

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

JAIRO ERNESTO CORREALES RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C

2020

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

JAIRO ERNESTO CORREALES RODRÍGUEZ

Trabajo de diplomado presentado para obtener el título de:
INGENIERO ELECTRÓNICO

Tutor:
Msc. HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C

2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá 15 de mayo de 2020

Dedico este diplomado a mis padres Javier y Mery, a mis hermanos quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más.

AGRADECIMIENTOS

Le agradezco a Dios, familia y amigos por haberme acompañado y guiado a lo largo de mi carrera por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y mucha felicidad.

TABLA DE CONTENIDO

1. INTRODUCCIÓN	11
2. OBJETIVOS	12
2.1 Objetivo general.....	12
2.1 Objetivos específico.....	12
3. PLANTEAMIENTO DEL PROBLEMA	13
3.1 Definición del problema	13
3.2 Justificación	13
4. DESARROLLO DE LOS DOS ESCENARIOS	14
4.1 ESCENARIO 1.....	14
4.1.1 Parte 1: Inicializar dispositivos.....	15
Paso 1: Inicializar y volver a cargar los routers y los switches	15
4.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos	15
Paso 1: Configurar la computadora de Internet	15
Paso 2: Configurar R1	16
Paso 3: Configurar R2.....	17
Paso 4: Configurar R3.....	20
Paso 5: Configurar S1	22
Paso 6: Configurar el S3	23
Paso 7: Verificar la conectividad de la red.....	24
4.1.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	26
Paso 1: Configurar S1	26
Paso 2: Configurar el S3	27
Paso 3: Configurar R1	28
Paso 4: Verificar la conectividad de la red.....	29
4.1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2	32
Paso 1: Configurar RIPv2 en el R1.....	32
Paso 2: Configurar RIPv2 en el R2.....	33
Paso 3: Configurar RIPv2 en el R3.....	34
Paso 4: Verificar la información de RIP	35

4.1.5 Parte 5: Implementar DHCP y NAT para IPv4	37
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	37
Paso 2: Configurar la NAT estática y dinámica en el R2	38
Paso 3: Verificar el protocolo DHCP y la NAT estática.....	39
4.1.6 parte 6: Configurar NTP.....	42
4.1.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	43
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	43
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	45
4.2 Escenario 2.....	49
4.2.1 Parte 1: Configuración del enrutamiento.....	50
4.2.2 Parte 2: Tabla de Enrutamiento	59
4.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.....	65
4.2.4 Parte 4: Verificación del protocolo OSPF.....	66
4.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP	70
4.2.6 Parte 6: Configuración de PAT.	71
4.2.7 Parte 7: Configuración del servicio DHCP.	73
5. CONCLUSIONES.....	75
6. REFERENCIAS BIBLIOGRÁFICAS	76

LISTA DE FIGURAS

Figura 1. Topología indicada para la configuración.....	14
Figura 2. Ping desde R1 a R2-S0/0/0	25
Figura 3. Ping desde R2 a R3- S0/0/1	25
Figura 4. Ping PC de Internet a Gateway predeterminado.....	26
Figura 5. Ping desde S1 a R1-dirección VLAN 99	30
Figura 6. Ping desde S3 a R1-dirección VLAN 99	31
Figura 7. Ping desde S1 a R1-dirección VLAN 21	31
Figura 8. Ping desde S3 a R1-dirección VLAN 23	32
Figura 9. Comando show ip protocols.....	36
Figura 10. Comando show ip route ospf	36
Figura 11. Comando show running-config	37
Figura 12. PC-A Ok - DHCP adquirido correctamente	40
Figura 13. PC-C Ok - DHCP adquirido correctamente	41
Figura 14. El ping PC-A a PC-C ha sido satisfactorio	41
Figura 15. El navegador al acceder pide tiempo fuera	42
Figura 16. El ACL funciona, se realiza telnet a la dirección de R2 y funciona perfecto.	44
Figura 17. Comando R2#show access-lists	46
Figura 18. Comando R2#clear ip access-list counters	46
Figura 19. Comando R2#show running-config.....	47
Figura 20. Comando R2#show ip nat translations.....	47
Figura 21. Comando R2#clear ip nat translation *	48
Figura 22. Topología de red.....	49
Figura 23. Conexión física de los equipos con base en la topología de red.....	50
Figura 24. Ping en la red de MEDELLIN: Desde PC-A a PC-B.....	57
Figura 25. Ping en la red de BOGOTA: Desde PC-C a PC-D.....	57
Figura 26. Ping de PC-A a Router ISP.....	59
Figura 27. Ping de PC-B a Router ISP.....	59
Figura 28. Ping de PC-C a Router ISP.....	60
Figura 29. Ping de PC-D a Router ISP.....	60
Figura 30. MEDELLIN-1#show ip route.....	61
Figura 31. BOGOTA-1#show ip route	61
Figura 32. MEDELLIN-2#show ip route.....	62
Figura 33. BOGOTA-2#show ip route	62
Figura 34. MEDELLIN-3#show ip route.....	63
Figura 35. BOGOTA-3#show ip route	63
Figura 36. ISP#show ip route.....	64
Figura 37. MEDELLIN-1#show ip protocols	66
Figura 38. MEDELLIN-2#show ip protocols	66
Figura 39. MEDELLIN-3#show ip protocols	67
Figura 40. BOGOTA-1#show ip protocols.....	67
Figura 41. BOGOTA-2#show ip protocols.....	68
Figura 42. BOGOTA-3#show ip protocols.....	68

LISTA DE TABLAS

Tabla 1. Inicializar Routers y Switches.....	15
Tabla 2. Configurar la computadora de Internet.....	16
Tabla 3. Configurar R1.....	16
Tabla 4. Configurar R2.....	18
Tabla 5. Configurar R3.....	20
Tabla 6. Configurar S1.....	22
Tabla 7. Configurar el S3.....	23
Tabla 8. Verificar la conectividad de la red.....	24
Tabla 9. Configurar S1.....	26
Tabla 10. Configurar S3.....	27
Tabla 11. Configurar R1.....	29
Tabla 12. Verificar la conectividad de la red.....	30
Tabla 13. Configurar RIPv2 en el R1.....	32
Tabla 14. Configurar RIPv2 en el R2.....	33
Tabla 15. Configurar RIPv2 en el R3.....	34
Tabla 16. Verificar la información de RIP.....	35
Tabla 17. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	37
Tabla 18. Configurar la NAT estática y dinámica en el R2.....	38
Tabla 19. Verificar el protocolo DHCP y la NAT estática.....	39
Tabla 20. Configurar NTP.....	42
Tabla 21. Restringir el acceso a las líneas VTY en el R2.....	43
Tabla 22. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.....	45
Tabla 23. Configuración del enrutamiento.....	50
Tabla 24. Configuración Routers Bogota1 y Medellín-1.....	56
Tabla 25. Sumarización Red Medellín.....	58
Tabla 26. Sumarización Red Bogotá.....	58
Tabla 27. Configuración Router ISP.....	58
Tabla 28. Deshabilitar protocolo OSPF.....	65
Tabla 29. Rutas y puerto de conexión.....	69
Tabla 30. Autenticación PAT.....	70
Tabla 31. Autenticación CHAT.....	71
Tabla 32. Configuración de PAT.....	72
Tabla 33. Configuración del servicio DHCP.....	73
Tabla 34. Configuración del servicio DHCP.....	74

RESUMEN

El presente trabajo muestra el desarrollo de las actividades llevadas a cabo durante el diplomando de profundización cisco diseño e implementación de soluciones integradas LAN / WAN, lo cual permite planificar, implementar, verificar y solucionar problemas de redes. El desarrollo de este diplomado permite establecer la importancia sobre los niveles de seguridad y los conocimientos necesarios para el diseño de redes, así como la incorporación de tecnologías y protocolos de comunicación.

PALABRAS CLAVE: Diplomado, Cisco, Casos de estudio

1. INTRODUCCIÓN

Las redes de datos son de gran importancia ya que permiten que cada persona pueda transmitir y adquirir información dentro de su área correspondiente, la seguridad es una parte vital dentro de las redes de datos, la cual recae sobre los administradores de red, los cuales permiten la autorización y privilegios a cada uno de los usuarios.

Las redes de datos nos permiten unir distintos dispositivos informáticos, los cuales realizan un intercambio de datos por medio de conexiones alámbricas e inalámbricas, la red LAN está compuesta por dispositivos informáticos con bastante proximidad y suelen compartir el mismo módem, enrutador y conexión a Internet, por otro lado, la red WAN comprende un grupo de redes de área local que por lo general se extiende por un área geográfica extensa.

El presente trabajo muestra el desarrollo de dos actividades prácticas como prueba de habilidades del diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN), en el desarrollo de los escenarios se presenta un informe con los pasos a seguir para llevar a cabo enrutamiento, aplicación de los parámetros de seguridad en Routers y Switch, configuraciones OSPF, RIP ver 2.0, implementación DHCP, NAT, verificación de ACL.

2. OBJETIVOS

2.1 OBJETICO GENERAL

- Implementar diferentes topologías que permitan soportar diferentes servicios en las redes de telecomunicaciones.

2.1 OBJETIVOS ESPECIFICO

- Configurar una red que permita dar solución al escenario 1, cumpliendo con las condiciones de conectividad, protocolos y configuración de equipos.
- Proponer una solución para el escenario 2, realizando la configuración e interconexión de equipos acorde con lineamientos y a la topología de la red.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Plantear la solución de dos estudios de caso bajo el uso de tecnología cisco haciendo uso de todos los conocimientos adquiridos dura el diplomado de pronunciación Cisco.

3.2 JUSTIFICACIÓN

Llevar acabo la solución de los dos casos de estudio bajos el uso de la tecnología cisco, además de cumplir con el requisito para adquirir el título profesional, nos plantea un escenario real y nos prepara para el desarrollo de nuestras actividades laborales futuras, así como también pone a prueba todos nuestro conocimiento adquiridos duran el desarrollo del diplomado de profundización cisco, diseño e implementación de soluciones integradas LAN / WAN

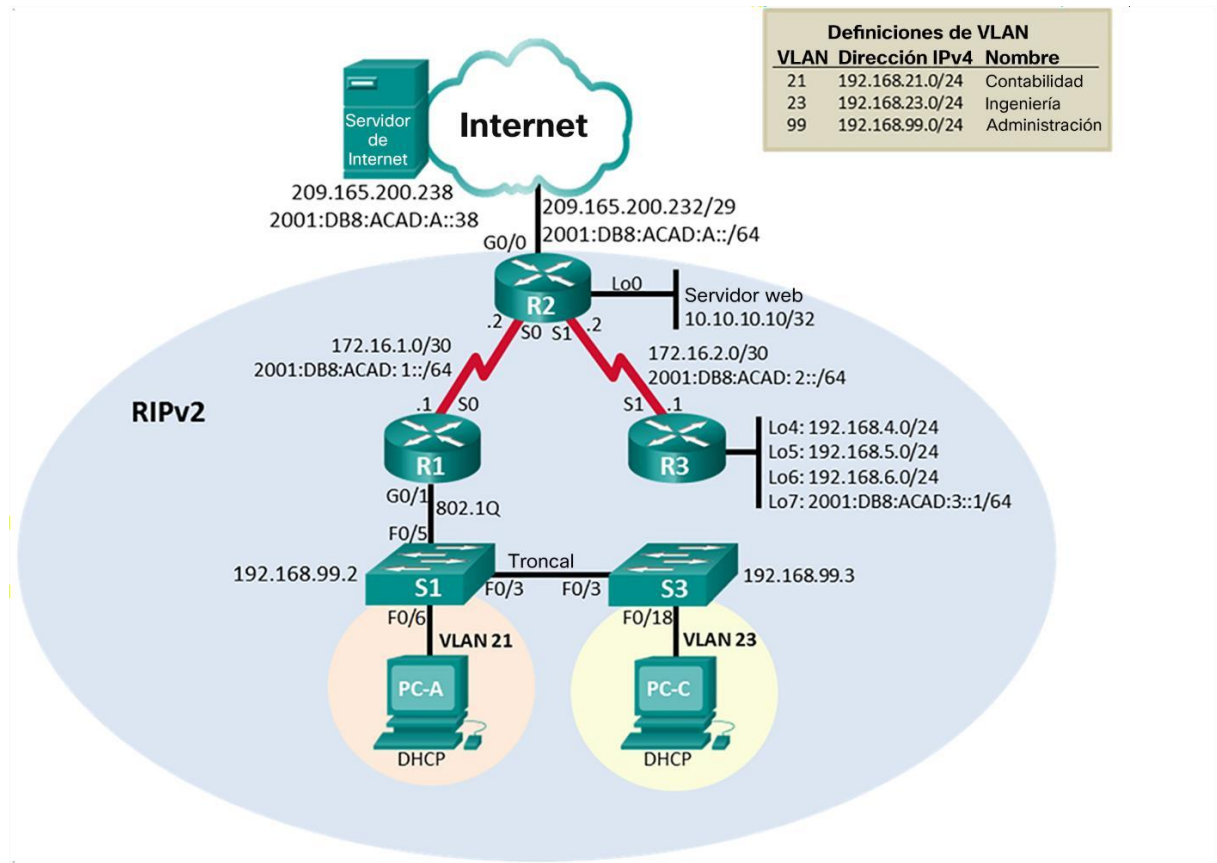
4. DESARROLLO DE LOS DOS ESCENARIOS

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.

Topología

Figura 1. Topología indicada para la configuración



4.1.1 PARTE 1: INICIALIZAR DISPOSITIVOS

PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Se llevan a cabo las configuraciones de inicio y se vuelven a cargar los dispositivos, se solicita al instructor que verifique la inicialización de los dispositivos, así como lo indica la tabla 1.

Tabla 1. Inicializar Routers y Switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	R1#erase startup-config R2#erase startup-config R3#erase startup-config
Volver a cargar todos los routers	R1#reload R2#reload R3#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	S1#erase startup-config S3#erase startup-config S1#delete vlan.dat S3#delete vlan.dat
Volver a cargar ambos switches	S1#reload S3#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	S1#dir flash: S3#dir flash:

4.1.2 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

PASO 1: CONFIGURAR LA COMPUTADORA DE INTERNET

Se configura el servidor de Internet incluyendo las tareas indicadas en la tabla 2, se consulta la topología de la red para obtener información de las direcciones IP.

Tabla 2. Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
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

Se realiza la configuración para el Router R1 teniendo en cuenta las siguientes tareas indicadas en la tabla 3:

Tabla 3. Configurar R1

Elemento o tarea de configuración	Especificación
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 password class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit

Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)# banner motd " Se prohíbe el acceso no autorizado!"
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config)#description connetion to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#ipv6 unicast-routing R1(config)#interface serial 0/0/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no se configura G0/1.

PASO 3: CONFIGURAR R2

Se realiza la configuración del Router R2 teniendo en cuentas las siguientes tareas indicadas en la tabla 4:

Tabla 4. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	R2(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable password class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server % Invalid input detected at '^' marker.
Mensaje MOTD	R2(config)#service password-encryption

<p>Interfaz S0/0/0</p>	<pre> R2(config)#interface serial 0/0/0 R2(config)#description connetion to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/0 R2(config)#description connetion to R1 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit </pre>
<p>Interfaz S0/0/1</p>	<pre> R2(config)#interface serial 0/0/1 R2(config)#description connetion to R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#interface serial 0/0/1 R2(config)#description connetion to R3 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit </pre>

Interfaz G0/0 (simulación de Internet)	<pre> R2(config)#interface gigabitEthernet 0/0 R2(config)#description connetion to ISP R2(config-if)#ip address 209.165.200.233 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#interface gigabitEthernet 0/0 R2(config)#description connetion to ISP R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown </pre>
Interfaz loopback 0 (servidor web simulado)	<pre> R2(config)#interface gigabitEthernet 0/1 R2(config)#description connetion to Web Server R2(config-if)#ip address 10.10.10.1 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#exit </pre>
Ruta predeterminada	<pre> R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 </pre>

PASO 4: CONFIGURAR R3

Se realiza la configuración del Router R3 incluyendo las siguientes tareas indicadas en la tabla 5:

Tabla 5. Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup

Nombre del router	R3(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable password class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)# banner motd "Unauthorized access is prohibited!"
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config)#description connetion to R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#interface serial 0/0/1 R3(config)#description connetion to R2 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config-if)#exit

Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 7	R3(config)#ipv6 unicast-routing R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::2/64 R3(config-if)#no shutdown
Rutas predeterminadas	

PASO 5: CONFIGURAR S1

Se realiza la configuración del Switch S1 incluyendo las siguientes tareas incluidas en la tabla 6:

Tabla 6. Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del switch	S1(config)#hostname S1

Contraseña de exec privilegiado cifrada	S1(config)#enable password class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)# banner motd "Unauthorized access is prohibited!"

PASO 6: CONFIGURAR EL S3

Se realiza la configuración del Switch S3 incluyendo las siguientes tareas indicadas en la tabla 7:

Tabla 7. Configurar el S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	S3(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable password class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit

Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)# banner motd "Unauthorized access is prohibited!"

PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED

Se utiliza el comando ping para probar la conectividad entre los dispositivos de red, además se utiliza la tabla 8 para verificar metódicamente la conectividad con cada dispositivo de red. En el caso de que la conectividad falle se tomarán medidas correctivas para establecer la conectividad.

Tabla 8. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	El ping ha sido satisfactorio. Ver figura 2.
R2	R3, S0/0/1	172.16.2.2	El ping ha sido satisfactorio. Ver figura 3.
PC de Internet	Gateway predeterminado	209.165.200.233	El ping ha sido satisfactorio. Ver figura 4.

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

Figura 2. Ping desde R1 a R2-S0/0/0.

