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

CARLOS ANDRÉS ACOSTA ACEVEDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
PROGRAMA DE INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

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

CARLOS ANDRÉS ACOSTA ACEVEDO

Trabajo de Diplomado para optar por el título de Ingeniero de Sistemas

HÉCTOR JULIÁN PARRA MOGOLLÓN
Msc. Dirección Estratégica Especialidad Telecomunicaciones

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
PROGRAMA DE INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

Nota de Aceptación

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ibagué, 08 de mayo de 2020

Dedicatoria

A mi padre que siempre estuvo cuando lo necesite y me brindo los mejores valores éticos, experiencias y conocimientos para ser la persona que soy, fue muy importante para lograr una de las metas más importantes para mí en el ámbito académico, a mi Madre que en la distancia me apoyaba moralmente brindándome su apoyo, a todos mis seres queridos que de una u otra forma pusieron su granito de arena y a Dios por darme la vida, salud, prosperidad y el conocimiento requerido.

AGRADECIMIENTOS

Primero que todo doy gracias a Dios porque me ha permitido alcanzar las metas que deseo realizar, a la Red Educativa y tutores en general de la Universidad Nacional Abierta y a Distancia.

A mis padres que me dieron la vida y me permitieron ser un estudiante ejemplar y responsable para realizar mis deberes educativos y personales.

A Sandra Gómez Melo que siempre fue como una Madre para mí, por sus consejos y valiosa compañía cuando lo necesité, a mi hermano Juan David Acosta que gracias a él me dan ganas de prosperar para que en un futuro no nos falte nada, a Mónica Victoria Muñoz por su apoyo incondicional y a todos mis seres queridos que creyeron en mi infinitas gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACL: Lista de control de acceso. Permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Las listas de acceso de control pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a unos cortafuegos.

DHCP: Protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales. Además de la dirección IP, DHCP también asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes.

ENRUTADOR: Dispositivo de interconexión de redes que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Pueden proporcionar conectividad dentro de las empresas, entre las empresas e Internet, y en el interior de proveedores de servicios de Internet (ISP).

NAT: Funciona en un enrutador, generalmente conectando dos redes juntas, y traduce las direcciones privadas (no globalmente únicas) en la red interna en direcciones legales, antes de que los paquetes se envíen a otra red. Se puede configurar para anunciar solo una dirección para toda la red al mundo exterior. Esto proporciona seguridad adicional al ocultar de manera efectiva toda la red interna detrás de esa dirección. NAT ofrece las funciones duales de seguridad y conservación de direcciones y, por lo general, se implementa en entornos de acceso remoto.

NTP: Protocolo que proporciona los mecanismos de protocolo básicos necesarios para sincronizar los relojes de los diferentes sistemas con una precisión del orden de nanosegundos. Contiene indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local, así como las propiedades del reloj de referencia.

OSPF: Open Shortest Path First (OSPF), definido en RFC 2328, es un Internal Gateway Protocol (IGP) que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo. Está basado en tecnología de estado de link, la cual es una desviación del algoritmo basado en el vector Bellman-Ford usado en los protocolos de ruteo de Internet tradicionales, como el RIP.

RIP: protocolo de encaminamiento interno. Protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino. Es muy usado en sistemas de conexión a internet como infovía, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

SWITCH: Dispositivo que se utiliza para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Actúa también de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Permiten ahorrar dinero y aumentar la productividad mediante el uso compartido de información y la asignación de recursos.

VLAN: Acrónimo de virtual LAN (red de área local virtual). Su utilidad radica en la posibilidad de separar aquellos segmentos lógicos que componen una LAN y que no tienen la necesidad de intercambiar información entre sí a través de la red de área local. Esta particularidad contribuye a una administración más eficiente de la red física. Puede formarse con dos redes de computadoras (ordenadores) que se hallan conectadas, en sentido físico, a distintos segmentos de una LAN, pero que sin embargo actúan como si estuviesen unidos al mismo puerto.

RESUMEN

Con el desarrollo de pruebas de habilidades prácticas es posible potenciar conocimientos, establecer herramientas de apoyo para el proceso educativo, y la adquisición de competencias y habilidades en la solución de problemas a través de simuladores, con los que puede interactuar y experimentar para luego llevar a la realidad los conocimientos y experiencias adquiridos y presentar soluciones de networking según el caso presentado. Como resultado de este proceso, se presenta la solución a dos estudios de caso bajo el uso de la tecnología Cisco, trabajados en la herramienta Packet Tracer la cual permite trabajar los diferentes protocolos de enrutamiento, configuración de dispositivos, creación de redes virtuales, configuración y verificación de traducciones de direcciones de red, entre otras funcionalidades, que permiten al estudiante adquirir y afianzar lo aprendido durante su proceso formativo.

PALABRAS CLAVE: Solución de problemas, tecnología Cisco, VLAN, OSPF, NAT, RIP, Packet Tracer.

1. INTRODUCCIÓN

El trabajo presentado se centra en la solución de dos estudios de caso mediante el uso de la tecnología Cisco. Esta tecnología es líder mundial en TI y red, pues ofrece soluciones de todo tipo, para networking robustas y eficientes. El crecimiento de las redes de comunicación a nivel mundial aumenta a un ritmo acelerado, con el Internet de Todo hoy día es más posible y accesible la conexión en red de personas, procesos, datos y objetos, las cuales están dando lugar a la toma de decisiones y acciones para buscar nuevas experiencias y oportunidades de crecimiento a personas, empresas y países.

La evaluación de habilidades prácticas como producto final del Diplomado de Profundización en Cisco CCNA, busca que el estudiante adquiera competencias y habilidades en la búsqueda de soluciones eficaces a problemas relacionados con diferentes aspectos de networking, entre ellos los modelos y protocolos de comunicación de redes, el direccionamiento IPv4 e IPv6, la configuración de dispositivos de red y la verificación de la red.

De acuerdo a lo anterior, se desarrollan dos escenarios, el primero de ellos, involucra la configuración de una red pequeña que admite conectividad entre protocolos IPv4 e IPv6, seguridad de switches, routing entre VLAN, routing dinámico RIPv2, protocolo de configuración de host dinámicos DHCP, Traducción de direcciones de red dinámicas y estáticas NAT, listas de control de acceso ACL, y el protocolo de tiempo de red NTP. Y un segundo escenario, que busca la conexión entre dos ciudades, planteando el uso del protocolo de enrutamiento OSPF, encapsulamiento PPP y su autenticación.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Identificar el grado de desarrollo de competencias y habilidades adquiridas a lo largo del Diplomado de profundización Cisco CCNA, evidenciando el nivel de comprensión y solución de problemas relacionados con diferentes aspectos de Networking.

2.2 OBJETIVOS ESPECÍFICOS

- Diseño de topologías en el software de simulación Packet Tracer.
- Creación, configuración y asginación de VLAN
- Configuración y verificación de protocolos de enrutamiento RIPv2 y OSPF.
- Creación de listas de acceso para permiso o negación de tráfico.

3. DESARROLLO DE ESCENARIOS

3.1 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.

3.1.1 Topología

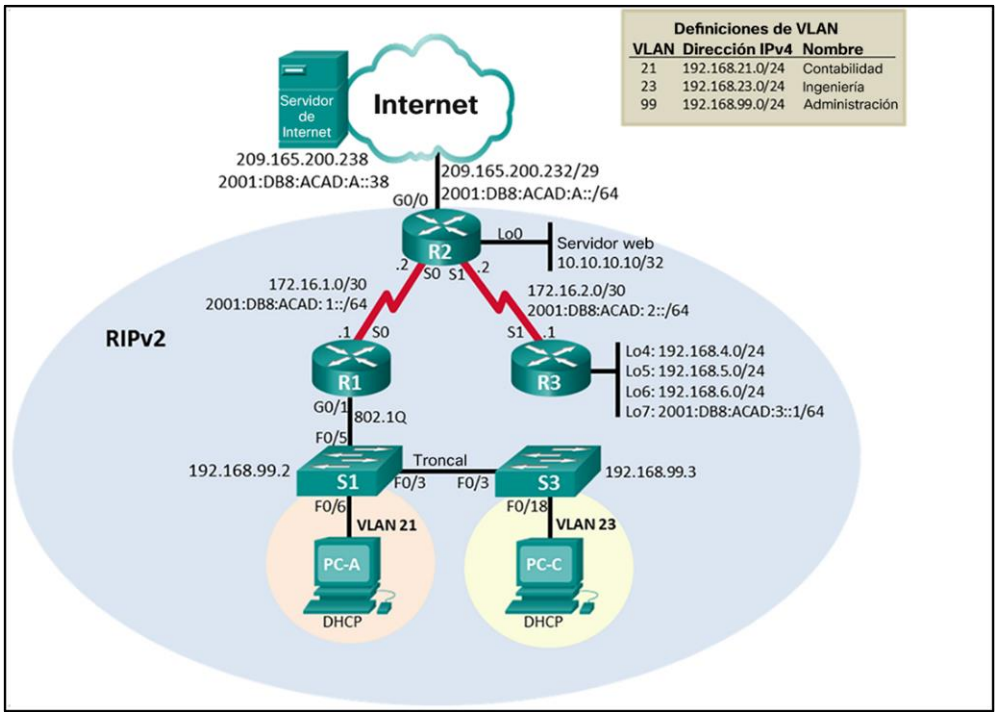

Figura 1. Topología Escenario 1

3.1.2 Inicializar dispositivos

Se realiza la implementación de la topología en el software Packet Tracer versión 7.3.0.0838. Se utilizarán los siguientes dispositivos:

- 3 Router 1941
- 2 Switch C2960
- 2 PC Escritorio
- 1 Servidor Internet

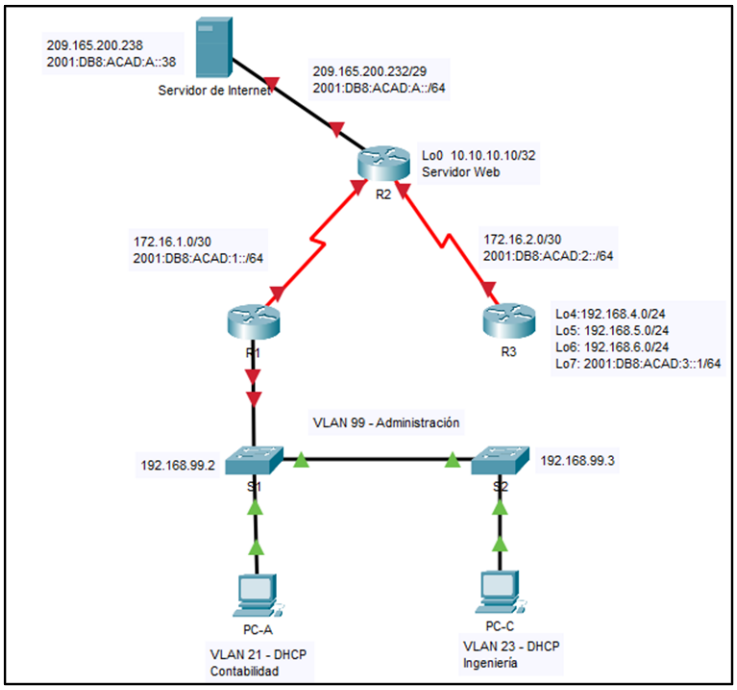

Figura 2. Topología Escenario 1. Packet Tracer

3.1.3 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.

