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

PRESENTADO POR:

ANDRES FELIPE RAMIREZ MARULANDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERÍA DE SISTEMAS
CHINCHINA, CALDAS
2020

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

ANDRES FELIPE RAMIREZ MARULANDA

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

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES
Docente Ocasional

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERÍA DE SISTEMAS
CHINCHINÁ, CALDAS
2020

INDICE

INDICE DE IMAGENES

INDICE DE TABLAS

RESUMEN

Implementando los conocimiento a adquiridos en el diplomado de Cisco específicamente en los entornos de conocimientos CCNA1 y CCNA 2, se pudo comprender que hay diferentes plataformas y software que son necesarios para diseñar, configurar, y administrar redes. Esto será aplicado en este documento denominado “Solución de dos estudios de caso bajo el uso de tecnología Cisco” donde ejecutaremos lo aprendido a lo largo del diplomado y así se pondrá a prueba los niveles de comprensión y solución con la configuración de dos escenarios con diferentes aspectos de configuraciones relacionado con el Networking.

ABSTRACT

Implementing the knowledge acquired in the Cisco Diplomat specifically in the CCNA1 and CCNA 2 knowledge environments, it was understood that there are different platforms and software that are necessary to design, configure, and manage networks. This will be applied in this document called "Solution of two case studies under the use of Cisco technology" where we will execute what we have learned throughout the course and thus the levels of understanding and solution will be tested with the configuration of two scenarios with different aspects related to Networking.

INTRODUCCION

Las pruebas de habilidades identifican las competencias obtenidas por el estudiante realizando lo aprendido en el diplomado de profundización CNNA. En el presente documento se imprentan varios elementos fundamentales en la conformación, administración y ejecución de redes de telecomunicaciones, como el enrutamiento y direccionamiento de redes, parámetros de seguridad, configuración de protocolos OSPF, RIP, implementación de DHCP entre otros. Como futuro profesional son conocimientos fundamentales que conforman el perfil de ingeniero de sistemas donde se podrá brindar soluciones a problemas que se presenten en un futuro en el campo de la informática.

OBJETIVOS

- Implementar los conocimientos adquiridos en el diplomado Cisco para realizar los ejercicios propuestos.

- Investigar acerca de protocolos que se implementaran en los dos escenarios propuestos del taller.

- Conectar dispositivos y desarrollar esquemas de direccionamiento, configuración de DHCP, enrutamiento entre otros.

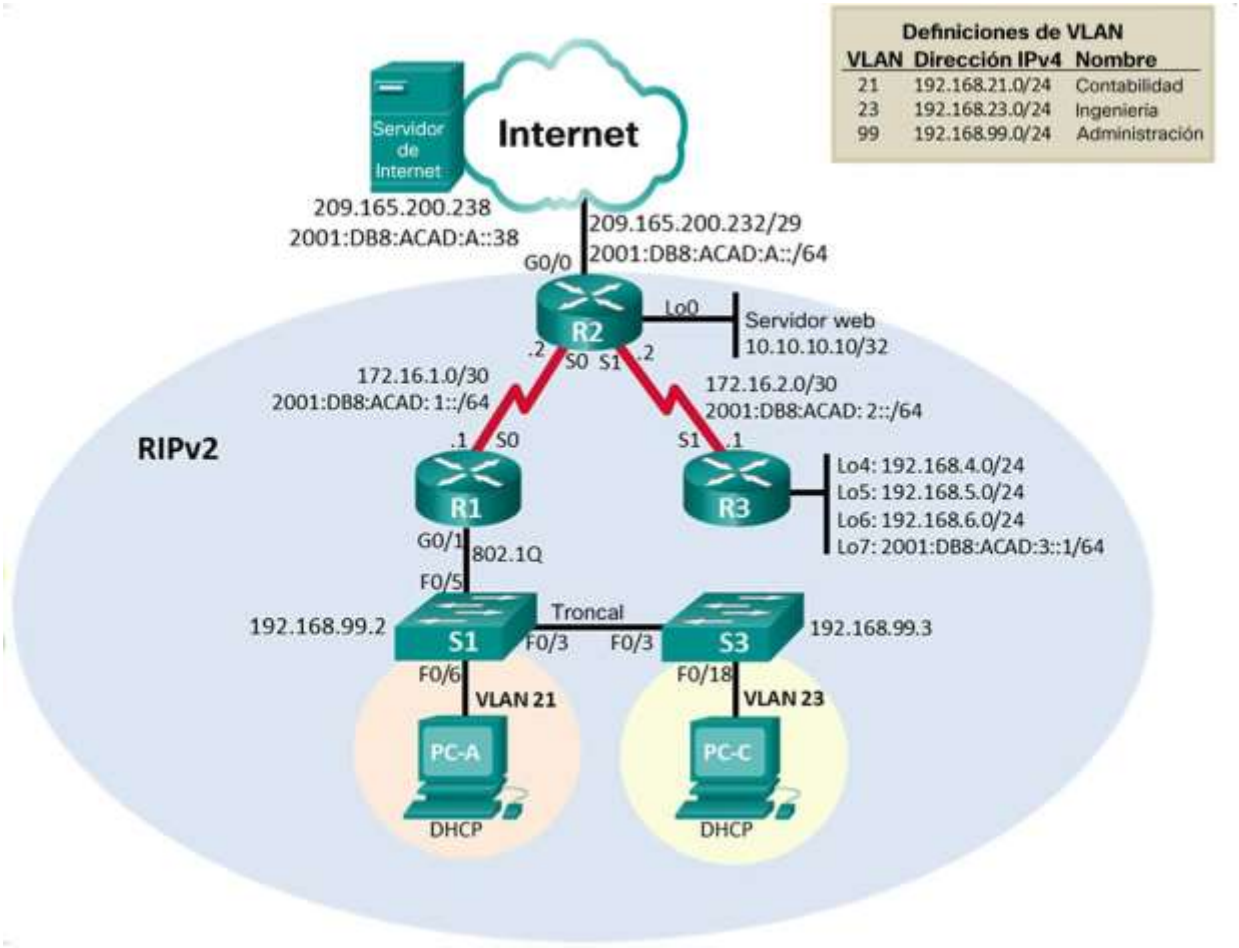
- Diferencias los protocolos RIPv2 y OSPF 1 que serán implementados en los dos escenarios

- Ejecutar los pasos que se encuentran en los dos escenarios propuestos en el taller final.

PRIMER ESCENARIO

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

Topología



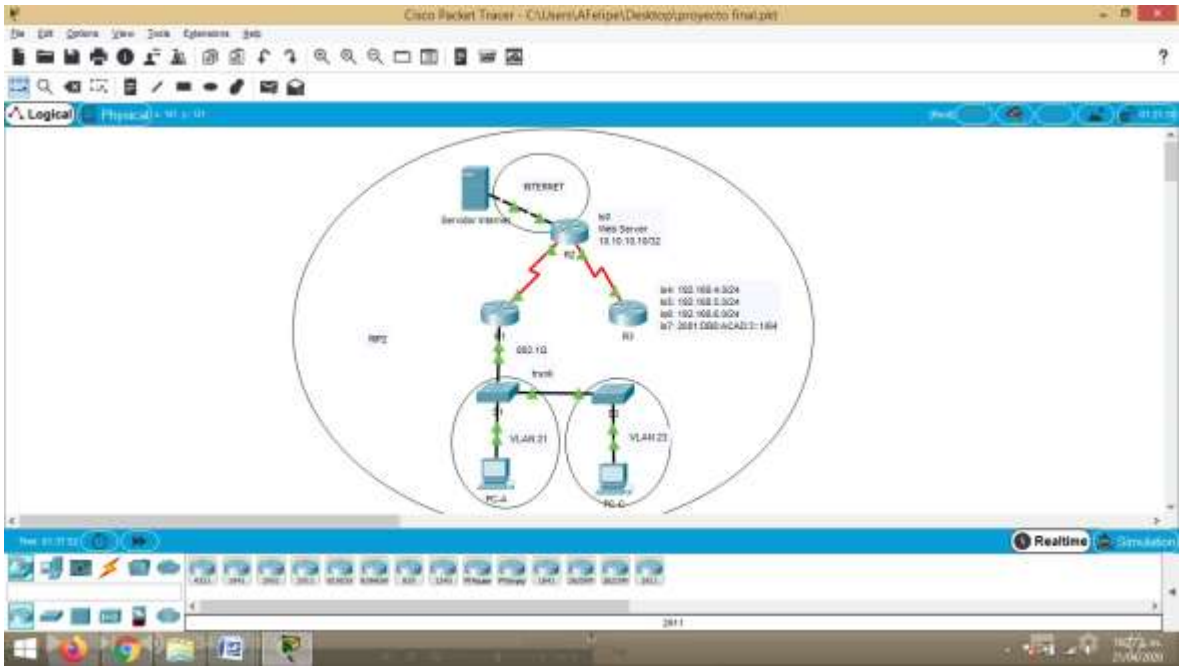


Imagen 1. estructura red escenario 1 en packet tracer

PARTE 1: INICIALIZAR DISPOSITIVOS

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

- Para cada router y switch se debe ingresar a la opción CLI para digitar los comandos que se encuentran en la siguiente tabla y ejecutar los requerimientos de la columna tarea.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Router#
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Switch#delete vlan.dat

Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#dir flash

Tabla 1. Comando IOS

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

Se configura la IP de la computadora de internet con los siguientes datos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:2::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2. Configuración computadora de internet.

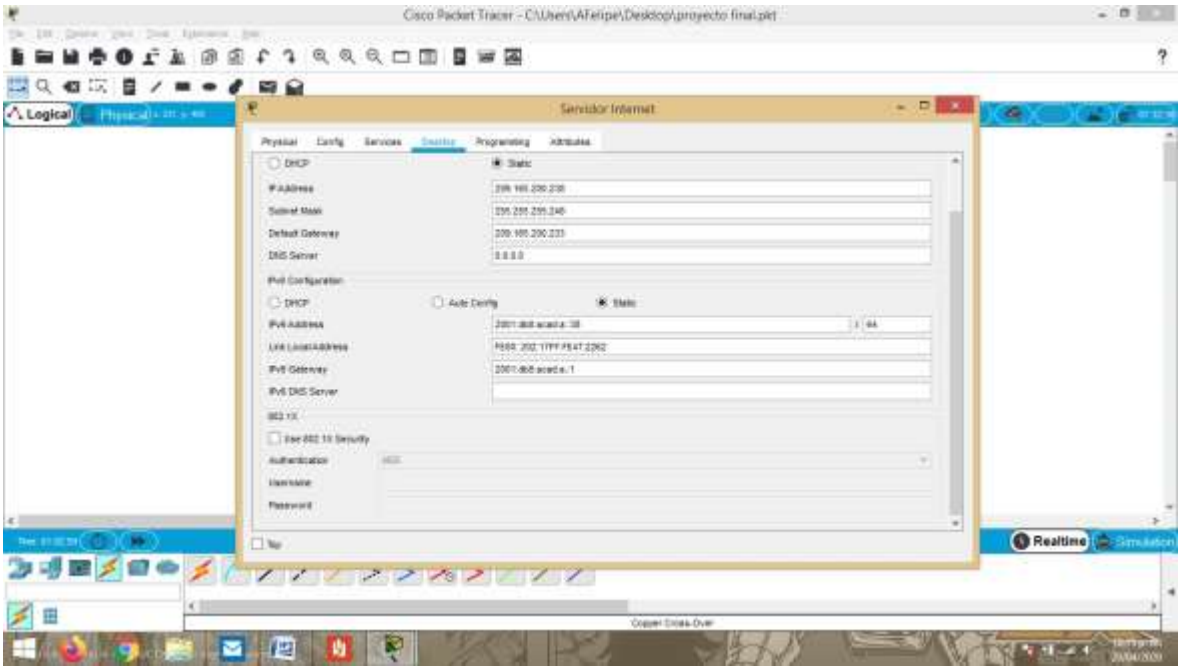


Imagen 2. evidencia de asignación de dirección IP en Internet PC

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Tabla 3. Configuración en R1

Comandos En R1

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#host R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd %se prohibe el acceso no autorizado%
```

Interfaz S0/0/0

```
R1(config)#int s0/0/0
R1(config-if)#description connection to R2
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 add 2001:db8:acad::a/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

R1(config-if)#exit

Rutas predeterminadas
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

R1(config)#ipv6 route ::/0 s0/0/0

Paso 1: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Tabla 4. Configuración en R2

Comandos En R2

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#host R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server este comando no es soportado en packet tracer
R2(config)#banner motd %se prohibe el acceso no autorizado%

Interfaz S0/0/0

R2(config)#int s0/0/0
R2(config-if)#description connection to R1
R2(config-if)#ip add 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 add 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

Interfaz S0/0/1

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

Interfaz G0/0

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

Interfaz loopback 0

```
R2(config-if)#int loopback 0
R2(config-if)#
R2(config-if)#ip add 10.10.10.10 255.255.255.255
R2(config-if)#description servidor web simulado
R2(config-if)#exit
```

Ruta predeterminada

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)#ipv6 route ::/0 g0/0
```

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class

Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Tabla 5. Configuración en R3

Comandos En R3

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#host R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#pass cisco
R3(config-line)#login
```

```
R3(config-line)#service password-encryption
R3(config)#banner motd %se prohibe el acceso no autorizado%
```

Interfaz S0/0/1

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

Interfaz loopback 4

```
R3(config-if)#int loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
```

Interfaz loopback 5

```
R3(config-if)#int loopback 5
R3(config-if)#ip add 192.168.5.1 255.255.255.0
```

Interfaz loopback 6

```
R3(config-if)#int loopback 6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
```

Interfaz loopback 7

```
R3(config-if)#int loopback 7
R3(config-if)#ipv6 add 2001:db8:acad:3::1/64
R3(config-if)#exit
```

Rutas predeterminadas

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

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 6. Configuración en S1

Comandos En S1

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#host S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %se prohibe el acceso no autorizado%
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 7 configuración en S3

