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

JOHANNES EDUARDO ROJAS AGUIRRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS.
TUNJA
2020

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

JOHANNES EDUARDO ROJAS AGUIRRE

GRUPO NO 22

PRUEBA DE HABILIDADES

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

TUTOR
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS.
TUNJA
2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma Jurado

_____

Firma Presidente del Jurado

Tunja, 02 de Mayo del 2020

AGRADECIMIENTOS:

El presente trabajo es dedicado primordialmente a Dios, a mi familia, a mi querida esposa y a mi hija quienes han sido la motivación para el desarrollo de este trabajo.

Gracias a su estímulo y apoyo han sido los protagonistas de este sueño alcanzado.

CONTENIDO

pag

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En la actualidad es de gran importancia el procesamiento y distribución de información, con el empleo de equipos de cómputo que cada vez son más sofisticados en base a su procesamiento, pero es necesario para un trabajo en conjunto que haya interconexiones entre los ordenadores para lo cual las redes prestan servicios de transferencia de información, para lograr estos enlaces es importante el empleo de dispositivos, enlaces de transmisión y protocolos que permitan que los datos estén disponibles para cualquier usuario en la red que tenga los permiso y credenciales necesarias. En lo relacionado con fundamentos de Networking, que son la base para la configuración de pequeñas redes locales (LAN) que es empleada para conectar servidores, estaciones dentro de un mimos zona geográfico en base al tipo de arquitectura, los modelos de red en capas, que son el proceso donde se emplean los diversos protocolos en cada una de las capas, con el fin de lograr una comunicación eficiente. También se refleja en el desarrollo de los escenarios el empleo de direccionamiento IPV4 e IPV6, sus funcionalidades, que procesos emplean según la topología que se desarrolle, donde se evidencian configuraciones diversas de enrutamientos, switch y servidores, para la correcta comunicación de estos dispositivos según las exigencias solicitadas en las topologías de los escenarios estudiados, con el empleo del Simulador Packet tracer.

OBJETIVOS

General:

- Realizar la correcta topología y configuración de los dispositivos en cada uno de los escenarios establecidos para lograr la comunicación acertada cada una de las terminales en las diferentes redes.

Específicos:

- El empleo de las configuraciones básicas por consola en los Sistemas operativos IOS de Cisco, mediante condigos de comando (CLI), para las interfaces de los dispositivos como Swith, Routers y host de PC.
- Configurar el direccionamiento para la comunicación entre dispositivos con el empleo de protocolos IP.
- Conocer las diferentes capas y protocolos que se emplean para la comunicación de paquetes de datos.
- Establecer el direccionamiento según la topología de red.
- Conocer y emplear la configuración adecuada del enrutamiento estatico, dinamico, Ospf y Riv2, entre las redes.
- Aplicación de listas de control, banco de direcciones (pool) para el empleo de DHPC

Prueba de habilidades prácticas CCNA

Descripción general de la prueba de habilidades

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros.**

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer**

DESARROLLO DE ACTIVIDAD

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.

Topología

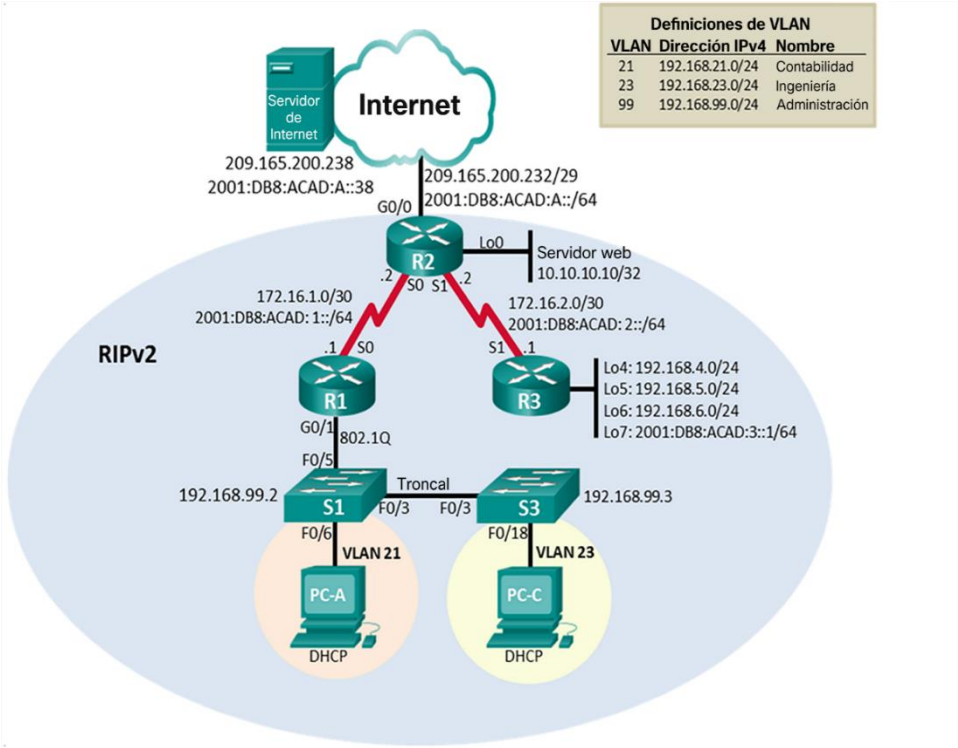


Figura1. Topologia de red escenario 1

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Servidor PC	Nic	209.165.200.238		209.165.200.225
	Nic	2001:db8:acad:a::38 /64		2001:DB8:ACAD:2::1
R1	S0/0/0	172.16.1.1 /30	255.255.255.252	172.16.1.1
		2001:db8:acad:1:: /64		
	G0/1			
R2	G0/0	209.165.200.232 /29	255.255.255.0	
		2001:db8:acad:a:: /64		
	S0/0/0	172.16.1.2 /30	255.255.0.0	
		2001:db8:acad:2:: /64		
	S0/0/1	172.16.2.1 /30	255.255.255.252	
		2001:db8:acad:2:: /64		
	Lo0	10.10.10.10 /32 servidor web	255.0.0.0	
R3	S0/0/1	172.16.2.2 /30	255.255.255.252	N/A
	Lo4	192.168.4.1 /24	255.255.255.0	
	Lo5	192.168.5.1 /24	255.255.255.0	
	Lo6	192.168.6.1 /24	255.255.255.0	
	Lo7	2001:db8:acad:3:: 1 /64	255.255.255.0	
S1	IP	192.168.99.2		N/A
	F0/5 R1			
	F0/6 VLAN21 PCA			
	F0/3 TRONC S3			
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Tabla 1. Tabla de direccionamiento Escenario 1

Máscara de subred	Dirección de 32 bits	Longitud de prefijo
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

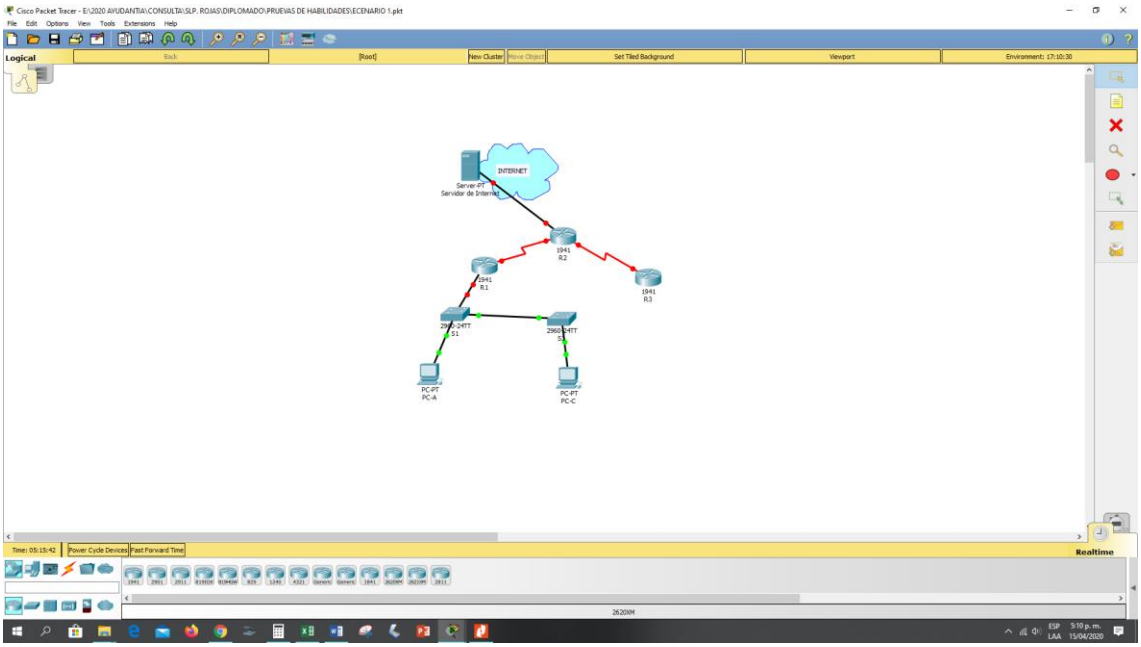


Figura2. Evidencia creacion de Red

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
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#sh flash:

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	255.255.255.0
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38 /64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	class R1(config)#enable secret class
Contraseña de acceso a la consola	cisco R1(config)#line con 0 R1(config-line)#password cisco
Contraseña de acceso Telnet	cisco R1(config)#line vty 0 4 R1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#

Interfaz S0/0/0	R1(config)#int s0/0/0 Establezca la descripción R1(config-if)#description Conexion al R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ipv6 address 2001:db8:acad:1::/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#clock rate 128000 Activar la interfaz R1(config-if)#no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)#int s0/0/0 R1(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

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	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	class R2(config)#enable secret class
Contraseña de acceso a la consola	cisco R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#logging synchronous

Contraseña de acceso Telnet	cisco R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#logging synchronous
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)# ip http secure-server
Mensaje MOTD	R2(config)#banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	R2(config)#int s0/0/0 Establezca la descripción R2(config-if)#description Conexion al R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config-if)#ip address 172.16.1.1 255.255.0.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:db8:acad:1::/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 Establecer la descripción R2(config-if)#description Conexion al R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 172.161.2.0 255.255.0.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:db8:acad:2::/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 Establecer la descripción. R2(config-if)#description Conexion al Servidor de Internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 209.165.200.232 255.255.255.0 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. R2(config-if)#ipv6 address 2001:db8:acad:a::/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)#description Conexion al servidor Web Establezca la dirección IPv4. R2(config-if)#ip address 10.10.10.10 255.0.0.0
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.238 Configure una ruta IPv6 predeterminada de G0/0. ipv6 route ::/0 s0/0/0

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	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	class R3(config)#enable secret class
Contraseña de acceso a la consola	cisco R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#logging synchronous

Contraseña de acceso Telnet	cisco R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#logging synchronous
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)#banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config-if)#ip address 172.161.3.0 255.255.0.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#ipv6 address 2001:db8:acad:2::/64 Activar la interfaz R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred R3(config)#int lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#int lo7 R3(config-if)#ip address 192.168.7.1 255.255.255.0
Rutas predeterminadas	R3(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.2.1

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	S1 Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	class S1(config)#enable secret class
Contraseña de acceso a la consola	cisco S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#logging SYnchronous
Contraseña de acceso Telnet	cisco S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#logging SYnchronous
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. 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	Switch(config)#no ip domain-lookup
Nombre del switch	S3 Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	class S3(config)#enable secret class

Contraseña de acceso a la consola	cisco S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#logging synchronous
Contraseña de acceso Telnet	cisco S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#logging synchronous
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)#banner motd #SE PROHIBE EL ACCESO 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	R1>ping 172.16.1.2	**Satisfactorio**
R2	R3, S0/0/1	R2>ping 172.16.2.2	**Satisfactorio**
PC de Internet	Gateway predeterminado	C:\>ping 209.165.200.232	**Satisfactorio**

