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

CARLOS ALBERTO MARTINEZ MATIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2020

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

CARLOS ALBERTO MARTINEZ MATIZ

INFORME FINAL PARA OBTENER EL TITULO DE INGENIERO ELECTRONICO

HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá, 22 de mayo de 2020

DEDICATORIA

Quiero agradecer a Dios y la Santísima Virgen María por llenar mi vida con sus bendiciones y otorgarme la fortaleza necesaria para poder culminar con mi proceso formativo, cumpliendo así con las metas que me propuse desde un inicio y logrando el objetivo de convertirme en un profesional.

Dedico este trabajo con todo mi amor a mis padres, mi hermana y mi sobrina quienes, con su cariño, alegría y apoyo incondicional, fueron mi motivación en todo momento.

AGRADECIMIENTOS

Doy gracias a Dios y a la Santísima Virgen María por llenar de bendiciones y fortaleza mi vida y permitirme terminar con éxito mi proceso formativo. De igual manera, quiero agradecer muy especialmente a mis padres por sus enseñanzas y la educación que me brindaron desde mi niñez, inculcando en mí valores como la responsabilidad, la honestidad y la perseverancia lo cual fue de gran relevancia para cumplir con mis sueños profesionales.

Por último, pero no menos importante, deseo expresar mis agradecimientos a la UNAD por permitirme hacer parte de esta gran institución. Gracias a los tutores y directores de cada curso por acompañarme y guiarme durante toda la carrera brindándome siempre su apoyo incondicional y compartiéndome su conocimiento en todo momento.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

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

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

Red, Switch, Router, Protocolos de enrutamiento, listas de control de acceso, DHCP, NAT, NTP.

1. INTRODUCCION

Las redes de telecomunicaciones son de gran importancia en la vida de las personas y sin lugar a duda para las empresas, ya que permiten una comunicación más efectiva tanto al interior de las organizaciones como con los clientes, brindando mejores niveles de atención y prestación de servicios, por lo que es necesario para cualquier profesional en tecnología tener buenos conocimientos en cuanto a la configuración, administración y resolución de fallas que se puedan presentar en una red.

El siguiente trabajo está enfocado en la aplicación de los conocimientos adquiridos a lo largo del curso de Diplomado de Profundización Cisco compuesto por los módulos de CCNA1 y CCNA2 en donde, entre otros aspectos, se pondrá en práctica temáticas relacionadas con configuraciones básicas de los equipos de telecomunicaciones (Routers, Switches, PCs, Servidores de Internet), protocolos de enrutamiento, listas de control de accesos (ACL), configuraciones de DHCP, NAT, NTP, entre otros temas, haciendo uso de la herramienta Packet Tracer de Cisco la cual hace una simulación de una red real lo cual nos será de gran utilidad para la implementación, análisis y administración de redes de telecomunicaciones permitiéndonos crecer como profesionales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del Diplomado de Profundización CCNA de Cisco mediante la implementación y solución de los escenarios propuestos.

2.2 OBJETIVOS ESPECÍFICOS

- Diseñar, configurar e implementar redes mediante la herramienta Packet Tracer de Cisco.
- Configurar protocolos de enrutamiento en una red.
- Implementar DHCP y NAT para IPv4.
- Configurar y verificar listas de control de acceso ACL.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Se requiere dar solución a dos (2) escenarios propuestos, con el fin de cumplir las necesidades de telecomunicaciones de una empresa, en donde el estudiante será quien configure y administre cada red.

En primera instancia, se debe configurar una red pequeña 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.

En segundo lugar, se deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte de la red de la empresa, la cual cuenta con sucursales distribuidas en las ciudades de Bogotá y Medellín, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de topología de red.

3.2 JUSTIFICACIÓN

Las redes de telecomunicaciones son de vital importancia para las empresas y cada vez más se busca una forma de comunicación e intercambio de datos de una manera ágil y efectiva a un costo reducido.

Teniendo en cuenta esto, se hace necesario el diseño, configuración e implementación de una red que cumpla con todos los requerimientos de la empresa y que además permita una administración más confiable y centralizada utilizando equipos de última tecnología que brinden la seguridad de poder transmitir datos, incluso entre sedes o sucursales que se encuentren en diferentes ciudades, sin tener perdida de información a una velocidad o tasa de transferencia que permita mantener la calidad del servicio y dando la posibilidad de ampliar el negocio cuando la empresa así lo considere pertinente.

4. ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

4.1 ESCENARIO 1

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.

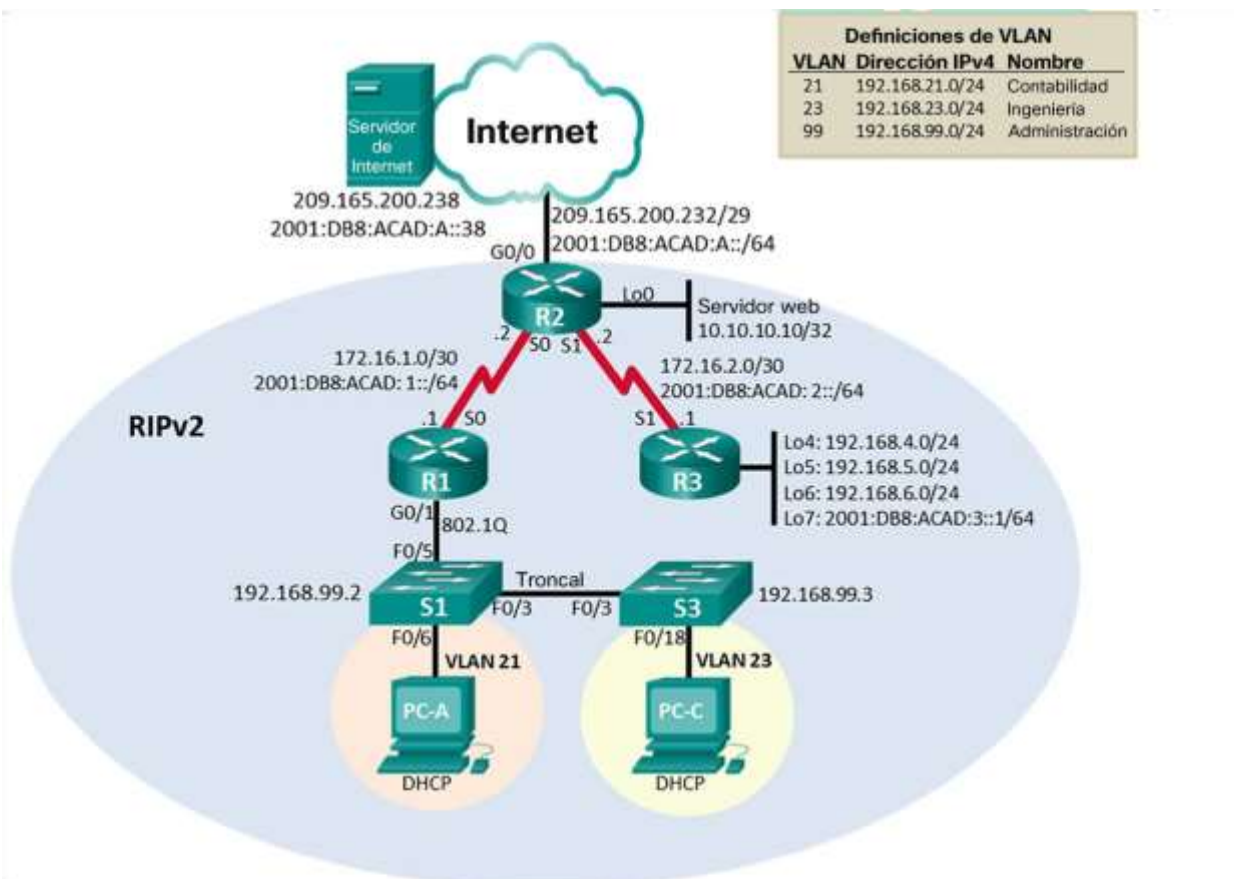


Figura 1. Topología de Red Escenario1

4.1.1 INICIALIZAR DISPOSITIVOS

4.1.1.1 Inicializar y volver a cargar los routers y los switches

Como primera medida debemos eliminar las configuraciones de los equipos a fin de garantizar que se encuentren sólo con la configuración de fábrica antes de proceder con la implementación requerida.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router> **enable** Router# **erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar todos los routers	Router# r**eload** Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch> **enable** Switch# **erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch# **delete flash:vlan.dat** Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)
Volver a cargar ambos switches	Switch# **reload** Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch> **show vlan**

Tabla 1. Inicialización Dispositivos

4.1.2 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

4.1.2.1 Configurar la computadora de Internet

En la siguiente tabla se encuentran los parámetros de configuración del Servidor 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	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:2::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2. Configuración Servidor de Internet

Ingresando a las herramientas del Servidor, procedemos a configurar el direccionamiento del dispositivo (IP's, Máscaras y Gateway):

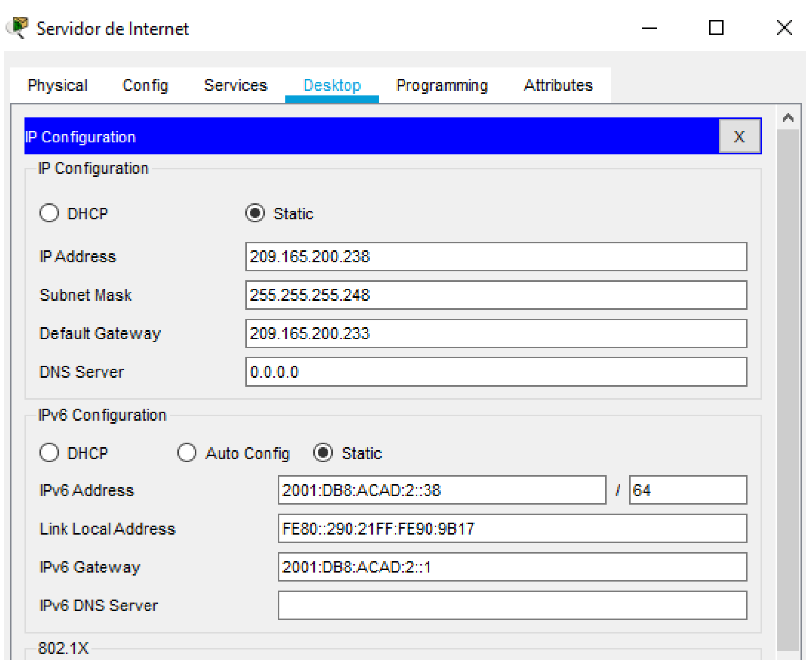


Figura 2. Configuración Servidor de Internet

4.1.2.2 Configurar R1

Realizamos la configuración básica del primer Router. Ingresamos por la Interfaz de línea de comandos (CLI) y procedemos a deshabilitar la búsqueda de un servidor de DNS y le asignamos un nombre al equipo.