Comandos En S3

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#host S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd %se prohibe el ingreso no autorizado%
```

Paso 7: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	exitoso
R2	R3, S0/0/1	172.16.2.1	exitoso
PC de Internet	Gateway predeterminado	200.165.200.233	exitoso

Tabla 8. Conectividad de dispositivos.

PASOS PARA REALIZAR PING EN R1, R2 Y PC INTERNET

Comando En R1

R1>enable
Password: cisco
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 = 1/3/5 ms

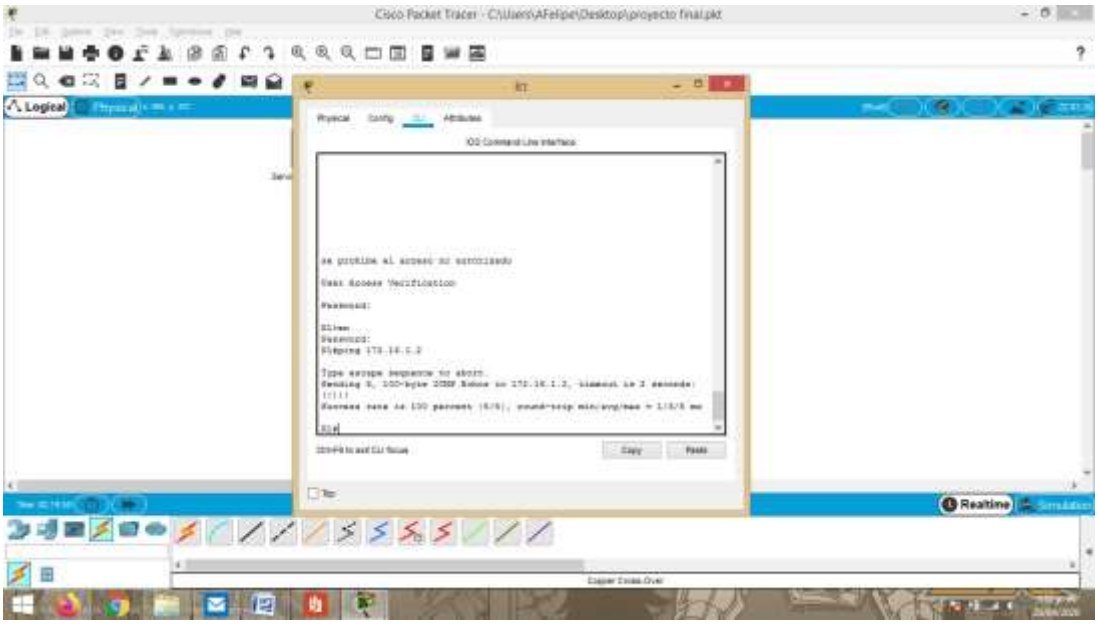


Imagen 3. ping r1a r2, s0/0/0

Comando En R2

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 = 1/2/6 ms

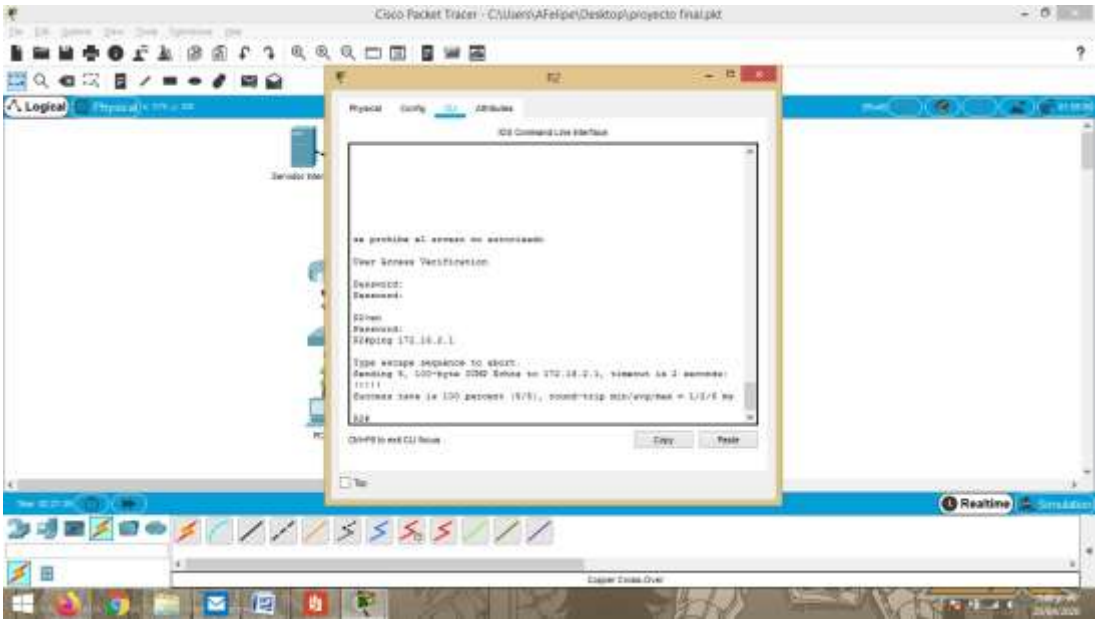


Imagen 4. ping R1a R3, S0/0/1

COMANDO PARA PC INTERNET

Ingresamos la símbolo del sistema e ingresamos el comando ping

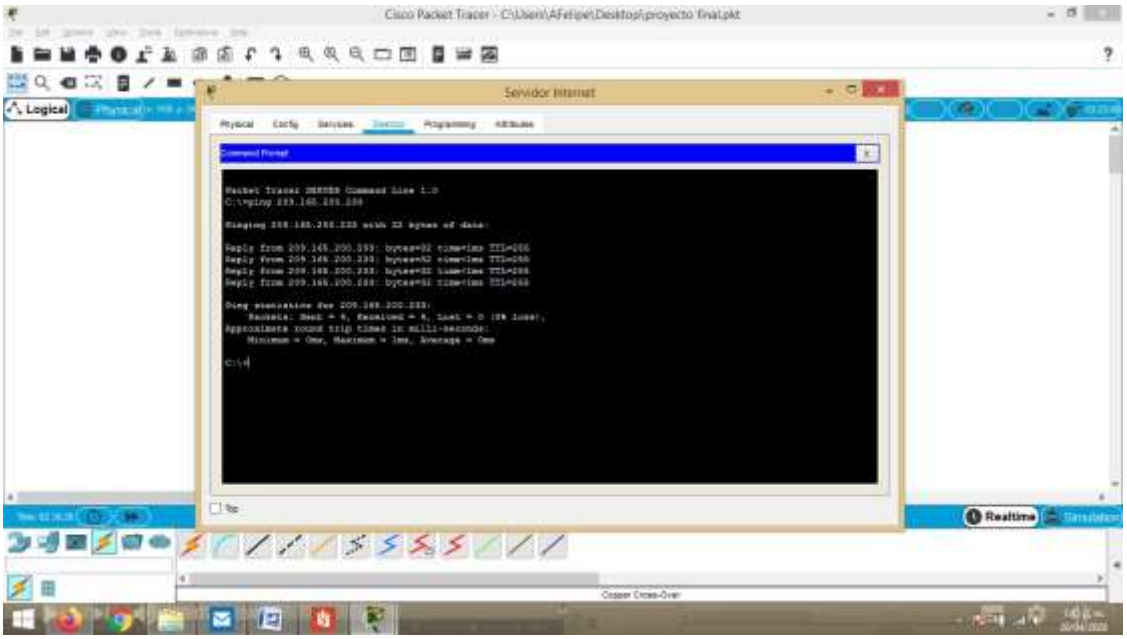


Imagen 5. ping pc internet a Gateway predeterminado

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:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 9. Configuración en S1

Comandos En S1

S1>enable
Password: cisco
S1#configure terminal
S1(config)#vlan 21
S1(config-vlan)#name contaduria
S1(config-vlan)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name administracion

S1(config-vlan)#

Asignar la dirección IP de administración.

S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5
S1(config-if)#int f0/5

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

Configurar el resto de los puertos como puertos de acceso

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

Asignar F0/6 a la VLAN 21
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23

Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 10. Configuración en S3

Comandos En S3

S3>enable
Password: class
S3#configure terminal

Crear la base de datos de VLAN
S3(config)#vlan 21
S3(config-vlan)#name contaduria
S3(config-vlan)#vlan 23
S3(config-vlan)#name ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name administracion
S3(config-vlan)#exit

Asignar la dirección IP de administración

S3(config)#int vlan 99
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3

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

Configurar el resto de los puertos como puertos de acceso

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

Asignar F0/18 a la VLAN 21

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

Apagar todos los puertos sin usar

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

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Tabla 11. Configuración en R1

Comandos En R1

R1>enable
Password: class
R1#configure terminal

Configurar la subinterfaz 802.1Q .21 en G0/1

R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21

R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip add 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1

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

Configurar la subinterfaz 802.1Q .99 en G0/1

R1(config-subif)#int g0/1.99
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0

Activar la interfaz G0/1

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

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:

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

Tabla 12. Resultados Ping

Ping En S1

S1>enable
Password: class
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

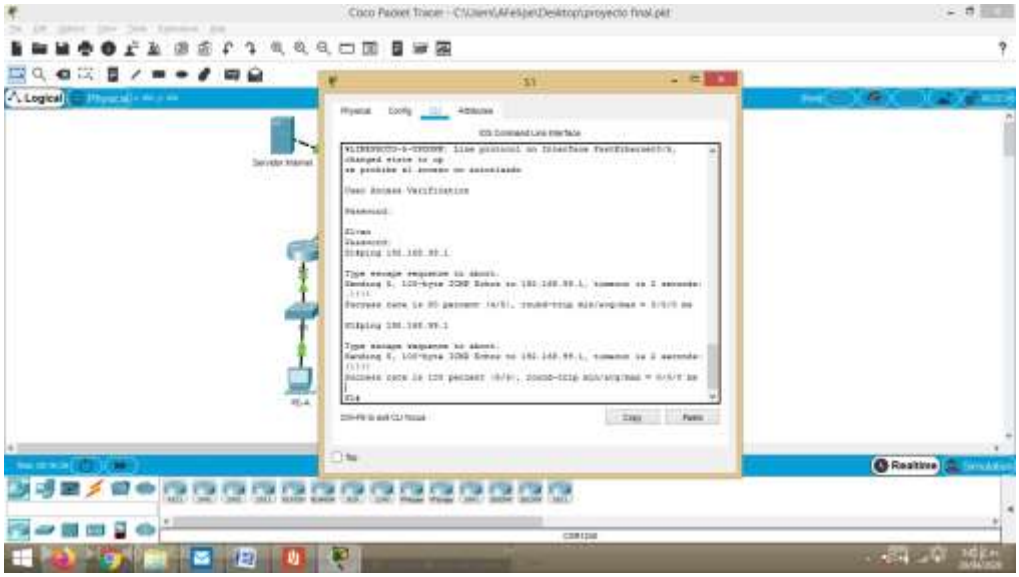


Imagen 6. ping de S3 a R1, dirección VLAN 99

Ping En S3

S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

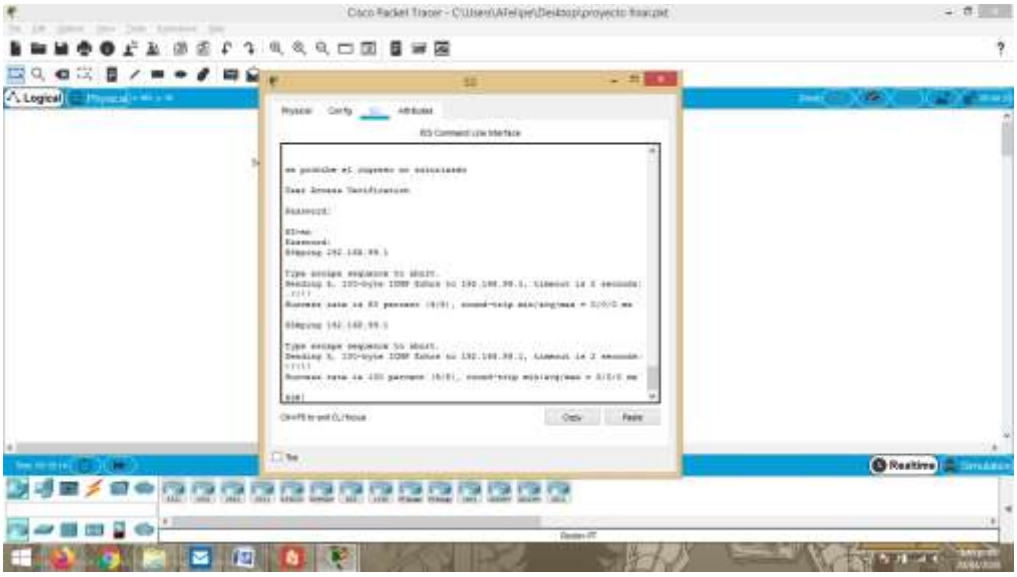


Imagen 7. ping de S1 a R1, dirección VLAN 99

Ping En S1

S1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

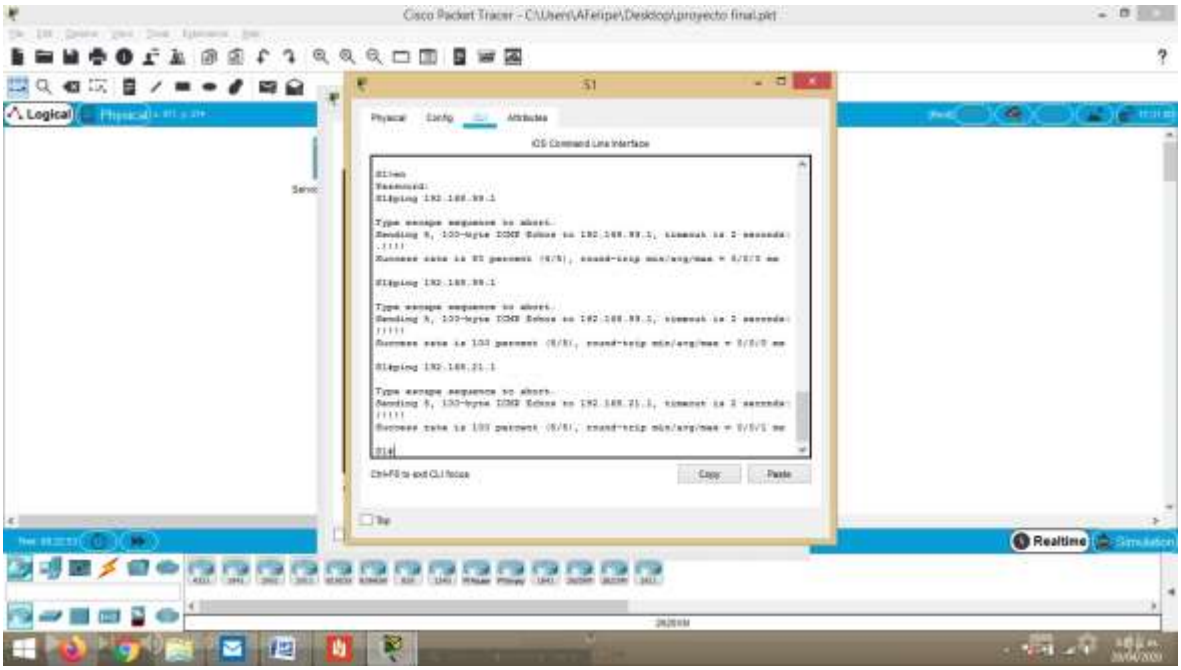


Imagen 8. ping de S1 a R1, dirección VLAN 21

Ping En S3

S3#ping 192.168.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

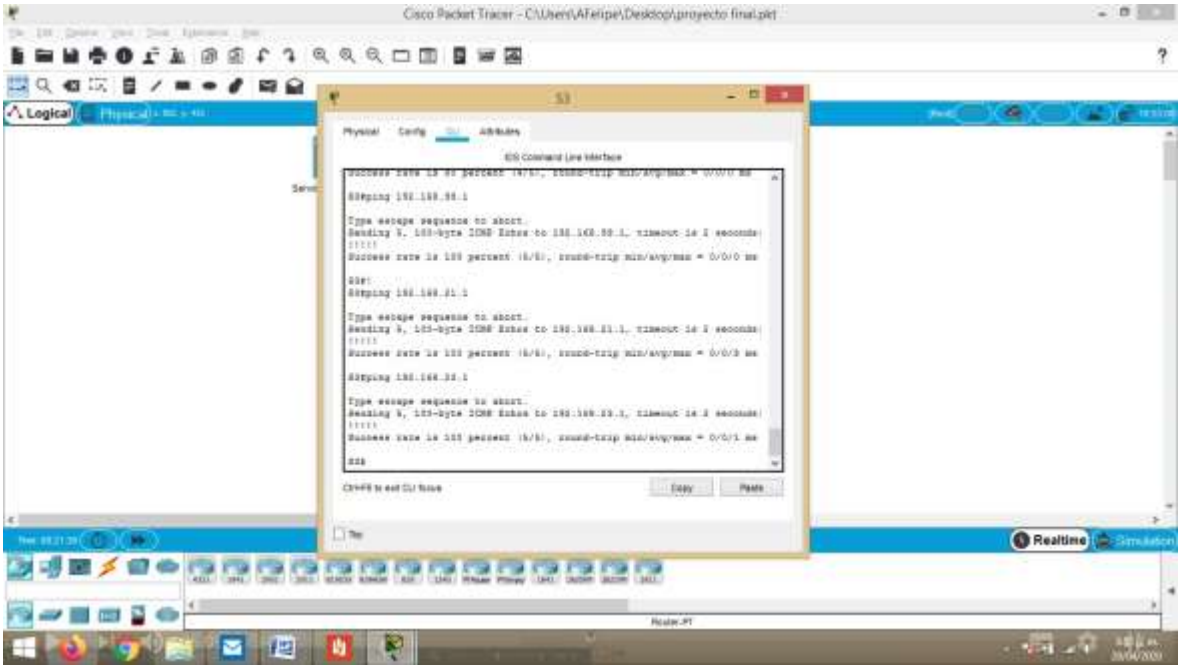


Imagen 9. ping de S3 a R1, dirección VLAN 23

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Tabla 14. Configuración RIPv2 en R1

Comandos En R1

R1#configure terminal

R1(config)#router rip

Configurar RIP versión 2
R1(config-router)#version 2

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

Establecer todas las interfaces LAN como pasivas

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

Desactive la sumarización automática

R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Tabla 15. Configuración en R2

Pasos En R2

R2>enable
Password: class
R2#configure terminal
Configurar RIP versión 2
R2(config)#router rip
R2(config-router)#version 2

Anunciar las redes conectadas directamente

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

Establecer la interfaz LAN (loopback) como pasiva
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0

Desactive la sumarización automática.

R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Tabla 16. Configuración en R3

Comandos En R3
R3>enable

Password: class
R3#configure terminal

Configurar RIP versión 2
R3(config)#router rip
R3(config-router)#version 2

Anunciar redes IPv4 conectadas directamente

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

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

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

Desactive la sumarización automática.

R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

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

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Se utiliza el comando show ip protocols para verificar la información.
¿Qué comando muestra solo las rutas RIP?	Se utiliza el comando show ip route rip para mostrar las rutas RIP
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	En packet tracer se utiliza el comando show run e ir a la sección de router RIP

Tabla 17.verificar información RIP

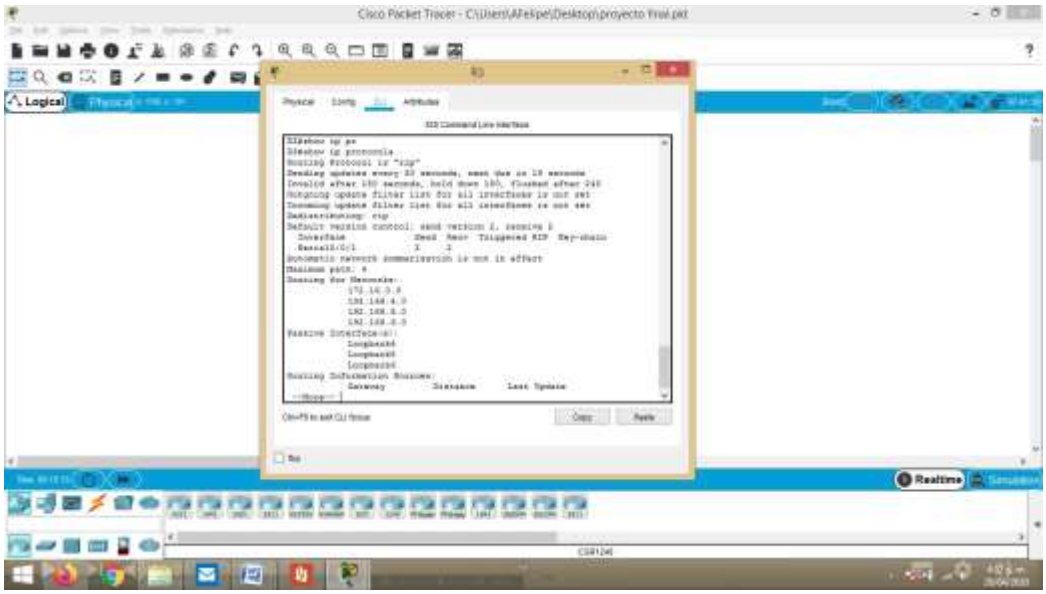


Imagen 10. comando show ip protocols

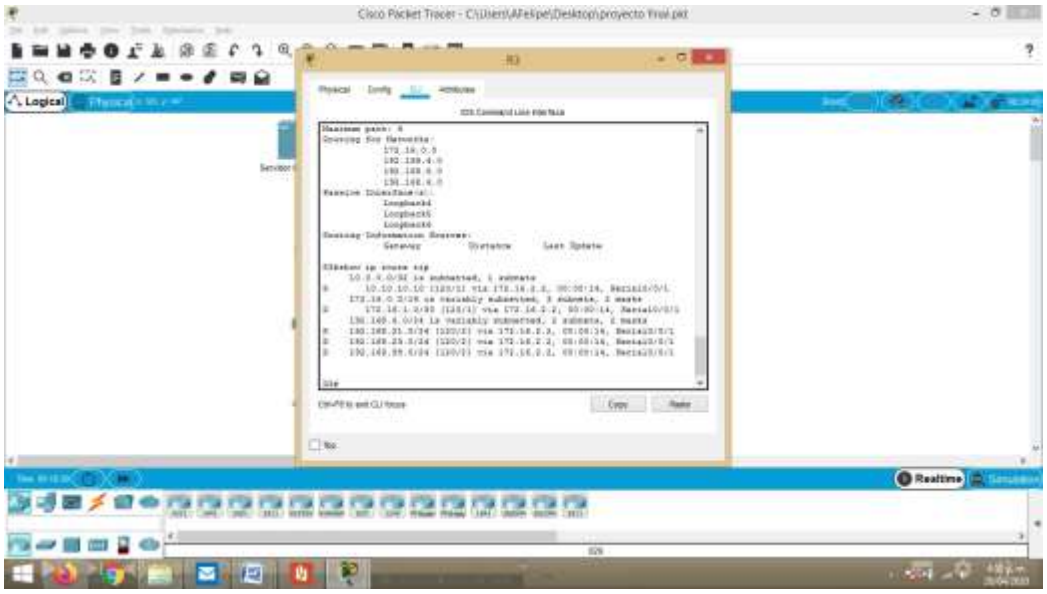


Imagen 11. show ip router rip

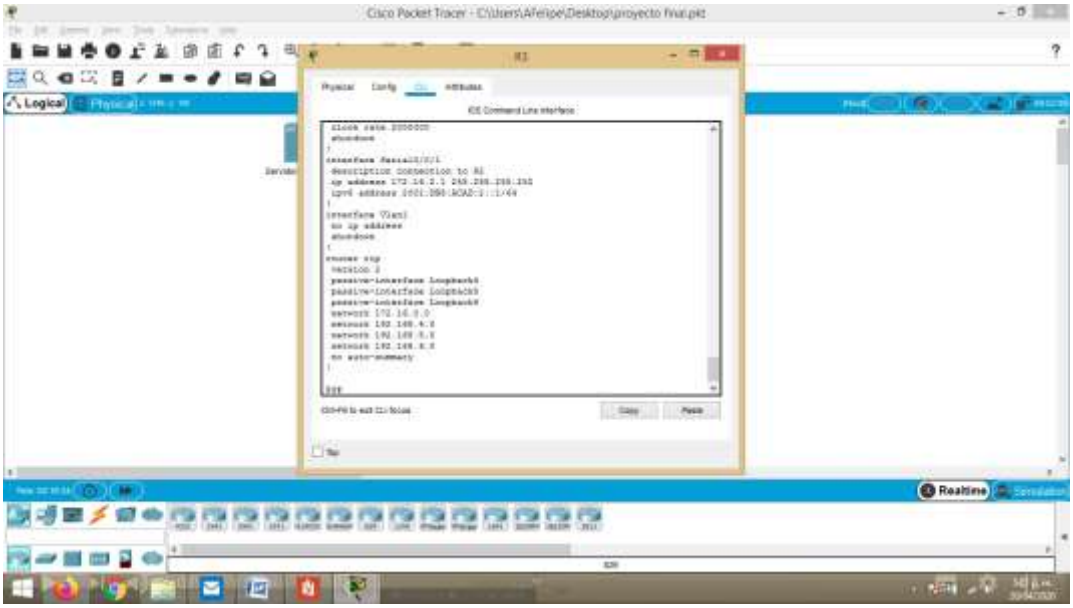


Imagen 12. comando show running

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:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Tabla 18. Configuracion en R1

Comando En R1

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#domain-name ccna-sa.com

Crear un pool de DHCP para la VLAN 23

R1(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

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	

Tabla 19. Configuración en R2

Comandos En R2

R2>enable
Password: class
R2#configure terminal

Crear una base de datos local con una cuenta de usuario

R2(config)#username webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP

R2(config)#ip http server

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

R2(config)#ip http authentication local
Estos comandos no son soportados en packet tracer pero en un servidor real deberían funcionar

Configurar la NAT dinámica dentro de una ACL privada

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

Configurar la NAT dinámica dentro de una ACL privada

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

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

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

Defina el pool de direcciones IP públicas utilizables.

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

Definir la traducción de NAT dinámica

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

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para el PC-A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para el PC-A
Verificar que la PC-A pueda hacer ping a la PC-C Nota:Quizá sea necesario deshabilitar el firewall de la PC.	El resultado es satisfactorio
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión	**Los PC no tienen comunicación a internet utilizando el comando http server porque en Packet tracer es soportadoa para activar el servidor web en R2. Pero si utilizamos la dirección IP del servidor web en el navegador PC-A y PC-C tenemos acceso a internet**

Tabla 21. Pruebas

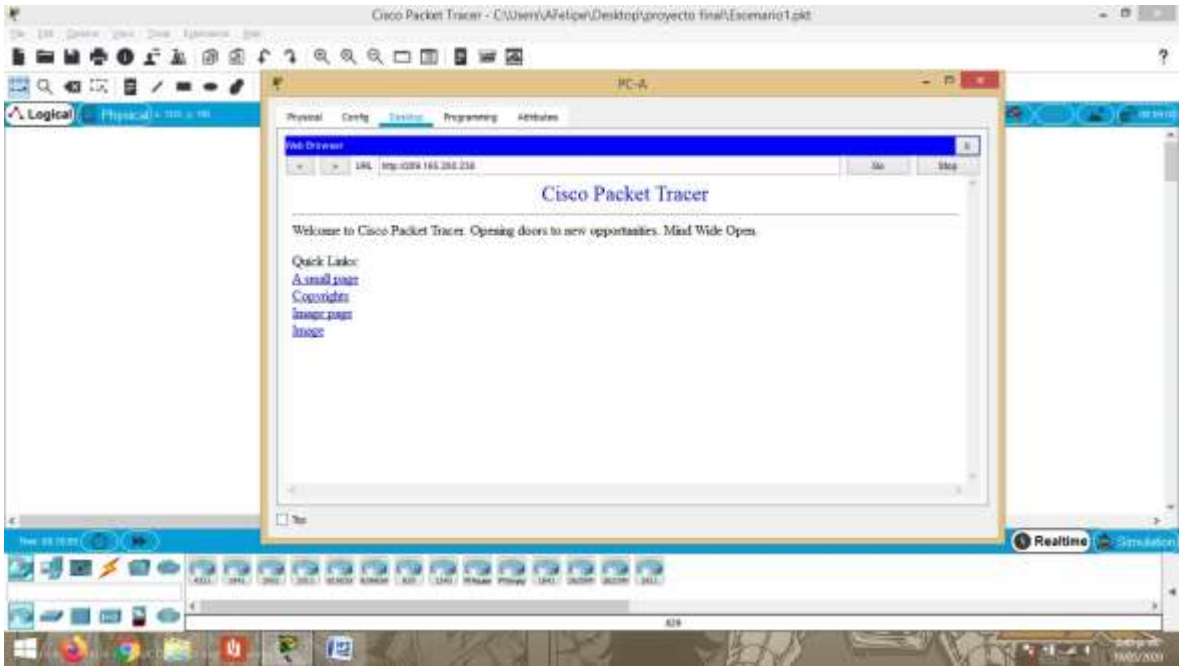


Imagen 13. conexión a internet desde PC-A utilizando la dirección IP del servidor de Internet

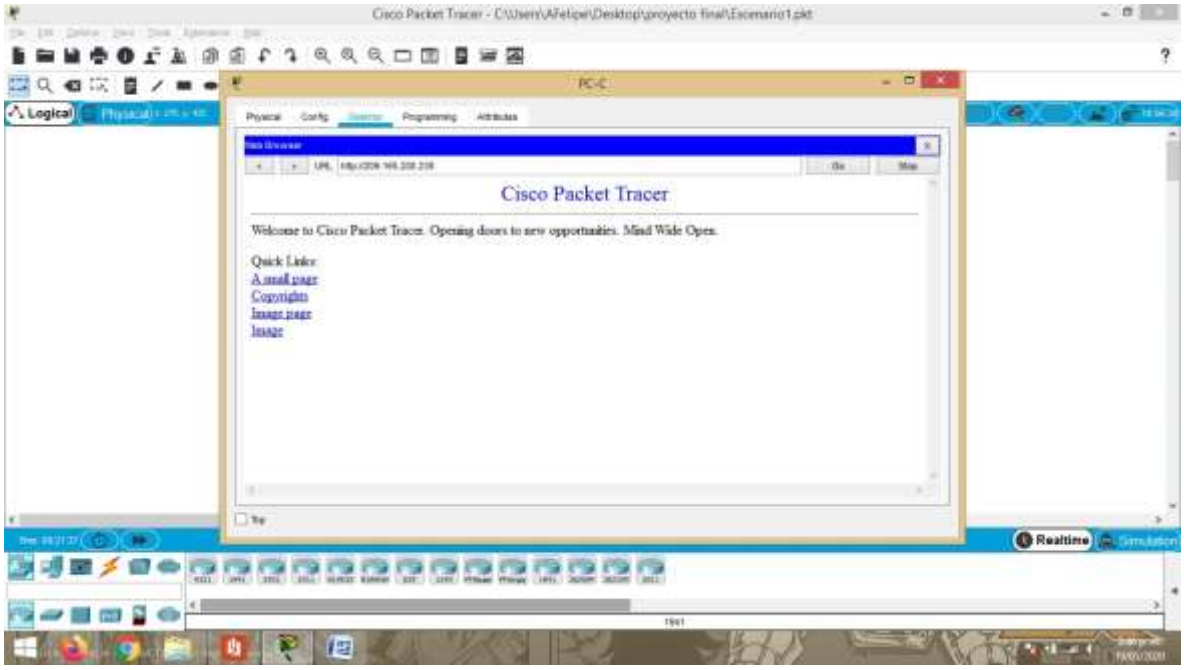


Imagen 14. conexión a internet desde PC-C utilizando la dirección IP del servidor de Internet

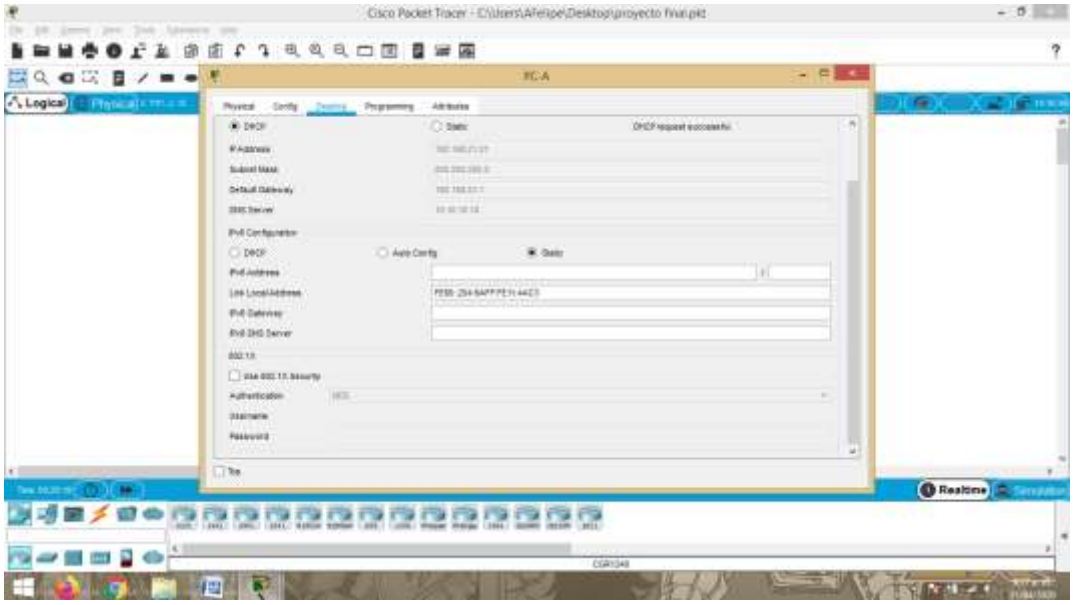


Imagen 15. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

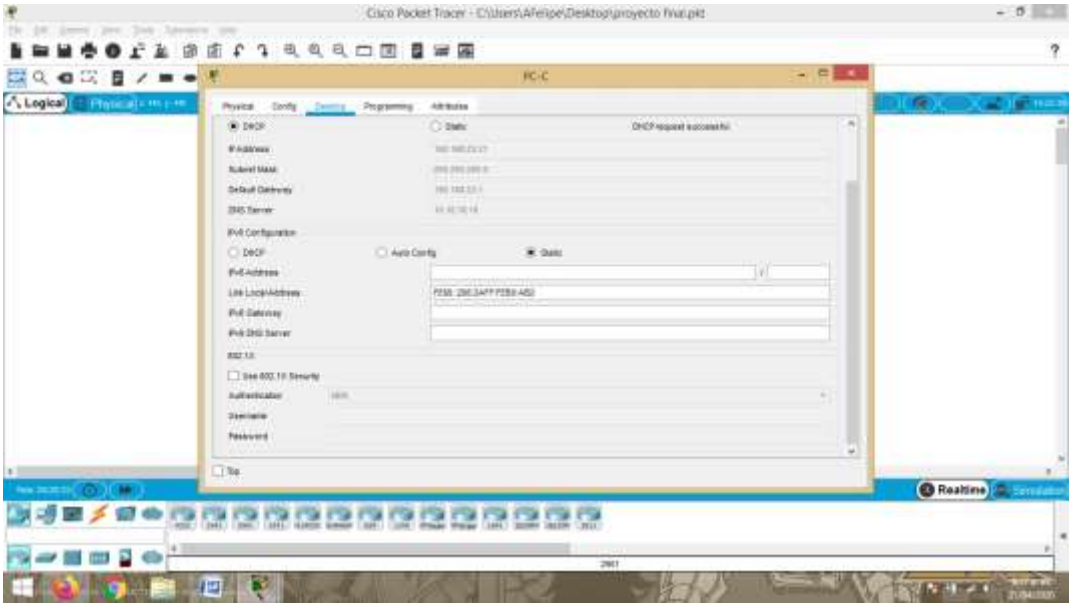


Imagen 16. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

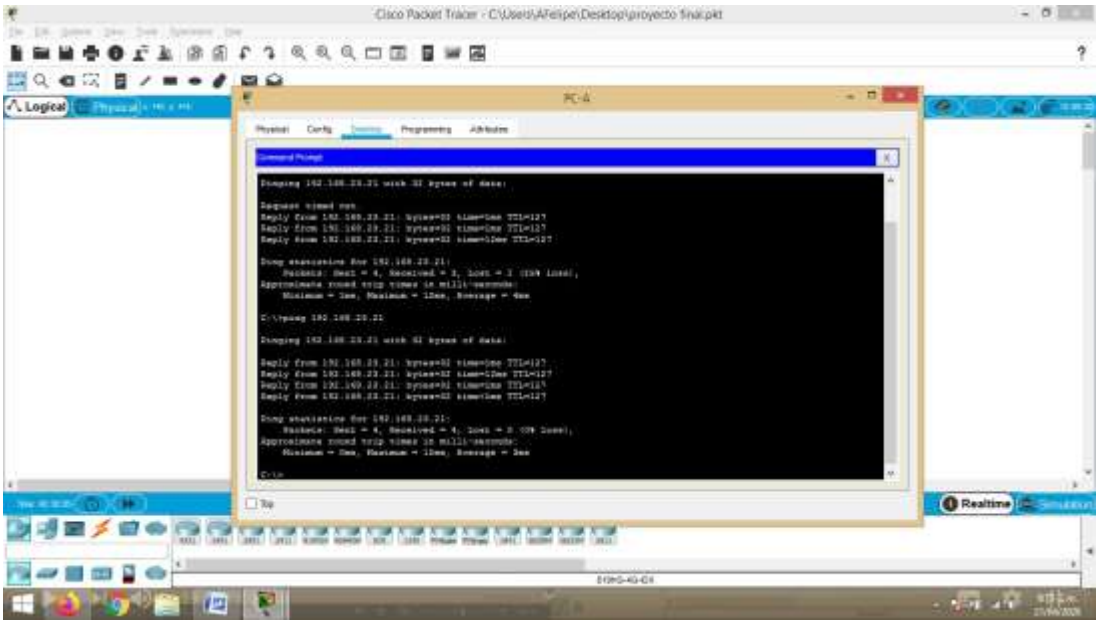


Imagen 17. Verificar que la PC-A pueda hacer ping a la PC-C

PARTE 6: CONFIGURAR NTP

Elemento o tarea deconfiguración	Especificación
Ajuste la fecha y hora en R2.	09:25: 00 21 de abril de 2020
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Tabla 22. Configurar NTP

Pasos Comando R2

R2>enable
Password: class

Ajuste la fecha y hora en R2.
R2#clock set 09:25:00 21 april 2020
R2#configure terminal

Configure R2 como un maestro NTP.

R2(config)#ntp master 5

Comando En R1

R1#configure terminal

Configurar R1 como un cliente NTP.
R1(config)#ntp server 172.16.1.2

Configure R1 para actualizaciones de calendario periódicas con hora NTP.
R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.
R1#show ntp associations
address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 5 16 7 3.00 856514837101.00 0.12

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Tabla 23. Configuracion VTY R2

Comandos En R2

R2#configure terminal

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

R2(config)#ntp master 5
R2(config)#
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet

Permitir acceso por Telnet a las líneas de VTY
R1#telnet 172.16.1.2
R2>

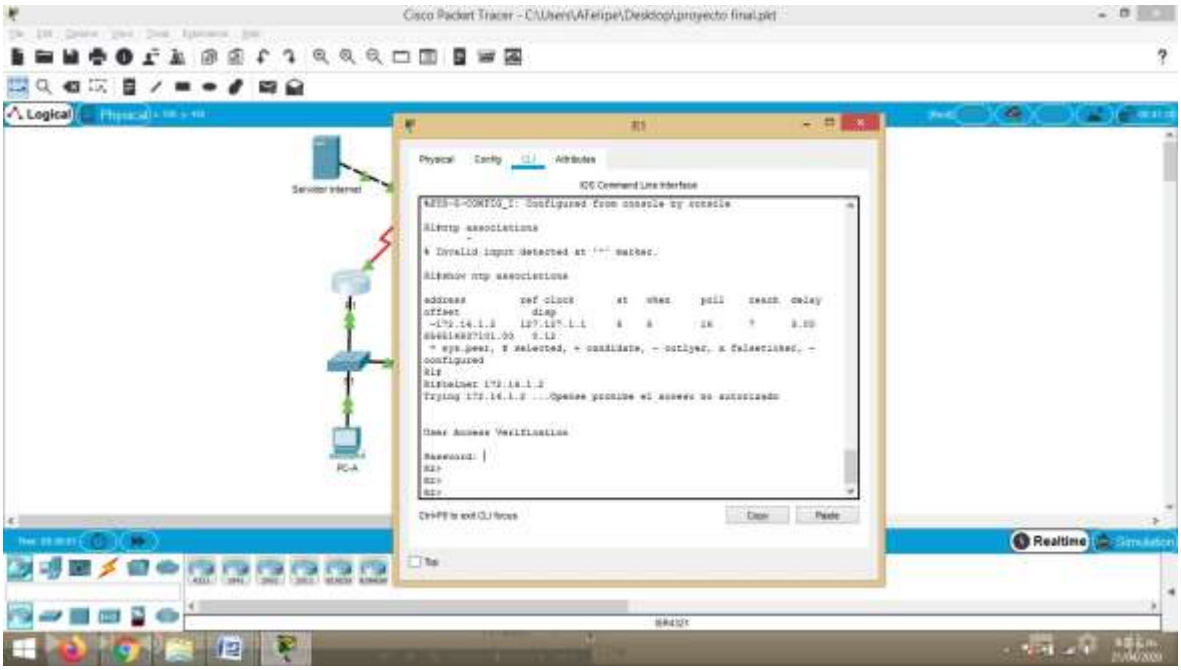


Imagen 18. Verificar que la ACL funcione como se espera

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

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

Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters ^ % Invalid input detected at '^' marker. R2#clear ip ? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries R2#clear ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show ip interface muestra la interfaz y las direccion
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.165.200.234:5 192.168.23.21:5 209.165.200.238:5 209.165.200.238:5 icmp 209.165.200.234:6 192.168.23.21:6 209.165.200.238:6 209.165.200.238:6 icmp 209.165.200.234:7 192.168.23.21:7 209.165.200.238:7 209.165.200.238:7 icmp 209.165.200.234:8 192.168.23.21:8 209.165.200.238:8 209.165.200.238:8 icmp 209.165.200.235:13192.168.21.21:13 209.165.200.238:13 209.165.200.238:13 icmp 209.165.200.235:14192.168.21.21:14 209.165.200.238:14 209.165.200.238:14 icmp 209.165.200.235:15192.168.21.21:15 209.165.200.238:15 209.165.200.238:15 icmp 209.165.200.235:16192.168.21.21:16 209.165.200.238:16 209.165.200.238:16 --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.234:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80 tcp 209.165.200.235:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80 tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025209.165.200.238:1025

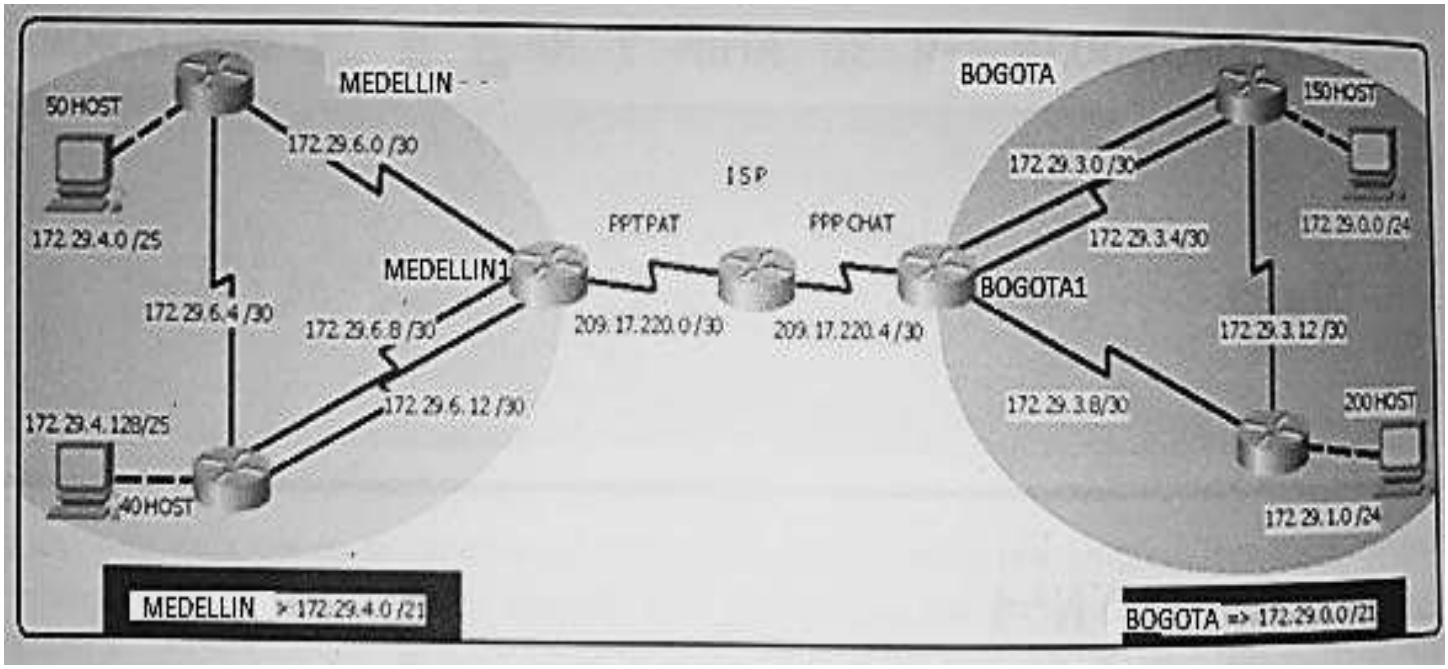
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Tabla 24. Comando CLI

SEGUNDO 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



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.

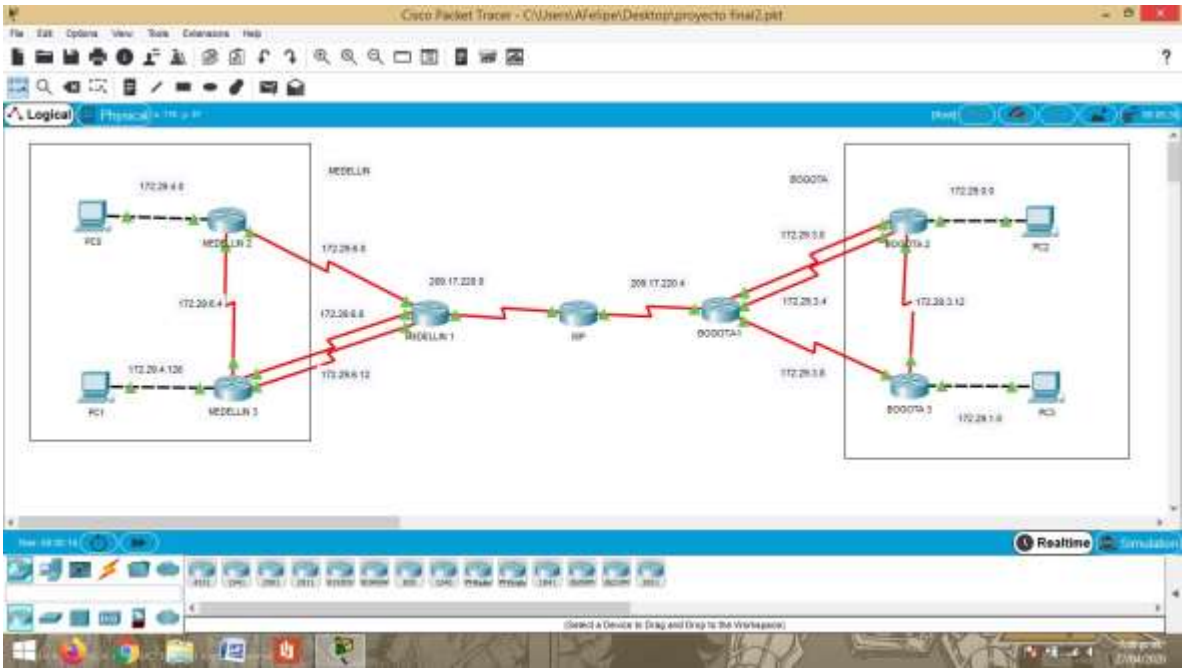


Imagen 19. estructura red escenario 2en packet tracer

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

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

Router#conf t

Router(config)#host ISP

Configuración En Router Ips

Interfaz S0/0/0

ISP(config)#int s0/0/0
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#descr
ISP(config-if)#description IPS-MEDELLIN1
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut

Interfaz S0/0/1
ISP(config)#int s0/0/1
ISP(config-if)#des
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut

Configuración Ospf 1

ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 255.255.255.252 area 0
ISP(config-router)#network 209.17.220.4 255.255.255.252 area 0

Configuración Router Medellín 1

Router>enable
Router#configure terminal
Router(config)#host MEDELLIN1

Interfaz S0/0/0

MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip add 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#description MEDELLIN1-ISP
MEDELLIN1(config-if)#no shut

Interfaz S0/0/1