Tabla 1. Inicialización Routers y Switch

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	*enable* *erase startup-config*
Volver a cargar todos los routers	*reload*
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	*erase startup-config* *erase nvram:* *delete vlan.dat*
Volver a cargar ambos switches	*reload*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	*Show flash:*

3.1.4 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):

Tabla 2. Configuración Servidor de Internet

Servidor de Internet	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.237
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Se ingresa al modo de configuración el dispositivo.

Tabla 3. Parámetros Configuración R1.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del router	*hostname R1*
Contraseña de exec privilegiado cifrada	*enable secret class*
Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*

Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*
Interfaz S0/0/0	Establezca la descripción: *description Conectado a R2* Establecer la dirección IPv4 *Ip address 172.16.1.1 255.255.255.252* Establecer la dirección IPv6 *Ipv6 address 2001:DB8:ACAD:1::1/64* Establecer la frecuencia de reloj en 128000 *clock rate 128000* Activar la interfaz *No shutdown*
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 *Ip route 0.0.0.0 0.0.0.0 172.16.1.2* Configurar una ruta IPv6 predeterminada de S0/0/0 *Ipv6 route ::/0 2001:DB8:ACAD:1::2*

Nota: Todavía no configuré G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Parámetros Configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del router	*hostname R2*
Contraseña de exec privilegiado cifrada	*enable secret class*
Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*
Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Habilitar el servidor HTTP	*Ip http server* *Ip http secure-server* *Ip http authentication local*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*
Interfaz S0/0/0	Establezca la descripción *description Conectado a R1* Establezca la dirección IPv4. *Ip add 172.16.1.2 255.255.255.252* Establezca la dirección IPv6. *Ipv6 add 2001:DB8:ACAD:1::2/64* Activar la interfaz *no shutdown*

Interfaz S0/0/1	Establecer la descripción *description Conectado a R3* Establezca la dirección IPv4. *Ip add 172.16.2.2 255.255.255.252* Establezca la dirección IPv6. *Ipv6 add 2001:DB8:ACAD:2::2/64* Establecer la frecuencia de reloj en 128000. *clock rate 128000* Activar la interfaz *no shutdown*
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. *description Conectado a Servidor Internet* Establezca la dirección IPv4. *Ip add 209.165.200.237 255.255.255.248* Establezca la dirección IPv6. *Ipv6 add 2001:DB8:ACAD:A::/64* Activar la interfaz *no shutdwon*
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. *description Conectado a Lo0* Establezca la dirección IPv4. *Ip add 10.10.10.10 255.255.255.252*
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. *Ip route 0.0.0.0 0.0.0.0 209.165.200.238* Configure una ruta IPv6 predeterminada de G0/0. *Ipv6 route ::/0 2001:DB8:ACAD:A::38*

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Parámetros Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*

Nombre del router	*hostname R3*
Contraseña de exec privilegiado cifrada	*enable secret class*
Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*
Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*
Interfaz S0/0/1	Establecer la descripción *description Conectado a R2* Establezca la dirección IPv4. *Ip add 172.16.2.1 255.255.255.252* Establezca la dirección IPv6. *Ipv6 add 2001:DB8:ACAD:2::1/64* Activar la interfaz *no shutdwon*
Interfaz loopback 4	Establezca la dirección IPv4. *Ip add 192.168.4.1 255.255.255.0*
Interfaz loopback 5	Establezca la dirección IPv4. *Ip add 192.168.5.1 255.255.255.0*
Interfaz loopback 6	Establezca la dirección IPv4. *Ip add 192.168.6.1 255.255.255.0*
Interfaz loopback 7	Establezca la dirección IPv6. *Ipv6 add 2001:DB8:ACAD:3::1/64*
Rutas predeterminadas	*Ip route 0.0.0.0 0.0.0.0 172.16.2.2*

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Parámetros Configuración S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del switch	*hostname S1*
Contraseña de exec privilegiado cifrada	*enable secret class*
Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*
Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Parámetros Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del switch	*hostname S3*
Contraseña de exec privilegiado cifrada	*enable secret class*
Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*
Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso. Ver Figura 3
R2	R3, S0/0/1	172.16.2.1	Exitoso. Ver Figura 4
PC de Internet	Gateway predeterminado	209.165.200.237	Exitoso. Ver Figura 5

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

```
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 = 4/7/8 ms
```

Figura 3 Ping desde R1 a R2

```
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/10 ms
```

Figura 4 PIng desde R2 a R3

```
C:\>ping 209.165.200.237

Pinging 209.165.200.237 with 32 bytes of data:

Reply from 209.165.200.237: bytes=32 time<1ms TTL=255
Reply from 209.165.200.237: bytes=32 time<1ms TTL=255
Reply from 209.165.200.237: bytes=32 time<1ms TTL=255
Reply from 209.165.200.237: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 5 Ping desde Servidor a Gateway Predeterminado

3.1.5 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Parámetros Configuración S1- VLAN

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	*Vlan 21* *Name Contabilidad* *Vlan 23* *Name Ingenieria* *Vlan 99* *Name Administración*
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología *Interface vlan 99* (Se ingresa a la interfaz) *Ip add 192.168.99.2 255.255.255.0* (Se asigna la dirección ip) No shutdown
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. *Ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native Interface fa0/3 (Ingreso al modo de configuración de la interfaz) Switchport mode trunk (Establecer el modo troncal) Switchport trunk native vlan 1 (Asignar la vlan 1 como nativa)

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native Interface fa0/5 (Ingreso al modo de configuración de la interfaz) Switchport mode trunk (Establecer el modo troncal) Switchport trunk native vlan 1 (Asignar la vlan 1 como nativa)
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range: interface range fa0/1-2,fa0/7-24,fa0/4 switchport mode access
Asignar F0/6 a la VLAN 21	interface fa0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	Interface range fa0/7-24 shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Parámetros Configuración S3- VLAN

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	*Vlan 21* *Name Contabilidad* *Vlan 23* *Name Ingenieria* *Vlan 99* *Name Administracion*
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología *Interface vlan 99* (Se ingresa a la interfaz) *Ip add 192.168.99.3 255.255.255.0* (Se asigna la dirección ip) No shutdown

Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. *Ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native Interface fa0/3 (Ingreso al modo de configuración de la interfaz) Switchport mode trunk (Establecer el modo troncal) Switchport trunk native vlan 1 (Asignar la vlan 1 como nativa)
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range: interface range fa0/1-2,fa0/4-7,fa0/19-24 switchport mode access
Asignar F0/18 a la VLAN 23	interface fa0/18 switchport mode access switchport access vlan 23
Apagar todos los puertos sin usar	interface range fa0/1-2,fa0/4-7,fa0/19-24 shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Parámetros Configuración R1 - Subinterfaces

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz Interface g0/1.21 Description LAN de Contabilidad Encapsulation dot1q 21 Ip add 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz Interface g0/1.23 Description LAN de Contabilidad Encapsulation dot1q 23 Ip add 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz Interface g0/1.99 Description LAN de Contabilidad Encapsulation dot1q 99 Ip add 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	No shutdown

Paso 5: 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:

Tabla 12Verificación de la conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso. Ver Figura 6
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso Ver Figura 7
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso Ver Figura 8
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso Ver Figura 9

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Figura 6 Ping desde S1 a R1 Vlan 99

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Figura 7 Ping desde S3 a R1 Vlan 99

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos 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
```

Figura 8 Ping desde S1 a R1 Vlan 21

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Figura 9 Ping desde S3 a R1 Vlan 23

3.1.6 Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Parámetros Configuración RIPv2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip (Se ingresa al modo de configuración del router) version 2 (seleccionar la version 2)

Anunciar las redes conectadas directamente	Network 172.16.1.0 Network 192.168.99.0 Network 192.168.21.0 Network 192.168.23.0
Establecer todas las interfaces LAN como pasivas	Router rip Passive-interface g0/0-1
Desactive la sumarización automática	No auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Parámetros Configuración RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip (Se ingresa al modo de configuración del router) version 2 (seleccionar la version 2)
Anunciar las redes conectadas directamente	Network 172.16.1.0 Network 172.16.2.0 Network 10.10.10.10 **Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	Router rip Passive-interface Lo0
Desactive la sumarización automática.	No auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Parámetros Configuración RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Router rip (Se ingresa al modo de configuración del router) version 2 (seleccionar la version 2)

Anunciar redes IPv4 conectadas directamente	Network 172.16.2.0 Network 192.168.4.0 Network 192.168.5.0 Network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Router rip Passive-interface Lo4,Lo5,Lo6,Lo7
Desactive la sumarización automática.	No auto-summary

Paso 4: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 16 Verificación RIPv2

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. Ver Figuras 10,11 y 12
¿Qué comando muestra solo las rutas RIP?	Show ip route rip / Show ip rip database Ver Figuras 13,14 y 15
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show ip protocols / show running-config

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
  GigabitEthernet0/1.99 2     2
  GigabitEthernet0/1.21 2     2
  GigabitEthernet0/1.23 2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
           172.16.0.0
           192.168.21.0
           192.168.23.0
           192.168.99.0
Passive Interface(s):
           GigabitEthernet0/0
           GigabitEthernet0/1
Routing Information Sources:
           Gateway         Distance      Last Update
           172.16.1.2           120      00:04:01
Distance: (default is 120)
```

Figura 10 Verificación RIP en R1

```
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           2     2
  Serial0/0/1           2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
           10.0.0.0
           172.16.0.0
Passive Interface(s):
           Loopback0
Routing Information Sources:
           Gateway         Distance      Last Update
           172.16.2.1           120      00:00:22
           172.16.1.1           120      00:00:18
Distance: (default is 120)
```

Figura 11 Verificación RIP en R2

```
R3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 2 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface              Send  Recv  Triggered RIP  Key-chain
  Serial0/0/1            2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
            172.16.0.0
            192.168.4.0
            192.168.5.0
            192.168.6.0
Passive Interface(s):
            Loopback4
            Loopback5
            Loopback6
            Loopback7
Routing Information Sources:
            Gateway         Distance      Last Update
            172.16.2.2           120      00:00:28
Distance: (default is 120)
R3#
```

Figura 12 Verificación RIP en R3

```
R1#show ip route rip
     10.0.0.0/30 is subnetted, 1 subnets
R       10.10.10.8 [120/1] via 172.16.1.2, 00:00:12, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:12, Serial0/0/0
R    192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
R    192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
R    192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
```

Figura 13 Verificación Rutas RIP en R1

```
R2#show ip route rip
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R    192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/1
R    192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/1
R    192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/1
R    192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:13, Serial0/0/0
R    192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:13, Serial0/0/0
R    192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:13, Serial0/0/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
```

Figura 14 Verificación Rutas RIP en R2