Acto seguido debemos configurar las contraseñas de acceso con lo que podemos tener un mecanismo de seguridad para el ingreso y operación del dispositivo. De igual forma configuramos el direccionamiento del Router.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router# **configure terminal** 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** R1(config-line)# **exit**
Contraseña de acceso Telnet	R1(config)# **line vty 0 4** R1(config-line)# **password cisco** R1(config-line)# **login** R1(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	R1(config)# **service password-encryption**
Mensaje MOTD	R1(config)# **banner motd $Se prohibe el acceso no autorizado.$**
Interfaz S0/0/0	R1(config)# **interface s0/0/0** R1(config-if)# **description Conection to R2** R1(config-if)# **ip address 172.16.1.1 255.255.255.252** R1(config-if)# **ipv6 address 2001:DB8:ACAD:1::1/64** R1(config-if)# **clock rate 128000** R1(config-if)# **no shutdown**
Rutas predeterminadas	R1(config)# **ip route 0.0.0.0 0.0.0.0 172.16.1.2** R1(config)# **ipv6 route ::/0 2001:DB8:ACAD:1::2**

Tabla 3. Configuración Básica R1

4.1.2.3 Configurar R2

Realizamos la configuración básica del segundo Router. Ingresamos por la Interfaz de línea de comandos (CLI) y procedemos a deshabilitar la búsqueda de un servidor de DNS y le asignamos un nombre al equipo.

Acto seguido debemos configurar las contraseñas de acceso con lo que podemos tener un mecanismo de seguridad para el ingreso y operación del dispositivo. De igual forma configuramos el direccionamiento del Router.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router> **enable** Router# **configure terminal** 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** R2(config-line)# **exit**
Contraseña de acceso Telnet	R2(config)# **line vty 0 4** R2(config-line)# **password cisco** R2(config-line)# **login** R2(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	R2(config)# **service password-encryption**
Habilitar el servidor HTTP	R2(config)# **ip http sever**
Mensaje MOTD	R2(config)# **banner motd $Se prohibe el acceso no autorizado.$**

Interfaz S0/0/0	R2(config)# **interface s0/0/0** R2(config-if)# **description Conection 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)# **clock rate 128000** R2(config-if)# **no shutdown**
Interfaz S0/0/1	R2(config)# **interface s0/0/1** R2(config-if)# **description Conection 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)# **interface g0/0** R2(config-if)# **description Conection 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)# **interface loopback 0** R2(config-if)# **description Conection to Web Server** R2(config-if)# **ip address 10.10.10.10 255.255.255.255**
Ruta predeterminada	R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.238** R2(config)# **ipv6 route ::/0 2001:DB8:ACAD:A::38**

Tabla 4. Configuración R2

4.1.2.4 Configurar R3

Realizamos la configuración básica del tercer Router. Ingresamos por la Interfaz de línea de comandos (CLI) y procedemos a deshabilitar la búsqueda de un servidor de DNS y le asignamos un nombre al equipo.

Acto seguido debemos configurar las contraseñas de acceso con lo que podemos tener un mecanismo de seguridad para el ingreso y operación del dispositivo. De igual forma configuramos el direccionamiento del Router.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> **enable** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. 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** R3(config-line)# **exit**
Contraseña de acceso Telnet	R3(config)# **line vty 0 4** R3(config-line)# **password cisco** R3(config-line)# **login** R3(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	R3(config)# **service password-encryption**
Mensaje MOTD	R3(config)# **banner motd $Se prohibe el acceso no autorizado. $**
Interfaz S0/0/1	R3(config)# **interface s0/0/1** R3(config-if)# **description Conection 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)# **clock rate 128000** R3(config-if)# **no shutdown**
Interfaz loopback 4	R3(config)# **interface loopback 4** R3(config-if)# **ip address 192.168.4.1 255.255.255.0**
Interfaz loopback 5	R3(config)# **interface loopback 5** R3(config-if)# **ip address 192.168.5.1 255.255.255.0**
Interfaz loopback 6	R3(config)# **interface loopback 6** R3(config-if)# **ip address 192.168.6.1 255.255.255.0**
Interfaz loopback 7	R3(config)# **interface loopback 7** R3(config-if)# **ipv6 address 2001:DB8:ACAD:3::1/64**
Rutas predeterminadas	R3(config)# **ip route 0.0.0.0 0.0.0.0 192.168.4.0** R3(config)# **ip route 0.0.0.0 0.0.0.0 192.168.5.0** R3(config)# **ip route 0.0.0.0 0.0.0.0 192.168.6.0** R3(config)# **ipv6 route ::/0 2001:DB8:ACAD:3::0**

Tabla 5. Configuración R3

4.1.2.5 Configurar S1

Realizamos la configuración básica del primer Switch. Ingresamos por la Interfaz de línea de comandos (CLI) y procedemos a deshabilitar la búsqueda de un servidor de DNS y le asignamos un nombre al equipo.

Acto seguido debemos configurar las contraseñas de acceso con lo que podemos tener un mecanismo de seguridad para el ingreso y operación del dispositivo.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch> **enable** Switch# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(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** S1(config-line)# **exit**
Contraseña de acceso Telnet	S1(config)# **line vty 0 4** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	S1(config)# **service password-encryption**
Mensaje MOTD	S1(config)# **banner motd $Se prohibe el acceso no autorizado.$**

Tabla 6. Configuración S1

4.1.2.6 Configurar el S3

Realizamos la configuración básica del segundo Switch. Ingresamos por la Interfaz de línea de comandos (CLI) y procedemos a deshabilitar la búsqueda de un servidor de DNS y le asignamos un nombre al equipo.

Acto seguido debemos configurar las contraseñas de acceso con lo que podemos tener un mecanismo de seguridad para el ingreso y operación del dispositivo.

En la siguiente tabla se encuentran las tareas a realizar con su respectivo comando de ejecución:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch> **enable** Switch# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)# **no ip domain-lookup**
Nombre del switch	Switch(config)# **hostname S3**
Contraseña de exec privilegiado cifrada	S3(config)# **enable secret class**
Contraseña de acceso a la consola	S3(config)# **line console 0** S3(config-line)# **password cisco** 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** S3(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	S3(config)# **service password-encryption**
Mensaje MOTD	S3(config)# **banner motd $Se prohibe el acceso no autorizado.$**

Tabla 7. Configuración S3

4.1.2.7 Verificar la conectividad de la red

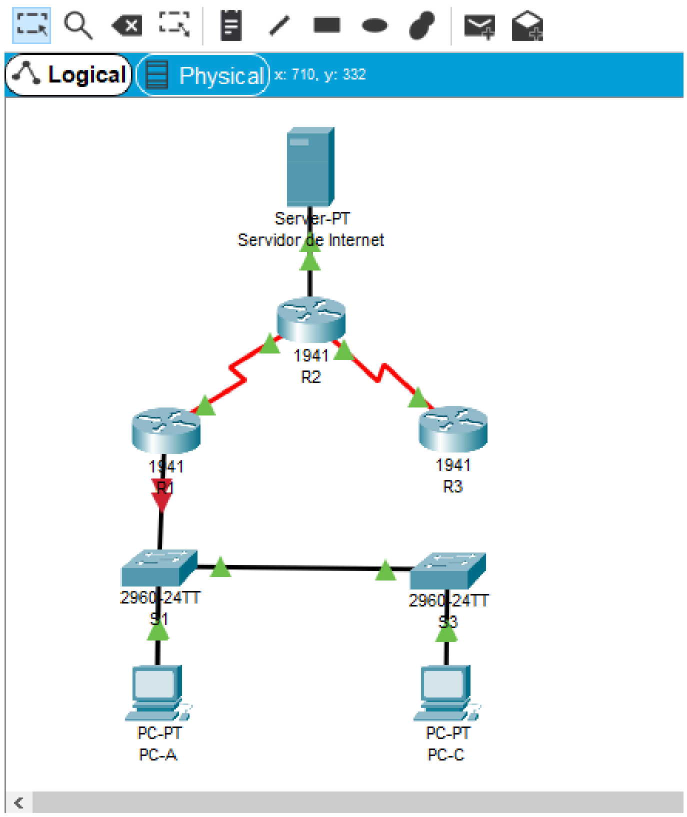
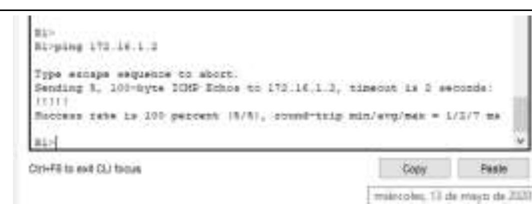


Figura 3. Red Escenario1

Una vez realizadas las configuraciones básicas de los dispositivos, procedemos a verificar la conectividad entre los equipos de la red mediante el comando ‘ping’

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 Figura 4. Conexión Exitosa R1-R2

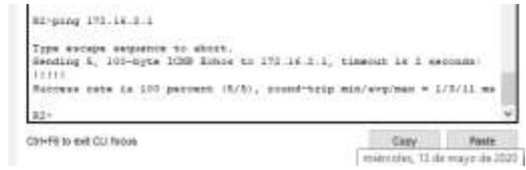
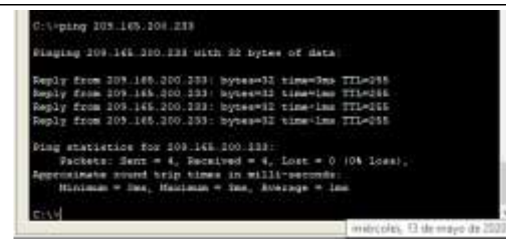
R2	R3, S0/0/1	172.16.2.1	 Figura 5. Conexión Exitosa R2-R3
PC de Internet	Gateway predeterminado	209.165.200.233	 Figura 6. Conexión PC de Internet

Tabla 8. Validación Conectividad Red

4.1.2.8 Configurar Web Server

Teniendo en cuenta que Packet tracer no soporta los comandos para configurar el servicio de HTTP en los Router, se hace necesario modificar la topología e incluir un servidor Web dentro de la red.