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

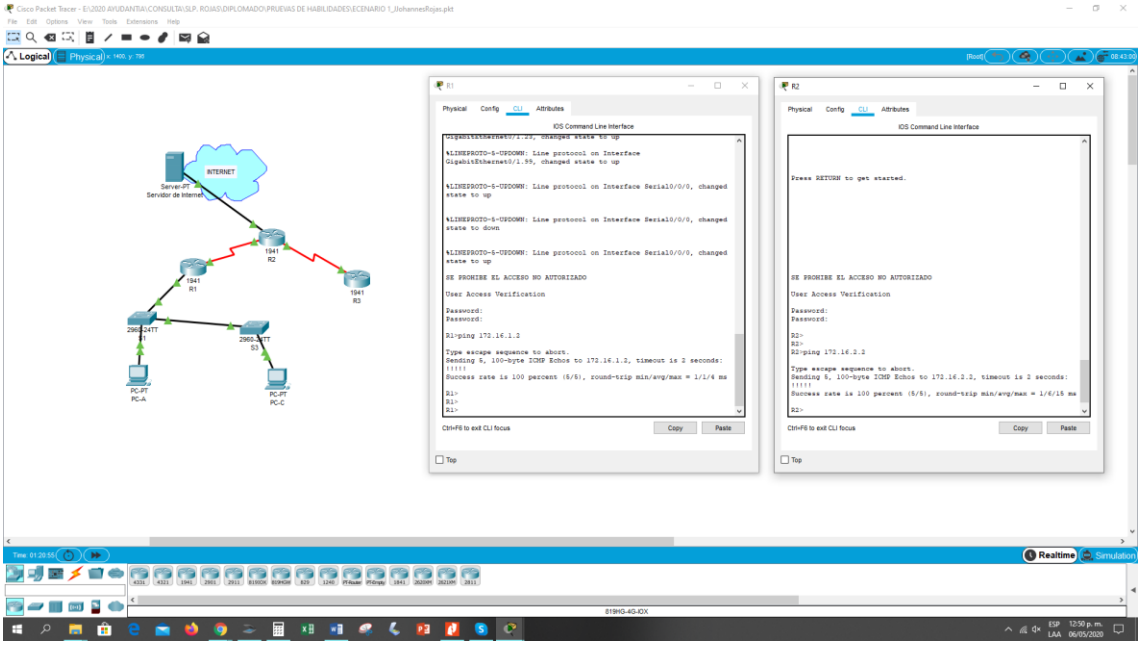


Figura3. Evidencia conectividad de dispositivos

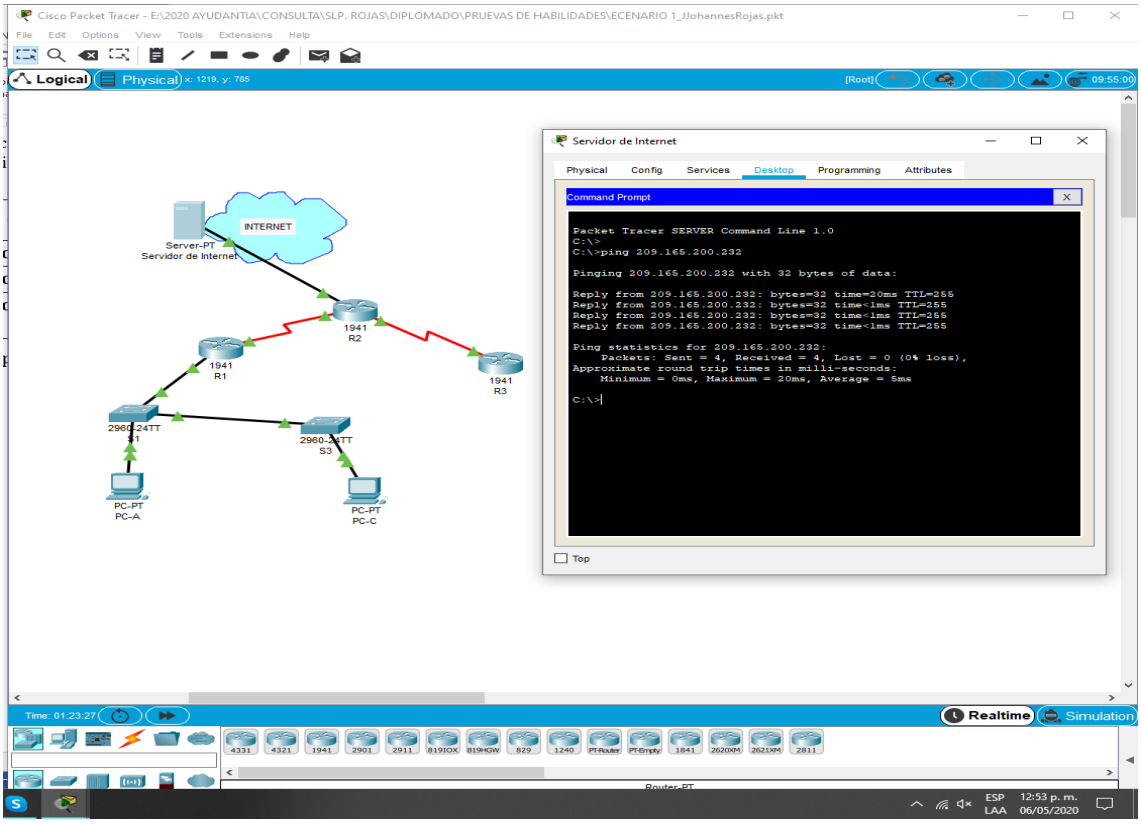


Figura4. Evidencia conectividad de dispositivos

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

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1.99	192.168.99.1	255.255.255.0	N/A
	G0/1.21	192.168.21.1	255.255.255.0	N/A
	G0/1.23	192.168.23.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 99	192.168.99.2	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.3	255.255.255.0	192.168.99.1
PC-A	NIC	192.168.21.3	255.255.255.0	192.168.21.1
PC-B	NIC	192.168.23.3	255.255.255.0	192.168.21.1

Tabla 2. Tabla de direccionamiento Vlans Escenario 1

Especificaciones de la asignación de puertos de switch

Puertos	Asignaciones	Red
S1 F0/1	Enlace troncal de 802.1Q	N/A
S2 F0/1	Enlace troncal de 802.1Q	N/A
S1 F0/5	Enlace troncal de 802.1Q	N/A
S1 F0/6	VLAN 21: Contabilidad	192.168.21.0/24
S2 F0/18	VLAN 20: Ingenieria	192.168.23.0/24

Tabla 3. Tabla de asignación de Swith escenario 1

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 indicant S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion
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 S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native 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	Utilizar la red VLAN 1 como VLAN nativa S1(config)#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	Utilizar el comando interface range S1(config)# 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)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2,f0/4,f0/7-24 ,g0/1 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. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config)#vlan 23 S3(config-vlan)#name ingenieria S3(config)#vlan 99 S3(config-vlan)#name Administracion
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 S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#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)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2,f0/4-17,f0/19-24 ,g0/1 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 R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad Asignar la VLAN 21 R1(config-subif)#encapsulation dot1Q 21 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria Asignar la VLAN 23 R1(config-subif)#encapsulation dot1Q 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config)#int g0/1.99 R1(config-subif)#description LAN de Administracion Asignar la VLAN 99 R1(config-subif)#encapsulation dot1Q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdow

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	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

Tabla 4. Tabla de conectividad de red Escenario 1

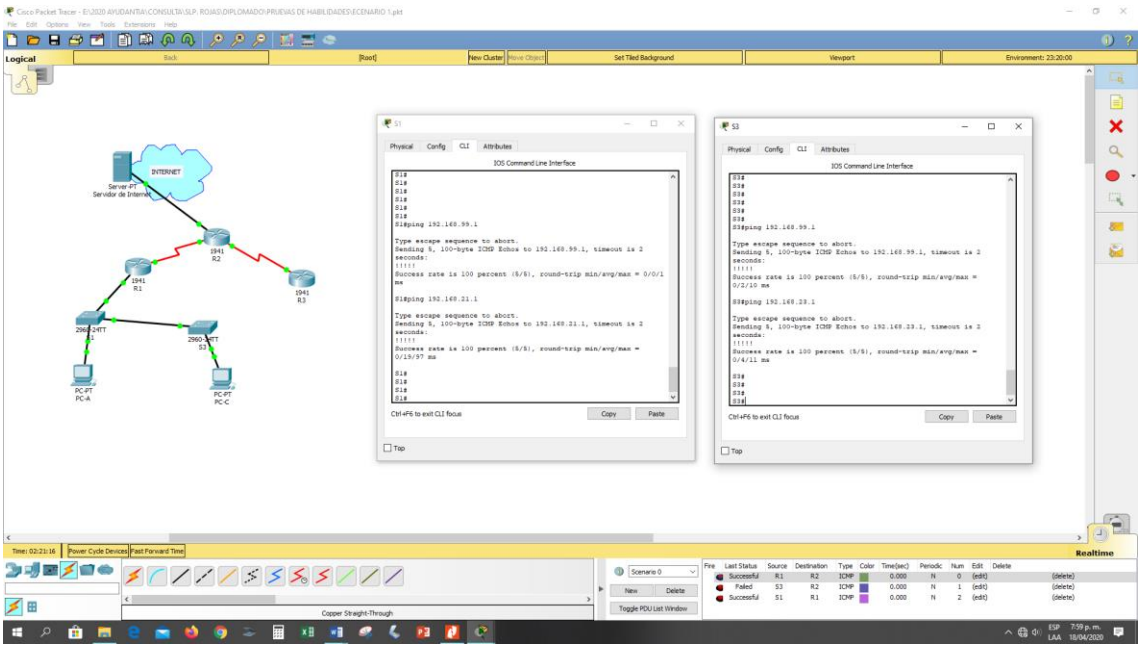


Figura5. Evidencia conectividad Swits con las Vlan

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#confg t R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.0.0

Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1
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	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0 R2(config-router)#network 172.16.0.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 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)#network 172.16.0.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#passive-interface lo7
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?	R1#show ip protocols

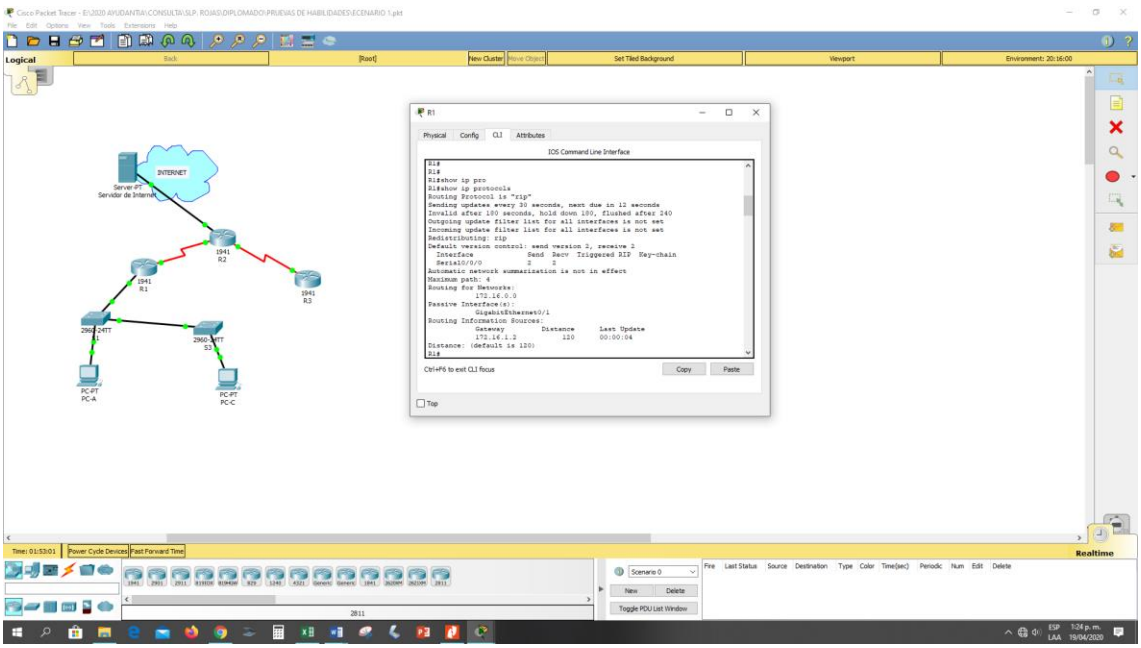


Figura6. Ejecucion comando para ver los protocolos R1

¿Qué comando muestra solo las rutas RIP?	R1#show ip route rip

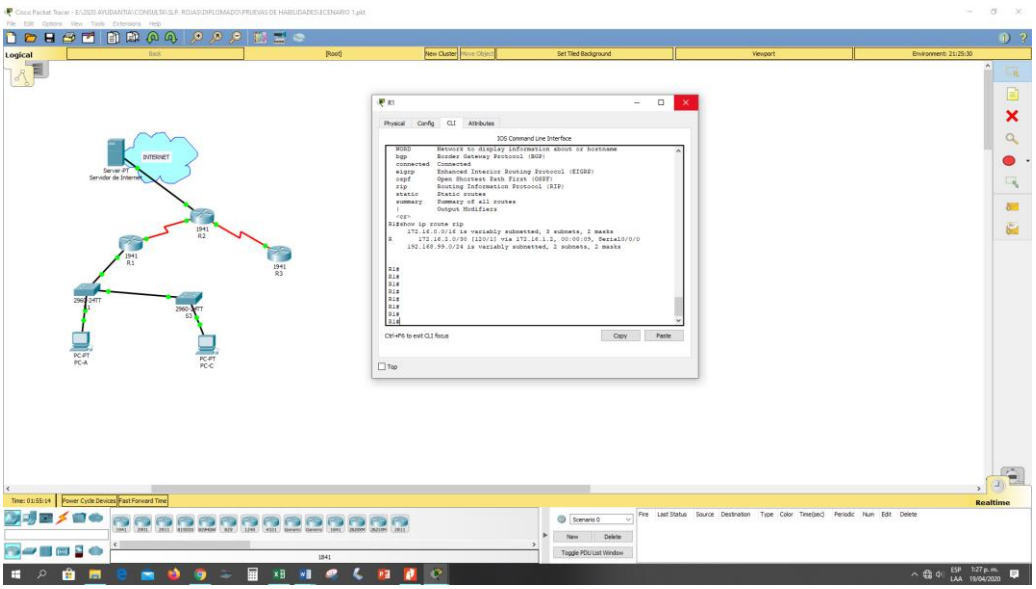


Figura 7. Ejecucion comando para ver las rutas RIP

¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#show run

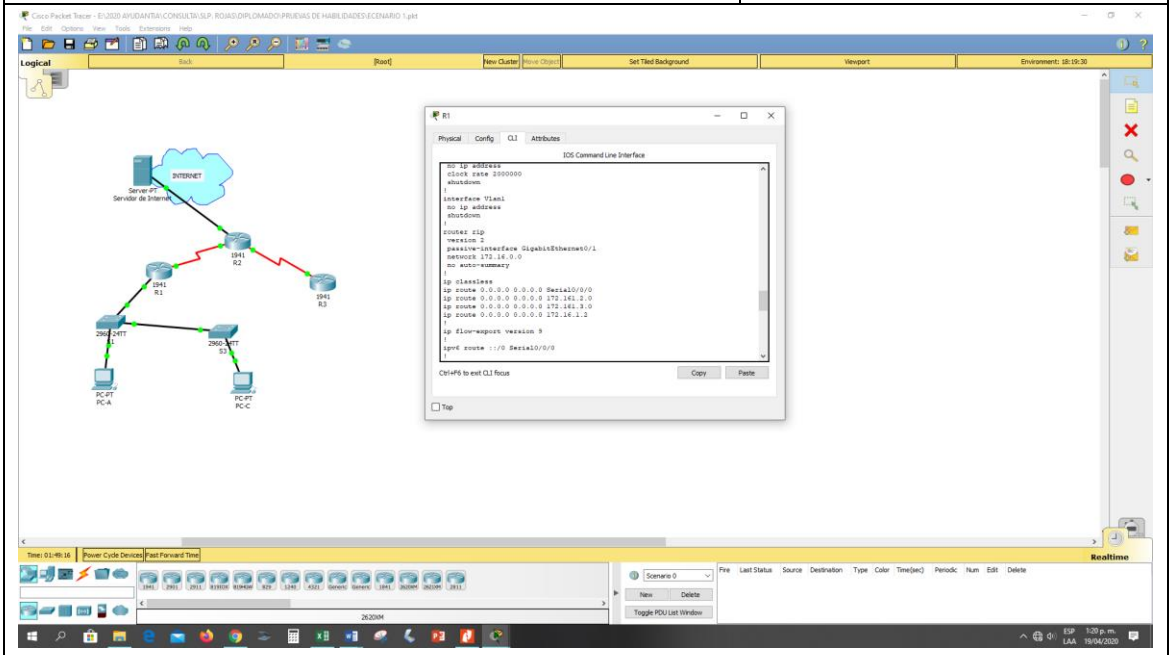


Figura 8. Ejecucion comando para ver ejecucion de RIP

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.	Nombre: ACCT R1(config)#ip dhcp pool ACCT R1(dhcp-config)#NETwork 192.168.21.0 255.255.255.0 Servidor DNS: 10.10.10.10 R1(dhcp-config)#DNS-SErver 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#NETwork 192.168.23.0 255.255.255.0 Servidor DNS: 10.10.10.10 R1(dhcp-config)#DNS-SErver 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.23.1

