

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA
CISCO

FRANK JOHAN RAMIREZ GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD.
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS – ECBTI.
PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES.
FLORENCIA
2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA
CISCO

FRANK JOHAN RAMIREZ GARCIA

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

ING. NILSON ALBEIRO FERREIRA.
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD.
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS – ECBTI.
PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES.
FLORENCIA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Florencia, 18 mayo de 2020

*Dedicado a mi familia, en especial
a mi madre Yolanda y mi hermana
Milena quienes con su gran amor
y cariño han hecho de mí una
mejor persona.*

AGRADECIMIENTOS

Agradezco primeramente a Dios por haberme dado la oportunidad de estar donde estoy.

A mi familia por ser ese gran pilar fundamental en mi vida y motivarme a ser mejor persona cada día.

A la universidad por darme la bienvenida al maravilloso mundo del conocimiento, brindarme las herramientas y oportunidades necesarias para culminar este proceso.

A mis profesores por compartir su conocimiento, su tiempo y paciencia para guiarme en este maravilloso proceso.

Al lector por dedicar parte de su tiempo en leer este trabajo.

CONTENIDO

1. INTRODUCCIÓN	12
2. OBJETIVOS.....	13
2.1 OBJETIVO GENERAL.....	13
2.2 OBJETIVOS ESPECÍFICOS	13
3 PLANTEAMIENTO DEL PROBLEMA	14
3.1 DEFINICIÓN DEL PROBLEMA	14
6 DESARROLLO DEL PROYECTO.....	15
6.1 ESCENARIO 1.....	15
Parte 1: Inicializar Dispositivos	16
Parte 2: Configurar los parámetros básicos de los dispositivos	16
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN.....	23
Parte 4: Configurar el protocolo de routing dinámico RIPv2.....	28
Parte 5: Implementar DHCP y NAT para IPv4	30
Parte 6: Configurar NTP.....	34
Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	34
6.2 ESCENARIO 2	37
Parte 1: Configuración del enrutamiento.....	38
Parte 2: Tabla de Enrutamiento.....	40
Parte 3: Deshabilitar la propagación del protocolo OSPF	47
Parte 4: Verificación del protocolo OSPF	48
Parte 5: Configurar encapsulamiento y autenticación PPP.....	53
Parte 6: Configuración de PAT.....	54
Parte 7: Configuración del servicio DHCP	57
7 CONCLUSIONES	62
8 BIBLIOGRAFÍA.....	63

LISTA DE TABLAS

	Pág.
Tabla 1. Configuración parámetros básicos. Desarrollo del proyecto	14
Tabla 2. Configuraciones parámetros básicos de dispositivos. Desarrollo del proyecto.	14
Tabla 3. Configuración R1. Desarrollo del proyecto.	16
Tabla 4. Configuración R2. Desarrollo del proyecto.	18
Tabla 5. Configuración R3. Desarrollo del proyecto.	19
Tabla 6. Configuración S1. Desarrollo del proyecto.	20
Tabla 7. Configuración S3. Desarrollo del proyecto.	20
Tabla 8. Verificación Conectividad. Desarrollo del proyecto.	22
Tabla 9. Configuración S1. Desarrollo del proyecto.	23
Tabla 10. Configuración S3. Desarrollo del proyecto.	24
Tabla 11. Configuración R1 Desarrollo del proyecto	24
Tabla 12. Verificación conectividad.	26
Tabla 13. Configuración RIPv2 en R1. Desarrollo del proyecto	27
Tabla 14. Configuración RIPv2 en R2. Desarrollo del proyecto.	28
Tabla 15. Configuración RIPv2 en R3. Desarrollo del proyecto	28
Tabla 16. Verificación RIP. Desarrollo del proyecto.	28
Tabla 17. Configuración R1 como servidor DHCP. Desarrollo del proyecto	29
Tabla 18. Configuración NAT. Desarrollo del proyecto	30
Tabla 19. Verificación protocolo DHCP y NAT. Desarrollo del proyecto	32
Tabla 20. Configuración NTP. Desarrollo del proyecto.	33
Tabla 21. Restricción líneas VTY R2. Desarrollo del proyecto	34
Tabla 22. Tabla comando CLI. Desarrollo del proyecto	35
Tabla 23. Descripción topología escenario 2. Desarrollo del proyecto	46

LISTA DE FIGURAS

	Pág.
Figura 1. Topología de red Escenario 1.	14
Figura 2. Ping R1 –R2.	21
Figura 3. Ping R2 – R3.	21
Figura 4. Ping Pc Internet – Gateway.	22
Figura 5. Ping S1-R1.	25
Figura 6. Ping S3 – R1	25
Figura 7. Ping S1- R1.	26
Figura 8. Ping S3 – R1.	26
Figura 9. DHCP – PCA.	31
Figura 10. DHCP - PC-C.	31
Figura 11. Ping PC-A – PC-C.	34
Figura 12. Servidor Web 209.165.200.229	32
Figura 13. Topología de red Escenario 2.	36
Figura 14. Ping PC-1 Medellin1 S0/0/0	54
Figura 15. Ping PC-3 Bogota1 S0/0/0	56
Figura 16. Ping PC3 – PC4.	58
Figura 17. Ping PC1- PC2.	58
Figura 18. Ping PC4 – Router ISP S0/0/0.	60
Figura 19. Ping PC2- Router ISP S0/0/0.	60
Figura 20. Ping PC2 – PC3.	61

GLOSARIO

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

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

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

Encapsulamiento: Es el proceso en el que los datos que se encuentran dispuestos para ser enviados a través de una red se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red

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

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

Ping: Comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

Protocolos de enrutamiento: Conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.

Lista de Control de Acceso o ACL: Es un concepto de seguridad informática usado para fomentar la separación de privilegios

El protocolo de tiempo de red o NTP: protocolo para sincronizar varios relojes de red usando un conjunto de clientes y servidores repartidos.

El Protocolo de Información de Encaminamiento, Routing Information Protocol (RIP): Es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP).

RESUMEN

En este trabajo se plantean dos problemas llamados casos de Estudio, los cuales son analizados y simulados utilizando el software Packet Tracer de propiedad de CISCO con sus diferentes dispositivos.

El primer escenario se configura 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.

El segundo escenario es una empresa que posee dos sucursales distribuidas en las ciudades de Bogotá y Medellín, donde se configuraron e interconectaron entre sí cada uno de los dispositivos que forman parte de las sucursales, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

PALABRAS CLAVE: Topología de red, DHCP, RIPv2, NAT.

ABSTRACT

In this work, two problems are called study cases, which are analyzed and simulated using CISCO's proprietary Packet Tracer software with its different devices.

The first scenario is configuring a small network to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, RIPv2 dynamic routing protocol, dynamic host configuration protocol (DHCP), dynamic network address translation, and Static (NAT), Access Control Lists (ACL) and Network Time Protocol (NTP) server / client.

The second scenario is a company that has two branches distributed in the cities of Bogotá and Medellín, where each of the devices that are part of the branches were configured and interconnected, in accordance with the guidelines established for IP addressing, protocols for routing and other aspects that are part of the network topology.

1. INTRODUCCIÓN

Con el desarrollo del presente trabajo se busca dar solución a los casos de estudios propuestos, bajo el uso de tecnología CISCO, donde se desarrolló la parte práctica de los cursos CP CCNA1- CP CCNA2.

En la topología planteada para el primer escenario se procede a inicializar, configurar y verificar los parámetros básicos de los dispositivos entre los cuales se encuentran: Seguridad del switch, VLAN y el routing entre VLAN, Protocolo de routing dinámico RIPv2, NTP (Network Time Protocol), Listas de control de acceso (ACL), DHCP y NAT para IPv4.

El segundo escenario es una empresa que posee dos sucursales distribuidas en las ciudades de Bogotá y Medellín, donde se realiza la conexión física de los equipos con base en la topología de red planteada, se configura el enrutamiento, se deshabilita la propagación del protocolo OSPF, se verifica el protocolo OSPF, se configura el encapsulamiento y la autenticación PPP, el PAT (Port Address Translation) y el servicio DHCP.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar la práctica de los conocimientos adquiridos durante el diplomado de profundización CISCO, consistente en dos módulos CCNA1 y CCNA2, utilizando el software Packet Tracer.