```
MEDELLIN1#conf t
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip add 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shut
```

Interfaz S0/1/0

```
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#description MEDELLIN1-MEDELLIN3
MEDELLIN1(config-if)#ip add 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shut
```

Interfaz S0/1/1

```
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#description MEDELLIN3-MEDELLIN1
MEDELLIN1(config-if)#ip add 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shut
```

Configuracion OSPF 1

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 209.17.220.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.6.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.8.0 255.255.255.252 area 0
MEDELLIN1(config-router)#network 172.29.12.0 255.255.255.252 area 0
MEDELLIN1(config-router)#exit
```

Configuración Router Medellín 2

Interfaz S0/0/1

```
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#description MEDELLIN3-MEDELLIN1
MEDELLIN1(config-if)#ip add 172.29.6.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shut
```

Interfaz S0/0/0

```
MEDELLIN2#conf t
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#description MEDELLIN1-MEDELLIN2
MEDELLIN2(config-if)#ip add 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shut
```

Interfaz G0/0

```
MEDELLIN2(config-if)#int g0/0
MEDELLIN2(config-if)#description MEDELLIN2-PC0
MEDELLIN2(config-if)#ip add 172.29.4.1 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shut
```

Configuracion OSPF 1

```
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.6.0 255.255.255.252 area 0
MEDELLIN2(config-router)#network 172.29.6.4 255.255.255.252 area 0
```

Configuración Router Medellin3

Interfaz s0/0/0

```
Router#
Router#conf t
Router(config)#int s0/0/0
Router(config-if)#description MEDELLIN3-MEDELLIN2
Router(config-if)#ip address 172.29.6.6 255.255.255.252
Router(config-if)#no shut
```

Interfaz S0/1/0

```
Router(config-if)#int s0/1/0
Router(config-if)#description MEDELLIN3-MEDELLIN2
Router(config-if)#ip add 172.29.6.10 255.255.255.252
Router(config-if)#no shut
```

Interfaz S0/1/1

```
Router(config-if)#int s0/1/1
Router(config-if)#description MEDELLIN1-MEDELLIN3
Router(config-if)#ip add 172.29.6.14 255.255.255.252
Router(config-if)#no shut
```

Interfaz G0/0

```
Router(config-if)#int g0/0
Router(config-if)#description MDELLIN3-PC1
Router(config-if)#ip add 172.29.4.129 255.255.255.128
Router(config-if)#no shut
```

Configuración OSPF 1

```
Router(config)#router ospf 1
Router(config-router)#network 172.29.6.4 255.255.255.252 area 0
Router(config-router)#network 172.29.6.4 255.255.255.252 area 0
Router(config-router)#network 172.29.6.8 255.255.255.252 area 0
Router(config-router)#network 172.29.6.12 255.255.255.252 area 0
Router(config-router)#exit
```