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

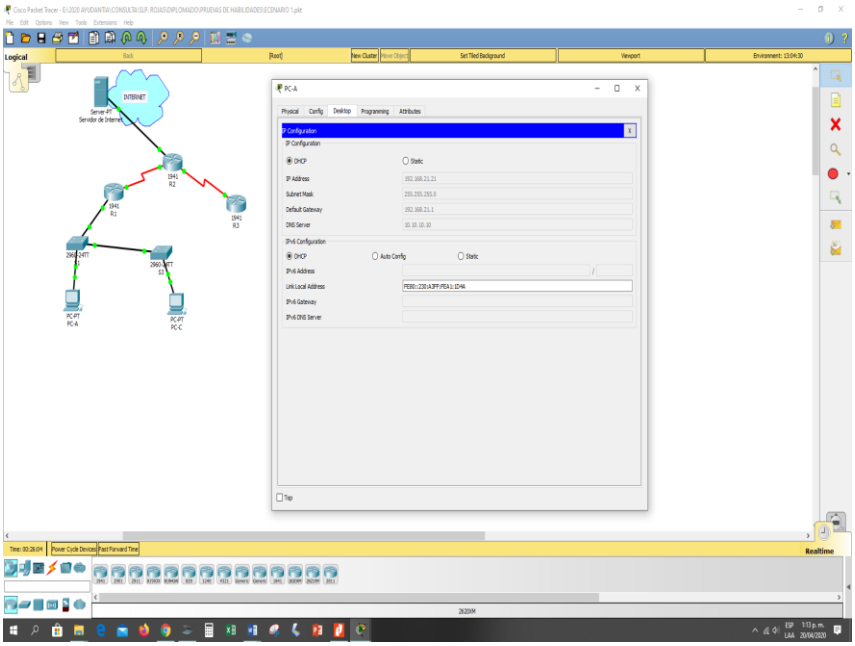
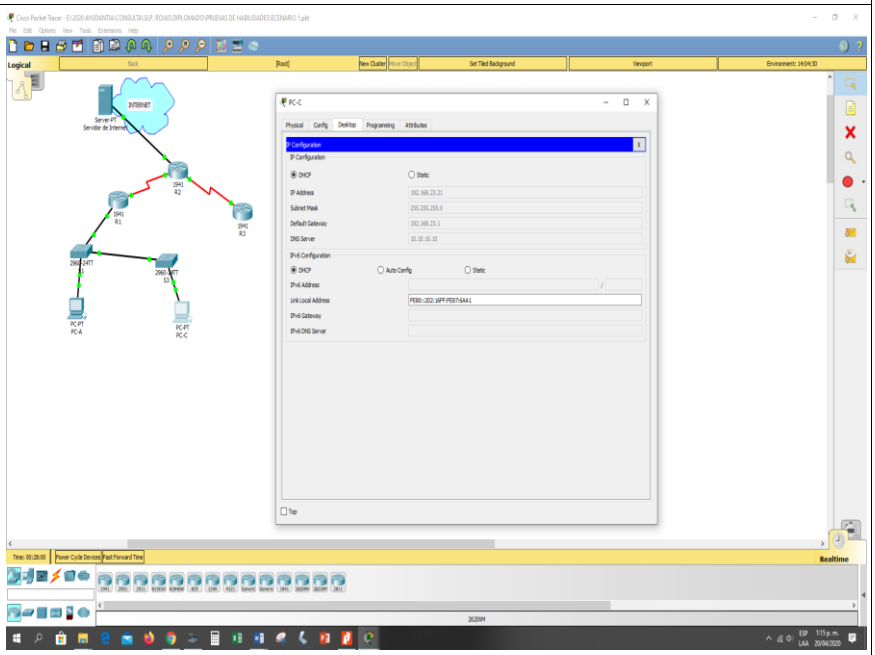
La configuración del R2 incluye las siguientes tareas:

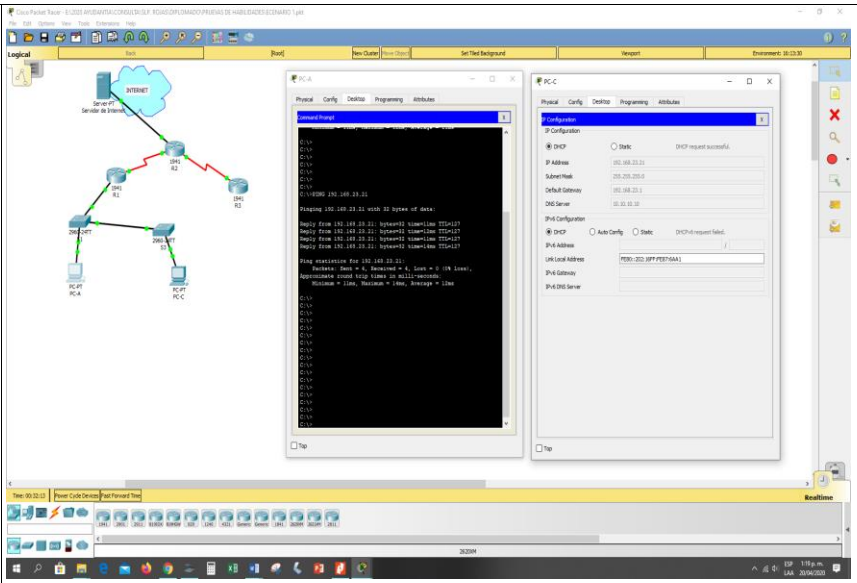
Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática	R2(config-if)#int g0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat outside
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 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 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.3.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.3.255
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** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 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	 Figura 9. Verificacion de adquicicion de ip del servidor DHCP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 10. Verificacion de adquicicion de ip del servidor DHCP

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 Figura 11. Verificacion del comando PING
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**	

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 16:00:00 March 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)# ntp update-calendar

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 R2(config-std-nacl)#PERMIt host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R2#show run

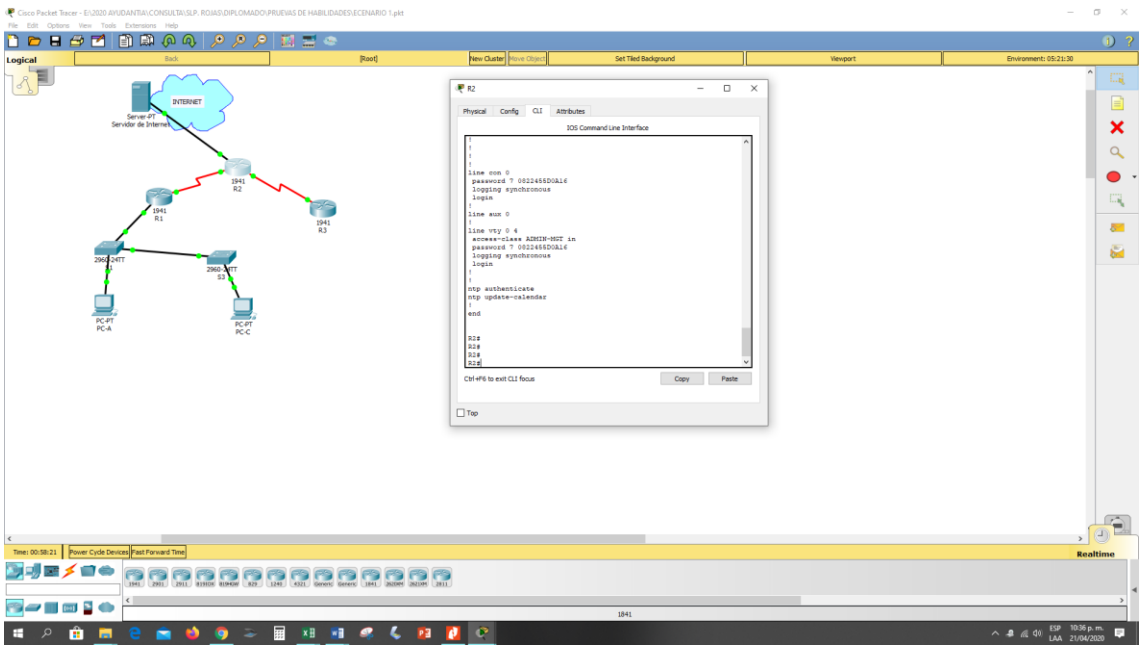
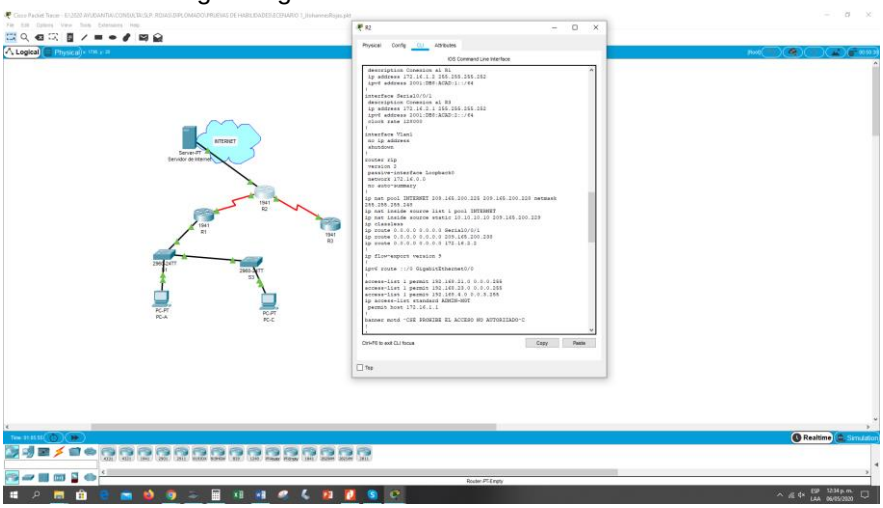
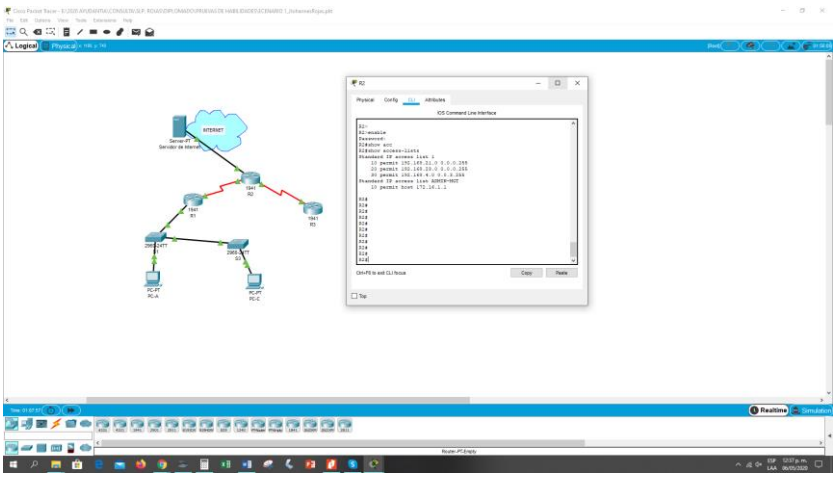
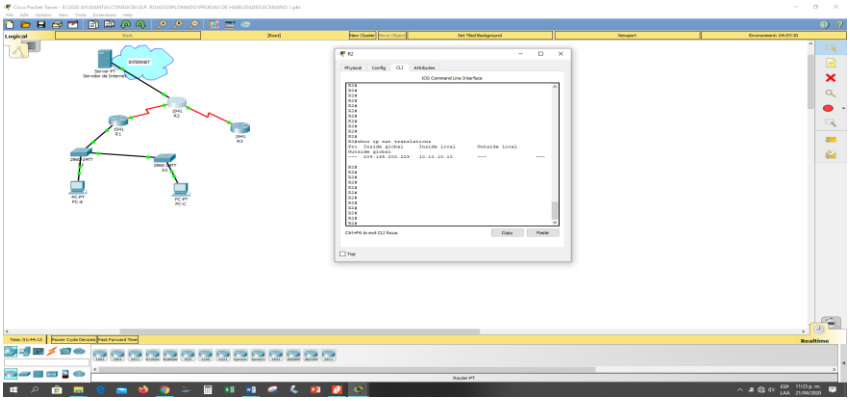


Figura 12. Verificacion del funcionamiento de la ACL

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 running-config  Figura 13. Verificacion de lista de acceso
Restablecer los contadores de una lista de acceso	R2#clear access-list counter
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show access-lists  Figura 14. Verificacion de aplicacion de ACL

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations  Figura 15. Comando para verificar las traducciones Nat
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