A continuación, se relacionan los datos para la configuración del equipo:

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	10.10.10.10
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	10.10.10.1

Tabla 9. Configuración Web Server

En la Figura 7 podemos apreciar la topología de la red con la modificación requerida:

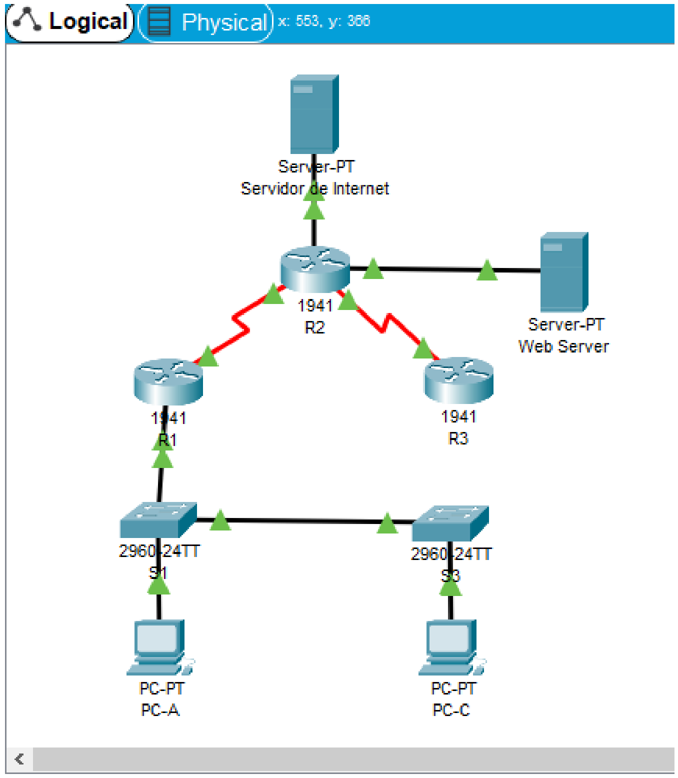


Figura 7. Red con Web Server

Una vez conectado el equipo a la red, procedemos con su configuración:

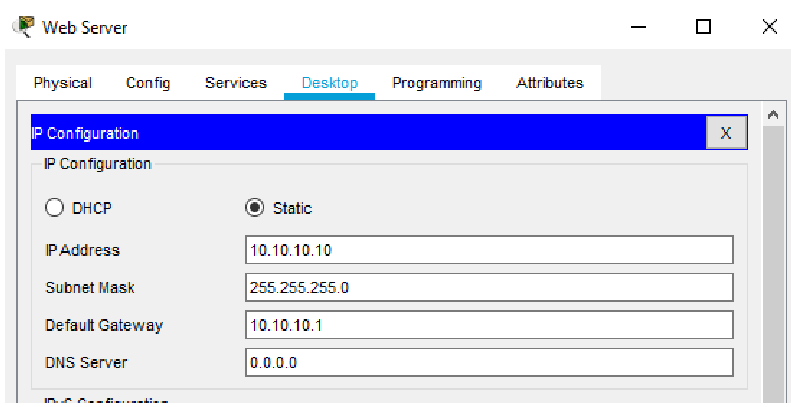


Figura 8. Configuración Web Server

Se configura la interfaz G0/1 en R2 para conexión hacia el Web Server:

R2(config)# **interface loopback 0**

R2(config-if)# **shutdown**

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down

R2(config-if)# **exit**

R2(config)# **int g0/1**

R2(config-if)# **description Conection to Web Server**

R2(config-if)# **ip address 10.10.10.1 255.255.255.0**

R2(config-if)# **exit**

Por último, desde el Web Server se procede a corroborar la conexión exitosa hacia el Gateway Predeterminado (R2) y hacia el servidor de Internet:

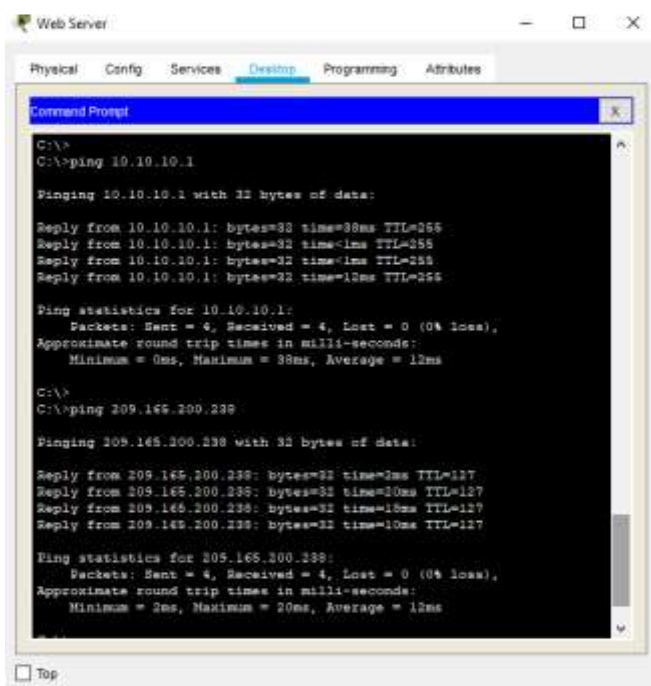


Figura 9. Conexión Exitosa Web Server

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

Debemos realizar la configurar las Vlan y el enrutamiento entre cada una de ellas. Para la red en implementación, contaremos con tres Vlan diferentes:

- Vlan 21: Contabilidad
- Vlan 23: Ingeniería
- Vlan 99: Administración

A continuación, se indicarán las tareas a realizar con el respectivo comando a ejecutar para cada Switch y Router:

4.1.3.1 Configurar S1

Las tareas de configuración para S1 incluyen las siguientes:

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)# **exit** S1(config)# **vlan 23** S1(config-vlan)# **name Ingenieria** S1(config-vlan)# **exit** S1(config)# **vlan 99** S1(config-vlan)# **name Administracion** S1(config-vlan)# **exit**
Asignar la dirección IP de administración.	S1(config)# **interface vlan 99** S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)# **ip address 192.168.99.2 255.255.255.0**
Asignar el gateway predeterminado	S1(config)# **ip default-gateway 192.168.99.1**

Forzar el enlace troncal en la interfaz F0/3	S1(config)# **interface f0/3** S1(config-if)# **switchport mode trunk** S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S1(config-if)# **switchport trunk native vlan 1** S1(config-if)# **exit**
Forzar el enlace troncal en la interfaz F0/5	S1(config)# **interface f0/5** S1(config-if)# **switchport mode trunk** S1(config-if)# **switchport trunk native vlan 1** S1(config-if)# **exit**
Configurar el resto de los puertos como puertos de acceso	S1(config)# **interface range f0/1-2, f0/4, f0/6-24, g0/1-2** S1(config-if-range)# **switchport mode access** S1(config-if-range)# **exit**
Asignar F0/6 a la VLAN 21	S1(config)# **interface f0/6** S1(config-if)# **switchport access vlan 21** S1(config-if)# **exit**
Apagar todos los puertos sin usar	S1(config)# **interface range f0/1-2, f0/4, f0/7-24, g0/1-2** S1(config-if-range)# **shutdown**

Tabla 10. Configuración Vlan S1

4.1.3.2 Configurar el S3

Las tareas de configuración para S3 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)# **vlan 21** S3(config-vlan)# **name Contabilidad** S3(config-vlan)# **exit** S3(config)# **vlan 23** S3(config-vlan)# **name Ingenieria** S3(config-vlan)# **exit** S3(config)# **vlan 99** S3(config-vlan)# **name Administracion** S3(config-vlan)# **exit**
Asignar la dirección IP de administración	S3(config)# **interface vlan 99** S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S3(config-if)# **ip address 192.168.99.3 255.255.255.0**
Asignar el gateway predeterminado.	S3(config)# **ip default-gateway 192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	S3(config)# **interface f0/3** S3(config-if)# **switchport mode trunk** S3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)# **switchport trunk native vlan 1** S3(config-if)# **exit**
Configurar el resto de los puertos como puertos de acceso	S3(config)# **interface range f0/1-2, f0/4-24, g0/1-2** S3(config-if-range)# **switchport mode access** S3(config-if-range)# **exit**
Asignar F0/18 a la VLAN 21	S3(config)# **interface f0/18** S3(config-if)# **switchport access vlan 21** S3(config-if)# **exit**
Apagar todos los puertos sin usar	S3(config)# **interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2** S3(config-if-range)# **shutdown**

Tabla 11. Configuración Vlan S2

4.1.3.3 Configurar R1

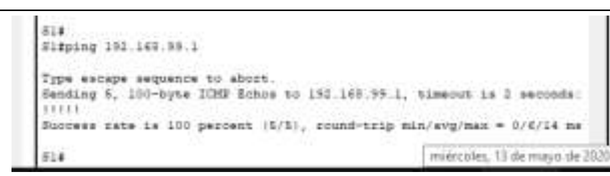
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)# **int g0/1.21** R1(config-subif)# **description LAN de Contabilidad** R1(config-subif)# **encapsulation dot1Q 21** R1(config-subif)# **ip address 192.168.21.2 255.255.255.0** R1(config-subif)# **exit**
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)# **int g0/1.23** R1(config-subif)# **description LAN de Ingenieria** R1(config-subif)# **encapsulation dot1Q 23** R1(config-subif)# **ip address 192.168.23.2 255.255.255.0** R1(config-subif)# **exit**
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)# **int g0/1.99** R1(config-subif)# **description LAN de Administracion** R1(config-subif)# **encapsulation dot1Q 99** R1(config-subif)# **ip address 192.168.99.1 255.255.255.0** R1(config-subif)# **exit**
Activar la interfaz G0/1	R1(config-if)# **no shutdown**

Tabla 12. Configuración Vlan R1

4.1.3.4 Verificar la conectividad de la red

Una vez realizadas las configuraciones básicas de los dispositivos, procedemos a verificar la conectividad entre los switches y R1 mediante el comando ‘ping’

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	 Figura 10. Conexión S1-R1 (Vlan 99)

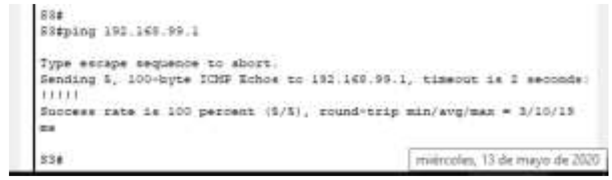
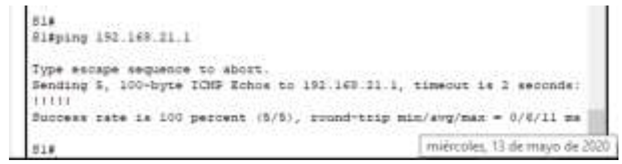
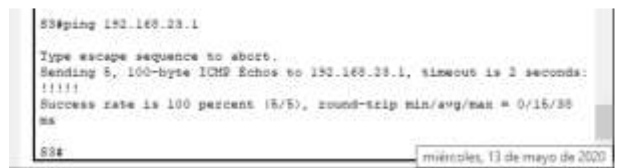
S3	R1, dirección VLAN 99	192.168.99.1	 Figura 11. Conexión S3-R1 (Vlan 99)
S1	R1, dirección VLAN 21	192.168.21.1	 Figura 12. Conexión S1-R1 (Vlan 21)
S3	R1, dirección VLAN 23	192.168.23.1	 Figura 13. Conexión S3-R1 (Vlan 23)

Tabla 13. Conectividad Red

4.1.4 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

RIP (Routing Information Protocol) es un protocolo de enrutamiento muy utilizado debido a su sencillez. Para la implementación de esta red, procederemos a configurar el enrutamiento a través de RIPv2

4.1.4.1 Configurar RIPv2 en el R1

Para la configuración de R1 en RIPv2, debemos anunciar aquellas redes que se encuentran conectadas directamente y dejar como pasivas las interfaces LAN. Por último, se desactivará la sumarización automática:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)# **router rip** R1(config-router)# **version 2**
Anunciar las redes conectadas directamente	R1(config-router)# **network 172.16.0.0** R1(config-router)# **network 192.168.0.0**
Establecer todas las interfaces LAN como pasivas	R1(config-router)# **passive-interface g0/1** 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 14. Configuración RIPv2 – R1

4.1.4.2 Configurar RIPv2 en el R2

Para la configuración de R2 en RIPv2, debemos anunciar aquellas redes que se encuentran conectadas directamente y dejar como pasivas las interfaces LAN. Por último, se desactivará la sumarización automática:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)# **router rip** R2(config-router)# **version 2**
Anunciar las redes conectadas directamente	R2(config-router)# **network 172.16.0.0** R2(config-router)# **network 10.10.0.0**
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 15. Configuración RIPv2 – R2

