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

WILLIAM VARGAS ARDILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA D.C.
2020

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

WILLIAM VARGAS ARDILA

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLMENTACION DE SOLUCIONES INTEGRADAS LAN / WAN))

DOCENTE

ING. JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA D.C.

2020

TABLA DE CONTENIDO

Pag.

LISTA DE FIGURAS

INTRODUCCIÓN

En el siguiente trabajo pretendemos desarrollar actividades practicas a través de 2 caso estudio propuestos con el fin de demostrar las habilidades y competencias adquiridas a lo largo del desarrollo del diplomado de profundización de cisco en el diseño e implementación de soluciones integradas LAN / WAN. Para el desarrollo practico de estas actividades nuestro recurso principal a usar es packet tracer (programa de simulación de redes) en el cual centralizaremos el montaje de las topologías de red del escenario 1 y 2 y la configuración de cada uno de los dispositivos de red, en el escenario número uno configuraremos una red pequeña la cual debe admitir conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, aplicaremos el protocolo de routing dinámico (RIPv2), el protocolo de host dinámicos DHCP, la traducción de direcciones de red dinámicas y estáticas (NAT), aplicaremos listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) todo esto documentado dentro del ejercicio práctico en cada una de las configuraciones de estos servicios.

En el desarrollo del escenario número 2 en nuestro rol de administradores de red debemos configurar e interconectar una red WAN / LAN distribuida en 2 sucursales en las ciudades de Medellín y Bogotá, para ello tendremos que tener en cuenta los lineamientos de direccionamiento IP, los protocolos de enrutamiento en este caso se aplicara el protocolo OSPF (Open Shortest Path First) el cual es un poco más inteligente al ayudarnos a determinar la vía las rápida o más corta para él envió de paquetes, de igual manera tendremos que habilitar el encapsulamiento PPP y su autenticación, dentro de cada red LAN tanto en Bogotá y Medellín, habilitaremos en un router que brindara el servicio DHCP a su propia red LAN y a los demás routers de cada ciudad, además aplicaremos PPP en los enlaces hacia el router ISP con su respectiva autenticación con el fin de garantizar un enlace seguro para la transmisión de los datos y por ultimo habilitaremos el servicio de NAT por sobrecarga o PAT en los routers Bogota 1 y Medellin 1 que están conectados al Router ISP.

RESUMEN

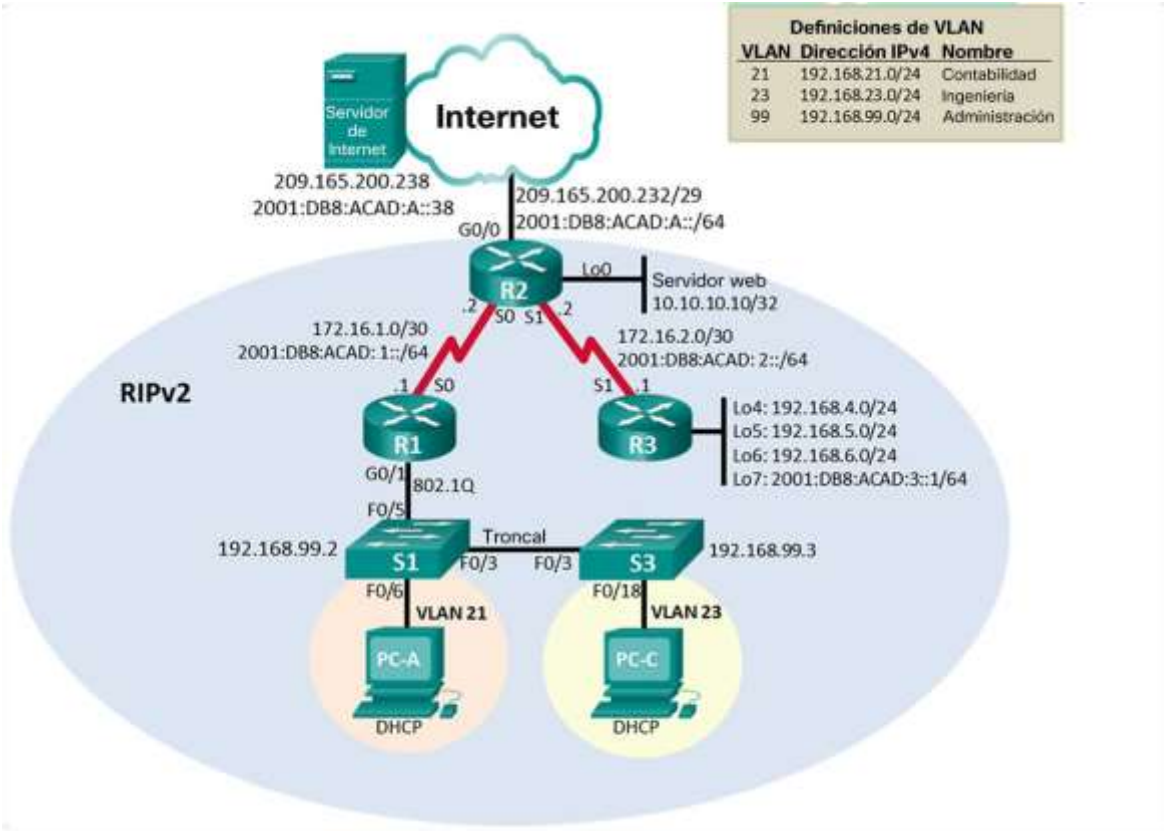
Solución practica de dos estudios de caso bajo el uso de tecnología cisco, se compone de una prueba de habilidades basados en la adquisición de conocimiento y competencias de la tecnologia de CISCO, con sus respectivos procesos de documentación, configuración y descripcion de la metodología utilizada para dar solucion a los escenarios planteados. con el fin de evidenciar la aplicación de los conocimientos adquiridos en el diplomado de profundizacion de cisco.