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

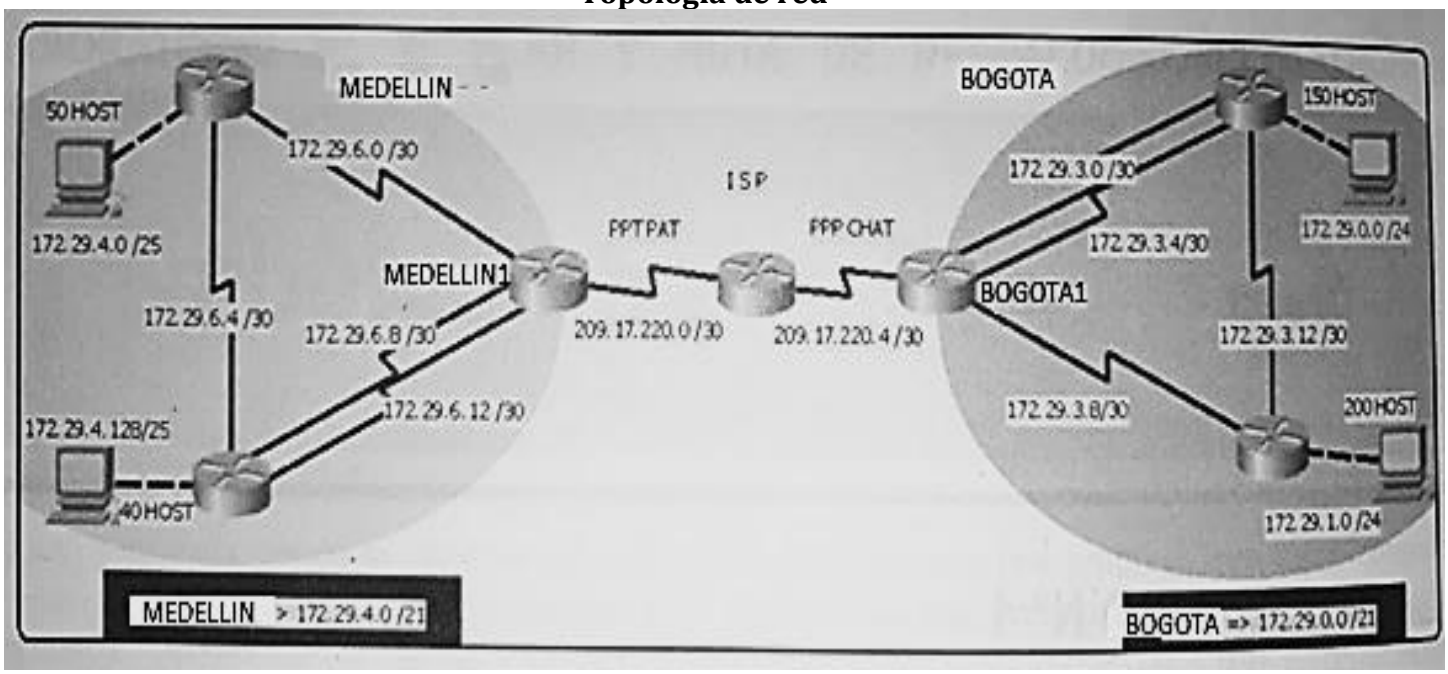


Figura 16. Topologia Escenario 2

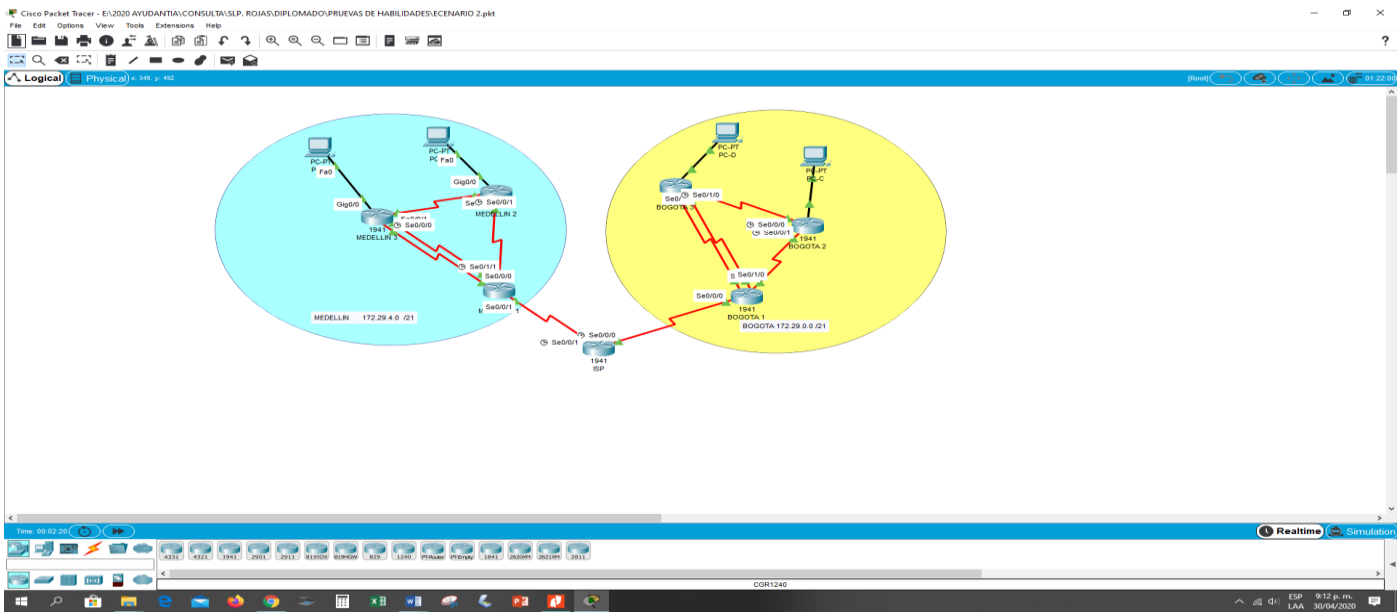


Figura 17. Evidencia creacion Topologia Escenario 2

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

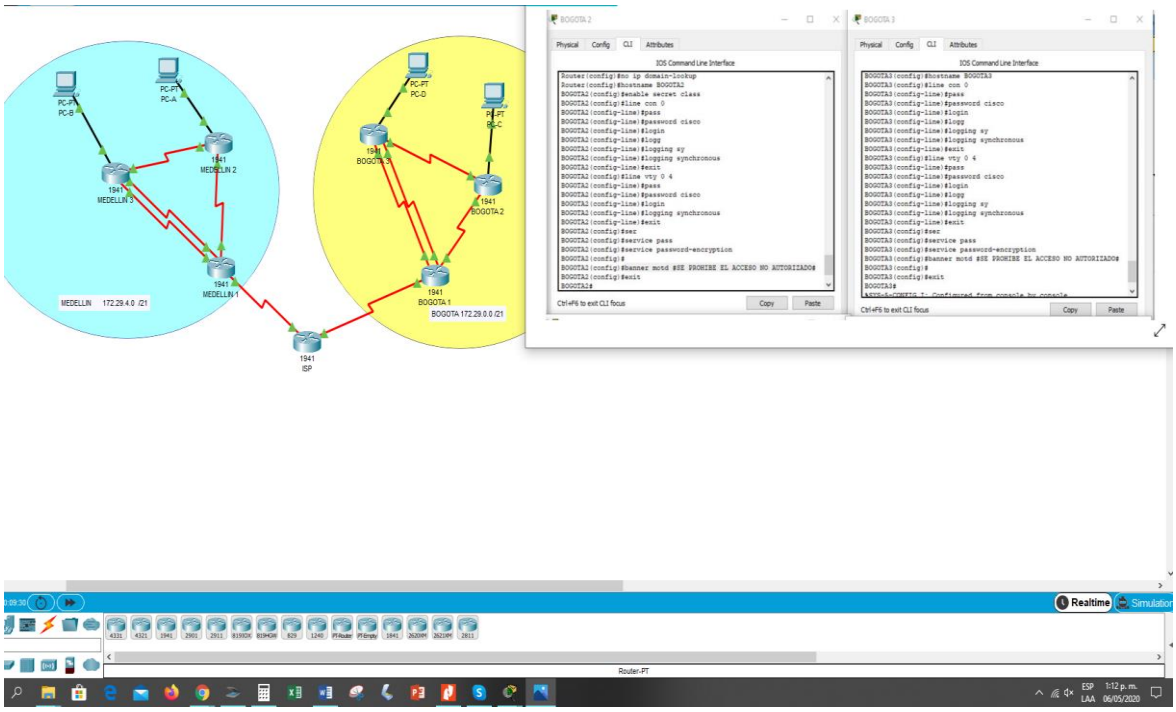


Figura 18. Evidencia comandos para configuracion de equipos

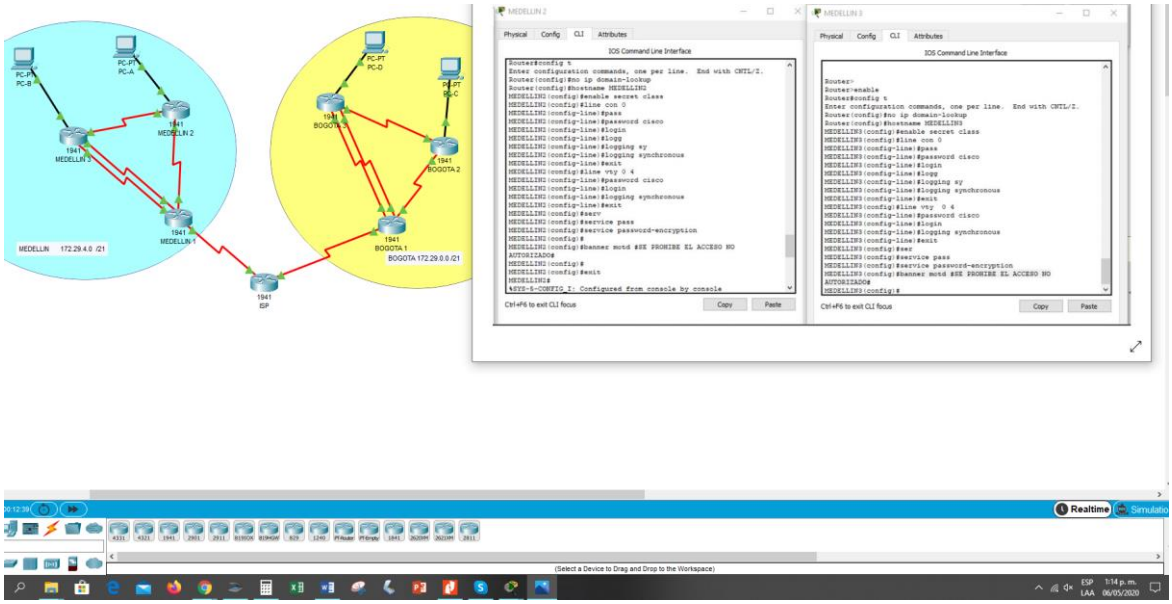


Figura 19. Evidencia comandos para configuracion de equipos

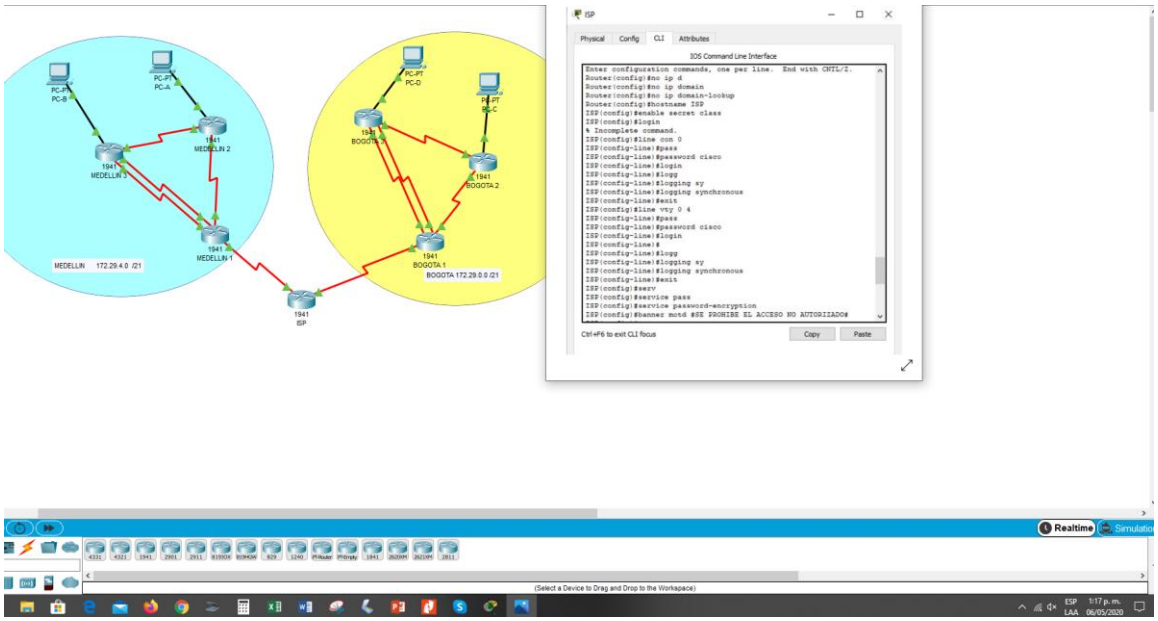


Figura 20. Evidencia comandos para configuracion de equipos

- 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.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	
ISP	S0//0/0	209.17.220.5 /30	255.255.255.252	
	S0/0/1	209.17.220.1 / 30	255.255.255.252	
MEDELLIN 1	S0/0/0	172.29.6.13 / 30	255.255.255.252	
	S0/0/1	209.17.220.2 / 30	255.255.255.252	
	S0/1/0	172.29.6.9 /30	255.255.255.252	
	S0/1/1 DCE	172.29.6.1 / 30	255.255.255.252	
MEDELLIN 2	G0/0	172.29.4.1 /25	255.255.255.128	
	S0/0/1 DCE	172.29.6.5 /30	255.255.255.252	
	S0/1/1	172.29.6.2 /30	255.255.255.252	
MEDELLIN 3	G0/0	172.29.4.129 /25	255.255.255.128	
	S0/0/1	172.29.6.6 /30	255.255.255.252	
	S0/1/0 DCE	172.29.6.10 /30	255.255.255.252	
	S0/0/0 DCE	172.29.6.14 /30	255.255.255.252	
BOGOTA 1	S0/0/0	209.17.220.6 /30	255.255.255.252	
	S0/1/0	172.29.3.1 / 30	255.255.255.252	
	S0/0/1 DCE	172.29.3.9 /30	255.255.255.252	
	S0/1/1	172.29.3.5 / 30	255.255.255.252	
BOGOTA 2	G0/0	172.29.1.1 / 24	255.255.255.0	
	S0/0/0 DCE	172.29.3.13 /30	255.255.255.252	
	S0/0/1	172.29.3.10 /30	255.255.255.252	
BOGOTA 3	G0/0	172.29.0.1 /24	255.255.255.0	
	S0/1/1	172.29.3.6 /30	255.255.255.252	
	S0/1/0 DCE	172.29.3.2 /30	255.255.255.252	
	S0/0/0	172.29.3.14 /30	255.255.255.252	
PC-A	NIC	172.29.4.12	255.255.255.0	172.29.4.1
PC-B	NIC	172.29.4.133	255.255.255.0	172.29.4.129
PC-C	NIC	172.29.1.14	255.255.255.0	172.29.1.1
PC-D	NIC	172.29.0.15	255.255.255.0	172.29.0.1

Tabla 5. Tabla de direccionamiento Escenario 2 .

