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

RAMSÉS CAMILO TORRES NARVÁEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
INGENIERÍA DE SISTEMAS
PASTO - NARIÑO
2020

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

RAMSÉS CAMILO TORRES NARVÁEZ

INFORME FINAL DE HABILIDADES PRACTICAS PARA OPTAR POR EL TITULO DE INGENIERO DE SISTEMAS

TUTOR: HECTOR JULIAN PARRA
MSC. DIRECCION ESTRATEGICA ESPECIALIDAD TELECOMUNICACIONES

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
INGENIERÍA DE SISTEMAS
PASTO - NARIÑO
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Pasto (18/05/2020) (18/05/2020)

Este trabajo está dedicado a todas las personas que creyeron en mí y me apoyaron en todo momento.

AGRADECIMIENTOS

Agradezco el apoyo de mi familia y a todas las personas que estuvieron a mi lado en todo este proceso para alcanzar mis metas y sueños, gracias a su constante ánimo y a brindar todas las herramientas necesarias durante toda la carrera de Ingeniería de Sistemas.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

PROTOCOLOS: Se refiere a un conjunto de patrones predestinados con el propósito de normalizar el intercambio de información en dinamismos informáticos.

RIP V2: es un protocolo de puerta de enlace interna o interior manejado por los routers o encaminadores para realizar el intercambio de información sobre las redes del Internet Protocol (IP) a las que se hallan conectados.

ACL: Son filtros de tráfico de una lista de redes y acciones ordenadas que se usan para optimizar la Seguridad. Bloquea o permite el acceso para que los usuarios accedan a los recursos específicos.

NTP: Network Time Protocol nos permite sincronizar los dispositivos que funcionan en una red. Esto es de suma importancia ya que hay una extensa variedad de servicios de red que se fundan en la correcta sincronización de horarios de los servidores.

NAT: La traducción de direcciones de red se diseñada para archivar direcciones IP. También permite que se puedan conectar a Internet las redes de IP privada que utilizan direcciones IP no registradas.

PPP: Es un protocolo WAN de enlace de datos. Se creó como un protocolo abierto para implementar a varios protocolos de capa de red, como IP, IPX y Apple Talk.

PAP: Es un protocolo simple de autenticación para legitimar un usuario contra un servidor de acceso remoto o contra un distribuidor de servicios de internet. PAP es un sub protocolo utilizado para la autenticación del protocolo PPP.

CISCO: Es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también brinda el servicio de recursos de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.

SWITCHING: Se utiliza para interconectar varios dispositivos a través de la misma red dentro de un mismo edificio.

RUTEO: Tiene como función buscar un camino entre todos los disponibles en una red de paquetes cuyas topologías poseen una diversa y extensa conectividad.

PACKET TRACER: es un programa de simulación de redes que brinda a los estudiantes realizar pruebas con el comportamiento de la red y resolver dudas.

RESUMEN

En el presente trabajo se realizó la configuración de dos escenarios, aplicando las correspondientes configuraciones iniciales, como hostname, password, encriptado, de igual manera se determinan las ip de cada una de las redes, también se establece 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. Como complemento del módulo 2 de CCNA se realiza el uso de OSPF como protocolo de enrutamiento, configurando las rutas por defecto redistribuidas; asimismo, la habilitación de encapsulamiento PPP y su autenticación con el fin de identificar las habilidades adquiridas durante el diplomado en redes cisco.

PALABRAS CLAVE: Protocolo RIP V2, ACL, NTP, NAT, PPP, PAP, CISCO, CCNA, Switching, Routeo, Mapeo, Packet Tracer.

1. INTRODUCCIÓN

Con el fin de presentar e implementar soluciones integradas en redes LAN y WAN en esta prueba de habilidades practicas se logró utilizar todos los conocimientos adquiridos durante el diplomado de redes cisco, desde el enrutamiento, parámetros de seguridad, Configuración OSPF, RIP V2, verificación de ACL y el acceso a diferentes dispositivos dentro de una red, todo con su correspondiente configuración.

De igual manera, durante el desarrollo de los escenarios planteados en la rúbrica se pretende implementar sistemas integrados de redes LAN y WAN aplicando los distintos comandos aprendidos en las actividades, lecciones, artículos y demás material brindado en los cursos del diplomado y la plataforma Cisco.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Realizar la correcta configuración de dos escenarios donde se aplicarán todos los conocimientos adquiridos durante el diplomado de redes cisco, con sus respectivos protocolos y funcionalidades.

2.2. OBJETIVOS ESPECÍFICOS

Realizar la configuración inicial en todos los dispositivos utilizados para el adecuado funcionamiento de las redes a implementar.

Identificar posibles errores que se puedan presentar durante el desarrollo de los escenarios planteados en la actividad final del diplomado.

Realizar un reporte con todos los hallazgos encontrados durante la implementación, generando capturas de pantalla evidenciando el adecuado funcionamiento.

Implementar todos los protocolos propuestos en la guía de actividades planteada para la solución de los escenarios a implementar como actividad final.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. DEFINICIÓN DEL PROBLEMA

Actualmente en las grandes empresas es de suma importancia que exista una comunicación, conexión y una administración centralizada por lo que plantear una adecuada solución integrada de redes WAN y LAN para solventar el déficit interno de comunicación se requiere la implementación de una red con unos lineamientos establecidos de enrutamiento, para resolver las necesidades presentadas en las dos sucursales de Bogotá y Medellín.

3.2. JUSTIFICACIÓN

El principal propósito es implementar una solución integrada de redes WAN y LAN con los múltiples servicios de enrutamiento, parámetros de seguridad, configuración OSPF, RIP V2, verificación de ACL y el acceso a diferentes dispositivos dentro de una red todo con su correspondiente configuración, con el fin de solventar los inconvenientes de comunicación entre las sucursales Bogotá y Medellín.

4. DESARROLLO DE LOS ESCENARIOS

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

4.1 ESCENARIO 1

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.

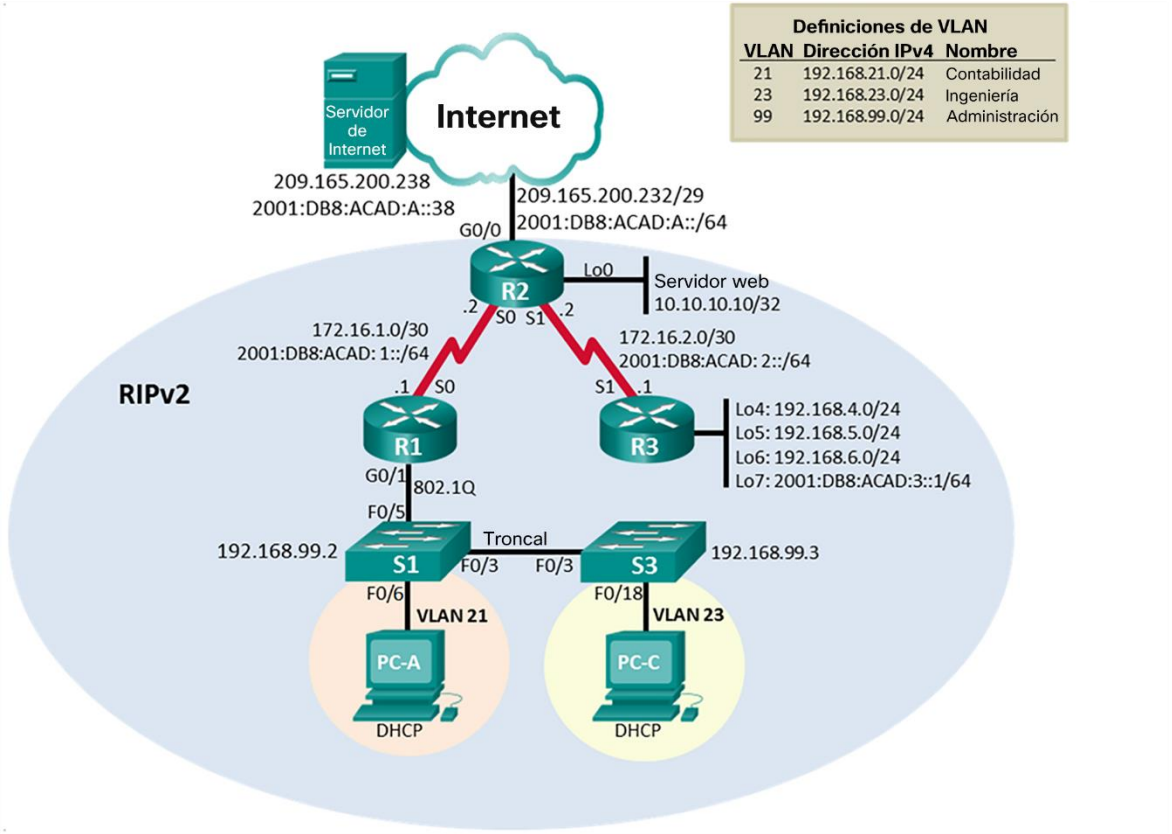


Fig. 1. Primer escenario a implementar.

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.

TAREA	**COMANDO DE IOS**
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
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#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#show flash

Tabla 1. Configuración inicial de los dispositivos

PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

PASO 1. CONFIGURAR LA COMPUTADORA DE INTERNET

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 2. Configuración del servidor de internet

PASO 2. CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	R1#configure terminal
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config-line)# Password cisco
Contraseña de acceso Telnet	R1(config-line)#linevty 0 15 R1(config-line)# Password cisco
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config-line)#banner motd %Unauthorized Access is Prohibiter%
Interfaz S0/0/0	R1(config)# int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 3. Configuración de router 1

PASO 3. CONFIGURAR R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	Packet tracer no soportado
Mensaje MOTD	R2(config)#banner motd %Unaauthorized access is prohibited%
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#description Simulador Servidor Web R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Tabla 4. Configuración Router 2

PASO 4. CONFIGURAR R3

. La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	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 address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Configuración Router 5

PASO 5. CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd %Se prohibe el acceso no autorizado%

Tabla 6. Configuración Switch 1

PASO 6. CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd %Se Prohibe el acceso no autorizado%

Tabla 7. Configuración Switch 3.

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	R1#ping 172.16.1.2	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 = 4/4/4 ms
R2	R3, S0/0/1	R2#ping 172.16.2.1	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 = 1/4/7 ms
PC de Internet	Gateway predeterminado	ping 209.165.200.233	Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233:

			Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Tabla 8. Prueba de conectividad Ping