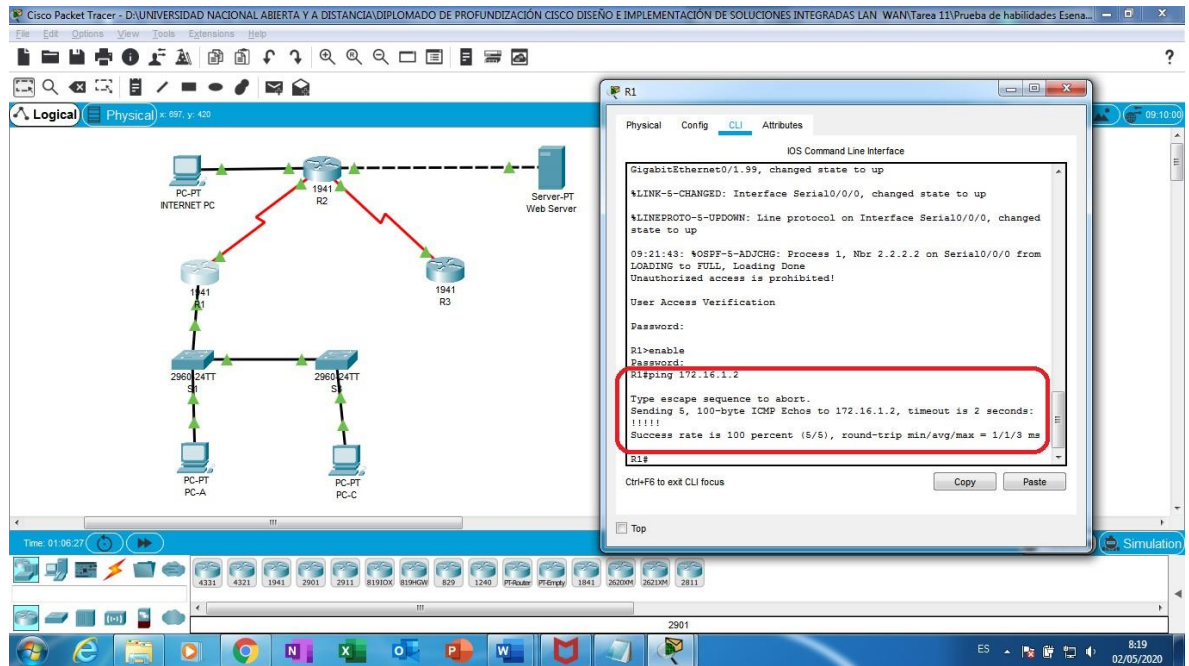


Figura 3. Ping desde R2 a R3- S0/0/1

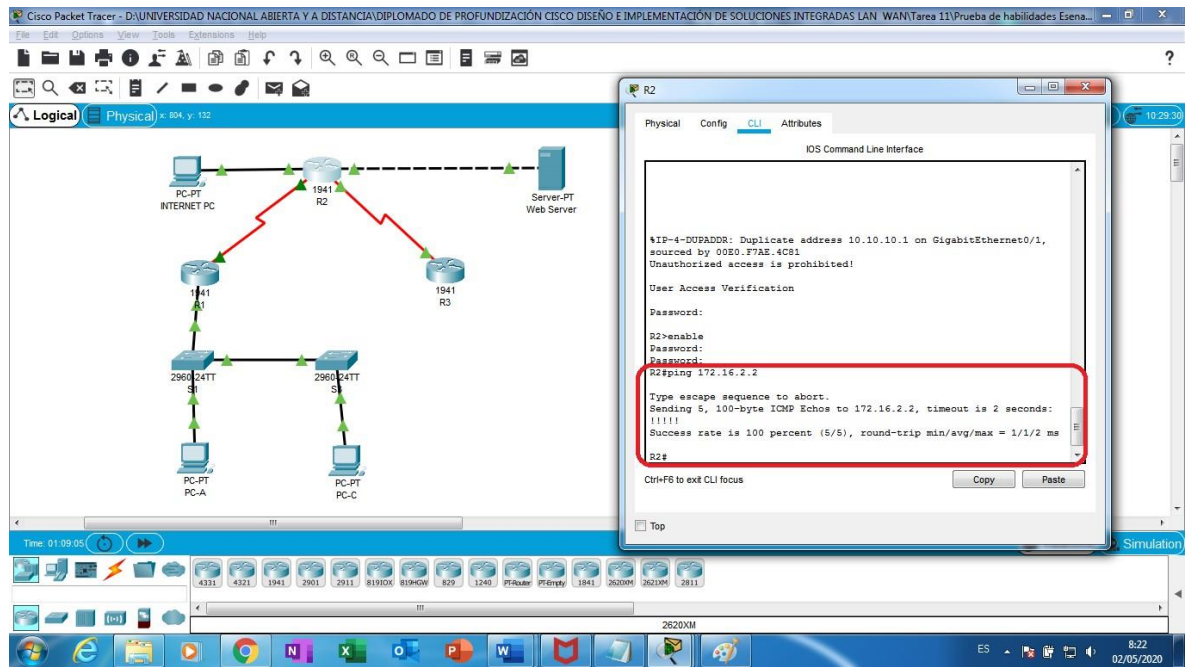
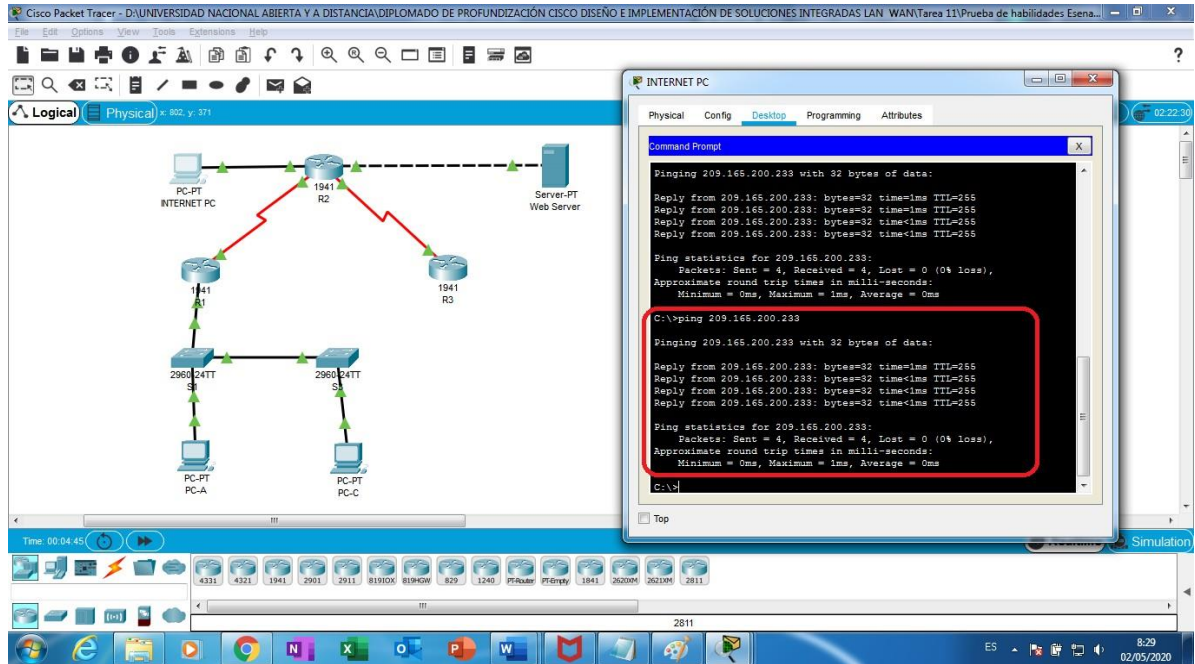


Figura 4. Ping PC de Internet a Gateway predeterminado.



4.1.3 PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

PASO 1: CONFIGURAR S1

Se realiza la configuración del Switch S1 incluyendo las siguientes tareas incluidas en la tabla 9:

Tabla 9. Configurar S1

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 23 S1(config-vlan)#name Ingenieria S1(config)#vlan 99 S1(config-vlan)#name Administracion

Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config)#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)#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)##int range fa0/1-2,fa0/4, fa0/6-24,g0/1-2 S1(config-if)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range fa0/1-2,fa0/4, fa0/7-24,g0/1-2 S1(config-if)#shutdown

PASO 2: CONFIGURAR EL S3

Se realiza la configuración del Switch S3 incluyendo las siguientes tareas incluidas en la tabla 10:

Tabla 10. Configurar S3

Elemento o tarea de configuración	Especificación
-----------------------------------	----------------

Crear la base de datos de VLAN	<pre>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</pre>
Asignar la dirección IP de administración	<pre>S3(config)#int vlan 99 S3(config)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown</pre>
Asignar el gateway predeterminado.	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S3(config)#int range fa0/1-2, fa0/4-24,g0/1-2 S3(config-if)#switchport mode access</pre>
Asignar F0/18 a la VLAN 21	<pre>S3(config)#int fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21</pre>
Apagar todos los puertos sin usar	<pre>S3(config)#int range fa0/1-2,fa0/4-17, fa0/19-24,g0/1-2 S3(config-if)#shutdown</pre>

PASO 3: CONFIGURAR R1

Se realiza la configuración para el Router R1 incluyendo las siguientes tareas indicadas en la tabla 11:

Tabla 11. Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<pre>R1(config)#int g0/1.21 R1(config-subif)#description Contabilidad LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0</pre>
Configurar la subinterfaz 802.1Q .23 en G0/1	<pre>R1(config)#int g0/1.23 R1(config-subif)#description Ingenieria LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>R1(config)#int g0/1.99 R1(config-subif)#description Administracion LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0</pre>
Activar la interfaz G0/1	<pre>R1(config)#int g0/1 R1(config-if)#no shutdown</pre>

PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

Se utiliza el comando ping para probar la conectividad entre los Switches y el Router R1, para verificar metódicamente la conectividad con cada dispositivo de red se tiene en cuenta la tabla 12 y en caso de ser necesario se tomarán medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	El ping ha sido satisfactorio. Ver figura 5.
S3	R1, dirección VLAN 99	192.168.99.1	El ping ha sido satisfactorio. Ver figura 6.
S1	R1, dirección VLAN 21	192.168.21.1	El ping ha sido satisfactorio. Ver figura 7.
S3	R1, dirección VLAN 23	192.168.23.1	El ping ha sido satisfactorio. Ver figura 8.

Figura 5. Ping desde S1 a R1-dirección VLAN 99

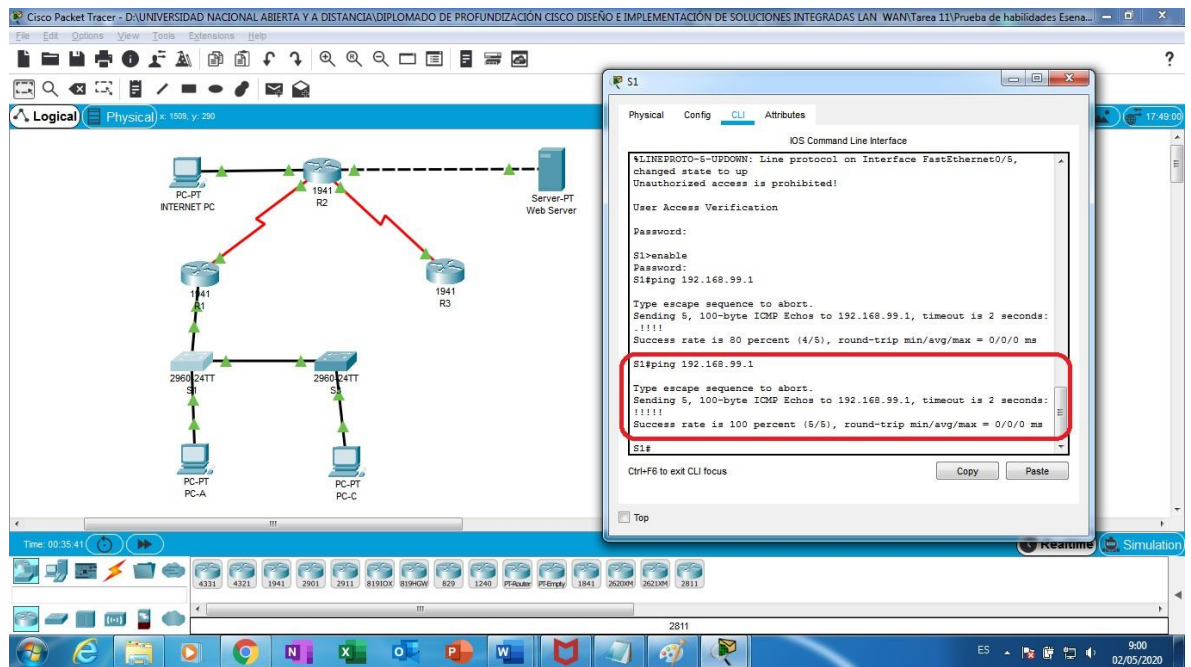


Figura 6. Ping desde S3 a R1-dirección VLAN 99

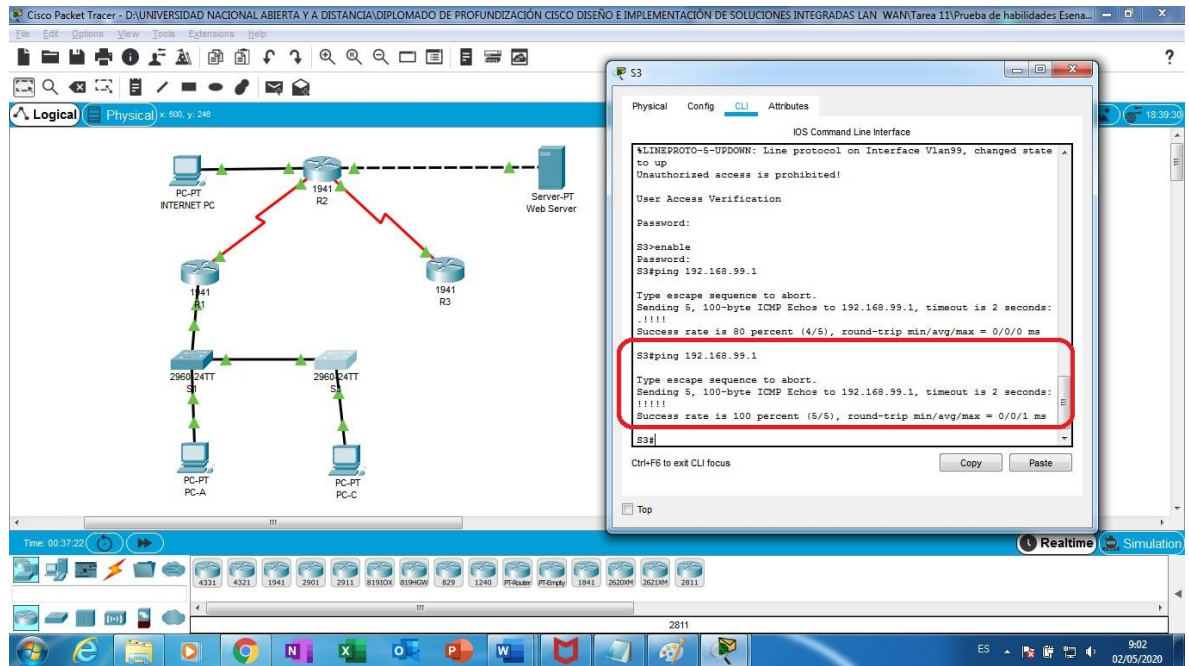


Figura 7. Ping desde S1 a R1-dirección VLAN 21

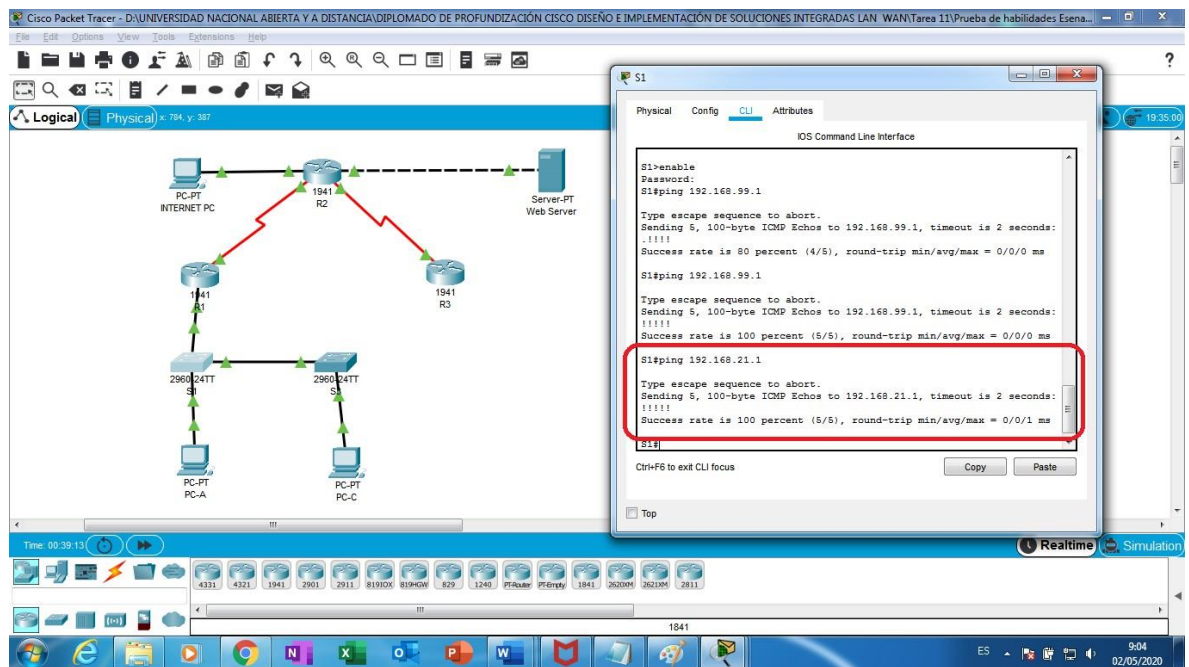
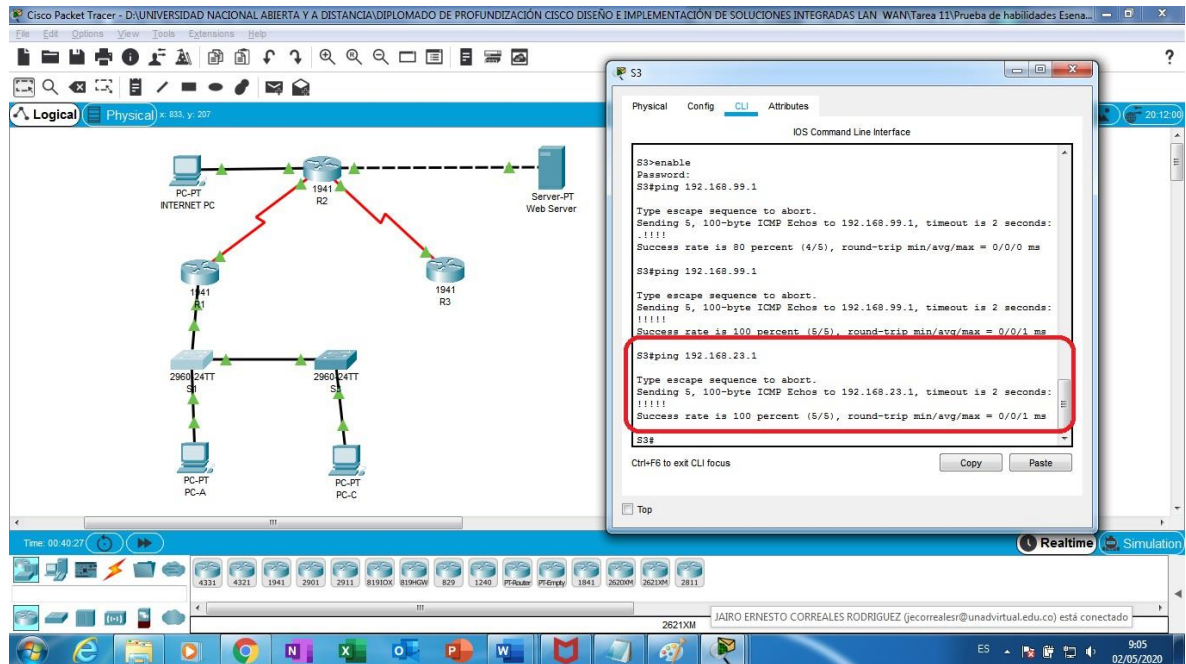