ASIGNACION DE DIRECCIONES IP EN CADA UNA DE LAS INTERFAZES DE LOS DISPOSITIVOS

ISP

```
ISP(config)#int s0/0/0
ISP(config-if)#description Conexion ISP-BOGOTA1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

ISP(config)#int s0/0/1
ISP(config-if)#description Conexion ISP-MEDELLIN1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown
```

BOGOTA 1

```
BOGOTA1#config t

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

BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#description Conexion BOGOTA1-BOGOTA3
BOGOTA1(config-if)#IP ADDress 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#NO shutdown

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

BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#description Coneexion BOGOTA3
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

BOGOTA 2

```
BOGOTA2#config t

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

```
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#description Conexion BOGOTA3
BOGOTA2(config-if)#IP ADDress 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#CLock rate 128000
BOGOTA2(config-if)#NO SHUtdown

BOGOTA2(config)#INT S0/0/1
BOGOTA2(config-if)#description Conexion BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
```

BOGOTA 3

```
BOGOTA3#config t

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

BOGOTA3(config)#int s0/1/1
BOGOTA3(config-if)#description Conexion BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown

BOGOTA3(config-if)#int s0/1/0
BOGOTA3(config-if)#description Conexion BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown

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

MEDELLIN 1

```
MEDELLIN1#config t
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#description Conexion MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.25
MEDELLIN1(config-if)#clock rate 128000

MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#description Conexion ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
```

```
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#description Conexion MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#no shutdown

MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#description Conexion MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown

MEDELLIN2#config t

MEDELLIN2(config)#int g0/0
MEDELLIN2(config-if)#description Conexion PC-A
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config)#int s0/0/1
MEDELLIN2(config-if)#description Conexion MEDELLIN3
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config)#int s0/1/1
MEDELLIN2(config-if)#description Conexion MEDELLIN1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no shutdown
```

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.

```
MEDELLIN1#config t
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.2 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.2 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.2 0.0.0.3 area 0
MEDELLIN1(config-router)#no auto-sumary

MEDELLIN2#config t
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#network 172.29.6.1 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.5 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 0

MEDELLIN3#config t
MEDELLIN3(config)#router ospf 1
```

```
MEDELLIN3(config-router)#network 172.29.6.5 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.13 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.9 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.255 area 0
MEDELLIN3(config-router)#no auto-cost

BOGOTA1#config t
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#network 172.29.3.10 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.6 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.2 0.0.0.3 area 0

BOGOTA2#config t
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#network 172.29.3.9 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.14 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 0
BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0

BOGOTA3#config t
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.3.13 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.5 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.1 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 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.

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 209.17.220.1 0.0.0.3 area 0

