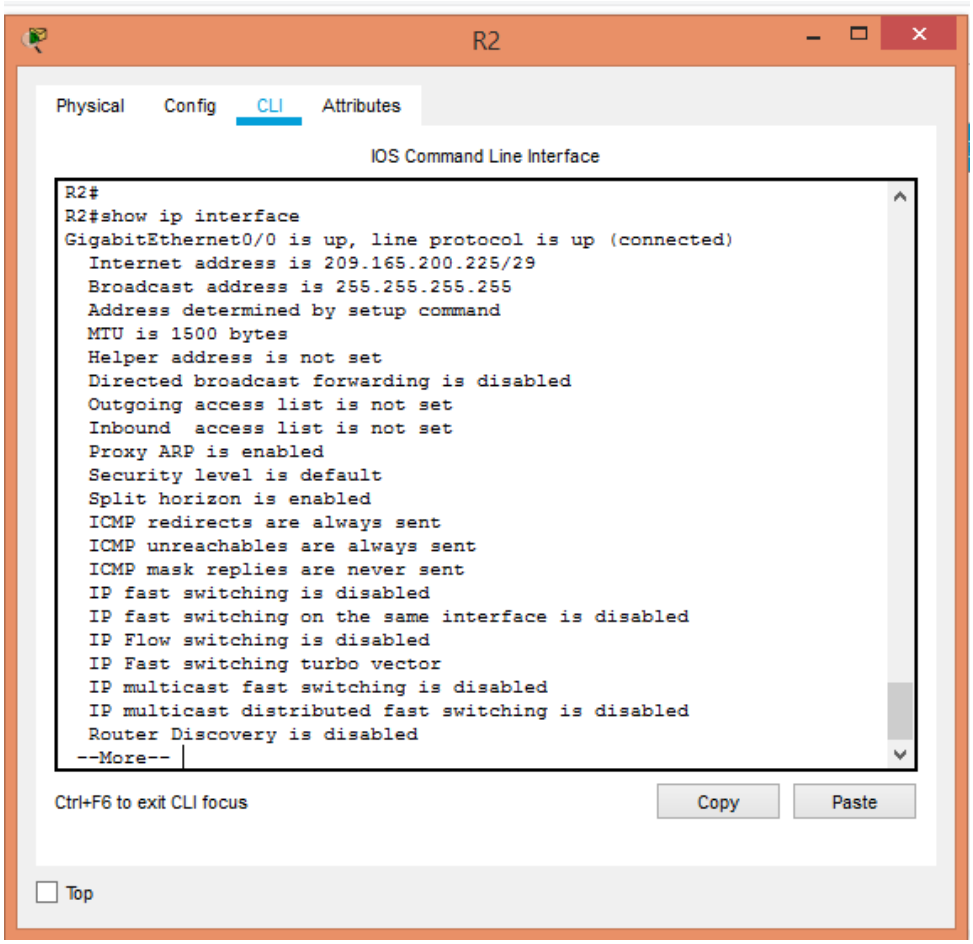


Figure 23 ACL aplicada a la interfaz

d. ¿Con qué comando se muestran las traducciones NAT?

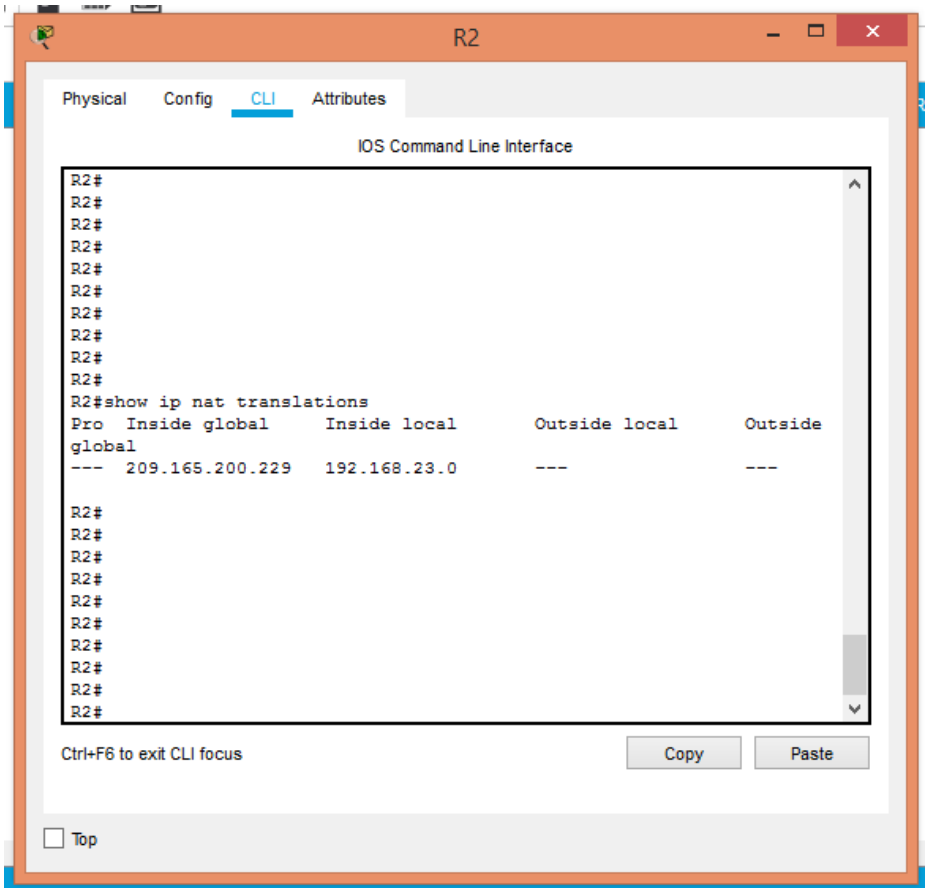


Figure 24 Traducciones NAT

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.

e. ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

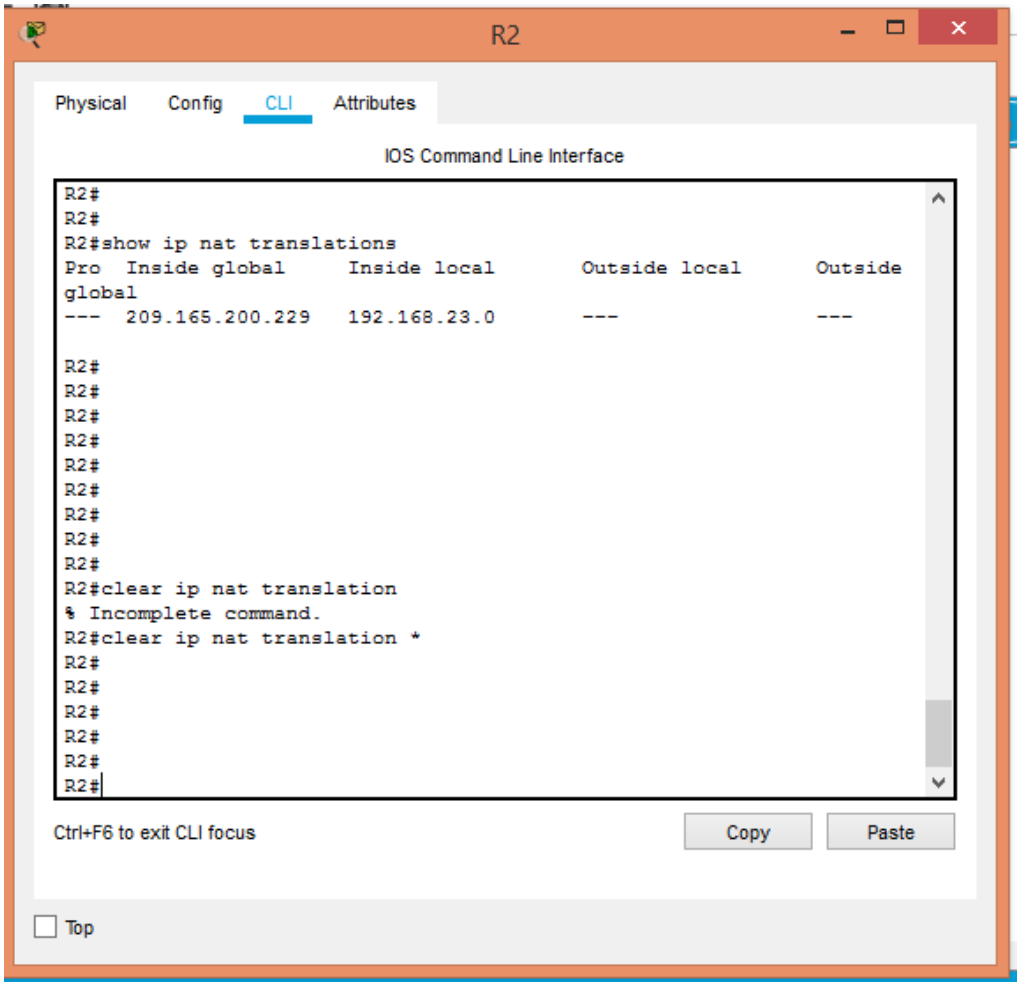


Figure 25 Eliminar traducciones NAT

3.2. Escenario 2

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

Topología de red

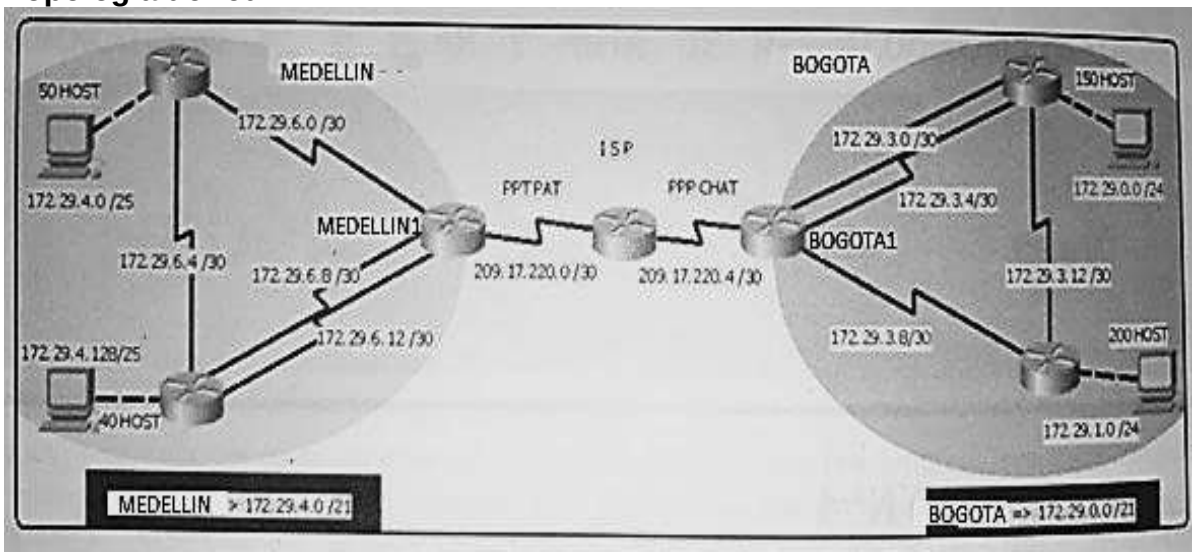


Figure 26 Topologia Escenario 2

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

Parte 1: Configuración del enrutamiento

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

- ✓ **ISP:**

```
ISP>enable
ISP(config)#router ospf 1
ISP(config-router)#router-id 1.1.1.1
ISP(config-router)#no network 209.17.220.4 0.0.0.3 area 1
ISP(config-router)#no network 209.17.220.4 0.0.0.3 area 2
ISP(config-router)#exit
ISP(config)#ip default-network 209.17.220.0
```

- ✓ **BOGOTA1:**

```
BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 2.2.2.2
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 2
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 2
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 2
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 2
BOGOTA1(config-router)#exit
BOGOTA1(config)#ip default-network 172.29.3.0
```

- ✓ **BOGOTA2:**

```
BOGOTA2>enable
BOGOTA2#configure terminal
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 3.3.3.3
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 2
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 2
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 2
BOGOTA2(config-router)#exit
BOGOTA2(config)#ip default-network 172.29.3.0
```

- ✓ **BOGOTA3:**

```
BOGOTA3>enable
BOGOTA3#configure terminal
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 4.4.4.4
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 2
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 2
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 2
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.3 area 2
BOGOTA3(config-router)#exit
BOGOTA3(config)#ip default-network 172.29.3.0
```

- ✓ **MEDELLIN1:**

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 5.5.5.5
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)#exit
MEDELLIN1(config)#ip default-network 172.29.6.0

- ✓ **MEDELLIN2:**

MEDELLIN2>enable
MEDELLIN2#configure terminal
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 6.6.6.6
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)#exit
MEDELLIN2(config)#ip default-network 172.29.6.0

- ✓ **MEDELLIN3:**

MEDELLIN3>enable
MEDELLIN3#configure terminal
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 7.7.7.7
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)#exit
MEDELLIN3(config)#ip default-network 172.29.6.0

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

- ✓ **BOGOTA1:**

```
BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#redistribute connected subnets tag 1
BOGOTA1(config-router)#exit
```

- ✓ **MEDELLIN1:**

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#redistribute connected subnets tag 1
MEDELLIN1(config-router)#exit
```

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