```
R3#show ip route rip
     10.0.0.0/30 is subnetted, 1 subnets
R       10.10.10.8 [120/1] via 172.16.2.2, 00:00:10, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:10, Serial0/0/1
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
R    192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
R    192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:10, Serial0/0/1
```

Figura 15 Verificación Rutas RIP en R3

3.1.7 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:

Tabla 17 Parámetros Configuración DHCP y NAT

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	*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	*Ip dhcp excluded-address 192.168.23.1 192.168.23.20*
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado *Ip dhcp pool ACCT* *network 192.168.21.0 255.255.255.0* *Dns-server 10.10.10.10* *Domain-name ccna-sa.com* *Default-router 192.168.21.1*

Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado *Ip dhcp pool ENGNR* *network 192.168.23.0 255.255.255.0* *Dns-server 10.10.10.10* *Domain-name ccna-sa.com* *Default-router 192.168.23.1*

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configuración NAT estática y dinámica en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** *aaa new-model* *aaa authentication login default local* *aaa authorization network default local* *username webuser privilege 15 pass cisco12345*
Habilitar el servicio del servidor HTTP	*Ip http server* Este comando no se encuentra habilitado en la última versión de packet tracer 7.3.0.0838
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	*ip http authentication local* Este comando no se encuentra habilitado en la última versión de packet tracer 7.3.0.0838

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** *Ip nat inside source static 209.165.200.238 209.165.200.229*
Asignar la interfaz interna y externa para la NAT estática	*int g0/0* *ip nat inside* *int s0/0/0* *ip nat outside* *int s0/0/1* *ip nat outside*
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 *Access-list 1 permit 192.168.21.0 0.0.0.255* *Access-list 1 permit 192.168.23.0 0.0.0.255*
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** *Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248*
Definir la traducción de NAT dinámica	*Ip nat inside source list 1 pool nat overload*

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.

Tabla 19 Verificación Protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ver Figura 16

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ver Figura 17
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso. Ver Figura 18
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**	Se muestra la página Web. Ver Figura 19

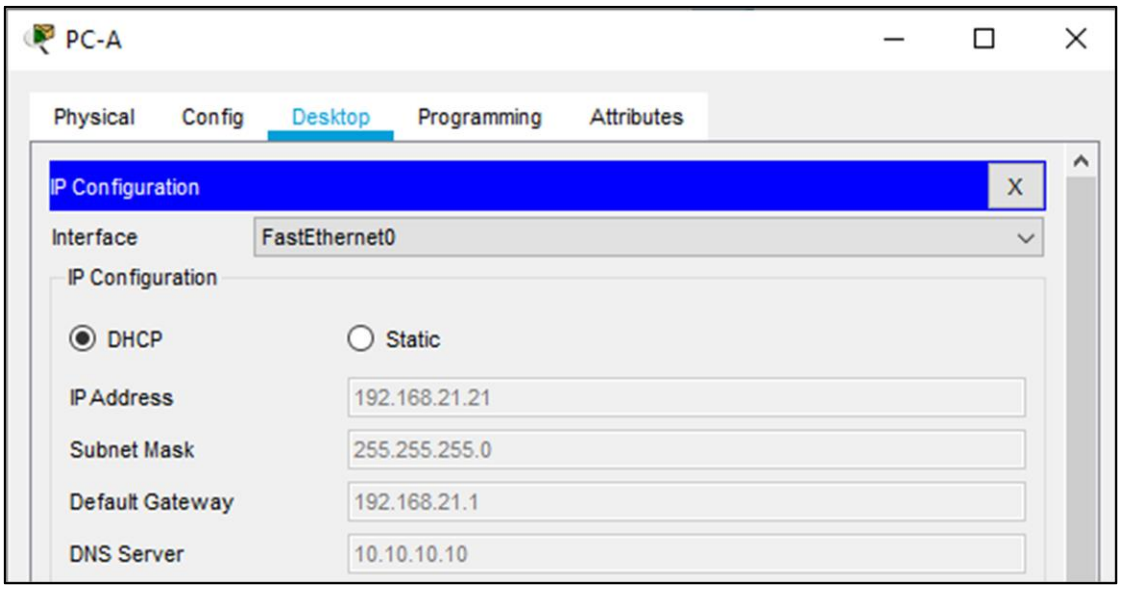

Figura 16 Verificación DHCP en PCA

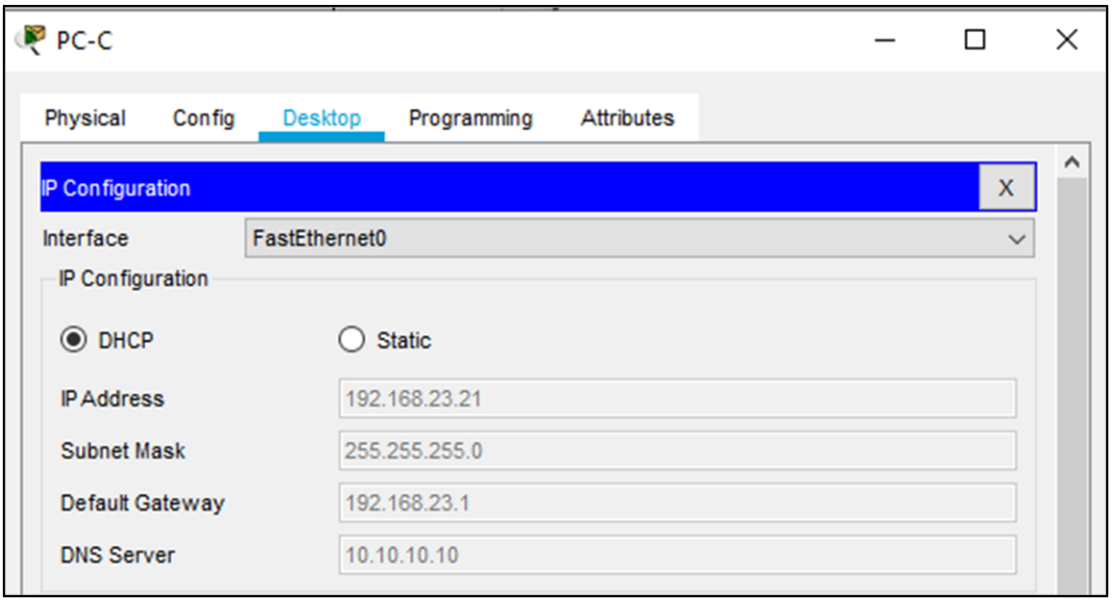

Figura 17 Verificación DHCP en PCC

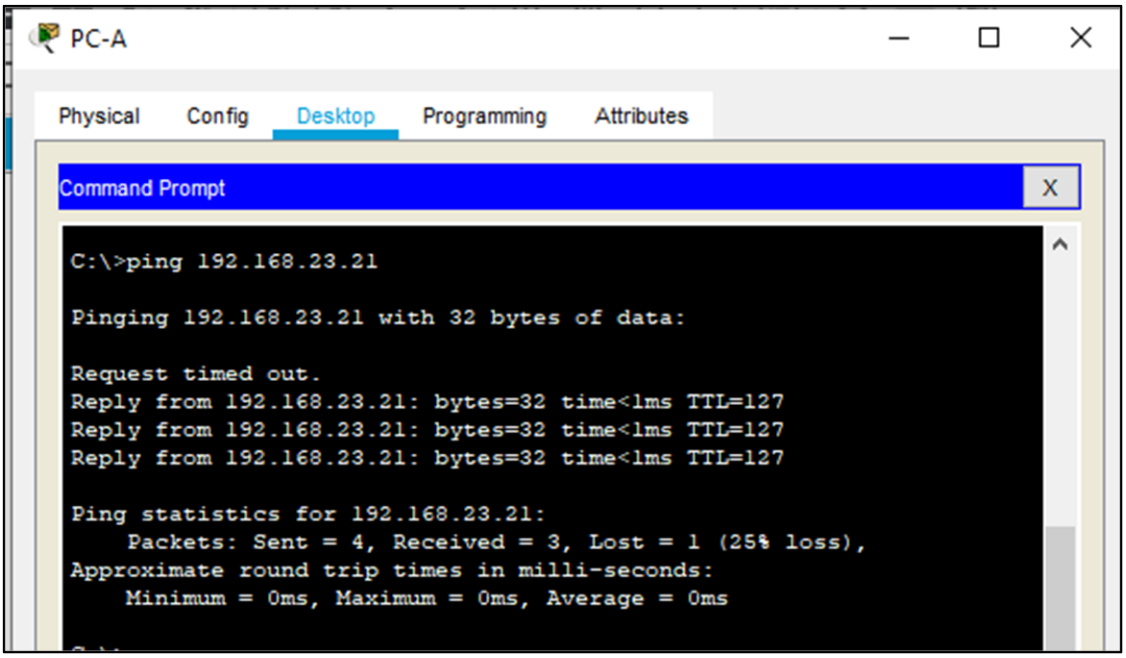

Figura 18 Verificación Ping PCA a PCC

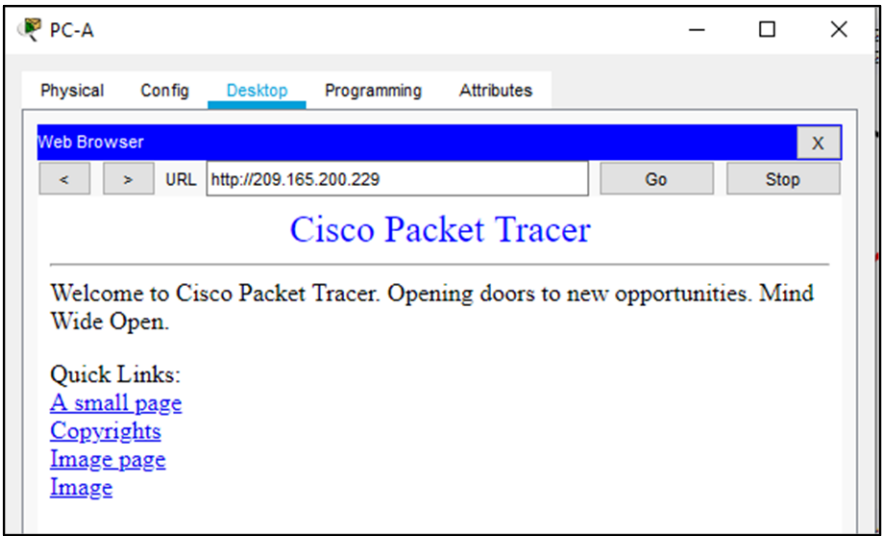

Figura 19 Navegador Web

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.229:5 209.165.200.238:5  172.16.2.1:5       172.16.2.1:5
icmp 209.165.200.229:6 209.165.200.238:6  172.16.2.1:6       172.16.2.1:6
icmp 209.165.200.229:7 209.165.200.238:7  172.16.2.1:7       172.16.2.1:7
icmp 209.165.200.229:8 209.165.200.238:8  172.16.2.1:8       172.16.2.1:8
---  209.165.200.229   209.165.200.238    ---                ---

R2#
```