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate


ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.6 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.6 0.0.0.3 area 0
```

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.

BOGOTA

Pasamos las direcciones a binario de cada una de las redes internas:

172.29.0.0 /24 → **10101100 . 00011101 . 000000**00 . 00000000
172.29.1.0 /24 : → **10101100 . 00011101 . 000000**01 . 10000000
172.29.3.0 /30 : → **10101100 . 00011101 . 00000011** ..00000000
172.29.3.4 /30 : → **10101100 . 00011101 . 00000011** . 00000100
172.29.3.8 /30 : → **10101100 . 00011101 . 00000011** . 00001000
172.29.3.12 /30 : → **10101100 . 00011101 . 00000011** . 00001100

Vemos cuantos bits coinciden de izquierda a derecha en todas las redes y sumamos para sacar el prefijo : **/22**

Ponemos en cero todos los bits que no coinciden lo lo pasamos a decimal:
10101100 . 00011101 . 00000100 . 00000000 → **172.29.0.0 / 22**

MEDELLIN

Pasamos las direcciones a binario de cada una de las redes internas:
172.29.4.0 /25 → **10101100 . 00011101 . 000001**00 . 00000000
172.29.4.128 /25 : → **10101100 . 00011101 . 000001**00 . 10000000
172.29.6.0 /30 : → **10101100 . 00011101 . 000001**10 ..00000000
172.29.6.4 /30 : → **10101100 . 00011101 . 000001**10 . 00000100
172.29.6.8 /30 : → **10101100 . 00011101 . 000001**10 . 00001000
172.29.6.12 /30 : → **10101100 . 00011101 . 000001**10 . 00001100

Vemos cuantos bits coinciden de izquierda a derecha en todas las redes y sumamos para sacar el prefijo : **/22**

Ponemos en cero todos los bits que no coinciden lo lo pasamos a decimal:

10101100 . 00011101 . 00000100 . 00000000 → **172.29.4.0 / 22**

Ahora agregamos la rutas estaticas en el ISP

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

Se verifica su funcionamiento

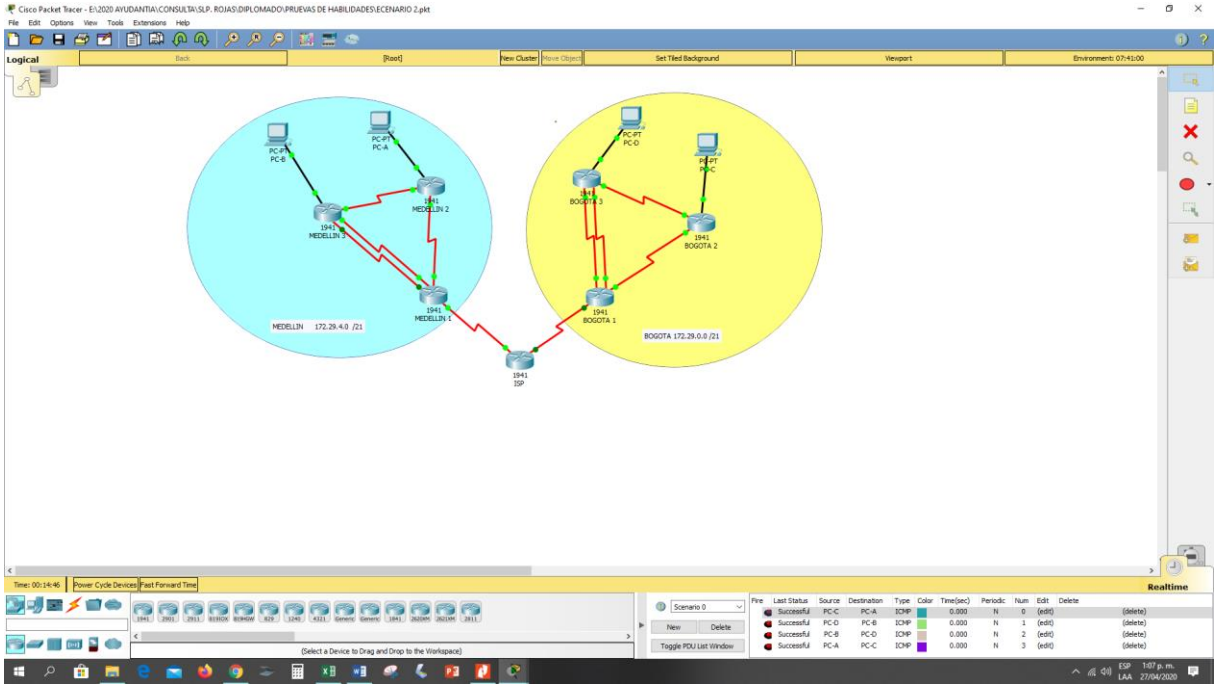


Figura 21. Evidencia conexion exitosa de los dispositivos

Parte 2: Tabla de Enrutamiento.

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

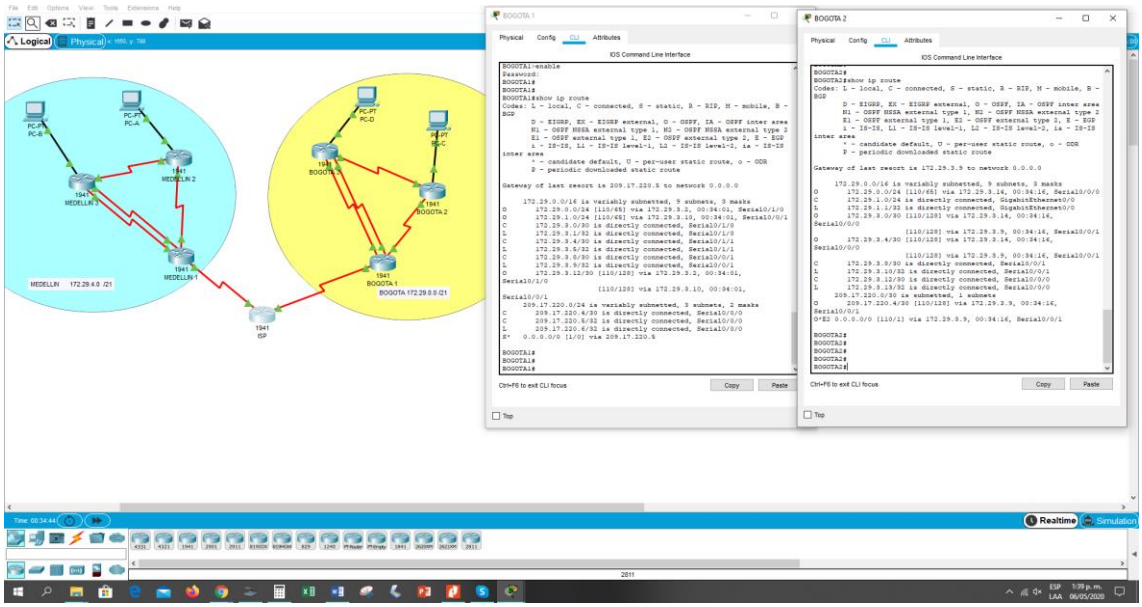


Figura 22. Evidencia verificacion tabla de enrutamiento