Configuración Router Bogotá 1

Interfaz S0/1/1

```
Router#configure terminal
Router(config)#int s0/0/1
Router(config-if)#description BOGOTA1-ISP
Router(config-if)#ip add 209.17.220.5 255.255.255.252
Router(config-if)#no shut
```

Interfaz S0/0/0

```
Router#conf t
Router(config)#int s0/0/0
Router(config-if)#description BOGOTA1-BOGOTA3
Router(config-if)#ip add 172.29.3.9 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#no shut
```

Interfaz S0/1/1

```
Router#conf t
Router(config)#int s0/1/1
Router(config-if)#description BOGOTA1-BOGOTA2
Router(config-if)#ip add 172.29.3.1 255.255.255.252
Router(config-if)#no shut
```

Interfaz S0/1/0

```
Router(config-if)#int s0/1/0
Router(config-if)#description BOGOTA2-BOGOTA1
Router(config-if)#ip address 172.29.3.5 255.255.255.252
Router(config-if)#no shut
```

Configuración OSPF 1

```
Router(config)#router ospf 1
Router(config-router)#network 172.29.3.8 255.255.255.252 area 0
Router(config-router)#network 172.29.3.4 255.255.255.252 area 0
Router(config-router)#network 172.29.3.3 255.255.255.252 area 0
Router(config-router)#network 209.17.220.4 255.255.255.252 area 0
```

CONFIGURACION ROUTER BOGOTA 2

Interfaz S0/1/1

```
Router#conf t
Router(config)#int s0/1/1
Router(config-if)#description BOGOTA2-BOGOTA1
Router(config-if)#ip add 172.29.3.2 255.255.255.252
```

Router(config-if)#clock rate 128000
Router(config-if)#no shut

Interfaz S0/1/0

Router(config-if)#int s0/1/0
Router(config-if)#description BOGOTA1-BOGOTA2
Router(config-if)#ip add 172.29.3.6 255.255.255.252
Router(config-if)#no shut

Interfaz S0/0/1

Router(config-if)#int s0/0/1
Router(config-if)#DESCription BOGOTA2-BOGOTA3
Router(config-if)#ip add 172.29.3.13 255.255.255.252
Router(config-if)#no shut

Interfaz g0/0

Router(config-if)#int g0/0
Router(config-if)#description BOGOTA2-PC2
Router(config-if)#ip add 172.29.0.1 255.255.255.0
Router(config-if)#no shut

Configuración OSPF1

Router(config)#router ospf 1
Router(config-router)#network 172.29.3.4 255.255.255.252 area 0
Router(config-router)#network 172.29.3.4 255.255.255.252 area 0
Router(config-router)#network 172.29.3.0 255.255.255.252 area 0
Router(config-router)#network 172.29.3.12 255.255.255.252 area 0

Configuración Router Bogotá 3

Interfaz S0/0/0

Router>
Router>en
Router#conf t
Router(config)#int s0/0/0

Router(config-if)#description BOGOTA3-BOGOTA1
Router(config-if)#ip add 172.29.3.10 255.255.255.252
Router(config-if)#no shut

Interfaz S0/0/1

Router(config-if)#int s0/0/1
Router(config-if)#description BOGOTA3-BOGOTA2
Router(config-if)#ip add 172.168.3.14 255.255.255.252
Router(config-if)#clock rate 128000
Router(config-if)#no shut

Interfaz G0/0

Router(config-if)#int g0/0
Router(config-if)#description BOGOTA3-PC3
Router(config-if)#ip add 172.29.1.1 255.255.255.0
Router(config-if)#no shut

Configuración OSPF 1

Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 172.29.3.8 255.255.255.252 area 0
Router(config-router)#network 172.29.3.12 255.255.255.252 area 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.

Comando Medellin1

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

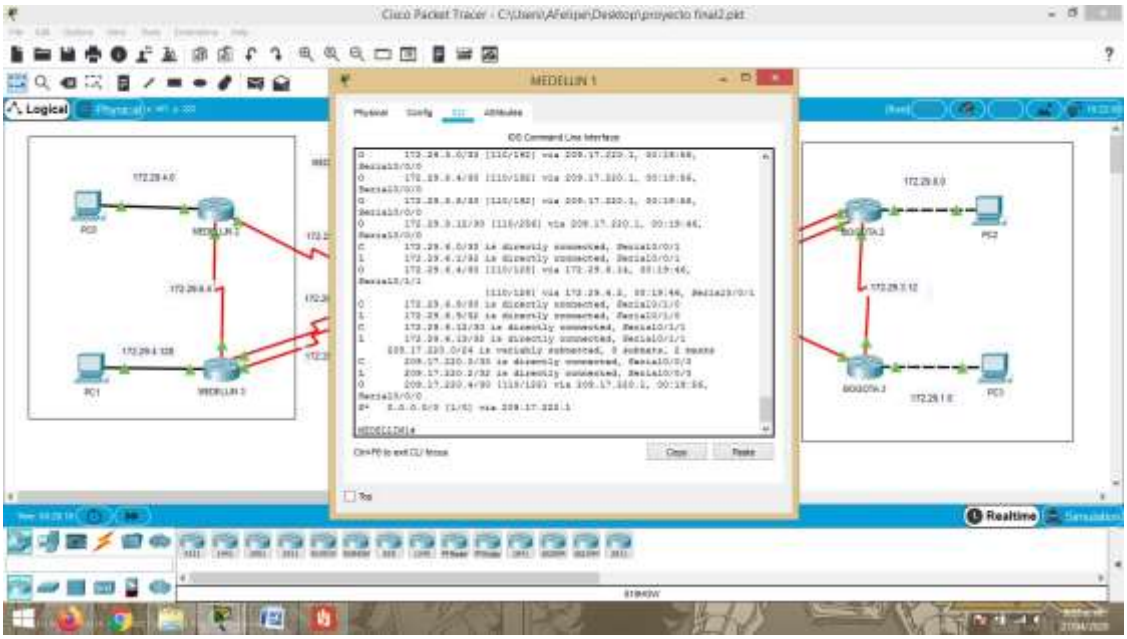


Imagen 20. router Medellin 1 comando show ip route

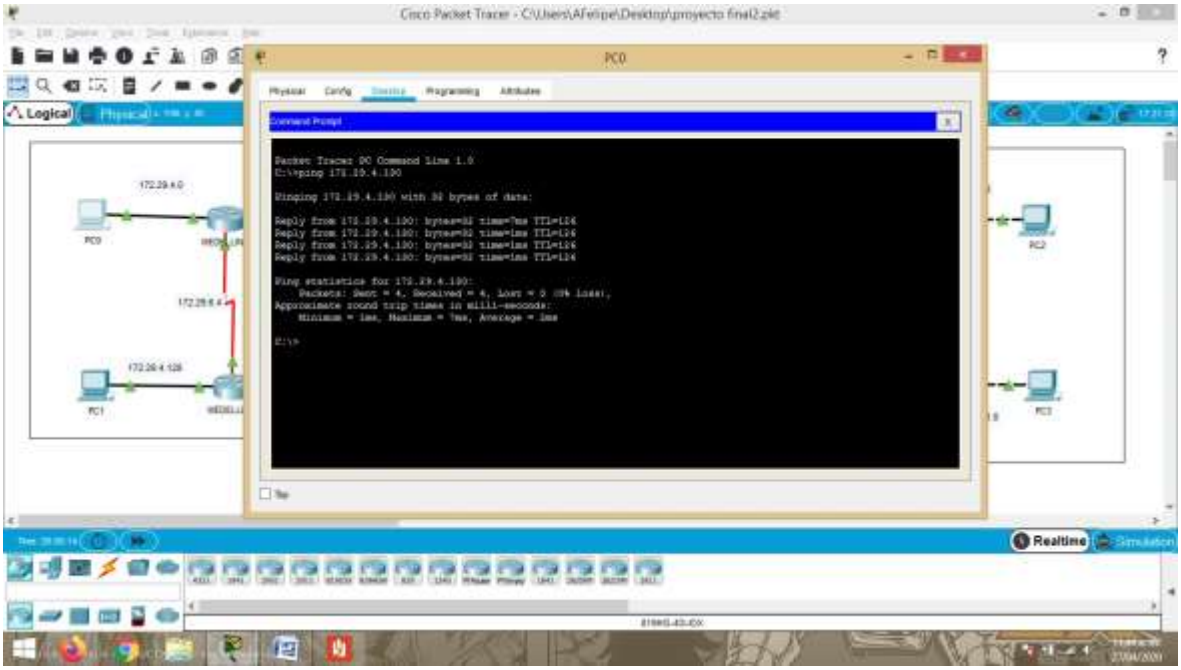


Imagen 21. ping red MEDELLIN de PC0 a PC1

Comandos Bogota1

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.5

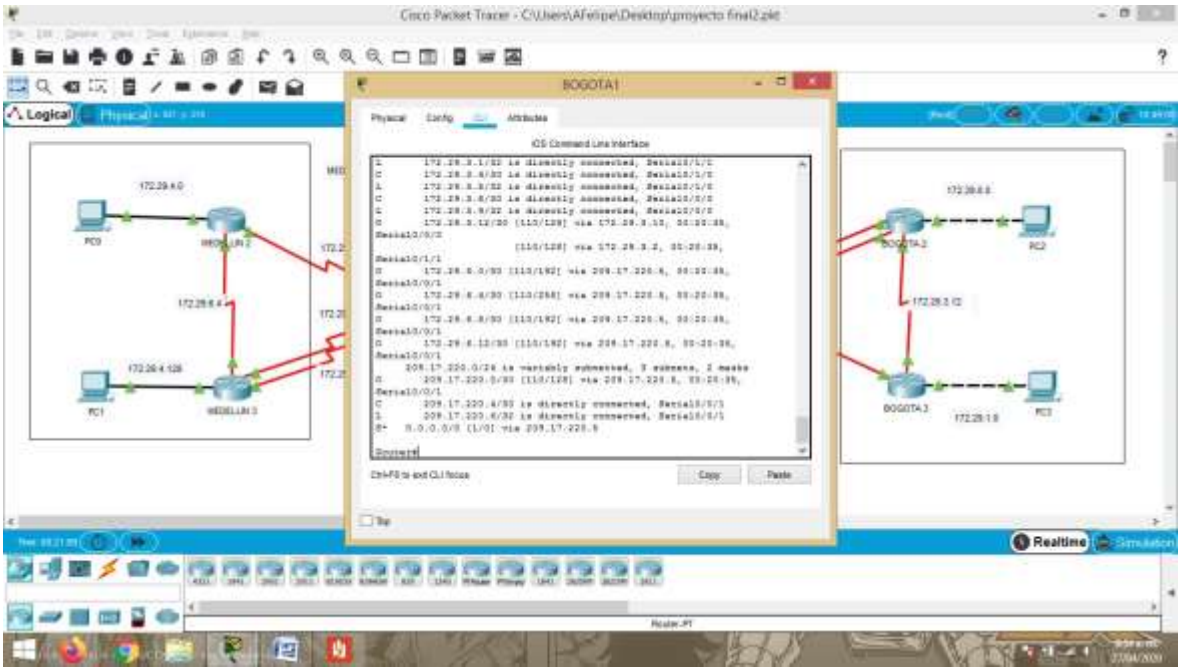


Imagen 22. router Bogota 1 comando show ip route

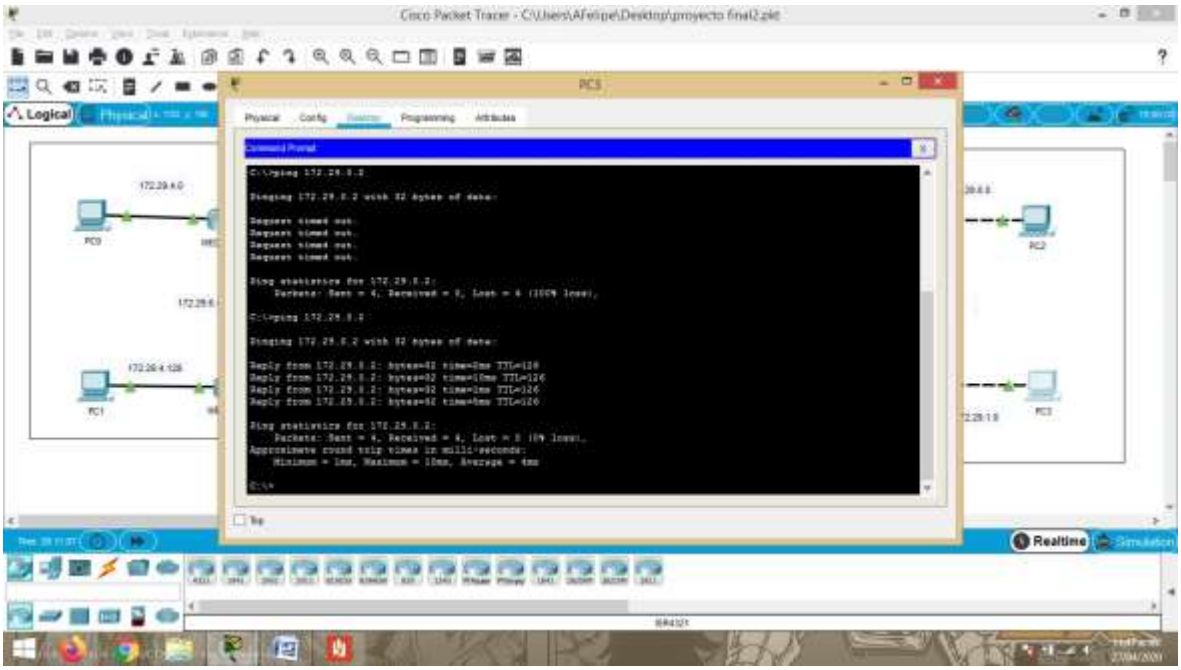


Imagen 23. ping red MEDELLIN de PC0 a PC1

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.

Comando Ruta Estatica ISP

ISP#conf t
ISP(config)# ip route 172.29.4.0 255.255.255.0 Serial0/0/0
ISP(config)# ip route 172.29.0.0 255.255.255.0 Serial0/0/1
ISP(config)# ip route 172.29.4.128 255.255.255.128 Serial0/0/0
ISP(config)# ip route 172.29.1.0 255.255.255.0 Serial0/0/1

PARTE 2: TABLA DE ENRUTAMIENTO.