Figura 20 Verificación NAT estática

3.1.8 Configurar NTP

Tabla 20 Parámetros Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** *clock set 09:00:00 6 May 2020* *Ver Figura 21*
Configure R2 como un maestro NTP.	Servidor: **R2** Nivel de estrato: **5** *ntp master 5*
Configurar R1 como un cliente NTP.	*ntp server 172.16.1.2*
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	*ntp update-calendar*

Verifique la configuración de NTP en R1.	Show ntp status Ver Figura 22

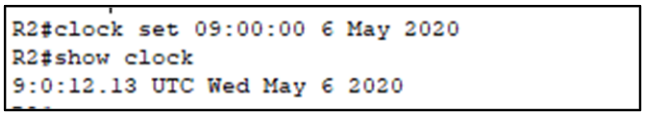

Figura 21 Ajuste Fecha y hora en R2

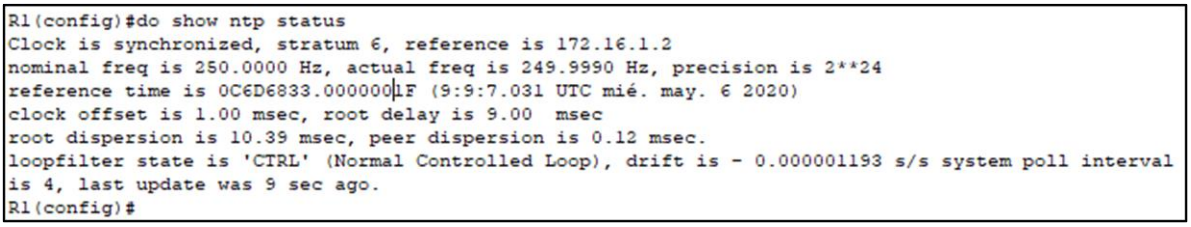

Figura 22 Verificación Configuración NTP en R1

3.1.9 Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 21 Configuración listas de acceso en VTY

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** *Ip access-list standard ADMIN-MGT* *Permit host 172.16.1.1*
Aplicar la ACL con nombre a las líneas VTY	*Line vty 0 4* *Access-class ADMIN-MGT in*
Permitir acceso por Telnet a las líneas de VTY	*Transport input telnet*
Verificar que la ACL funcione como se espera	Show access-lists / show running config Ver Figuras 23 y 24

```
R2#show acc
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
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

Figura 23 Verificación ACL en R2

```
!
line aux 0
!
line vty 0 4
 access-class ADMIN-MGT in
 password 7 0822455D0A16
!
!
```

Figura 24 Verificación ACL en líneas VTY en R2

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

Tabla 22 Comandos de verificación

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Con el comando *clear access-list counters* se restablece el resultado para mostrar 42olo las nuevas coincidencias./ *show ip access-lists*
Restablecer los contadores de una lista de acceso	*clear access-list counters / clear access-list ipv4*
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*show access-lists / show ip interface*
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. *Show ip nat translations*

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*clear ip nat translation* *

3.2 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

3.2.1 Topología de red

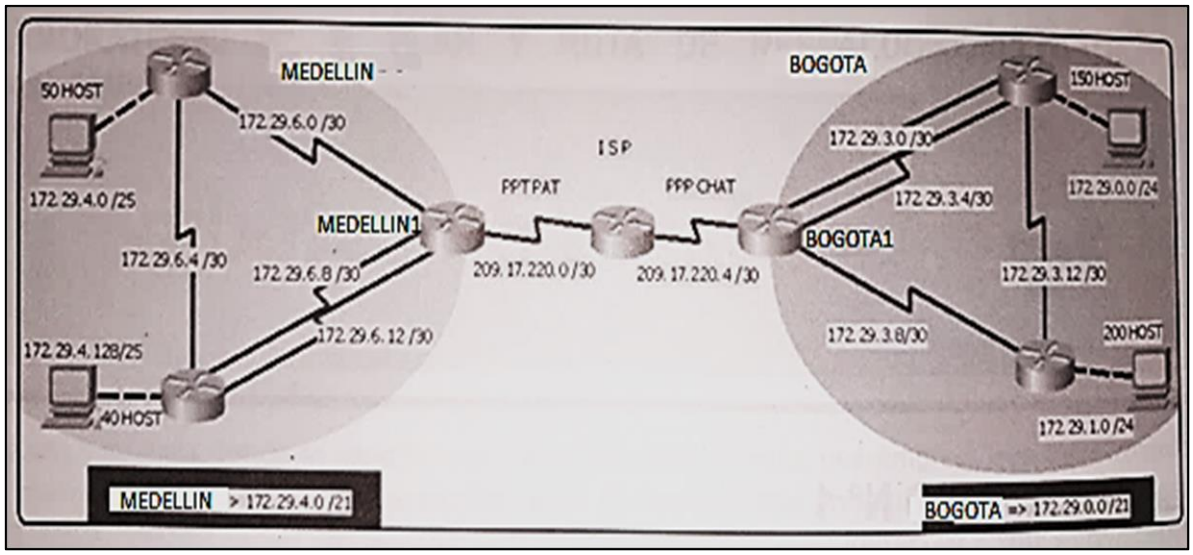

Figura 25 Topología Escenario 2

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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

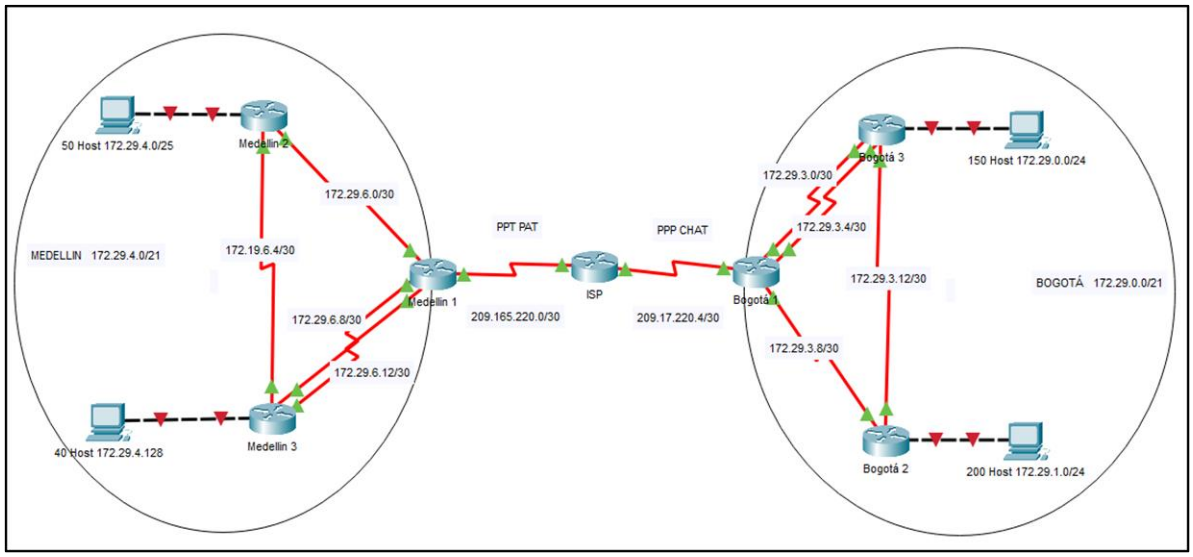

Figura 26 Diseño Topología Escenario 2

Se realiza la implementación de la topología en el software Packet Tracer versión 7.3.0.0838. Se utilizarán los siguientes dispositivos:

- 7 Router Cisco 1841
- 4 PC Escritorio

3.2.2 Configuración Inicial de Dispositivos

Para todos los routers se aplica la configuración inicial que se observa en la Tabla 23 de acuerdo a los requerimientos solicitados.

Tabla 23 Configuración Inicial de dispositivos

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del router	*Se asigna el nombre a cada dispositivo con el comando hostname*
Contraseña de exec privilegiado cifrada	*enable secret class*

Contraseña de acceso a la consola	*Line console 0 (se ingresa al modo de configuración de la línea de consola)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Configura el equipo para que requiera autenticación al iniciar sesión)*
Contraseña de acceso Telnet	*Line vty 0 4 (se ingresa al modo de configuración de la línea vty)* *Password cisco (Se asigna la contraseña como cisco)* *Login (Impide el acceso al dispositivo mediante telnet sin autenticación)*
Cifrar las contraseñas de texto no cifrado	*Service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado. *banner motd "Se prohibe el acceso no autorizado"*

Como ejemplo, se muestra a continuación la configuración para el router Medellin 1:

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname Medellin1
Medellin1(config)#enable secret class
Medellin1(config)#line console 0
Medellin1(config-line)#pass cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#line vty 0 4
Medellin1(config-line)#pass cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#service password-encryption
Medellin1(config)#banner motd "Se prohibe el acceso no autorizado"
Medellin1(config)#
```

Se configuran las direcciones Ip indicadas en la Tabla 24 para cada uno de los dispositivos, así mismo se utilizan los parámetros de configuración ip indicados en la Tabla 25.

Tabla 24 Direccionamiento IP

Dispositivo	Interfaz	Descripción Conectado a	Dirección IP/Máscara de subred
Bogotá 1	S0/0/0	S0/0/0 ISP	209.17.220.6/30
	S0/0/1	S0/1/0 Bogota3	172.29.3.1/30
	S0/1/0	S0/0/1 Bogota3	172.29.3.5/30
	S0/1/1	S0/0/0 Bogota 2	172.29.3.9/30
Bogotá 2	S0/0/0	S0/1/1 Bogota1	172.29.3.10/30
	S0/0/1	S0/0/0 Bogota3	172.29.3.13/30
Bogotá 3	S0/0/0	S0/0/1 Bogota2	172.29.3.14/30
	S0/0/1	S0/1/0 Bogota1	172.29.3.6/30
	S0/1/0	S0/0/1 Bogota1	172.29.3.2/30
ISP	S0/0/0	S0/0/0 Bogota1	209.17.220.5/30
	S0/0/1	S0/1/0 Medellin 1	209.17.220.2/30
Medellin 1	S0/0/0	S0/0/0 Medellin 2	172.29.6.1/30
	S0/0/1	S0/0/1 Medellin 3	172.29.6.9/30
	S0/1/1	S0/1/0 Medellin 3	172.29.6.13/30
	S0/1/0	S0/0/1 ISP	209.17.220.1/30
Medellin 2	S0/0/0	S0/0/0 Medellin 1	172.29.6.2/30
	S0/0/1	S0/0/0 Medellin 3	172.29.6.5/30
Medellin 3	S0/0/0	S0/0/1 Medellin 2	172.29.6.6/30
	S0/0/1	S0/0/1 Medellin 1	172.29.6.10/30
	S0/1/0	S0/1/1 Medellin 1	172.29.6.14/30