Figura 8. Ping desde S3 a R1-dirección VLAN 23



4.1.4 PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPv2

PASO 1: CONFIGURAR RIPv2 EN EL R1

Se realiza la configuración RIPv2 para el Router 1 incluyendo las siguientes actividades de la tabla 13:

Tabla 13. Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1

Anunciar las redes conectadas directamente	<pre>R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0</pre>
Establecer todas las interfaces LAN como pasivas	<pre>R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99</pre>
Desactive la summarización automática	<pre>R1(config)router rip R1(config-router)#no auto-summary R1(config-router)#exit</pre>

PASO 2: CONFIGURAR RIPv2 EN EL R2

Se realiza la configuración RIPv2 en el Router R2 incluyendo las siguientes tareas de la tabla 14:

Tabla 14. Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<pre>R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2</pre>
Anunciar las redes conectadas directamente	<pre>R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0 0.255 area 0 Nota: Omitir la red G0/0.</pre>

Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1
Desactive la summarización automática.	R2(config)#router rip R2(config-router)#no auto-summary R2(config-router)#exit

PASO 3: CONFIGURAR RIPv2 EN EL R3

Se realiza la configuración de RIPv2 en el Router R3 incluyendo las siguientes tareas de la tabla 15:

Tabla 15. Configurar RIPv2 en el R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.21.0 0.0 0.255 area 0 R3(config-router)#network 192.168.23.0 0.0 0.255 area 0 R3(config-router)#network 192.168.99.0 0.0 0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6

Desactive la summarización automática.	<pre>R3(config)router rip R3(config-router)#no auto-summary R3(config-router)#exit</pre>
----------------------------------------	------------------------------------------------------------------------------------------

PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

Se verifica que RIP esté funcionando correctamente y para esto se introduce los comandos de CLI adecuados para obtener la siguiente información de la tabla 16:

Tabla 16. Verificar la información de RIP

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?	<pre>show ip protocols</pre> <p>Ver figura 9.</p>
¿Qué comando muestra solo las rutas RIP?	<pre>show ip route ospf</pre> <p>Ver figura 10.</p>
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	<pre>show running-config</pre> <p>Ver figura 11.</p>

Figura 9. Comando show ip protocols

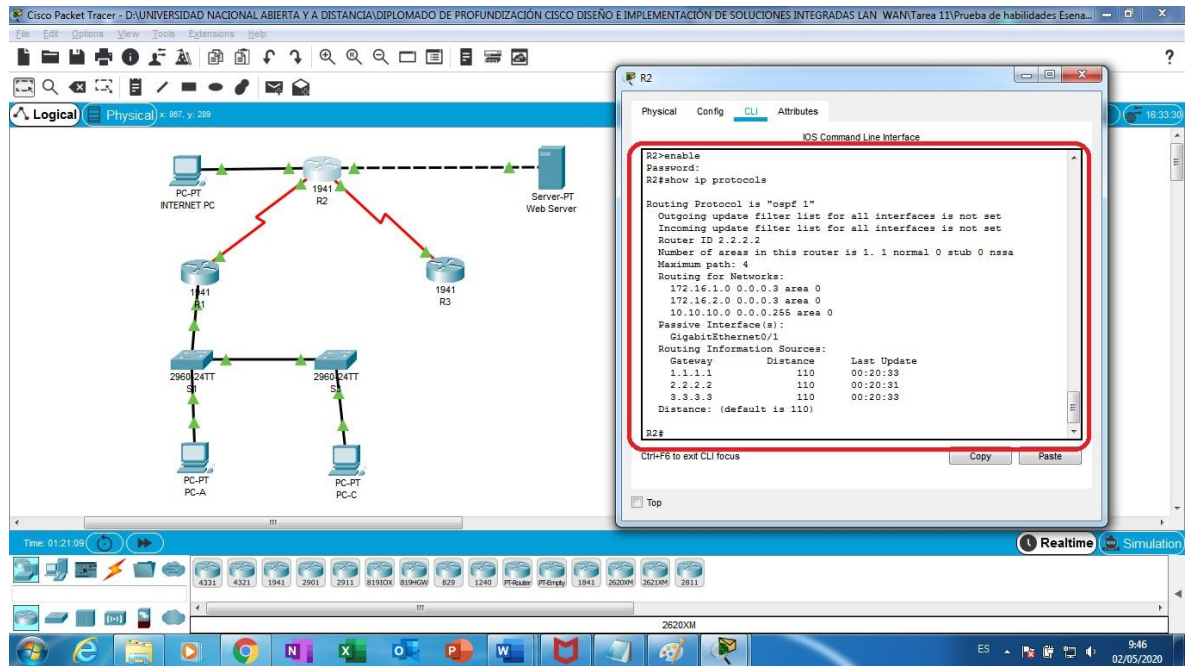


Figura 10. Comando show ip route ospf

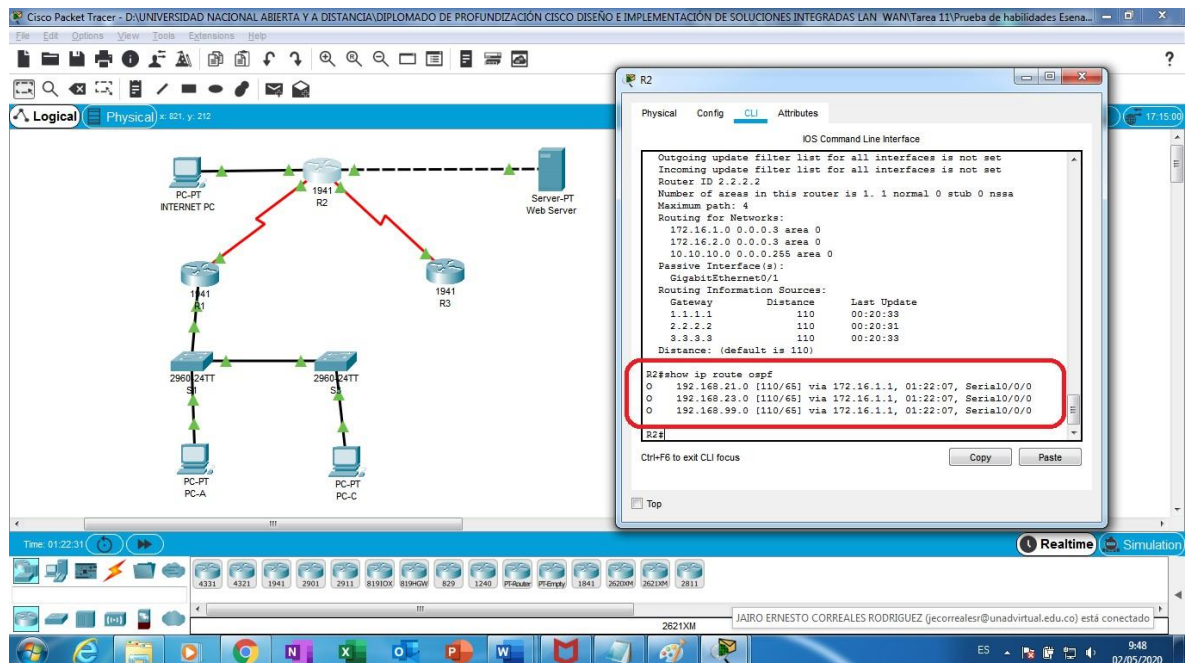
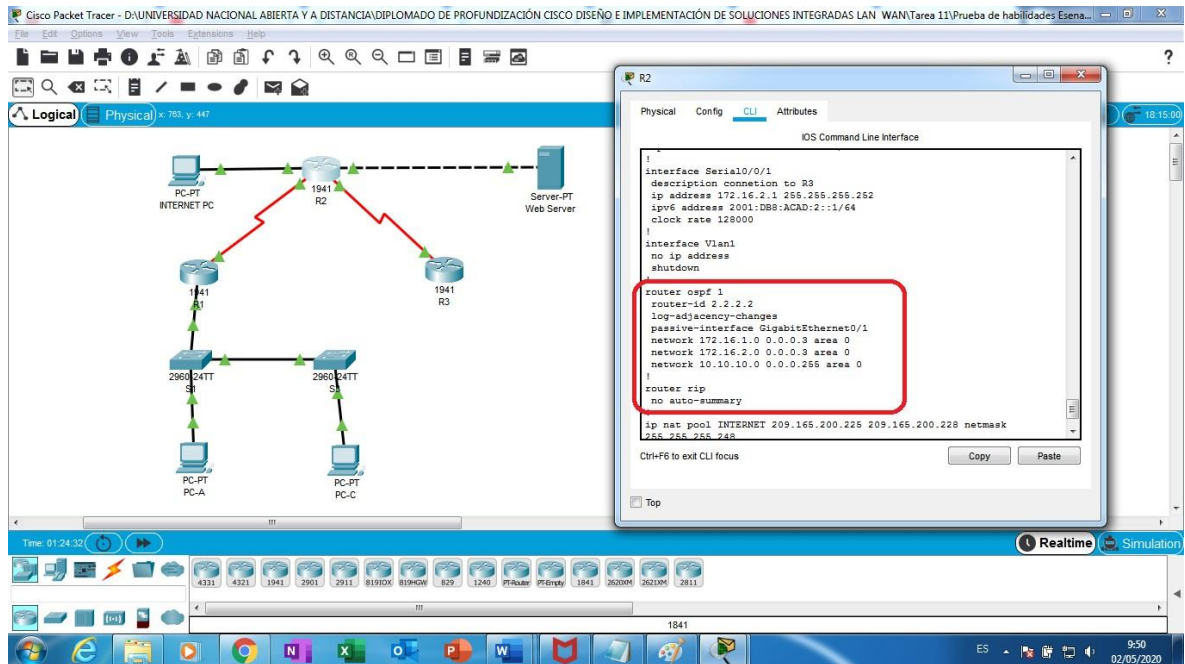


Figura 11. Comando show running-config



4.1.5 PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

Se realiza la configuración para el Router R1 incluyendo las tareas indicadas en la tabla 17:

Tabla 17. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

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 192.168.21.1 192.168.21.10
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.10

Crear un pool de DHCP para la VLAN 21.	<pre>R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0</pre> <p>Nombre de dominio: ccna-sa.com // no soporta el comando</p>
Crear un pool de DHCP para la VLAN 23	<pre>R1(config)#ip dhcp pool ENGR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0</pre> <p>Nombre de dominio: ccna-sa.com // no soporta el comando</p>

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

Se realiza la configuración del Router R2 incluyendo las siguientes tareas indicadas en la tabla 18:

Tabla 18. Configurar la NAT estática y dinámica en el R2

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

Crear una NAT estática al servidor web.	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)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int g0/1 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 209.165.200.225 209.165.200.228 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

Se realizan las tareas indicadas en la tabla 19 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.

Tabla 19. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	PC-A Ok - DHCP adquirido correctamente Ver figura 12.

<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<p>PC-C Ok - DHCP adquirido correctamente Ver figura 13.</p>
<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<p>El ping PC-A a PC-C ha sido satisfactorio Ver figura 14.</p>
<p>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</p>	<p>El navegador al acceder pide tiempo fuera Ver figura 15. webuser y la contraseña cisco12345 // servidor simulado en R2 Packet Tracer no soporta esos comandos</p>