```
ISP>enable
ISP#configure terminal
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial 0/0/1
```

Parte 2: Tabla de Enrutamiento.

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

b. Verificar el balanceo de carga que presentan los routers.

c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

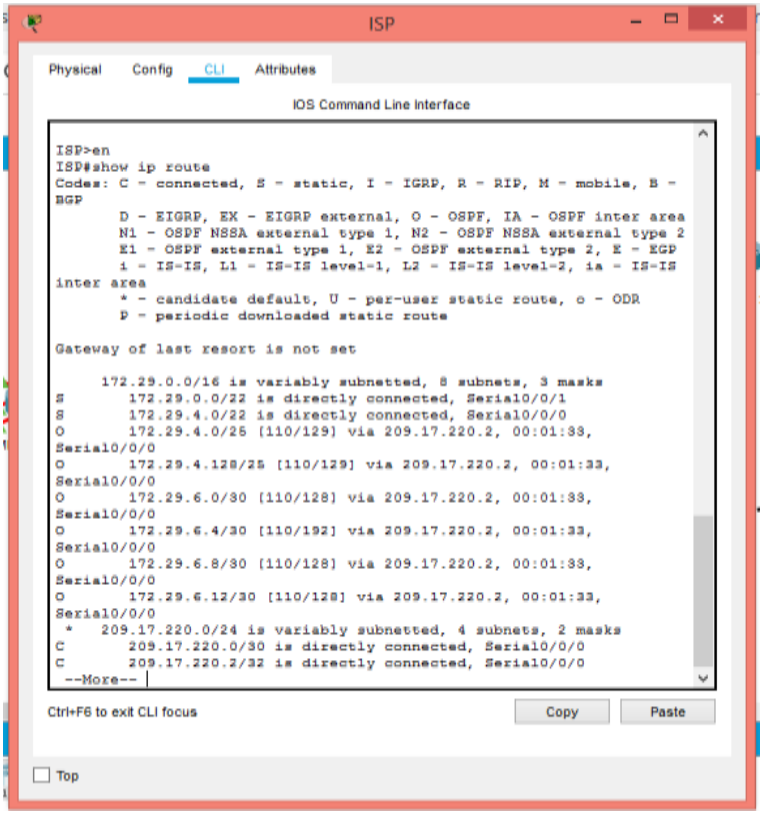


Figure 27 Tabla enrutamiento y balanceo de cargas del ISP

Figure 28 Tabla enrutamiento y balanceo de cargas del BOGOTA1

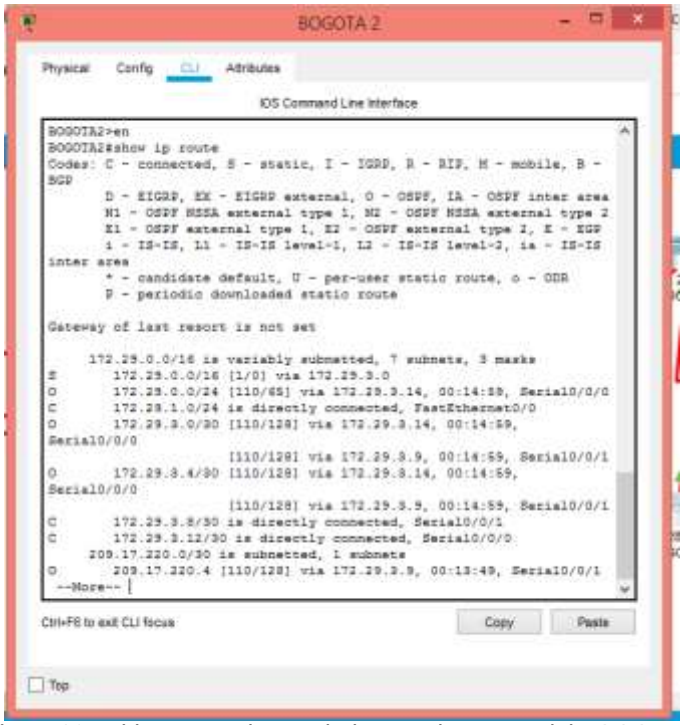


Figure 29 Tabla enrutamiento y balanceo de cargas del BOGOTA 2

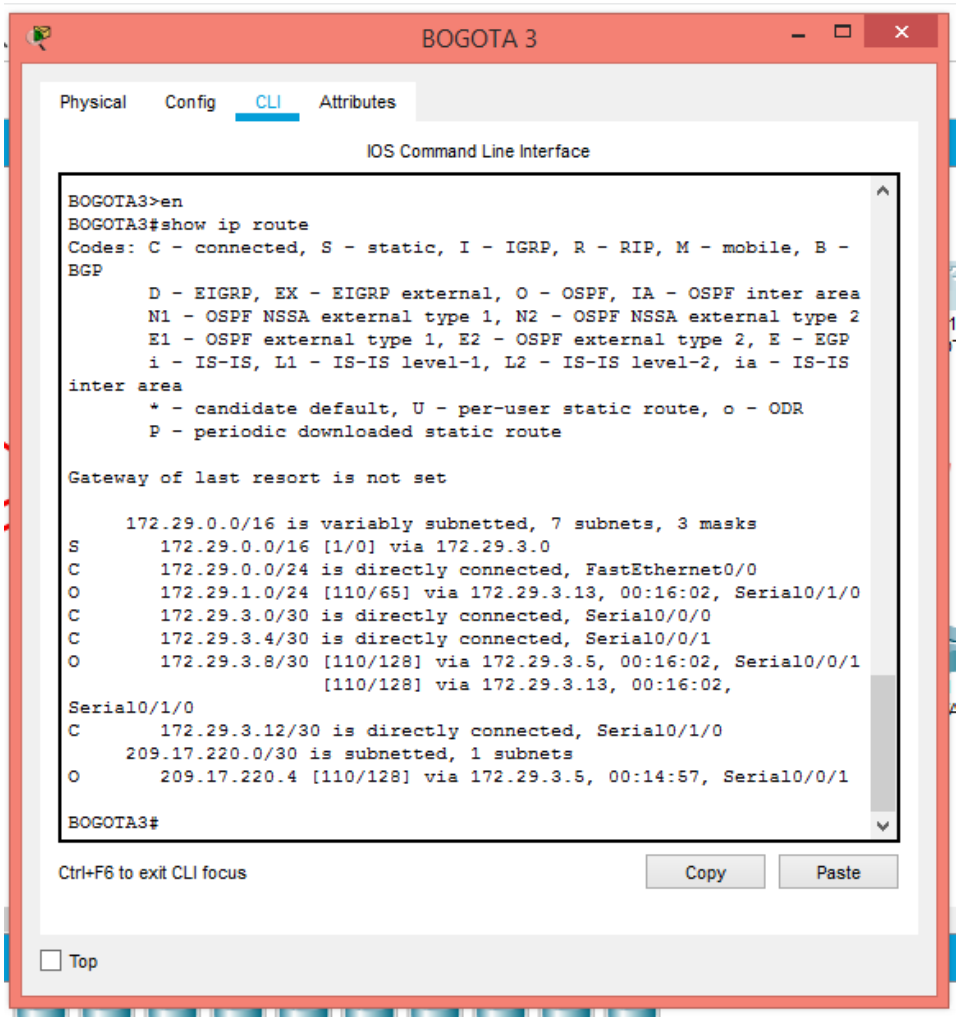


Figure 30 Tabla enrutamiento y balanceo de cargas del BOGOTA 3

Figure 31 Tabla enrutamiento y balanceo de cargas del MEDELLIN 1

Figure 32 Tabla enrutamiento y balanceo de cargas del MEDELLIN 2

Figure 33 Tabla enrutamiento y balanceo de cargas del MEDELLIN 3

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Tabla 2. Interfaces correspondiente a los routers

- ✓ **ISP:**

```
ISP>enable
ISP#configure terminal
ISP(config)#router ospf 1
ISP(config-router)#passive-interface fastethernet0/0
ISP(config-router)#passive-interface fastethernet0/1
ISP(config-router)#passive-interface Vlan1
ISP(config-router)#exit
```

- ✓ **BOGOTA1:**

```
BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface fastethernet0/0
BOGOTA1(config-router)#passive-interface fastethernet0/1
BOGOTA1(config-router)#passive-interface Vlan1
BOGOTA1(config-router)#exit
```

- ✓ **BOGOTA2:**

```
BOGOTA2>enable
BOGOTA2#configure terminal
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface fastethernet 0/0
BOGOTA2(config-router)#passive-interface fastethernet 0/1
BOGOTA2(config-router)#passive-interface Vlan1
BOGOTA2(config-router)#exit
```

- ✓ **BOGOTA3:**

```
BOGOTA3>enable
BOGOTA3#configure terminal
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface fastethernet0/0
BOGOTA3(config-router)#passive-interface fastethernet0/1
BOGOTA3(config-router)#passive-interface serial0/1/1
BOGOTA3(config-router)#passive-interface Vlan1
BOGOTA3(config-router)#exit
```

- ✓ **MEDELLIN1:**

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface fastethernet0/0
MEDELLIN1(config-router)#passive-interface fastethernet0/1
MEDELLIN1(config-router)#passive-interface Vlan1
MEDELLIN1(config-router)#exit
```

- ✓ **MEDELLIN2:**

```
MEDELLIN2>enable
MEDELLIN2#configure terminal
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface fastethernet0/0
MEDELLIN2(config-router)#passive-interface fastethernet0/1
MEDELLIN2(config-router)#passive-interface Vlan1
MEDELLIN2(config-router)#exit
```

- ✓ **MEDELLIN3:**

```
MEDELLIN3>enable
MEDELLIN3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface fastethernet0/0
```

MEDELLIN3(config-router)#passive-interface fastethernet0/1
MEDELLIN3(config-router)#passive-interface serial 0/0/0
MEDELLIN3(config-router)#passive-interface Vlan1
MEDELLIN3(config-router)#exit

Parte 4: Verificación del protocolo OSPF.