4.1.4.3 Configurar RIPv2 en el R3

Para la configuración de R3 en RIPv2, debemos anunciar aquellas redes que se encuentran conectadas directamente y dejar como pasivas las interfaces LAN. Por último, se desactivará la sumarización automática:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)# **router rip** R3(config-router)# **version 2**
Anunciar redes IPv4 conectadas directamente	R3(config-router)# **network 192.168.0.0** R3(config-router)# **network 172.16.0.0**
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 16. Configuración RIPv2 – R3

4.1.4.4. Verificar la información de RIP

Una vez configurado el protocolo RIPv2 es importante realizar las validaciones necesarias a fi de garantizar su correcta configuración. A continuación, se detallan y evidencian los comandos a utilizar para tal fin:

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 rip database** *** # show ip route:** Permite visualizar la información de enrutamiento total (Incluidas las rutas RIP)
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**# show run**

Tabla 17. Verificación RIP

Figura 14. Show IP Protocols - Routers

Figura 15. Show RIP Database - Routers

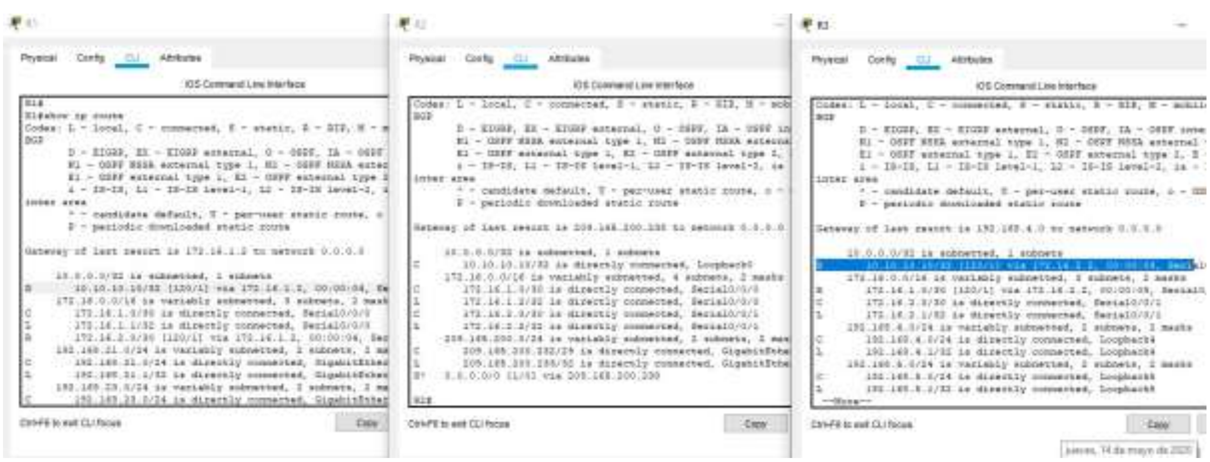


Figura 16. Show IP Route

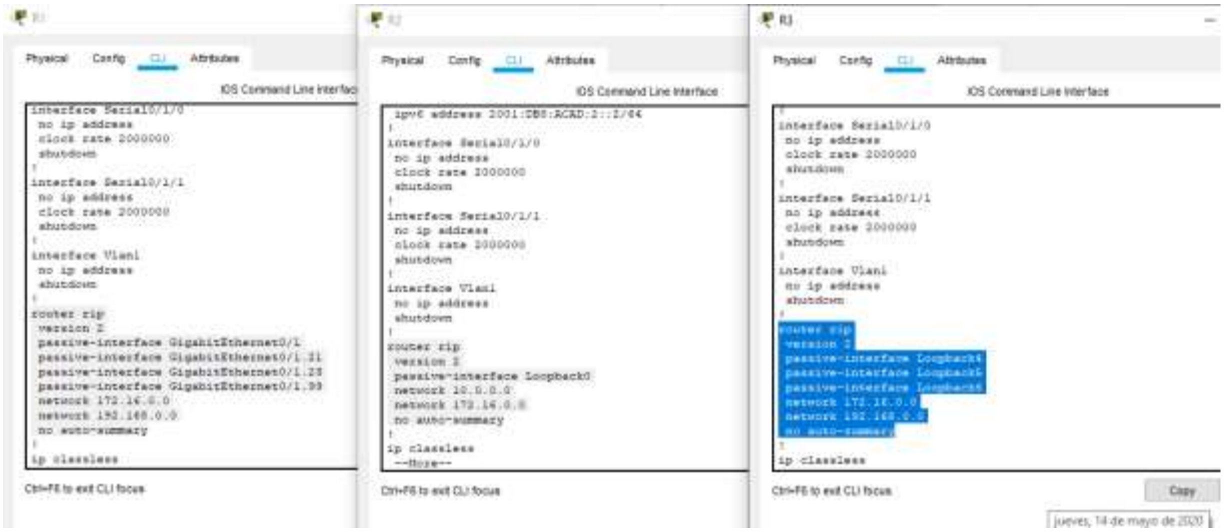


Figura 17. Show Run - Routers

4.1.5 IMPLEMENTAR DHCP Y NAT PARA IPV4

A continuación, realizaremos la configuración del protocolo DHCP para proporcionar direccionamiento de forma automática a los hosts de la red. Por otra parte, por medio de NAT traduciremos el direccionamiento público y privado dentro de nuestra red lo cual nos permitirá acceso al servidor de Internet.

4.1.5.1 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Para realizar la configuración de R1 como servidor de DHCP para las Vlan de Ingeniería y Contabilidad, por línea de comandos ejecutamos las siguientes tareas:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)# **ip dhcp excluded-address 192.168.21.1 192.168.21.20**
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)# **ip dhcp excluded-address 192.168.23.1 192.168.23.20**

Crear un pool de DHCP para la VLAN 21.	R1(config)# **ip dhcp pool ACCT** R1(dhcp-config)# **network 192.168.21.0 255.255.255.0** R1(dhcp-config)# **default-router 192.168.21.1** R1(dhcp-config)# **dns-server 10.10.10.10** R1(dhcp-config)# **domain-name ccna-sa.com** R1(dhcp-config)# **exit**
Crear un pool de DHCP para la VLAN 23	R1(config)# **ip dhcp pool ENGNR** R1(dhcp-config)# **network 192.168.23.0 255.255.255.0** R1(dhcp-config)# **default-router 192.168.23.1** R1(dhcp-config)# **dns-server 10.10.10.10** R1(dhcp-config)# **domain-name ccna-sa.com** R1(dhcp-config)# **exit**

Tabla 18. Implementación DHCP – R1

4.1.5.2 Configurar la NAT estática y dinámica en el R2

Para realizar la configuración de la NAT en R2, por la línea de comandos ejecutamos las siguientes tareas (Debido a que Packet Tracer no soporta los comandos para configurar el servicio de HTTP en los Router, en el punto 4.1.2.8, fue necesario incluir un servidor Web dentro de la red):

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)# **user 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.	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** R2(config-if)# **exit**

Configurar la NAT dinámica dentro de una ACL privada	R2(config)# **access-list 1 permit 192.168.21.0 0.0.0.255** R2(config)# **access-list 1 permit 192.168.23.0 0.0.0.255** R2(config)# **access-list 1 permit 192.168.4.0 0.0.3.255**
Defina el pool de direcciones IP públicas utilizables.	R2(config)# **ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	R2(config)# **ip nat inside source list 1 pool INTERNET**

Tabla 19. Implementación DHCP – R2

4.1.5.3 Verificar el protocolo DHCP y la NAT estática

Una vez realizadas las configuraciones de DHCP y NAT, realizamos las validaciones respectivas a fin de garantizar su corrcto funcionamiento:

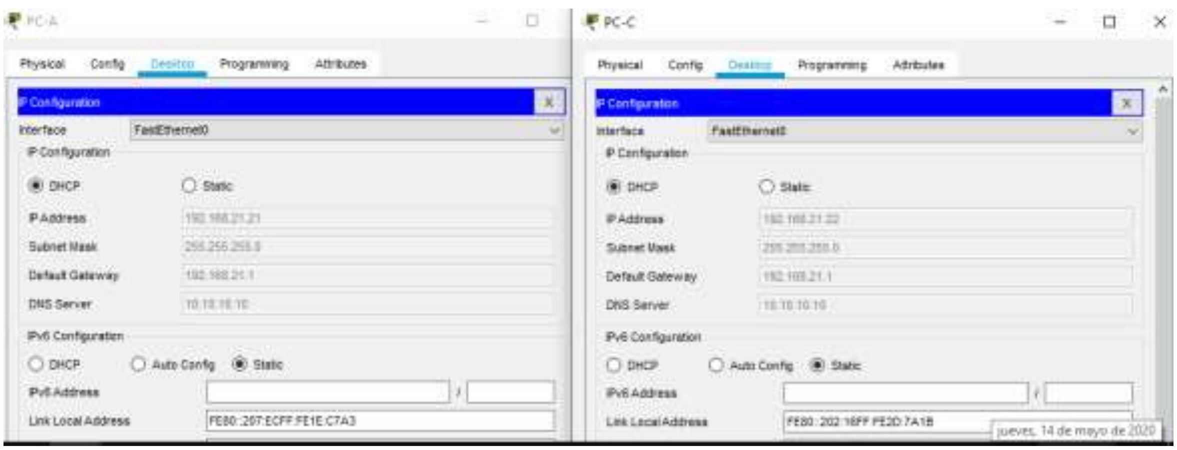
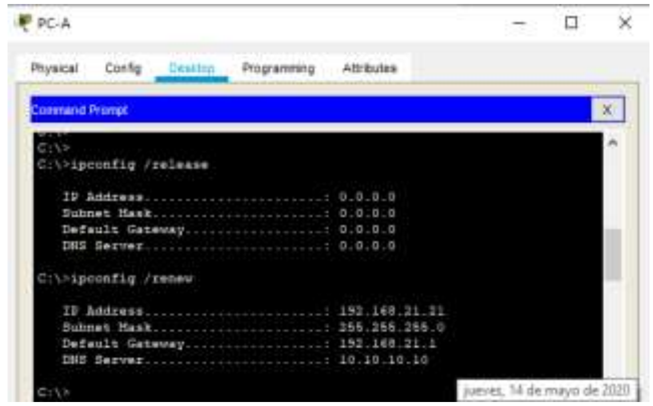
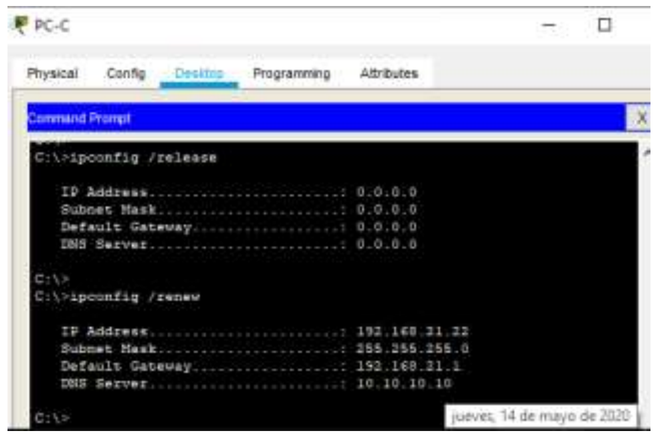
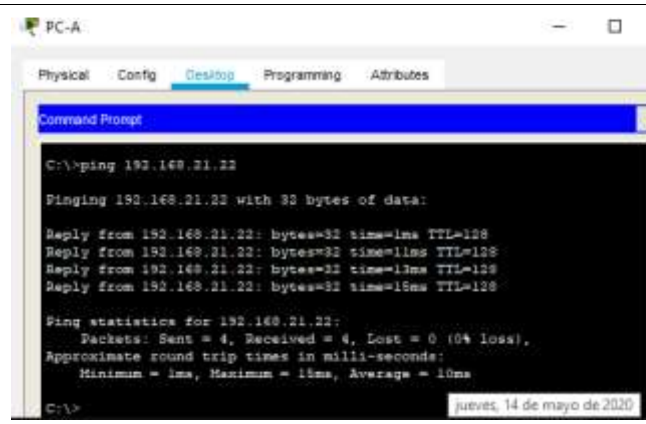


Figura 18. Configuración DHCP - PCs

En la Figura 18 podemos observar cómo los Host adquieren de manera automática el direccionamiento del servidor DHCP.