Prueba de Ping R1 a R2 S/0/0/0

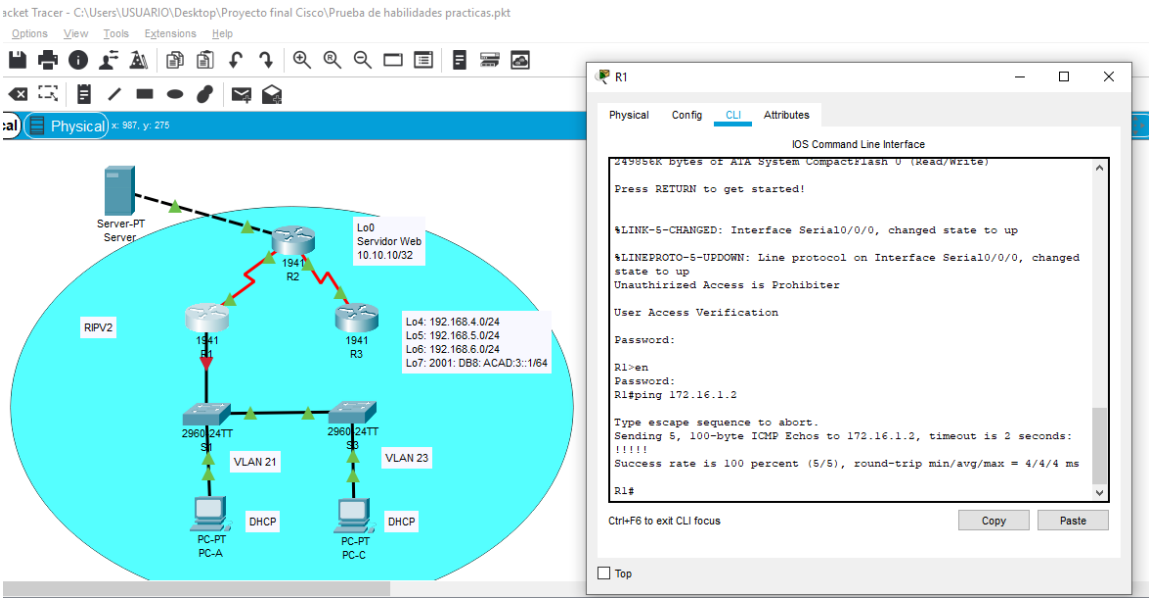


Fig. 1. Resultado del Ping Realizado entre R1 a R2

Prueba de Ping R2 a R1 S0/0/1

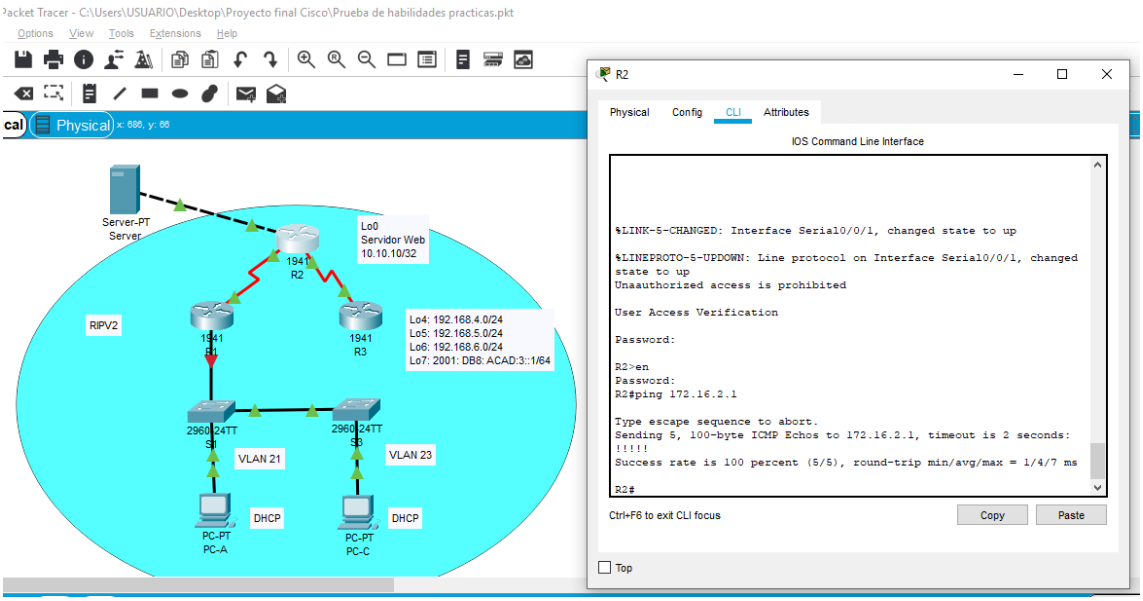


Fig. 2. Resultado del Ping realizado entre R2 y R1

Ping Pc Internet a Gateway predeterminado

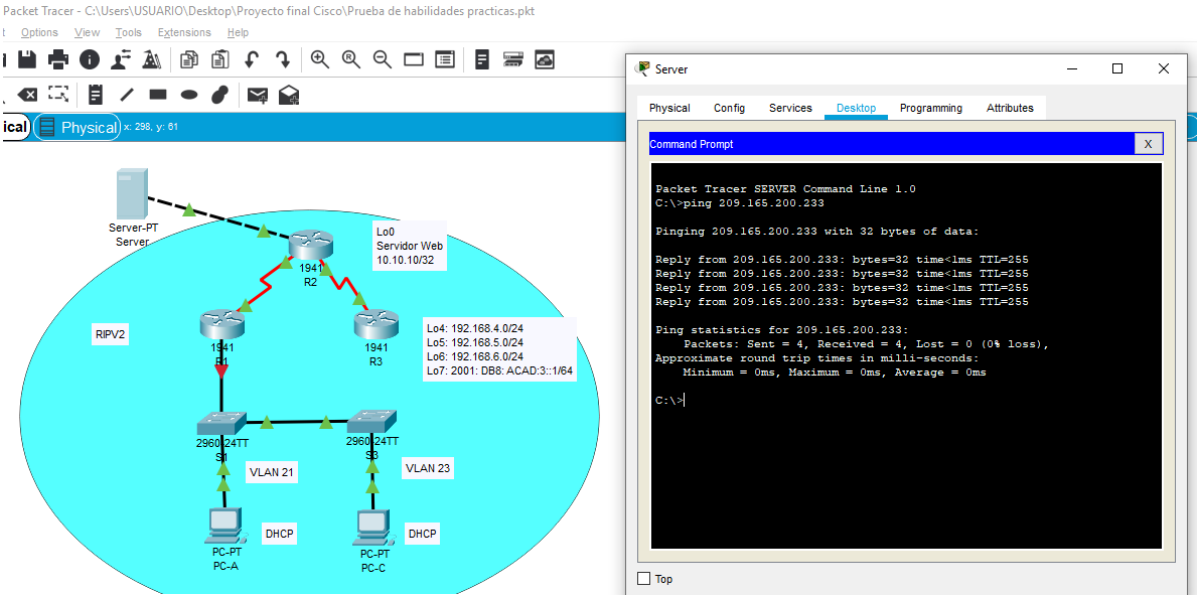


Fig. 3. Ping realizado de PC a Gateway predeterminado

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	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	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)#switch port mode access 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, f0/6-24, g0/1-2 S1(config-if-range)#switch port mode access

Tabla 9. Configuración Switch 1

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	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	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 23	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 Switch 3.

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	R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
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 address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Tabla 11. Configuración para R1

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	S1#ping 192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	S3#ping 192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	S1#ping 192.168.21.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	S3#ping 192.168.23.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Tabla 12. Verificación de conectivida de la Red.

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	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13. Configuración para Router 1

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	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 **Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14. Configuración RIP V2 en Router 2

PASO 3. CONFIGURAR RIPV2 EN EL R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
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
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
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 15. Configuración RIPV2 en Router 2

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?	R3#show ip protocols Routing Protocol is "rip" Routing for Networks: 172.16.0.0 192.168.4.0 192.168.5.0 192.168.6.0 Passive Interface(s): Loopback4 Loopback5 Loopback6
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run

Tabla 16. Verificación de la configuración RIP

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.	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

Tabla 17. Configuración para Router 1

PASO 2. CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

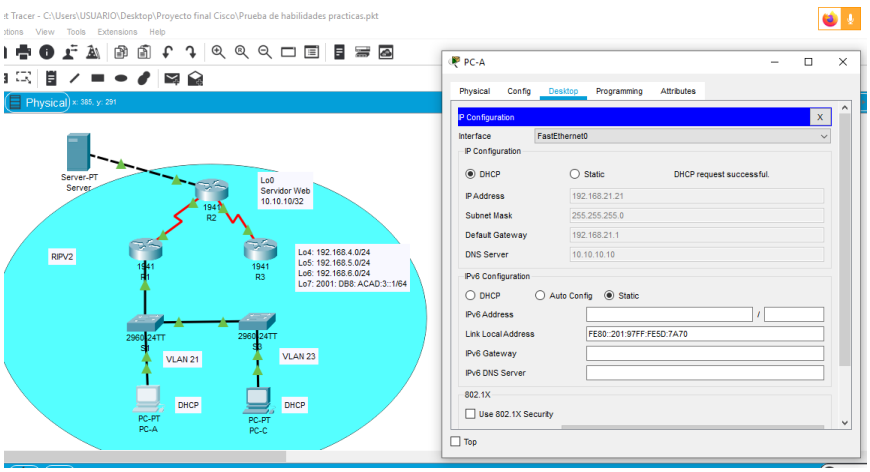
Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Packet tracer no soporta este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local Packet tracer no soporta este comando

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237** R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	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
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

Tabla 18. Configuración NAT estática y dinámica para Router 2

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	 Fig. 4. Prueba de información de IP DHCP

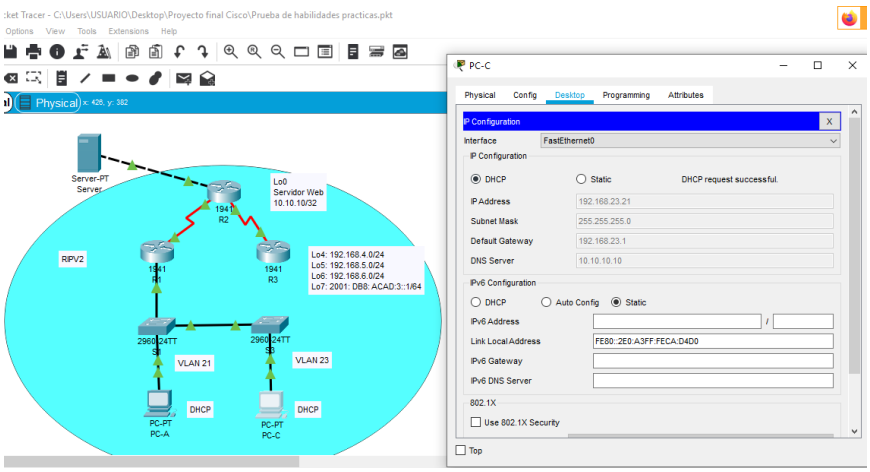
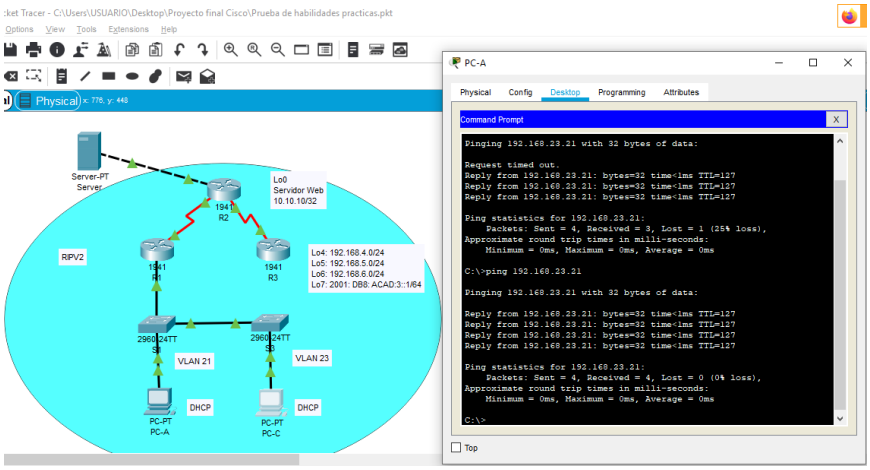
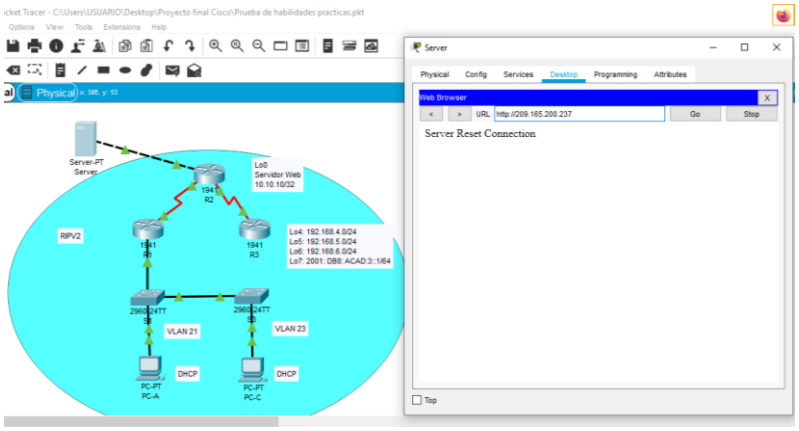
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Fig. 5. PC-C con la IP DHCP
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 Fig. 6. Ping de PC-A a PC-C
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 Fig. 7. Acceso a internet hacia el Servidor Web Packet Tracer no soporta este comando

Tabla 19. Verificación protocolo DHCP y NAT

PARTE 6. CONFIGURAR NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:00:00 5 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
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

Tabla 20. Configuración NTP para R2 y 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

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** R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-std-nacl)#permit host 172.16.1.1 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenUnaauthorized access is prohibited User Access Verification R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host

Tabla 21. Restricción de acceso en VTY para R2.

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 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
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025209.165.200.238:1025 R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- tcp 209.165.200.234:1025192.168.23.21:1025 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 * R2#show ip nat translations

Tabla 22. Comandos utilizados para el paso 2.