Figura 12. PC-A Ok - DHCP adquirido correctamente

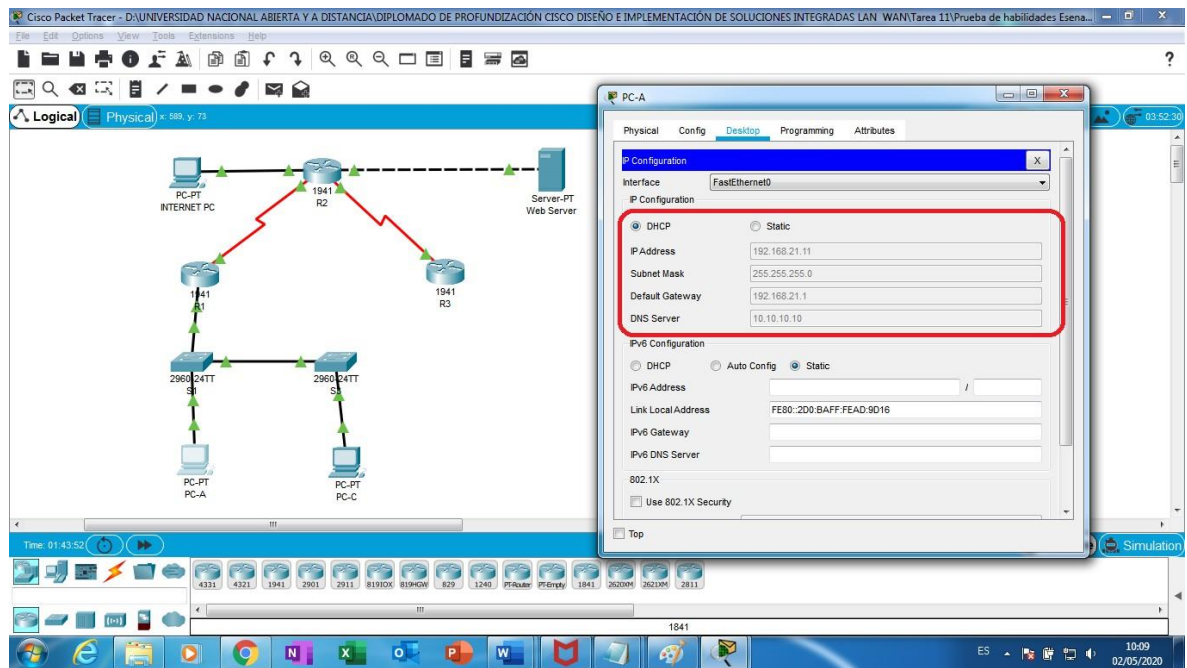


Figura 13. PC-C Ok - DHCP adquirido correctamente

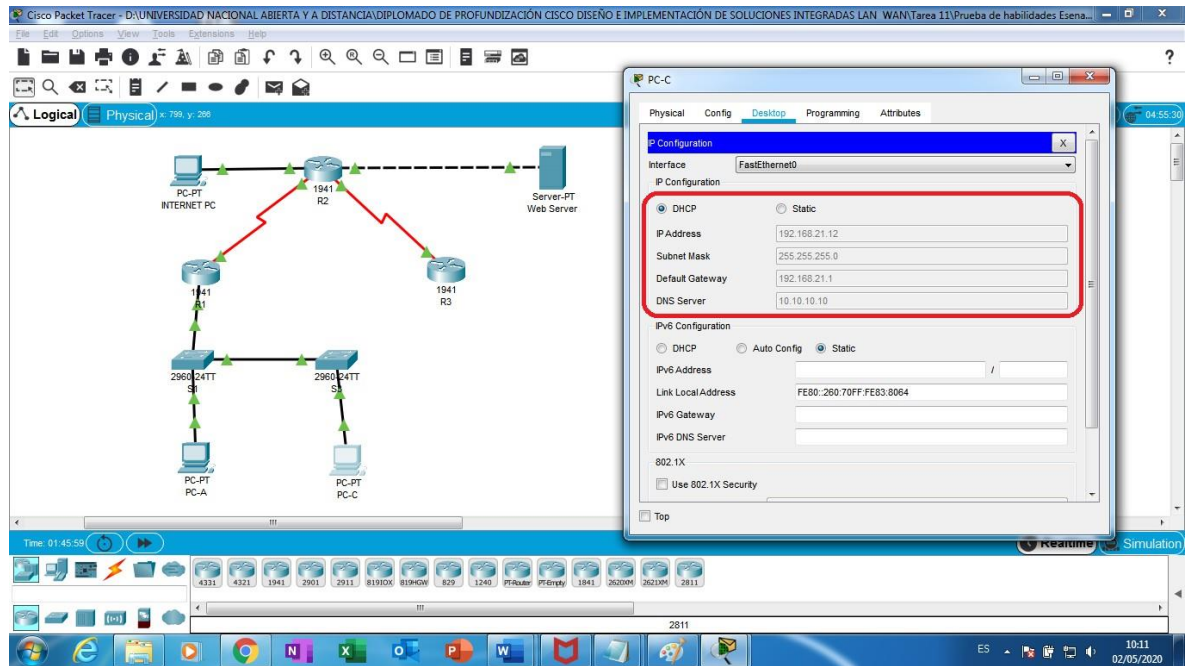


Figura 14. El ping PC-A a PC-C ha sido satisfactorio

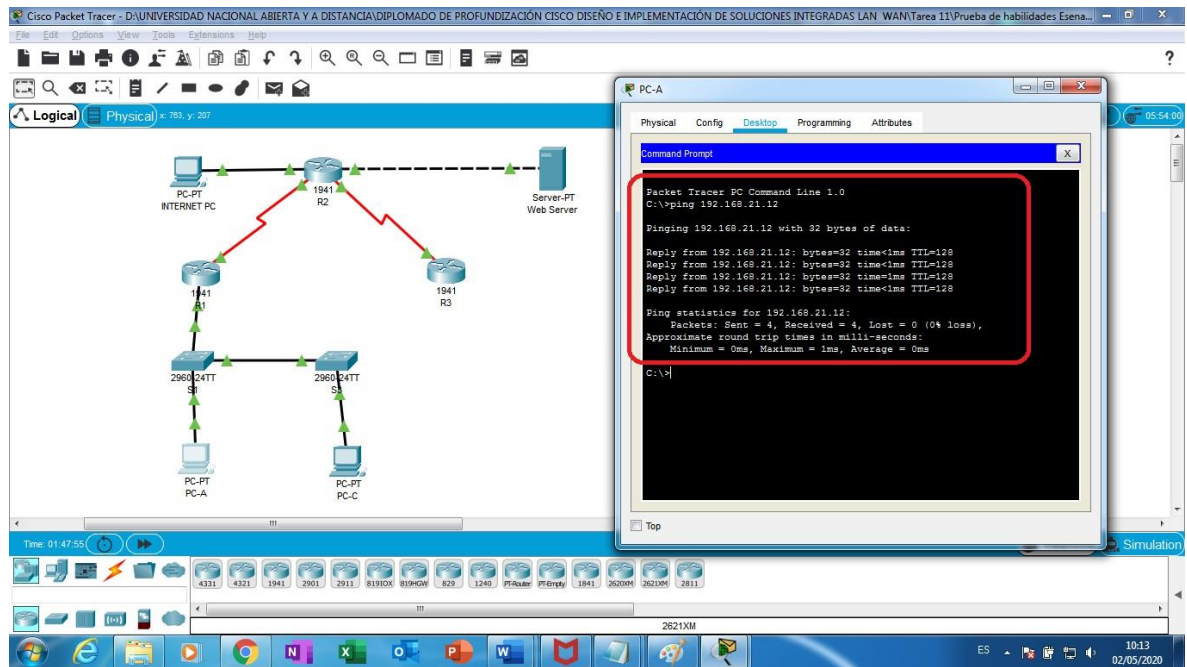
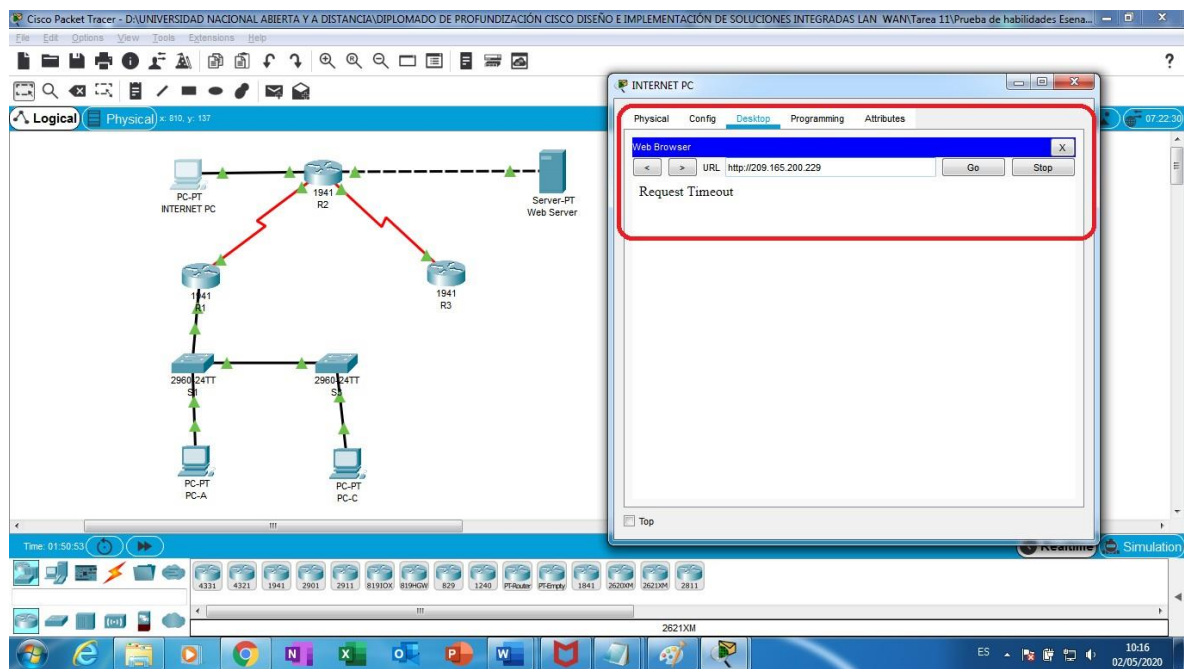


Figura 15. El navegador al acceder pide tiempo fuera



4.1.6 PARTE 6: CONFIGURAR NTP

Se realiza la configuración de los Router R1 y R2 de acuerdo a las tareas indicadas en la tabla 20:

Tabla 20. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 March 5 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.	R2#show ntp associations

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

PASO 1: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2.

Se realiza la configuración para restringir el acceso a las líneas VTY en el Router R2, siguiendo las tareas indicadas en la tabla 21:

Tabla 21. 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 R2(config-line)#exit

Verificar que la ACL funcione como se espera

El ACL funciona, se realiza telnet a la dirección de R2 y funciona perfecto.

```
R1#telnet 172.16.1.2
```

```
Trying 172.16.1.2 ...OpenUnauthorized access is prohibited!
```

```
User Access Verification
```

```
Password:
```

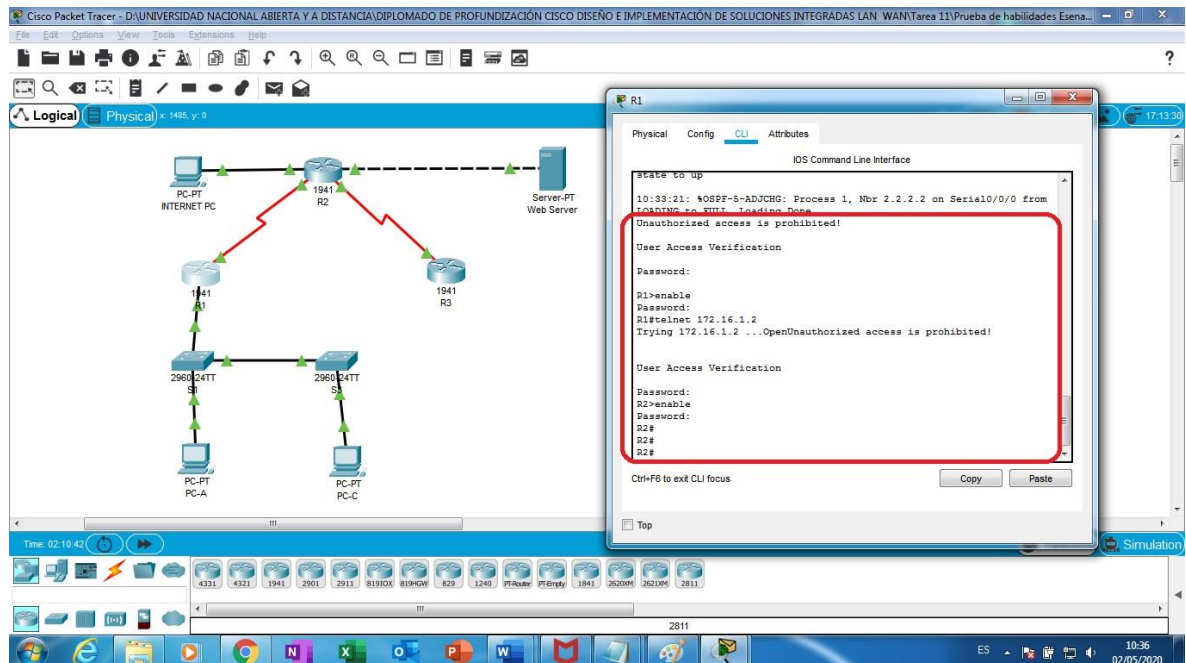
```
R2>enable
```

```
Password:
```

```
R2#
```

Ver figura 16.

Figura 16. El ACL funciona, se realiza telnet a la dirección de R2 y funciona perfecto.



PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE.

Se introduce el comando de CLI adecuado para obtener la información requerida en la tabla 22:

Tabla 22. 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-lists Ver figura 17.
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters // no soporta el comando Ver figura 18.
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show running-config Ver figura 19.
¿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 Ver figura 20.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * Ver figura 21.