2.2 OBJETIVOS ESPECÍFICOS

- Analizar e implementar la simulación de la arquitectura propuesta por medio del software Packet Tracer.
- Implementar el enrutamiento OSPF y el RIPv2 en cada uno de los escenarios de acuerdo con los requerimientos establecidos.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

En la topología del primer escenario se plantea el problema de configurar y verificar los parámetros básicos de los dispositivos, Seguridad del switch, VLAN y el routing entre VLAN, Protocolo de routing dinámico RIPv2, NTP (Network Time Protocol), Listas de control de acceso (ACL), DHCP y NAT para IPv4.

El segundo escenario es una empresa que posee dos sucursales distribuidas en las ciudades de Bogotá y Medellín, del cual surge la necesidad de conectar físicamente los equipos con base en la topología de red planteada, configurar el enrutamiento, deshabilitar la propagación del protocolo OSPF, verificar el protocolo OSPF, configurar el encapsulamiento y la autenticación PPP, el PAT (Port Address Translation) y el servicio DHCP.

6 DESARROLLO DEL PROYECTO

6.1 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

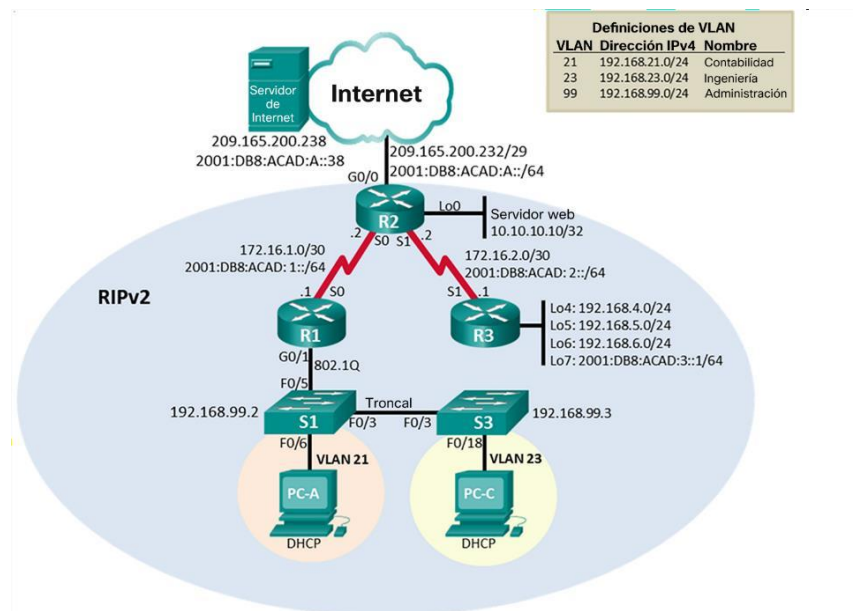


Figura 1. Topología de red escenario 1.

Parte 1: Inicializar Dispositivos

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

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

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

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>en 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#show flash

Tabla 1. Configuración parámetros básicos. Desarrollo del problema.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2. Configuraciones parámetros básicos de dispositivos. Desarrollo del proyecto.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#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

Tabla 3. Configuración R1. Desarrollo del proyecto.

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>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker.
Mensaje MOTD	R2(config)#banner motd # Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Tabla 4. Configuración R2. Desarrollo del proyecto.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd # Se prohíbe el acceso no autorizado.#

Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 5. Configuración R3. Desarrollo del proyecto.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>en Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login

Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd # Se prohíbe el acceso no autorizado. #

Tabla 6. Configuración S1. Desarrollo del proyecto.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación.
Desactivar la búsqueda DNS	Switch>en Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd # Se prohíbe el acceso no autorizado. #

Tabla 7. Configuración S3. Desarrollo del proyecto.

Paso 7: Verificar la conectividad de la red

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

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

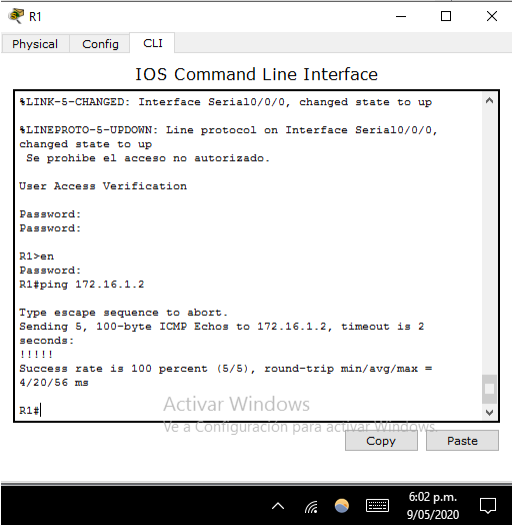
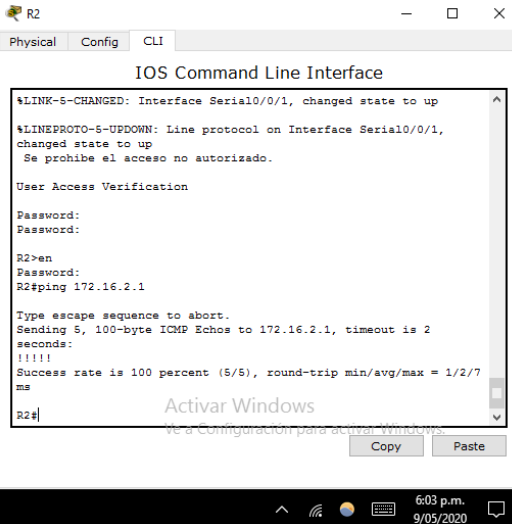
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 <pre> R1 Physical Config CLI IOS Command Line Interface %LINK-5-CHANGED: Interface Serial10/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/0, changed state to up Se prohíbe el acceso no autorizado. User Access Verification Password: Password: R1>en R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 4/20/56 ms R1# </pre>
R2	R3, S0/0/1	176.16.2.1	 <pre> R2 Physical Config CLI IOS Command Line Interface %LINK-5-CHANGED: Interface Serial10/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to up Se prohíbe el acceso no autorizado. User Access Verification Password: Password: R2>en R2#ping 176.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 176.16.2.1, timeout is 2 seconds: !!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms R2# </pre>

Figura 2. Ping R1 –R2.

Figura 3. Ping R2 – R3.

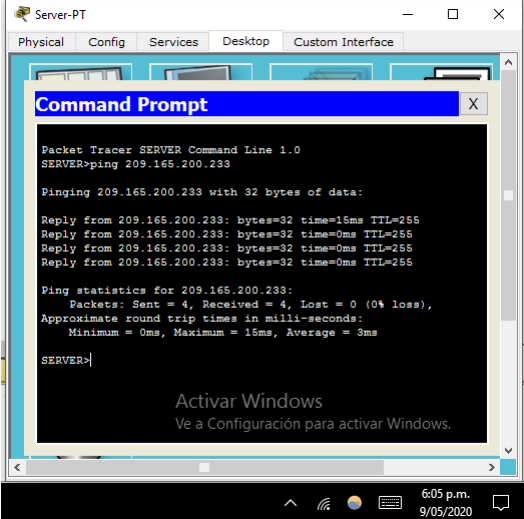
PC de Internet	Gateway predeterminado	209.165.200.233	 <p>Figura 4. Ping Pc Int – Gateway.</p>
----------------	------------------------	-----------------	--

Tabla 8. Verificación Conectividad. Desarrollo del proyecto.

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1#conf t S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Management S1(config-vlan)#exit</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit</pre>

Asignar el gateway predeterminado	<code>1(config)#ip default-gateway 192.168.99.1</code>
Forzar el enlace troncal en la interfaz F0/3	<code>S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</code>
Forzar el enlace troncal en la interfaz F0/5	<code>S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if-range)#switchport mode access</code>
Configurar el resto de los puertos como puertos de acceso	<code>S1(config-if)#int range f0/1-2, f0/4, f0/6-2, g0/1-2 S1(config-if-range)#switchport mode access</code>
Asignar F0/6 a la VLAN 21	<code>S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21</code>
Apagar todos los puertos sin usar	<code>S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown</code>

Tabla 9. Configuración S1. Desarrollo del proyecto.