Acceso a internet desde PC-C

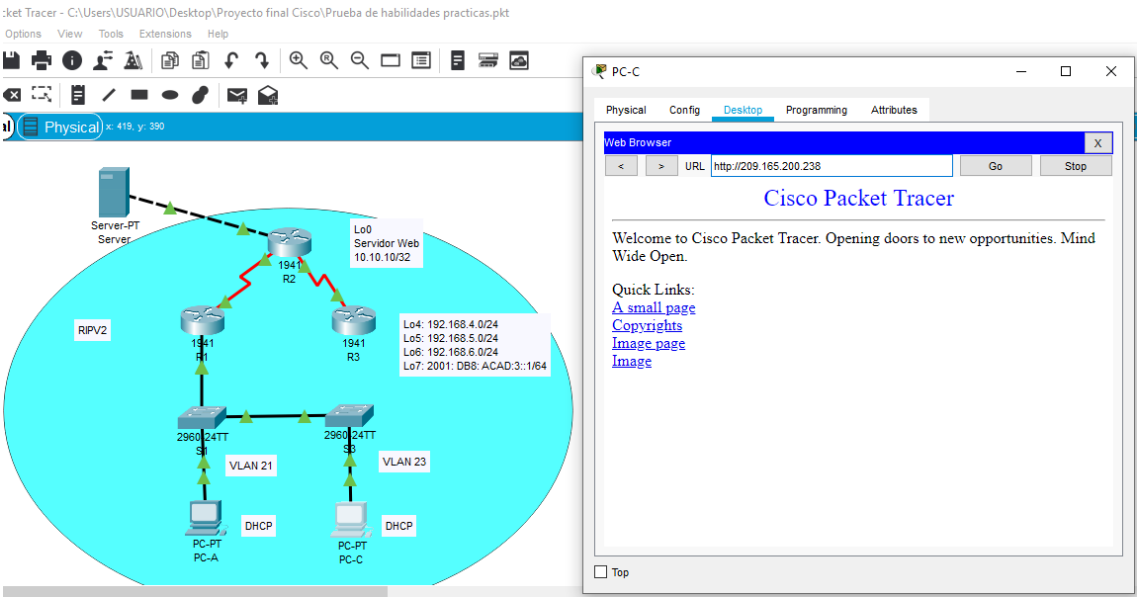


Fig. 8. Comprobación de Acceso a internet desde PC-C

Acceso a internet desde PC-A

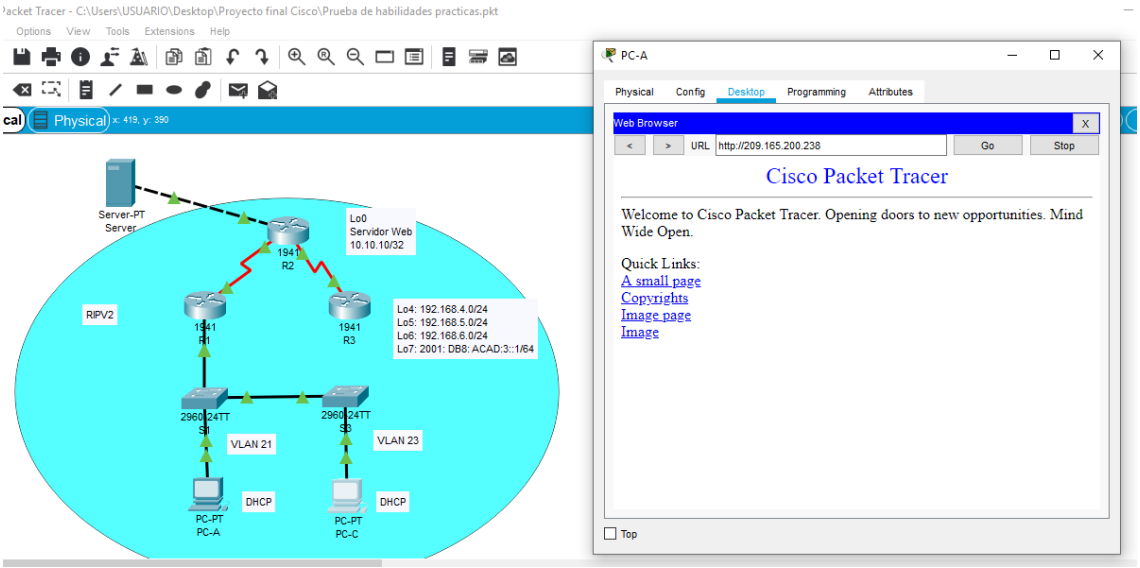


Fig. 9. Comprobación de acceso a Internet desde PC-A

4.2 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.

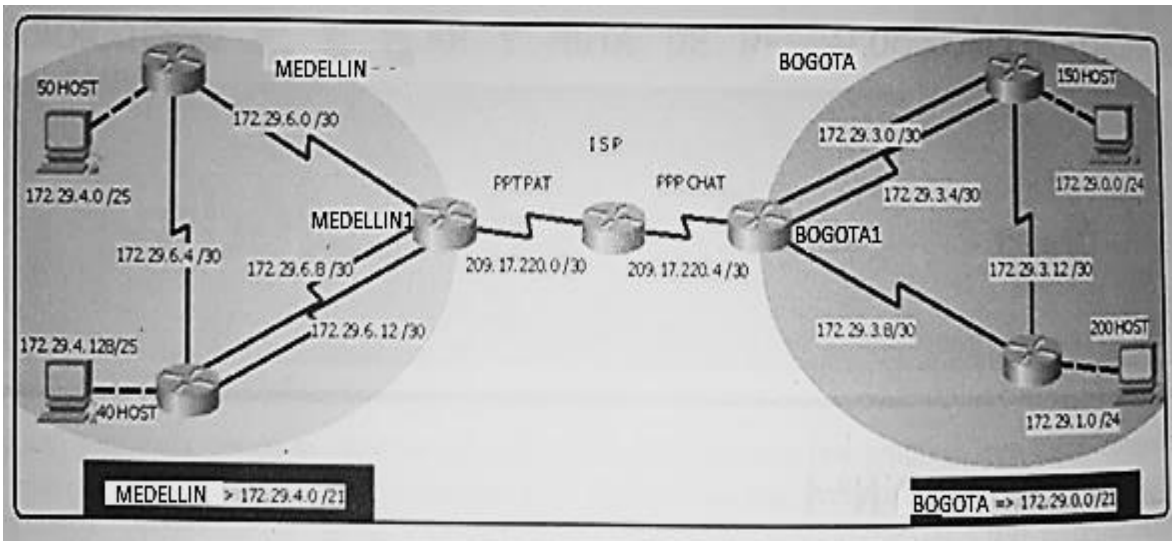


Fig.1 Diseño a realizar 2 escenario.

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán 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 física de los equipos con base en la topología de red

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

PARTE 1. CONFIGURACIÓN INICIAL

```
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#banner motd %Acceso Denegado - Ramses Torres%
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login

MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#banner motd %Acceso Denegado - Ramses Torres%
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login

MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#banner motd %Acceso Denegado - Ramses Torres%
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#

MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#banner motd %Acceso Denegado - Ramses Torres%
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
```

```
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#

BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#enable secret class
BOGOTA1(config)#banner motd %Acceso Denegado - Ramses Torres%
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login

BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#enable secret class
BOGOTA2(config)#banner motd %Acceso Denegado - Ramses Torres%
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login

BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#banner motd %Acceso Denegado - Ramses Torres%
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
```

PARTE 2. CONFIGURACIÓN DEL ENRUTAMIENTO

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

Comandos en ISP:

Router(config)#hostname ISP

ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

ISP(config-if)#int s0/0/1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

b. Los routers Bogota1 y Medellín1 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.

PASO 1. COMANDOS EJECUTADOS EN EL ROUTER MEDELLIN1:

MEDELLIN1(config)#interface s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown

MEDELLIN1 (config-if)#int s0/0/1
MEDELLIN1 (config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1 (config-if)#clock rate 4000000
MEDELLIN1 (config-if)#no shutdown

MEDELLIN1 (config-if)#int s0/1/0
MEDELLIN1 (config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1 (config-if)#clock rate 4000000
MEDELLIN1 (config-if)#no shutdown

MEDELLIN1 (config-if)#int s0/1/1
MEDELLIN1 (config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1 (config-if)#clock rate 4000000
MEDELLIN1 (config-if)#no shutdown

PASO 2. COMANDOS EJECUTADOS EN EL ROUTER MEDELLIN2:

```
MEDELLIN2 (config)#int s0/0/0
MEDELLIN2 (config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2 (config-if)#no shutdown

MEDELLIN2 (config-if)#int s0/0/1
MEDELLIN2 (config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2 (config-if)#clock rate 4000000
MEDELLIN2 (config-if)#no shutdown

MEDELLIN2 (config-if)#int g0/0
MEDELLIN2 (config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2 (config-if)#no shutdown
```

PASO 3. COMANDOS EJECUTADOS EN EL ROUTER MEDELLIN 3:

```
MEDELLIN3 (config)#int s0/0/0
MEDELLIN3 (config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3 (config-if)#no shutdown

MEDELLIN3 (config-if)#int s0/0/1
MEDELLIN3 (config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3 (config-if)#no shutdown

MEDELLIN3 (config-if)#int s0/1/0
MEDELLIN3 (config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3 (config-if)#no shutdown

MEDELLIN3 (config-if)#int g0/0
MEDELLIN3 (config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3 (config-if)#no shutdown
```

PASO 4. COMANDOS EJECUTADOS EN EL ROUTER BOGOTA1:

```
BOGOTA1 (config)#int s0/0/0
BOGOTA1 (config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1 (config-if)#no shutdown

BOGOTA1 (config-if)#int s0/0/1
BOGOTA1 (config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1 (config-if)#clock rate 4000000
BOGOTA1 (config-if)#no shutdown
```

```
BOGOTA1 (config-if)#int s0/1/0
BOGOTA1 (config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1 (config-if)#clock rate 4000000
BOGOTA1 (config-if)#no shutdown

BOGOTA1 (config-if)#int s0/1/1
BOGOTA1 (config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1 (config-if)#clock rate 4000000
BOGOTA1 (config-if)#no shutdown
```

PASO 5. COMANDOS EJECUTADOS EN EL ROUTER BOGOTA2:

```
BOGOTA2 (config)#int s0/0/0
BOGOTA2 (config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2 (config-if)#no shutdown

BOGOTA2 (config-if)#int s0/0/1
BOGOTA2 (config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2 (config-if)#clock rate 4000000
BOGOTA2 (config-if)#no shutdown

BOGOTA2 (config-if)#int g0/0
BOGOTA2 (config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2 (config-if)#no shutdown
```