Figura 17. Comando R2#show access-lists

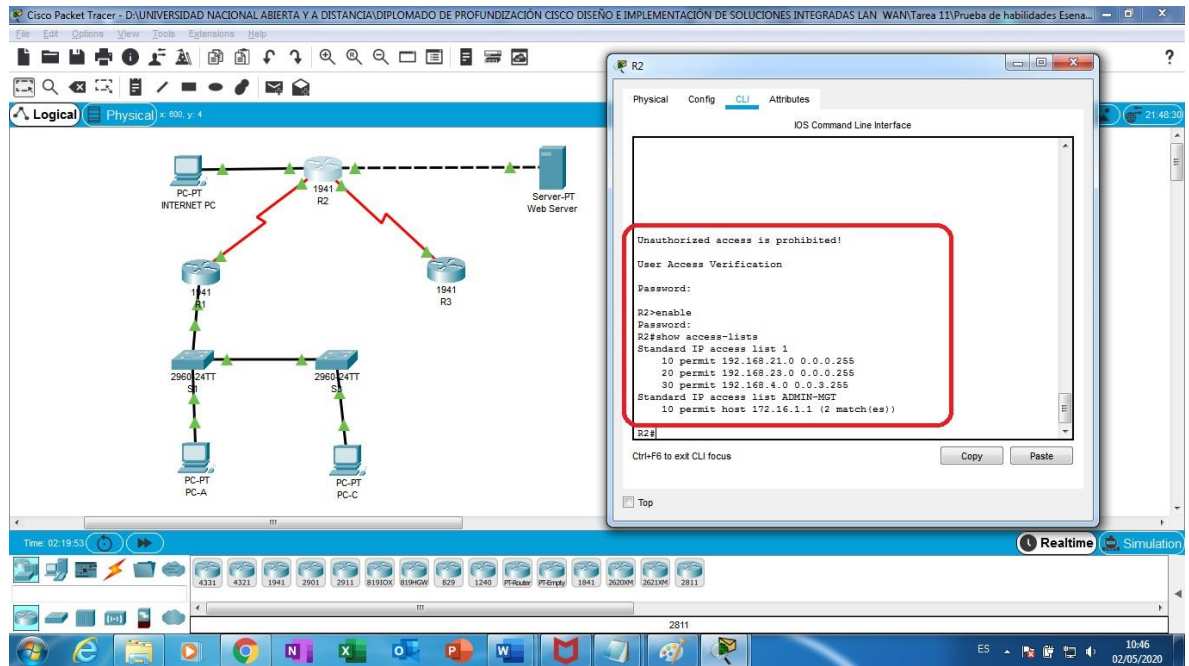


Figura 18. Comando R2#clear ip access-list counters

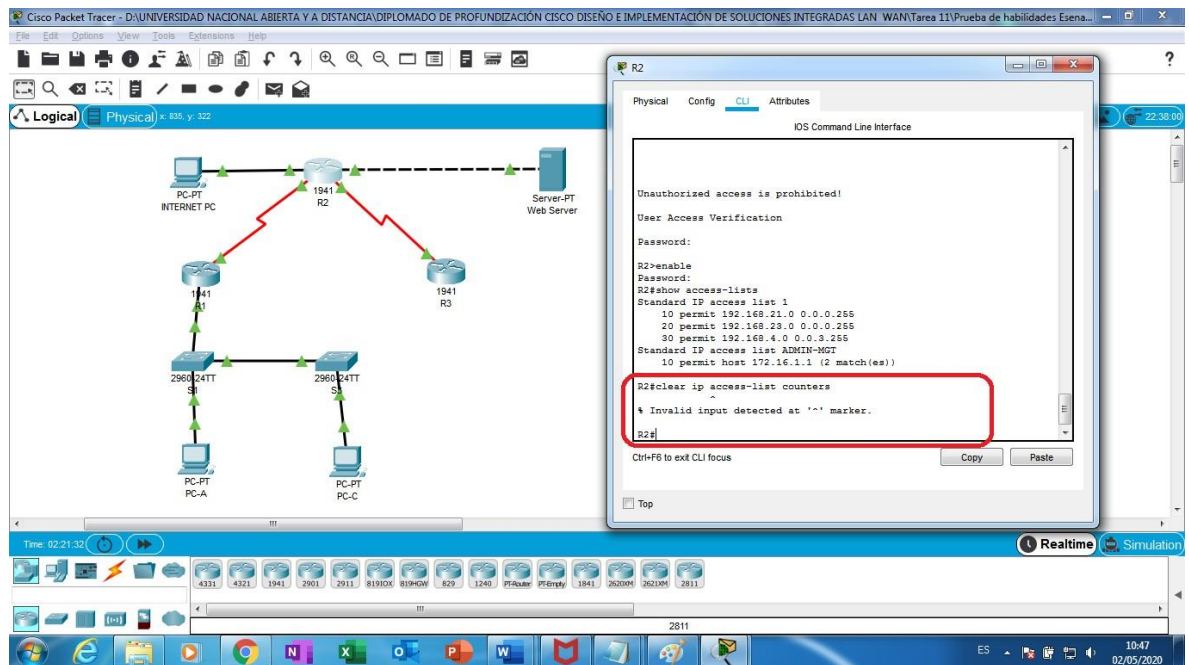


Figura 19. Comando R2#show running-config

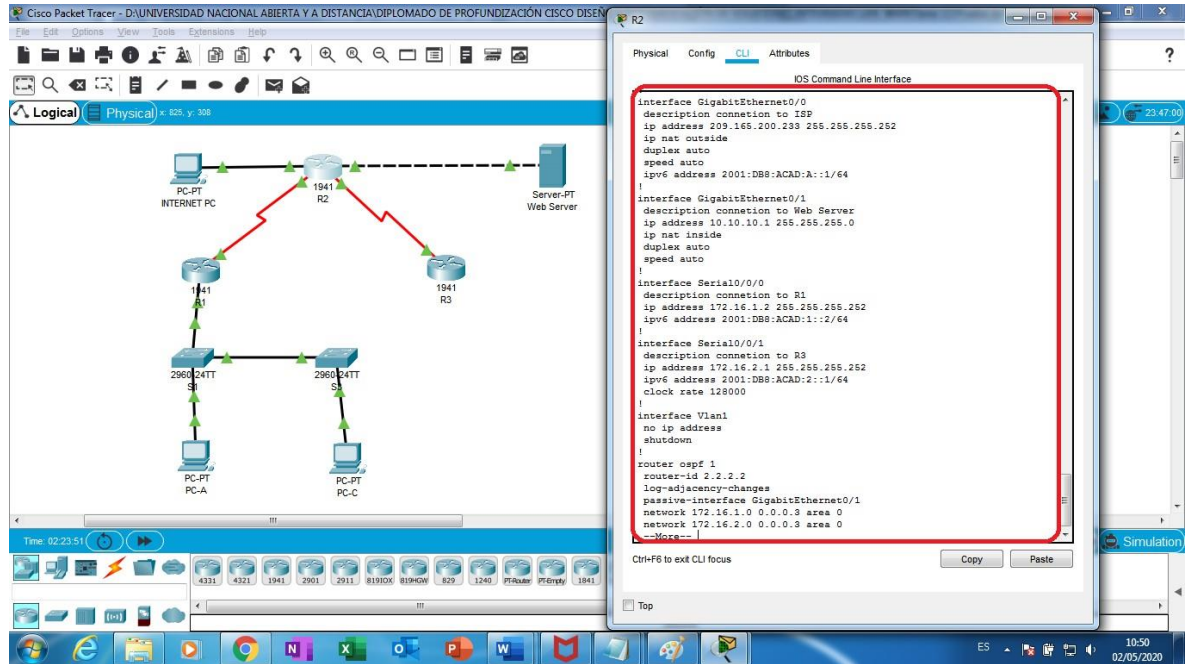


Figura 20. Comando R2#show ip nat translations

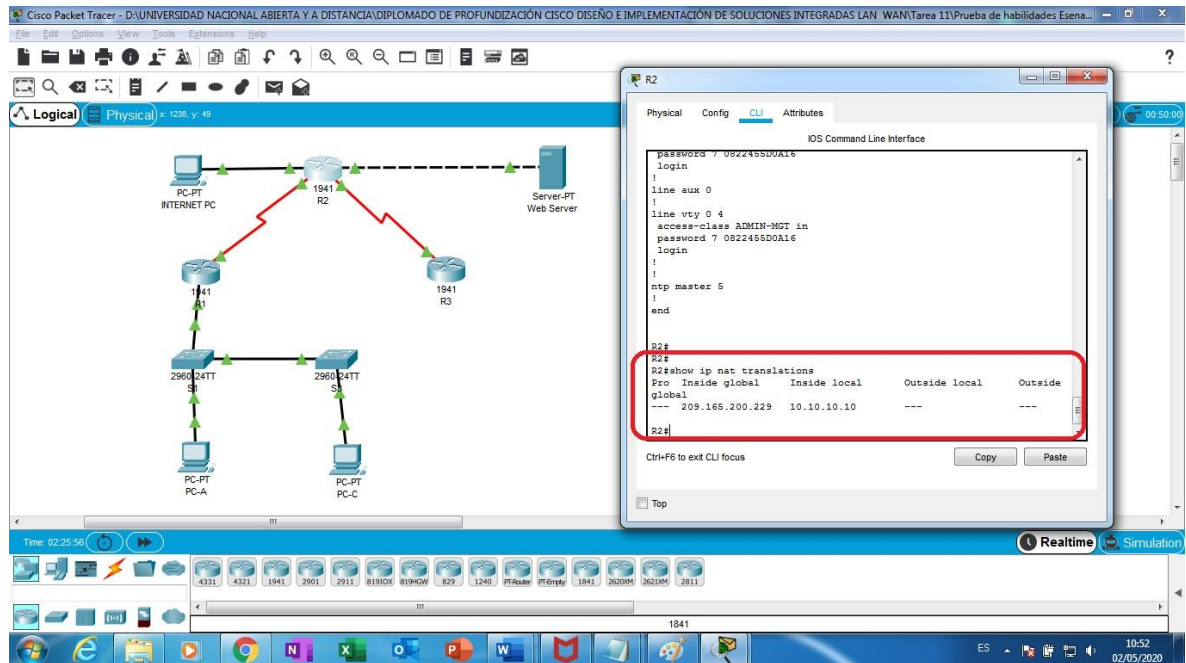


Figura 21. Comando R2#clear ip nat translation *

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram is visible with several devices: R1 (1941), R2 (1941), R3 (1941), S1 (2960-24TT), S2 (2960-24TT), PC-A, PC-C, INTERNET PC, and Web Server. On the right, the CLI window for R2 is open, showing the following commands and output:

```
password ? 0822455D0A1e
login
!
ntp master 5
!
end

R2#
R2#
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside
global
--- 209.165.200.229 10.10.10.10 --- ---

R2#
R2#clear ip nat translation *
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside
global
--- 209.165.200.229 10.10.10.10 --- ---

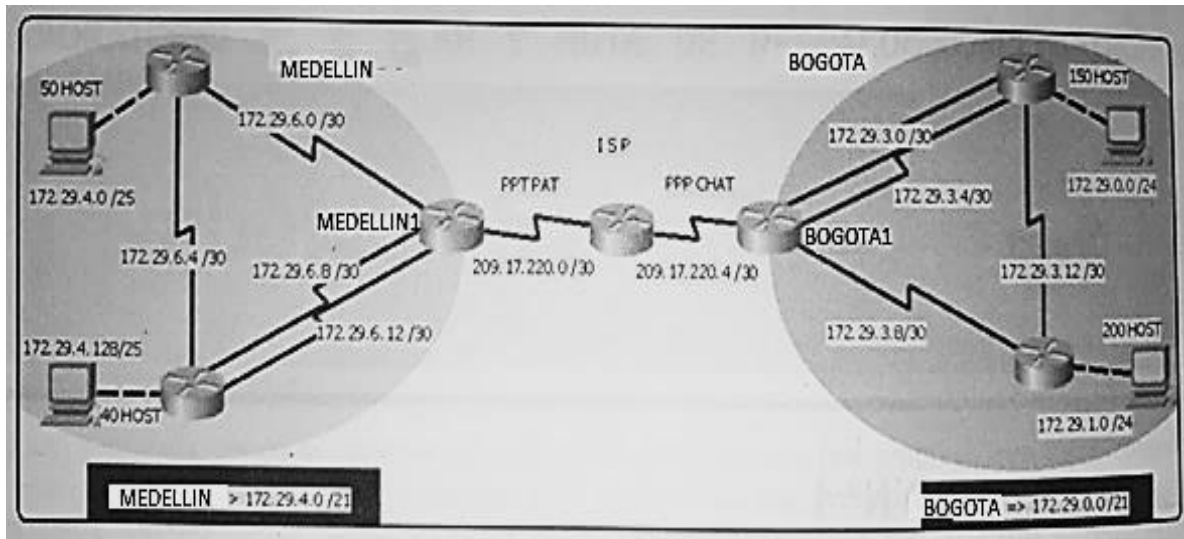
R2#
```

The output of the second 'show ip nat translations' command is highlighted with a red box. The bottom of the window shows the system tray with the time 10:54 and date 02/05/2020.

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.

Figura 22. Topología de red



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.

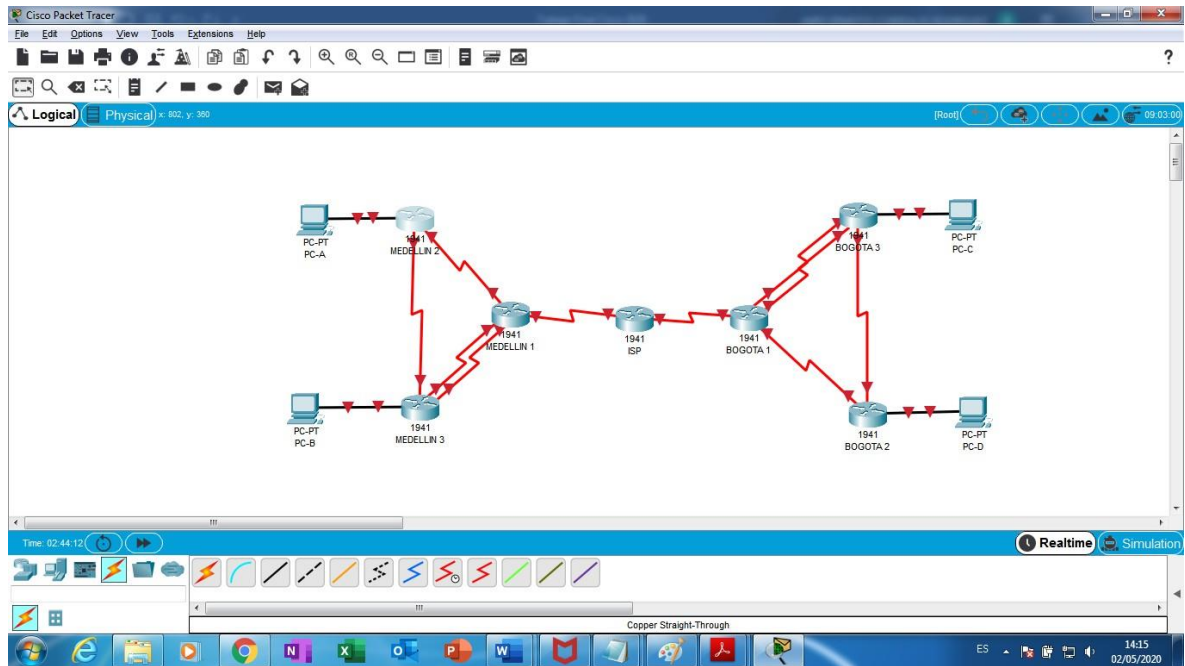
Debe habilitar NAT de sobrecarga en los Routers Bogota1 y medellin1.

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.

Figura 23. Conexión física de los equipos con base en la topología de red



4.2.1 PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

- a. Se configura el enrutamiento en la red usando el protocolo OSPF versión 2, se declara la red principal y se desactiva la summarización automática como lo indica la tabla 23.

Tabla 23. Configuración del enrutamiento

Elemento o tarea de configuración	Especificación
Router ISP	<pre> Router>enable Router#conf t 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 128000 ISP(config-if)#no shutdown ISP(config-if)#int s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown </pre>

<p>Router MEDELLIN-1</p>	<pre> Router>enable Router#conf t Router(config)#hostname MEDELLIN-1 MEDELLIN-1(config)#int s0/0/0 MEDELLIN-1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN-1(config-if)#clock rate 128000 MEDELLIN-1(config-if)#no shutdown MEDELLIN-1(config-if)#int s0/0/1 MEDELLIN-1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN-1(config-if)#clock rate 128000 MEDELLIN-1(config-if)#no shutdown MEDELLIN-1(config-if)#int s0/1/0 MEDELLIN-1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN-1(config-if)#clock rate 128000 MEDELLIN-1(config-if)#no shutdown MEDELLIN-1(config)#int s0/1/1 MEDELLIN-1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN-1(config-if)#clock rate 128000 MEDELLIN-1(config-if)#no shutdown MEDELLIN-1(config)#router rip MEDELLIN-1(config-router)#version 2 MEDELLIN-1(config-router)#do show ip route connected MEDELLIN-1(config-router)#network 172.29.6.0 MEDELLIN-1(config-router)#network 172.29.6.8 MEDELLIN-1(config-router)#network 172.29.6.12 MEDELLIN-1(config-router)#network 209.17.220.0 MEDELLIN-1(config-router)#no auto summary </pre>
--------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Router MEDELLIN-2</p>	<pre> Router>enable Router#conf t Router(config)#hostname MEDELLIN-2 MEDELLIN-2(config)#int s0/0/0 MEDELLIN-2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN-2(config-if)#clock rate 128000 MEDELLIN-2(config-if)#no shutdown MEDELLIN-2(config-if)#int s0/0/1 MEDELLIN-2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN-2(config-if)#clock rate 128000 MEDELLIN-2(config-if)#no shutdown MEDELLIN-2(config-if)#int g0/0 MEDELLIN-2(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN-2(config-if)#no shutdown MEDELLIN-2(config)#router rip MEDELLIN-2(config-router)#version 2 MEDELLIN-2(config-router)#do show ip route connected MEDELLIN-2(config-router)#network 172.29.4.0 MEDELLIN-2(config-router)#network 172.29.6.0 MEDELLIN-2(config-router)#network 172.29.6.4 MEDELLIN-2(config-router)#no auto summary MEDELLIN-2(config-router)#passive- interface g0/0 </pre>
<p>Router MEDELLIN-3</p>	<pre> Router>enable Router#conf t Router(config)#hostname MEDELLIN-3 MEDELLIN-3(config)#int s0/0/0 MEDELLIN-3(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN-3(config-if)#clock rate 128000 MEDELLIN-3(config-if)#no shutdown MEDELLIN-3(config-if)#int s0/0/1 MEDELLIN-3(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN-3(config-if)#clock rate 128000 </pre>

	<pre> MEDELLIN-3(config-if)#no shutdown MEDELLIN-3(config-if)#int s0/1/0 MEDELLIN-3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN-3(config-if)#clock rate 128000 MEDELLIN-3(config-if)#no shutdown MEDELLIN-3(config-if)#int g0/0 MEDELLIN-3(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN-3(config-if)#no shutdown MEDELLIN-3(config)#router rip MEDELLIN-3(config-router)#version 2 MEDELLIN-3(config-router)#do show ip route connected MEDELLIN-3(config-router)#network 172.29.4.128 MEDELLIN-3(config-router)#network 172.29.6.4 MEDELLIN-3(config-router)#network 172.29.6.8 MEDELLIN-3(config-router)#network 172.29.6.12 MEDELLIN-3(config-router)#no auto summary MEDELLIN-3(config-router)#passive- interface g0/0 </pre>
<p>Router BOGOTA-1</p>	<pre> Router>enable Router#conf t Router(config)#hostname BOGOTA-1 BOGOTA-1(config)#int s0/0/0 BOGOTA-1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA-1(config-if)#clock rate 128000 BOGOTA-1(config-if)#no shutdown BOGOTA-1(config-if)#int s0/0/1 BOGOTA-1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA-1(config-if)#clock rate 128000 BOGOTA-1(config-if)#no shutdown BOGOTA-1(config-if)#int s0/1/0 BOGOTA-1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA-1(config-if)#clock rate 128000 </pre>

	<pre> BOGOTA-1(config-if)#no shutdown BOGOTA-1(config-if)#int s0/1/1 BOGOTA-1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA-1(config-if)#clock rate 128000 BOGOTA-1(config-if)#no shutdown BOGOTA-1(config)#router rip BOGOTA-1(config-router)#version 2 BOGOTA-1(config-router)#do show ip route connected BOGOTA-1(config-router)#network 172.29.3.0 BOGOTA-1(config-router)#network 172.29.3.4 BOGOTA-1(config-router)#network 172.29.3.8 BOGOTA-1(config-router)#network 209.17.220.4 BOGOTA-1(config-router)#no auto summary </pre>
<p>Router BOGOTA-2</p>	<pre> Router>enable Router#conf t Router(config)#hostname BOGOTA-2 BOGOTA-2(config)#int s0/0/0 BOGOTA-2(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA-2(config-if)#clock rate 128000 BOGOTA-2(config-if)#no shutdown BOGOTA-2(config-if)#int s0/0/1 BOGOTA-2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA-2(config-if)#clock rate 128000 BOGOTA-2(config-if)#no shutdown BOGOTA-2(config-if)#int g0/0 BOGOTA-2(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA-2(config-if)#no shutdown </pre>

	<pre> BOGOTA-2(config)#router rip BOGOTA-2(config-router)#version 2 BOGOTA-2(config-router)#do show ip route connected BOGOTA-2(config-router)#network 172.29.1.0 BOGOTA-2(config-router)#network 172.29.3.8 BOGOTA-2(config-router)#network 172.29.3.12 BOGOTA-2(config-router)#no auto summary BOGOTA-2(config-router)#passive-interface g0/0 </pre>
<p>Router BOGOTA-3</p>	<pre> Router>enable Router#conf t Router(config)#hostname BOGOTA-3 BOGOTA-3(config)#int s0/0/0 BOGOTA-3(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA-3(config-if)#clock rate 128000 BOGOTA-3(config-if)#no shutdown BOGOTA-3(config-if)#int s0/0/1 BOGOTA-3(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA-3(config-if)#clock rate 128000 BOGOTA-3(config-if)#no shutdown BOGOTA-3(config-if)#int s0/1/0 BOGOTA-3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA-3(config-if)#clock rate 128000 BOGOTA-3(config-if)#no shutdown BOGOTA-3(config-if)#int g0/0 BOGOTA-3(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA-3(config-if)#no shutdown </pre>

	<pre> BOGOTA-3(config)#router rip BOGOTA-3(config-router)#version 2 BOGOTA-3(config-router)#do show ip route connected BOGOTA-3(config-router)#network 172.29.0.0 BOGOTA-3(config-router)#network 172.29.3.0 BOGOTA-3(config-router)#network 172.29.3.4 BOGOTA-3(config-router)#network 172.29.3.12 BOGOTA-3(config-router)#no auto summary BOGOTA-3(config-router)#passive-interface g0/0 </pre>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- b. A los Routers Bogota1 y Medellín-1 se les añade en su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, se redistribuye dentro de las publicaciones de OSPF como lo indica la tabla 24.