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	<code>S3>en S3#conf t S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit</code>
Asignar la dirección IP de administración	<code>S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit</code>
Asignar el gateway predeterminado.	<code>S3(config)#ip default-gateway 192.168.99.1</code>

Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
Apagar todos los puertos sin usar	S3(config-if-range)#shutdown

Tabla 10. Configuración S3. Desarrollo del proyecto.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

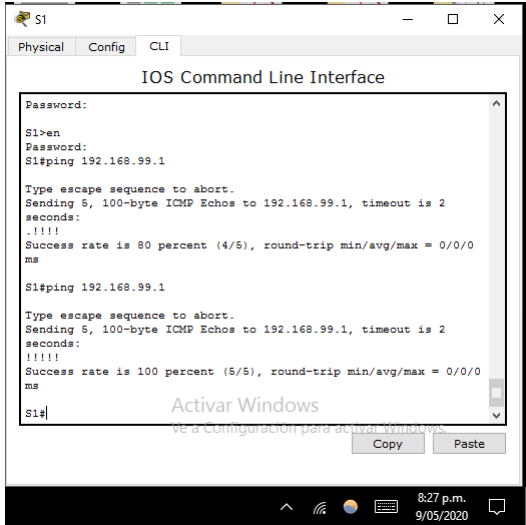
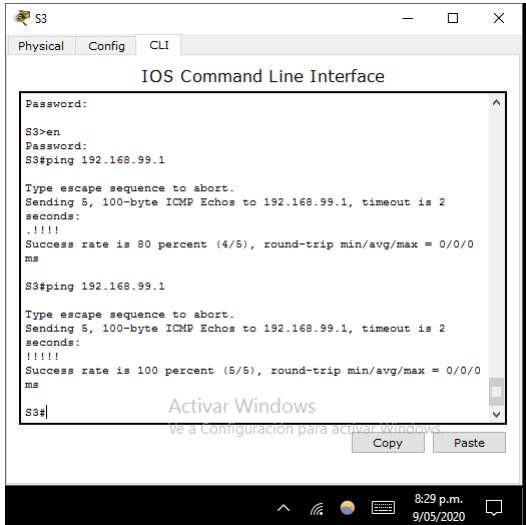
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>en R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int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

Tabla 11. Configuración R1. Desarrollo del proyecto.

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	 <p>Figure 5. Ping S1-R1.</p>
S3	R1, dirección VLAN 99	192.168.99.1	 <p>Figure 6. Ping S3 – R1.</p>

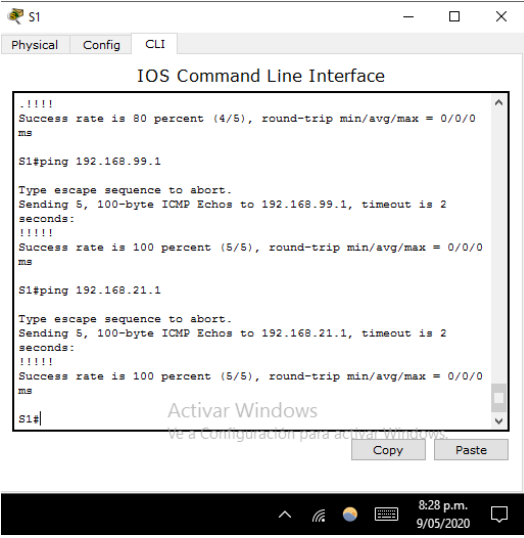
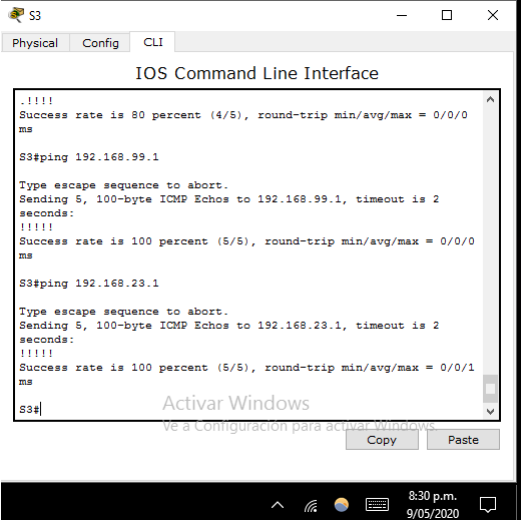
S1	R1, dirección VLAN 21	192.168.21.1	 <p>IOS Command Line Interface</p> <pre> Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to 192.168.99.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to 192.168.21.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1# </pre>
S3	R1, dirección VLAN 23	192.168.23.1	 <p>IOS Command Line Interface</p> <pre> Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to 192.168.99.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to 192.168.23.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms S3# </pre>

Figura 7. Ping S1- R1.

Figura 8. Ping S3 – R1.

Tabla 12 Verificacion conectividad.

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>en Password: R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13. Configuración RIPv2 en R1. Desarrollo del proyecto

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>en R2#conf t R2(config)#router rip R2(config-router)#version 2

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

Tabla 14. Configuración RIPv2 en R2. Desarrollo del proyecto.

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>en Password: R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
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 sumarización automática.	R3(config-router)#no auto-summary

Tabla 15. Configuración RIPv2 en R3. Desarrollo del proyecto

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?	#show ip protocols

¿Qué comando muestra solo las rutas RIP?	# show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	# show run

Tabla 16. Verificación RIP. Desarrollo del proyecto.

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>en R1#conf t R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com ^ % Invalid input detected at '^' marker.
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com ^ % Invalid input detected at '^' marker.

Tabla 17. Configuración R1 como servidor DHCP. Desarrollo del proyecto.

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

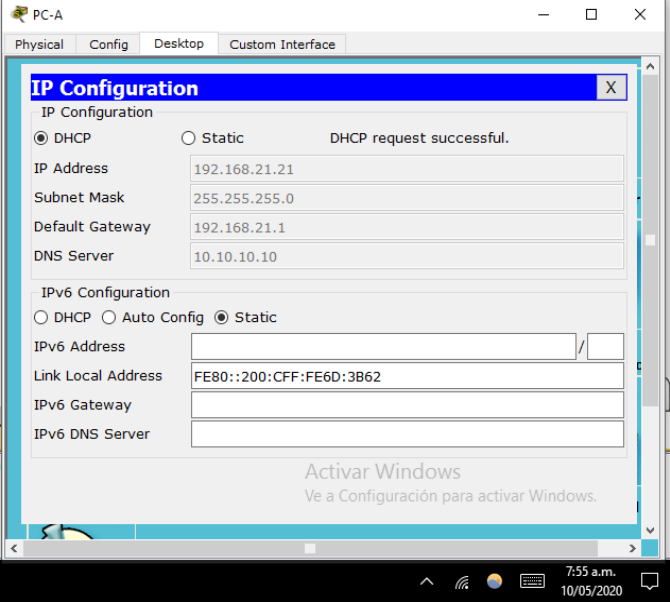
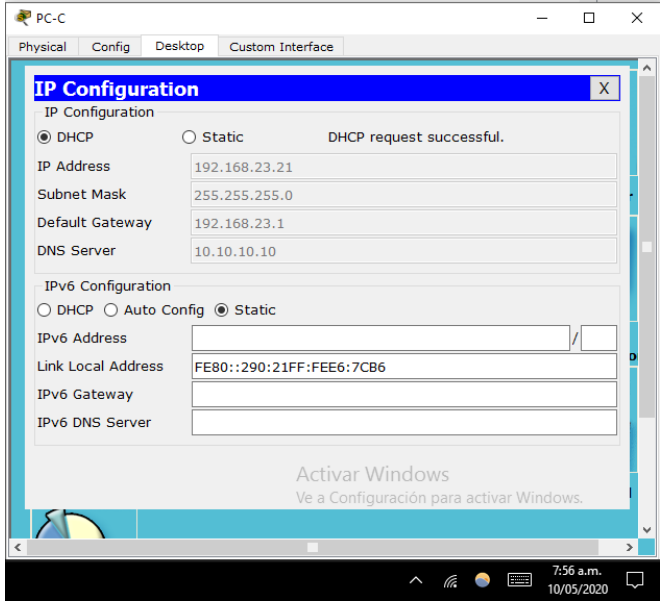
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2>en R2#conf t R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local ^ % Invalid input detected at '^' marker.
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 18. Configuración NAT. Desarrollo del proyecto

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
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	 <p>Figura 9. DHCP – PCA.</p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p>Figura 10. DHCP - PC-C.</p>