PASO 6. COMANDOS EJECUTADOS EN EL ROUTER BOGOTA3:

```
BOGOTA3 (config)#int s0/0/0
BOGOTA3 (config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3 (config-if)#no shutdown

BOGOTA3 (config-if)#int s0/0/1
BOGOTA3 (config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3 (config-if)#no shutdown

BOGOTA3 (config-if)#int g0/0
BOGOTA3 (config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3 (config-if)#no shutdown

BOGOTA3(config)#int s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

PASO 7. CONFIGURACIÓN DE PROTOCOL RIP ROUTER MEDELLIN1

MEDELLIN1(config)#router rip
MEDELLIN1 (config-router)#version 2
MEDELLIN1 (config-router)#no au
MEDELLIN1 (config-router)#no auto-summary
MEDELLIN1 (config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0

MEDELLIN1 (config-router)#network 172.29.6.0
MEDELLIN1 (config-router)#network 172.29.6.8
MEDELLIN1 (config-router)#network 172.29.6.12
MEDELLIN1 (config-router)#passive-interface s0/0/0

PASO 8. CONFIGURACIÓN DE PROTOCOL RIP ROUTER MEDELLIN2

MEDELLIN2(config)#router rip
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#no auto-summary
MEDELLIN2(config-router)#do show ip route connected

C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1

MEDELLIN2(config-router)#network 172.29.4.0
MEDELLIN2(config-router)#network 172.29.6.0
MEDELLIN2(config-router)#network 172.29.6.4
MEDELLIN2(config-router)#passive-interface g0/0

PASO 9. CONFIGURACIÓN DE PROTOCOL RIP ROUTER MEDELLIN3

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#do show ip route connected

C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1

Router(config-router)#network 172.29.4.128
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#passive-interface g0/0

PASO 10. CONFIGURACION DE PROTOCOLO RIP ROUTER BOGOTA 1

BOGOTA1(config)#router rip
BOGOTA1 (config-router)#version 2
BOGOTA1 (config-router)#no au
BOGOTA1 (config-router)#no auto-summary
BOGOTA1 (config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0

BOGOTA1 (config-router)#network 172.29.3.0
BOGOTA1 (config-router)#network 172.29.3.4
BOGOTA1 (config-router)#network 172.29.3.8
BOGOTA1 (config-router)#passive-interface s0/0/0

PASO 11. CONFIGURACION DE PROTOCOLO RIP ROUTER BOGOTA 2

BOGOTA2(config)#router rip
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#no auto-summary
BOGOTA2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1

BOGOTA2(config-router)#network 172.29.1.0
BOGOTA2(config-router)#network 172.29.3.8
BOGOTA2(config-router)#network 172.29.3.12
BOGOTA2(config-router)#passive-interface g0/0

PASO 12. CONFIGURACION DE PROTOCOLO RIP ROUTER BOGOTA 3

BOGOTA3(config-if)#router rip
BOGOTA3(config-router)#version 2
BOGOTA3(config-router)#no auto-summary
BOGOTA3(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0

BOGOTA3(config-router)#network 172.29.0.0
BOGOTA3(config-router)#network 172.29.3.0
BOGOTA3(config-router)#network 172.29.3.4
BOGOTA3(config-router)#network 172.29.3.12
BOGOTA3(config-router)#passive-interface g0/0

Se Ejecuta el comando show ip route para verificar las redes asignadas

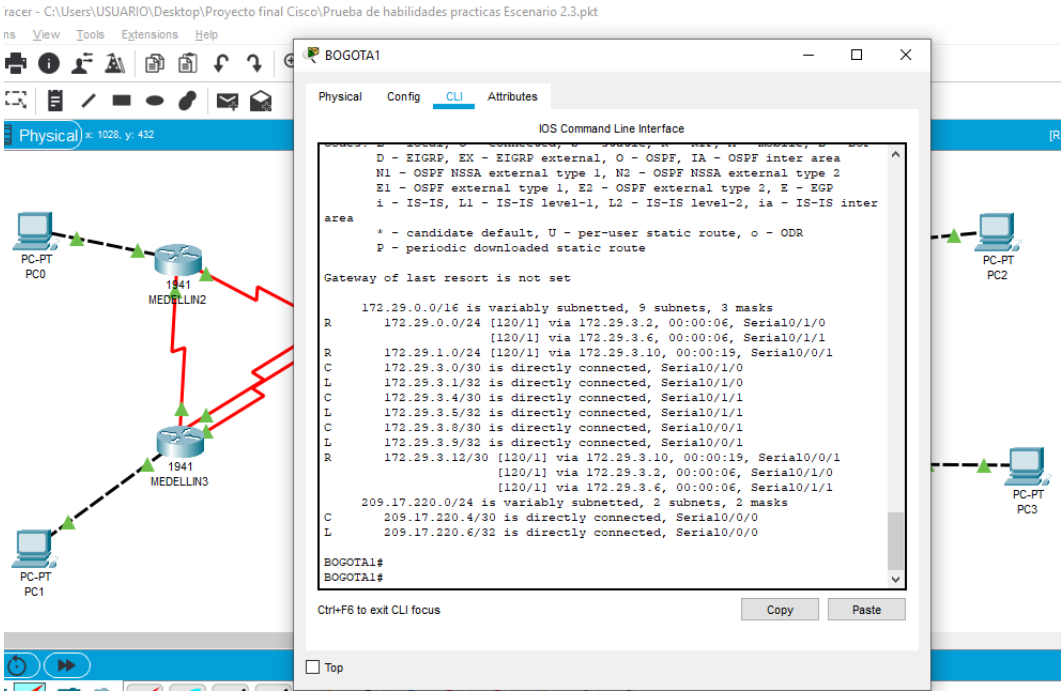


Fig. 10. Verificación de Redes Asignadas en BOGOTA1.

Se Ejecuta el comando show ip route para verificar las redes asignadas

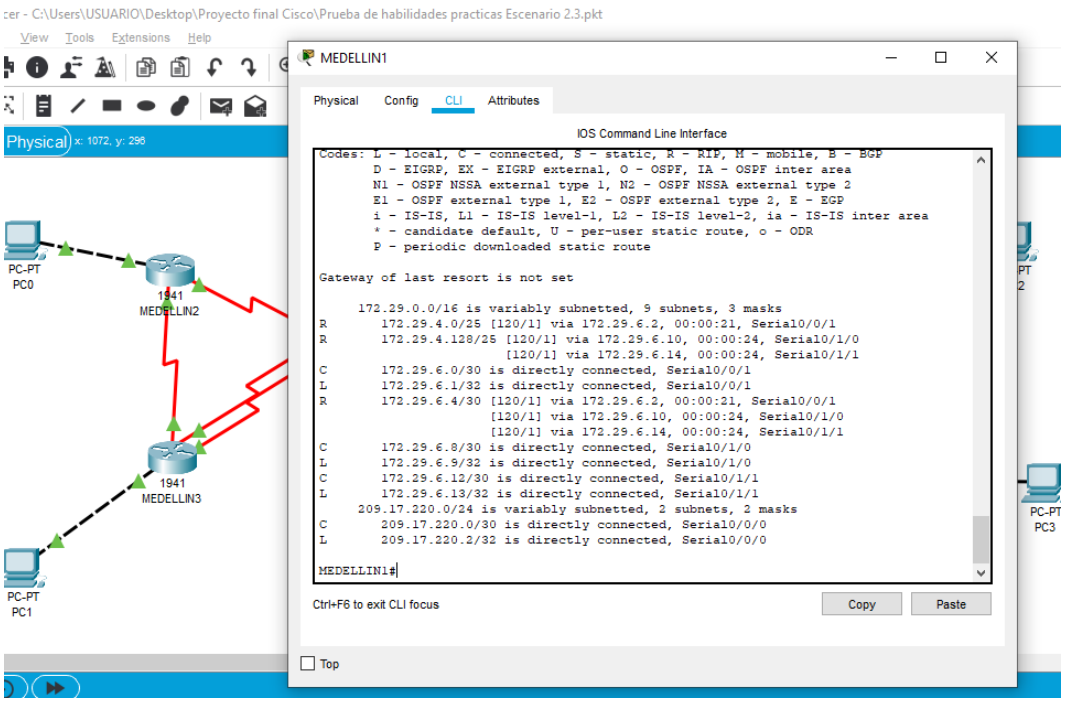


Fig. 11. Verificación de redes asignadas en MEDELLIN1.

Se Ejecuta el comando Show Run y visualizar la red principal

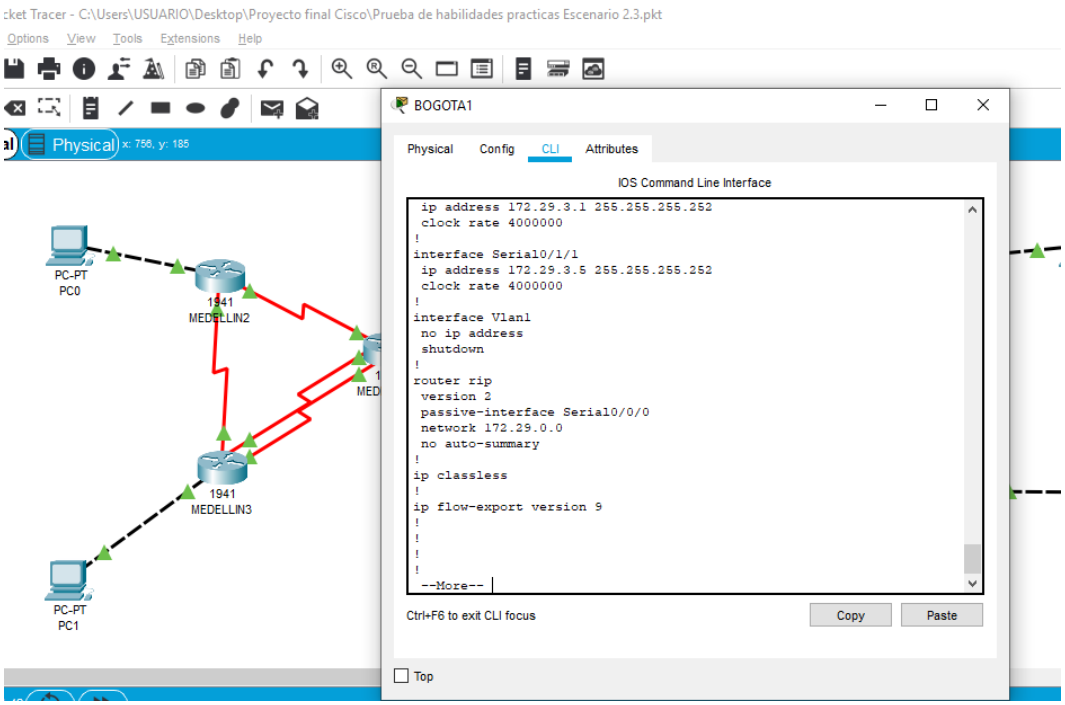


Fig. 12. Comprobación de configuración de Red Principal en Bogota1.

ROUTER MEDELLIN1

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#route rip
MEDELLIN1(config-router)#default-information originate

Se verifica en MEDELLIN2 con el commando show ip route

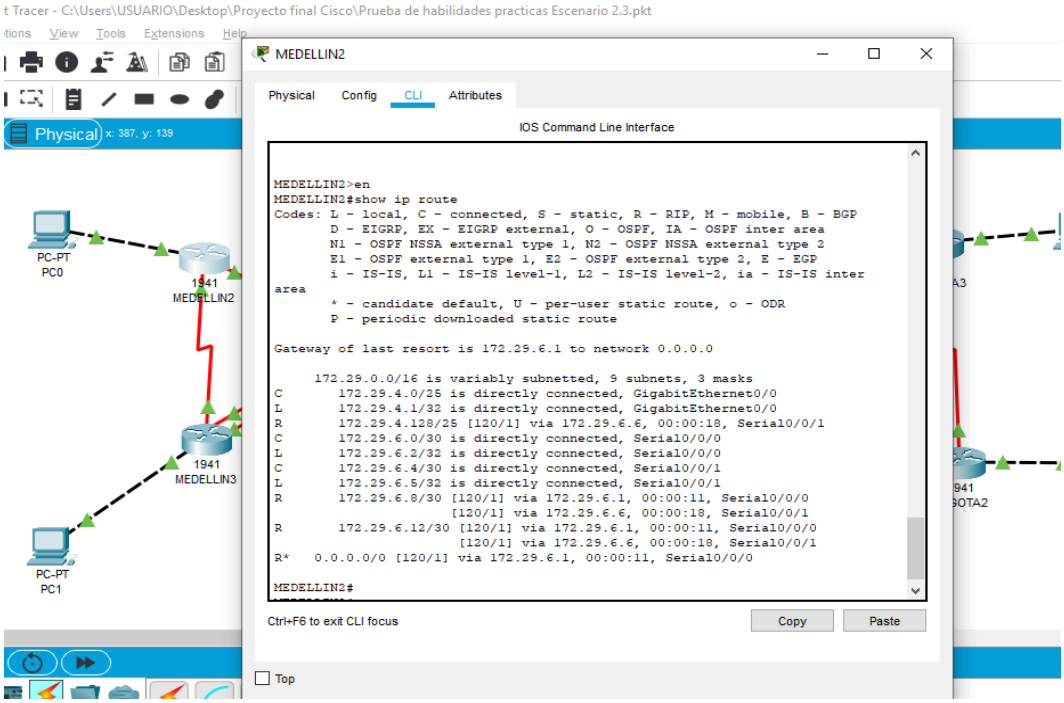


Fig. 13. Comprobación de configuración Default en MEDELLIN2.

ROUTER BOGOTA 1

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router rip
BOGOTA1(config-router)#default-information originate