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

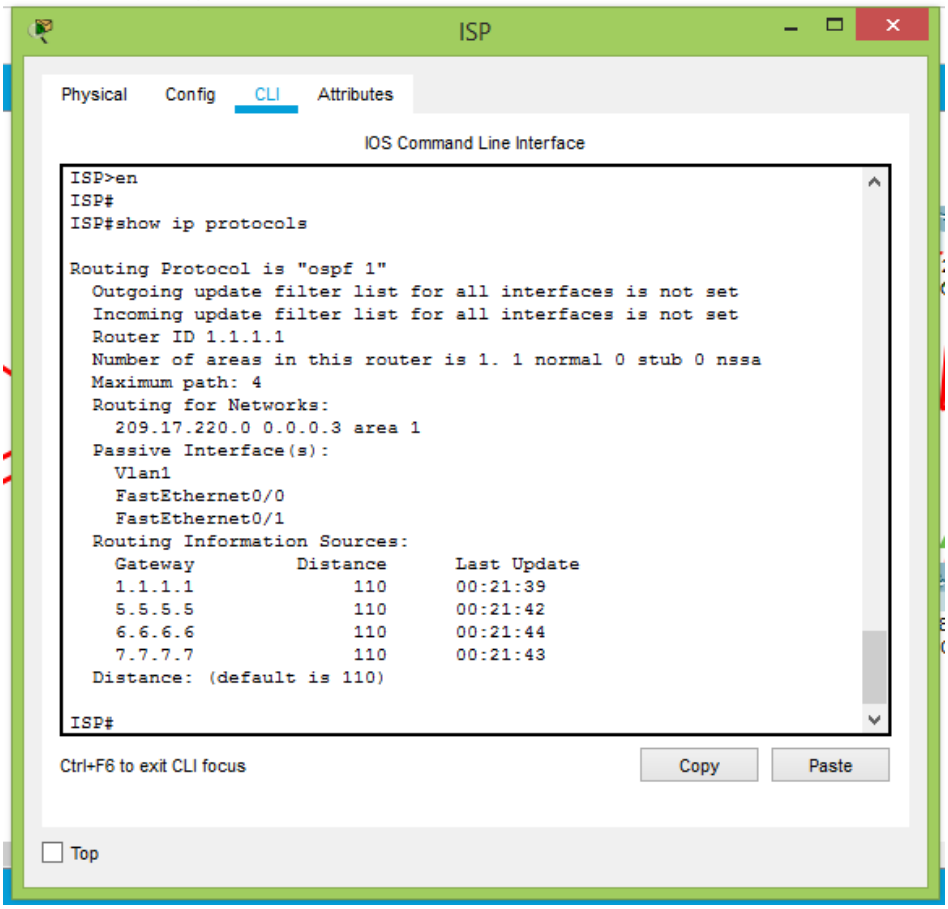


Figure 34 Opciones de enrutamiento ISP

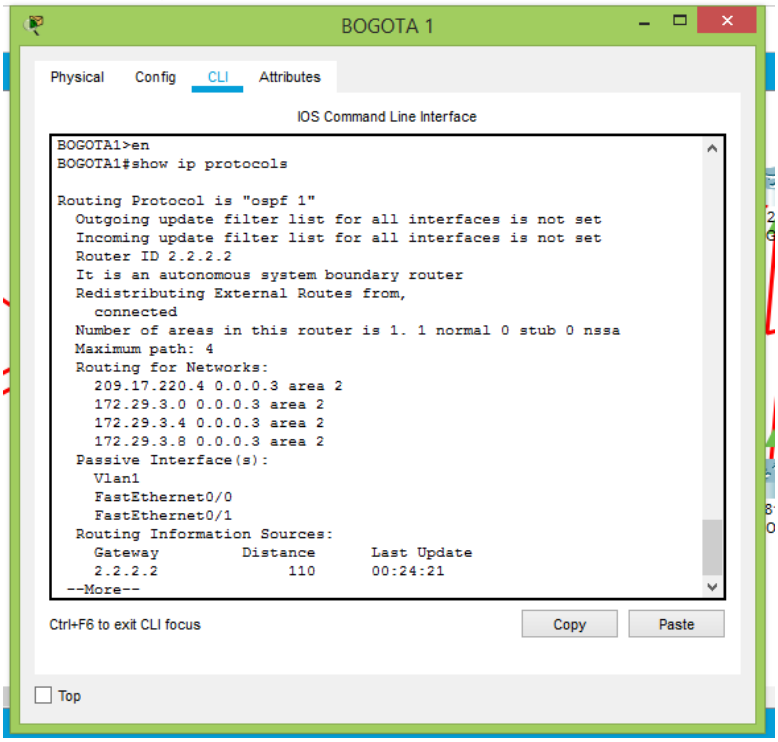


Figure 35 Opciones de enrutamiento BOGOTA 1

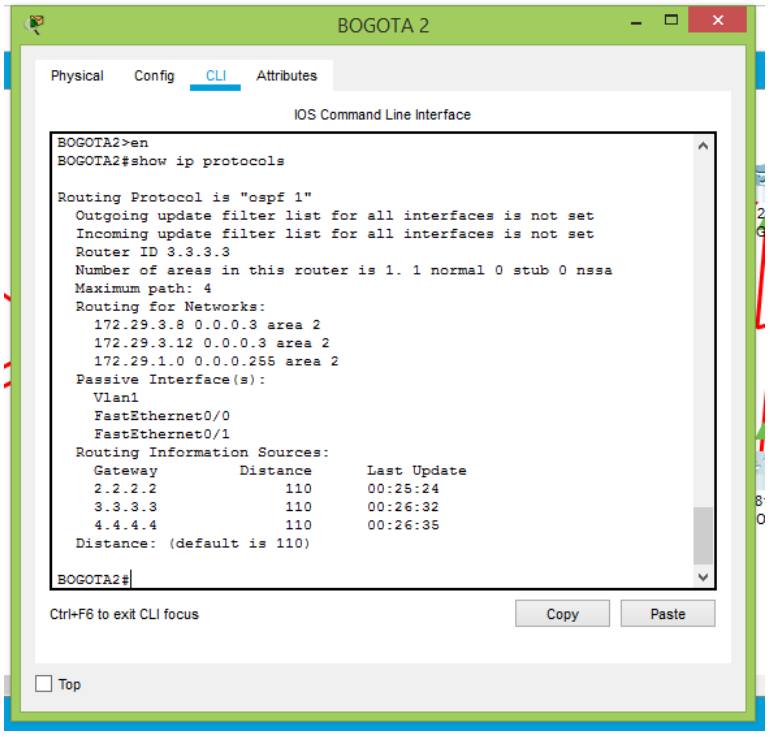


Figure 36 Opciones de enrutamiento BOGOTA 2

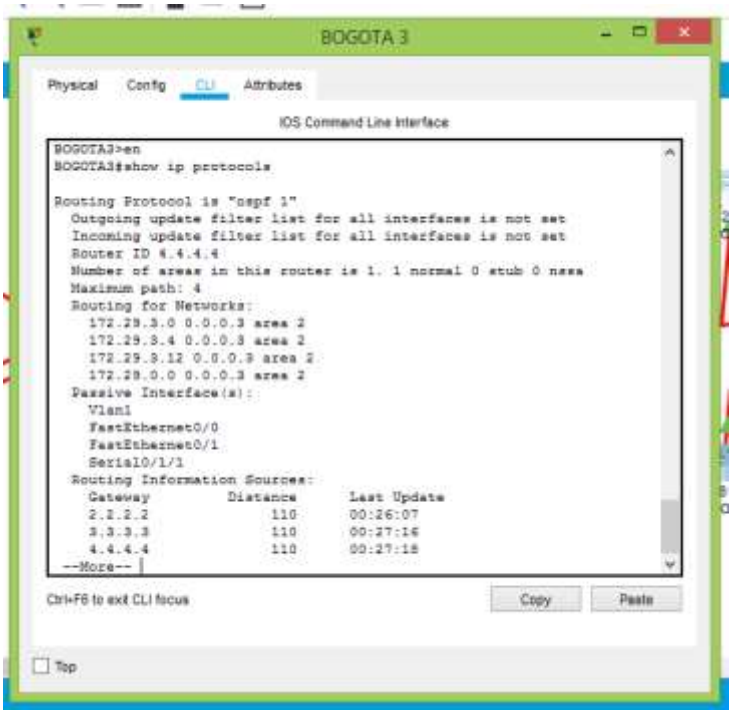


Figure 37 Opciones de enrutamiento BOGOTA 3

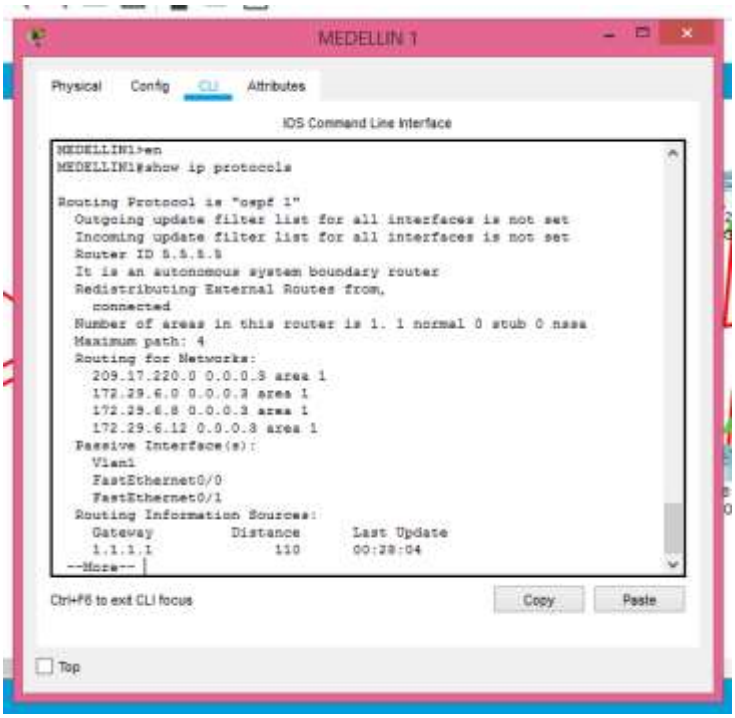


Figure 38 Opciones de enrutamiento MEDELLIN 1

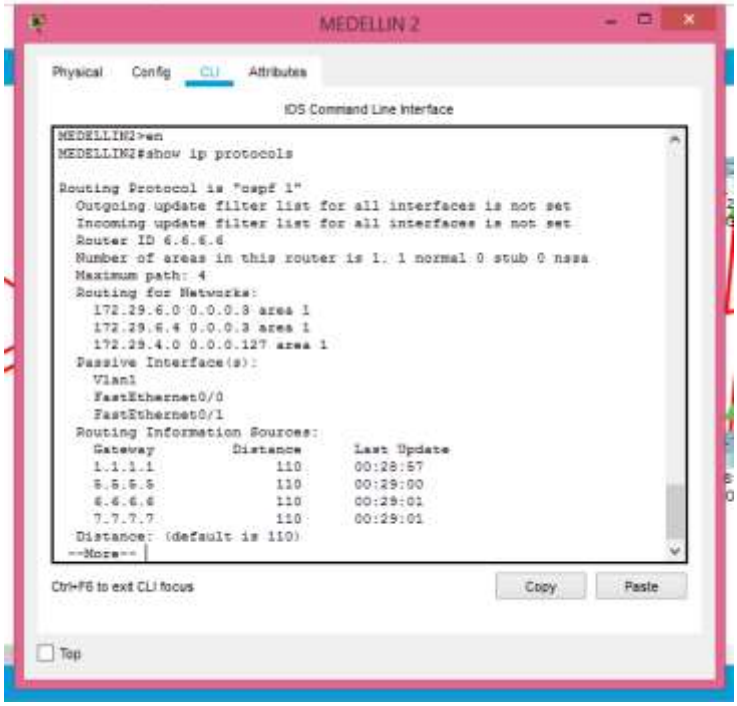


Figure 39 Opciones de enrutamiento MEDELLIN 2

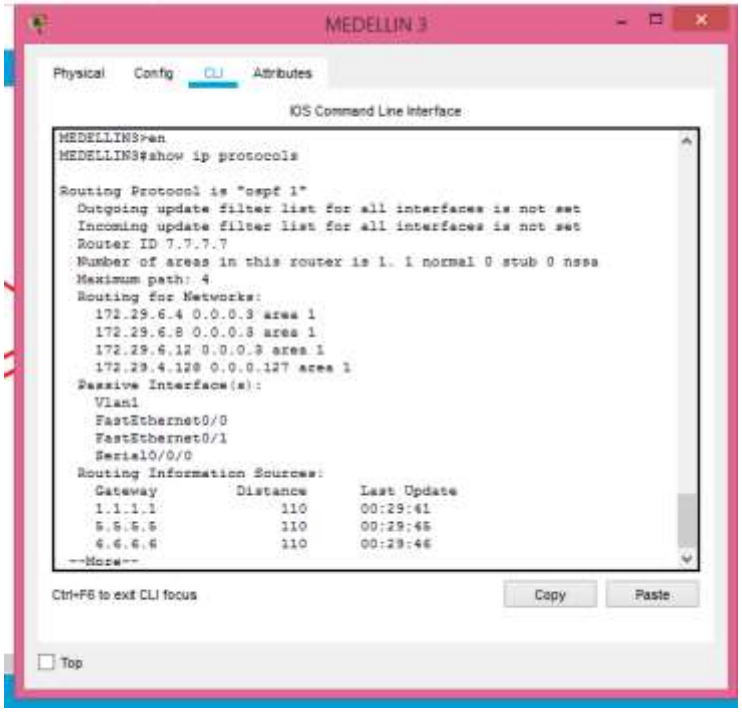


Figure 40 Opciones de enrutamiento MEDELLIN 3

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

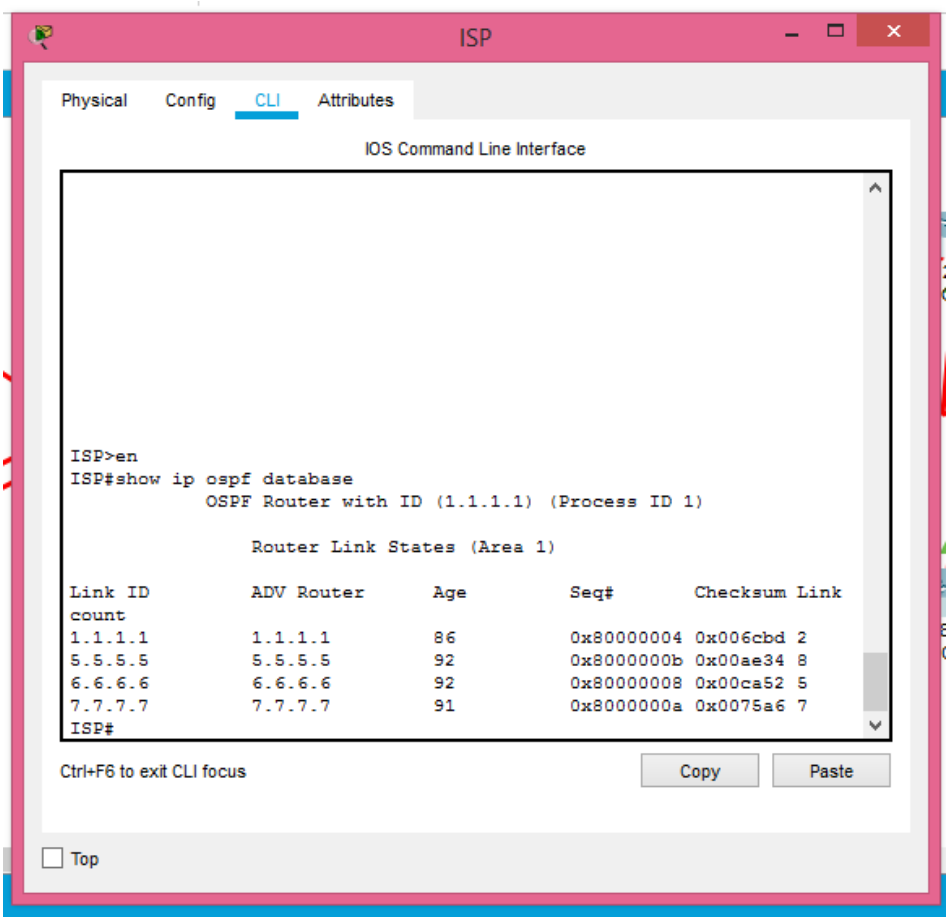


Figure 41 Base de datos OSPF ISP

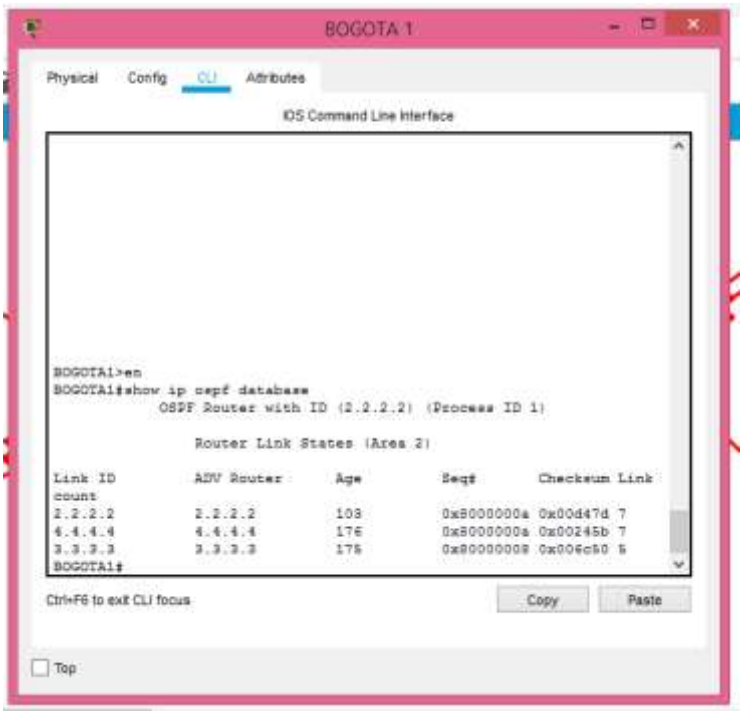


Figure 42 Base de datos OSPF BOGOTA 1

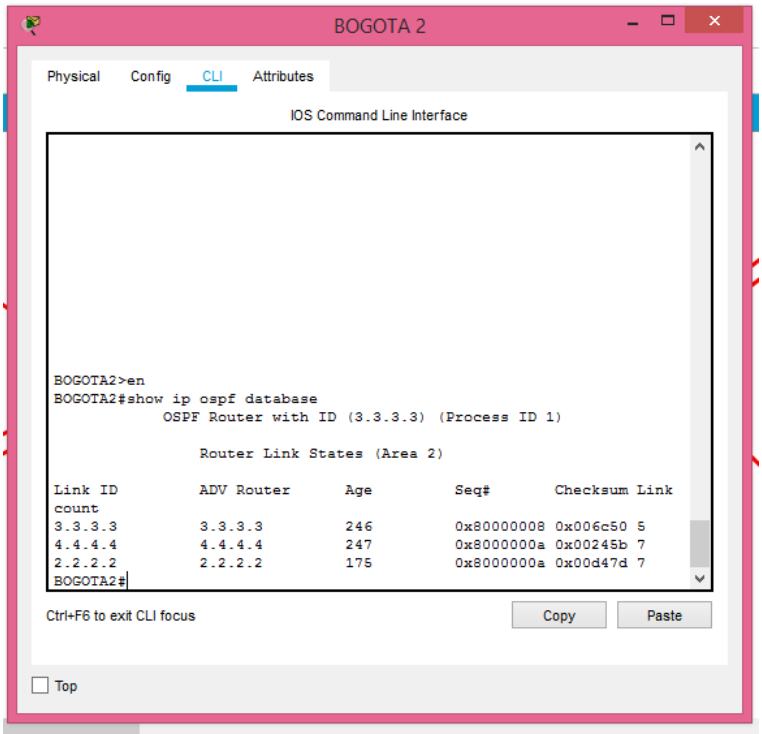