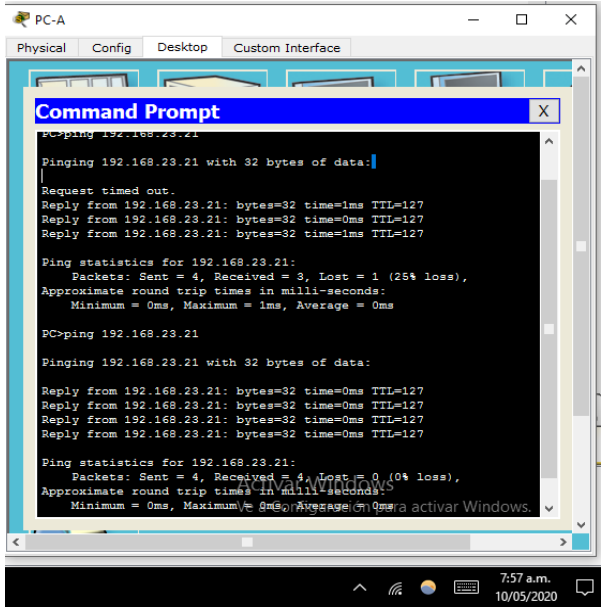
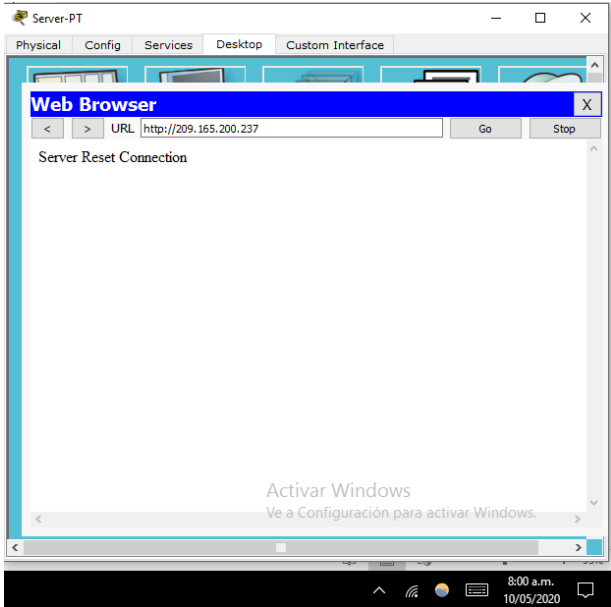
<p>Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	 <p>Figura 11. Ping PC-A – PC-C.</p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	 <p>Figura 12. Servidor Web 209.165.200.229</p>

Tabla 19. Verificación protocolo DHCP y NAT. Desarrollo del proyecto

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 12:23:00 10 may 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5 ^ % Invalid input detected at '^' marker.
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 R1(config)#end
Verifique la configuración de NTP en R1.	R1#show ntp associations ^ % Invalid input detected at '^' marker.

Tabla 20. Configuración NTP. Desarrollo del proyecto.

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	R2>en R2#conf t R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

<p>Verificar que la ACL funcione como se espera</p>	<pre> R1>en Password: R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open Se prohíbe el acceso no autorizado. User Access Verification Password: R2> ----- R3>en Password: R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host R3# </pre>
---	--

Tabla 21. Restriccion lineas VTY R2. Desarrollo del proyecto.

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

Descripción del comando	Comando
<p>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</p>	<pre> R2>en Password: R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) </pre>
<p>Restablecer los contadores de una lista de acceso</p>	<pre> R2# clear ip </pre>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<pre> R2# show ip interface </pre>
<p>¿Con qué comando se muestran las traducciones NAT?</p>	<pre> R2# show ip nat translations </pre>

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2# C lear i p nat t ranslations
--	---

Tabla 22. Tabla comando CLI. Desarrollo del proyecto

6.2 ESCENARIO 2

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

Topología de red

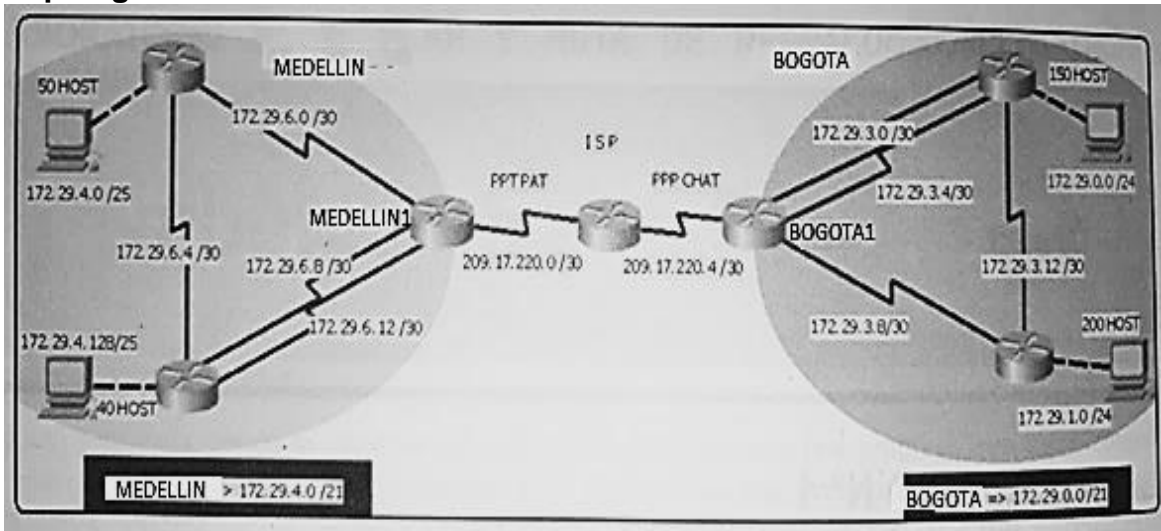


Figura 13. Topología de red Escenario 2.

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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

Parte 1: Configuración del enrutamiento.

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

```
!MEDELLIN1
router ospf 1
 log-adjacency-changes
 passive-interface Serial0/0/0
 network 172.29.6.0 0.0.0.3 area 0
 network 172.29.6.8 0.0.0.3 area 0
 network 172.29.6.12 0.0.0.3 area 0

!MEDELLIN2
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.29.4.0 0.0.0.127 area 0
 network 172.29.6.0 0.0.0.3 area 0
 network 172.29.6.4 0.0.0.3 area 0

!MEDELLIN3
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.29.4.128 0.0.0.127 area 0
 network 172.29.6.4 0.0.0.3 area 0
 network 172.29.6.8 0.0.0.3 area 0
 network 172.29.6.12 0.0.0.3 area 0
```

```

!BOGOTA1
router ospf 1
 log-adjacency-changes
 passive-interface Serial10/0/0
 network 172.29.3.0 0.0.0.3 area 0
 network 172.29.3.4 0.0.0.3 area 0
 network 172.29.3.8 0.0.0.3 area 0

```

```

!BOGOTA2
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.29.1.0 0.0.0.255 area 0
 network 172.29.3.8 0.0.0.3 area 0
 network 172.29.3.12 0.0.0.3 area 0

```

```

!BOGOTA3
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.29.0.0 0.0.0.255 area 0
 network 172.29.3.0 0.0.0.3 area 0
 network 172.29.3.4 0.0.0.3 area 0
 network 172.29.3.12 0.0.0.3 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.

```

!MEDELLIN
ip route 0.0.0.0 0.0.0.0 209.17.220.1
router ospf 1
 default-information originate

```

```

!BOGOTA1
ip route 0.0.0.0 0.0.0.0 209.17.220.5
router ospf 1
 default-information originate

```

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

```

ip route 172.29.4.0 255.255.252.0 209.17.220.2
ip route 172.29.0.0 255.255.252.0 209.17.220.6

```

Parte 2: Tabla de Enrutamiento.

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