Se verifica en BOGOTA2 con el commando show ip route

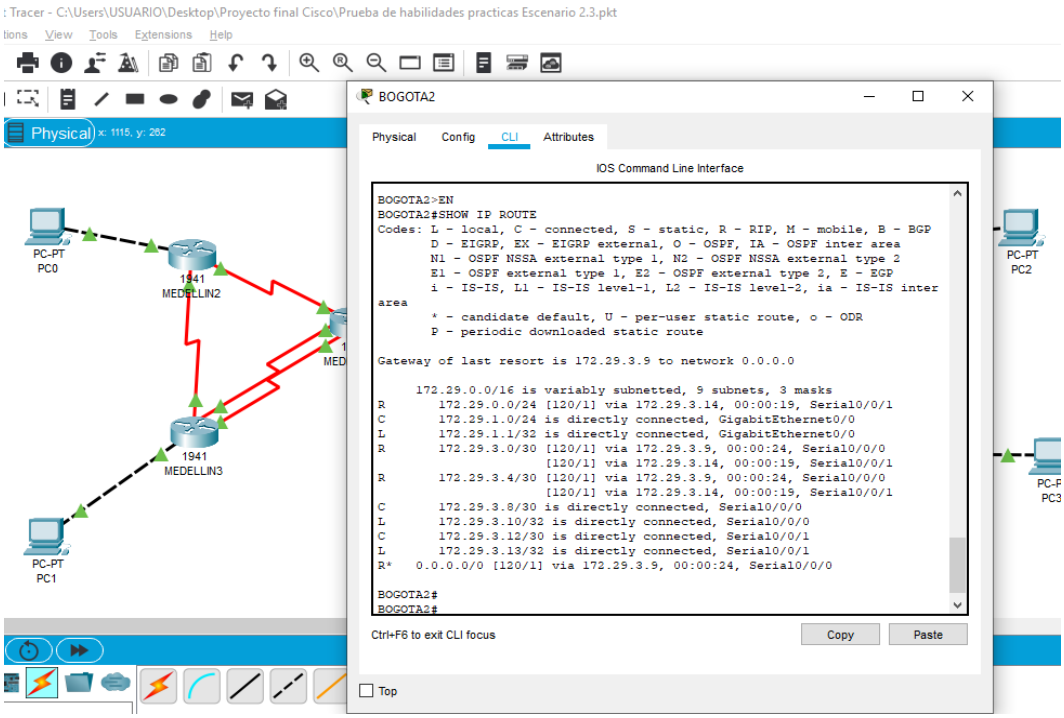


Fig. 14. Comprobación de configuración Default en BOGOTA2

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.

Tabla 23. Sumarización de Subredes Medellín.

MEDELLIN	172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	172.29.4.0/25
	172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	172.29.4.128/25
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	172.29.6.4/30
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	172.29.6.8/30
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	172.29.6.12/30
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	172.29.6.0/30
	172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	172.29.4.0/22

Tabla 24. Sumarización de Subredes Bogotá

BOGOTÁ	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	172.29.0.0/24
	172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	172.29.1.0/24
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	172.29.3.12/30
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	172.29.3.8/30
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	172.29.3.0/30
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	172.29.3.4/30
	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	172.29.0.0/22

En el router ISP ejecutamos los siguientes comandos para definir la conexión con las redes Bogota y Medellin

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

PARTE 3. TABLA DE ENRUTAMIENTO.

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

Realizamos las pruebas de Ping

En la siguiente imagen se observa el enrutamiento de BOGOTA3 A BOGOTA1

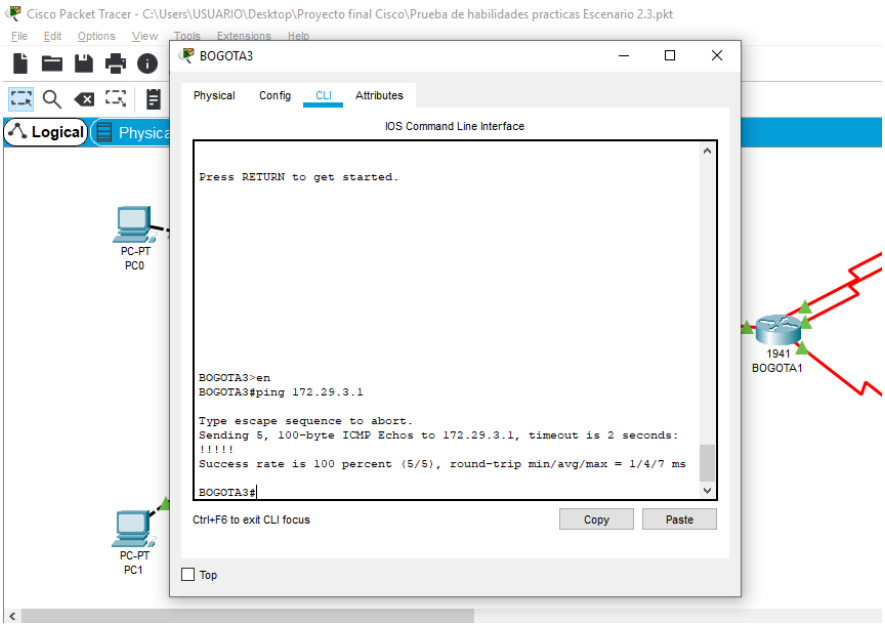


Fig. 15. Verificación de Enrutamiento desde BOGOTA 3 A BOGOTA1

En la siguiente imagen se observa el enrutamiento de BOGOTA3 A ISP

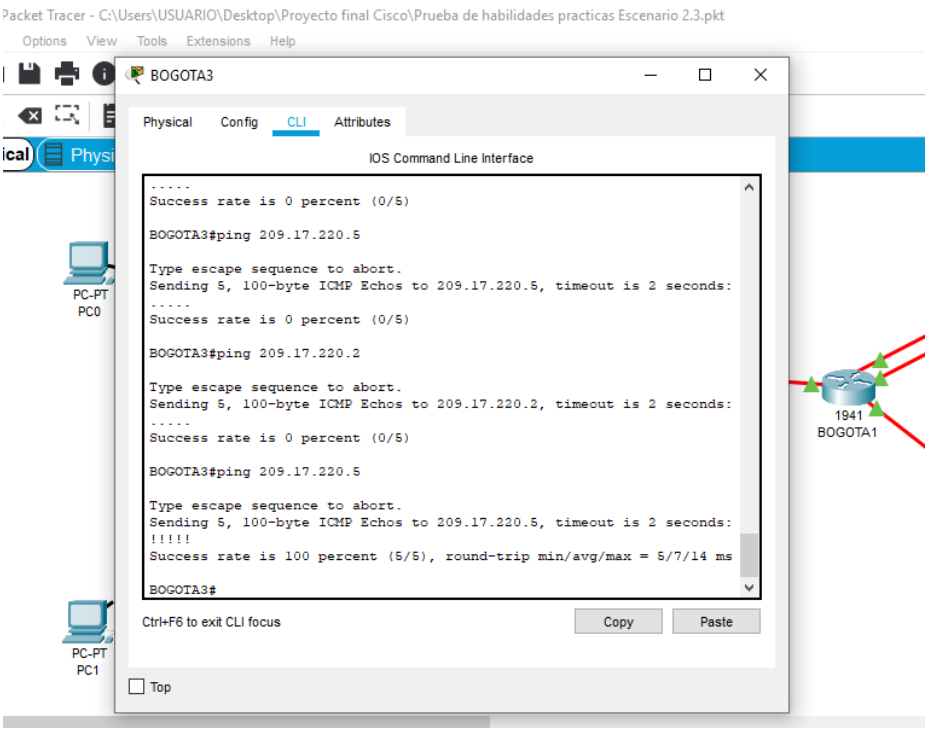


Fig. 16. Verificación de enrutamiento desde BOGOTA3 a ISP.

En la siguiente imagen se observa el enrutamiento de BOGOTA 3 A MEDELLIN 1

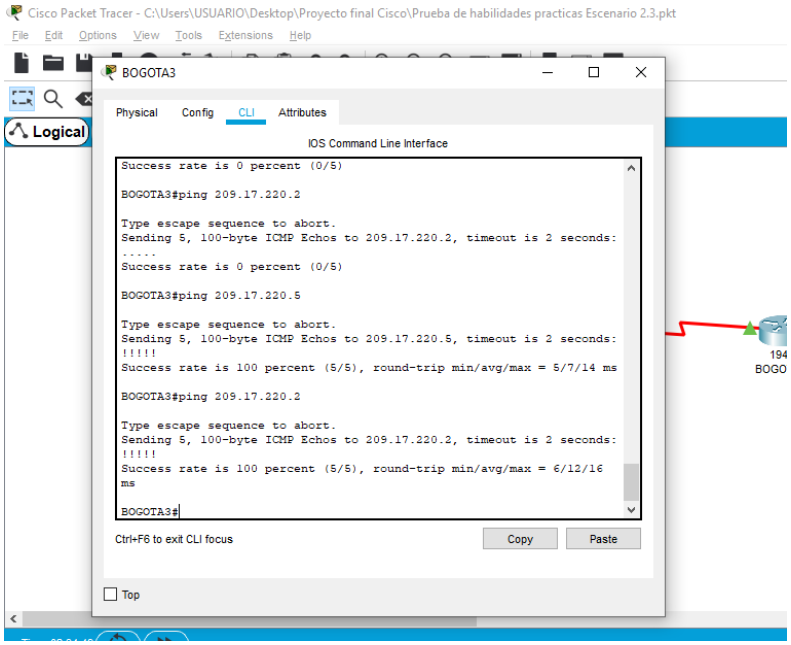


Fig. 17. Verificación de enrutamiento desde BOGOTA3 A MEDELLIN1.

En la siguiente imagen se observa el enrutamiento de BOGOTA 3 A MEDELLIN 2

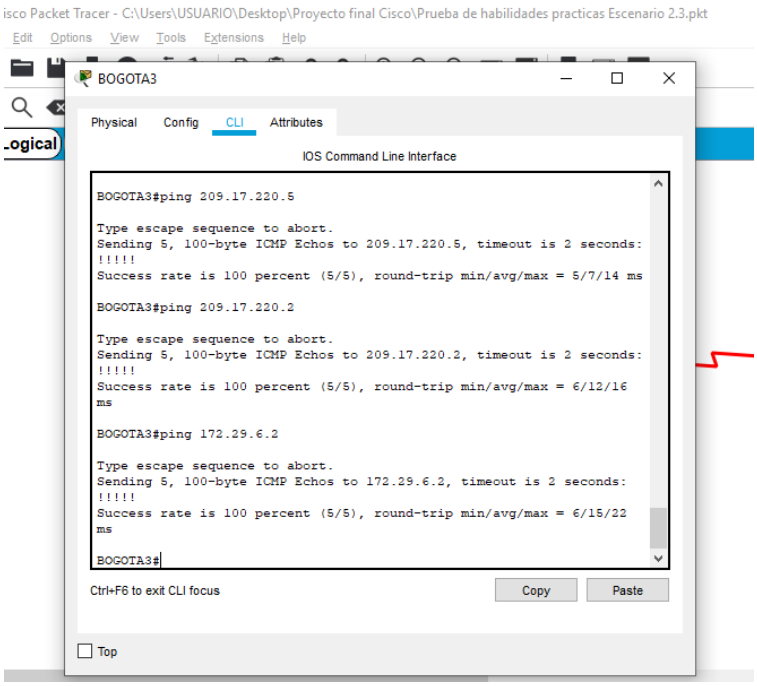


Fig. 18. Verificación de enrutamiento desde BOGOTA3 A MEDELLIN2.

b. Verificar el balanceo de carga que presentan los routers.
Observamos en los Routers MEDELLIN 3 Y BOGOTA 3 que la carga se distribuye conforme los accesos que tiene disponibles como se puede observar con el comando show ip route

Balanceo de cargas en MEDELLIN 3

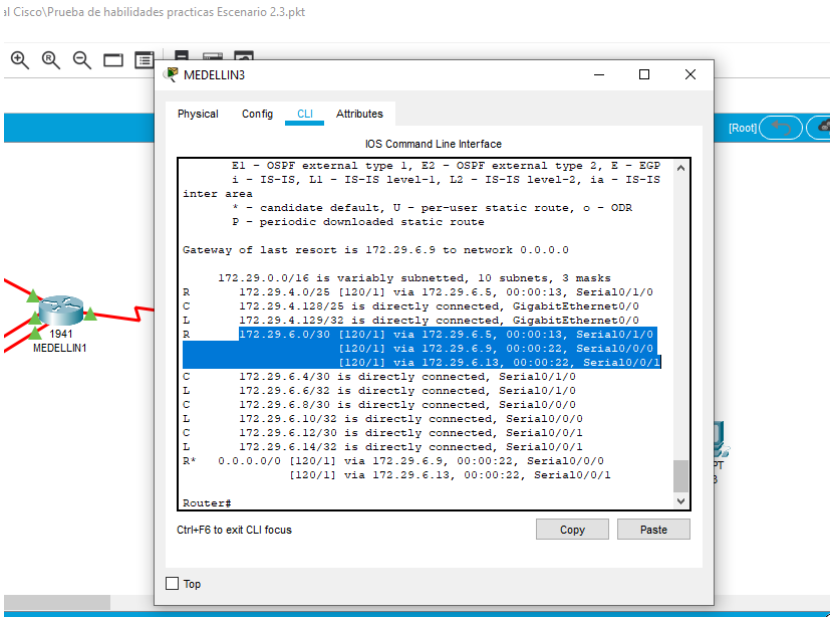


Fig. 19. Balanceo de Carga en MEDELLIN3.

Balanceo de cargas en BOGOTA 3

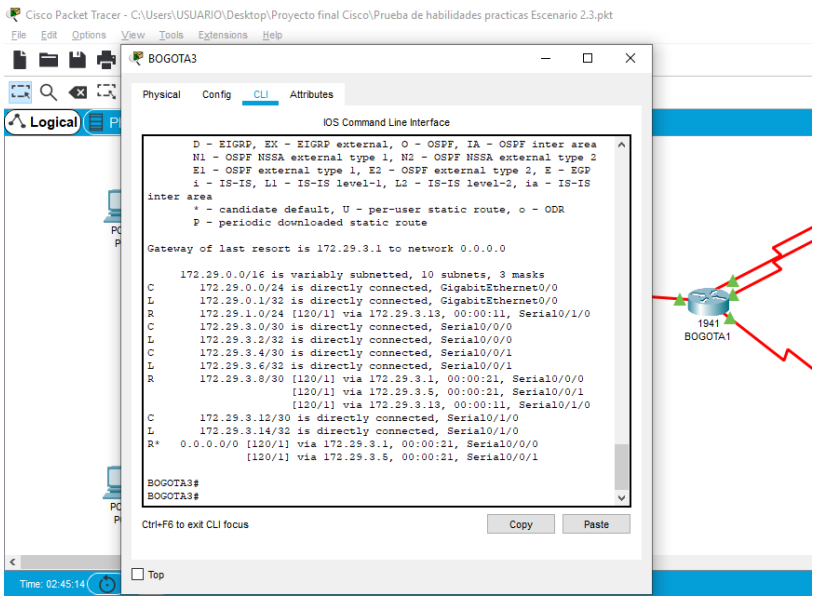


Fig. 20. Balanceo de Carga en BOGOTA3

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.

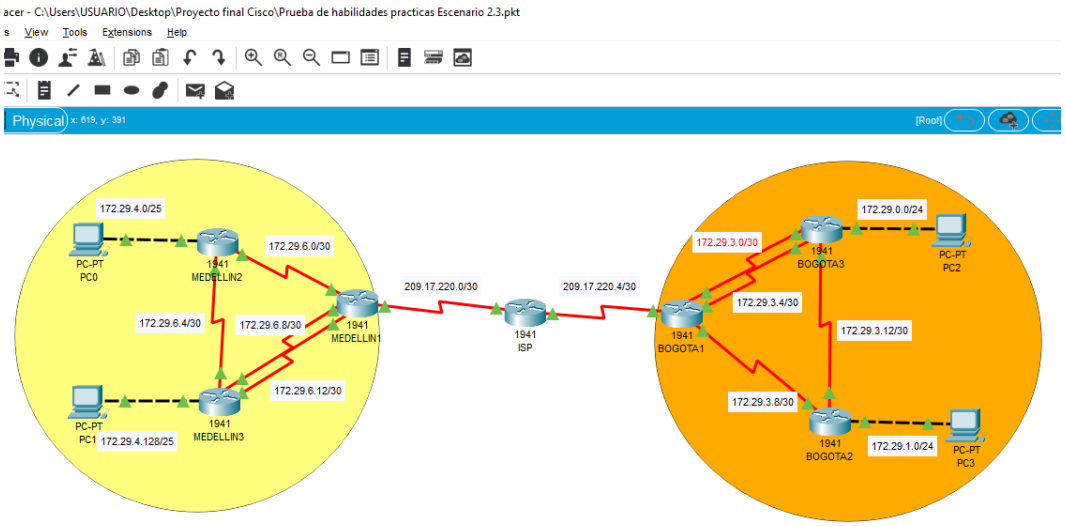


Fig. 21. Similitud en configuración de Router BOGOTA Y MEDELLIN.

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

Se Verifica con el comando Show IP Route en MEDELLIN2

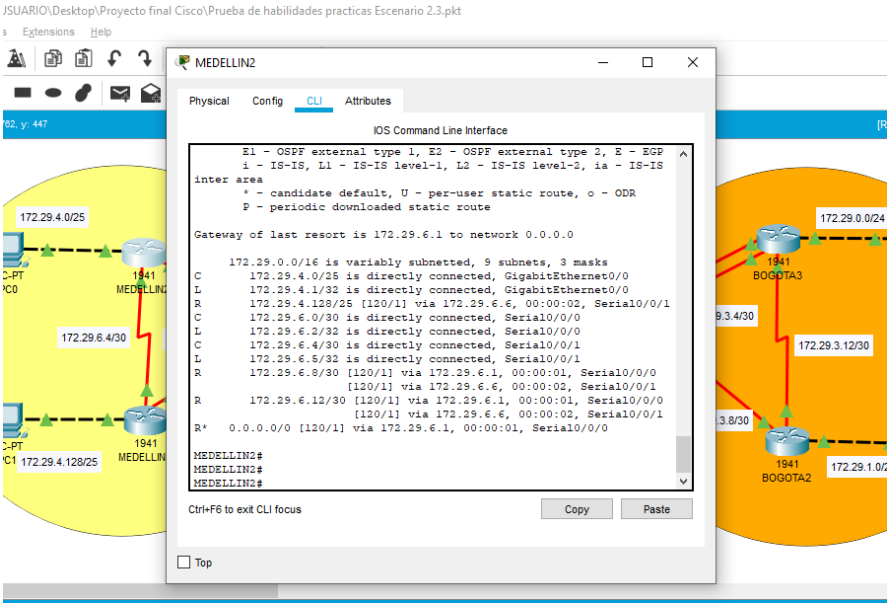


Fig. 22. Verificación de conexión de redes en MEDELLIN2.

Se Verifica con el comando Show IP Route en BOGOTA2

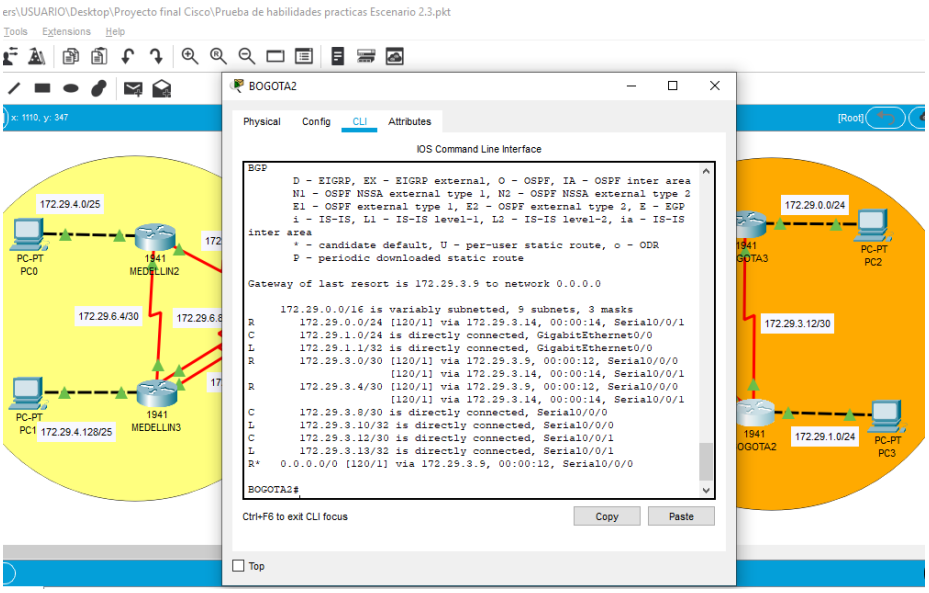


Fig. 23. Verificación de conexión de redes en BOGOTA2.

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

Se Visualiza en BOGOTA 3 con el comando show ip route

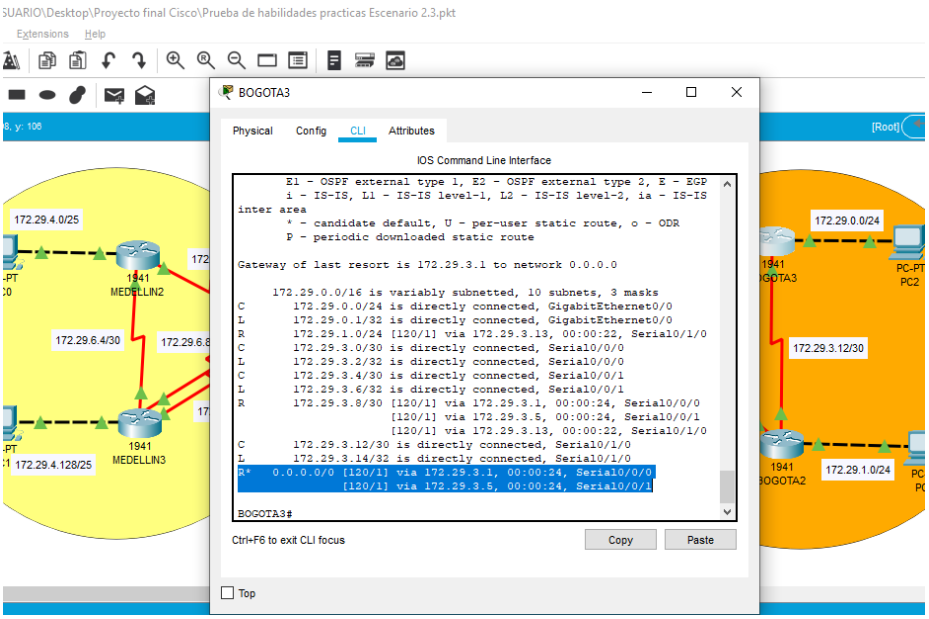


Fig. 24. Tablas de Router con rutas redundantes en BOGOTA3.

Se Verifica en MEDELLIN 3 con el comando Show ip route

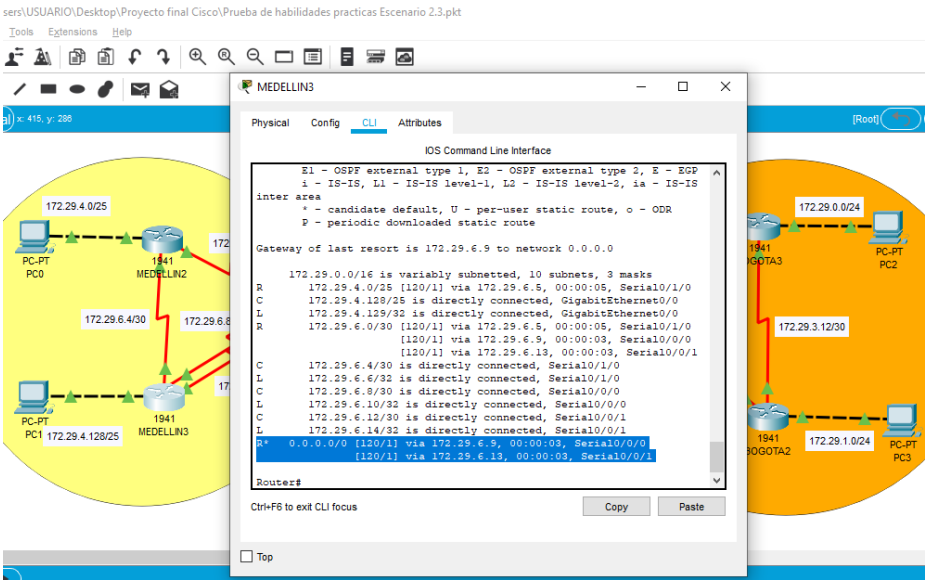


Fig. 25. Tablas de Router con rutas redundantes en MEDELLIN3.

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

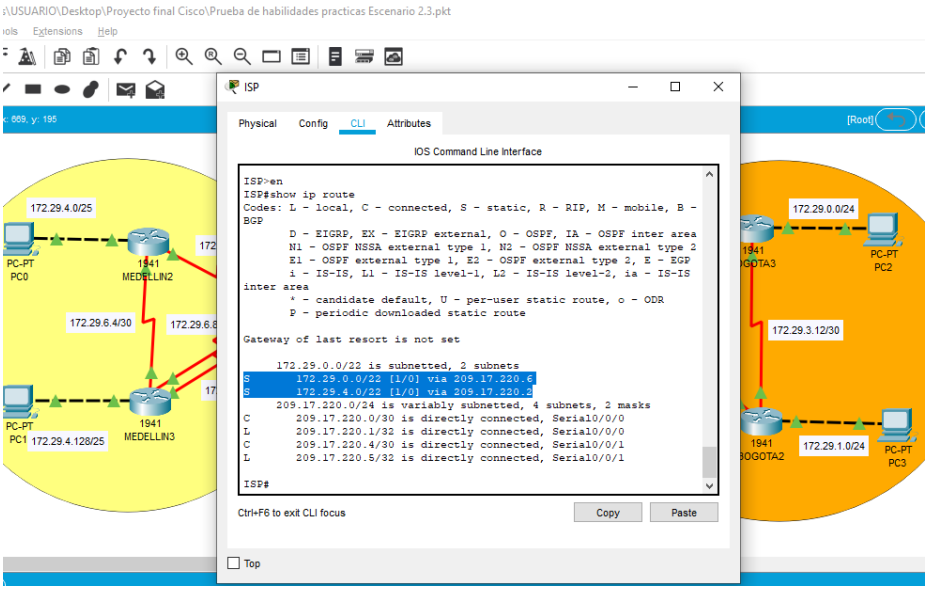


Fig. 26. Rutas estáticas en ISP.

PARTE 4. 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

Fig. 27. Tabla para deshabilitar propagación del protocolo OSPF.

Configuración para evitar la propagación del protocolo OSPF.