Tabla 24. Configuración Routers Bogota1 y Medellín-1

Elemento o tarea de configuración	Especificación
Router MEDELLIN-1	<pre> MEDELLIN-1#conf t MEDELLIN-1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 </pre>
Router BOGOTA-1	<pre> BOGOTA-1#conf t BOGOTA-1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 </pre>

Se realizan pruebas de conexión dentro de la red Bogotá y Medellín la cuales se pueden verificar en las Figura 24 Ping en la red de MEDELLIN: Desde PC-A a PC-B y la Figura 25 Ping en la red de BOGOTA: Desde PC-C a PC-D

Figura 24. Ping en la red de MEDELLIN: Desde PC-A a PC-B

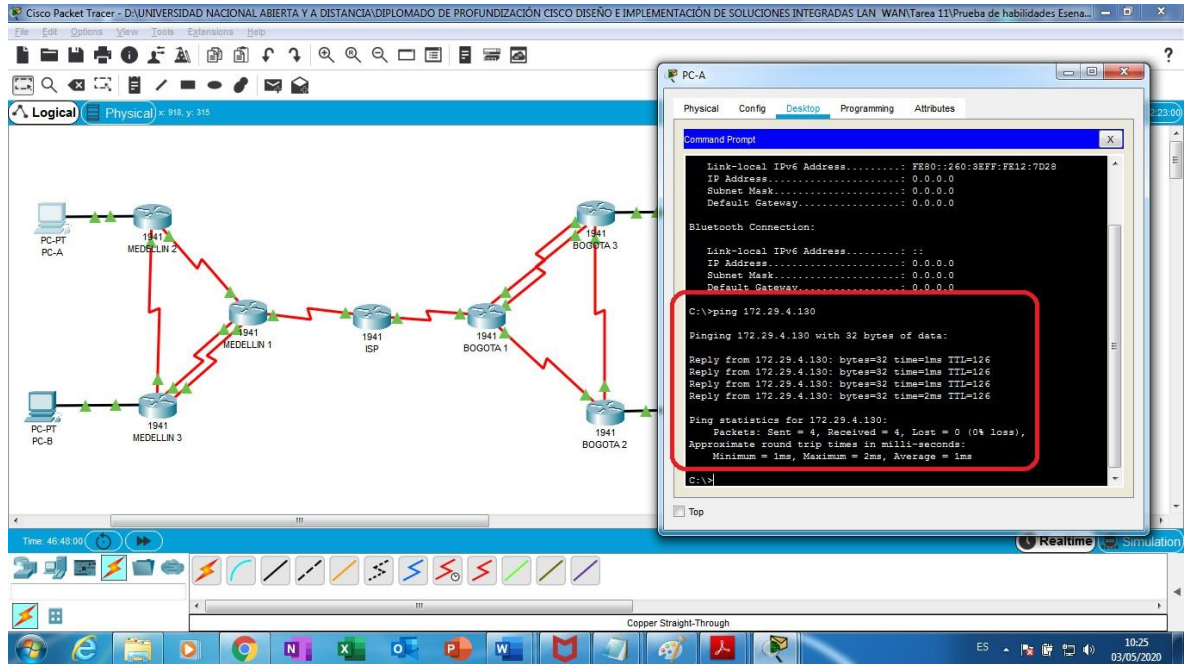
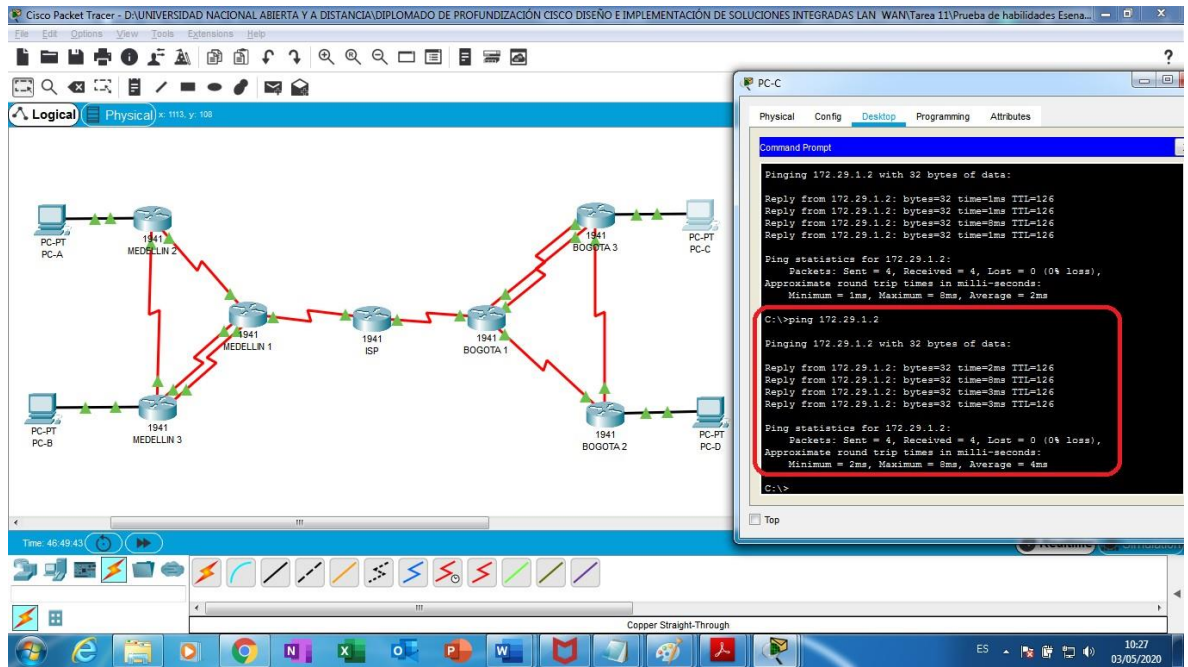


Figura 25. Ping en la red de BOGOTA: Desde PC-C a PC-D



- c. Se configura el Router ISP con una ruta estática dirigida hacia cada red interna de Bogotá y Medellín como indica la tabla 27, se lleva a cabo la sumarización de la red interna Medellín ver tabla 25 y se lleva a cabo la sumarización de la red interna Bogotá ver tabla 26.

Tabla 25. Sumarización Red Medellín

Red interna MEDELLÍN	172.29.4.0/25 172.29.4.128/25 172.29.6.0/30 172.29.6.12/30 172.29.6.8/30 172.29.6.4/30
Sumarización	172.29.4.0/22

Tabla 26. Sumarización Red Bogotá

Red interna BOGOTÁ	172.29.1.0/24 172.29.3.0/30 172.29.0.0/24 172.29.3.8/30 172.29.3.4/30 172.29.3.12/30
Sumarización	172.29.0.0/22

Tabla 27. Configuración Router ISP

Elemento o tarea de configuración	Especificación
Router ISP	ISP#conf t ISP(config)#ip route 172.29.4.0 255.255.255.0 209.17.220.2 ISP(config)#ip route 172.29.0.0 255.255.255.0 209.17.220.6 ISP(config)#exit

4.2.2 PARTE 2: TABLA DE ENRUTAMIENTO.

- a. Se lleva acabo la verificación de la tabla de enrutamiento en cada uno de los Routers para comprobar las redes. Ver figuras 26, 27, 28 y 29

Figura 26. Ping de PC-A a Router ISP

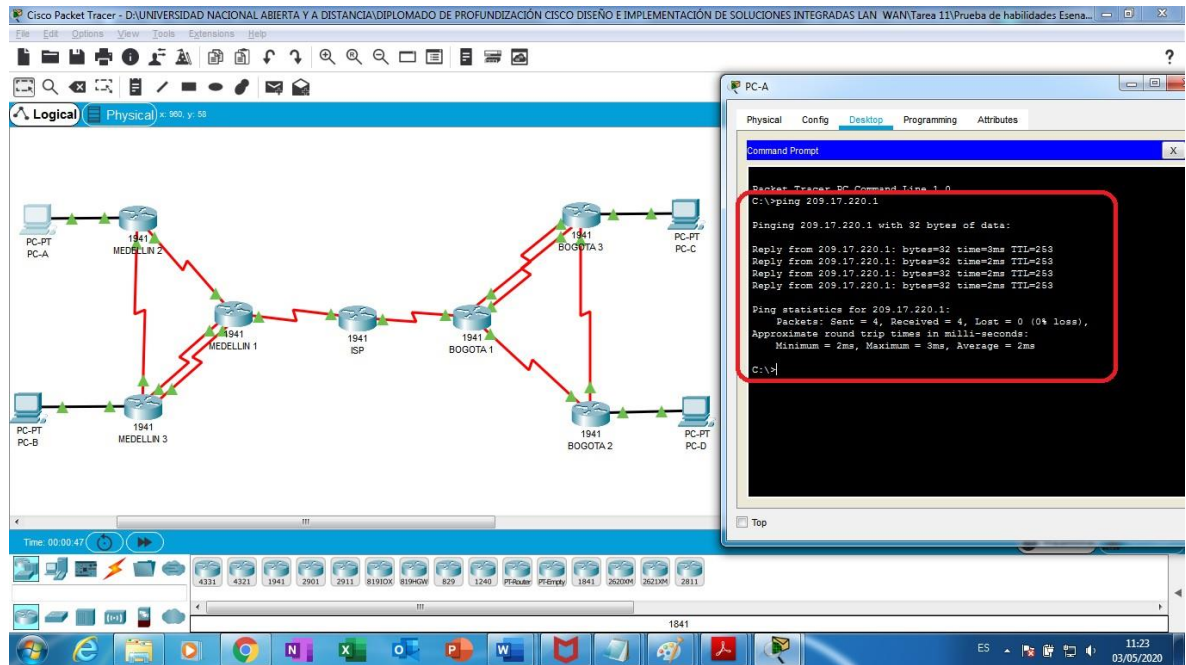


Figura 27. Ping de PC-B a Router ISP

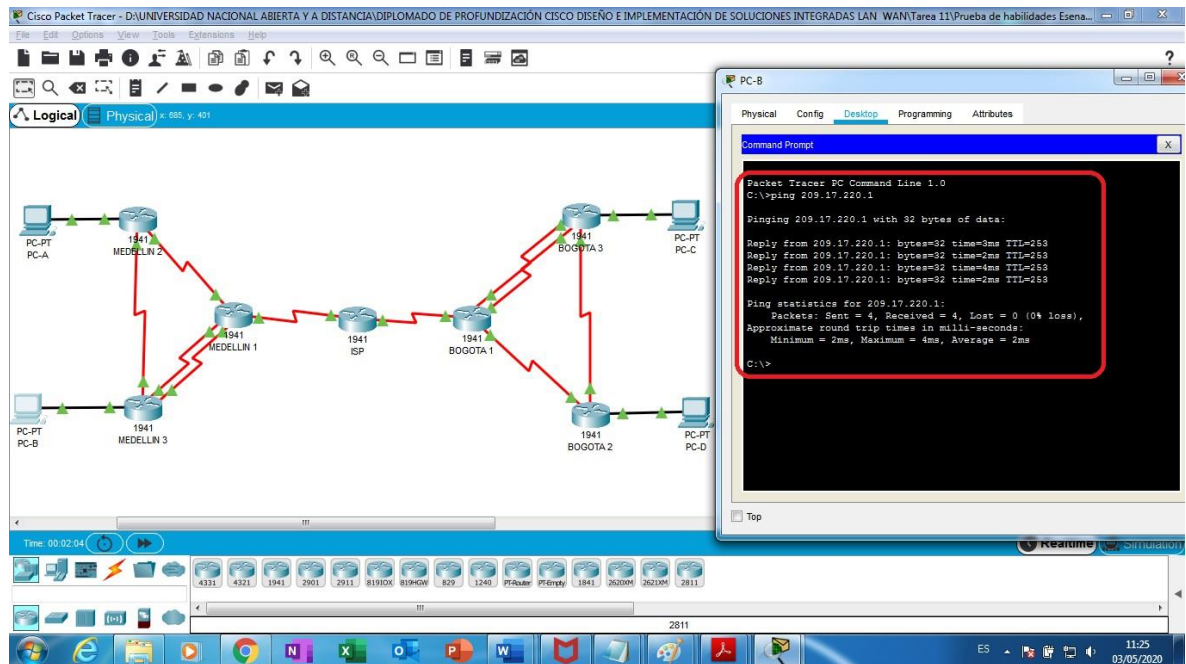


Figura 28. Ping de PC-C a Router ISP

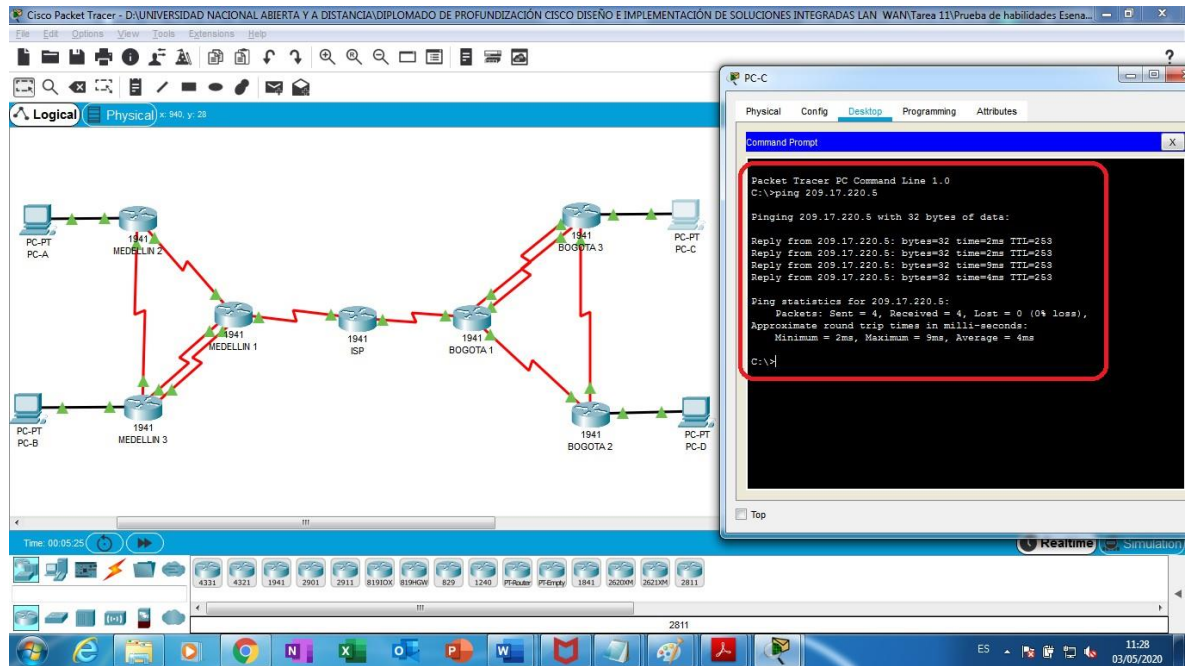
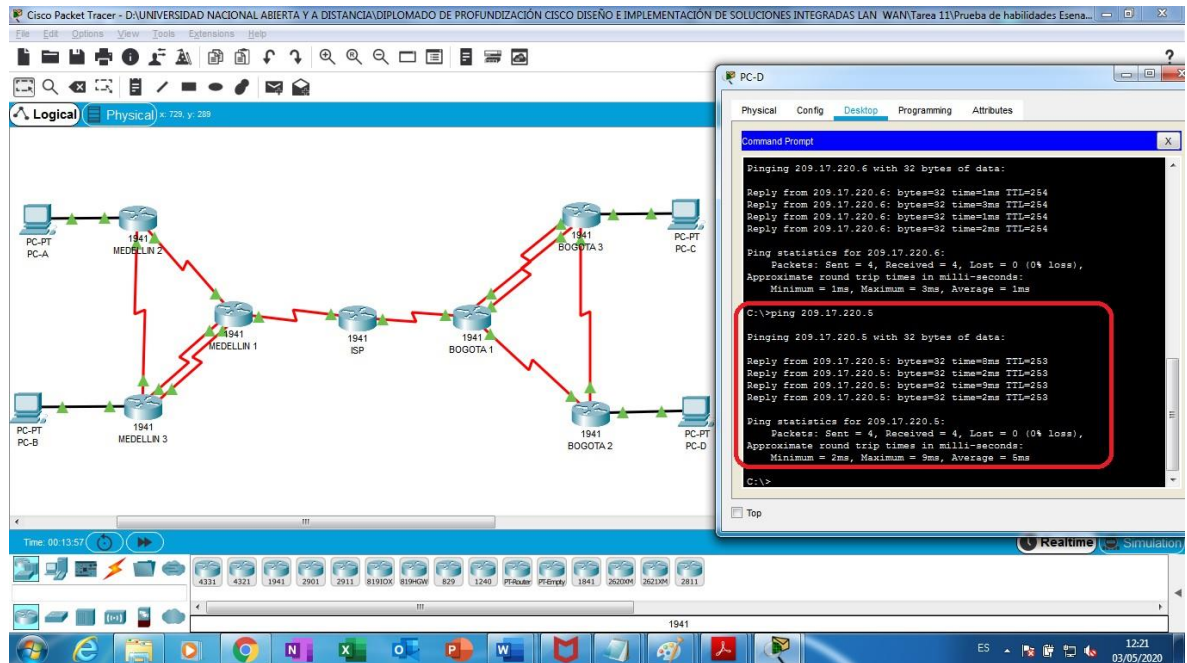


Figura 29. Ping de PC-D a Router ISP



- b. Se lleva acabo la verificación del balanceo de carga que presentan los Routers.
- c. Se observa 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.

El Router BOGOTA-1 y el Router MEDELLIN-1 manejan el mismo número de redes, tienen el mismo número de conexiones y se conectan el mismo número de Routers. ver figura 30 y 31.

Figura 30. MEDELLIN-1#show ip route

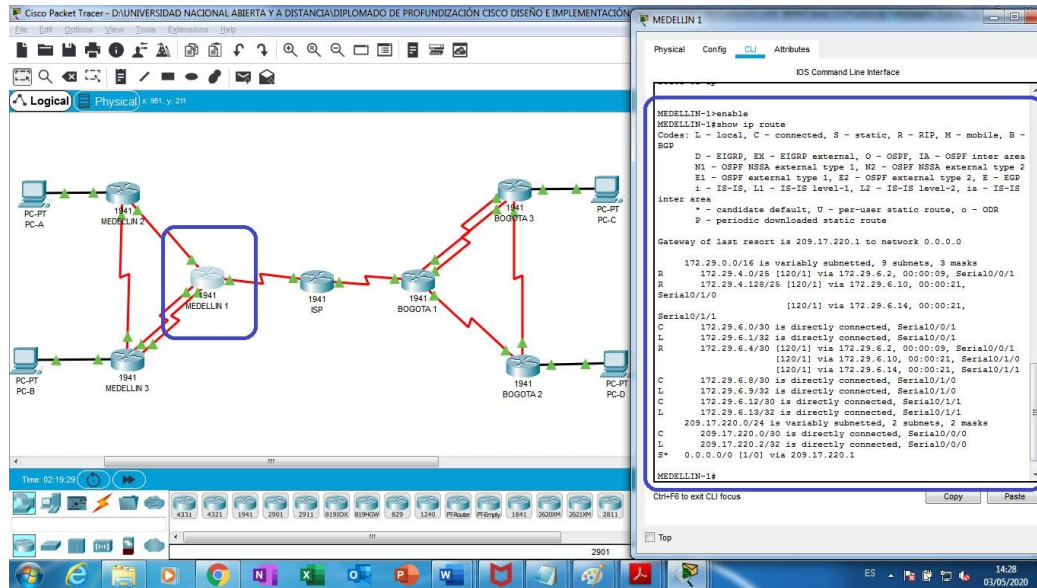
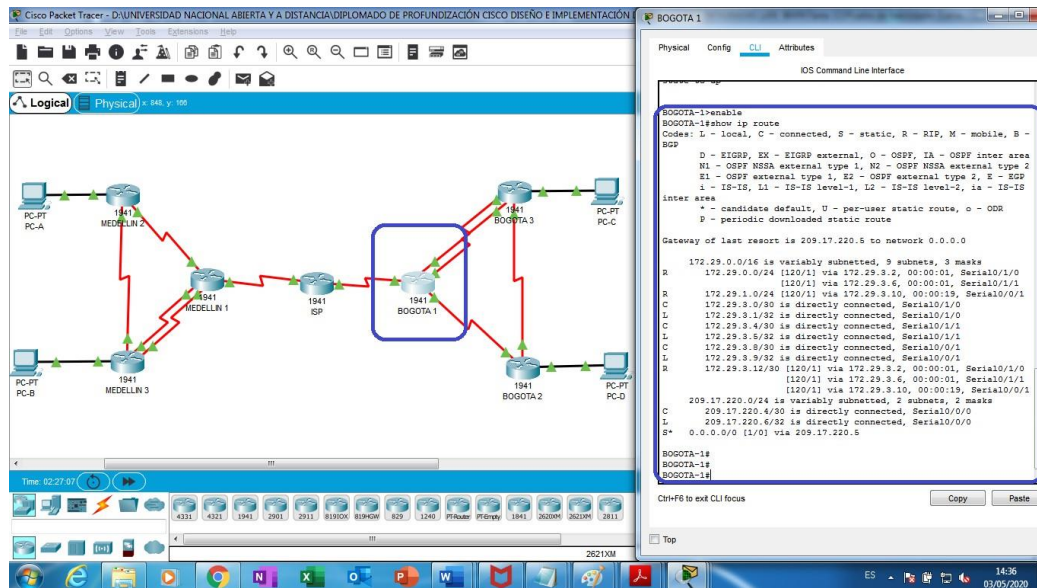


Figura 31. BOGOTA-1#show ip route



- d. Los Routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF ver figuras 32 y 33.