Figure 43 Base de datos OSPF BOGOTA 2

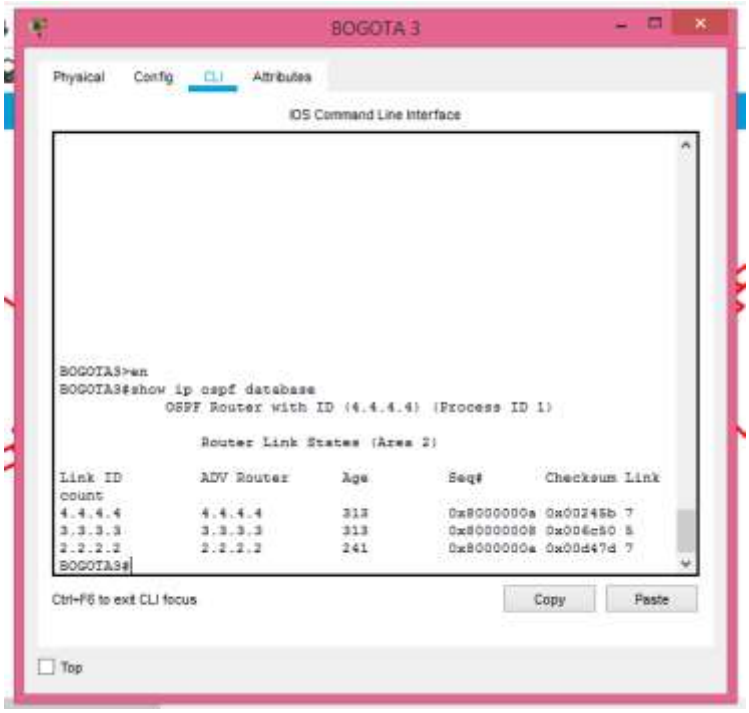


Figure 44 Base de datos OSPF BOGOTA 3

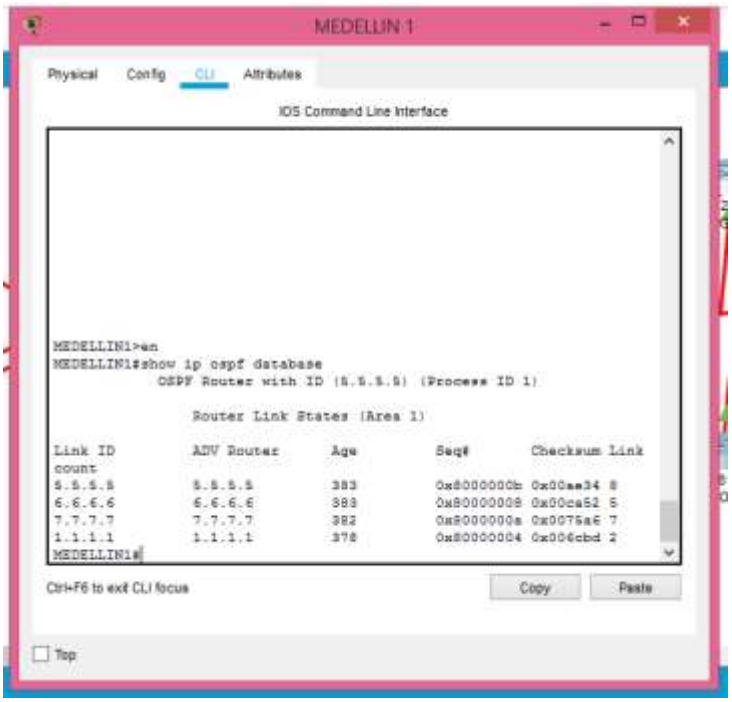


Figure 45 Base de datos OSPF MEDELLIN 1

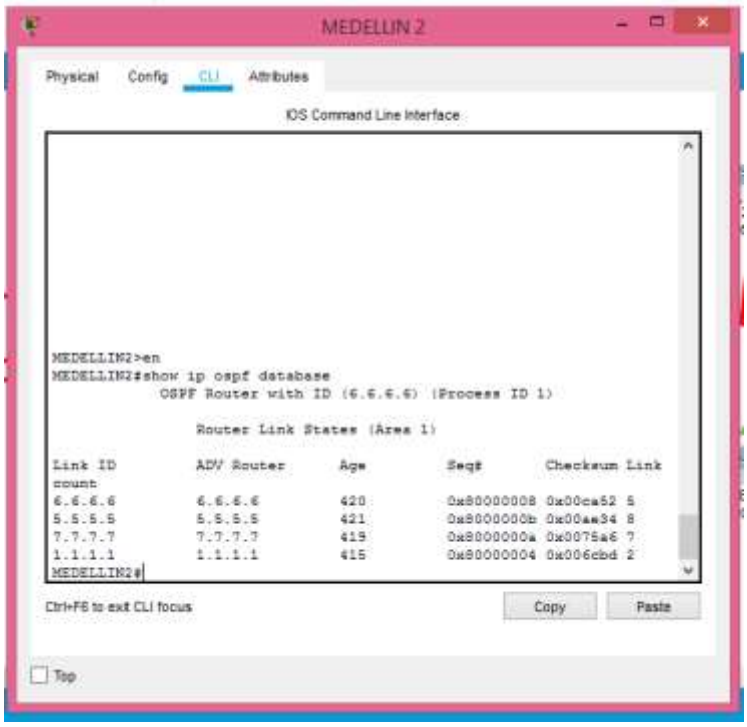


Figure 46 Base de datos OSPF MEDELLIN 2

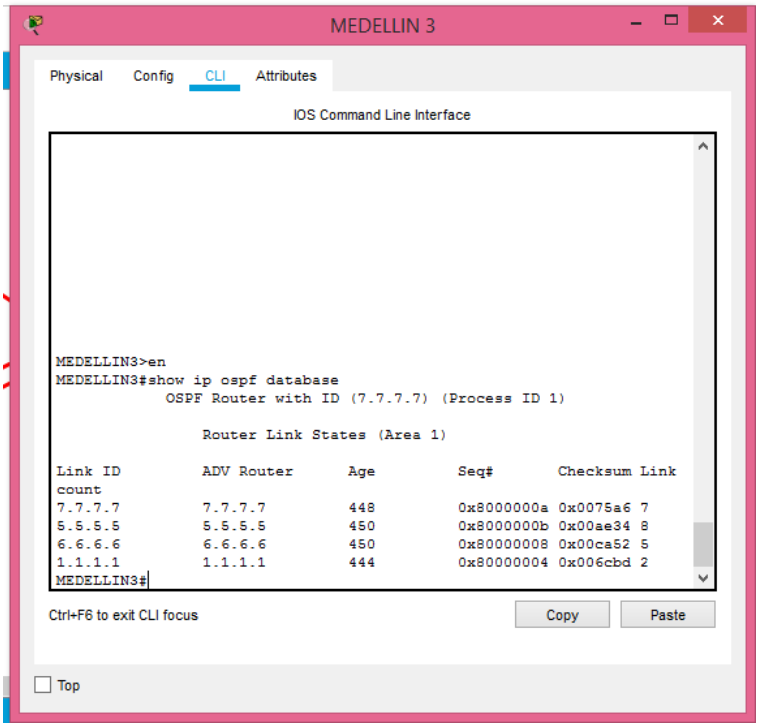


Figure 47 Base de datos OSPF MEDELLIN 3

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

✓**ISP:**

```
ISP>enable
ISP#configure terminal
ISP(config)#username ISP password ISP
ISP(config)#interface serial 0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username MEDELLIN1 password MEDELLIN1
ISP(config-if)#exit
```

✓**MEDELLIN1:**

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#username MEDELLIN1 password MEDELLIN1
MEDELLIN1(config)#interface serial 0/1/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username ISP password ISP
MEDELLIN1(config-if)#exit
```