Tabla 25 Parámetros Direccionamiento IP

Bogotá 1 Interfaz S0/0/0	Establezca la descripción: *description Conectado a ISP* Establecer la dirección IPv4 *Ip address 209.17.220.6 255.255.255.252* Establecer la frecuencia de reloj en 128000 en las interfaces en que sea necesario. *clock rate 128000* Activar la interfaz *No shutdown*

Como ejemplo, se muestra la línea de comandos utilizada en el router Bogota1:

```
Bogota1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota1(config)#int s0/0/0
Bogota1(config-if)#description Conectado a ISP
Bogota1(config-if)#ip add 209.17.220.6 255.255.255.252
Bogota1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#description Conectado a Bogota3
Bogota1(config-if)#ip add 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#description Conectado a Bogota3
Bogota1(config-if)#ip add 172.29.3.5 255.255.255.252
Bogota1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#ip add 172.29.3.9 255.255.255.252
Bogota1(config-if)#description Conectado a Bogota2
Bogota1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
```

3.2.3 Configuración del enrutamiento

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

Configuración protocolo OSPFv2	
Medellin 1	Medellin1#config t Enter configuration commands, one per line. End with CNTL/Z. Medellin1(config)#router ospf 1 Medellin1(config-router)#network 172.29.6.0 255.255.255.252 area 1 Medellin1(config-router)#network 172.29.6.8 255.255.255.252 area 1 Medellin1(config-router)#network 172.29.6.12 255.255.255.252 area 1 Medellin1(config-router)#network 209.17.220.0 255.255.255.252 area 1

	Medellin1(config-router)#no auto-summary
Medellin 2	Medellin2(config)#router ospf 1 Medellin2(config-router)#network 172.29.6.4 255.255.255.252 area 1 Medellin2(config-router)#network 172.29.6.0 255.255.255.252 area 1 Medellin2(config-router)#no auto-summary
Medellin 3	Medellin3(config)#router ospf 1 Medellin3(config-router)#network 172.29.6.4 255.255.255.252 area 1 02:34:50: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/0/0 from LOADING to FULL, Loading Done Medellin3(config-router)#network 172.29.6.8 255.255.255.252 area 1 Medellin3(config-router)#network 172.29.6.12 255.255.255.252 area 1 Medellin3(config-router)# no auto-summary
ISP	ISP(config)#router ospf 1 ISP(config-router)#network 209.17.220.0 255.255.255.252 area 1 02:36:18: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/0/1 from LOADING to FULL, Loading Done ISP(config-router)#network 209.17.220.4 255.255.255.252 area 1 ISP(config-router)# no auto-summary
Bogota 1	Bogota1(config)#router ospf 1 Bogota1(config-router)#network 209.17.220.4 255.255.255.252 area 1 Bogota1(config-router)#network 172.29.3.0 255.255.255.252 area 1 02:37:52: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.5 on Serial0/0/0 from LOADING to FULL, Loading Done Bogota1(config-router)#network 172.29.3.0 255.255.255.252 area 1 Bogota1(config-router)#network 172.29.3.4 255.255.255.252 area 1 Bogota1(config-router)#network 172.29.3.8 255.255.255.252 area 1

	Bogota1(config-router)#no auto-summary
Bogota 2	Bogota2(config)#router ospf 1 Bogota2(config-router)#network 172.29.3.8 255.255.255.252 area 1 Bogota2(config-router)#network 172.29.3.12 255.255.255.252 area 1 Bogota2(config-router)#noauto 02:38:51: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0 from LOADING to FULL, Loading Done Bogota2(config-router)#no auto-summary
Bogota 3	Bogota3(config)#router ospf 1 Bogota3(config-router)#network 172.29.3.0 255.255.255.252 area 1 Bogota3(config-router)#network 172.29.3.4 255.255.255.252 area 1 Bogota3(config-router)# 02:39:53: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/1/0 from LOADING to FULL, Loading Done Bogota3(config-router)#network 172.29.3.12 255.255.255.252 area 1 Bogota3(config-router)# 02:39:59: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/1 from LOADING to FULL, Loading Done 02:40:00: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.13 on Serial0/0/0 from LOADING to FULL, Loading Done Bogota3(config-router)#no auto-summary

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.

Tabla 26 Configuración rutas por defecto hacia ISP

Configuración de rutas por defecto hacia el ISP	
Bogota 1	*Ip route 0.0.0.0 0.0.0.0 S0/0/0* (Creación de ruta por defecto) *Router ospf 1* (Ingresar al modo de configuración de OSPF) *Default-information originate*
Medellin 1	*Ip route 0.0.0.0 0.0.0.0 S0/1/0* (Creación de ruta por defecto) *Router ospf 1* (Ingresar al modo de configuración de OSPF) *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 sumarizan las subredes de cada uno a /22.

Se configuran las rutas en el router ISP de la siguiente manera:

```
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial 0/0/0
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/1
ISP(config)#exit
```

3.2.4 Tabla de Enrutamiento

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

Se realiza esta verificación mediante el comando *show ip route:*

```
ISP#show ip route
Codes: C - connected, S - static, I - IGRP, 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, 10 subnets, 2 masks
S       172.29.0.0/22 is directly connected, Serial0/0/0
O       172.29.3.0/30 [110/128] via 209.17.220.6, 00:17:22, Serial0/0/0
O       172.29.3.4/30 [110/128] via 209.17.220.6, 00:17:22, Serial0/0/0
O       172.29.3.8/30 [110/128] via 209.17.220.6, 00:17:22, Serial0/0/0
O       172.29.3.12/30 [110/192] via 209.17.220.6, 00:17:22, Serial0/0/0
S       172.29.4.0/22 is directly connected, Serial0/0/1
O       172.29.6.0/30 [110/128] via 209.17.220.1, 00:17:32, Serial0/0/1
O       172.29.6.4/30 [110/192] via 209.17.220.1, 00:17:22, Serial0/0/1
O       172.29.6.8/30 [110/128] via 209.17.220.1, 00:17:32, Serial0/0/1
O       172.29.6.12/30 [110/128] via 209.17.220.1, 00:17:32, Serial0/0/1
     209.17.220.0/30 is subnetted, 2 subnets
C       209.17.220.0 is directly connected, Serial0/0/1
C       209.17.220.4 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 209.17.220.1, 00:07:02, Serial0/0/1
               [110/1] via 209.17.220.6, 00:06:29, Serial0/0/0
```

Figura 27 Verificación Tabla Enrutamiento ISP

```
Medellin1#show ip route
Codes: C - connected, S - static, I - IGRP, 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 0.0.0.0 to network 0.0.0.0

     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/192] via 209.17.220.2, 00:20:38, Serial0/1/0
O       172.29.3.4 [110/192] via 209.17.220.2, 00:20:38, Serial0/1/0
O       172.29.3.8 [110/192] via 209.17.220.2, 00:20:38, Serial0/1/0
O       172.29.3.12 [110/256] via 209.17.220.2, 00:20:38, Serial0/1/0
C       172.29.6.0 is directly connected, Serial0/0/0
O       172.29.6.4 [110/128] via 172.29.6.10, 00:20:38, Serial0/0/1
                   [110/128] via 172.29.6.2, 00:20:38, Serial0/0/0
C       172.29.6.8 is directly connected, Serial0/0/1
C       172.29.6.12 is directly connected, Serial0/1/1
     209.17.220.0/30 is subnetted, 2 subnets
C       209.17.220.0 is directly connected, Serial0/1/0
O       209.17.220.4 [110/128] via 209.17.220.2, 00:20:38, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

Figura 28 Verificación Tabla Enrutamiento Medellin1

```
Medellin2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/256] via 172.29.6.1, 00:21:45, Serial0/0/0
O       172.29.3.4 [110/256] via 172.29.6.1, 00:21:45, Serial0/0/0
O       172.29.3.8 [110/256] via 172.29.6.1, 00:21:45, Serial0/0/0
O       172.29.3.12 [110/320] via 172.29.6.1, 00:21:45, Serial0/0/0
C       172.29.6.0 is directly connected, Serial0/0/0
C       172.29.6.4 is directly connected, Serial0/0/1
O       172.29.6.8 [110/128] via 172.29.6.6, 00:21:45, Serial0/0/1
                   [110/128] via 172.29.6.1, 00:21:45, Serial0/0/0
O       172.29.6.12 [110/128] via 172.29.6.6, 00:21:45, Serial0/0/1
                    [110/128] via 172.29.6.1, 00:21:45, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.1, 00:21:45, Serial0/0/0
O       209.17.220.4 [110/192] via 172.29.6.1, 00:21:45, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:11:30, Serial0/0/0
```

Figura 29 Verificación Enrutamiento Medellin2

```
Medellin3#show ip route
Codes: C - connected, S - static, I - IGRP, 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 172.29.6.13 to network 0.0.0.0

     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/256] via 172.29.6.13, 00:22:36, Serial0/1/0
O       172.29.3.4 [110/256] via 172.29.6.13, 00:22:36, Serial0/1/0
O       172.29.3.8 [110/256] via 172.29.6.13, 00:22:36, Serial0/1/0
O       172.29.3.12 [110/320] via 172.29.6.13, 00:22:36, Serial0/1/0
O       172.29.6.0 [110/128] via 172.29.6.13, 00:22:36, Serial0/1/0
                   [110/128] via 172.29.6.5, 00:22:36, Serial0/0/0
C       172.29.6.4 is directly connected, Serial0/0/0
C       172.29.6.8 is directly connected, Serial0/0/1
C       172.29.6.12 is directly connected, Serial0/1/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.13, 00:22:36, Serial0/1/0
O       209.17.220.4 [110/192] via 172.29.6.13, 00:22:36, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:12:21, Serial0/1/0
```

Figura 30 Verificación Tabla Enrutamiento Medellin3

```
Bogota1#show ip route
Codes: C - connected, S - static, I - IGRP, 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 0.0.0.0 to network 0.0.0.0

     172.29.0.0/30 is subnetted, 8 subnets
C       172.29.3.0 is directly connected, Serial0/0/1
C       172.29.3.4 is directly connected, Serial0/1/0
C       172.29.3.8 is directly connected, Serial0/1/1
O       172.29.3.12 [110/128] via 172.29.3.6, 00:24:31, Serial0/1/0
                    [110/128] via 172.29.3.10, 00:24:31, Serial0/1/1
O       172.29.6.0 [110/192] via 209.17.220.5, 00:24:31, Serial0/0/0
O       172.29.6.4 [110/256] via 209.17.220.5, 00:24:31, Serial0/0/0
O       172.29.6.8 [110/192] via 209.17.220.5, 00:24:31, Serial0/0/0
O       172.29.6.12 [110/192] via 209.17.220.5, 00:24:31, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 209.17.220.5, 00:24:31, Serial0/0/0
C       209.17.220.4 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