```
!MEDELLIN1
```

```
MEDELLIN#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 209.17.220.1 to network 0.0.0.0
```

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks  
O 172.29.4.0/25 [110/65] via 172.29.6.2, 00:12:53, Serial0/0/1  
O 172.29.4.128/25 [110/65] via 172.29.6.10, 00:10:14, Serial0/1/0  
C 172.29.6.0/30 is directly connected, Serial0/0/1  
L 172.29.6.1/32 is directly connected, Serial0/0/1  
O 172.29.6.4/30 [110/128] via 172.29.6.2, 00:10:14, Serial0/0/1  
[110/128] via 172.29.6.10, 00:10:14, Serial0/1/0  
C 172.29.6.8/30 is directly connected, Serial0/1/0 L  
172.29.6.9/32 is directly connected, Serial0/1/0 C  
172.29.6.12/30 is directly connected, Serial0/1/1  
L 172.29.6.13/32 is directly connected, Serial0/1/1  
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks  
C 209.17.220.0/30 is directly connected, Serial0/0/0  
C 209.17.220.1/32 is directly connected, Serial0/0/0  
L 209.17.220.2/32 is directly connected, Serial0/0/0  
S* 0.0.0.0/0 [1/0] via 209.17.220.1
```

```
!MEDELLIN2
```

```
MEDELLIN2#show ip ro
```

```
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 172.29.6.1 to network 0.0.0.0
```



```

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C    172.29.4.0/25 is directly connected, GigabitEthernet0/0
L    172.29.4.1/32 is directly connected, GigabitEthernet0/0
O    172.29.4.128/25 [110/65] via 172.29.6.6, 00:12:39, Serial0/0/1
C    172.29.6.0/30 is directly connected, Serial0/0/0
L    172.29.6.2/32 is directly connected, Serial0/0/0
C    172.29.6.4/30 is directly connected, Serial0/0/1
L    172.29.6.5/32 is directly connected, Serial0/0/1
O    172.29.6.8/30 [110/128] via 172.29.6.1, 00:12:39, Serial0/0/0
      [110/128] via 172.29.6.6, 00:12:39, Serial0/0/1
O    172.29.6.12/30 [110/128] via 172.29.6.1, 00:12:39, Serial0/0/0
      [110/128] via 172.29.6.6, 00:12:39, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:15:18, Serial0/0/0

```

!MEDELLIN3

MEDELLIN3#show ip ro

```

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 172.29.6.9 to network 0.0.0.0

```

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
O    172.29.4.0/25 [110/65] via 172.29.6.5, 00:13:03, Serial0/1/0
C    172.29.4.128/25 is directly connected, GigabitEthernet0/0
L    172.29.4.129/32 is directly connected, GigabitEthernet0/0
O    172.29.6.0/30 [110/128] via 172.29.6.5, 00:13:03, Serial0/1/0
      [110/128] via 172.29.6.9, 00:13:03, Serial0/0/0
C    172.29.6.4/30 is directly connected, Serial0/1/0 L
      172.29.6.6/32 is directly connected, Serial0/1/0
C    172.29.6.8/30 is directly connected, Serial0/0/0 L
      172.29.6.10/32 is directly connected, Serial0/0/0
C    172.29.6.12/30 is directly connected, Serial0/0/1
L    172.29.6.14/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.9, 00:13:03, Serial0/0/0

```

!BOGOTA1

BOGOTA#show ip ro

```

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 209.17.220.5 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.2, 00:05:53, Serial0/1/0
O    172.29.1.0/24 [110/65] via 172.29.3.10, 00:08:27, Serial0/0/1
C    172.29.3.0/30 is directly connected, Serial0/1/0
L    172.29.3.1/32 is directly connected, Serial0/1/0
C    172.29.3.4/30 is directly connected, Serial0/1/1
L    172.29.3.5/32 is directly connected, Serial0/1/1
C    172.29.3.8/30 is directly connected, Serial0/0/1
L    172.29.3.9/32 is directly connected, Serial0/0/1
O    172.29.3.12/30 [110/128] via 172.29.3.2, 00:05:43, Serial0/1/0
      [110/128] via 172.29.3.10, 00:05:43, Serial0/0/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C    209.17.220.4/30 is directly connected, Serial0/0/0
C    209.17.220.5/32 is directly connected, Serial0/0/0
L    209.17.220.6/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.5
```

!BOGOTA2

Router#show ip ro

```
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 172.29.3.9 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.14, 00:06:04, Serial0/0/1
C    172.29.1.0/24 is directly connected, GigabitEthernet0/0
L    172.29.1.1/32 is directly connected, GigabitEthernet0/0
O    172.29.3.0/30 [110/128] via 172.29.3.9, 00:06:04, Serial0/0/0
      [110/128] via 172.29.3.14, 00:06:04, Serial0/0/1
O    172.29.3.4/30 [110/128] via 172.29.3.9, 00:06:04, Serial0/0/0
      [110/128] via 172.29.3.14, 00:06:04, Serial0/0/1
C    172.29.3.8/30 is directly connected, Serial0/0/0 L
      172.29.3.10/32 is directly connected, Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
L    172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:08:48, Serial0/0/0
```

!BOGOTA3

Router#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 172.29.3.1 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C    172.29.0.0/24 is directly connected, GigabitEthernet0/0
L    172.29.0.1/32 is directly connected, GigabitEthernet0/0
O    172.29.1.0/24 [110/65] via 172.29.3.13, 00:06:21, Serial0/1/0
C    172.29.3.0/30 is directly connected, Serial0/0/0
L    172.29.3.2/32 is directly connected, Serial0/0/0
C    172.29.3.4/30 is directly connected, Serial0/0/1
L    172.29.3.6/32 is directly connected, Serial0/0/1
O    172.29.3.8/30 [110/128] via 172.29.3.1, 00:06:21, Serial0/0/0
      [110/128] via 172.29.3.13, 00:06:21, Serial0/1/0
C    172.29.3.12/30 is directly connected, Serial0/1/0
L    172.29.3.14/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:06:31, Serial0/0/0
```

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

Se ve también en Parte 2: a. las rutas OSPF (O) con doble ruta hacia un mismo destino. Por ejemplo se resalta en negrita en uno de los routers:

!MEDELLIN1

MEDELLIN#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 209.17.220.1 to network 0.0.0.0

```

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O   172.29.4.0/25 [110/65] via 172.29.6.2, 00:12:53, Serial0/0/1
O   172.29.4.128/25 [110/65] via 172.29.6.10, 00:10:14, Serial0/1/0
C   172.29.6.0/30 is directly connected, Serial0/0/1
L   172.29.6.1/32 is directly connected, Serial0/0/1
O   172.29.6.4/30 [110/128] via 172.29.6.2, 00:10:14, Serial0/0/1
    [110/128] via 172.29.6.10, 00:10:14, Serial0/1/0
C   172.29.6.8/30 is directly connected, Serial0/1/0 L
    172.29.6.9/32 is directly connected, Serial0/1/0 C
    172.29.6.12/30 is directly connected, Serial0/1/1
L   172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C   209.17.220.0/30 is directly connected, Serial0/0/0
C   209.17.220.1/32 is directly connected, Serial0/0/0
L   209.17.220.2/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.1

```

- 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.

!MEDELLIN1

MEDELLIN#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 209.17.220.1 to network 0.0.0.0

```

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O   172.29.4.0/25 [110/65] via 172.29.6.2, 00:12:53, Serial0/0/1
O   172.29.4.128/25 [110/65] via 172.29.6.10, 00:10:14, Serial0/1/0
C   172.29.6.0/30 is directly connected, Serial0/0/1
L   172.29.6.1/32 is directly connected, Serial0/0/1
O   172.29.6.4/30 [110/128] via 172.29.6.2, 00:10:14, Serial0/0/1
    [110/128] via 172.29.6.10, 00:10:14, Serial0/1/0
C   172.29.6.8/30 is directly connected, Serial0/1/0 L
    172.29.6.9/32 is directly connected, Serial0/1/0 C
    172.29.6.12/30 is directly connected, Serial0/1/1
L   172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C   209.17.220.0/30 is directly connected, Serial0/0/0
C   209.17.220.1/32 is directly connected, Serial0/0/0
L   209.17.220.2/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.1

```

!BOGOTA1

BOGOTA#show ip ro

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 209.17.220.5 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.2, 00:05:53, Serial0/1/0
O    172.29.1.0/24 [110/65] via 172.29.3.10, 00:08:27, Serial0/0/1
C    172.29.3.0/30 is directly connected, Serial0/1/0
L    172.29.3.1/32 is directly connected, Serial0/1/0
C    172.29.3.4/30 is directly connected, Serial0/1/1
L    172.29.3.5/32 is directly connected, Serial0/1/1
C    172.29.3.8/30 is directly connected, Serial0/0/1
L    172.29.3.9/32 is directly connected, Serial0/0/1
O    172.29.3.12/30 [110/128] via 172.29.3.2, 00:05:43, Serial0/1/0
      [110/128] via 172.29.3.10, 00:05:43, Serial0/0/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C    209.17.220.4/30 is directly connected, Serial0/0/0
C    209.17.220.5/32 is directly connected, Serial0/0/0
L    209.17.220.6/32 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 209.17.220.5
```

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

!MEDELLIN2

MEDELLIN2#show ip ro

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 172.29.6.1 to network 0.0.0.0