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

✓ **ISP:**

```
ISP>enable
ISP#configure terminal
ISP(config)#username BOGOTA1 password 0828
ISP(config)#interface serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
```

✓ **BOGOTA1:**

```
BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#username ISP password 0828
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
```

Parte 6: Configuración de PAT.

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

✓**MEDELLIN1:**

```
MEDELLIN1>enable
MEDELLIN1#configure terminal
MEDELLIN1(config)#ip nat pool MED 209.17.220.1 209.17.220.2 netmask 255.255.255.252
MEDELLIN1(config)#access-list 1 permit 172.29.6.0 0.0.0.3
MEDELLIN1(config)#access-list 2 permit 172.29.6.8 0.0.0.3
MEDELLIN1(config)#access-list 3 permit 172.29.6.12 0.0.0.3
MEDELLIN1(config)#ip nat inside source list 1 pool MED
MEDELLIN1(config)#ip nat inside source list 2 pool MED
```

```
MEDELLIN1(config)#ip nat inside source list 3 pool MED
MEDELLIN1(config)#interface serial 0/1/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#interface serial 0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface serial 0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface serial 0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
```

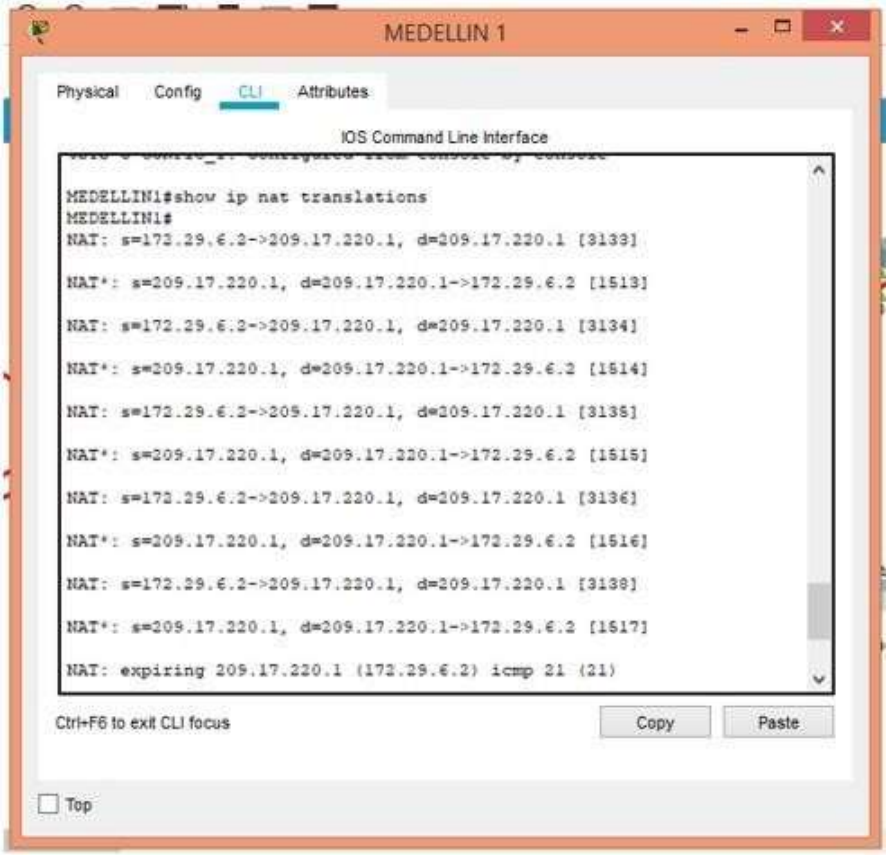


Figure 48 Traduccion MEDELLIN 1

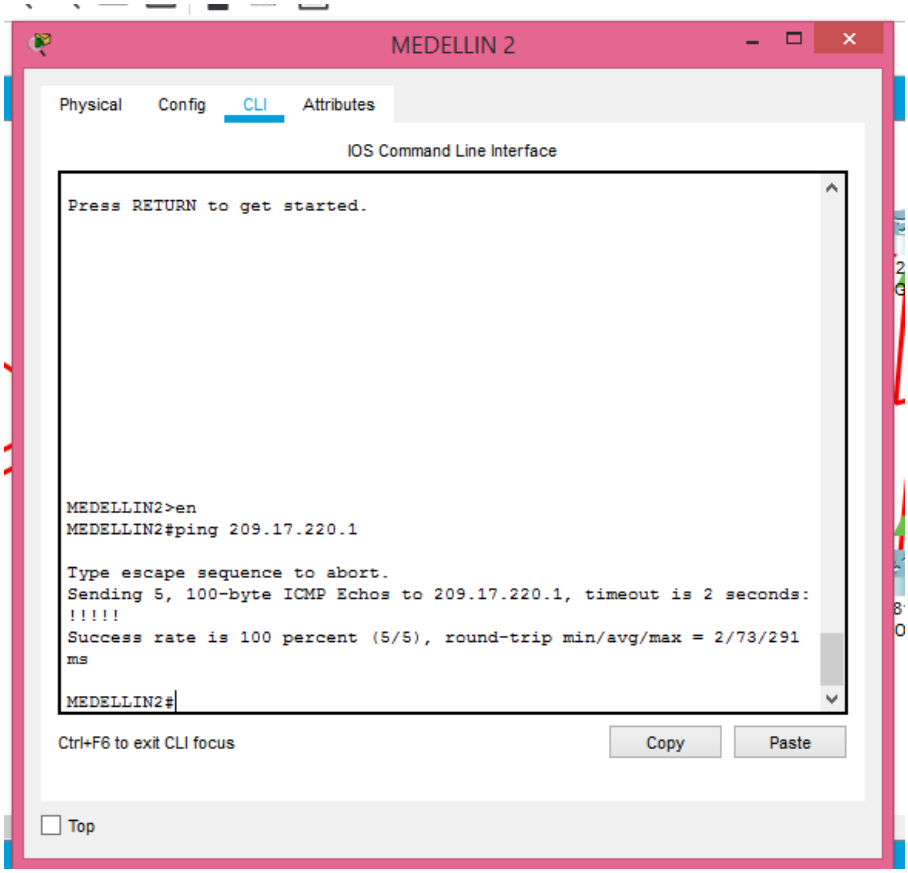


Figure 49 Ping interfaz serial 0/1/0

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

✓ **BOGOTA1:**

BOGOTA1>enable
BOGOTA1#configure terminal
BOGOTA1(config)#ip nat pool BOG 209.17.220.5 209.17.220.6 netmask 255.255.255.252
BOGOTA1(config)#access-list 4 permit 172.29.3.0 0.0.0.3
BOGOTA1(config)#access-list 5 permit 172.29.3.4 0.0.0.3
BOGOTA1(config)#access-list 6 permit 172.29.3.8 0.0.0.3
BOGOTA1(config)#ip nat inside source list 4 pool BOG