Figura 31 Verificación Tabla Enrutamiento Bogota1

```
Bogota2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/128] via 172.29.3.9, 00:25:28, Serial0/0/0
                   [110/128] via 172.29.3.14, 00:25:28, Serial0/0/1
O       172.29.3.4 [110/128] via 172.29.3.9, 00:25:28, Serial0/0/0
                   [110/128] via 172.29.3.14, 00:25:28, Serial0/0/1
C       172.29.3.8 is directly connected, Serial0/0/0
C       172.29.3.12 is directly connected, Serial0/0/1
O       172.29.6.0 [110/256] via 172.29.3.9, 00:25:28, Serial0/0/0
O       172.29.6.4 [110/320] via 172.29.3.9, 00:25:28, Serial0/0/0
O       172.29.6.8 [110/256] via 172.29.3.9, 00:25:28, Serial0/0/0
O       172.29.6.12 [110/256] via 172.29.3.9, 00:25:28, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/192] via 172.29.3.9, 00:25:28, Serial0/0/0
O       209.17.220.4 [110/128] via 172.29.3.9, 00:25:28, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:15:13, Serial0/0/0
```

Figura 32 Verificación Tabla Enrutamiento Bogota2

```
Bogota3#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     172.29.0.0/30 is subnetted, 8 subnets
C       172.29.3.0 is directly connected, Serial0/1/0
C       172.29.3.4 is directly connected, Serial0/0/1
O       172.29.3.8 [110/128] via 172.29.3.13, 00:26:38, Serial0/0/0
                   [110/128] via 172.29.3.1, 00:26:38, Serial0/1/0
C       172.29.3.12 is directly connected, Serial0/0/0
O       172.29.6.0 [110/256] via 172.29.3.1, 00:26:38, Serial0/1/0
O       172.29.6.4 [110/320] via 172.29.3.1, 00:26:38, Serial0/1/0
O       172.29.6.8 [110/256] via 172.29.3.1, 00:26:38, Serial0/1/0
O       172.29.6.12 [110/256] via 172.29.3.1, 00:26:38, Serial0/1/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/192] via 172.29.3.1, 00:26:38, Serial0/1/0
O       209.17.220.4 [110/128] via 172.29.3.1, 00:26:38, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:16:23, Serial0/1/0
```

Figura 33 Verificación Tabla Enrutamiento Bogota3

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

Se realiza esta verificación mediante el comando *show ip route ospf:*

```
ISP#show ip route ospf
     172.29.0.0/16 is variably subnetted, 10 subnets, 2 masks
O       172.29.3.0 [110/128] via 209.17.220.6, 00:31:03, Serial0/0/0
O       172.29.3.4 [110/128] via 209.17.220.6, 00:31:03, Serial0/0/0
O       172.29.3.8 [110/128] via 209.17.220.6, 00:31:03, Serial0/0/0
O       172.29.3.12 [110/192] via 209.17.220.6, 00:31:03, Serial0/0/0
O       172.29.6.0 [110/128] via 209.17.220.1, 00:31:13, Serial0/0/1
O       172.29.6.4 [110/192] via 209.17.220.1, 00:31:03, Serial0/0/1
O       172.29.6.8 [110/128] via 209.17.220.1, 00:31:13, Serial0/0/1
O       172.29.6.12 [110/128] via 209.17.220.1, 00:31:13, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 209.17.220.1, 00:20:43, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 209.17.220.6, 00:20:10, Serial0/0/0
```

Figura 34 Verificación Balanceo de Carga ISP

```
Medellin1#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/192] via 209.17.220.2, 00:33:09, Serial0/1/0
O       172.29.3.4 [110/192] via 209.17.220.2, 00:33:09, Serial0/1/0
O       172.29.3.8 [110/192] via 209.17.220.2, 00:33:09, Serial0/1/0
O       172.29.3.12 [110/256] via 209.17.220.2, 00:33:09, Serial0/1/0
O       172.29.6.4 [110/128] via 172.29.6.10, 00:33:09, Serial0/0/1
                   [110/128] via 172.29.6.2, 00:33:09, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.4 [110/128] via 209.17.220.2, 00:33:09, Serial0/1/0
```

Figura 35 Verificación Balanceo de Carga Medellin1

```
Medellin2#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/256] via 172.29.6.1, 00:33:45, Serial0/0/0
O       172.29.3.4 [110/256] via 172.29.6.1, 00:33:45, Serial0/0/0
O       172.29.3.8 [110/256] via 172.29.6.1, 00:33:45, Serial0/0/0
O       172.29.3.12 [110/320] via 172.29.6.1, 00:33:45, Serial0/0/0
O       172.29.6.8 [110/128] via 172.29.6.6, 00:33:45, Serial0/0/1
                   [110/128] via 172.29.6.1, 00:33:45, Serial0/0/0
O       172.29.6.12 [110/128] via 172.29.6.6, 00:33:45, Serial0/0/1
                    [110/128] via 172.29.6.1, 00:33:45, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.1, 00:33:45, Serial0/0/0
O       209.17.220.4 [110/192] via 172.29.6.1, 00:33:45, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:23:30, Serial0/0/0
```

Figura 36 Verificaicón Balanceo de Carga Medellin2

```
Medellin3#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/256] via 172.29.6.13, 00:34:21, Serial0/1/0
O       172.29.3.4 [110/256] via 172.29.6.13, 00:34:21, Serial0/1/0
O       172.29.3.8 [110/256] via 172.29.6.13, 00:34:21, Serial0/1/0
O       172.29.3.12 [110/320] via 172.29.6.13, 00:34:21, Serial0/1/0
O       172.29.6.0 [110/128] via 172.29.6.13, 00:34:21, Serial0/1/0
                   [110/128] via 172.29.6.5, 00:34:21, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 172.29.6.13, 00:34:21, Serial0/1/0
O       209.17.220.4 [110/192] via 172.29.6.13, 00:34:21, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:24:06, Serial0/1/0
```

Figura 37 Verificación Balanceo de Carga Medellin3

```
Bogota1#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.12 [110/128] via 172.29.3.6, 00:35:18, Serial0/1/0
                    [110/128] via 172.29.3.10, 00:35:18, Serial0/1/1
O       172.29.6.0 [110/192] via 209.17.220.5, 00:35:18, Serial0/0/0
O       172.29.6.4 [110/256] via 209.17.220.5, 00:35:18, Serial0/0/0
O       172.29.6.8 [110/192] via 209.17.220.5, 00:35:18, Serial0/0/0
O       172.29.6.12 [110/192] via 209.17.220.5, 00:35:18, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/128] via 209.17.220.5, 00:35:18, Serial0/0/0
```

Figura 38 Verificación Balanceo de Carga Bogota1

```
Bogota2#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.0 [110/128] via 172.29.3.9, 00:36:01, Serial0/0/0
                   [110/128] via 172.29.3.14, 00:36:01, Serial0/0/1
O       172.29.3.4 [110/128] via 172.29.3.9, 00:36:01, Serial0/0/0
                   [110/128] via 172.29.3.14, 00:36:01, Serial0/0/1
O       172.29.6.0 [110/256] via 172.29.3.9, 00:36:01, Serial0/0/0
O       172.29.6.4 [110/320] via 172.29.3.9, 00:36:01, Serial0/0/0
O       172.29.6.8 [110/256] via 172.29.3.9, 00:36:01, Serial0/0/0
O       172.29.6.12 [110/256] via 172.29.3.9, 00:36:01, Serial0/0/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/192] via 172.29.3.9, 00:36:01, Serial0/0/0
O       209.17.220.4 [110/128] via 172.29.3.9, 00:36:01, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:25:46, Serial0/0/0
```

Figura 39 Verificación Balanceo de Carga Bogota2

```
Bogota3#show ip route ospf
     172.29.0.0/30 is subnetted, 8 subnets
O       172.29.3.8 [110/128] via 172.29.3.13, 00:36:36, Serial0/0/0
                   [110/128] via 172.29.3.1, 00:36:36, Serial0/1/0
O       172.29.6.0 [110/256] via 172.29.3.1, 00:36:36, Serial0/1/0
O       172.29.6.4 [110/320] via 172.29.3.1, 00:36:36, Serial0/1/0
O       172.29.6.8 [110/256] via 172.29.3.1, 00:36:36, Serial0/1/0
O       172.29.6.12 [110/256] via 172.29.3.1, 00:36:36, Serial0/1/0
     209.17.220.0/30 is subnetted, 2 subnets
O       209.17.220.0 [110/192] via 172.29.3.1, 00:36:36, Serial0/1/0
O       209.17.220.4 [110/128] via 172.29.3.1, 00:36:36, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:26:21, Serial0/1/0
```

Figura 40 Verificación Balanceo de Carga Bogota3

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

Para los puntos c, d, e, f se realizaron las comprobaciones mediante observación de las tablas de enrutamiento que se muestran en las Figuras 27, 28, 29, 30, 31,32 y 33. Allí se pueden observar las rutas en cada uno de los dispositivos.

3.2.4 Deshabilitar la propagación del protocolo OSPF

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

Tabla 27 Interfaces de routers que no necesitan activacion

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

Para deshabilitar la propagación del protocolo OSPF se utiliza la siguiente línea de comandos, tan solo necesaria en los routers Medellin 3 y Bogota 3:

Medellin3(config)#router ospf 1

Medellin3(config-router)#pas

Medellin3(config-router)#passive-interface s0/1/1

Medellin3(config-router)#exit

Medellin3(config)#

Bogota3(config)#router ospf 1

Bogota3(config-router)#pas

Bogota3(config-router)#passive-interface s0/1/1

Bogota3(config-router)#exit

Bogota3(config)#

3.2.5 Verificación del protocolo OSPF

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

A continuación se observa la verificación mediante el comando show ip protocols en cada uno de los routers:

```
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 1
    209.17.220.4 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:19:20
    172.29.3.14          110      00:19:21
    172.29.6.5           110      00:19:20
    172.29.6.14          110      00:19:20
    209.17.220.1         110      00:08:52
    209.17.220.5         110      00:19:21
    209.17.220.6         110      00:08:19
  Distance: (default is 110)
```

Figura 41 Verificación Protocolo OSPF en 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 209.17.220.1
  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 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
    209.17.220.0 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:21:10
    172.29.3.14          110      00:21:11
    172.29.6.5           110      00:21:09
    172.29.6.14          110      00:21:10
    209.17.220.1         110      00:10:41
    209.17.220.5         110      00:21:11
    209.17.220.6         110      00:10:09
  Distance: (default is 110)
```

Figura 42Verificación Protocolo OSPF en 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:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.0 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:21:57
    172.29.3.14          110      00:21:58
    172.29.6.5           110      00:21:56
    172.29.6.14          110      00:21:57
    209.17.220.1         110      00:11:28
    209.17.220.5         110      00:21:58
    209.17.220.6         110      00:10:55
  Distance: (default is 110)
```

Figura 43 Verificación Protocolo OSPF 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:
    172.29.6.4 0.0.0.3 area 1
    172.29.6.8 0.0.0.3 area 1
    172.29.6.12 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:22:57
    172.29.3.14          110      00:22:58
    172.29.6.5           110      00:22:57
    172.29.6.14          110      00:22:57
    209.17.220.1         110      00:12:29
    209.17.220.5         110      00:22:59
    209.17.220.6         110      00:11:56
  Distance: (default is 110)
```

Figura 44 Verificación Protocolo OSPF en Medellin3