```

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C    172.29.4.0/25 is directly connected, GigabitEthernet0/0
L    172.29.4.1/32 is directly connected, GigabitEthernet0/0
O    172.29.4.128/25 [110/65] via 172.29.6.6, 00:12:39, Serial0/0/1
C    172.29.6.0/30 is directly connected, Serial0/0/0
L    172.29.6.2/32 is directly connected, Serial0/0/0
C    172.29.6.4/30 is directly connected, Serial0/0/1
L    172.29.6.5/32 is directly connected, Serial0/0/1
O    172.29.6.8/30 [110/128] via 172.29.6.1, 00:12:39, Serial0/0/0
      [110/128] via 172.29.6.6, 00:12:39, Serial0/0/1
      172.29.6.12/30 [110/128] via 172.29.6.1, 00:12:39, Serial0/0/0
      [110/128] via 172.29.6.6, 00:12:39, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:15:18, Serial0/0/0

```

!BOGOTA2

Router#show ip ro

```

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 172.29.3.9 to network 0.0.0.0

```

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    172.29.0.0/24 [110/65] via 172.29.3.14, 00:06:04, Serial0/0/1
C    172.29.1.0/24 is directly connected, GigabitEthernet0/0
L    172.29.1.1/32 is directly connected, GigabitEthernet0/0
O    172.29.3.0/30 [110/128] via 172.29.3.9, 00:06:04, Serial0/0/0
      [110/128] via 172.29.3.14, 00:06:04, Serial0/0/1
O    172.29.3.4/30 [110/128] via 172.29.3.9, 00:06:04, Serial0/0/0
      [110/128] via 172.29.3.14, 00:06:04, Serial0/0/1
C    172.29.3.8/30 is directly connected, Serial0/0/0 L
      172.29.3.10/32 is directly connected, Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
L    172.29.3.13/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:08:48, Serial0/0/0

```

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

Se ve también en Parte 2: a. las rutas OSPF (O) con doble ruta hacia un mismo destino.

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

ISP#show ip ro

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

```

172.29.0.0/22 is subnetted, 2 subnets
S    172.29.0.0/22 [1/0] via 209.17.220.6
S    172.29.4.0/22 [1/0] via 209.17.220.2
209.17.220.0/24 is variably subnetted, 6 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    209.17.220.2/32 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
C    209.17.220.6/32 is directly connected, Serial0/0/1

```

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 23. Descripción topología escenario 2. Desarrollo del proyecto.

```

!MEDELLIN1
router ospf 1
passive-interface Serial0/0/0

!MEDELLIN2
router ospf 1
passive-interface GigabitEthernet0/0

!MEDELLIN3
router ospf 1
passive-interface GigabitEthernet0/0

!BOGOTA1
router ospf 1
passive-interface Serial0/0/0

!BOGOTA2
router ospf 1
passive-interface GigabitEthernet0/0

!BOGOTA3
router ospf 1
passive-interface GigabitEthernet0/0

```

Parte 4: Verificación del protocolo OSPF.

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

```

!MEDELLIN1
MEDELLIN#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.2
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway          Distance          Last Update

```



```

172.29.6.5          110      00:24:57
172.29.6.14         110      00:24:38
209.17.220.2        110      00:24:38
Distance: (default is 110)

```

!MEDELLIN2

MEDELLIN2#show ip pro

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 172.29.6.5

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.4.0 0.0.0.127 area 0

172.29.6.0 0.0.0.3 area 0

172.29.6.4 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
172.29.6.5	110	00:25:39
172.29.6.14	110	00:25:19
209.17.220.2	110	00:25:19

Distance: (default is 110)

!MEDELLIN3

MEDELLIN3#show ip pro

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 172.29.6.14

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

172.29.4.128 0.0.0.127 area 0

172.29.6.4 0.0.0.3 area 0

172.29.6.8 0.0.0.3 area 0

172.29.6.12 0.0.0.3 area 0

Passive Interface(s):

GigabitEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
172.29.6.5	110	00:26:01
172.29.6.14	110	00:25:42
209.17.220.2	110	00:25:42

Distance: (default is 110)

```
!BOGOTA1
BOGOTA#show ip pro
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.6
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:18:21
    172.29.3.14      110          00:18:21
    209.17.220.6     110          00:18:35
  Distance: (default is 110)
```

```
!BOGOTA2
BOGOTA2#show ip pro
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.13
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.1.0 0.0.0.255 area 0
    172.29.3.8 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:18:42
    172.29.3.14      110          00:18:42
    209.17.220.6     110          00:18:56
  Distance: (default is 110)
```

```
!BOGOTA3
BOGOTA3#show ip pro
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.255 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13     110          00:18:59
    172.29.3.14     110          00:18:59
    209.17.220.6    110          00:19:13
  Distance: (default is 110)
```

- 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.

```
!MEDELLIN1
MEDELLIN1#show ip ospf database
          OSPF Router with ID (209.17.220.2) (Process ID 1)
```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.29.6.5	172.29.6.5	1655	0x80000005	0x000c2b	5
209.17.220.2	209.17.220.2	1636	0x80000007	0x007dee	6
172.29.6.14	172.29.6.14	1636	0x80000007	0x00255e	7

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.2	377	0x80000002	0x001cf3	1

!MEDELLIN2

MEDELLIN2#show ip ospf data

OSPF Router with ID (172.29.6.5) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.29.6.5	172.29.6.5	1671	0x80000005	0x000c2b	5
172.29.6.14	172.29.6.14	1651	0x80000007	0x00255e	7
209.17.220.2	209.17.220.2	1651	0x80000007	0x007dee	6

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.2	393	0x80000002	0x001cf3	1

!MEDELLIN3

MEDELLIN3#show ip ospf data

OSPF Router with ID (172.29.6.14) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.29.6.5	172.29.6.5	1686	0x80000005	0x000c2b	5
172.29.6.14	172.29.6.14	1667	0x80000007	0x00255e	7
209.17.220.2	209.17.220.2	1667	0x80000007	0x007dee	6

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.2	409	0x80000002	0x001cf3	1

!BOGOTA1

BOGOTA#show ip ospf data

OSPF Router with ID (209.17.220.6) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
209.17.220.6	209.17.220.6	1244	0x80000007	0x00ea9c	6
172.29.3.13	172.29.3.13	1230	0x80000005	0x00c7d3	5
172.29.3.14	172.29.3.14	1230	0x80000007	0x00d1d1	7

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.6	1556	0x80000001	0x000607	1

```

!BOGOTA2
BOGOTA2#show ip ospf data
      OSPF Router with ID (172.29.3.13) (Process ID 1)

```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
209.17.220.6	209.17.220.6	1261	0x80000007	0x00ea9c	6
172.29.3.13	172.29.3.13	1247	0x80000005	0x00c7d3	5
172.29.3.14	172.29.3.14	1247	0x80000007	0x00d1d1	7

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.6	1572	0x80000001	0x000607	1

```

!BOGOTA3
BOGOTA3#show ip ospf data
      OSPF Router with ID (172.29.3.14) (Process ID 1)

```

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
209.17.220.6	209.17.220.6	1278	0x80000007	0x00ea9c	6
172.29.3.14	172.29.3.14	1264	0x80000007	0x00d1d1	7
172.29.3.13	172.29.3.13	1264	0x80000005	0x00c7d3	5

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
0.0.0.0	209.17.220.6	1589	0x80000001	0x000607	1

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Nota: La autenticación debería ser PAP

```

jISP
!
username MEDELLIN password cisco
!
interface Serial0/0/0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username ISP password 0 cisco
!

```

```

jMEDELLIN1
username ISP password cisco
interface Serial0/0/0
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username MEDELLIN password 0 cisco
!

```

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

Nota: La autenticación debería ser CHAP

```

jISP
username BOGOTA password cisco
interface Serial0/0/1
  encapsulation ppp
  ppp authentication chap

```

```

jBOGOTA1
username ISP password cisco
interface Serial0/0/0
  encapsulation ppp
  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.

- 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, como diferente puerto.