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

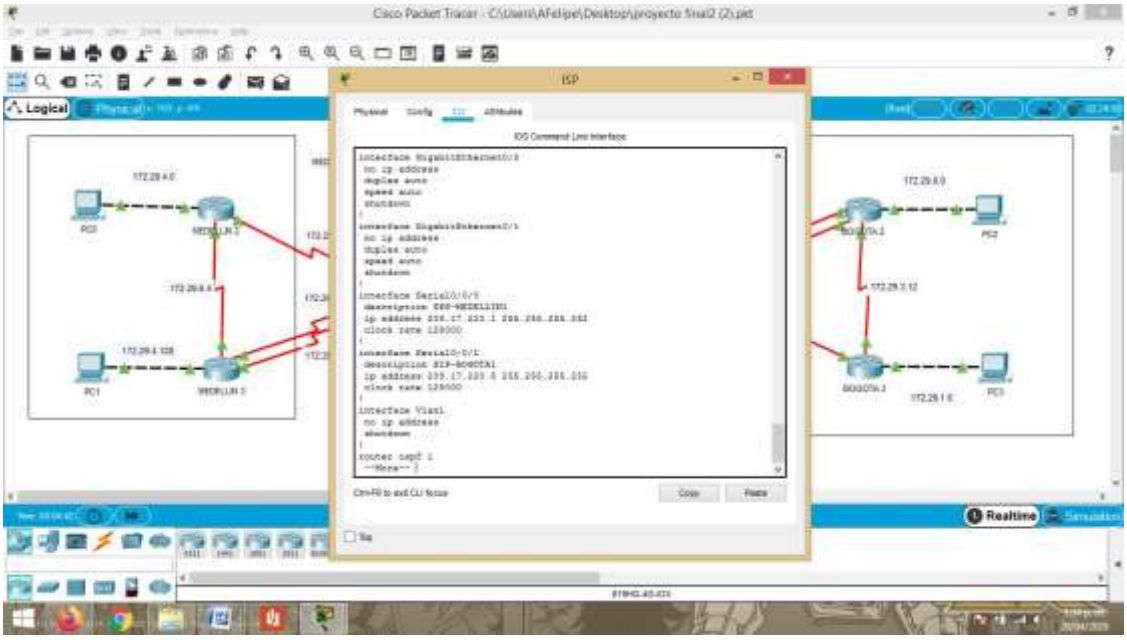


Imagen 24. tabla enrutamiento ROUTER ISP

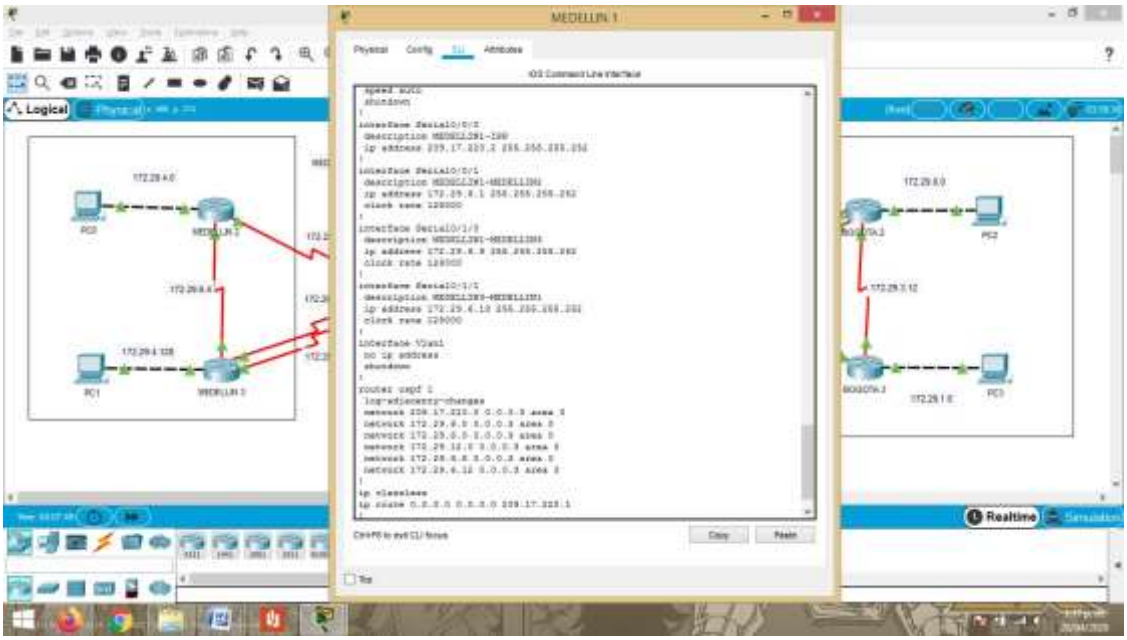


Imagen 25. tabla enrutamiento MEDELLIN1

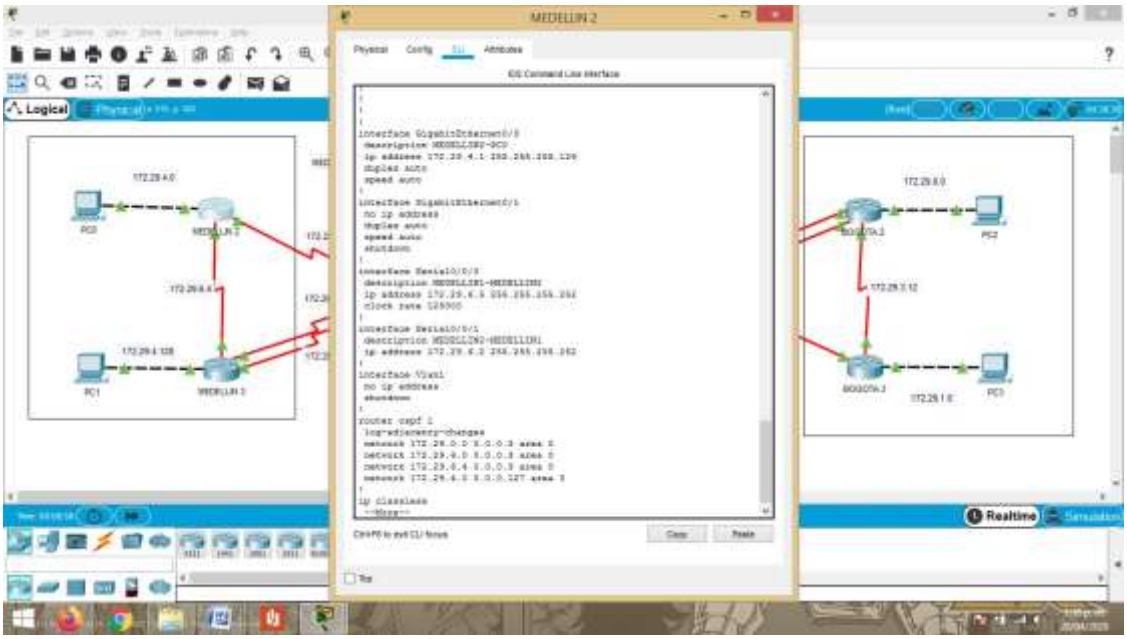


Imagen 26. tabla enrutamiento MEDELLIN2

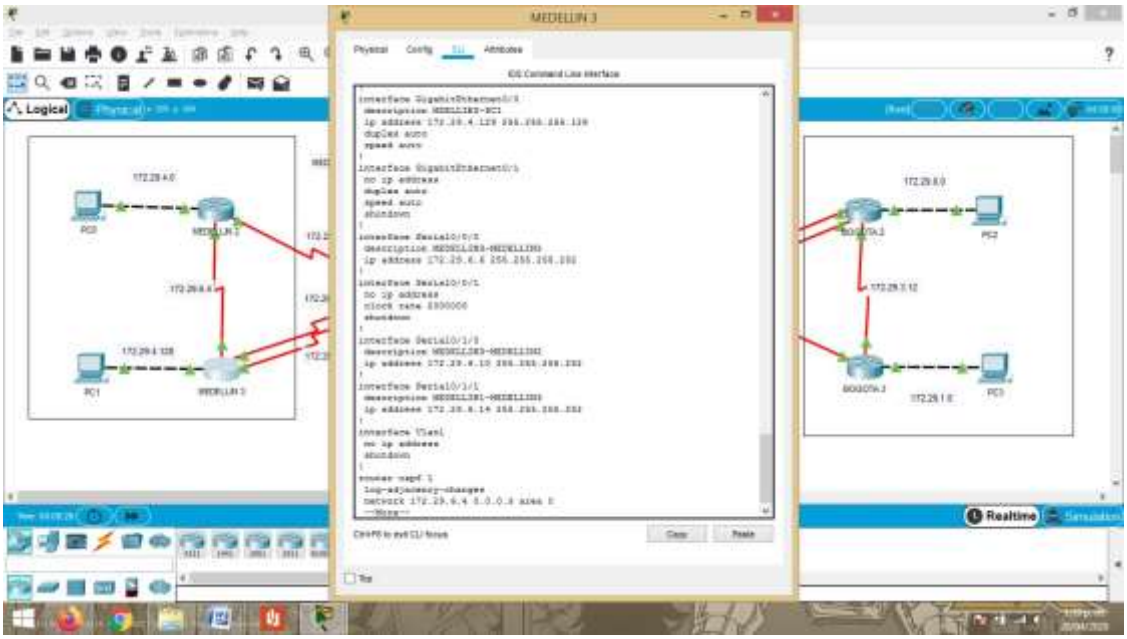


Imagen 27. tabla enrutamiento MEDELLIN3

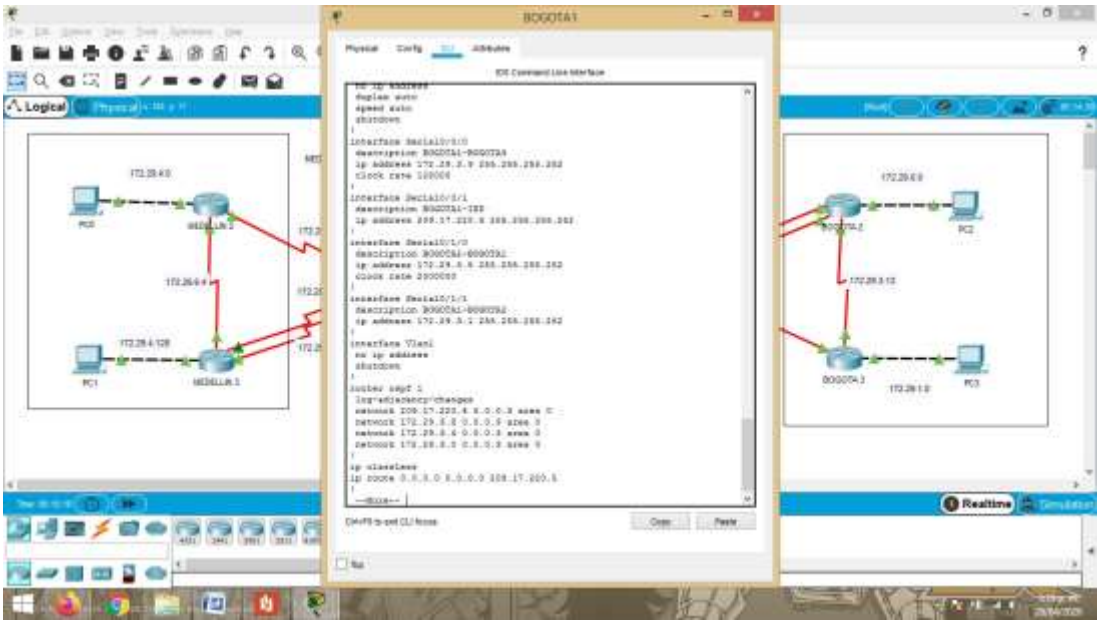


Imagen 28. tabla enrutamiento BOGOTA1

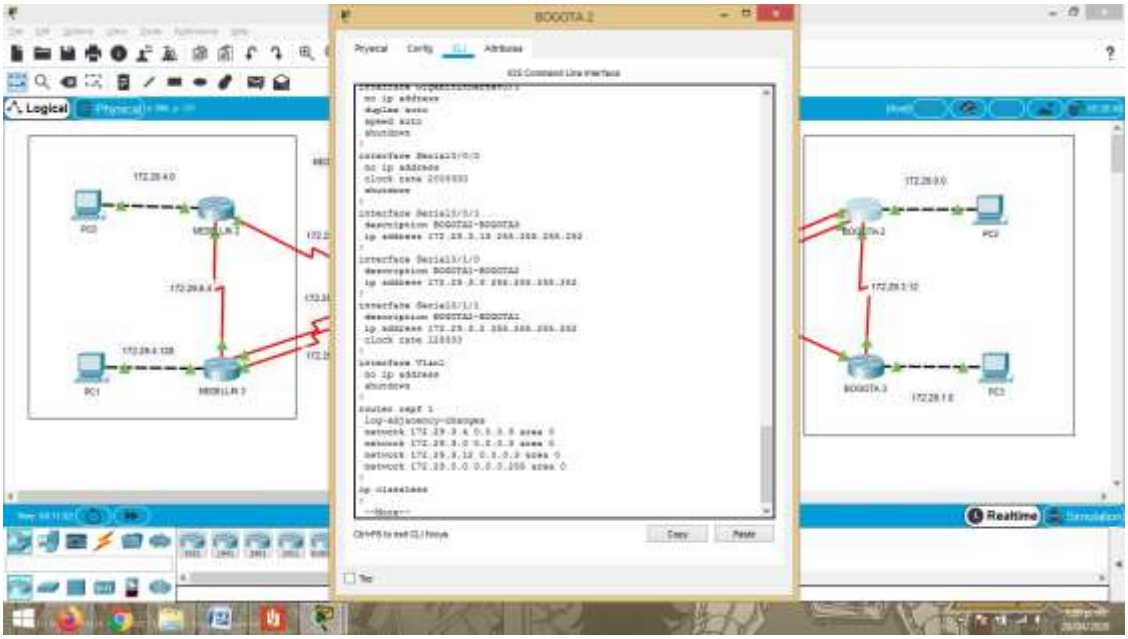


Imagen 29. tabla enrutamiento BOGOTA2

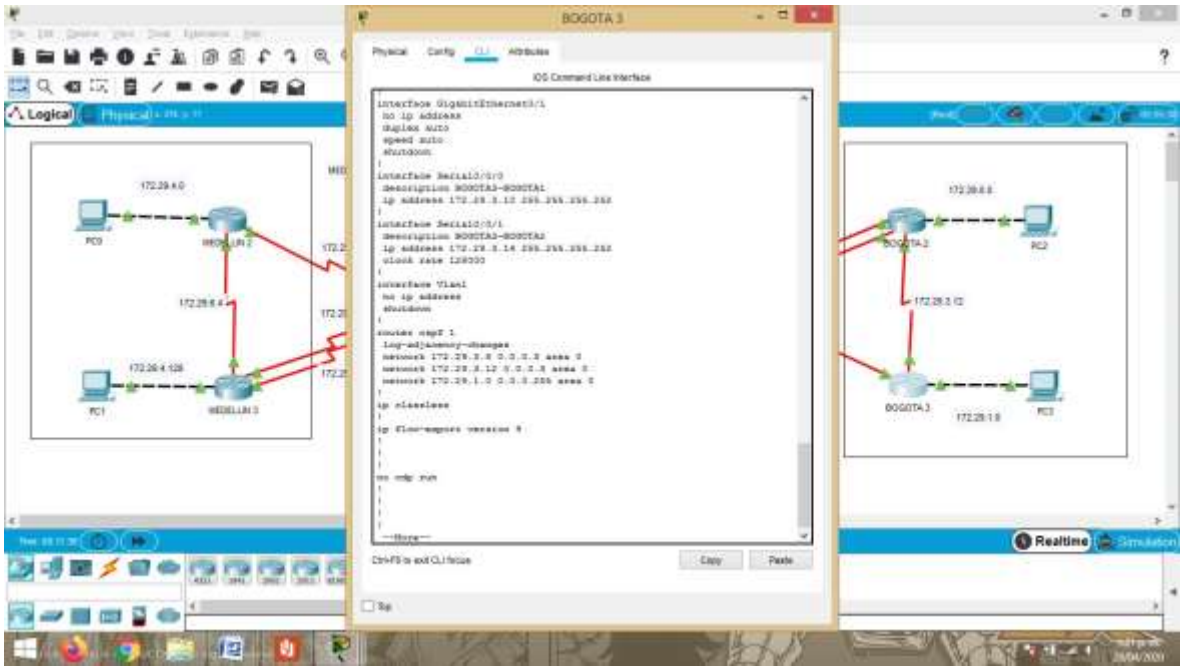


Imagen 30. tabla enrutamiento BOGOTA3

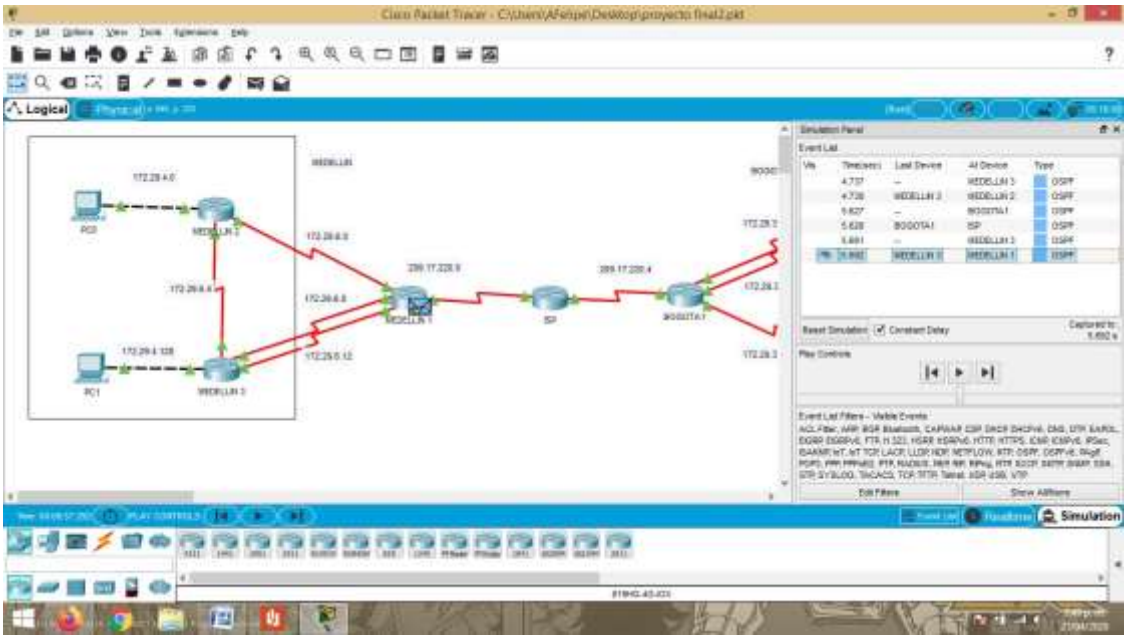


Imagen 31. envío de paquetes desde MEDELLIN2 A MEDELLIN1

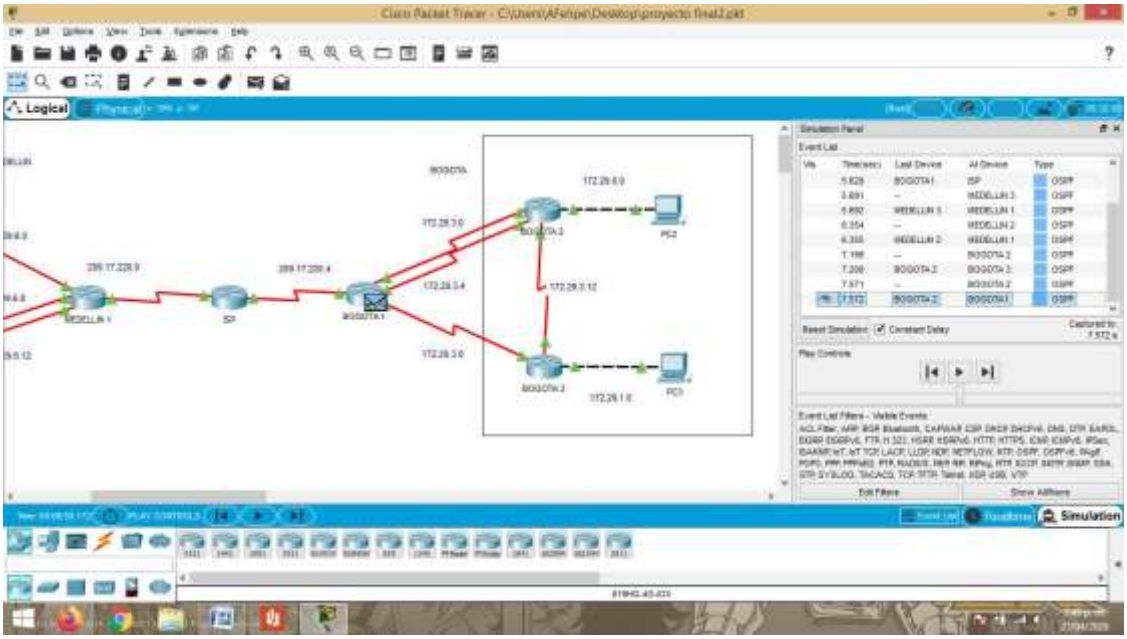


Imagen 32. envió de paquetes BOGOTA2- BOGOTA1

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

R: Estos se presentan en los router MEDELLIN3 Y BOGOTA2, donde las conexiones dobles nos permiten balancear la información.

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.

R: BOGOTA1 Y MEDELLIN1 Son redes similares en el número de conexiones que estos se encuentran pero además están conectadas al ROUTER ISP

d. Los routers Medellín2 y Bogotá3 también presentan redes conectadas directamente y recibidas mediante OSPF.

R: Podemos verificar por el comando show ip route las redes conectadas por OSPF EN LOS ROUTERS MEDELLIN2 Y BOGOTA3

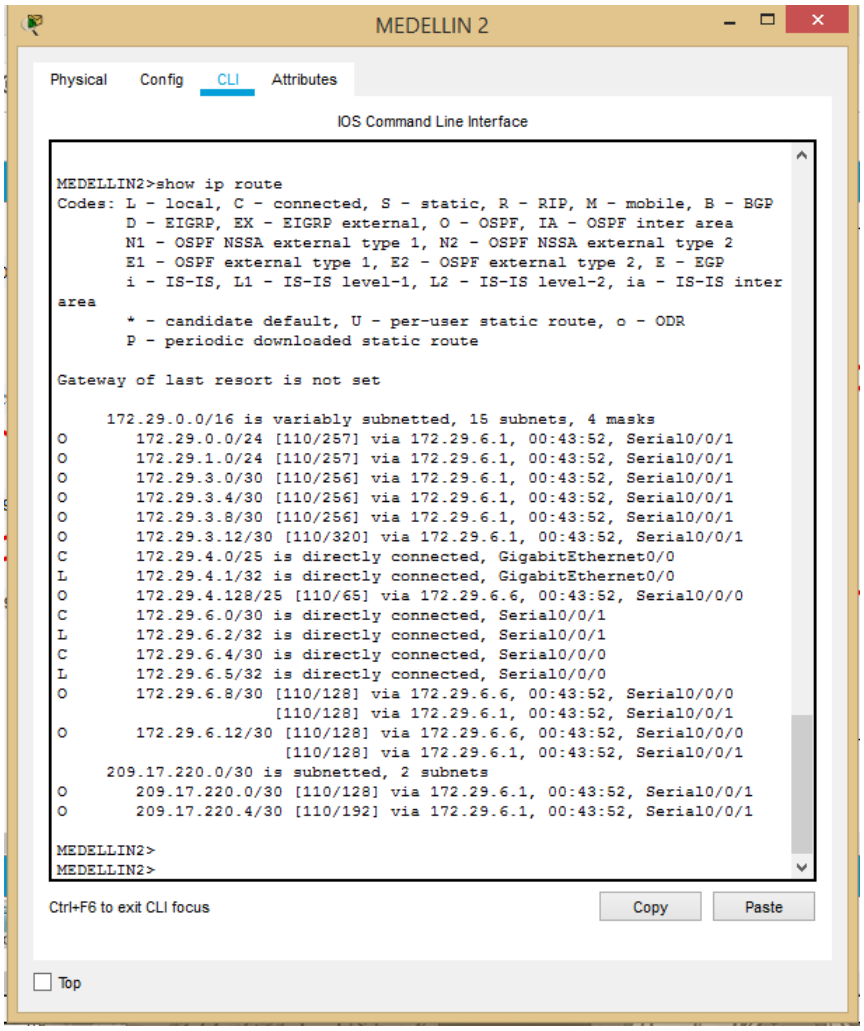


Imagen 33. show ip route en Router Medellin2

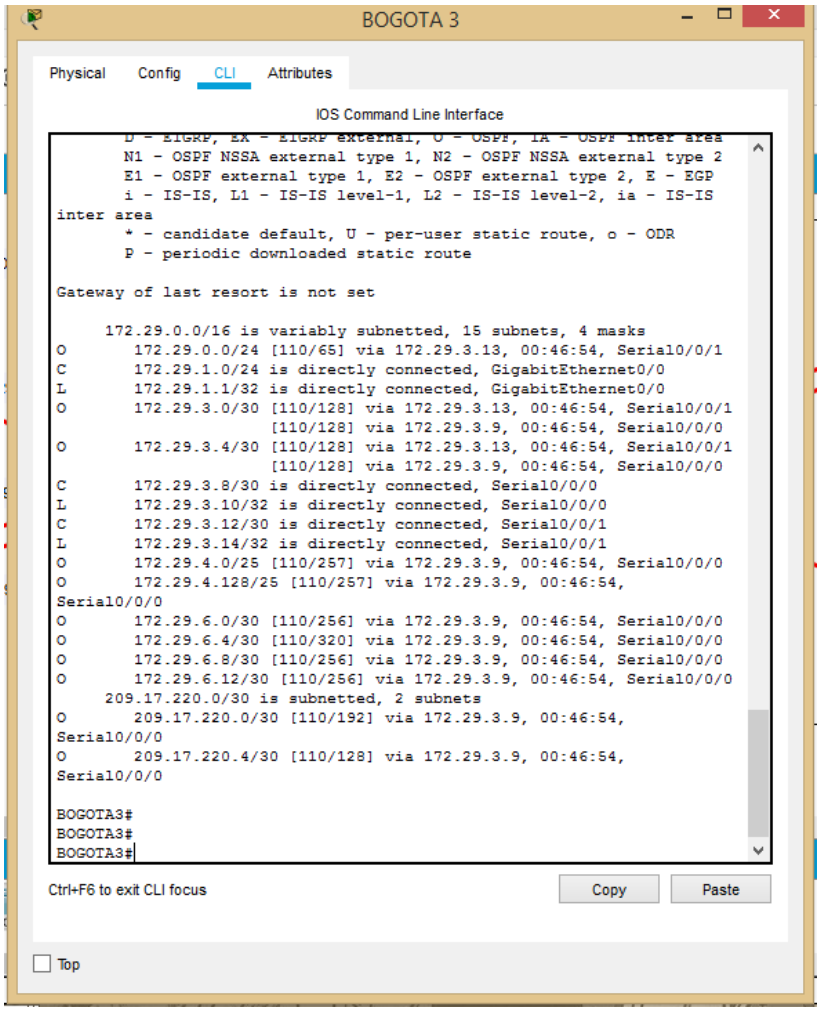


Imagen 34. show ip route en Router BOGOTA3

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

.

R: Estas son las especificadas en el punto b, donde se halla más de una ruta para acceder a internet.

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

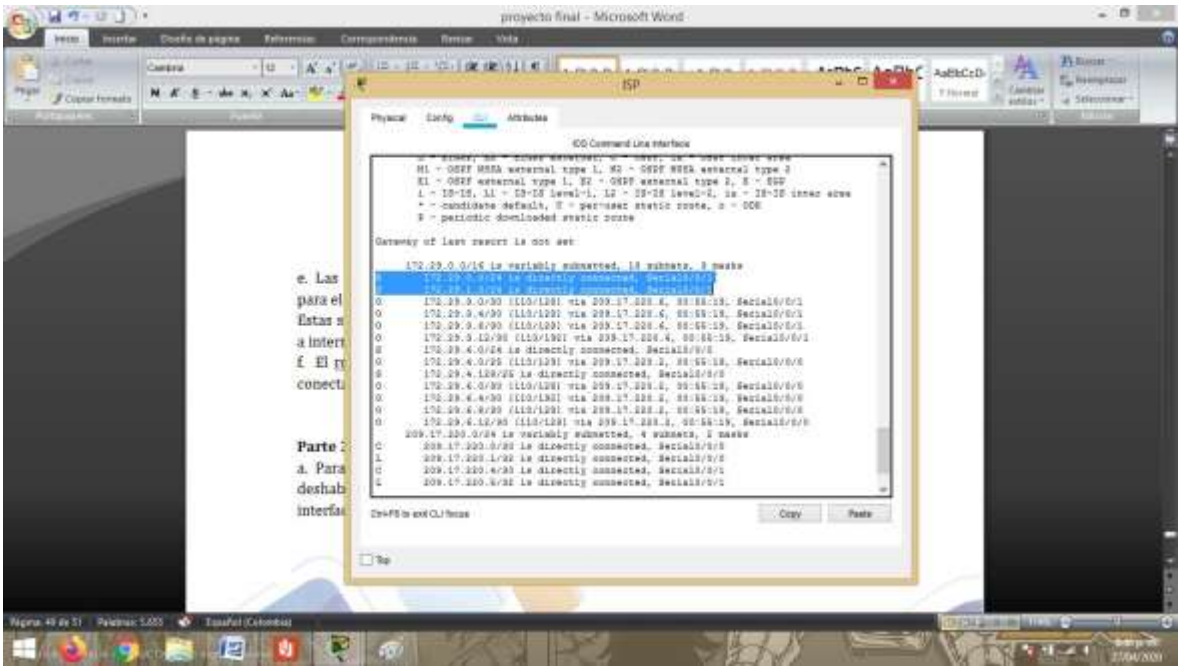


Imagen 35. router ISP donde se verifica las redes estáticas en este

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

R: revisando la documentación del protocolo OSPF se configuro adecuadamente cada puerto que se utiliza con el protocolo OSPF. Cabe recalcar que no se puede deshabilitar la propagación de los puertos que quedan sobrantes en OSPF como se hace con RIP ver 2

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.