```
BOGOTA1(config-router)#passive-interface s0/0/0
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1(config-router)#passive-interface s0/0/0
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#passive-interface g0/0
```

PARTE 5. 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/ La configuración se puede evidenciar en los primeros pasos donde se realizaron los correspondientes comandos para los routers

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.

R/ La configuración se puede evidenciar en los primeros pasos donde se realizaron los correspondientes comandos para los routers

PARTE 6. CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP passw
ISP(config-if)#ppp pap sent-username ISP password cisco

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

Verificamos la configuración hacienda Ping entre los dos extremos

Ping desde MEDELLIN1 a ISP

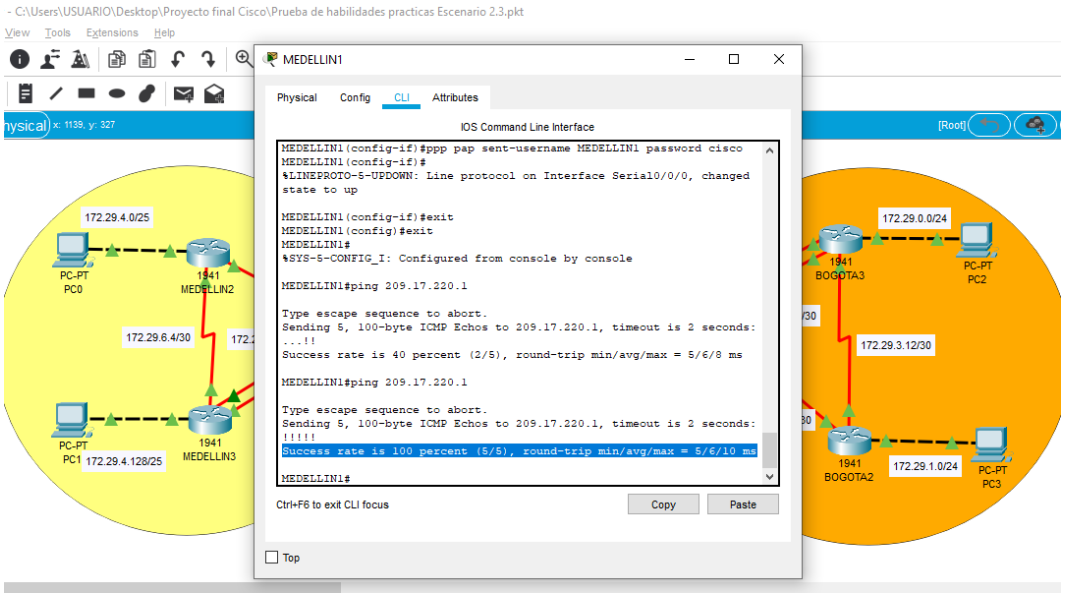


Fig. 28. Verificación de conexión entre MEDELLIN1 a ISP

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

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

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

Verificamos la configuración realizada hacienda Ping desde ISP a MEDELLIN1

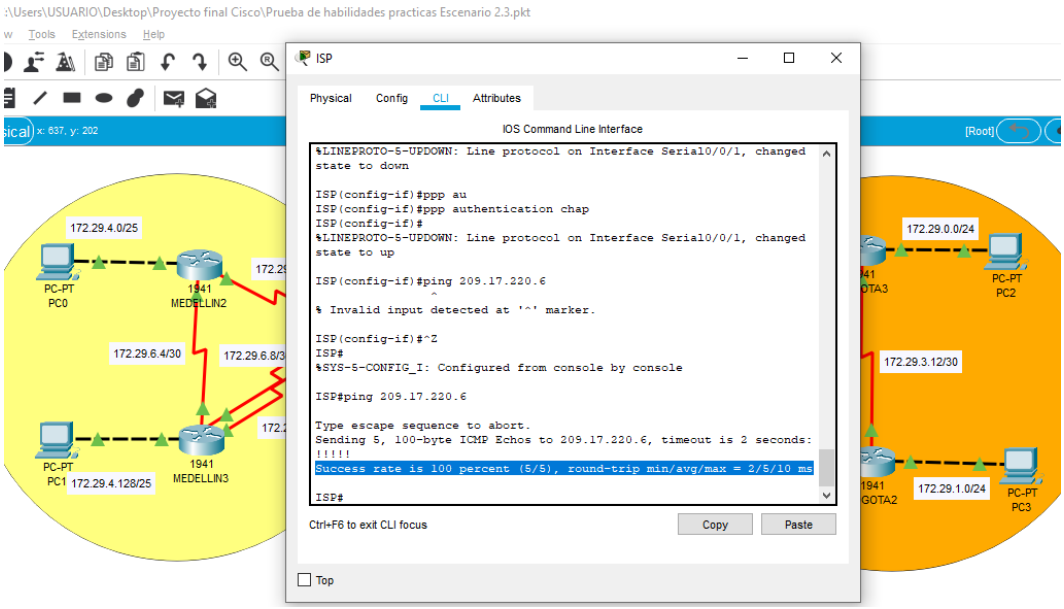


Fig. 29. Verificación de Conexión entre ISP y MEDELLIN1.

PARTE 7. 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.