De igual forma, en la Tabla 20 podemos corroborar la conectividad entre los PCs y el acceso al servidor web:

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Figura 19. Configuración DHCP - PCA
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 20. Configuración DHCP – PCC
Verificar que la PC-A pueda hacer ping a la PC-C	 Figura 21. Ping Exitoso PCA - PCC

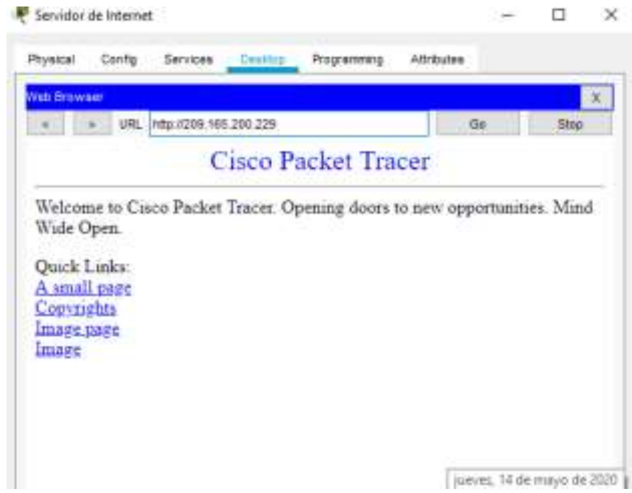
<table>
<tr>
<td>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)
Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</td>
<td>

Figura 22. Acceso Exitoso al Web Server</td>
</tr>
</table>

Tabla 20. Verificación DHCP y NAT

4.1.6 CONFIGURAR NTP

A continuación, configuramos fecha y hora en los Router definiendo el maestro y el cliente entre os equipos:

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2# **clock set 09:00:00 Mar 5 2016** R2# **show clock** 9:0:2.623 UTC Sat Mar 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.	R1# **show ntp associations** address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 13 16 377 1.00 6.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Tabla 21. Configuración NTP

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

4.1.7.1 Restringir el acceso a las líneas VTY en el R2

Por último, restringimos el acceso por Telnet a R2 (Solamente R1 podrá establecer conexión por telnet con 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(config)# **ip access-list standard ADMIN-MGT** R2(config-std-nacl)# **permit host 172.16.1.1** R2(config-std-nacl)# **exit**
Aplicar la ACL con nombre a las líneas VTY	R2(config)# **line vty 0 4**
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)# **access-class ADMIN-MGT in**
Verificar que la ACL funcione como se espera	R2# **show access-lists** 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

Tabla 22. Configuración VTY – R2

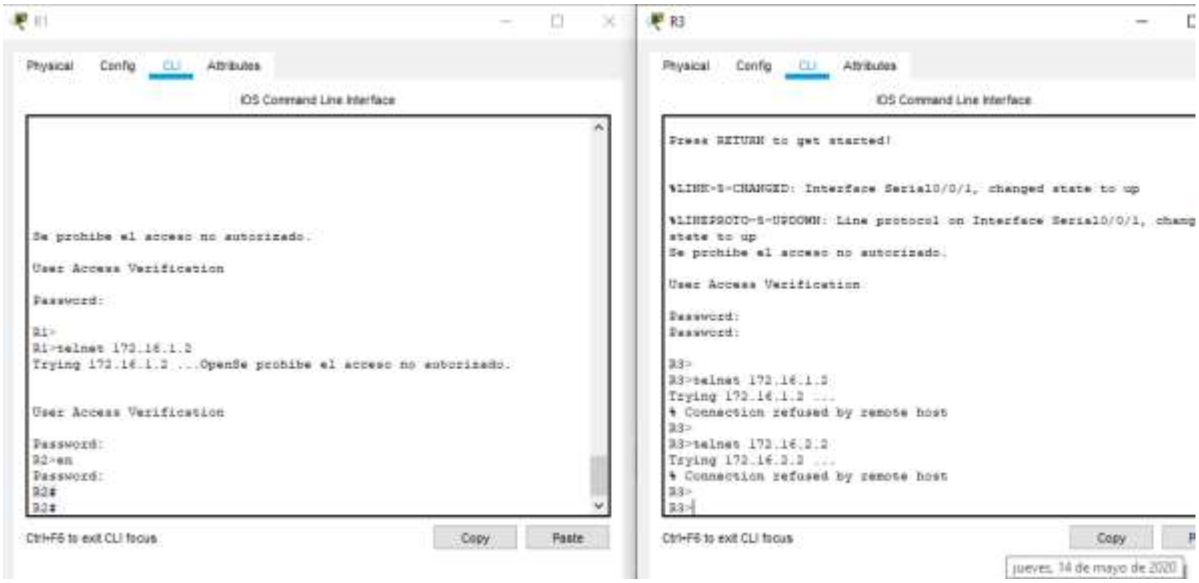


Figura 23. Validación Acceso por Telnet

4.1.7.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Los siguientes comando se usan para configurar o eliminar traducciones NAT y listas de acceso:

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	**#show access-list**
Restablecer los contadores de una lista de acceso	**#clear ip access-list counters**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	**#show ip interface**
¿Con qué comando se muestran las traducciones NAT?	**#show ip nat translations**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**#clear ip nat translation**

Tabla 23. Comandos Validación

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.

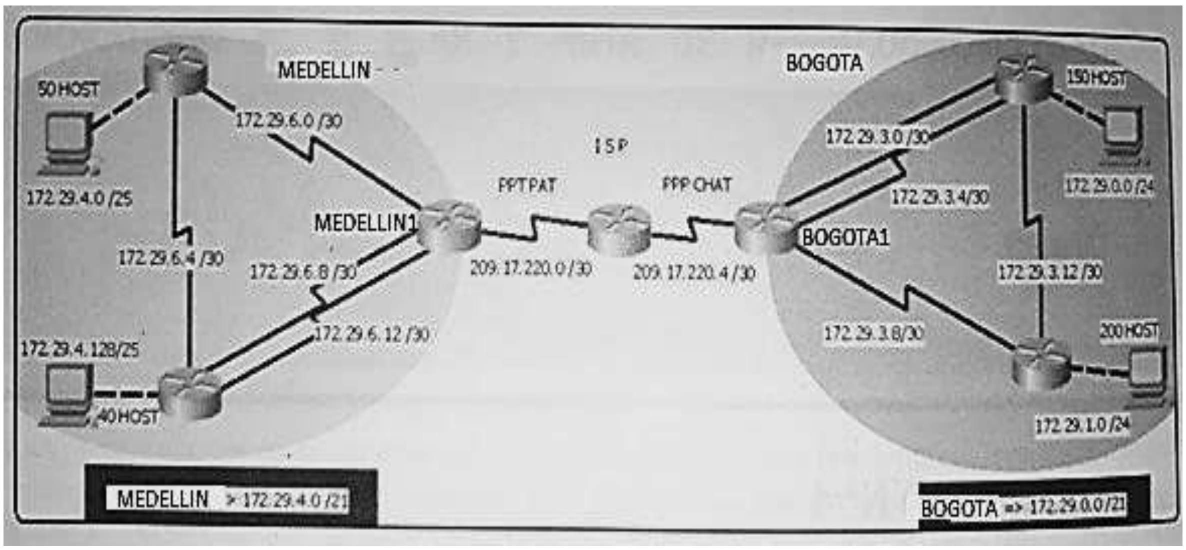


Figura 24. Topología de Red Escenario2

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.

4.2.1 DESARROLLO

En la siguiente tabla se muestran las tareas y comando a ejecutar para realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (Se asignan nombres de equipos, claves de seguridad, etc).

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router> **enable** Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)# **no ip domain-lookup**
Nombre del router	Router(config)# **hostname Medellin1**
Contraseña de exec privilegiado cifrada	Medellin1(config)# **enable secret class**
Contraseña de acceso a la consola	Medellin1(config)# **line console 0** Medellin1(config-line)# **password cisco** Medellin1(config-line)# **login** Medellin1(config-line)# **exit**
Contraseña de acceso Telnet	Medellin1(config)# **line vty 0 4** Medellin1(config-line)# **password cisco** Medellin1(config-line)# **login** Medellin1(config-line)# **exit**
Cifrar las contraseñas de texto no cifrado	Medellin1(config)# **service password-encryption**
Mensaje MOTD	Medellin1(config)# **banner motd %Se prohibe el acceso no autorizado.%**

Tabla 24. Configuración Inicial Router

Esta configuración se ejecuta en cada uno de los Router que conforman la Red.

Procedemos a realizar la conexión física de los equipos con base en la topología de red:

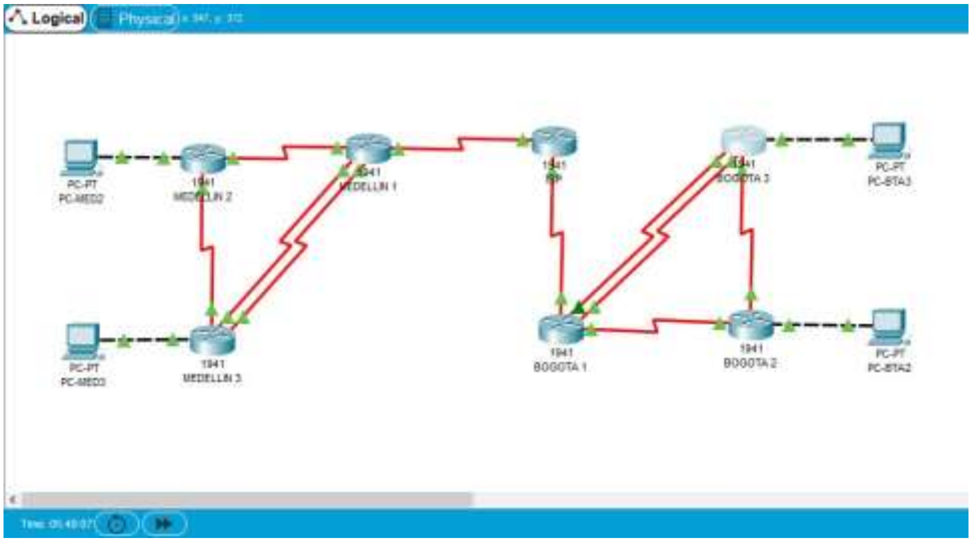


Figura 25. Red Escenario2

4.2.2 CONFIGURACIÓN DEL ENRUTAMIENTO

OSPF (Open Shortest Path First) es un protocolo de enrutamiento que utiliza un algoritmo para calcular y enrutar el tráfico de red por el camino más corto lo cual brinda mayor velocidad y eficiencia.