R: Verificamos los passive interface configurados en los routers MEDELLIN2-MEDELLIN3-BOGOTA2-BOGOTA3 en los purtos g0/0 utilizando el comando show ip ospf interface

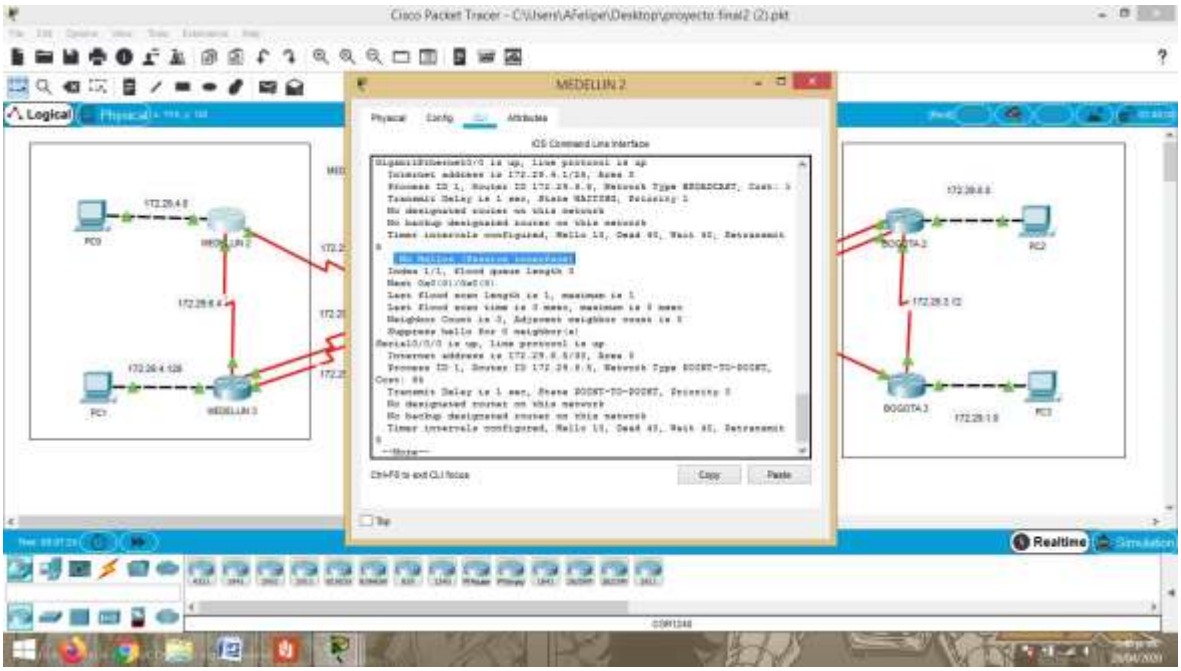


Imagen 36. passive interface router MEDELLIN2

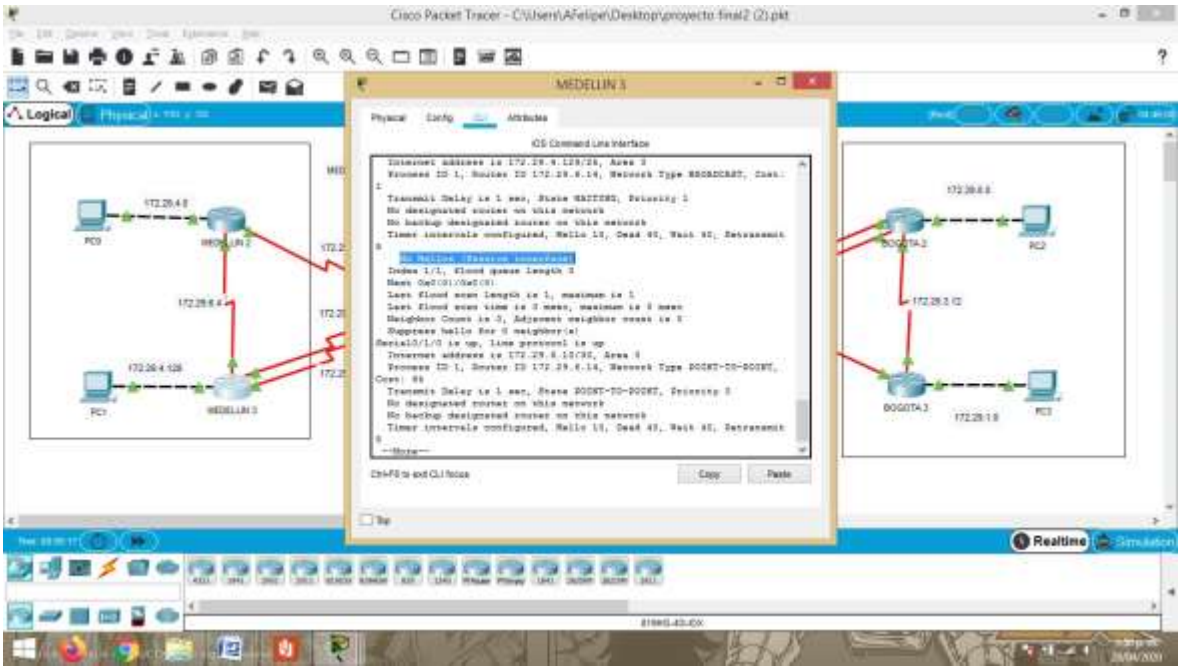


Imagen 37. passive interface router MEDELLIN2

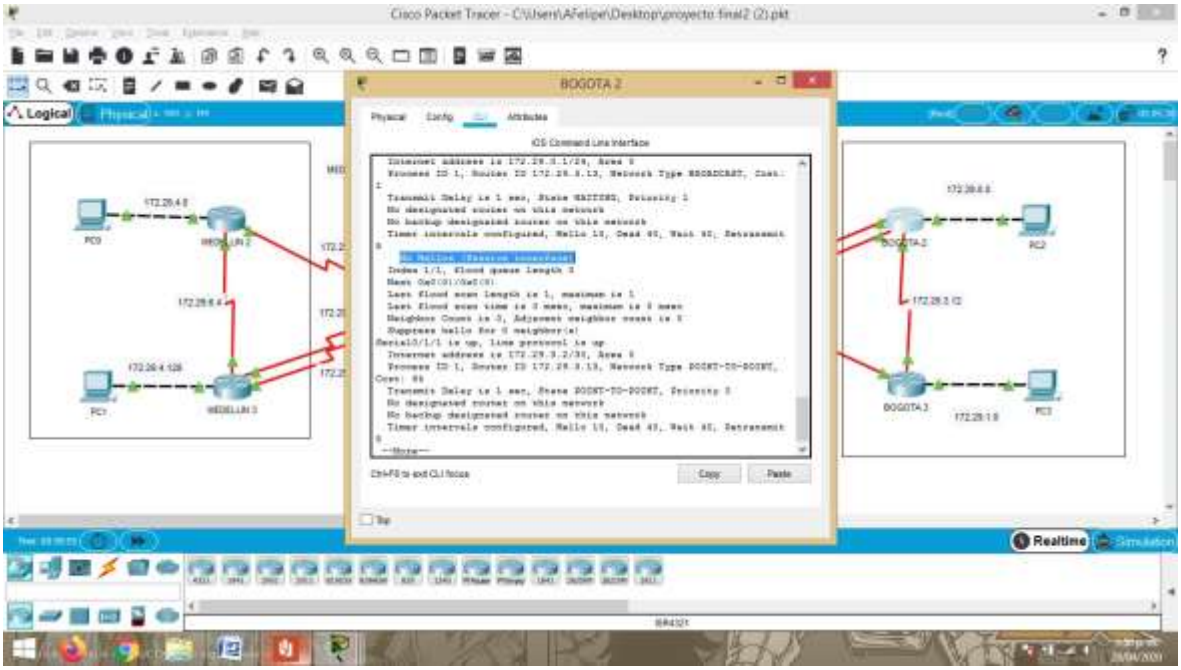


Imagen 38. passive interface router BOGOTA2

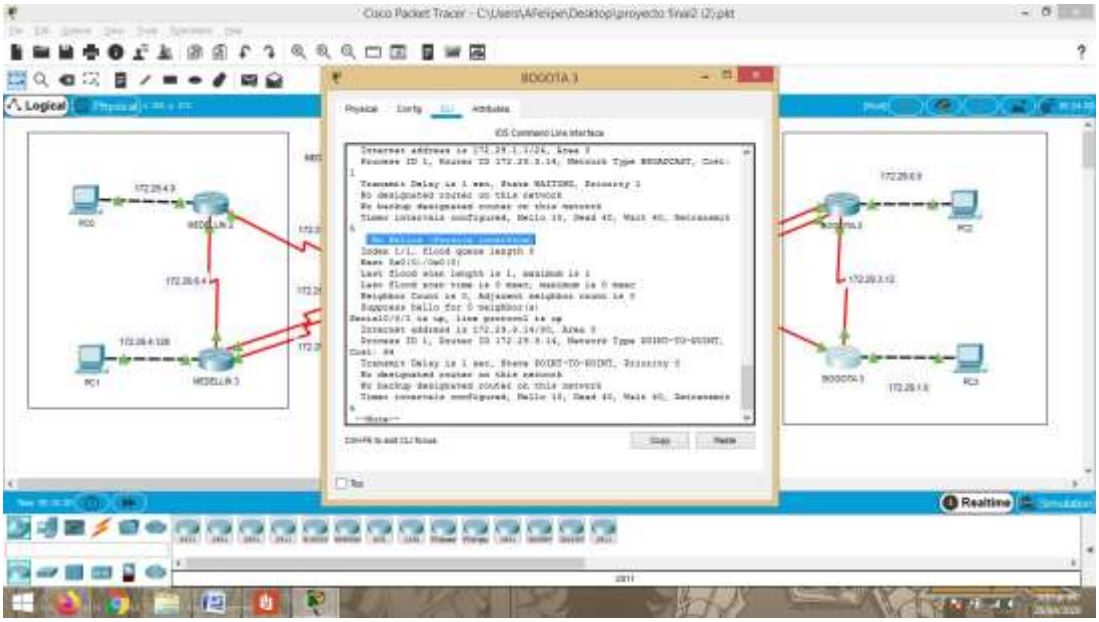


Imagen 39. passive interface router MEDELLIN2

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.