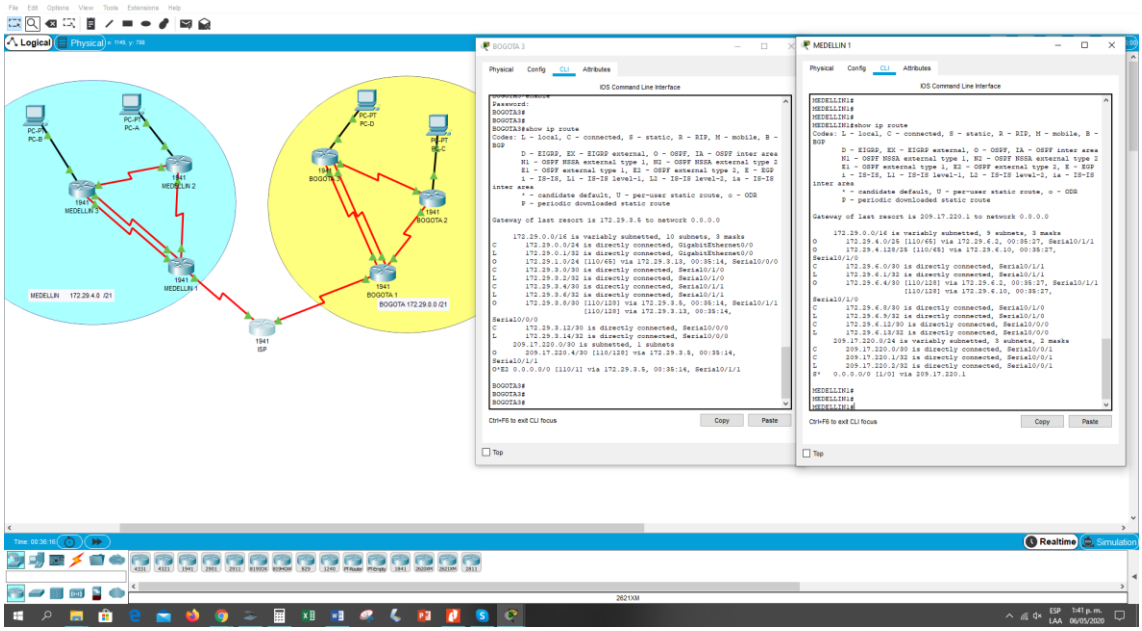


Figura 23. Evidencia verificacion table de enrutamiento

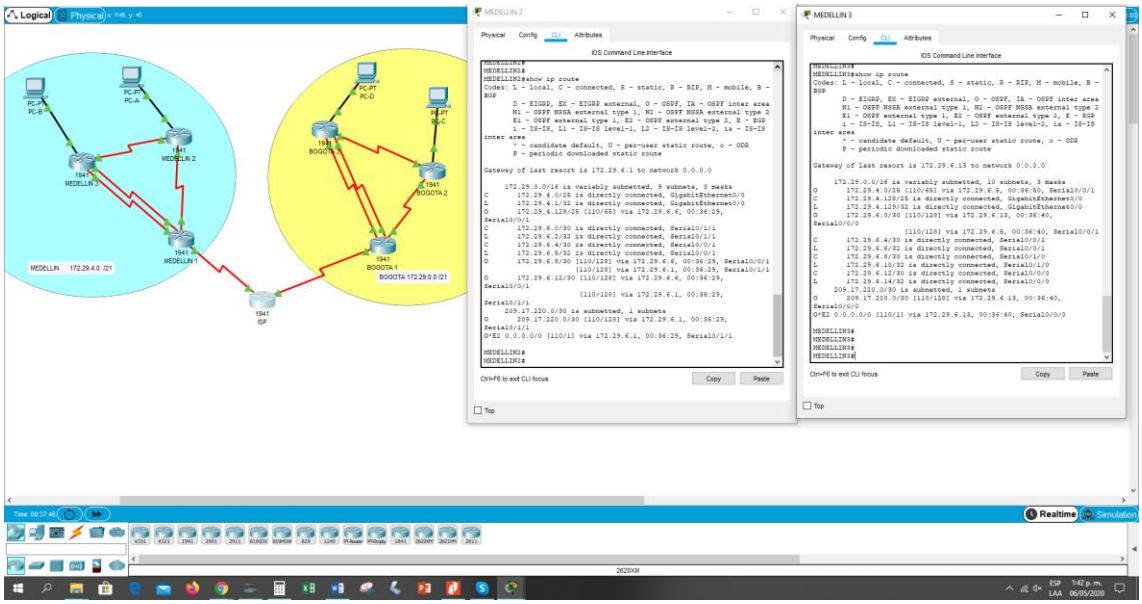


Figura 24. Evidencia verificacion table de enrutamiento

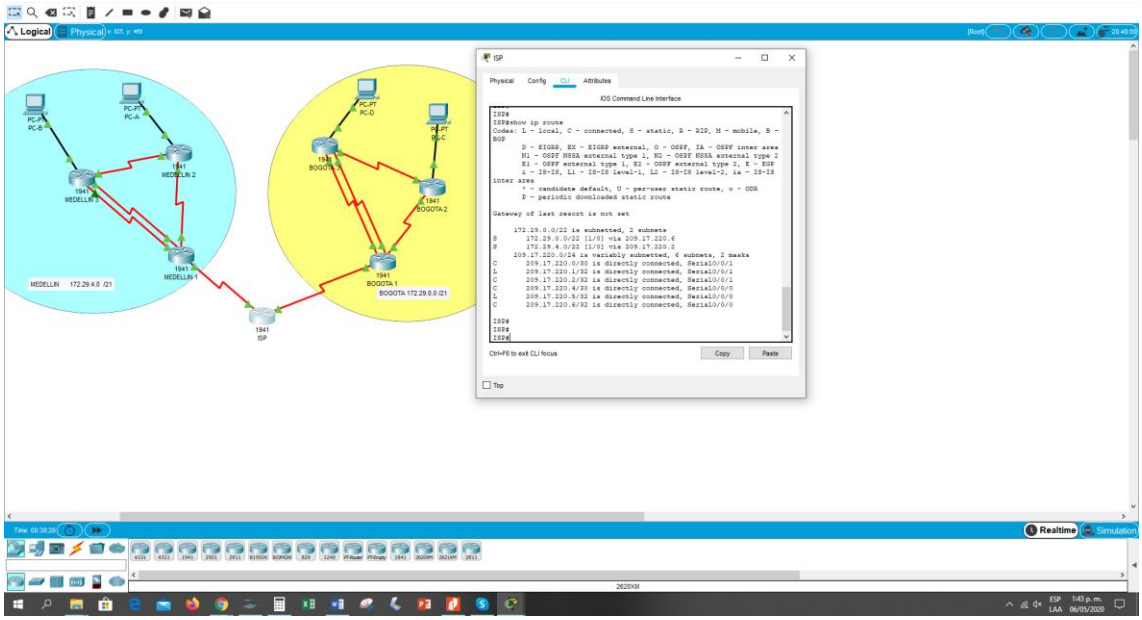


Figura 25. Evidencia verificacion table de enrutamiento

b. Verificar el balanceo de carga que presentan los routers.
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1;

	SERIAL0/1/0
ISP	No lo requiere

Tabla 6. Tabla de deshabilitacion protocolo OSPF Escenario 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.

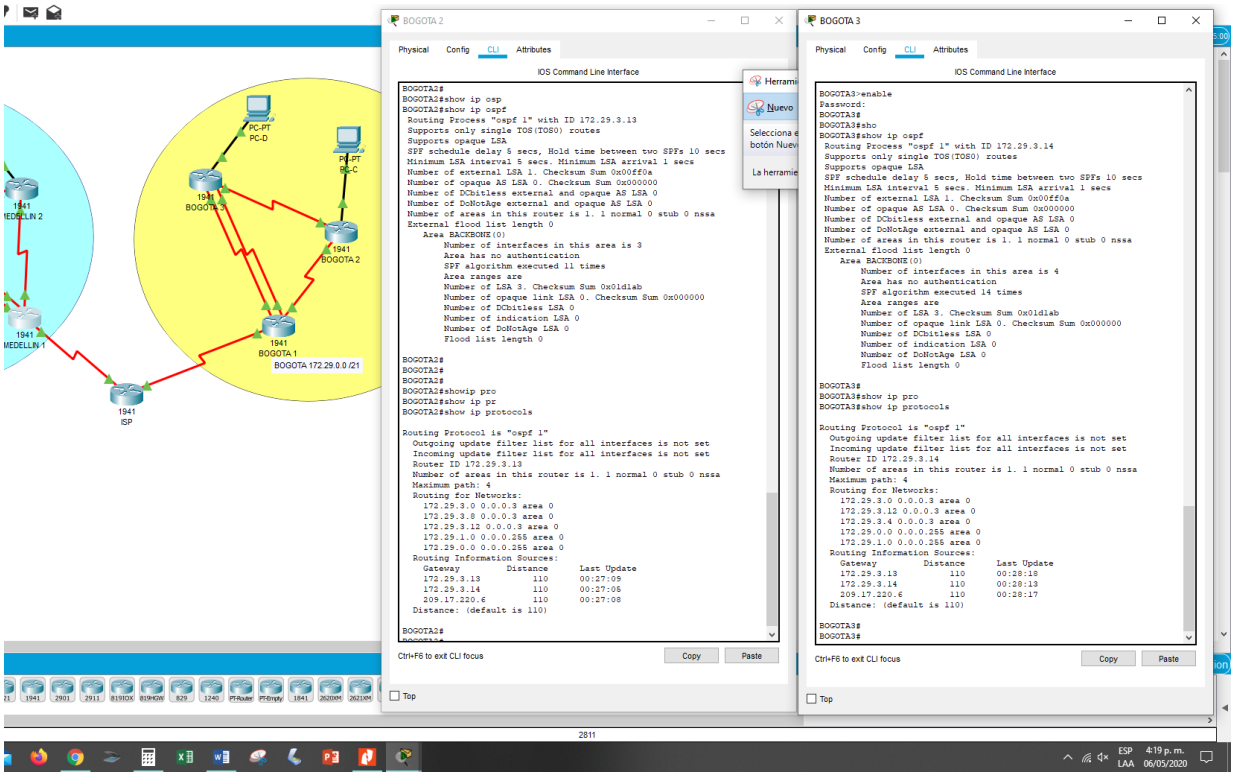


Figura 26. Evidencia verificacion del comando para evidenciar el enrutamiento

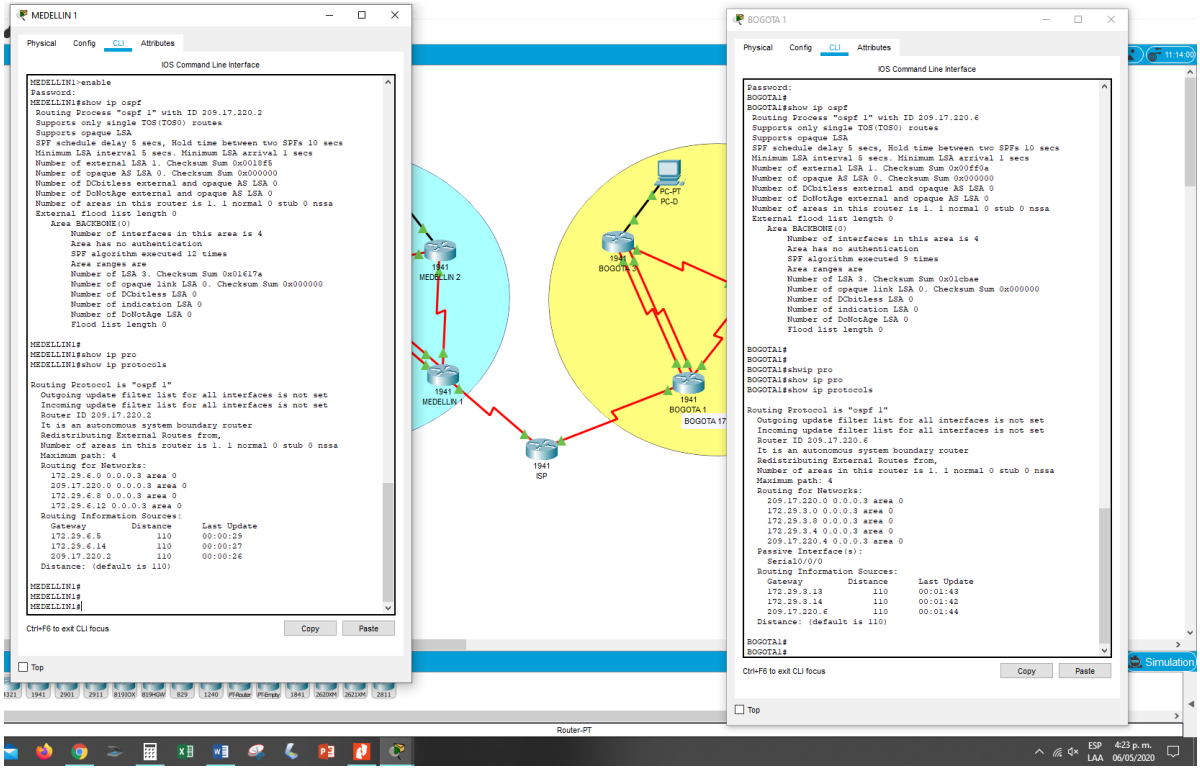


Figura 27. Evidencia verificacion del comando para evidenciar el enrutamiento

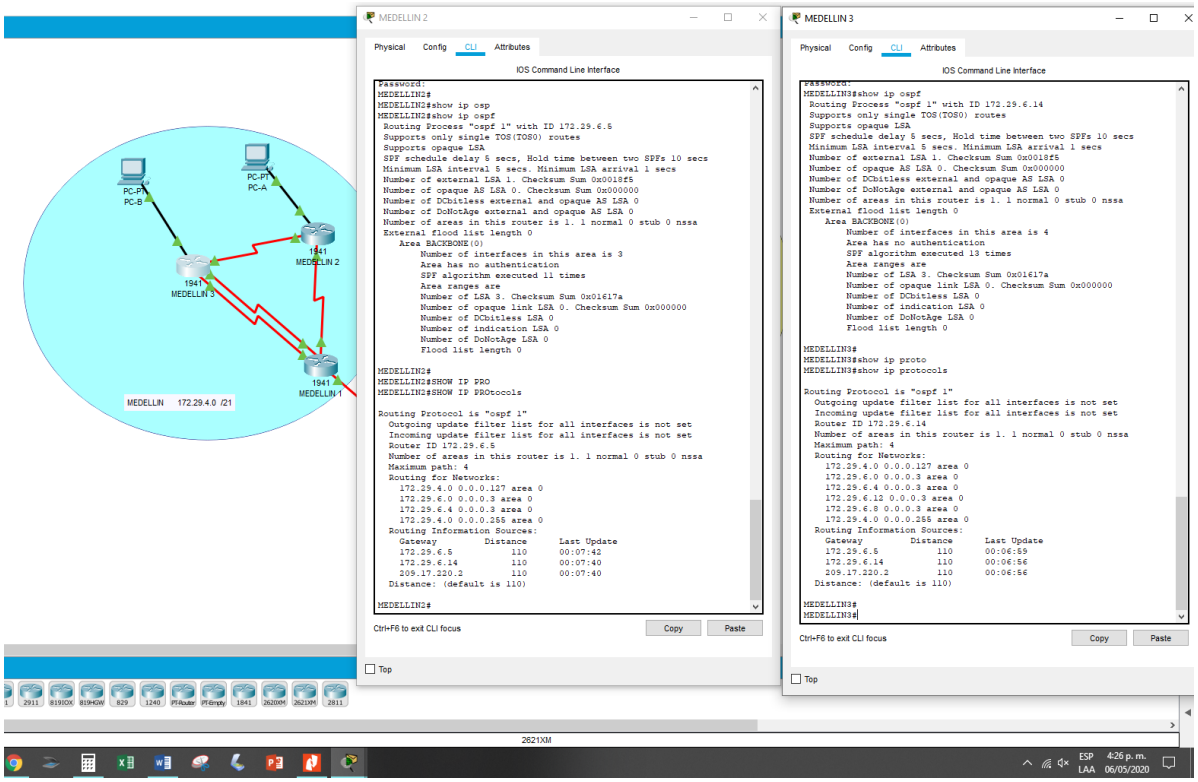


Figura 28. Evidencia verificacion del comando para evidenciar el enrutamiento

Las interfaces que participan de la publicación entre otros datos.

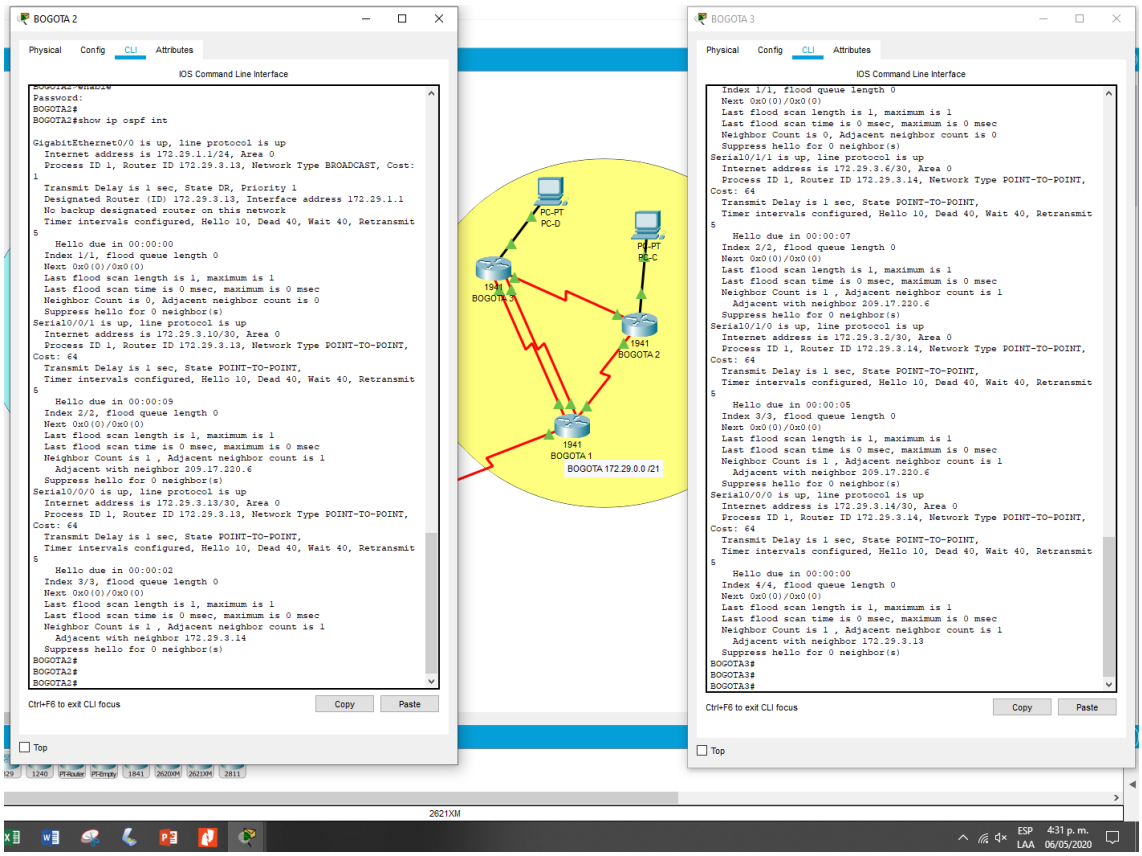


Figura 29. Evidencia participacion de las interfaces en los dispositivos

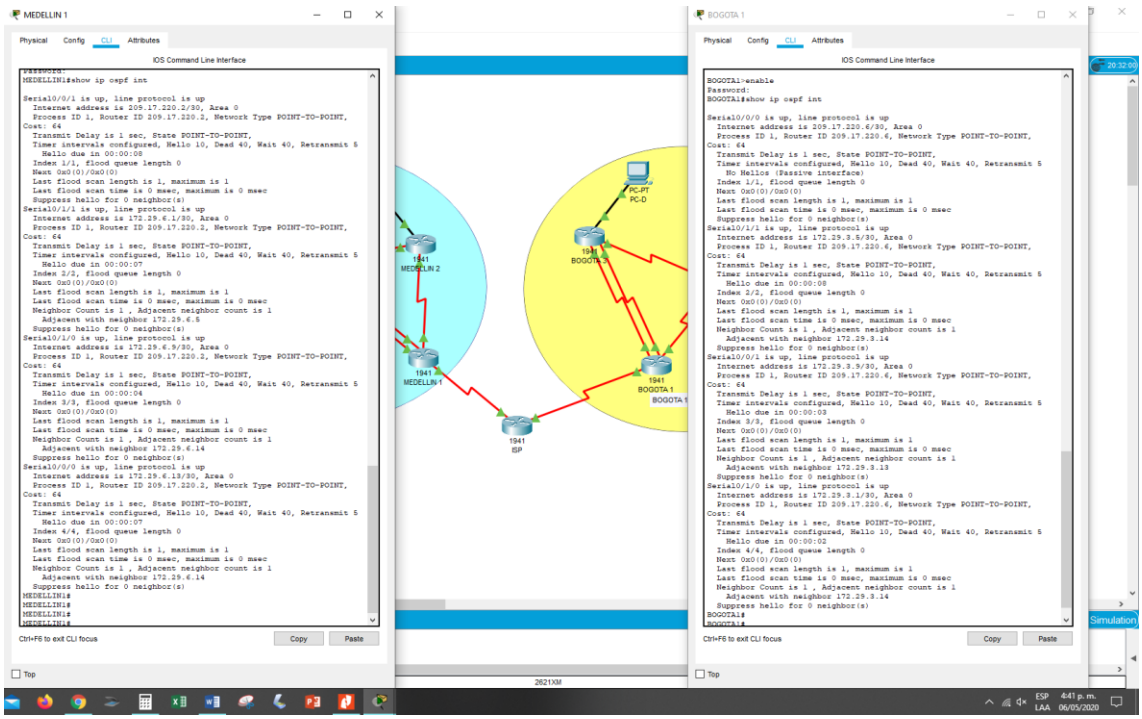


Figura 30. Evidencia participacion de las interfaces en los dispositivos

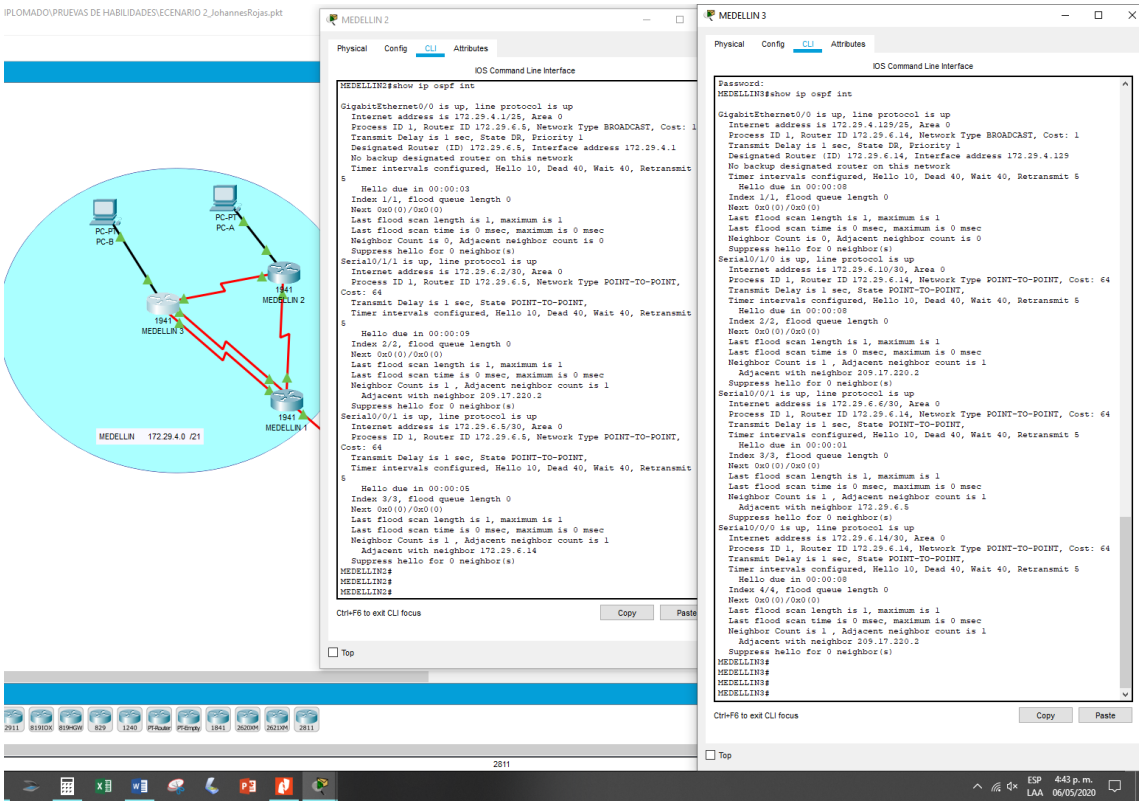


Figura 31. Evidencia participacion de las interfaces en los dispositivos

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.

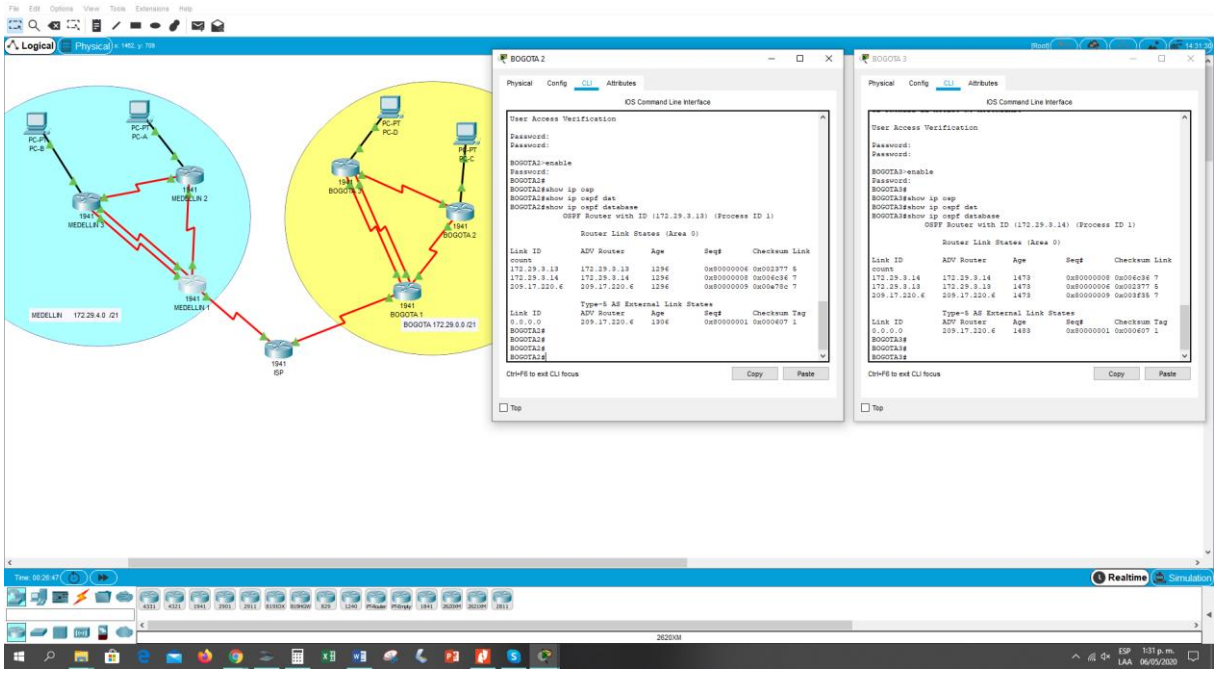


Figura 32. Evidencia verificacion de la base de datos OPSF en los routers

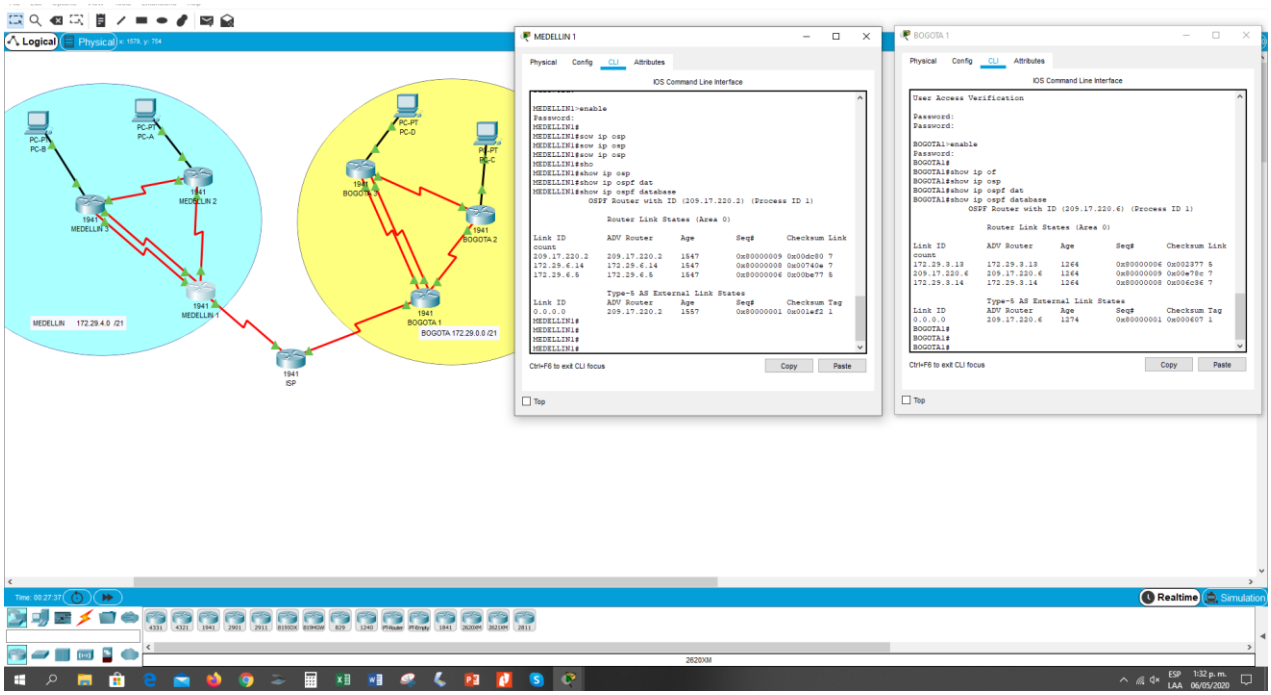


Figura 33. Evidencia verificacion de la base de datos OPSF en los routers

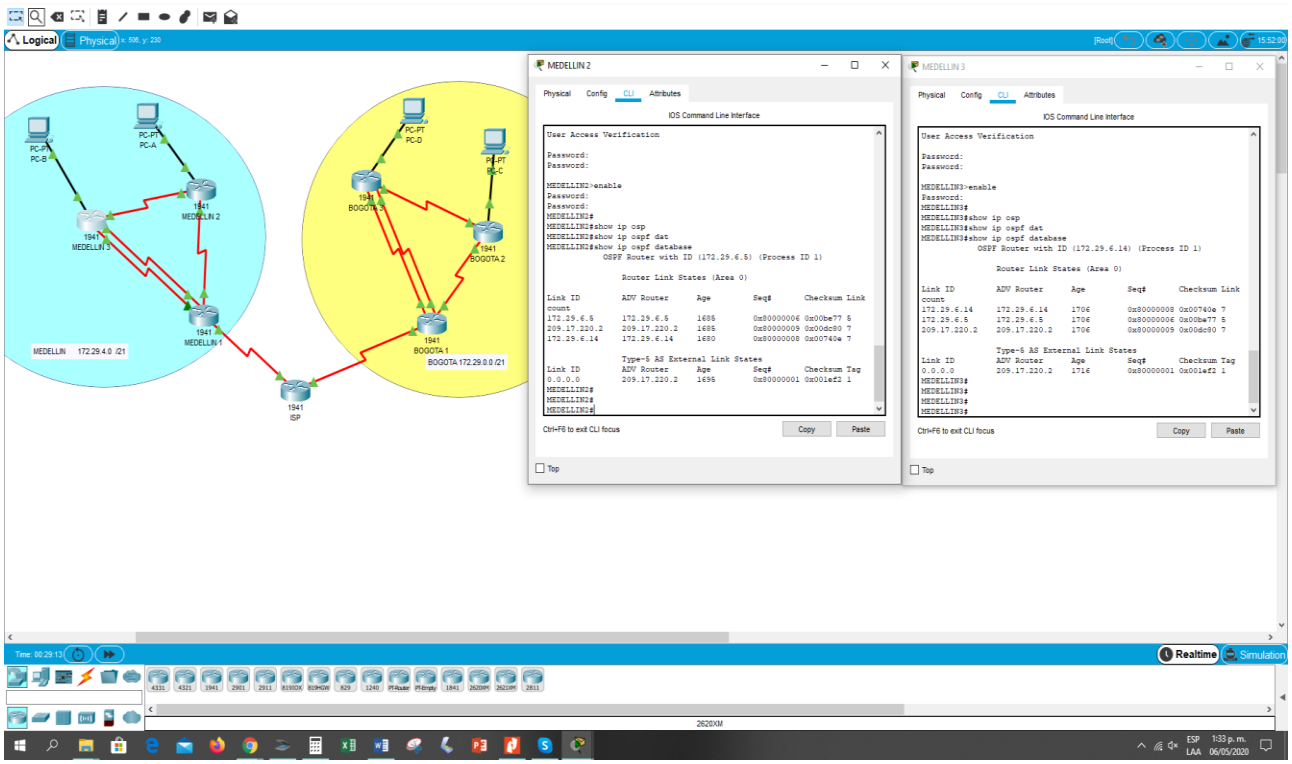


Figura 34. Evidencia verificacion de la base de datos OPSF en los routers

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
MEDELLIN1#config t
MEDELLIN1(config)#username ISP PASSword 12345
MEDELLIN1(config)#INT S0/0/1
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password 12345

ISP#config t
ISP(config)#username MEDELLIN1 password 12345
ISP(config)#interface s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password 12345
```