La configuración de nuestra red por medio de OSPF, se realizará ejecutando los comandos que se relacionan a continuación:

Comandos configuración Router ISP:

```
ISP#configure terminal
ISP(config)#interface s0/0/1
ISP(config-if)#description ISP-MEDELLIN1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#exit
```

ISP(config-if)#interface s0/1/1
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#exit

Comandos configuración Router Medellin1:

```
Medellin1#config t
Medellin1(config)#interface s0/1/1
Medellin1(config-if)#description MEDELLIN1-ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface s0/0/1
Medellin1(config-if)#description MEDELLIN1-MEDELLIN3
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config)#interface s0/1/0
Medellin1(config-if)#description MEDELLIN1-2_MEDELLIN3
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface s0/0/0
Medellin1(config-if)#description MEDELLIN1-MEDELLIN2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown

Medellin1(config)#do show ip route connected
    C 172.29.6.0/30 is directly connected, Serial0/0/0
    C 172.29.6.8/30 is directly connected, Serial0/1/0
    C 172.29.6.12/30 is directly connected, Serial0/0/1

Medellin1(config)#router ospf 1
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.128 0.0.0.3 area 0
Medellin1(config-router)#exit
```

Comandos configuración Router Medellin2:

```
Medellin2#config t
Medellin2(config)#interface s0/0/0
Medellin2(config-if)#description MEDELLIN2-MEDELLIN1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface s0/0/1
Medellin2(config-if)# description MEDELLIN2-MEDELLIN
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface g0/0
Medellin2(config-if)#description MEDELLIN2-PC2
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit

Medellin2(config)#do show ip route connected
     C   172.29.4.0/25  is directly connected, GigabitEthernet0/0
     C   172.29.6.0/30  is directly connected, Serial0/0/0
     C   172.29.6.4/30  is directly connected, Serial0/0/1

Medellin2(config)#router ospf 1
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#exit
```

Comandos configuración Router Medellin3:

```
Medellin3#conf t
Medellin3(config)#interface s0/0/1
Medellin3(config-if)#description MEDELLIN3-MEDELLIN1
Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface s0/1/0
Medellin3(config-if)#description 2_MEDELLIN3-MEDELLIN1
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
```

```
Medellin3(config-if)#exit
Medellin3(config)#interface s0/0/0
Medellin3(config-if)#description MEDELLIN3-MEDELLIN2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#clock rate 128000
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit
Medellin3(config)#interface g0/0
Medellin3(config-if)#description MEDELLIN3-PC3
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
Medellin3(config-if)#exit

Medellin3(config)#do show ip route connected
        C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
        C 172.29.6.4/30 is directly connected, Serial0/0/0
        C  172.29.6.8/30  is directly connected, Serial0/1/0
        C 172.29.6.12/30 is directly connected, Serial0/0/1

Medellin3(config)#router ospf 1
Medellin3(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin3(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin3(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin3(config-router)#exit
```

Comandos configuración Router Bogota1:

```
Bogota1#config t
Bogota1(config)#interface s0/1/1
Bogota1(config-if)#description BOGOTA1-ISP
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#description BOGOTA1-BOGOTA2
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#no shutdown
Bogota1(config)#interface s0/0/1
Bogota1(config-if)#description BOGOTA1-BOGOTA3
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface s0/1/0
```

```
Bogota1(config-if)#description BOGOTA1-2_BOGOTA3
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown

Bogota1(config)#do show ip route connected
    C   172.29.3.0/30  is directly connected, Serial0/0/1
    C   172.29.3.4/30  is directly connected, Serial0/1/0
    C   172.29.3.8/30  is directly connected, Serial0/0/0

Bogota1(config)#router ospf 1
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#exit
```

Comandos configuración Router Bogota2:

```
Bogota2#conf t
Bogota2(config)#interface s0/0/0
Bogota2(config-if)#description BOGOTA2-BOGOTA1
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface s0/0/1
Bogota2(config-if)#description BOGOTA2-BOGOTA3
Bogota2(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface g0/0
Bogota2(config-if)#description BOGOTA2-PCBTA2
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shutdown

Bogota2(config)#do show ip route connected
    C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
    C 172.29.3.8/30 is directly connected, Serial0/0/0
    C 172.29.3.12/30 is directly connected, Serial0/0/1

Bogota2(config)#router ospf 1
Bogota2(config-router)#network 172.29.1.0 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#exit
```

Comandos configuración Router Bogota3:

```
Bogota3#config t
Bogota3(config)#interface s0/0/1
Bogota3(config-if)#description BOGOTA3-BOGOTA1
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#interface s0/1/0
Bogota3(config-if)#description 2_BOGOTA3_BOGOTA1
Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#interface s0/0/0
Bogota3(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota3(config-if)#clock rate 128000
Bogota3(config-if)#description BOGOTA3-BOGOTA2
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit
Bogota3(config)#int g0/0
Bogota3(config-if)#description BOGOTA3-PCBTA3
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota3(config-if)#no shutdown
Bogota3(config-if)#exit

Bogota3(config)#do show ip route connected
    C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
    C 172.29.3.0/30 is directly connected, Serial0/0/1
    C  172.29.3.4/30  is directly connected, Serial0/1/0
    C 172.29.3.12/30 is directly connected, Serial0/0/0

Bogota3(config)#router ospf 1
Bogota3(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota3(config-router)#exit
```

Una vez tenemos configurado el direccionamiento y el protocolo OSPF en los equipos, debemos añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Comandos configuración Router Medellin1:

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
Medellin1(config)#router ospf 1
Medellin1(config-router)#default-information originate
Medellin1(config-router)#exit
```

Comandos configuración Router Bogota1:

```
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
Bogota1(config)#router ospf 1
Bogota1(config-router)#default-information originate
Bogota1(config-router)#exit
```

Acto seguido, en el router ISP adicionaremos una ruta estática dirigida hacia cada red interna de Bogotá y Medellín (Para el caso se sumarizan las subredes de cada uno a /22)

Comandos configuración Router ISP:

```
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
```

4.2.3 TABLA DE ENRUTAMIENTO.

Mediante el comando show ip route, verificamos la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas. De igual forma, podemos validar, entre otros aspectos:

- Verificamos el balanceo de carga que presentan los routers.

- Podemos observar 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.

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

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

- El router ISP solo indica sus rutas estáticas adicionales a las directamente conectadas.

```
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

     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 is directly connected, Serial0/1/1
                      [1/0] via 209.17.220.0
S       172.29.4.0/22 is directly connected, Serial0/0/1
                      [1/0] via 209.17.220.0
     209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/0/1
L       209.17.220.1/32 is directly connected, Serial0/0/1
C       209.17.220.2/32 is directly connected, Serial0/0/1
C       209.17.220.4/30 is directly connected, Serial0/1/1
L       209.17.220.5/32 is directly connected, Serial0/1/1
C       209.17.220.6/32 is directly connected, Serial0/1/1
```

Figura 26. Show IP Route – ISP

```
Medellin1#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, 00:25:49, Serial0/0/0
O       172.29.4.128/25 [110/65] via 172.29.6.10, 00:22:35, Serial0/1/0
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.1/32 is directly connected, Serial0/0/0
O       172.29.6.4/30 [110/128] via 172.29.6.2, 00:22:35, Serial0/0/0
                      [110/128] via 172.29.6.10, 00:22:35, 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, Serial0/0/1
L       172.29.6.13/32 is directly connected, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/1
C       209.17.220.1/32 is directly connected, Serial0/1/1
L       209.17.220.2/32 is directly connected, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 209.17.220.1
```

Figura 27. Show IP Route – Medellin1

```
Medellin2#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 172.29.6.1 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, 00:23:02,
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, 00:22:51, Serial0/0/0
                      [110/128] via 172.29.6.6, 00:22:51, Serial0/0/1
O       172.29.6.12/30 [110/128] via 172.29.6.6, 00:22:41,
Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:26:05, Serial0/0/0
```

Figura 28. Show IP Route – Medellin2

```
Medellin3#
Medellin3#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 172.29.6.9 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, 00:23:13, Serial0/0/0
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, 00:23:02, Serial0/0/0
                      [110/128] via 172.29.6.9, 00:23:02, Serial0/1/0
C       172.29.6.4/30 is directly connected, Serial0/0/0
L       172.29.6.6/32 is directly connected, Serial0/0/0
C       172.29.6.8/30 is directly connected, Serial0/1/0
L       172.29.6.10/32 is directly connected, Serial0/1/0
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, 00:23:02, Serial0/1/0
```

Figura 29. Show IP Route – Medellin3

```
Bogota1#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 209.17.220.5 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, 00:00:25, Serial0/0/1
O       172.29.1.0/24 [110/65] via 172.29.3.10, 00:00:25, Serial0/0/0
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.1/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.5/32 is directly connected, Serial0/1/0
C       172.29.3.8/30 is directly connected, Serial0/0/0
L       172.29.3.9/32 is directly connected, Serial0/0/0
O       172.29.3.12/30 [110/128] via 172.29.3.10, 00:00:25, Serial0/0/0
                       [110/128] via 172.29.3.2, 00:00:25, Serial0/0/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/1/1
C       209.17.220.5/32 is directly connected, Serial0/1/1
L       209.17.220.6/32 is directly connected, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 209.17.220.5
```

Figura 30. Show IP Route – Bogota1

```
Bogota2#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 172.29.3.9 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 172.29.3.13, 00:01:44, 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 172.29.3.13, 00:01:44, Serial0/0/1
                      [110/128] via 172.29.3.9, 00:01:44, Serial0/0/0
O       172.29.3.4/30 [110/128] via 172.29.3.13, 00:01:44, Serial0/0/1
                      [110/128] via 172.29.3.9, 00:01:44, Serial0/0/0
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       172.29.3.14/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:01:44, Serial0/0/0
```

Figura 31. Show IP Route – Bogota2

```
Bogota3#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 172.29.3.5 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 172.29.3.14, 00:02:24, Serial0/0/0
C       172.29.3.0/30 is directly connected, Serial0/0/1
L       172.29.3.2/32 is directly connected, Serial0/0/1
C       172.29.3.4/30 is directly connected, Serial0/1/0
L       172.29.3.6/32 is directly connected, Serial0/1/0
O       172.29.3.8/30 [110/128] via 172.29.3.5, 00:02:24, Serial0/1/0
                      [110/128] via 172.29.3.14, 00:02:24, Serial0/0/0
C       172.29.3.12/30 is directly connected, Serial0/0/0
L       172.29.3.13/32 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.5, 00:02:24, Serial0/1/0
```

Figura 32. Show IP Route – Bogota3

4.2.4 DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

Para no propagar las publicaciones por interfaces que no lo requieran, debemos deshabilitar la propagación del protocolo OSPF mediante el comando passive-interface.

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

Router Medellin3:

```
Medellin3(config)#router ospf 1
Medellin3(config-router)#passive-interface g0/0
Medellin3(config-router)#passive-interface g0/1
Medellin3(config-router)#passive-interface s0/1/1
```

Router Medellin2:

```
Medellin2(config)#router ospf 1
Medellin2(config-router)#passive-interface s0/1/1
Medellin2(config-router)#passive-interface s0/1/0
Medellin2(config-router)#passive-interface g0/0
Medellin2(config-router)#passive-interface g0/1
```

Router Medellin1:

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#passive-interface g0/0
Medellin1(config-router)#passive-interface g0/1
```

Router Bogota1:

```
Bogota1(config)#router ospf 1
Bogota1(config-router)#passive-interface g0/0
Bogota1(config-router)#passive-interface g0/1
```

Router Bogota2:

```
Bogota2(config)#router ospf 1
Bogota2(config-router)#passive-interface g0/0
Bogota2(config-router)#passive-interface g0/1
Bogota2(config-router)#passive-interface s0/1/0
Bogota2(config-router)#passive-interface s0/1/1
```

Router Bogota3:

```
Bogota3(config)#router ospf 1
Bogota3(config-router)#passive-interface g0/0
Bogota3(config-router)#passive-interface g0/1
Bogota3(config-router)#passive-interface s0/1/1
```

4.2.5 VERIFICACIÓN DEL PROTOCOLO OSPF.

Para verificar 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, desde la interfaz de línea de comando ejecutamos: #show ip protocols

```
ISP#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 209.17.220.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    209.17.220.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.17.220.5         110      00:14:15
  Distance: (default is 110)
```

Figura 33. Show IP Protocols - ISP

```
Medellin1#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:
    172.29.0.0 0.0.0.3 area 0
    172.29.6.0 0.0.0.3 area 0
    172.29.6.8 0.0.0.3 area 0
    172.29.6.128 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5           110      00:26:22
    172.29.6.14          110      00:26:17
    209.17.220.2         110      00:26:22
  Distance: (default is 110)

Medellin1#
```

Figura 34. Show IP Protocols – Medellin1

```
Medellin2#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 172.29.6.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.3 area 0
    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
    GigabitEthernet0/1
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5           110      00:27:10
    172.29.6.14          110      00:27:05
    209.17.220.2         110      00:27:10
  Distance: (default is 110)
```

Figura 35. Show IP Protocols – Medellin2

```
Medellin3#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 172.29.6.14
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.3 area 0
    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
    GigabitEthernet0/1
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.6.5           110      00:27:55
    172.29.6.14          110      00:27:55
    209.17.220.2         110      00:27:55
  Distance: (default is 110)
```

Figura 36. Show IP Protocols – Medellin3

```
Bogota1#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 209.17.220.6
  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:
    172.29.0.0 0.0.0.3 area 0
    172.29.3.0 0.0.0.3 area 0
    172.29.3.4 0.0.0.3 area 0
    172.29.3.8 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:28:44
    172.29.3.14          110      00:28:44
    209.17.220.6         110      00:28:44
  Distance: (default is 110)
```

Figura 37. Show IP Protocols – Bogota1

```
Bogota2#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 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 0.0.0.3 area 0
    172.29.1.0 0.0.0.3 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
    GigabitEthernet0/1
    Serial0/1/0
    Serial0/1/1
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13           110      00:29:37
    172.29.3.14           110      00:00:05
    209.17.220.6          110      00:00:05
  Distance: (default is 110)
```

Figura 38. Show IP Protocols – Bogota2

```
Bogota3>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 172.29.3.13
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.0.0 0.0.0.3 area 0
    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
    GigabitEthernet0/1
    Serial0/1/1
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13           110      00:00:25
    172.29.3.14           110      00:00:52
    209.17.220.6          110      00:00:52
  Distance: (default is 110)
```

Figura 39. Show IP Protocols – Bogota3

Para 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 utilizamos el comando #show iproute el cual se verificó en la Parte 2: Tabla de Enrutamiento

4.2.6 CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

Según la topología de red se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT, para lo cual desde la interfaz de línea de comandos de cada Router ejecutamos lo siguiente:

```
ISP#conf t
ISP(config)#username Medellin1 password cisco
ISP(config)#int s0/0/1
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

Medellin1#conf t
Medellin1(config)#username ISP password cisco
Medellin1(config)#int s0/1/1
Medellin1(config-if)#encapsulation PPP
Medellin1(config-if)#ppp authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 password cisco
Medellin1(config-if)#exit
```

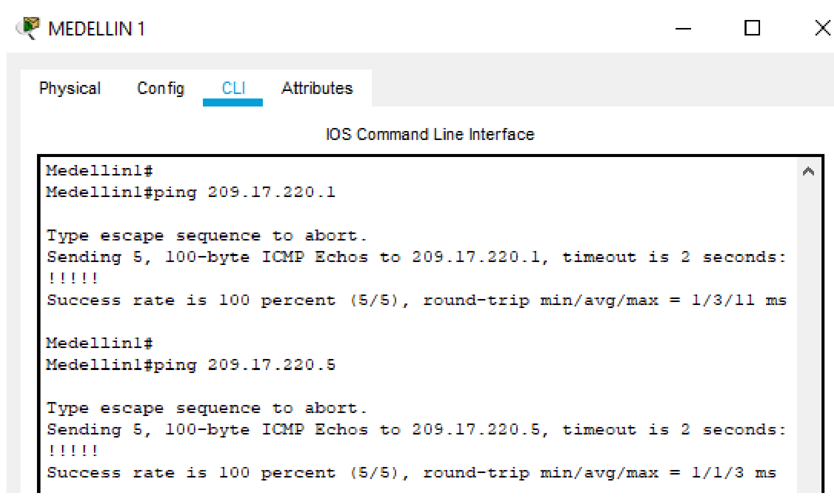


Figura 40. Conexión Exitosa Medellin1 - ISP

Para enlace Bogotá1 con ISP se debe configurar con autenticación CHAT, para lo cual desde la interfaz de línea de comandos de cada Router ejecutamos lo siguiente:

ISP#config t
ISP(config)#username Bogota1 password cisco
ISP(config)#inter s0/1/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit

Bogota1#conf t
Bogota1(config)#username ISP password cisco
Bogota1(config)#int s0/1/1
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#exit

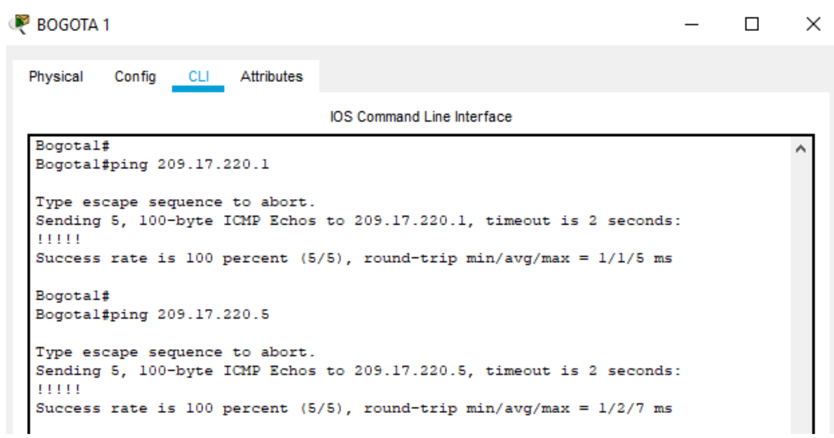


Figura 41. Conexión Exitosa Bogota1 - ISP

Por medio de las figuras 40 y 41 podemos confirmar la conexión exitosa desde los Router Bogotá 1 y Medellin1 hacia el ISP.

4.2.7 CONFIGURACIÓN DE PAT.

De acuerdo con 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.

Para configurar el NAT en el router Medellín1, realizamos lo siguiente:

```
Medellin1#conf t
Medellin1(config)#ip nat inside source list 1 interface s0/1/1 overload
Medellin1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
Medellin1(config)#int s0/1/1
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#int s0/0/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/0/1
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#ip nat inside
Medellin1(config-if)#exit
Medellin1(config)#exit
```

Para comprobar que la configuración de NAT fue exitosa y la traducción de direcciones indique las interfaces de entrada y de salida, realizamos un ping desde cada uno de los Host y la dirección es traducida automáticamente a la dirección de la interfaz serial 0/1/1 del router Medellín1.

En las figuras 42 y 43 se evidencia la conexión exitosa y la traducción de las direcciones al ejecutar el comando <u>show ip nat translations.</u>

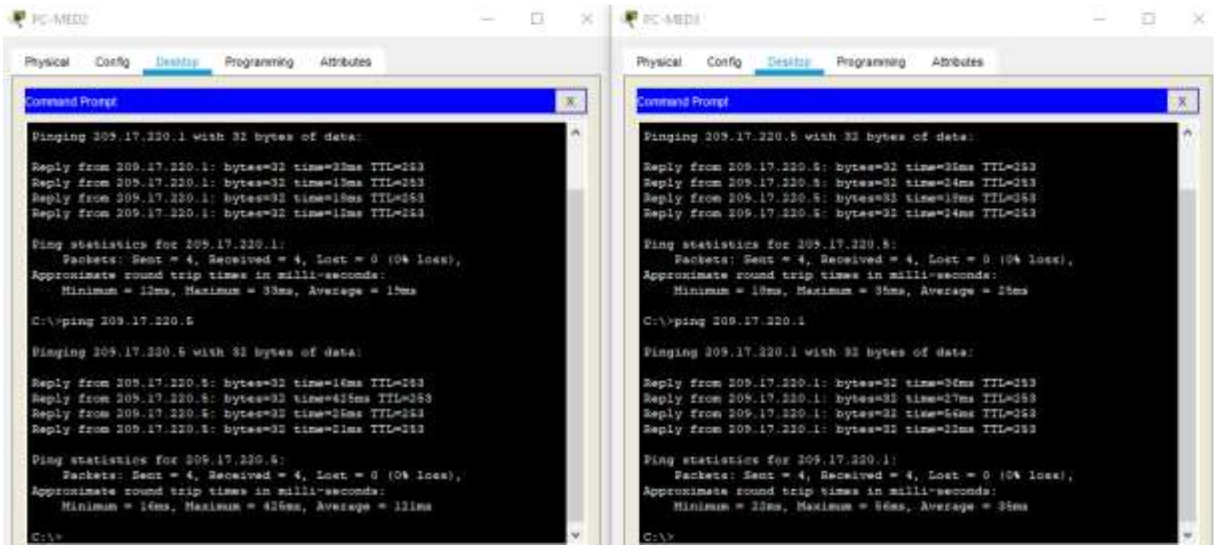


Figura 42. Conexión Exitosa PCs Medellín - ISP

```
Medellin1#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
icmp 209.17.220.2:1     172.29.4.6:1       209.17.200.1:1     209.17.200.1:1
icmp 209.17.220.2:2     172.29.4.6:2       209.17.200.1:2     209.17.200.1:2
icmp 209.17.220.2:3     172.29.4.6:3       209.17.200.1:3     209.17.200.1:3
icmp 209.17.220.2:4     172.29.4.6:4       209.17.200.1:4     209.17.200.1:4
icmp 209.17.220.2:5     172.29.4.6:5       209.17.200.2:5     209.17.200.2:5
icmp 209.17.220.2:6     172.29.4.6:6       209.17.200.2:6     209.17.200.2:6
icmp 209.17.220.2:7     172.29.4.6:7       209.17.200.2:7     209.17.200.2:7
icmp 209.17.220.2:8     172.29.4.6:8       209.17.200.2:8     209.17.200.2:8
```

Figura 43. Traducción Medellin1

Procedemos a configurar el NAT en el router Bogotá1:

Bogota1#conf t
Bogota1(config)#ip nat inside source list 1 interface s0/1/1 overload
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
Bogota1(config)#int s0/1/1
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int s0/0/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#exit
Bogota1(config)#exit

Para comprobar que la configuración de NAT fue exitosa y la traducción de direcciones indique las interfaces de entrada y de salida, realizamos un ping desde cada uno de los Host y la dirección es traducida automáticamente a la dirección de la interfaz serial 0/1/1 del router Medellín1.