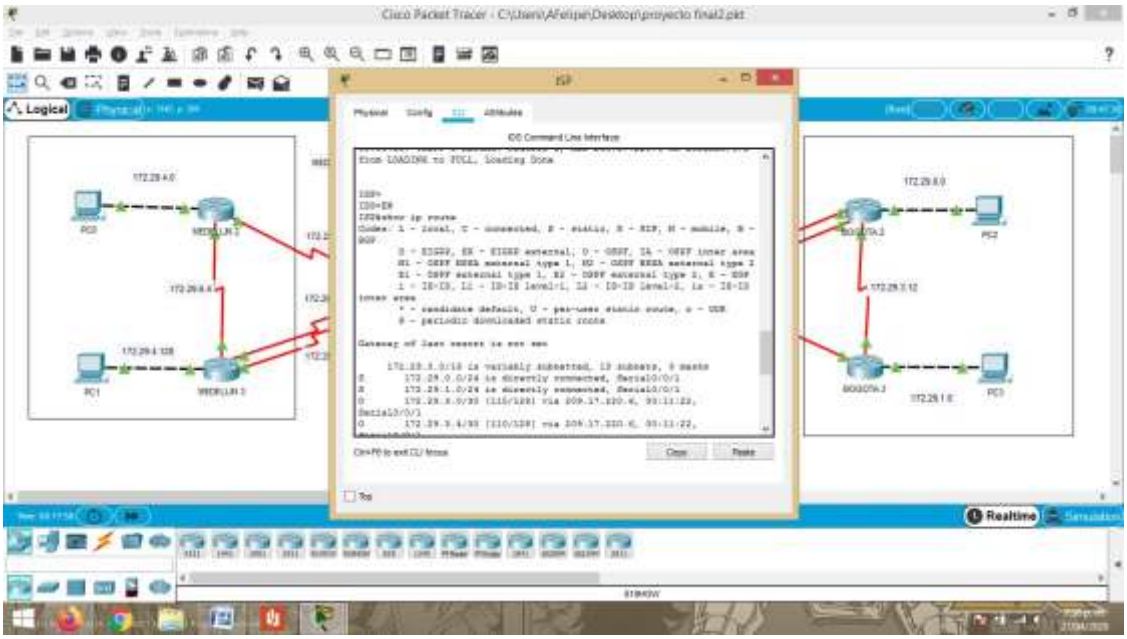


Imagen 40. rutas en router isp

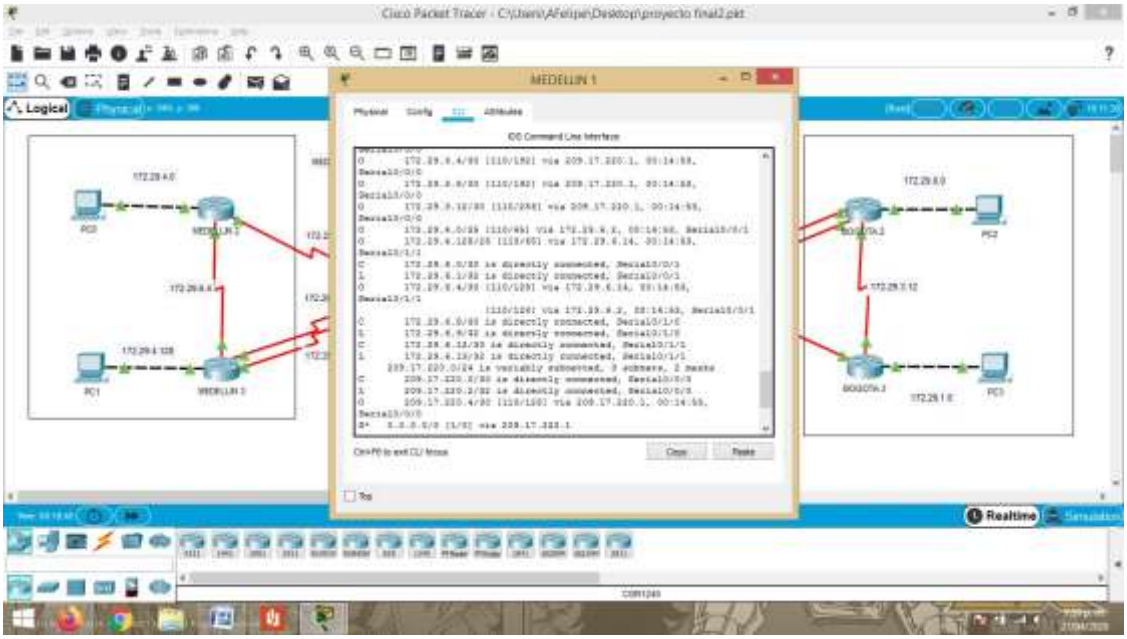


Imagen 41. rutas en router medellin1

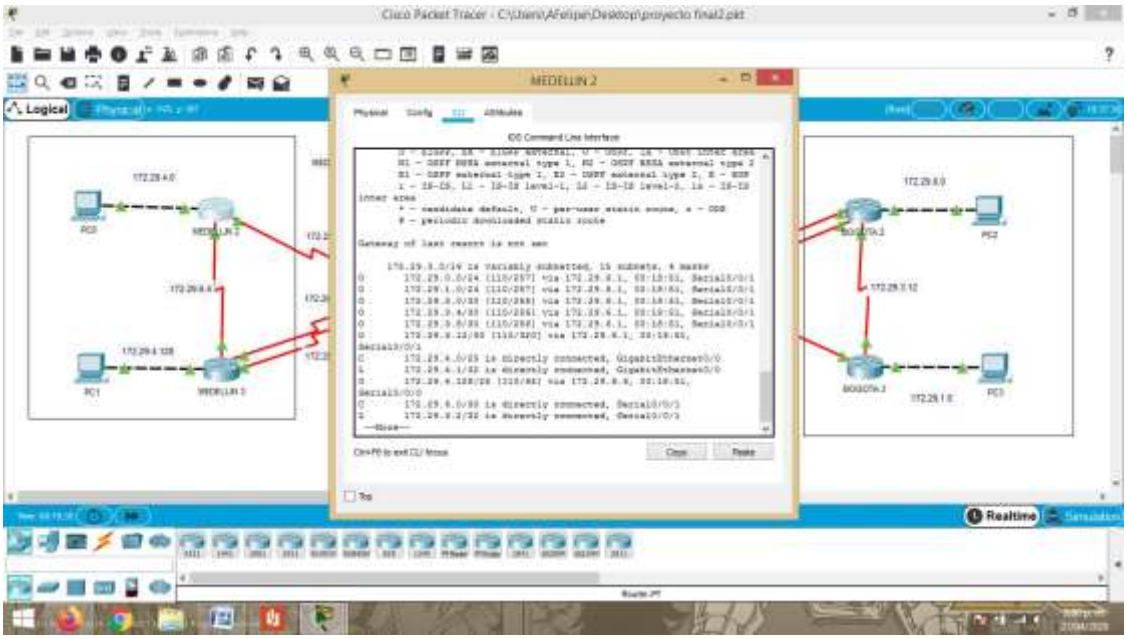


Imagen 42. rutas en router medellin2

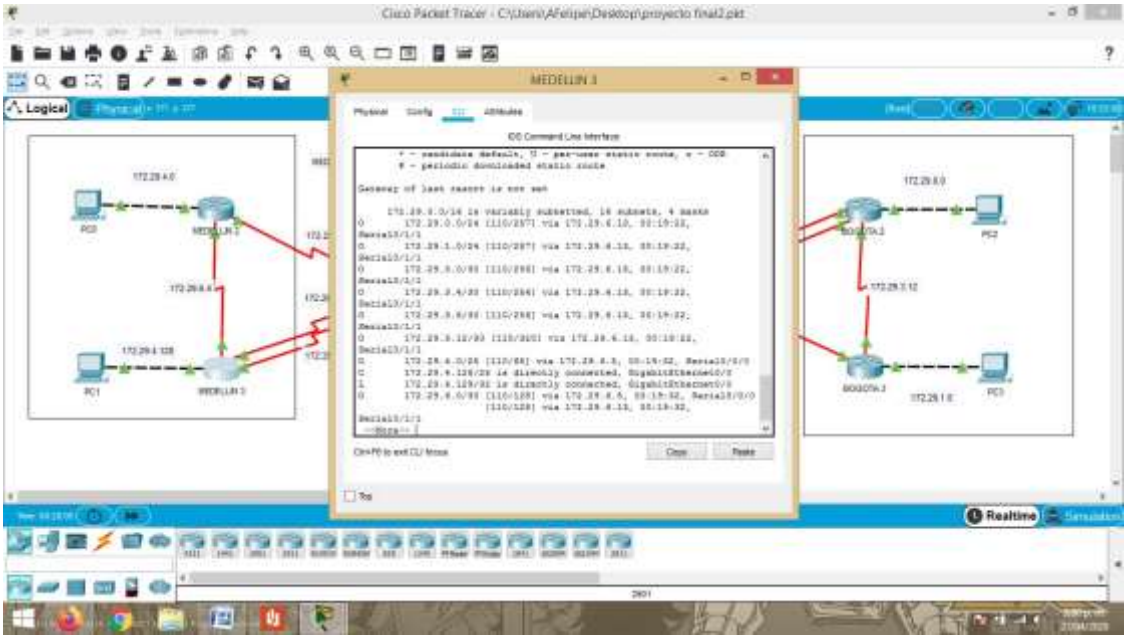


Imagen 43. rutas en router medellin3

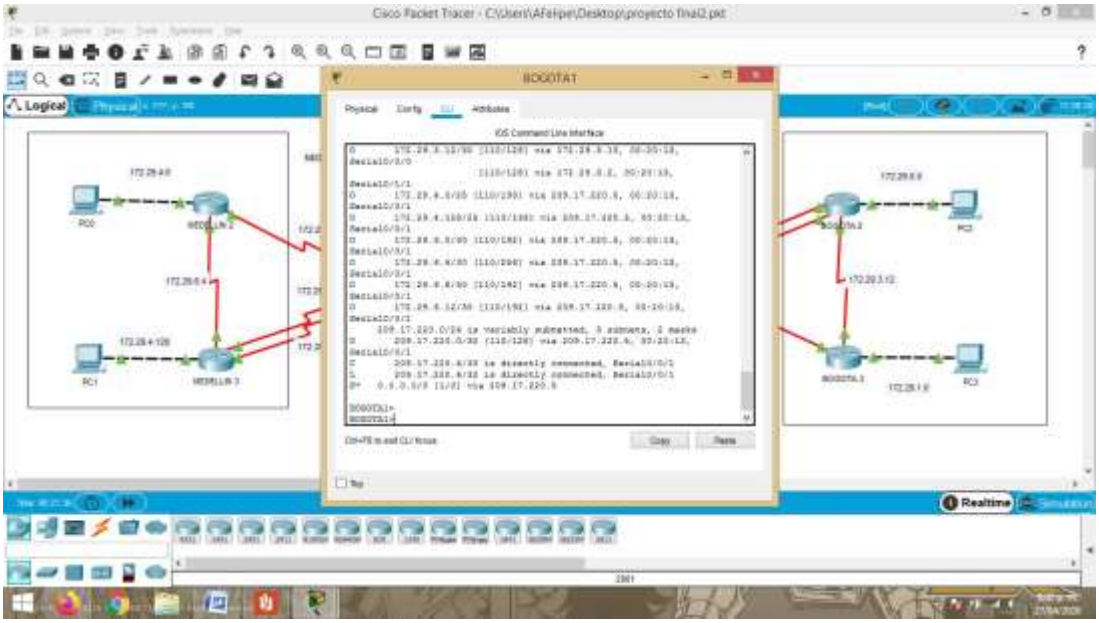


Imagen 44. rutas en router bogota1

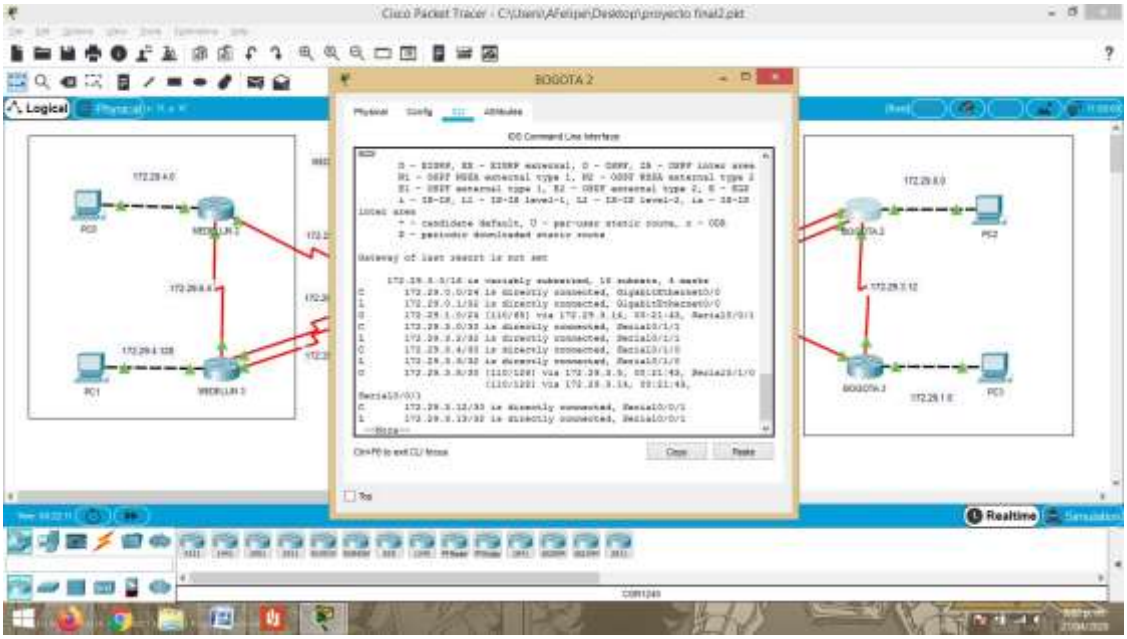


Imagen 45. rutas en router bogota2

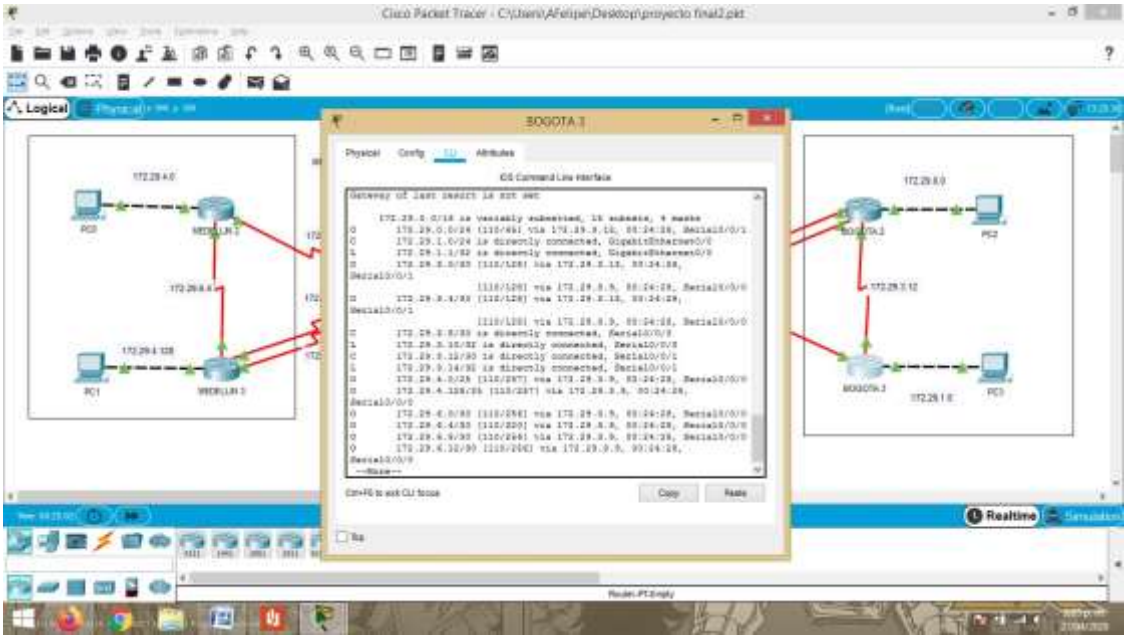


Imagen 46. rutas en router bogota3

PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

IPS

ISP#conf t
ISP(config)#username MEDELLIN1 pass 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 pass cisco
ISP(config-if)#exit

Medellin1

MEDELLIN1#en
MEDELLIN1#conf t
MEDELLIN1(config)#user
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 pass cisco
MEDELLIN1(config-if)#end

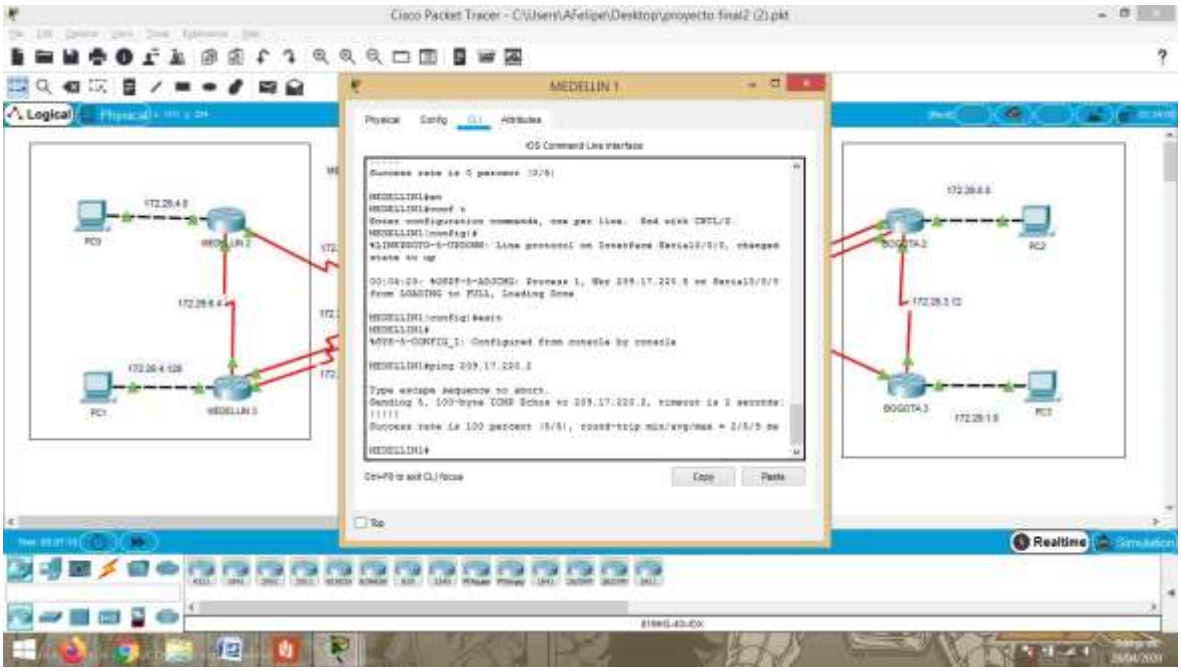


Imagen 47. Ping a ROUTER ISP

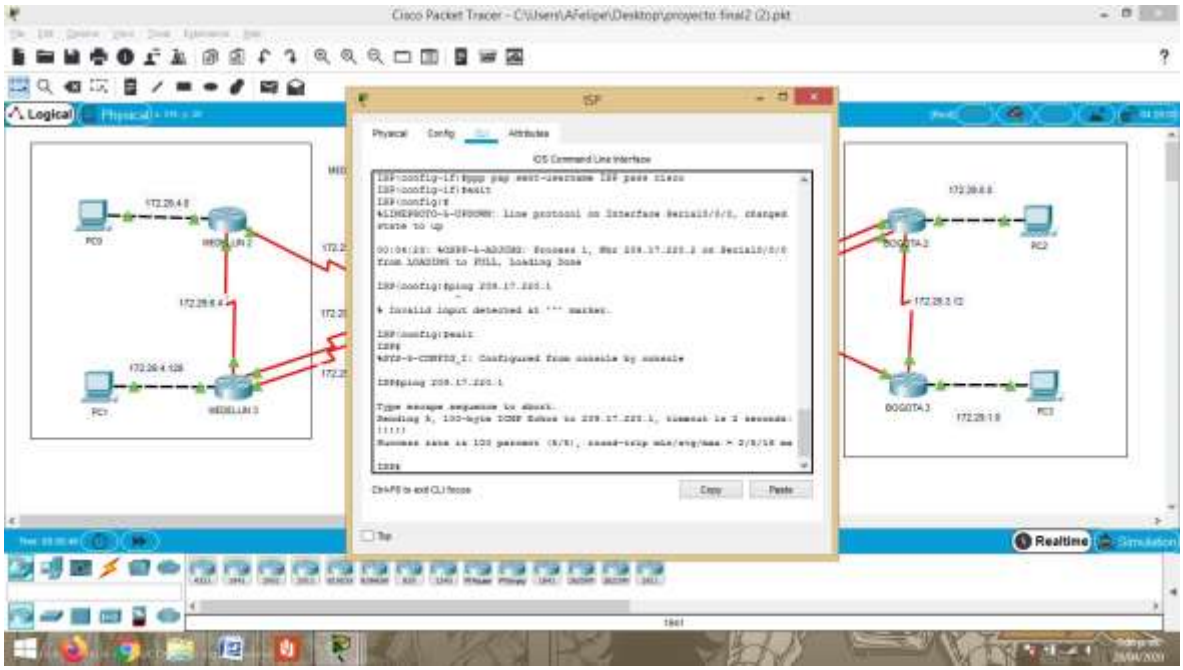


Imagen 48. Ping a ROUTER MEDELLIN1

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

ISP
ISP(config)#user
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#end

Bogota1

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#username ISP pass cisco
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#end

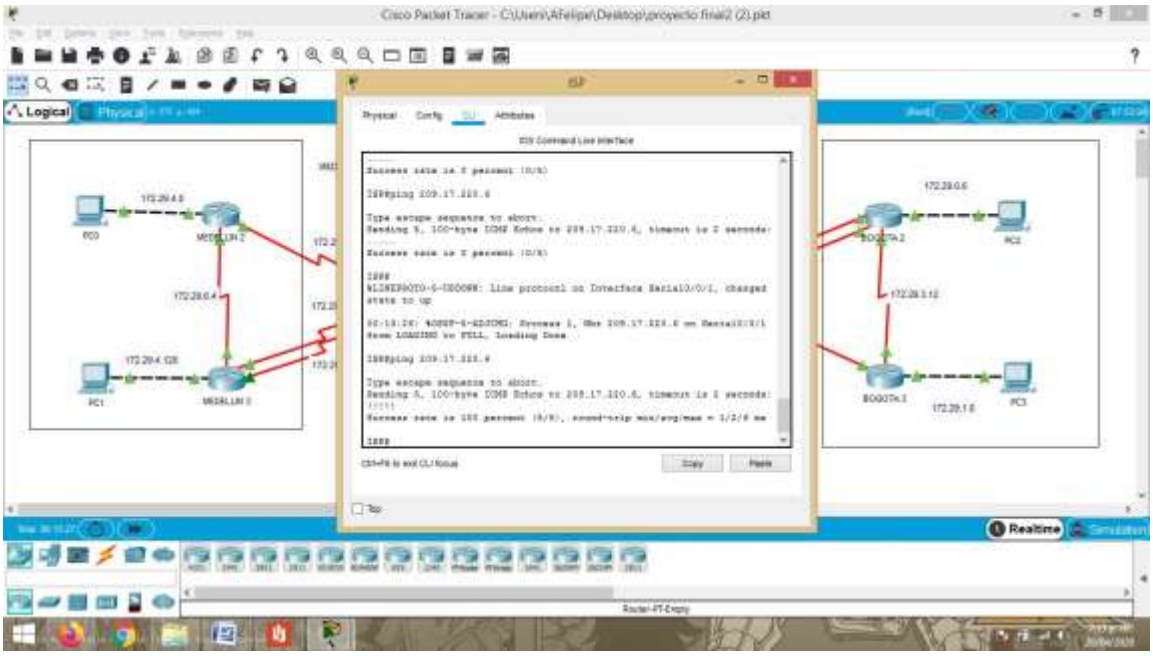


Imagen 49. Ping a ROUTER ISP

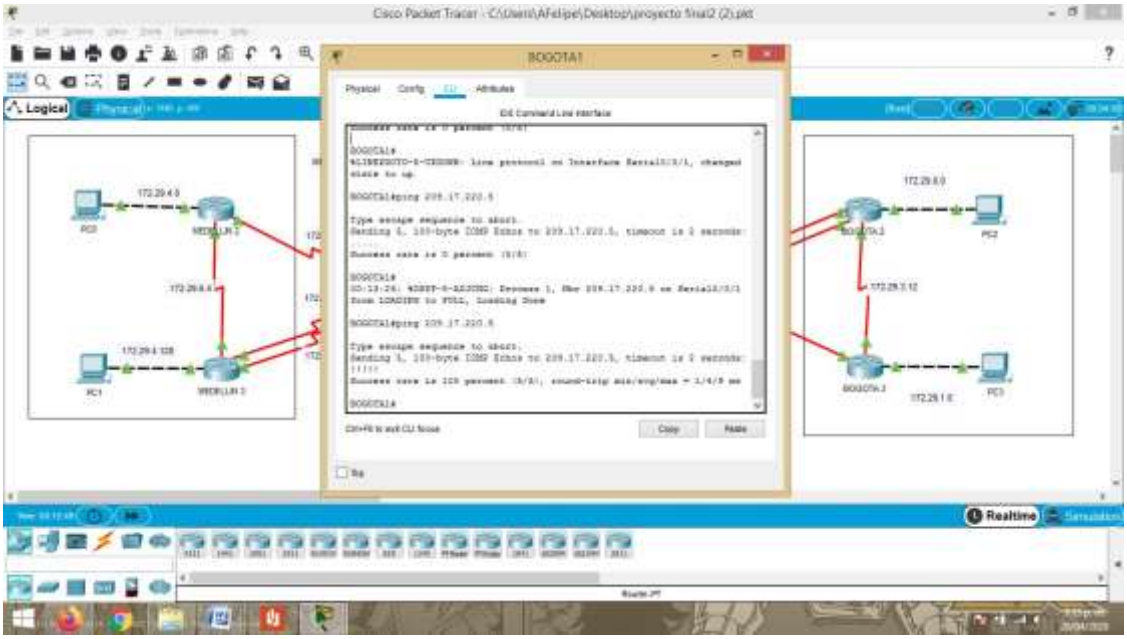


Imagen 50. Ping a ROUTER BOGOTA1

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.

R: al activar el NAT en los router Bogota1 y Medellin1 se restringe el envió de paquetes en router que se encuentran en las redes diferentes como observamos en los siguientes pantallazos

```
MEDELLIN1#conf t
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside source list HOST interface s0/0/0 overload
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#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
```

```
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/1 overload
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
```