```
MEDELLIN1#ping 209.17.220.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (0/5), round-trip min/avg/max = 2/4/8
ms
```

Fig. 30. El ping falla desde MEDELLIN1 a BOGOTA1

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.

Configuración NAT para Router MEDELLIN1 y BOGOTA1

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

BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
```

BOGOTA1(config-if)#ip nat inside

Realizamos Ping desde PC2 a ISP

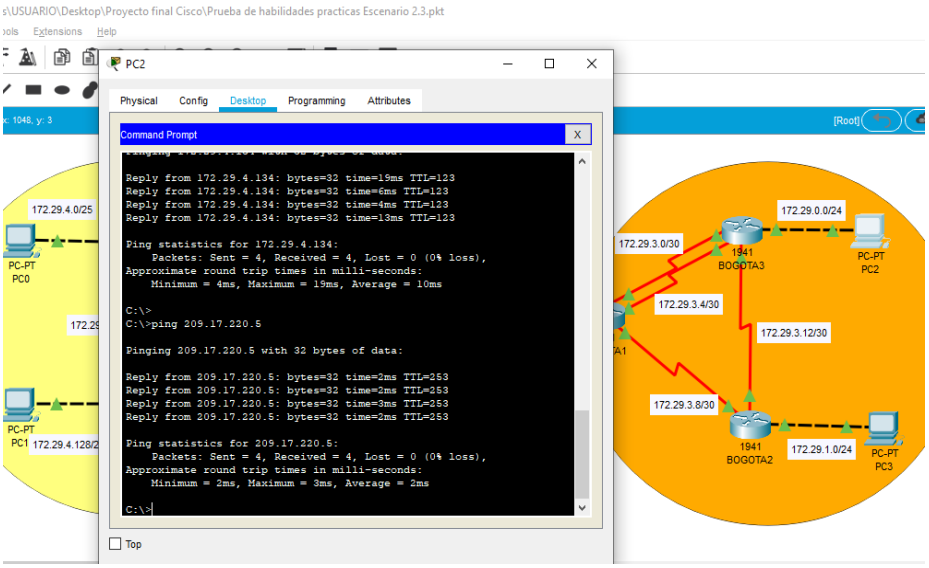


Fig. 31. Prueba de conectividad desde PC2 a ISP

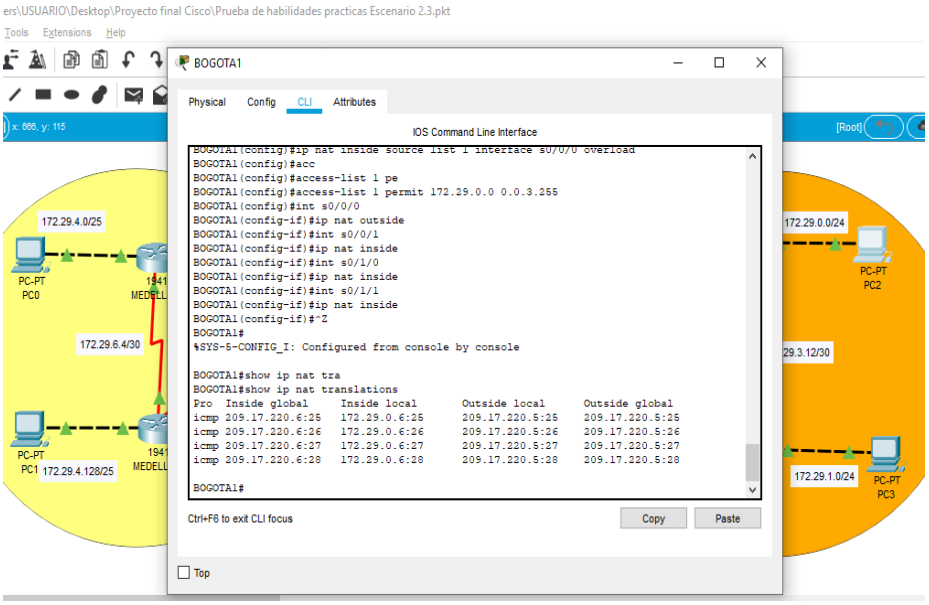


Fig. 32. Verificación de la Tabla de traducción en BOGOTA1.

Realizamos Ping de PC0 a ISP

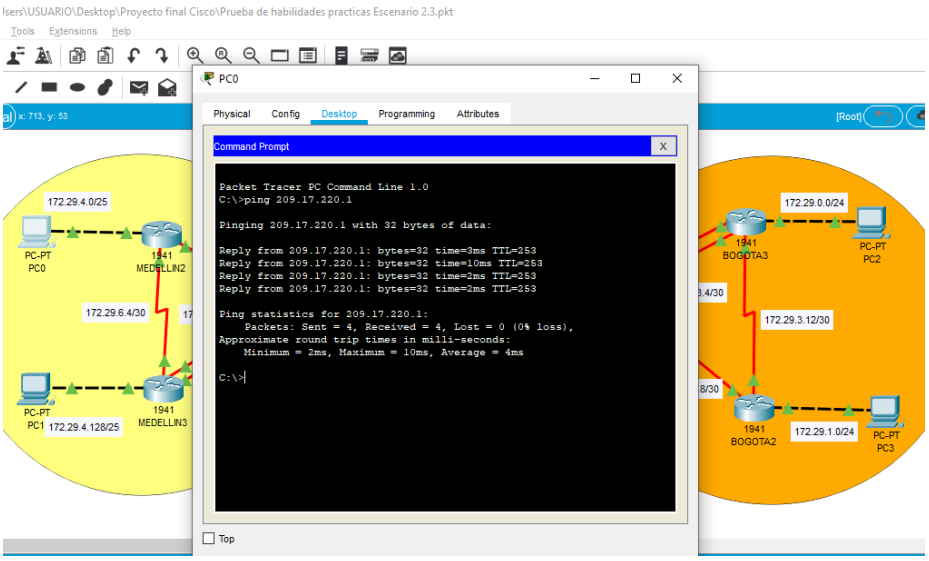


Fig. 33. Verificación de conectividad entre PC0 e ISP

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.

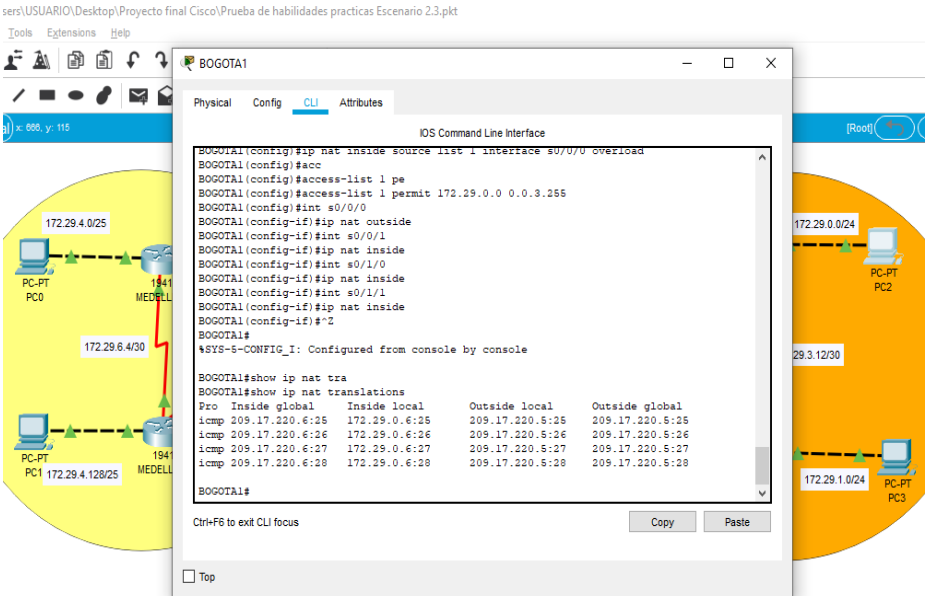


Fig. 34. Comprobación de tabla de traducción en BOGOTA1.

PARTE 8. 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(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MED2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MED3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#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.