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

```
BOGOTA1#config t
BOGOTA1(config)#username ISP password 12345
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
ISP#config t
ISP(config)#username BOGOTA1 password 12345
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
```

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.

El caso de NAT con sobrecarga o PAT emplamos los siguientes comandos en cada uno de los router externos

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

MEDELLIN1#show ip nat translations

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

BOGOTA1

```
BOGOTA1#config t
BOGOTA1(config)#access-list 10 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#ip nat inside source list 10 int s0/0/0 overload
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
```

MEDELLIN1

```
MEDELLIN1#config t
MEDELLIN1(config)#access-list 10 permit 172.24.4.0 0.0.3.255
MEDELLIN1(config)#ip nat inside source list 10 int s0/0/1 overload
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat outside
```

Parte 7: Configuración del servicio DHCP.

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

```
MEDELLIN2#config t
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.9
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138

MEDELLIN2(config)#ip dhcp pool MED-SERVIDOR_DHCP
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
```

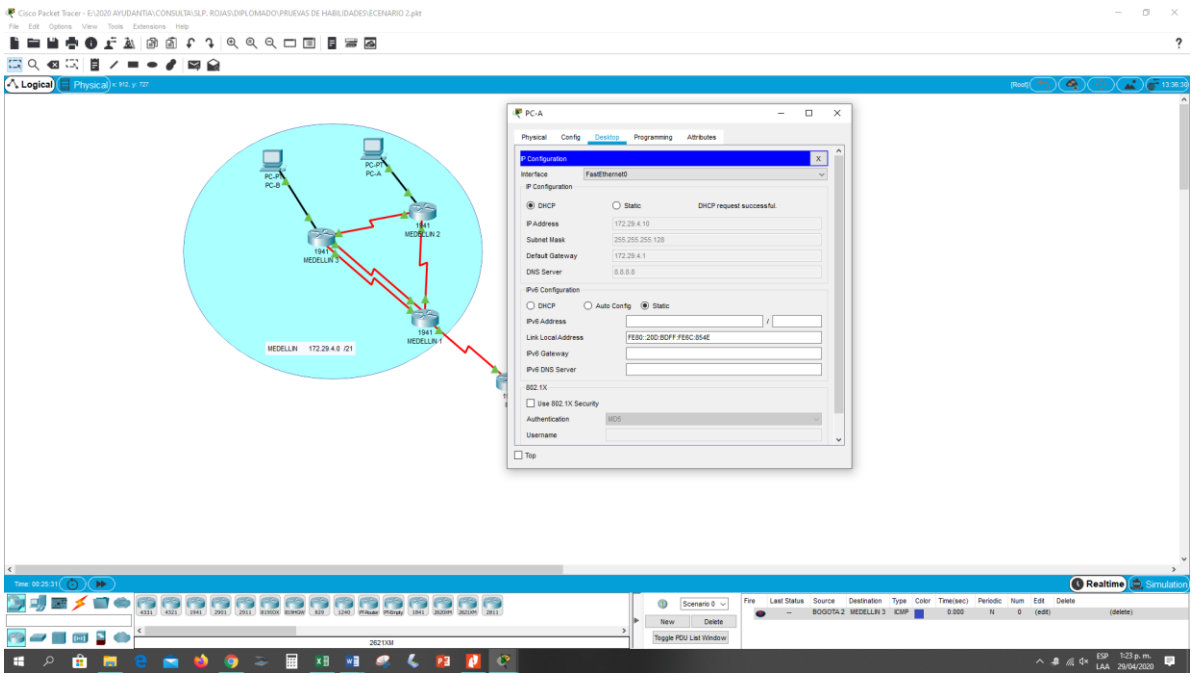


Figura 35. Evidencia funcionamiento servidor DHPC en el PC-A

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

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

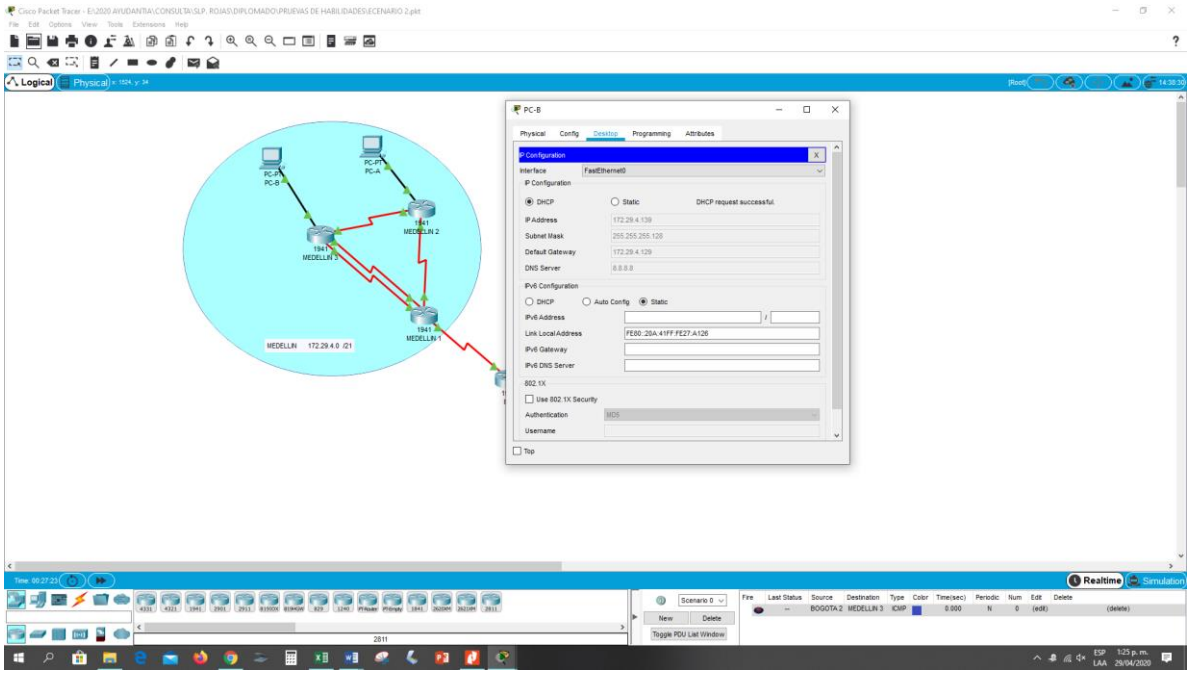


Figura 36. Evidencia funcionamiento servidor DHPC en el PC-B

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

```
BOGOTA2#config t
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10

BOGOTA2(config)#ip dhcp pool BOG-SERVIDOR_DHCP
BOGOTA2(dhcp-config)#NETwork 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#DEfault-router 172.29.4.1
BOGOTA2(dhcp-config)#DNS-server 8.8.8.8
BOGOTA2(dhcp-config)#EXIT

BOGOTA2(config)#ip dhcp pool BOG3-SERVIDOR_DHCP
BOGOTA2(dhcp-config)#NETwork 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#DEfault-router 172.29.4.1
BOGOTA2(dhcp-config)#DNS-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
```

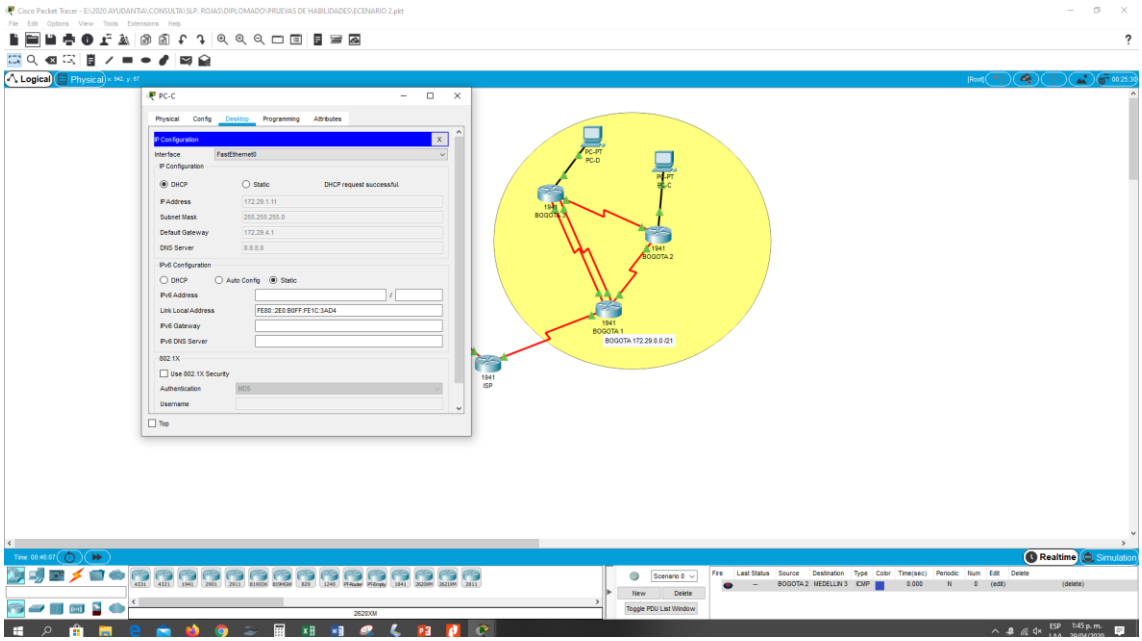


Figura 37. Evidencia funcionamiento servidor DHPC en el PC-C

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

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

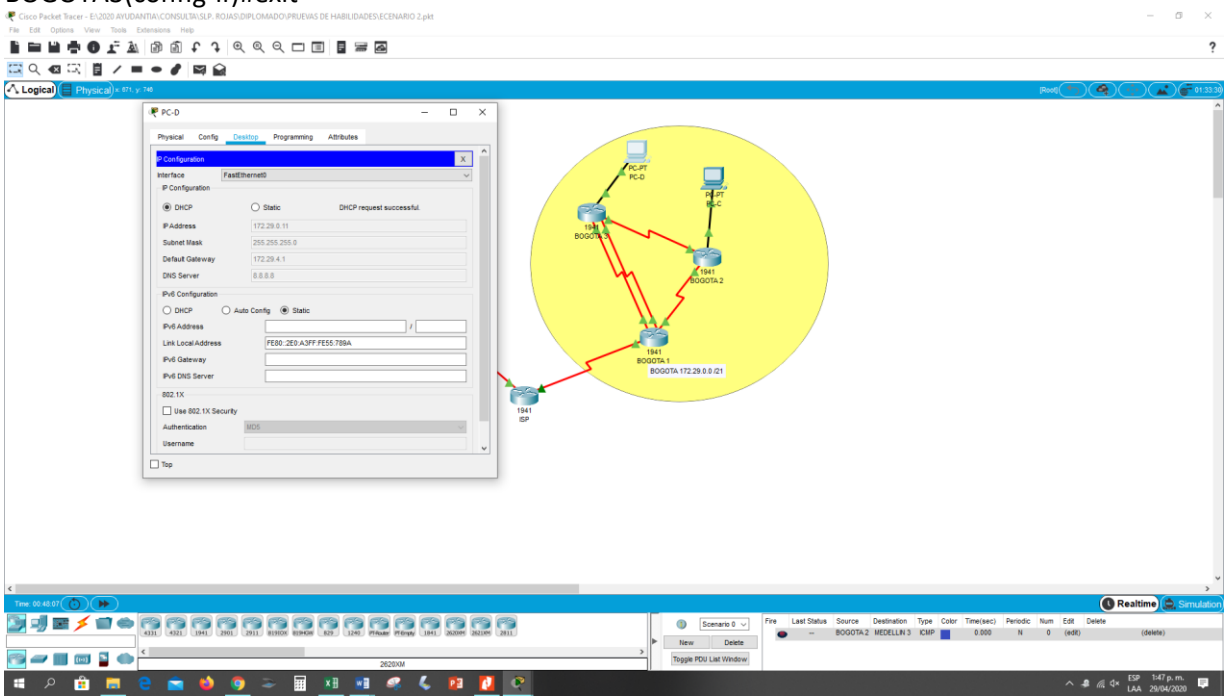


Figura 38. Evidencia funcionamiento servidor DHPC en el PC-D

CONCLUSIONES

- Gracias al empleo de direecionamiento IP en cada uno de los dispositivos de la red, proporcionan conexiones de forma ordenada que ayuda a garantizar el envio y recepción de paquete es de datos.

- Es de vital importancia hacer las configuraciones básicas de seguridad en cada uno de los dispositivos de la red, con el fin de mantener su integridad y correcto funcionamiento.

- En base a los requisitos para el desarrollo de una red , lo primero que se necesita es definir su sucapacidad , cuantas subredes se incluyen y en base a esto aproximar el servicio de red a tantos usuarios como sea posible, preveendo futuras ampliaciones

- La transmicion de datos mediante enrutamiento estatico es mas confiable, esta forma ayuda a garantizar un mejor desempeño de red mitigando la rebundacia.

- Es de buena practica para ell empleo de conexión remota hacer la configuración necesaria para tener activando protocolo SSH, con el fin de fortalecer la seguridad de a red.

- El protocolo RIp es una de los protocolos mas simples de configurar para lograr el enrutameinto de redes, y por tal es mas fácil su implemetacion.

- Con el empleo de DHCP , ayuda a gestionar las administración de direcciones IP encada uno de los dispositivos, para lo cual no se tiene que dedicar gran cantidad de tiempo en esta tarea.

REFERENCIAS

CISCO. (2017). *Asignación de direcciones IP.* Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). *SubNetting*. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). *Capa de Aplicación.* Fundamentosde Networking. Recuperado de ttps://staticcourseassets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). *Soluciones de Red.* Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO.(2017).Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://staticcourseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO SYSTEM. (2017). Capítulo 1. Introducción a redes conmutadas. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#1.0.1.1

CISCO SYSTEM. (2017). Capítulo 2. Configuración y conceptos básicos de switching. Recuperado de https://staticourseassets.s3.amazonaws.com/RSE503/es/index.html#2.0.1.1

CISCO SYSTEM. (2017). Capítulo 9. Listas decontrol de acceso. Recuperado de https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1.1

CISCO SYSTEM. (2017). Capítulo 10. DHCP.Recuperado de https://staticourseassets.s3.amazonaws.com/RSE503/es/index.html#10.0.1.1