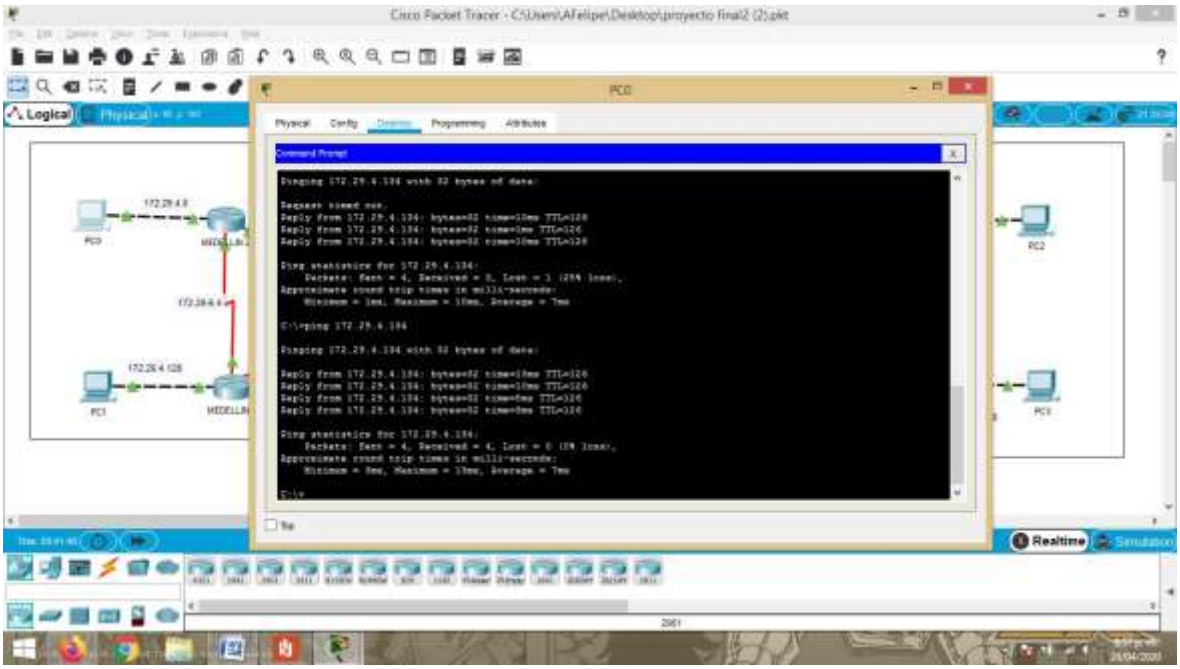


Imagen 51. Ping de pc0 a pc1 en la red Medellín 1

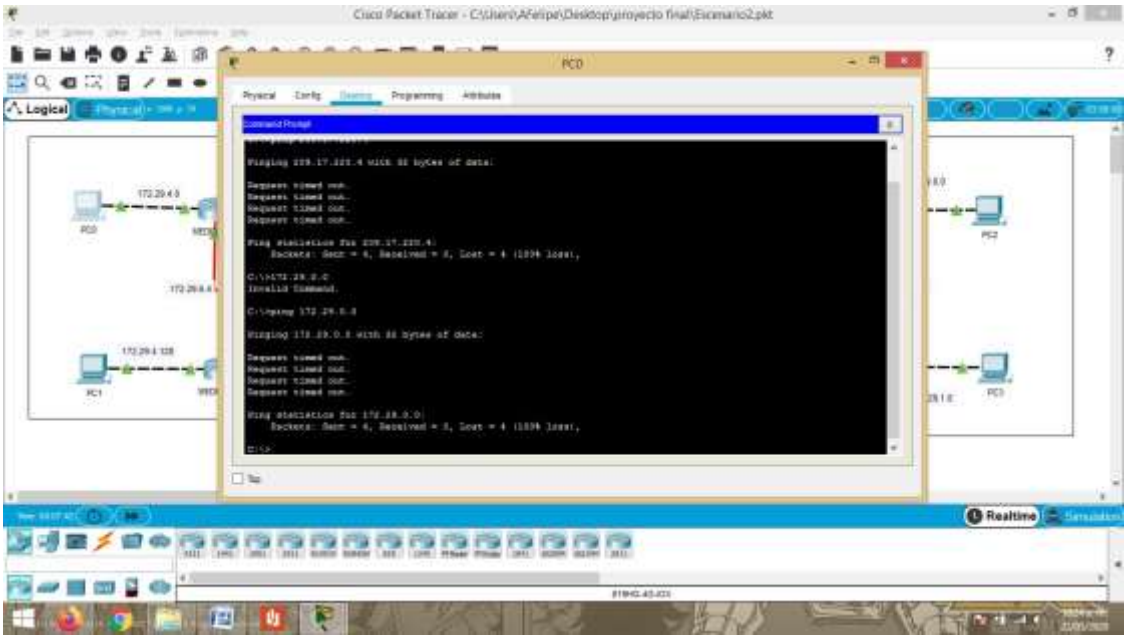


Imagen 52. Ping de PC-0 a red de Bogotá 1

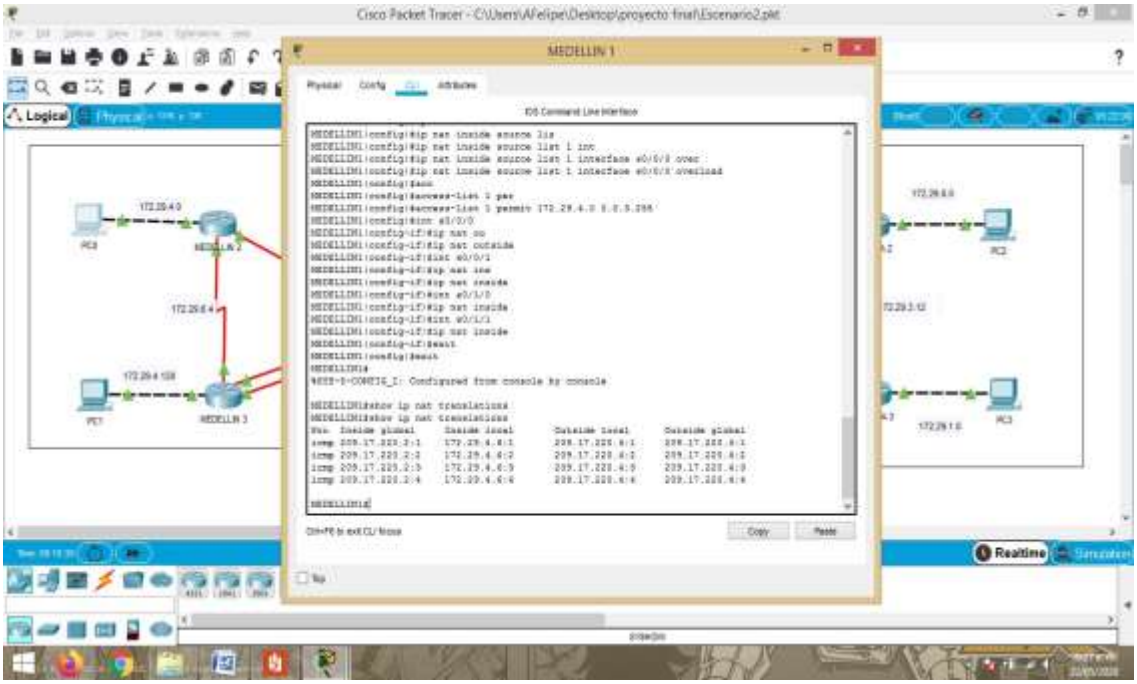


Imagen 53. Show ip nat Translations en Medellin1

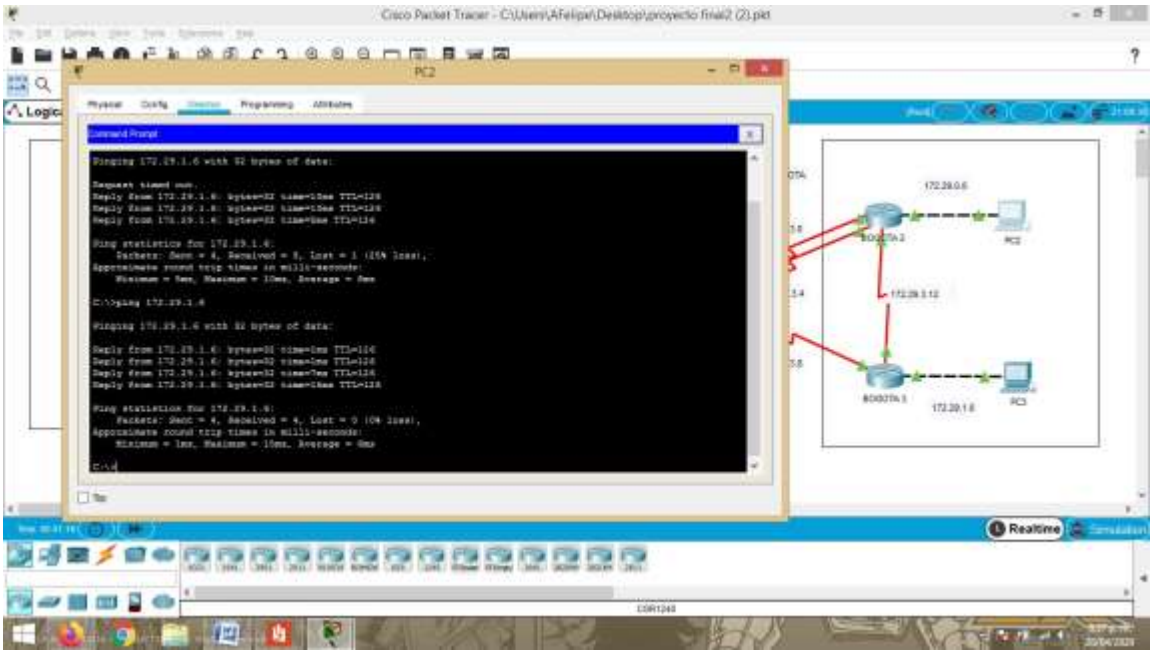


Imagen 54. Ping de pc2 a pc3 en la red Bogotá

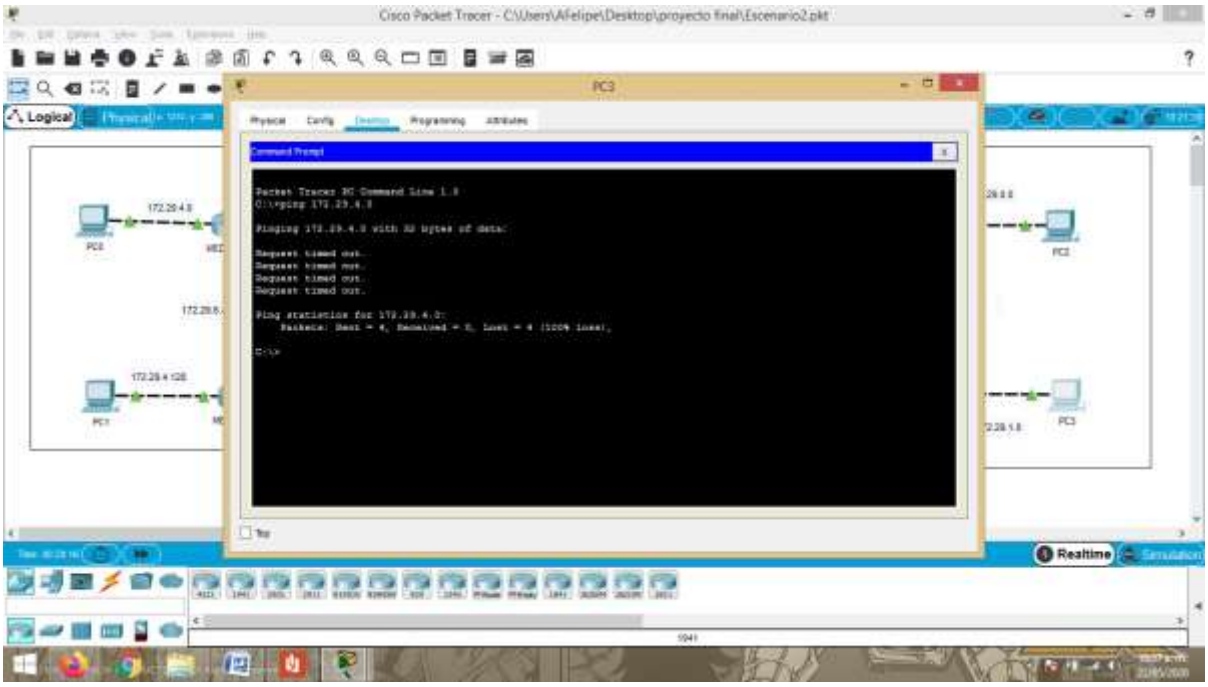


Imagen 55. Ping PC 3 a red Medellín

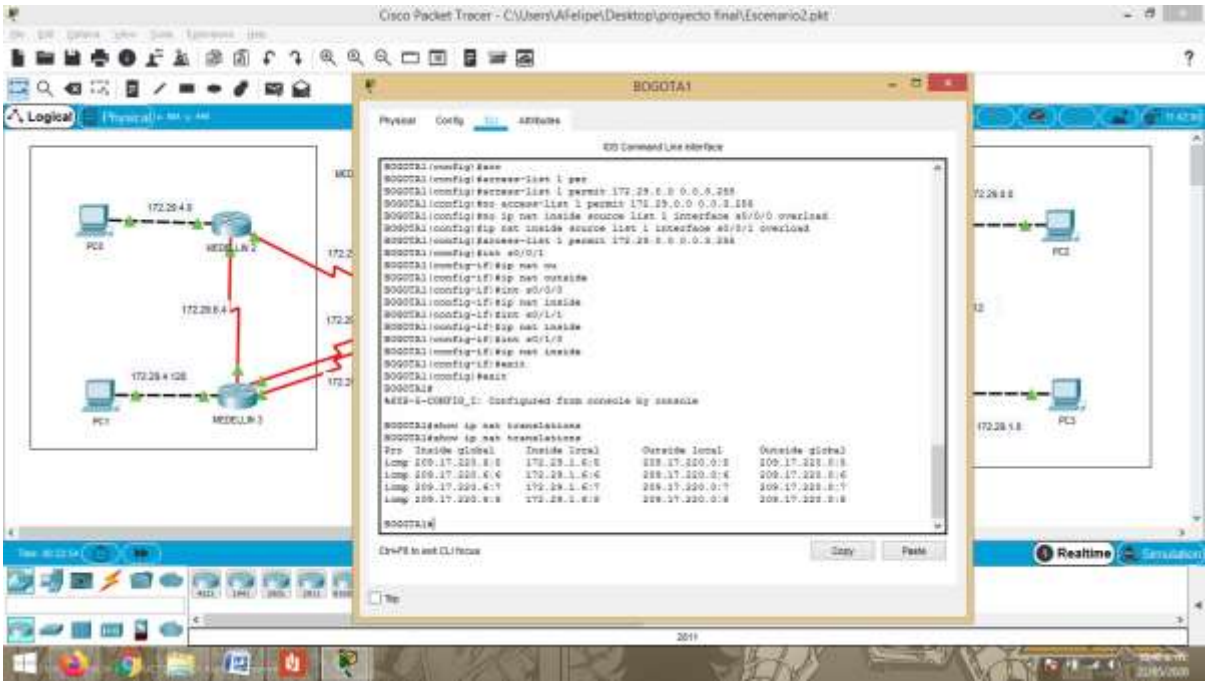


Imagen 56. Comando show ip nat translation en Bogotá 1

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.

Configuracion NAT En Router Medellin1

```
MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside source list HOST interface s0/0/0 overload
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
```

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

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.

Configuración NAT Bogota1

```
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/1 overload
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
```

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.

Configuración De DHCP Router Medellin2

```
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)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
```

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

Configuración Router Medellin3

```
MEDELLIN3>en
MEDELLIN3#conf t
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#
```

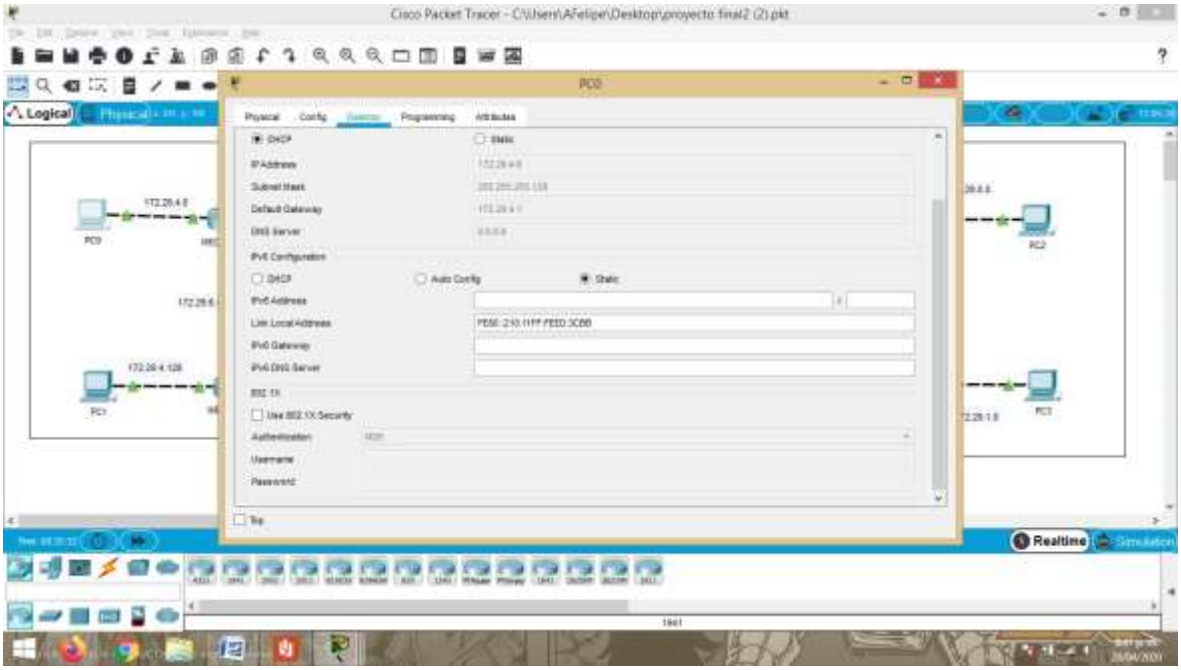


Imagen 57. DHCP pc0

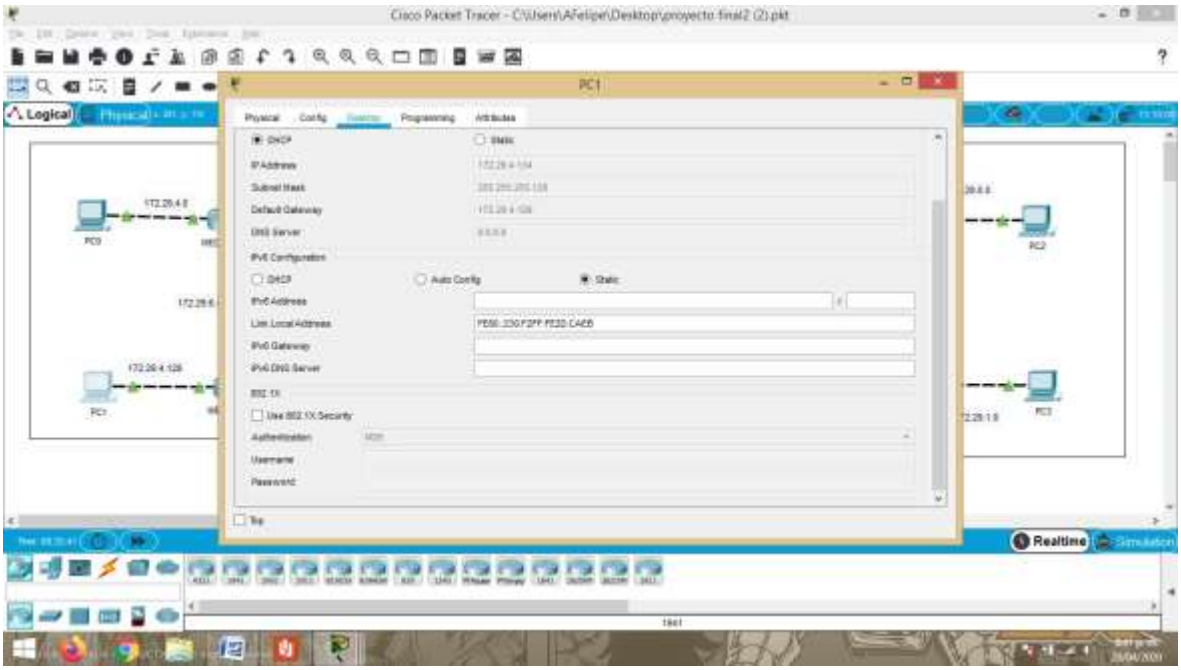


Imagen 58. DHCP pc1

c. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.
d. Configurar la red Bogotá2 y Bogotá3 donde el router BOGOTA2 debe ser el servidor DHCP para ambas redes Lan.

Bogota2

BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp pool Bog2
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(config)#ip dhcp pool Bog3
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
BOGOTA3>en

BOGOTA3#conf t

Bogota3

BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)#exit

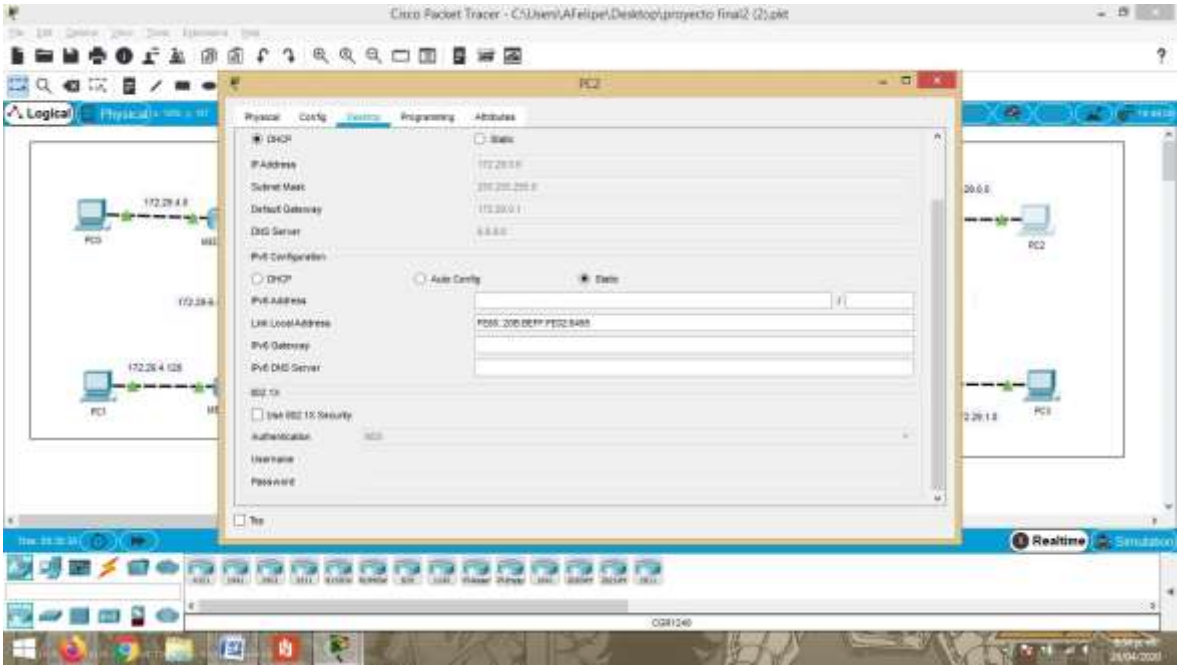


Imagen 59. DCHP en pc2

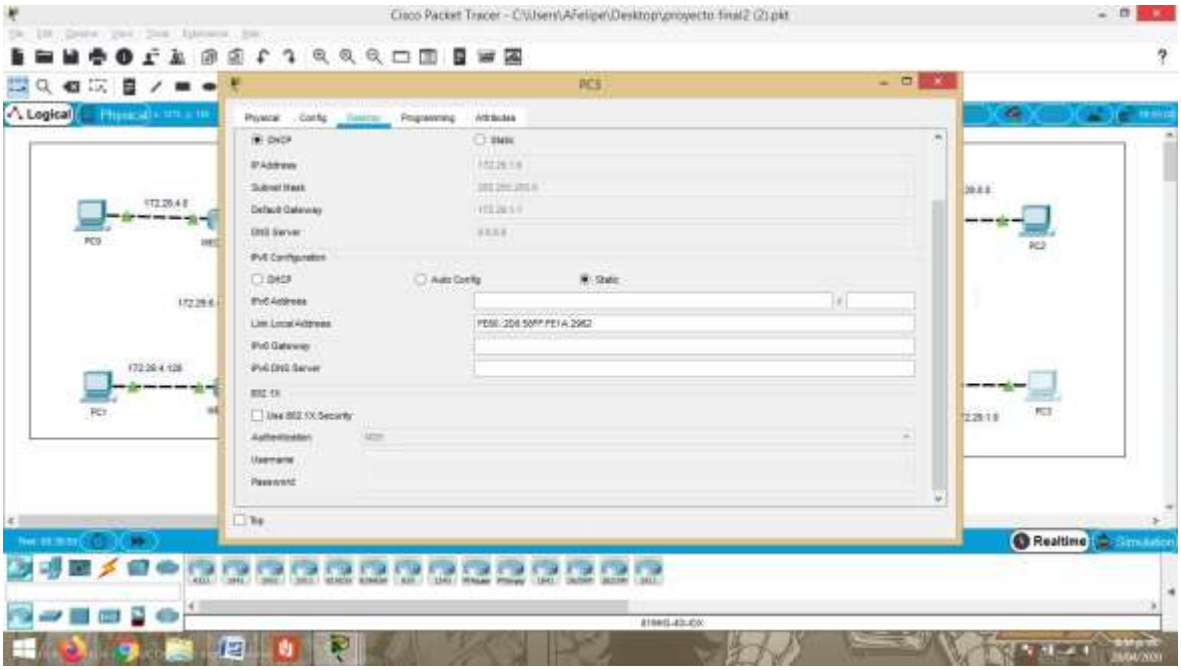


Imagen 60. DHCP en pc3

CONCLUSIONES

Realizando los ejercicios que fueron propuestos en el diplomado de Cisco logre comprender como se configura una red básica hasta una compleja, adquiriendo las habilidades suficientes para identificar que necesidades requiere una configuración de red y aplicarlas de forma adecuada. Estos elementos son fundamentales al momento de ser implementado en ambientes reales.

En el escenario uno se logró comprender la configuración de una red utilizando protocolos RIPv2, implementación de NAT, DHCP, configuración de servidor web, de internet y direccionamiento IP v4 y v6

Para el escenario dos se logró identificar el uso del protocolo OSPF1 en cada router, la implementación de PAT, enrutamiento por DHCP, encapsulamiento y autentificación PPP.

Agradezco todo lo aprendido en el diplomado de Cisco ya que los conocimientos adquirido son de gran importancia porque complementen mi perfil como ingeniero de sistemas.

BIBLIOGRAFIA

CONFIGURACIÓN Y CONCEPTOS BÁSICOS DE SWITCHINGCISCO. “Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación.” (2014). Disponible en: https://static-ourseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CONCEPTOS DE ROUTING CISCO. “Conceptos de Routing. Principios de Enrutamiento y Conmutación.” (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. “Listas de control de acceso. Principios de Enrutamiento y Conmutación.” (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. “Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación”. (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

ENRUTAMIENTO ENTRE VLANSCISCO. “Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación”. (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

ENRUTAMIENTO ESTÁTICOCISCO. “Enrutamiento Estático. Principios de Enrutamiento y Conmutación.” (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

VLANs CISCO. “Principios de Enrutamiento y Conmutación.” (2014). Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1