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

Así se configurará la dirección ip en PC1 como se observa en la imagen

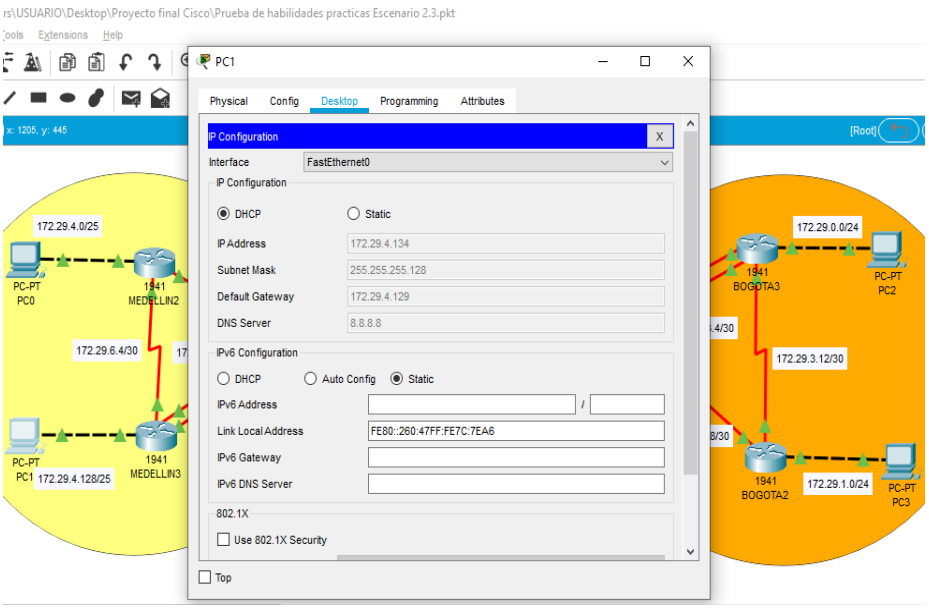


Fig. 35. Configuración DHCP en PC1

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

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp pool BOG2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#ip dhcp pool BOG3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
```

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

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

Así se configurará la dirección ip en PC3 como se observa en la imagen

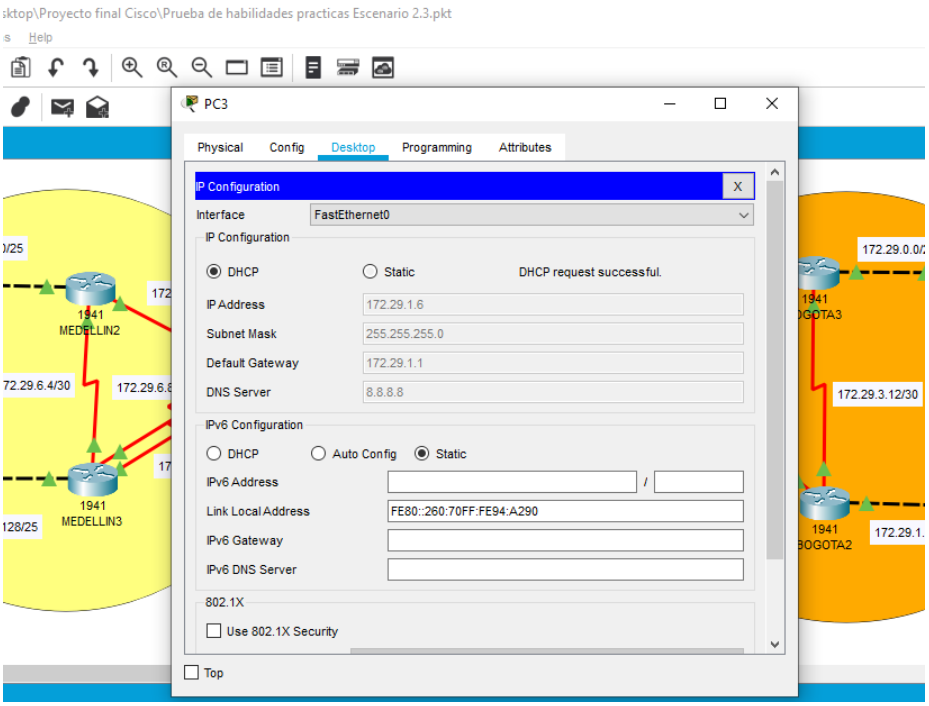


Fig. 36. Configuración IP DHCP en PC3.

Procedemos a realizar pruebas de Conexión entre PC´s

Se Realiza Ping desde PC2 a PC3

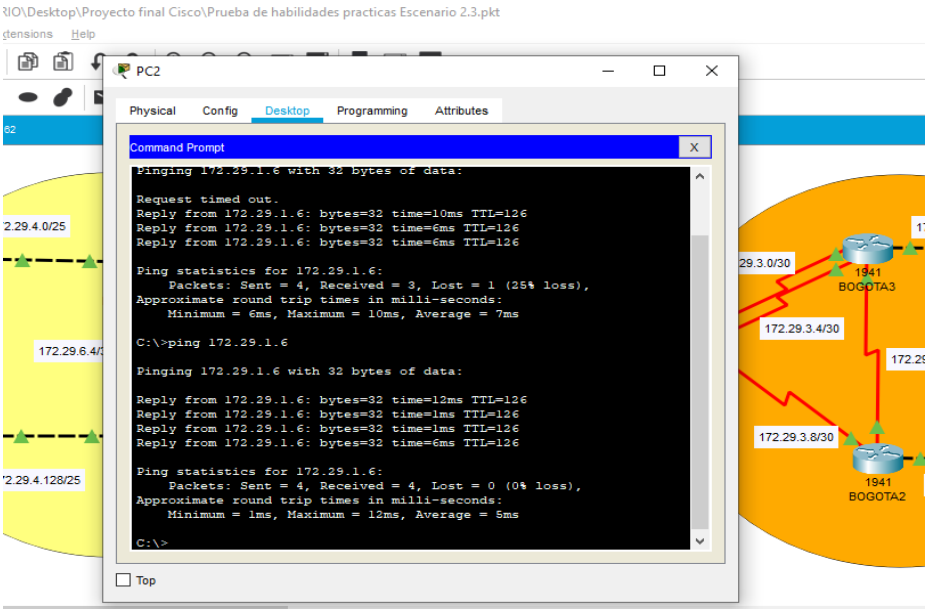


Fig. 37. Prueba de conexión entre PC2 a PC3.

Se Realiza Ping desde PC2 a PC0

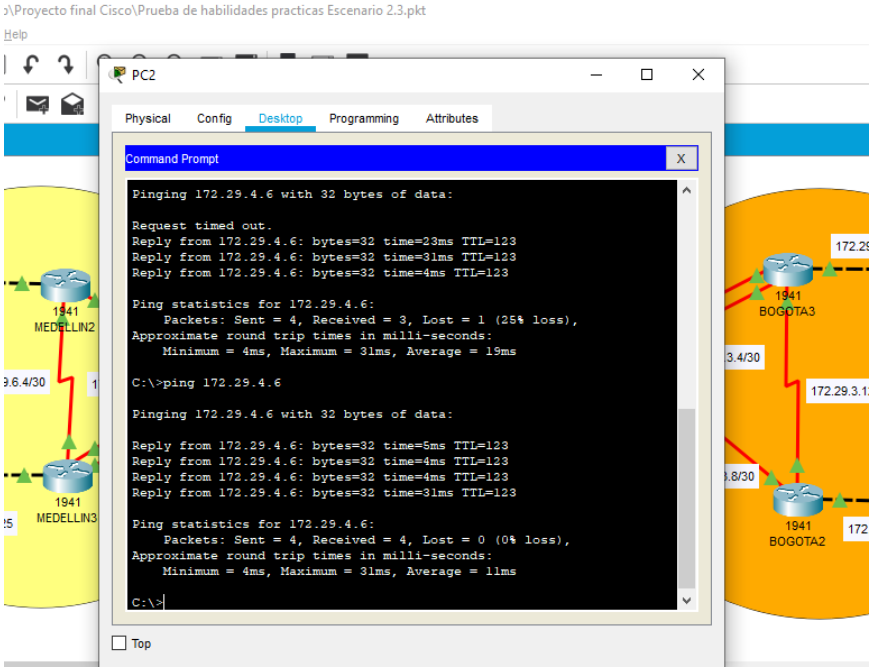


Fig. 38. Prueba de conexión entre PC2 a PC0.

Se Realiza Ping desde PC2 a PC1

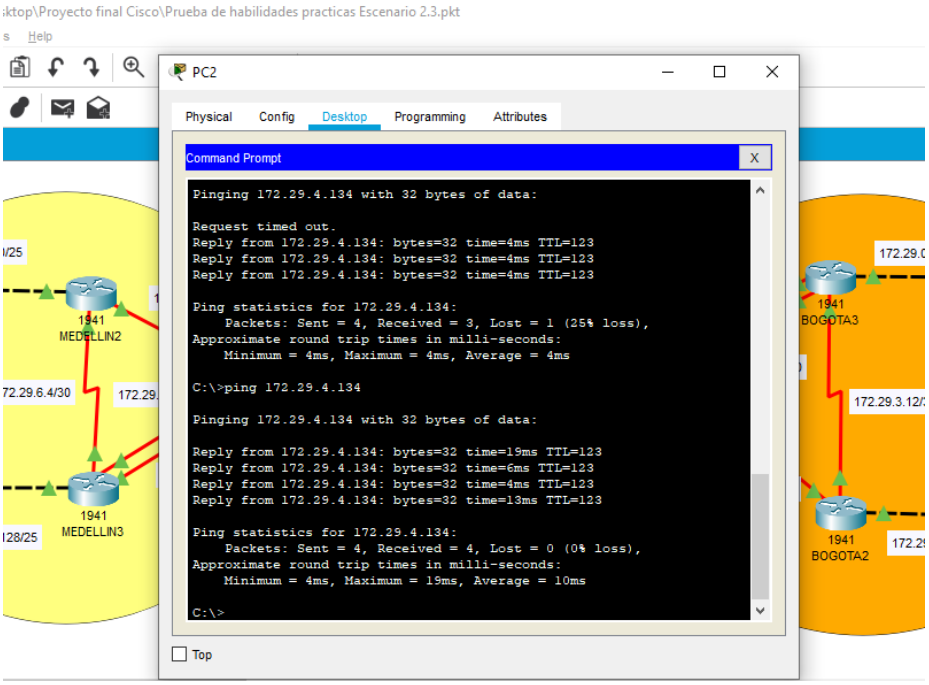


Fig. 39. Prueba de conexión entre PC2 a PC1.

5. CONCLUSIONES

- Se identificaron los diferentes comandos para el enrutamiento de la red además de la configuración de redes con RIP V2, configuración de seguridad, NAT, PPP, PAP de forma exitosa en la prueba de habilidades prácticas.

- Se realizó la implementación de la topología de forma adecuada con sus correspondientes configuraciones que permitieron realizar todas las pruebas pertinentes del módulo 2 del CCNA en el diplomado de redes Cisco.

- Se logró corregir la topología en la conexión de los puertos seriales de una forma adecuada que solucionó los inconvenientes encontrados durante el desarrollo de la práctica, además de realizaron las diferentes pruebas con el fin de revertir algunas configuraciones erróneas y se aplicaron las correspondientes correcciones.

- Se aplicaron todas las pruebas de conexión que demostraron cada una de las configuraciones establecidas en los dos escenarios planteados en la actividad final.

- Con la ayuda del tutor se despejaron dudas sobre la configuración de los dos escenarios planteados, logrando así realizar y efectuar de manera correcta tanto la topología y configuración de los dispositivos a utilizar y también el funcionamiento de las redes planteadas con todas las configuraciones básicas solicitadas.

6. REFERENCIAS BIBLIOGRAFICAS

Temática: Enrutamiento Dinámico
CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Temática: OSPF de una sola área
CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

Temática: DHCP
CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Configuración DHCP
Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado 10 mayo, 2020, de
http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar- dhcp-en-cisco-router/

Rutas Estáticas
Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 8 mayo, 2020, de
http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route- router-cisco/

Configuración PPP y PAP
Leandro Di Tommaso, L. D. T. (2010, 28 febrero). Configuración de PPP y PAP en Cisco. Recuperado 7 mayo, 2020, de
https://www.mikroways.net/2010/02/28/configuracion-de-ppp-y-pap-en- cisco/

Configuración NAT
Eugenio Duarte, E. D. (2016, 12 abril). Cisco CCNA – Cómo Configurar NAT Overload En Cisco Router. Recuperado 12 mayo, 2020, de
http://blog.capacityacademy.com/2014/06/18/cisco-ccna-como-configurar- nat-overload-en-cisco-router/

Configuración RIPV2

Victor E. Martinez G, V. E. M. (2015, 22 abril). Configuración de RIPv2 (protocolo dinámico). Recuperado 12 mayo, 2020, de http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/