Figura 32. MEDELLIN-2#show ip route

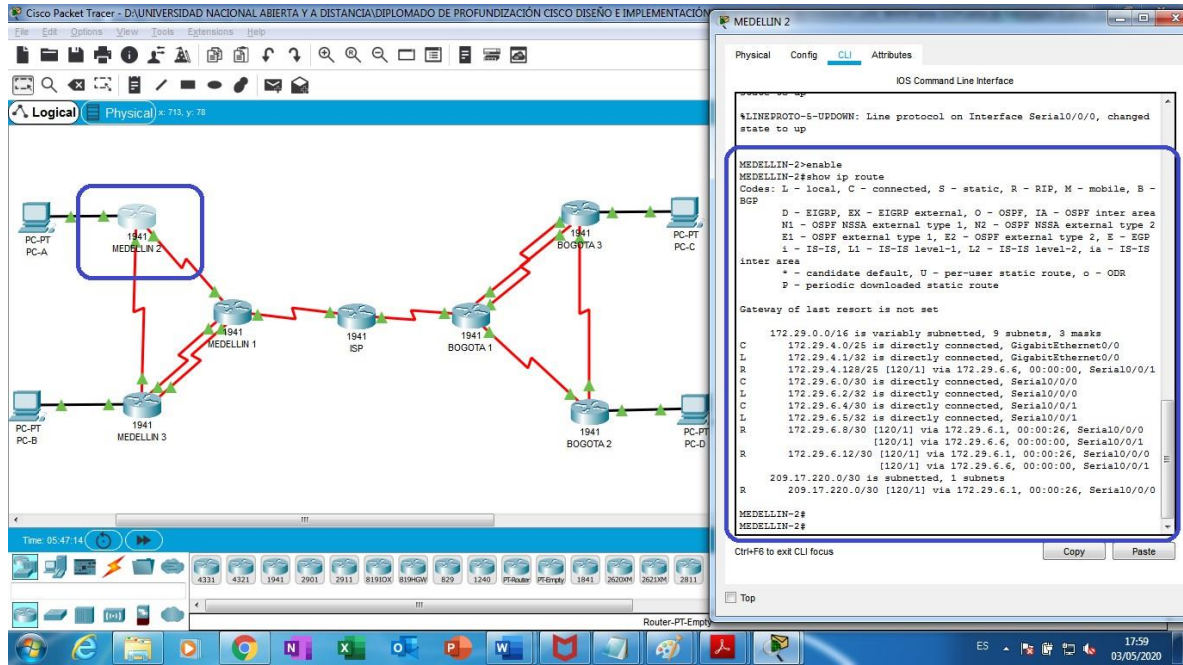
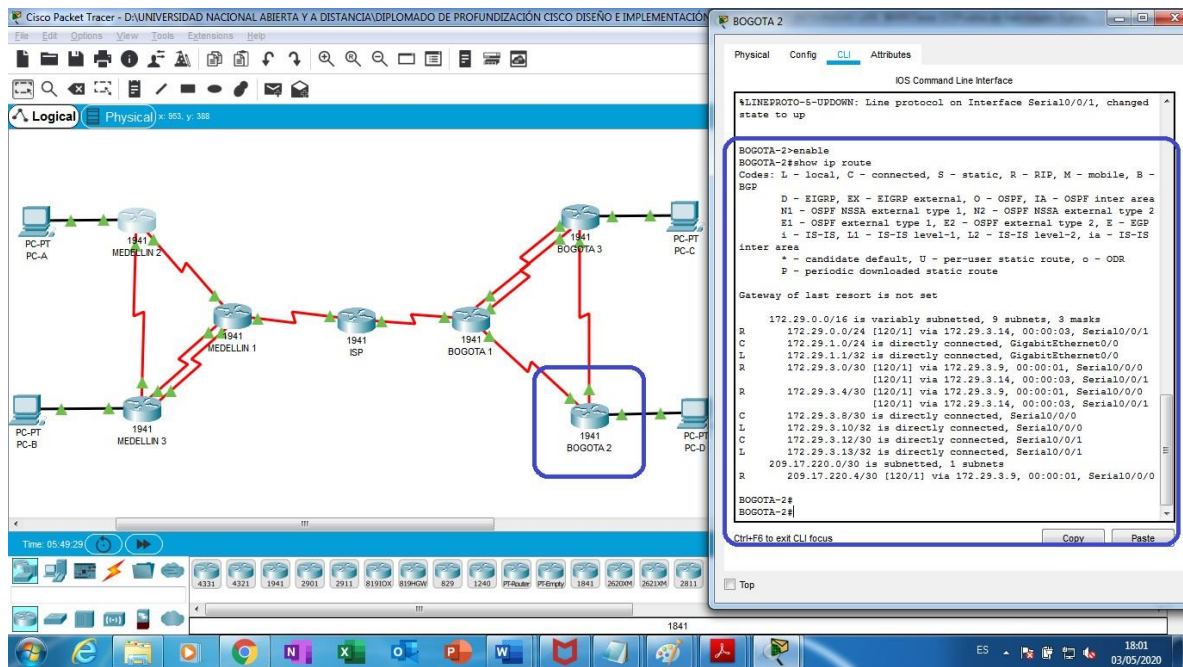


Figura 33. BOGOTA-2#show ip route



- e. Las tablas de los Routers restantes permiten visualizar rutas redundantes para el caso de la ruta por defecto, ver figuras 34 y 35.

Figura 34. MEDELLIN-3#show ip route

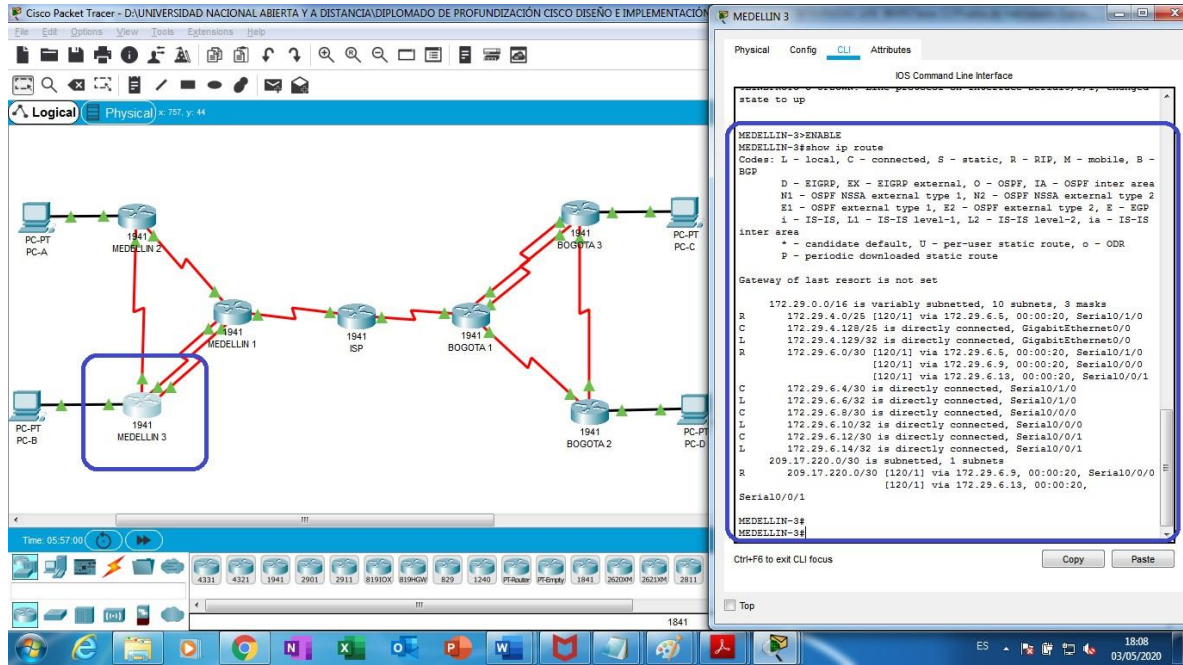
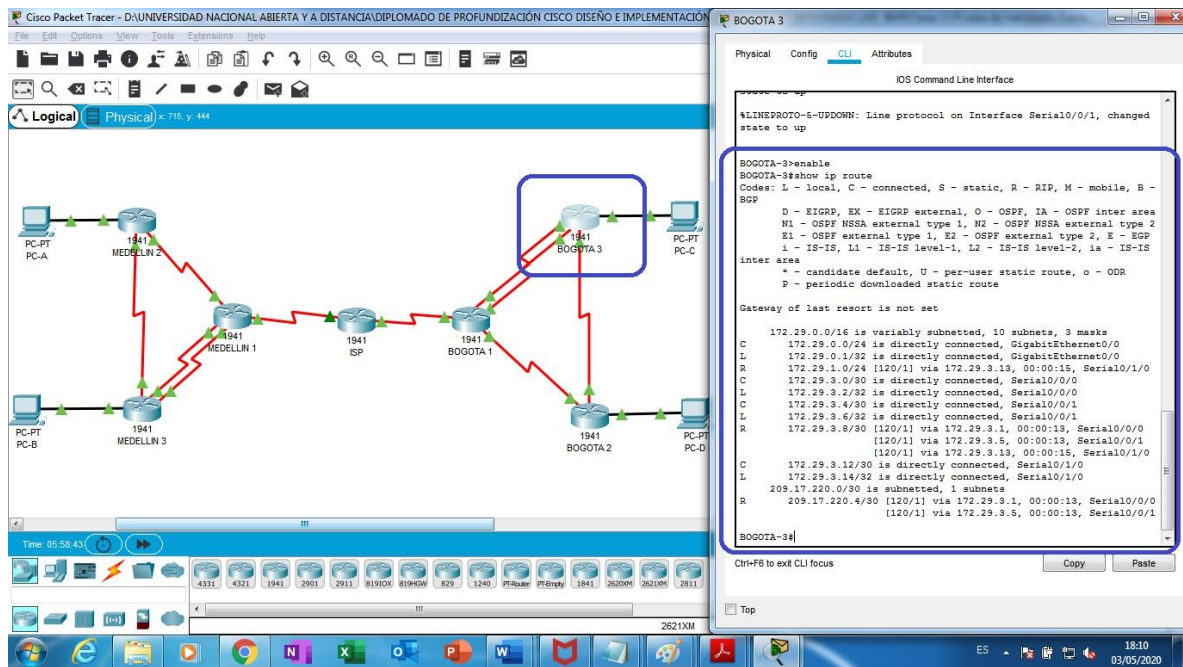


Figura 35. BOGOTA-3#show ip route



- f. El Router ISP indica sus rutas estáticas adicionales a las directamente conectadas, ver figura 36.

Figura 36. ISP#show ip route

The screenshot displays a network topology in Cisco Packet Tracer. The network consists of several 1941 routers and PCs. The routers are labeled: MEDELLIN 1, MEDELLIN 2, MEDELLIN 3, ISP, BOGOTA 1, BOGOTA 2, and BOGOTA 3. PCs are labeled PC-A, PC-B, PC-C, and PC-D. The topology shows a central ISP router connected to two groups of routers (MEDELLIN and BOGOTA) which are further connected to PCs. A red box highlights the output of the 'show ip route' command on the ISP router, showing static routes for various subnets.

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 4 subnets, 2 masks
S 172.29.0.0/24 [1/0] via 209.17.220.6
S 172.29.1.0/24 [1/0] via 209.17.220.6
S 172.29.4.0/24 [1/0] via 209.17.220.2
S 172.29.4.128/25 [1/0] via 209.17.220.2
209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.1/32 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
L 209.17.220.5/32 is directly connected, Serial0/0/1