En las figuras 44 y 45 se evidencia la conexión exitosa y la traducción de las direcciones al ejecutar el comando <u>show ip nat translations.</u>

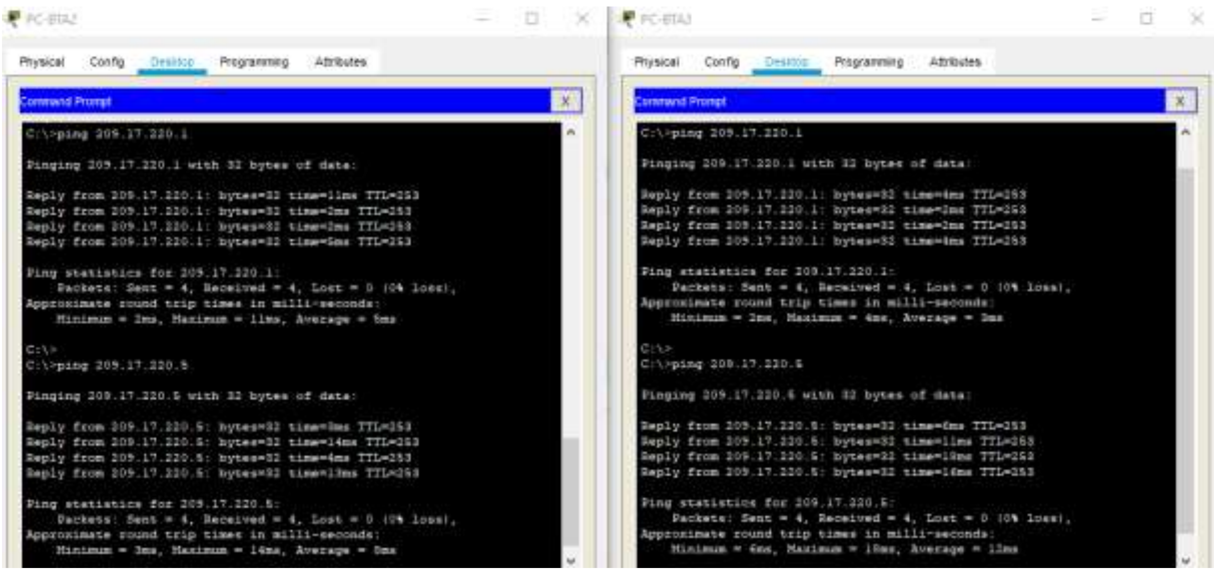


Figura 44. Conexión Exitosa PCs Bogotá - ISP

```
Bogota1#
Bogota1#show ip nat translations
Pro  Inside global     Inside local      Outside local     Outside global
icmp 209.17.220.6:13   172.29.1.6:13     172.19.220.6:13   172.19.220.6:13
icmp 209.17.220.6:14   172.29.1.6:14     172.19.220.6:14   172.19.220.6:14
icmp 209.17.220.6:15   172.29.1.6:15     172.19.220.6:15   172.19.220.6:15
icmp 209.17.220.6:16   172.29.1.6:16     172.19.220.6:16   172.19.220.6:16

Bogota1#show ip nat translations
Pro  Inside global     Inside local      Outside local     Outside global
icmp 209.17.220.6:17   172.29.1.6:17     209.17.220.5:17   209.17.220.5:17
icmp 209.17.220.6:18   172.29.1.6:18     209.17.220.5:18   209.17.220.5:18
icmp 209.17.220.6:19   172.29.1.6:19     209.17.220.5:19   209.17.220.5:19
icmp 209.17.220.6:20   172.29.1.6:20     209.17.220.5:20   209.17.220.5:20
```

Figura 45. Traducción Bogota1

4.2.8 CONFIGURACIÓN DEL SERVICIO DHCP.

Como paso final, configuramos la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN:

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
Medellin2(config)#ip dhcp pool MEDELLIN2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.1
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
Medellin2(config)#ip dhcp pool MEDELLIN3
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
Medellin2(dhcp-config)#default-route 172.29.4.129
Medellin2(dhcp-config)#dns-server 8.8.8.8
Medellin2(dhcp-config)#exit
```

En el router Medellín3 habilitamos el paso de los mensajes broadcast hacia la IP del router Medellín2.

```
Medellin3#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#int g0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#exit
```

Configuramos la red Bogotá2 y Bogotá3 donde el router Bogotá2 debe ser el servidor DHCP para ambas redes LAN.

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
Bogota2(config)#ip dhcp pool BOGOTA2
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.1.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#ip dhcp pool BOGOTA3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-route 172.29.0.1
Bogota2(dhcp-config)#dns-server 8.8.8.8
Bogota2(dhcp-config)#exit
```

Posteriormente configuramos el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
Bogota3(config)#int g0/0
Bogota3(config-if)#ip helper-address 172.29.3.14
Bogota3(config-if)#exit
```

Por último, verificamos que los hosts hayan tomado el direccionamiento de forma automática desde el servidor DCHP con lo cual garantizamos la configuración exitosa del servicio.

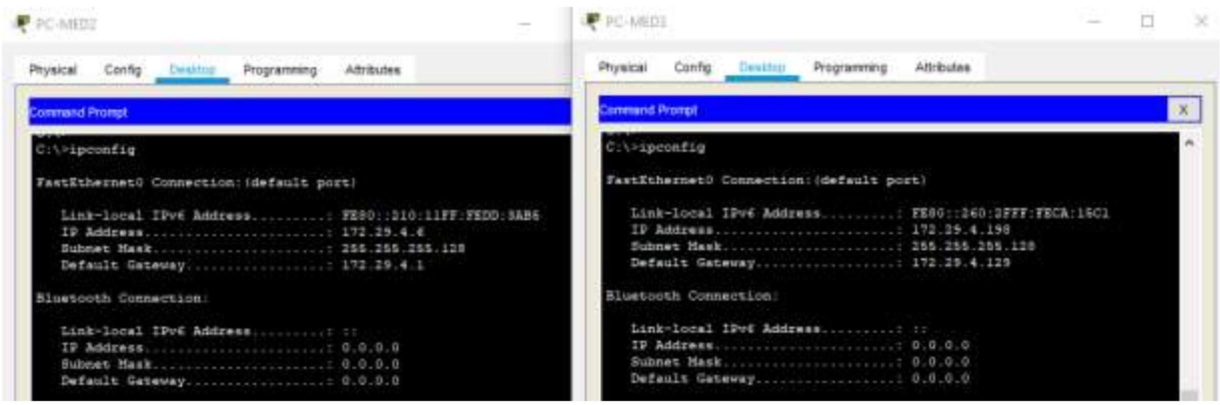


Figura 46. Direccionamiento DHCP PCs Medellín

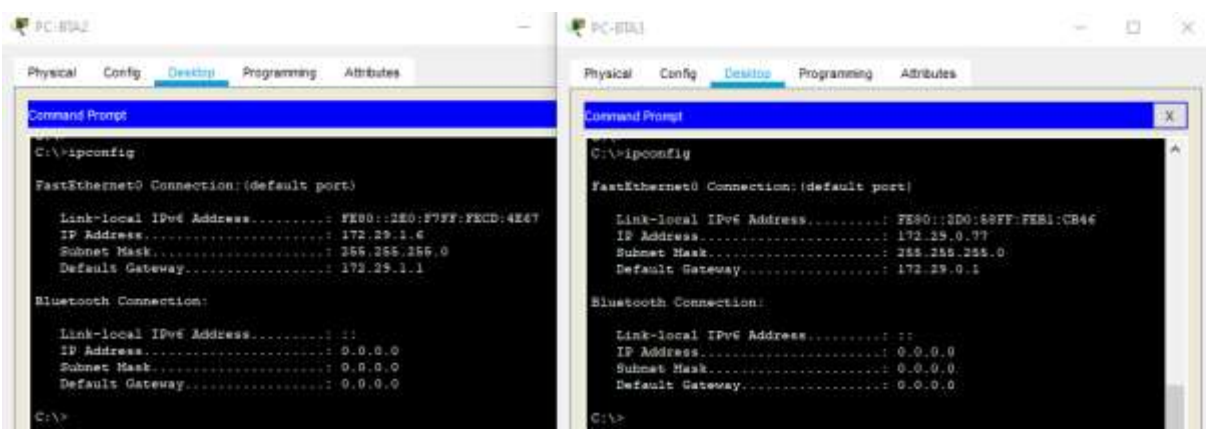


Figura 47. Direccionamiento DHCP PCs Bogotá

CONCLUSIONES

Mediante la realización y solución de los dos escenarios planteados como desarrollo de la Evaluación - Prueba de habilidades CCNA del Diplomado de Profundización de Cisco, se logró poner en práctica los conocimientos adquiridos a lo largo del curso logrando el diseño y configuración de las redes propuestas.

Se pudo apreciar el correcto funcionamiento de la herramienta Packet Tracer de Cisco la cual realiza una simulación real de los dispositivos y funcionamiento de las redes siendo esto de gran ayuda para poder aplicar los conocimientos adquiridos en el proceso de formación y de esta forma poder cumplir con los objetivos planteados con la realización de este trabajo.

Con el desarrollo de ese trabajo, de igual forma, se logró dar solución a los problemas presentados en cuanto a la conectividad y/o configuración de algunos dispositivos lo cual fue muy enriquecedor y será de gran utilidad para el desempeño de nuestras labores como profesionales en el campo de la tecnología.

BIBLIOGRAFÍA

CISCO. “DHCP. Principios de Enrutamiento y Conmutación”. {En línea}. {12 de mayo de 2020}. Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. “MODULO DE ESTUDIO CCNA1 EXPLORATION (Network Fundamentals)”. {En línea}. {11 de mayo de 2020}. Disponible en: http://www.mediafire.com/?9cq9h4jo23c1359

CISCO. “MODULO DE ESTUDIO CCNA2 EXPLORATION (Routing Protocols and Concepts)”. {En línea}. {12 de mayo de 2020}. Disponible en: http://www.mediafire.com/?5y052miul2vezhj

CISCO. “Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación”. {En línea}. {13 de mayo de 2020}. Disponible en: https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1