```
!MWEDELLIN1
ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 172.29.4.0 0.0.3.255
interface Serial0/0/0
ip nat outside
!
interface Serial0/0/1
ip nat inside
!
interface Serial0/1/0
ip nat inside
!
interface Serial0/1/1
ip nat inside
```

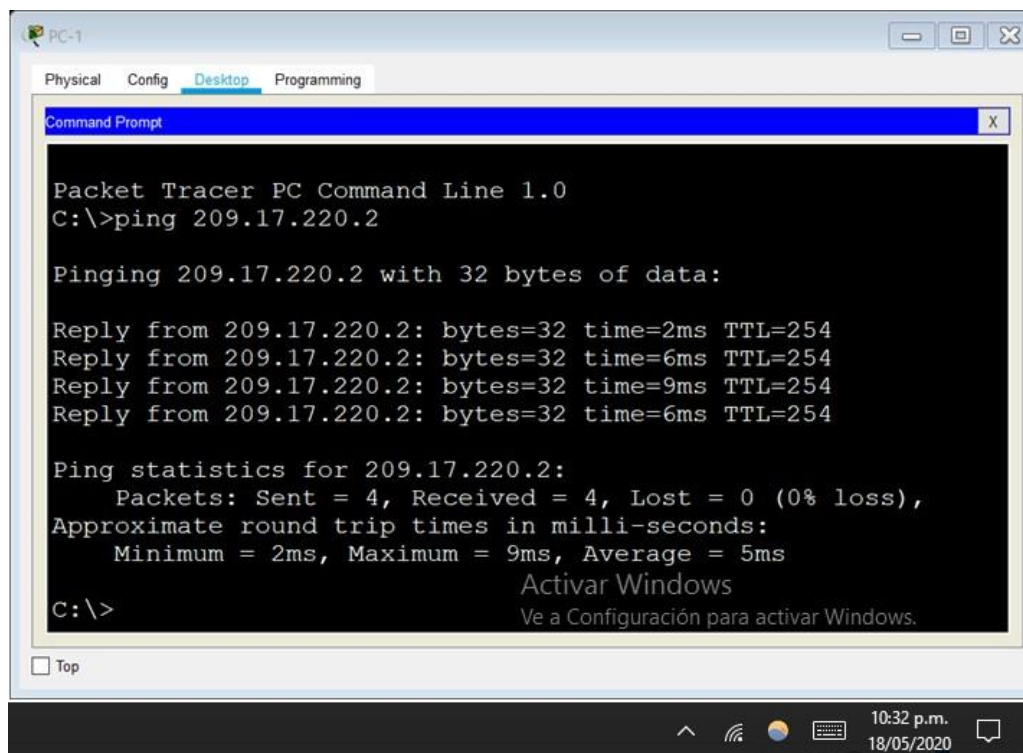


Figura 14. Ping PC-1 - Medellin1 S0/0/0.

```
MEDELLIN#show ip nat trans
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.17.220.2:29	172.29.4.6:29	209.17.220.1:29	209.17.220.1:29
icmp	209.17.220.2:30	172.29.4.6:30	209.17.220.1:30	209.17.220.1:30
icmp	209.17.220.2:31	172.29.4.6:31	209.17.220.1:31	209.17.220.1:31
icmp	209.17.220.2:32	172.29.4.6:32	209.17.220.1:32	209.17.220.1:32

- 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, como diferente puerto.

```
!BOGOTA1
ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 172.29.0.0 0.0.3.255
!
interface Serial0/0/0
 ip nat outside
!
interface Serial0/0/1
 ip nat inside

interface Serial0/1/0
 ip nat inside
!
interface Serial0/1/1
 ip nat inside
!
```

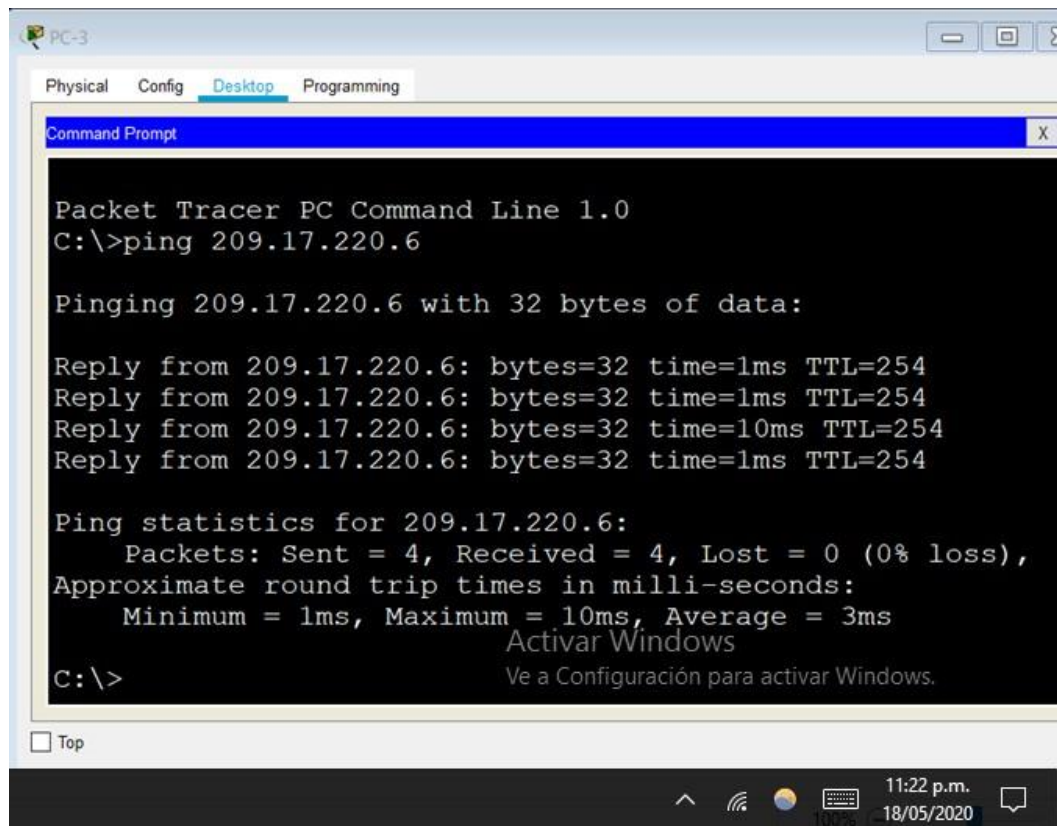



Figura 15. Ping PC-3 - Bogota1 S0/0/0.

BOGOTA#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.17.220.6:1	172.29.0.6:1	209.17.220.5:1	209.17.220.5:1
icmp	209.17.220.6:2	172.29.0.6:2	209.17.220.5:2	209.17.220.5:2
icmp	209.17.220.6:3	172.29.0.6:3	209.17.220.5:3	209.17.220.5:3
icmp	209.17.220.6:4	172.29.0.6:4	209.17.220.5:4	209.17.220.5:4

Parte 7: Configuración del servicio DHCP.

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

MEDELLIN2

```

ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.129 172.29.4.133
!

```

```

ip dhcp pool MED2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.8.8
ip dhcp pool MED3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.8.8
!

```

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

!MEDELLIN3

```

interface GigabitEthernet0/0
ip helper-address 172.29.6.5

```

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

Nota: el servidor deberá ser Bogotá 2

```

!BOGOTA2
ip dhcp excluded-address 172.29.1.1 172.29.1.5
ip dhcp excluded-address 172.29.0.1 172.29.0.5
!
ip dhcp pool BOG2
network 172.29.1.0 255.255.255.0
default-router 172.29.1.1
dns-server 8.8.8.8
ip dhcp pool BOG3
network 172.29.0.0 255.255.255.0
default-router 172.29.0.1
dns-server 8.8.8.8
!

```

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

!BOGOTA3

```

interface GigabitEthernet0/0
ip helper-address 172.29.3.13

```

En la red Bogotá, se utiliza el comando ping entre los dispositivos PC-3 – PC-4 para demostrar la comunicación entre los dispositivos terminales de la red, se observa que el resultado es satisfactorio lo que demuestra la correcta implementación de los protocolos.

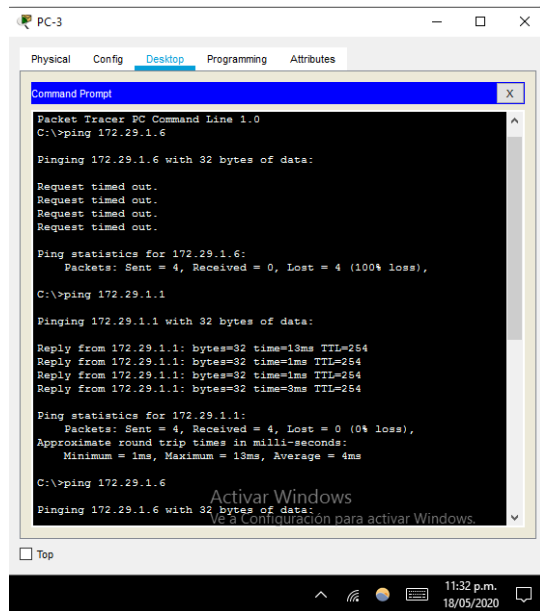


Figura 16. Ping PC3 – PC4.