ISP#
```

4.2.3 PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

Para no propagar las publicaciones por interfaces que no lo requieran se deshabilita la propagación del protocolo OSPF, en la tabla 28 se indican las interfaces de cada Router que no necesitan desactivación.

Tabla 28. Deshabilitar protocolo OSPF

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

En el desarrollo de la primera parte se configuraron los Routers y RIP con sus respectivas interfaces.

4.2.4 PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

- a. Se Verifica y documenta 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. Ver figuras 37, 38, 39, 40, 41 y 42

Figura 37. MEDELLIN-1#show ip protocols

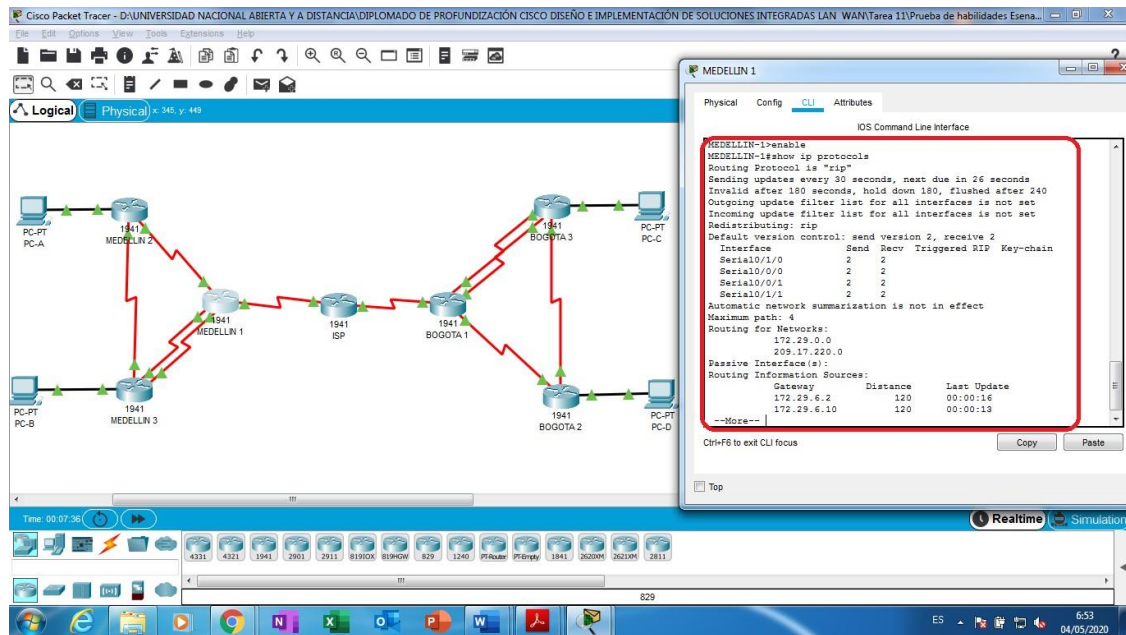


Figura 38. MEDELLIN-2#show ip protocols

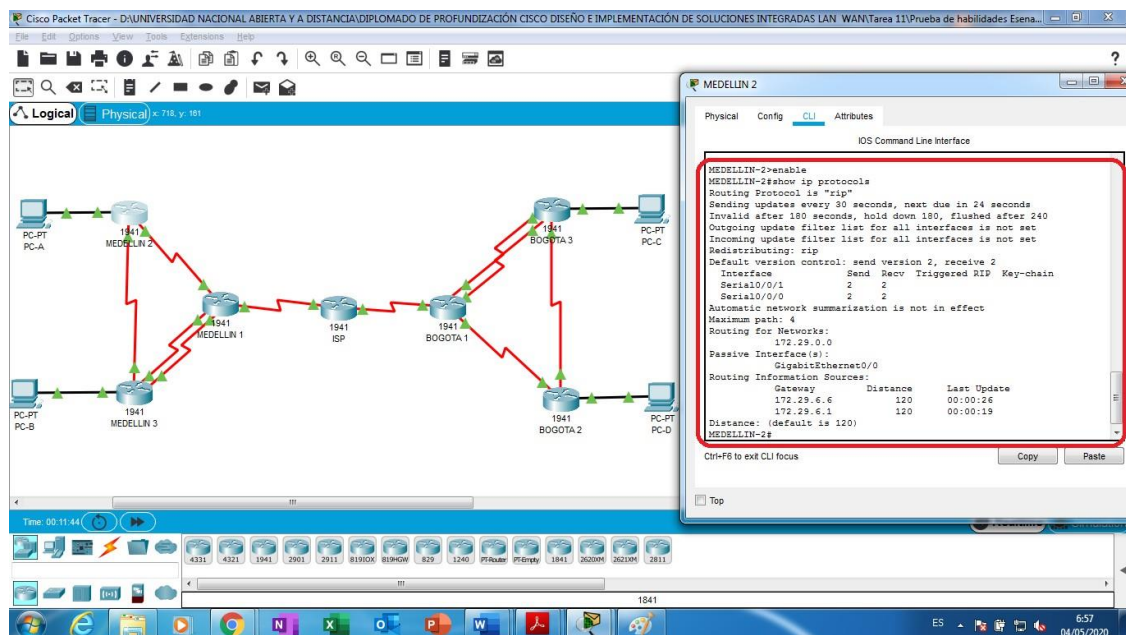


Figura 39. MEDELLIN-3#show ip protocols

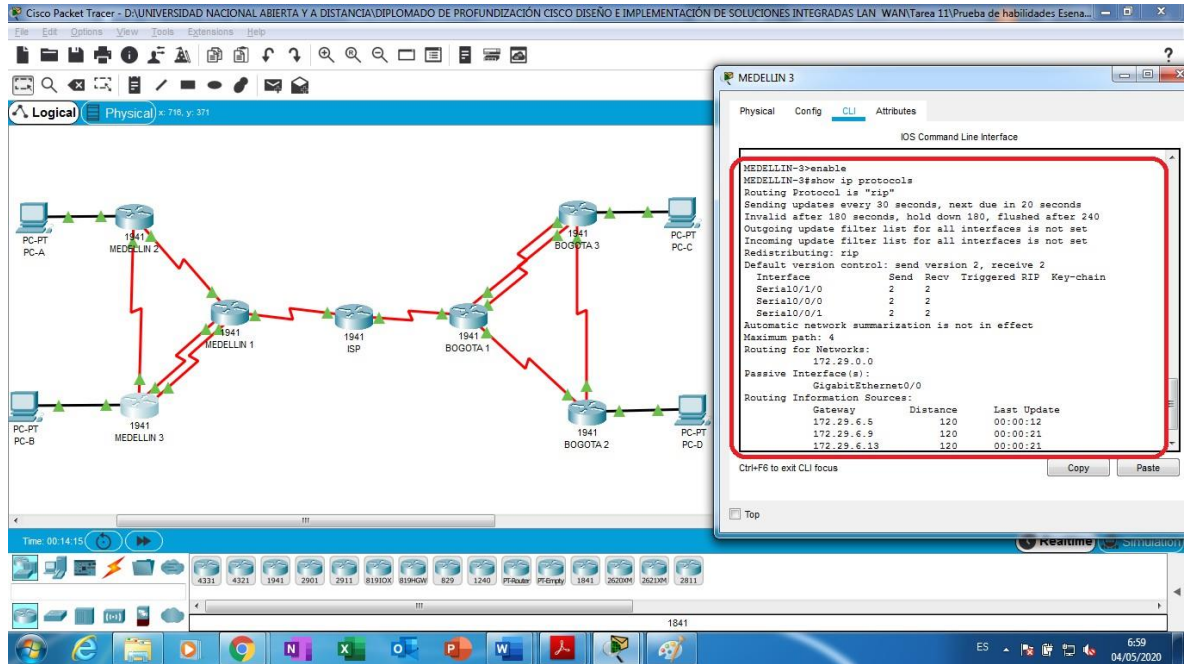


Figura 40. BOGOTA-1#show ip protocols

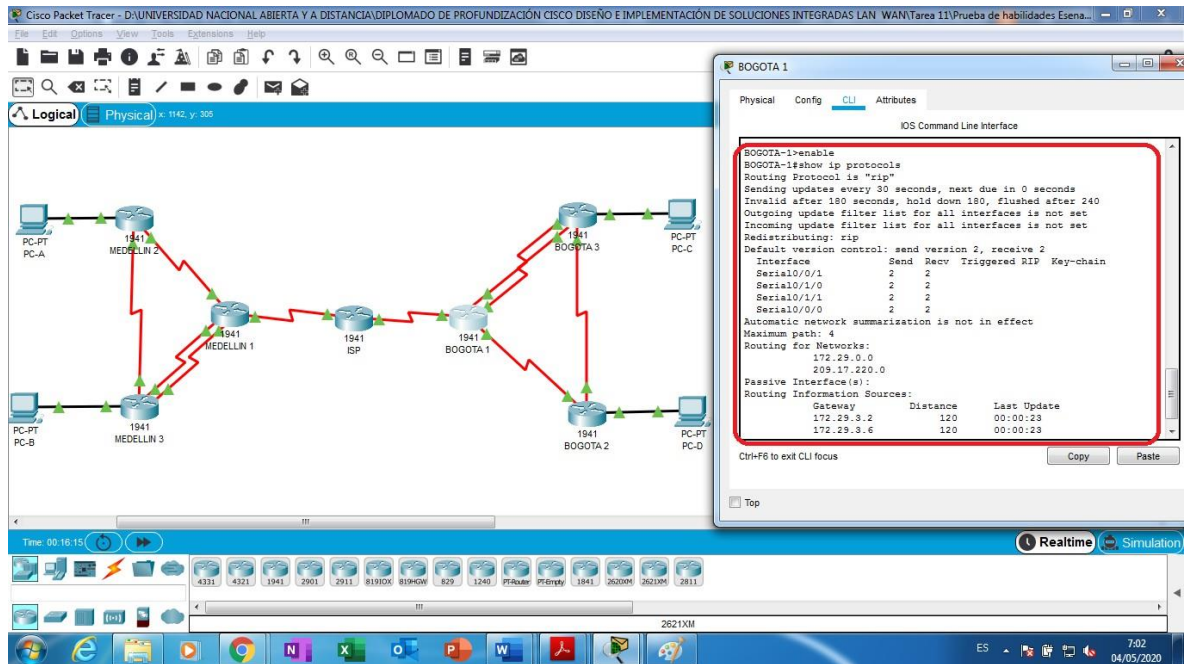


Figura 41. BOGOTA-2#show ip protocols

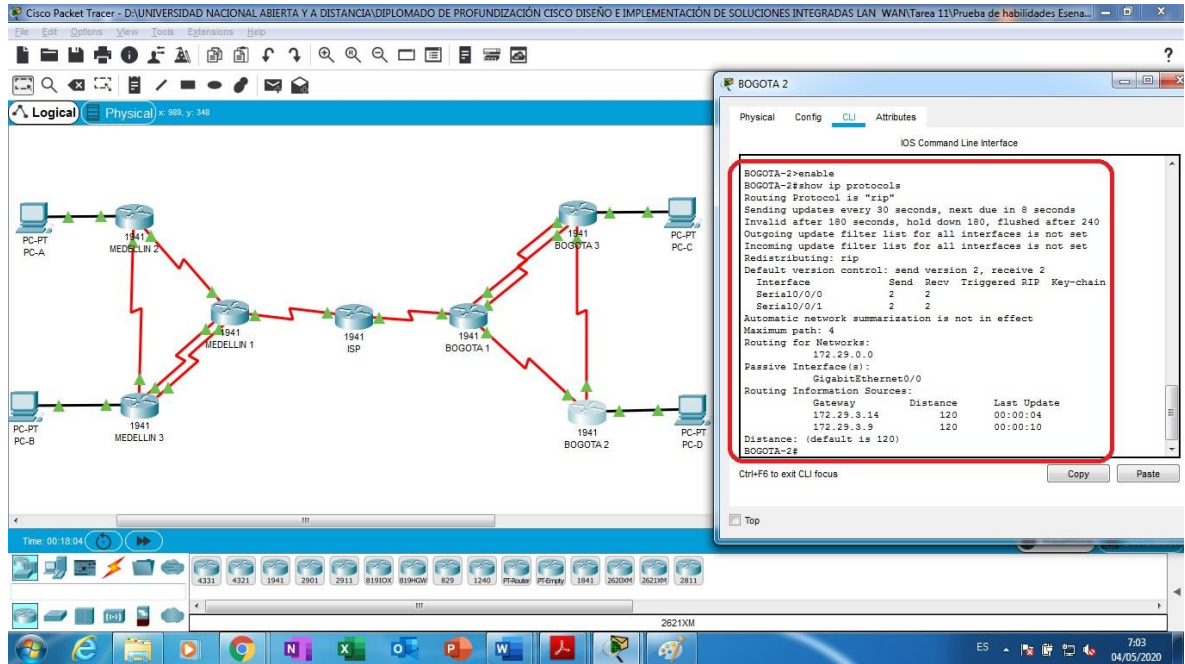
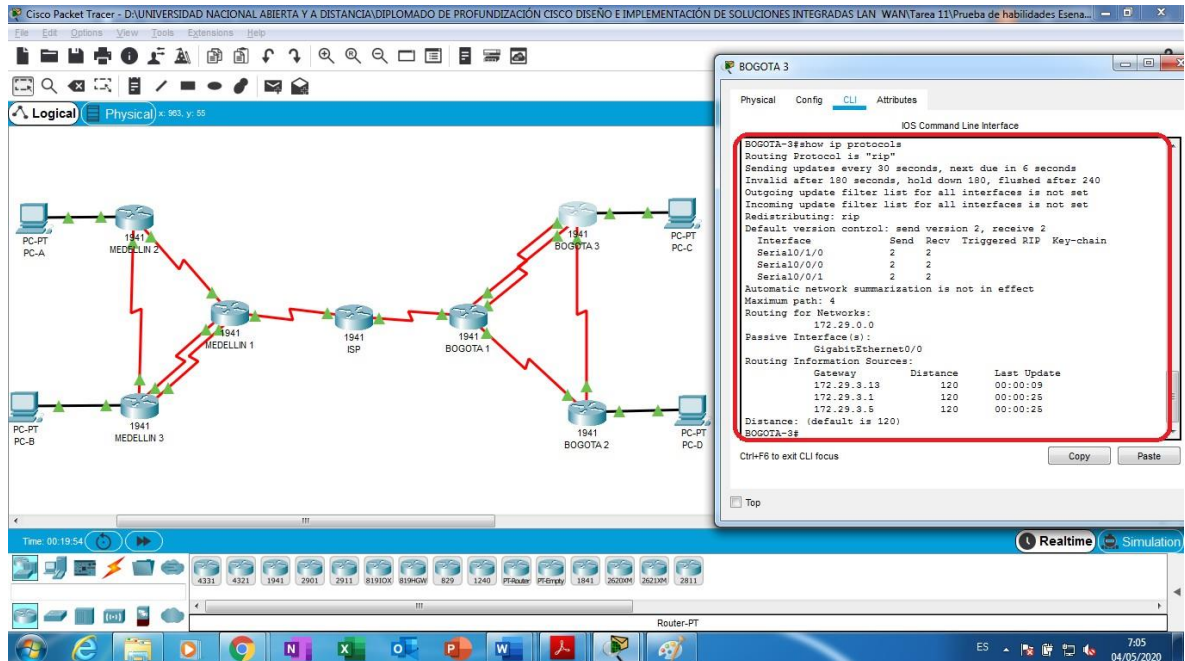


Figura 42. BOGOTA-3#show ip protocols



- b. Se verifica y documenta la base de datos de OSPF de cada Router, donde se informa de manera detallada de todas las rutas hacia cada red. En la tabla 29 se pueden ver las rutas que están conectadas y el puerto de conexión.

Tabla 29. Rutas y puerto de conexión.

Elemento o tarea de configuración	Especificación
Router MEDELLIN-1	MEDELLIN-1#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
Router MEDELLIN-2	MEDELLIN-2#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
Router MEDELLIN-3	MEDELLIN-3#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 BOGOTA-1	BOGOTA-1#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
Router BOGOTA-2	BOGOTA-2#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
Router BOGOTA-3	BOGOTA-3#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

4.2.5 PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

- a. Según los requisitos de la topología el enlace Medellín1 con ISP se configura con autenticación PAT, ver tabla 30.

Tabla 30. Autenticación PAT

Elemento o tarea de configuración	Especificación
Router ISP	ISP(config)#username MEDELLIN-1 password cisco ISP(config)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#exit
Router MEDELLIN-1	MEDELLIN-1(config)#username ISP password cisco MEDELLIN-1(config)#int s0/0/0 MEDELLIN-1(config-if)#encapsulation ppp MEDELLIN-1(config-if)#ppp authentication pap MEDELLIN-1(config-if)#ppp pap sent- username ISP password cisco MEDELLIN-1(config-if)#exit

- b. El enlace Bogotá1 con ISP se configura con autenticación CHAT, ver tabla 31.

Tabla 31. Autenticación CHAT.

Elemento o tarea de configuración	Especificación
Router ISP	<pre>ISP(config)#username BOGOTA-1 password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap ISP(config-if)#exit</pre>
Router BOGOTA-1	<pre>BOGOTA-1(config)#username ISP password cisco BOGOTA-1(config)#int s0/0/0 BOGOTA-1(config-if)#encapsulation ppp BOGOTA-1(config-if)#ppp authentication chap BOGOTA-1(config-if)#exit</pre>

4.2.6 PARTE 6: CONFIGURACIÓN DE PAT.

- 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.
- Se procede a configurar el NAT en el Router Medellín1. Se Comprueba que la traducción de direcciones indica las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección es traducida automáticamente a la dirección de la interfaz serial 0/1/0 del Router Medellín1, cómo diferente puerto.
- Se configurar el NAT en el Router Bogotá1. Se comprueba que la traducción de direcciones indica las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección es traducida automáticamente a la dirección de la interfaz serial 0/1/0 del Router Bogotá1, cómo diferente puerto.

Para la solución de la parte 6 del cosa dos todo el desarrollo está contenido en la tabla 32.

Tabla 32. Configuración de PAT

Elemento o tarea de configuración	Especificación
Router MEDELLIN-1	<pre> MEDELLIN-1(config)#ip nat inside source list 1 interface s0/0/0 overload MEDELLIN-1(config)#access-list 1 permit 172.29.4.0 0.0.3.255 MEDELLIN-1(config)#int s0/0/0 MEDELLIN-1(config-if)#ip nat outside MEDELLIN-1(config-if)#int s0/0/1 MEDELLIN-1(config-if)#ip nat outside MEDELLIN-1(config-if)#int s0/1/0 MEDELLIN-1(config-if)#ip nat outside MEDELLIN-1(config-if)#int s0/1/1 MEDELLIN-1(config-if)#ip nat outside MEDELLIN-1(config-if)#exit </pre>
Router BOGOTA-1	<pre> BOGOTA-1(config)#ip nat inside source list 1 interface s0/0/0 overload BOGOTA-1(config)#access-list 1 permit 172.29.0.0 0.0.3.255 BOGOTA-1(config)#int s0/0/0 BOGOTA-1(config-if)#ip nat outside BOGOTA-1(config-if)#int s0/0/1 BOGOTA-1(config-if)#ip nat outside BOGOTA-1(config-if)#int s0/1/0 BOGOTA-1(config-if)#ip nat outside BOGOTA-1(config-if)#int s0/1/1 BOGOTA-1(config-if)#ip nat outside BOGOTA-1(config-if)#exit </pre>

4.2.7 PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

- a. Se configurará la red Medellín2 y Medellín3 con el Router Medellín 2 como el servidor DHCP para ambas redes LAN, ver tabla 33.
- b. El Router Medellín3 es habilitado para el paso de los mensajes broadcast hacia la IP del Router Medellín2, ver tabla 33.

Tabla 33. Configuración del servicio DHCP.

Elemento o tarea de configuración	Especificación
Router MEDELLIN-2	<pre> MEDELLIN-2(config)#ip dhcp excluded- address 172.29.4.1 172.29.4.5 MEDELLIN-2(config)#ip dhcp excluded- address 172.29.4.129 172.29.4.133 MEDELLIN-2(config)#ip dhcp pool MEDELLIN-2 MEDELLIN-2(dhcp-config)#network 172.29.4.0 255.255.255.128 MEDELLIN-2(dhcp-config)#default-router 172.29.4.1 MEDELLIN-2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN-2(dhcp-config)#exit MEDELLIN-2(config)#ip dhcp pool MEDELLIN-3 MEDELLIN-2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN-2(dhcp-config)#default-router 172.29.4.129 MEDELLIN-2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN-2(dhcp-config)#exit </pre>
Router MEDELLIN-3	<pre> MEDELLIN-3(config)#int g0/0 MEDELLIN-3(config-if)#ip helper-address 172.29.6.5 MEDELLIN-3(config-if)#exit MEDELLIN-3(config)# </pre>

- c. Se configura la red Bogotá2 y Bogotá3 con el Router Medellín2 como el servidor DHCP para ambas redes LAN, ver tabla 34.
- d. Se configura el Router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del Router Bogotá2, ver tabla 34.

Tabla 34. Configuración del servicio DHCP.

Elemento o tarea de configuración	Especificación
Router BOGOTA-2	BOGOTA-2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 BOGOTA-2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5 BOGOTA-2(config)#ip dhcp pool BOGOTA-2 BOGOTA-2(dhcp-config)#network 172.29.1.0 255.255.255.0 BOGOTA-2(dhcp-config)#default-router 172.29.1.1 BOGOTA-2(dhcp-config)#dns-server 8.8.8.8 BOGOTA-2(dhcp-config)#ip dhcp pool BOGOTA-3 BOGOTA-2(dhcp-config)#network 172.29.0.0 255.255.255.0 BOGOTA-2(dhcp-config)#default-router 172.29.0.1 BOGOTA-2(dhcp-config)#dns-server 8.8.8.8 BOGOTA-2(dhcp-config)#exit
Router BOGOTA-3	BOGOTA-3(config)#int g0/0 BOGOTA-3(config-if)#ip helper-address 172.29.3.13 BOGOTA-3(config-if)#exit

5. CONCLUSIONES

Se llevó a cabo la configuración 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.

Se llevó a cabo el desarrollo del estudio 2 en el cual una empresa posee sucursales en la ciudad de Bogotá y Medellín, requiere 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.

Se llevó a cabo la solución de los dos casos de estudio bajos el uso de la tecnología cisco, los cuales nos plantearon un escenario real y nos permitió el desarrollo de todos los conocimientos adquiridos duran el desarrollo del diplomado de profundización cisco, diseño e implementación de soluciones integradas LAN / WAN

6. REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>