```
Bogotal#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:
    209.17.220.4 0.0.0.3 area 1
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:23:36
    172.29.3.14          110      00:23:37
    172.29.6.5           110      00:23:36
    172.29.6.14          110      00:23:36
    209.17.220.1         110      00:13:08
    209.17.220.5         110      00:23:38
    209.17.220.6         110      00:12:35
  Distance: (default is 110)
```

Figura 45 Verificación Protocolo OSPF en 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 172.29.3.13
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.8 0.0.0.3 area 1
    172.29.3.12 0.0.0.3 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:24:09
    172.29.3.14          110      00:24:10
    172.29.6.5           110      00:24:09
    172.29.6.14          110      00:24:09
    209.17.220.1         110      00:13:41
    209.17.220.5         110      00:24:11
    209.17.220.6         110      00:13:09
  Distance: (default is 110)
```

Figura 46 Verificación Protocolo OSPF en 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 172.29.3.14
  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 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.12 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/1/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13          110      00:24:40
    172.29.3.14          110      00:24:41
    172.29.6.5           110      00:24:40
    172.29.6.14          110      00:24:40
    209.17.220.1         110      00:14:12
    209.17.220.5         110      00:24:42
    209.17.220.6         110      00:13:40
  Distance: (default is 110)
```

Figura 47 Verificación Protocolo OSPF en Bogota3

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.

Se utiliza el comando show ip ospf database para obtener la información solicitada en cada router:

```
ISP#show ip ospf database
            OSPF Router with ID (209.17.220.5) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
209.17.220.5    209.17.220.5    1559        0x80000006 0x009c72 4
172.29.3.14     172.29.3.14     1559        0x80000008 0x002e4f 6
172.29.6.14     172.29.6.14     1558        0x80000008 0x00c1a2 6
172.29.3.13     172.29.3.13     1558        0x80000006 0x00a5d0 4
172.29.6.5      172.29.6.5      1558        0x80000006 0x00573f 4
209.17.220.1    209.17.220.1    930         0x8000000b 0x002267 8
209.17.220.6    209.17.220.6    897         0x8000000b 0x006930 8

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    930         0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    897         0x80000002 0x000408 1
```

Figura 48 Base de datos OSPF en ISP

```
Medellin1#show ip ospf database
            OSPF Router with ID (209.17.220.1) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
209.17.220.1    209.17.220.1    1073        0x8000000b 0x002267 8
209.17.220.5    209.17.220.5    1703        0x80000006 0x009c72 4
172.29.3.14     172.29.3.14     1703        0x80000008 0x002e4f 6
172.29.6.14     172.29.6.14     1702        0x80000008 0x00c1a2 6
172.29.3.13     172.29.3.13     1702        0x80000006 0x00a5d0 4
172.29.6.5      172.29.6.5      1701        0x80000006 0x00573f 4
209.17.220.6    209.17.220.6    1041        0x8000000b 0x006930 8

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    1073        0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    1041        0x80000002 0x000408 1
```

Figura 49 Base de datos OSPF en Medellin1

```
Medellin2#show ip ospf database
            OSPF Router with ID (172.29.6.5) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.6.5      172.29.6.5      1732        0x80000006 0x00573f 4
209.17.220.5    209.17.220.5    1734        0x80000006 0x009c72 4
172.29.3.14     172.29.3.14     1734        0x80000008 0x002e4f 6
172.29.6.14     172.29.6.14     1733        0x80000008 0x00c1a2 6
172.29.3.13     172.29.3.13     1733        0x80000006 0x00a5d0 4
209.17.220.1    209.17.220.1    1104        0x8000000b 0x002267 8
209.17.220.6    209.17.220.6    1071        0x8000000b 0x006930 8

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    1104        0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    1071        0x80000002 0x000408 1
```

Figura 50 Base de datos OSPF en Medellin2

```
Medellin3#show ip ospf database
            OSPF Router with ID (172.29.6.14) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.6.14     172.29.6.14     1759        0x80000008 0x00c1a2 6
209.17.220.5    209.17.220.5    1761        0x80000006 0x009c72 4
172.29.3.14     172.29.3.14     1760        0x80000008 0x002e4f 6
172.29.3.13     172.29.3.13     1759        0x80000006 0x00a5d0 4
172.29.6.5      172.29.6.5      1759        0x80000006 0x00573f 4
209.17.220.1    209.17.220.1    1131        0x8000000b 0x002267 8
209.17.220.6    209.17.220.6    1098        0x8000000b 0x006930 8

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    1131        0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    1098        0x80000002 0x000408 1
```

Figura 51 Base de datos OSPF en Medellin3

```
Bogota1#show ip ospf database
            OSPF Router with ID (209.17.220.6) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
209.17.220.6    209.17.220.6    1125        0x8000000b 0x006930 8
209.17.220.5    209.17.220.5    1788        0x80000006 0x009c72 4
172.29.3.14     172.29.3.14     1787        0x80000008 0x002e4f 6
172.29.3.13     172.29.3.13     1786        0x80000006 0x00a5d0 4
172.29.6.14     172.29.6.14     1786        0x80000008 0x00cla2 6
172.29.6.5      172.29.6.5      1786        0x80000006 0x00573f 4
209.17.220.1    209.17.220.1    1158        0x8000000b 0x002267 8

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.6    1125        0x80000002 0x000408 1
0.0.0.0         209.17.220.1    1158        0x80000002 0x0022ee 1
```

Figura 52 Base de datos OSPF en Bogota1

```
Bogota2#show ip ospf database
            OSPF Router with ID (172.29.3.13) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.3.13     172.29.3.13     10          0x80000007 0x00a3dl 4
209.17.220.1    209.17.220.1    1183        0x8000000b 0x002267 8
209.17.220.6    209.17.220.6    1151        0x8000000b 0x006930 8
209.17.220.5    209.17.220.5    13          0x80000007 0x009a73 4
172.29.3.14     172.29.3.14     12          0x80000009 0x002c50 6
172.29.6.5      172.29.6.5      11          0x80000007 0x005540 4
172.29.6.14     172.29.6.14     11          0x80000009 0x00bfa3 6

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    1183        0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    1151        0x80000002 0x000408 1
```

Figura 53 Base de datos OSPF en Bogota2

```
Bogota3#show ip ospf database
            OSPF Router with ID (172.29.3.14) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
172.29.3.14     172.29.3.14     37          0x80000009 0x002c50 6
209.17.220.1    209.17.220.1    1209        0x8000000b 0x002267 8
209.17.220.6    209.17.220.6    1177        0x8000000b 0x006930 8
209.17.220.5    209.17.220.5    38          0x80000007 0x009a73 4
172.29.6.5      172.29.6.5      36          0x80000007 0x005540 4
172.29.6.14     172.29.6.14     36          0x80000009 0x00bfa3 6
172.29.3.13     172.29.3.13     36          0x80000007 0x00a3d1 4

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         209.17.220.1    1209        0x80000002 0x0022ee 1
0.0.0.0         209.17.220.6    1177        0x80000002 0x000408 1
```

Figura 54 Base de datos OSPF en Bogota3

3.2.6 Configurar encapsulamiento y autenticación PPP.

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

Se realiza la siguiente configuración por línea de comandos en cada uno de los dispositivos:

```
ISP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#username Medellin1 pass cisco
ISP(config)#int s0/0/1
ISP(config-if)#enca
ISP(config-if)#encapsulation PPP
ISP(config-if)#PPP authentication pap
ISP(config-if)#ppp pap sent-username ISP pass cisco
ISP(config-if)#exit
ISP(config)#

Medellin1#config t
Medellin1(config)#username ISP pass cisco
Enter configuration commands, one per line.  End with CNTL/Z.
Medellin1(config)#int s0/1/0
Medellin1(config-if)#encapsulation PPP
Medellin1(config-if)#PPP authentication pap
Medellin1(config-if)#ppp pap sent-username Medellin1 pass cisco
Medellin1(config-if)#
```

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

Se realiza la siguiente configuración en cada uno de los dispositivos:

```
ISP(config)#username Bogota1 pass cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation PPP
ISP(config-if)#ppp authentication chap
ISP(config-if)#ppp pap sent-username ISP pass cisco
ISP(config-if)#exit
ISP(config)#

Bogota1(config)#username ISP pass cisco
Bogota1(config)#interface Serial0/0/0
Bogota1(config-if)#encapsulation PPP
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#ppp pap sent-username Bogota1 pass cisco
Bogota1(config-if)#exit
Bogota1(config)#
```

3.2.7 Configuración de PAT

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

Se realiza la siguiente configuración en el router Medellin1:

```
Medellin1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Medellin1(config)#ip ac
Medellin1(config)#ip access-list standard host
Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
Medellin1(config-std-nacl)#exit
Medellin1(config)#ip nat inside source list host interface s0/0/0 overload
Medellin1(config)#int s0/0/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#int s0/0/1
```

```
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#int s0/1/0
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#int s0/1/1
Medellin1(config-if)#ip nat outside
Medellin1(config-if)#
```

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

Se ingresan los siguientes comandos para la configuración de NAT en el router Bogotá 1:

```
Bogota1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota1(config)#ip acc
Bogota1(config)#ip access-list standard host
Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
Bogota1(config-std-nacl)#exit
Bogota1(config)#ip nat inside source list host interface serial 0/0/0 overload
Bogota1(config)#int s0/0/0
Bogota1(config-if)#ip nat inside
Bogota1(config-if)#int s0/0/1
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int s0/1/0
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#int s0/1/1
Bogota1(config-if)#ip nat outside
Bogota1(config-if)#exit
Bogota1(config)#
```

3.2.8 Configuración del servicio DHCP

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

Se realiza la siguiente configuración de los pool de DHCP para Medellin 2.