En la red Medellín, se utiliza el comando ping entre los dispositivos PC1 – PC2 para demostrar la comunicación entre los dispositivos terminales de la red, se observa que el resultado es satisfactorio lo que demuestra la correcta implementación de los protocolos.

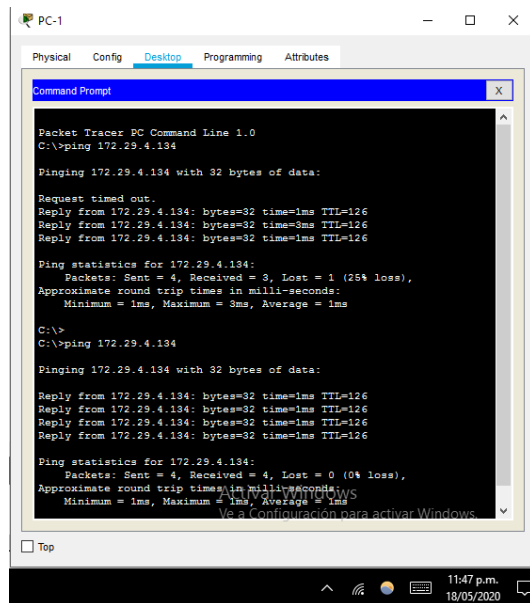
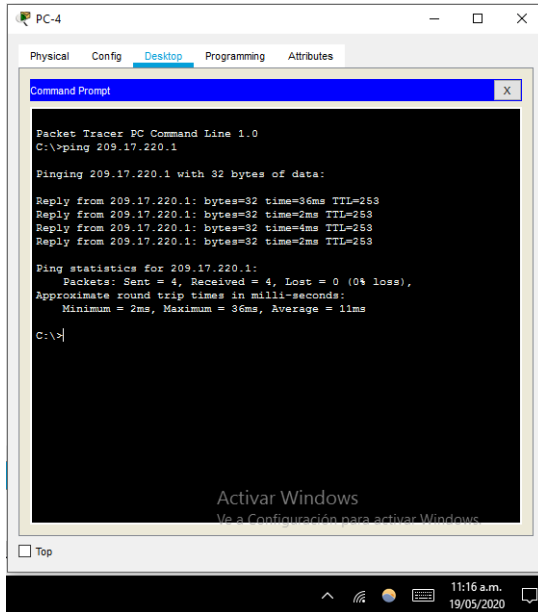


Figura 17. Ping PC1- PC2.

Se realiza ping desde el PC4 a la S0/0/0 del Router ISP, para comprobar la comunicación entre los hosts y el router ISP en la red Bogotá dando como resultado success.



```
Packet Tracer PC Command Line 1.0
C:\>ping 209.17.220.1

Pinging 209.17.220.1 with 32 bytes of data:

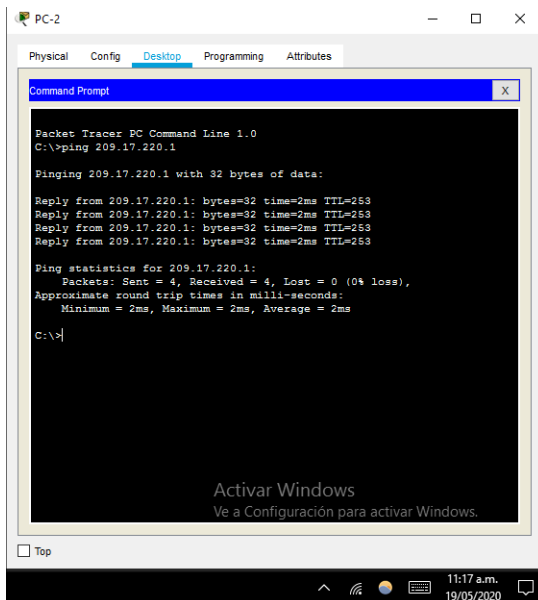
Reply from 209.17.220.1: bytes=32 time=36ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=4ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 36ms, Average = 11ms

C:\>
```

Figura 18. Ping PC4 – Router ISP S0/0/0.

Se realiza ping desde el PC2 a la S0/0/0 del Router ISP, para comprobar la comunicación entre los hosts y el router ISP en la red Medellín dando como resultado success.



```
Packet Tracer PC Command Line 1.0
C:\>ping 209.17.220.1

Pinging 209.17.220.1 with 32 bytes of data:

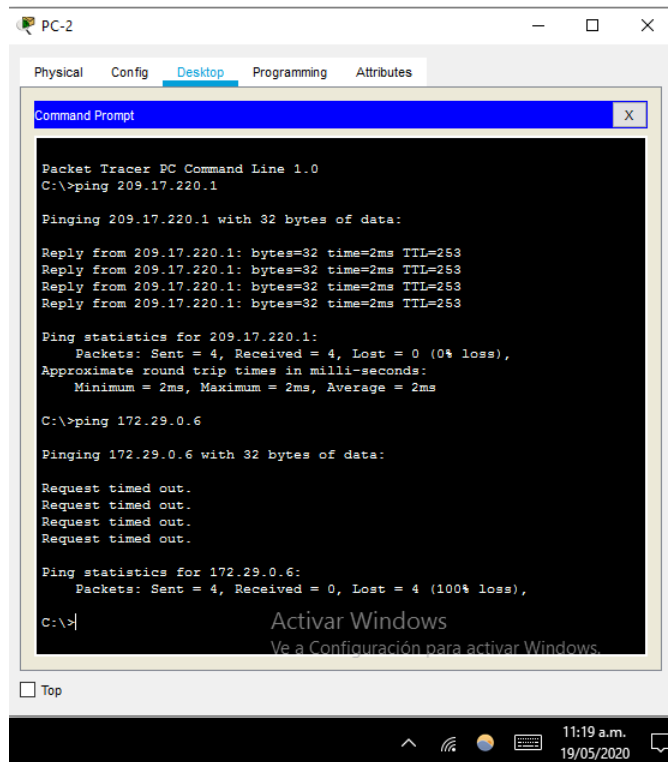
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
```

Figura 19. Ping PC2- Router ISP S0/0/0.

Mediante el comando ping verificamos que no haya conexión de PC2 a PC3 dando resultado satisfactorio ya que era lo establecido en la topología.



```
PC-2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.17.220.1

Pinging 209.17.220.1 with 32 bytes of data:

Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253
Reply from 209.17.220.1: bytes=32 time=2ms TTL=253

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ping 172.29.0.6

Pinging 172.29.0.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.29.0.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
Activar Windows
Ve a Configuración para activar Windows.
Top
11:19 a.m.
19/05/2020
```

Figura 20. Ping PC2 – PC3.

7 CONCLUSIONES

- Se dio solución práctica a los escenarios propuestos en la prueba de conocimiento, teniendo como base fundamental los conocimientos adquiridos durante el desarrollo del Diplomado de Profundización CCNA.
- Se realizó la práctica implementado el OSPF y RIPv2 como protocolos de enrutamiento, utilizando el software Packet Tracer para simular las topologías de red seleccionadas como la mejor solución a los casos.

8 BIBLIOGRAFÍA

CISCO SYSTEMS, CISCO. Asignación de direcciones IP. Fundamentos de Networking. [sitio web]. Bogotá; [Consultado; 10 de mayo 2020]. Disponible en : <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO SYSTEMS, CISCO. Capa de Transporte. Fundamentos de Networking. [sitio web]. Bogotá; [Consultado; 13 de mayo 2020]. Disponible en : <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO SYSTEMS, CISCO. Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 14 de mayo 2020]. Disponible en:
<https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO SYSTEMS, CISCO. DHCP. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 13 de mayo 2020]. Disponible en : <https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO SYSTEMS, CISCO. Exploración de la red. Fundamentos de Networking. [sitio web]. Bogotá; [Consultado: 12 de mayo 2020]. Disponible en: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO SYSTEMS, CISCO. Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 10 de mayo 2020]. Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO SYSTEMS, CISCO. Listas de control de acceso. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 13 de mayo 2020]. Disponible en : <https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO SYSTEMS, CISCO. Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 13 de mayo 2020]. Disponible en:
<https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

CISCO SYSTEMS, CISCO. VLANs. Principios de Enrutamiento y Conmutación. [sitio web]. Bogotá; [Consultado; 13 de mayo 2020]. Disponible en : <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>