```
BOGOTA1(config)#ip nat inside source list 5 pool BOG
BOGOTA1(config)#ip nat inside source list 6 pool BOG
BOGOTA1(config)#interface serial 0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface serial 0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface serial 0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#interface serial 0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
```

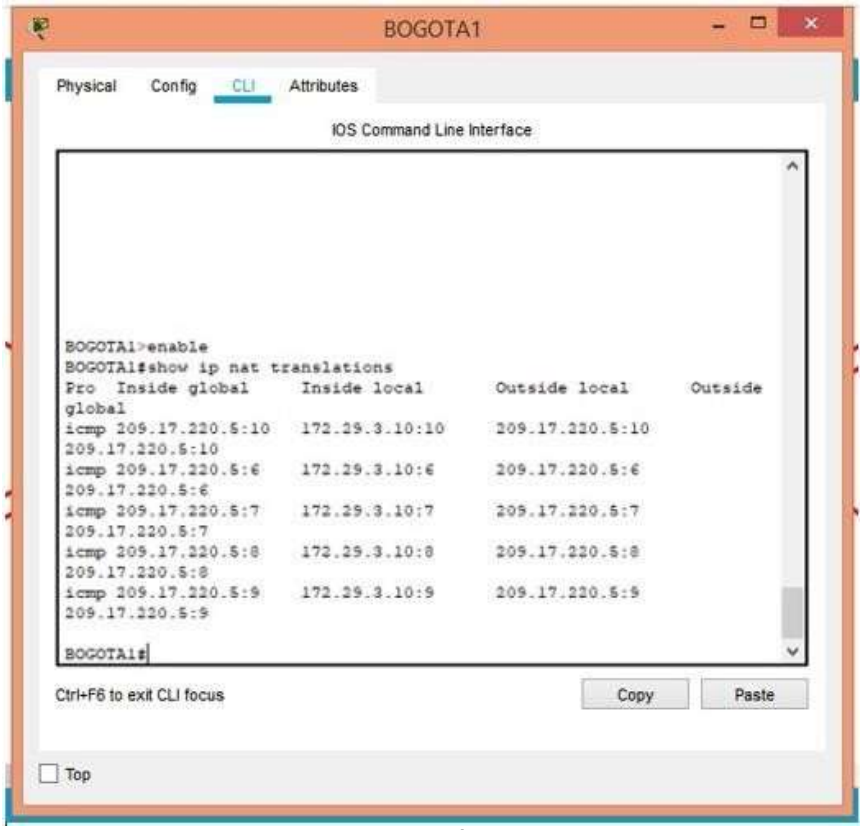


Figure 50 Traducción BOGOTA 1

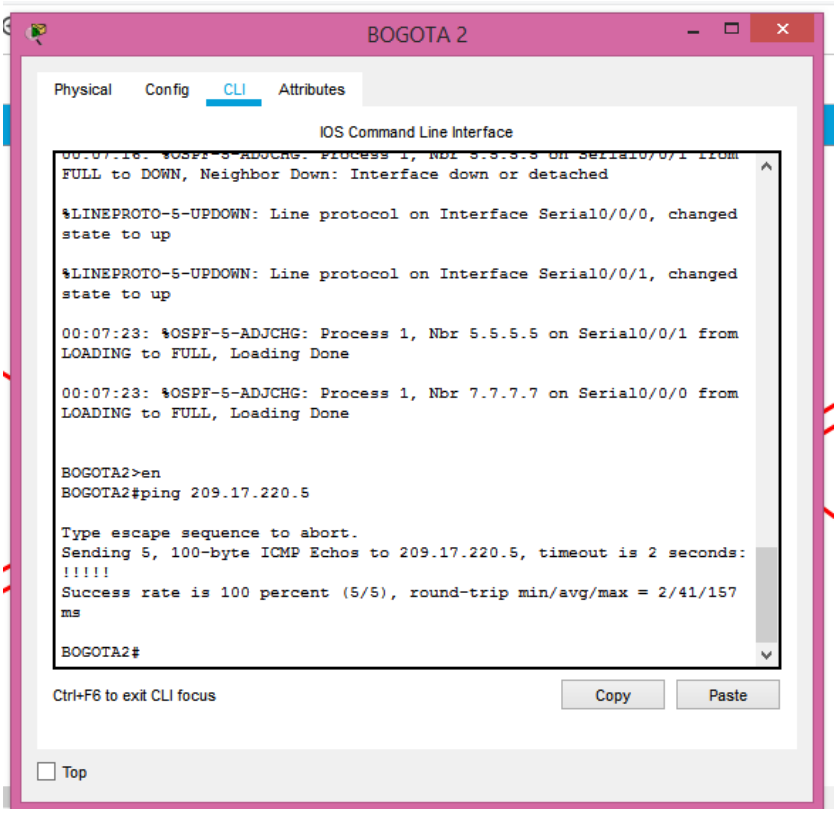


Figure 51 Ping interfaz serial 0/1/0

Parte 7: Configuración del servicio DHCP.

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

```
MEDELLIN2>enable
MEDELLIN2#configure terminal
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)#exit
MEDELLIN2(config)#ip dhcp pool MED3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#exit
```

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

```
MEDELLIN3>enable
MEDELLIN3#configure terminal
MEDELLIN3(config)#interface fastethernet 0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
```

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

```
MEDELLIN2>enable
MEDELLIN2#configure terminal
MEDELLIN2(config)#ip dhcp pool BOG2
MEDELLIN2(dhcp-config)#network 172.29.1.0 255.255.255.0
MEDELLIN2(dhcp-config)#default-router 172.29.1.1
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool BOG3
MEDELLIN2(dhcp-config)#network 172.29.0.0 255.255.255.0
MEDELLIN2(dhcp-config)#default-router 172.29.0.1
MEDELLIN2(dhcp-config)#exit
```

d. Configurar el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Lo realizamos en los router BOGOTA2 y BOGOTA3, para que los PC puedan tener la dirección IP

```
BOGOTA2>enable
BOGOTA2#configure terminal
BOGOTA2(config)#interface fastethernet 0/0
BOGOTA2(config-if)#ip helper-address 172.29.6.2
BOGOTA2(config-if)#exit
BOGOTA3>enable
BOGOTA3#configure terminal
BOGOTA3(config)#interface fastethernet 0/0
BOGOTA3(config-if)#ip helper-address 172.29.6.2
BOGOTA3(config-if)#exit
```

CONCLUSIONES

A partir de la creación de una red de área local virtual (VLAN), es posible reducir el dominio de difusión de una red y hacer su administración más sencilla; por esta razón, en el primer escenario se implementó el routing entre VLAN, ya que, por medio de este es posible crear redes lógicas independientes dentro de una misma red, lo cual contribuye a la creación de características independientes a cada red VLAN de acuerdo con las necesidades de cada uno de los sectores en los cuales se divide una empresa, con el fin de mantener la privacidad y orden en los datos que se manejan en cada sector o departamento de la empresa.

En la implementación del escenario uno, se empleó el protocolo de enrutamiento interior RIPv2, debido a que es uno de los más sencillos y, por lo tanto, es uno de los más utilizados actualmente; ya que, no hace uso de sistemas autónomos ni números de área que puedan identificar una unidad administrativa, lo que permite la reducción del uso de comandos complejos a la hora de realizar la configuración de los dispositivos presentes en la topología de la red.

En la red del escenario dos, fue necesario usar el protocolo de enrutamiento OSPF debido a que en comparación con el protocolo RIP, el protocolo OSPF no tiene límites para el conteo de saltos, presenta mejor convergencia, mejor balanceo de carga y, además, permite una definición lógica de redes en la que los routers se pueden dividir en áreas, lo que ayuda a reducir la propagación innecesaria de información de subred. No obstante, el uso del protocolo OSPF también fue importante en la configuración de la red dos debido a que permite la autenticación de ruteo a través de distintos métodos de autenticación de contraseñas, algo que en este caso es de vital importancia para proteger la integridad, privacidad y seguridad de la información de la empresa.

BIBLIOGRAFÍA

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 7: Direccionamiento IP. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159037

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 8: División de redes IP en subredes .Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159041

CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Capítulo 9: Capa de transporte. Recuperado de https://1314297.netacad.com/courses/973101/modules/items/65159046

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live