```
Medellin2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Medellin2(config)#ip dhcp excluded-address 172.29.4.1
```

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.129
Medellin2(config)#ip dhcp pool Medellin2
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
Medellin2(dhcp-config)#de
Medellin2(dhcp-config)#default-router 172.29.4.1
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)#def
Medellin2(dhcp-config)#default-router 172.29.4.129
Medellin2(dhcp-config)#
```

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

De acuerdo con esto, se utiliza la siguiente configuración para habilitar el paso de mensajes broadcast:

```
Medellin3(config)#int fa0/0
Medellin3(config-if)#ip helper-address 172.29.6.5
Medellin3(config-if)#
```

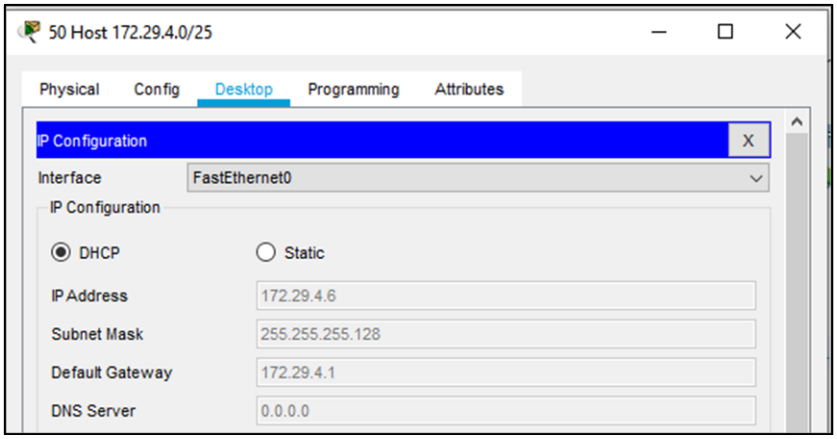

Figura 55 Verificación DHCP Medellin

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

A continuación se observa la configuración de pool de DHCP en router Bogota2:

```
Bogota2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota2(config)#ip dhcp pool Bogota2
```

```
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota2(dhcp-config)#de
Bogota2(dhcp-config)#default-router 172.29.1.1
Bogota2(dhcp-config)#ip dhcp pool Bogota3
Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota2(dhcp-config)#default-router 172.29.0.1
Bogota2(dhcp-config)#exit
Bogota2(config)#ip dhcp ex
Bogota2(config)#ip dhcp excluded-address 172.29.1.1
Bogota2(config)#ip dhcp excluded-address 172.29.0.1
Bogota2(config)#
```

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

De acuerdo con esto, se utiliza la siguiente configuración para habilitar el paso de mensajes broadcast:

```
Bogota3(config)#int fa0/0
Bogota3(config-if)#ip helper-address 172.29.3.13
Bogota3(config-if)#end
```

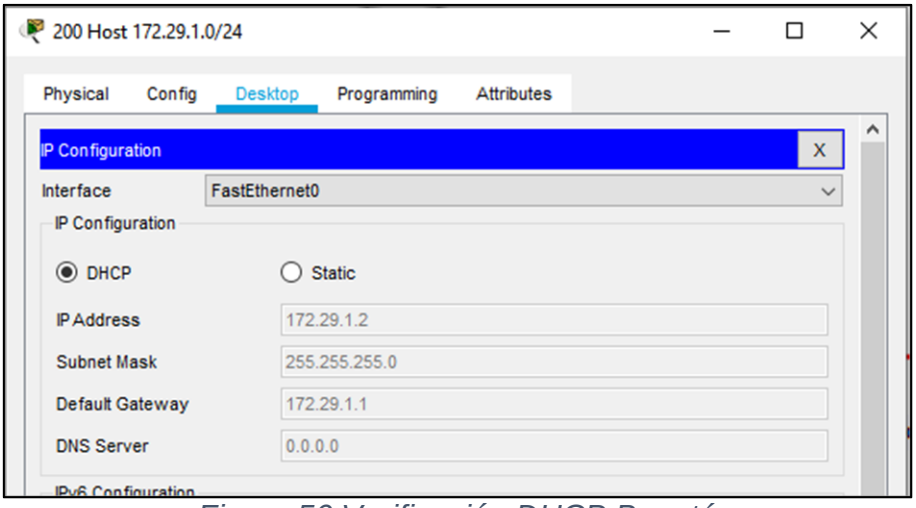

Figura 56 Verificación DHCP Bogotá

CONCLUSIONES

- Las listas de acceso son creadas para establecer filtros en el tráfico de la red, estas utilizan una numeración de identificación, siendo del 1 al 99 ACL de tipo estándar, mientras que del 100 al 100 son extenddidas. Las ACL se encargan de controlar si los paquetes ruteados se reenvían o bloquean la interfaz en el router, sus criterios incluyen dirección de origen de tráfico, dirección de destino de tráfico y protocolo de capa superior.

- A medida que aumenta el número de equipos de red conectados a Internet se presenta un agotamiento de direcciones IP, debido a ello surgió NAT o traducción de direcciones de red, utilizado para que redes de ordenadores utilicen un rango de direcciones especiales (privadas) para conectarse a Internet mediante una sola dirección ip pública, así cada vez que el host requiere conexión a Internet se le asigna una dirección pública que no esté siendo utilizada, para ello se aumenta la seguridad de la red al hacerle más diíficil a hosts externos ingresar a una red determinada pues las ip públicas no son la misma siempre.

- Una de las principales ventajas que ofrece la activación del protocolo de configuración dinámica de host, DHCP, se centra en la facilidad de la administración de direcciones ip en una red, pues se evita la asignación manual de cada dispositivo y al cambiar de red sería necesario volver a configurar, en cambio habilitando el DHCP al conectarse automáticamente a la red se le asigna una dirección dentro del rango disponible asignado.

- Routing Information Protocol versión 2 (RIPv2) es uno de los protocolos de enrutamiento interior más sencillos y utilizados. Introduce algunas mejoras críticas que la constituyeron en un recurso necesario para cualquier administrador de redes. Es de tipo vector distancia, su principal limitante está impuesta por la cantidad máxima de saltos que soporta que son 15. Sus principales mejoras incluyen: soporte para VLSM, actualizaciones de enrutamiento por multicast y actualizaciones con autenticación con clave encriptada.

BIBLIOGRAFÍA

GUÍA DE DISEÑO DE OSPF. 2005. [En línea] [Consultado el 05 de mayo de 2020]. Disponible en : https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

PREGUNTAS FRECUENTES SOBRE LA TRADUCCIÓN DE DIRECCIONES DE RED (NAT) 2014[En línea] [Consultado el 05 de mayo de 2020]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

PROTOCOLOS RIP/OSPF/BGP .s.f. [En línea] [Consultado el 05 de mayo de 2020] Disponible en : http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

QUÉ ES DHCP Y CÓMO FUNCIONA.2018[En línea] [Consultado el 05 de mayo de 2020] .Disponible en https://www.networkworld.es/telecomunicaciones/que-es-dhcp-y-como-funciona

CONFIGURACIÓN DE RUTAS ESTÁTICAS Y PREDETERMINADAS s.f. [En línea] [Consultado el 05 de mayo de 2020] Disponible en https://ccnadesdecero.es/configuracion-rutas-estaticas-predeterminadas/

ANEXOS

Anexo 1 Configuración de dispositivos Escenario 1

Configuración R1

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service pas
R1(config)#service password-encryption
R1(config)#banner motd "Se prohibe el acceso no autorizado"
R1(config)#int s0/0/0
R1(config-if)#description Conectado a R2
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 add 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
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
R1(config)#
```

Configuración R2

```
R2>ena
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
```

```
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd "Se prohibe el acceso no autorizado"
R2(config)#int s0/0/0
R2(config-if)#description Conectado a R1
R2(config-if)#ip add 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 add 2001:DB8:ACAD:1::2/64
R2(config-if)#no shu
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#description Conectado a R3
R2(config-if)#ip add 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shu
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#int g0/0
R2(config-if)#description Conectado a Servidor de Internet
R2(config-if)#ip add 209.165.200.237 255.255.255.248
R2(config-if)#Ipv6 add 2001:DB8:ACAD:A::/64
R2(config-if)#no shu
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#int lo0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#description Conectado a Lo0
R2(config-if)#ip add 10.10.10.10 255.255.255.252
R2(config-if)#exit
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
R2(config)#end
R2#
```

%SYS-5-CONFIG_I: Configured from console by console
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

Configuración R3

```
Router>ena
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd "Se prohibe el acceso no autorizado"
R3(config)#int s0/0/1
R3(config-if)#description Conectado a R2
R3(config-if)#ip add 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64
R3(config-if)#no shu
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R3(config-if)#int lo=
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
R3(config-if)#int Lo4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state
to up

R3(config-if)#Ip add 192.168.4.1 255.255.255.0
R3(config-if)#int Lo5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state
to up
```

```
R3(config-if)#Ip add 192.168.5.1 255.255.255.0
R3(config-if)#int Lo6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#Ip add 192.168.6.1 255.255.255.0
R3(config-if)#int Lo7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#Ipv6 add 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
R3(config)#
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

Configuración S1

```
Switch>ena
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config)#service password-encryption
S1(config)#banner motd "Se prohibe el acceso no autorizado"
```

Configuración S3

```
Switch>ena
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd "Se prohibe el acceso no autorizado"
S3(config)#
```

Configuración Seguridad y VLAN en S1

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#
S1(config-vlan)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip add 192.168.99.2
% Incomplete command.
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no shu
S1(config-if)#exit
S1(config)#ip def
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int fa0/3
S1(config-if)#switc
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)#s
S1(config-if)#switch
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int fa0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface range fa0/1-2,fa0/7-24,fa0/4
S1(config-if-range)#switch
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#int fa0/6
S1(config-if)#switchport mode access
S1(config-if)#swit
S1(config-if)#switchport access vlan 21
S1(config-if)#interface range fa0/1-2,fa0/7-24,fa0/4
S1(config-if-range)#shu

Configuración Seguridad y VLAN en S3

S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
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)#Interface vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no shu
S3(config-if)#
S3(config-if)#exit
S3(config)#Ip default-gateway 192.168.99.1
S3(config)#int fa0/3
S3(config-if)#switch
S3(config-if)#switchport mode trunk

```
S3(config-if)#swtuc
S3(config-if)#swt
S3(config-if)#swit
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#interface range fa0/1-2,fa0/4-7,fa0/19-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#int fa0/18
S3(config-if)#sw
S3(config-if)#switchport mode acces
S3(config-if)#swit
S3(config-if)#switchport acc vlan 23
S3(config-if)#interface range fa0/1-2,fa0/4-7,fa0/19-24
S3(config-if-range)#shut
```

Configuración Subinterfaces R1

```
R1(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encaps
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip add 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no shutdown
```

Configuración RIPv2 en R1

```
R1(config-router)#version 2
R1(config)#router rip
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.99.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#pas
R1(config-router)#passive-interface g0/0
R1(config-router)#passive-interface g0/1
R1(config-router)#no aut
R1(config-router)#no auto-summary
R1(config-router)#
```

Configuración RIPv2 en R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#network 10.10.10.10
R2(config-router)#pas
R2(config-router)#passive-interface lo0
R2(config-router)#no aut
R2(config-router)#no auto-summary
R2(config-router)#end
```

Configuración RIPv2 en R3

```
R3(config)#router rip
R3(config-router)#version 2
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
R3(config-router)#pas
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#passive-interface lo7
R3(config-router)#no au
R3(config-router)#no auto-summary
R3(config-router)#
```

Configuración DHCP y NAT en R1

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#def
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#
```

Configuración NAT estática y dinámica en R2

```
R2(config)#aaa new-model
R2(config)#aaa authentication login default local
R2(config)#username webuser privilege 15 pass cisco12345
R2(config)#aaa authorization network default local
R2(config)#
R2(config)#ip nat inside source static 209.165.200.238 209.165.200.229
R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat outside
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
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)#ip nat inside source list 1 pool nat overload
```