Palabras Clave:

CCNA, Escenarios, Telecomunicaciones, Redes.

ESCENARIO 1

Figura 1 Topología de red escenario 1



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

PARTE 1 INICIALIZAR DISPOSITIVOS

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos

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

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload

	System configuration has been modified. Save? [yes/no]:y
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# Switch#show flash No se evidencia ningun archivo vlan.dat en los switch.

Análisis y/o resultados

- En este paso inicial logramos borrar toda la configuración inicial de los routers y switches a usar en la topología y garantizamos también la eliminación de la base de datos de VLAN en cada uno de los switches con el fin de inicializar los dispositivos desde cero para la nueva configuración de la red.

PARTE 2 CONFIGURAR LOS PARÁMETROS BÁSICOS DEL DISPOSITIVO

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):

Según el **análisis** de la topología y del direccionamiento por sus rangos en la dirección IP del Gateway predeterminado debe ser 209.165.200.233 debido a que es la primera IP en la red según el rango disponible en la topología.

Elemento o tarea de configuración	Especificación
Dirección IPv4	200.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:acad:a::3b
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:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router#show run | include domain-lookup
Nombre del router	R1 - Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password Cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1#show startup-config
Mensaje MOTD	R1(config)#banner motd #Prohibido Accesso No Autorizado#
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description "Conexion R1 - R2" R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Análisis y/ resultados:

En este paso logramos la configuración inicial del router numero 1 al realizar la desactivación de la búsqueda del servicio DNS en el router como buena practica para no tener problemas de bloqueo o lentitud del dispositivo, establecimos los parámetros de seguridad de contraseñas para el acceso al dispositivo y configuramos el direccionamiento y activamos la interfaz de conexión serial hacia el router numero 2 de la topología de red.

PASO 3 CONFIGURAR R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router#show run | include domain
Nombre del router	R2 - Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Packet tracer no soporta este comando
Mensaje MOTD	R2(config)#banner motd #Se Prohibe el Acceso No Autorizado#
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description Conexion R2 - R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#description Conexion R2 - R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

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

Análisis y resultados:
Logramos la configuración inicial del dispositivo, establecimos la seguridad de acceso además de configurar el direccionamiento de sus interfaces en este caso ya tenemos comunicación con el router 1 a través de la conexión serial y con el servidor de simulación de internet a través de la interfaz G0/0.

PASO 4 CONFIGURAR R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router#show run | include domain-lookup no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description "Interface Serial R3 - R2" R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Rutas predeterminadas	R3(config)#interface s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Análisis y resultados:
Para la configuración del router 3 logramos realizar la configuración inicial del dispositivo, además de la configuración de la interfaz serial hacia el router 2 el cual verificamos y tenemos comunicación entre R" y R3.
Además, creamos y configuramos las interfaces virtuales loopback en R3 y asignamos el direccionamiento IPV4 e PIV6 para la loopback 7.

Paso 5 configurar s1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup Switch(config)#exit Switch#show run | include domain no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Análisis y resultados:
logramos la configuración básica de S1, la desactivación de la búsqueda dns, la configuración de seguridad para el acceso al switch a traves de las contraseñas.

PASO 6 CONFIGURAR S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup Switch#show run | include domain no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Análisis y resultados:
logramos la configuración básica de S3, la desactivación de la búsqueda dns, la configuración de seguridad para el acceso al switch a través de las contraseñas.

PASO 7 VERIFICAR LA CONECTIVIDAD DE LA RED

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

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.168.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

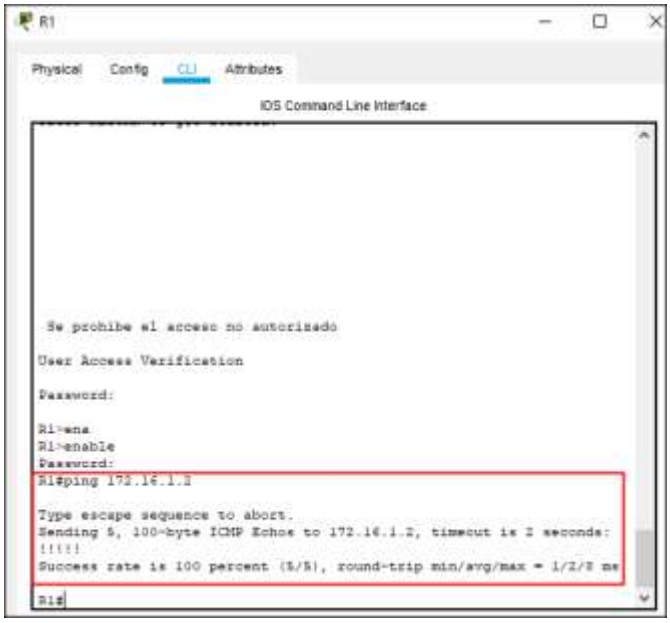
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Análisis y resultados:
En este paso como lo describimos en cada una de las configuraciones de los dispositivos anteriormente confirmamos la conectividad entre los routers 1 y 2 y el servidor de internet con el Gateway determinado. Se adjuntan las pruebas a continuación:

Evidencias de Ping

R1 – R2, S0/0/0 (172.16.1.2)

Figura 2 Evidencias de Ping R1 -R2

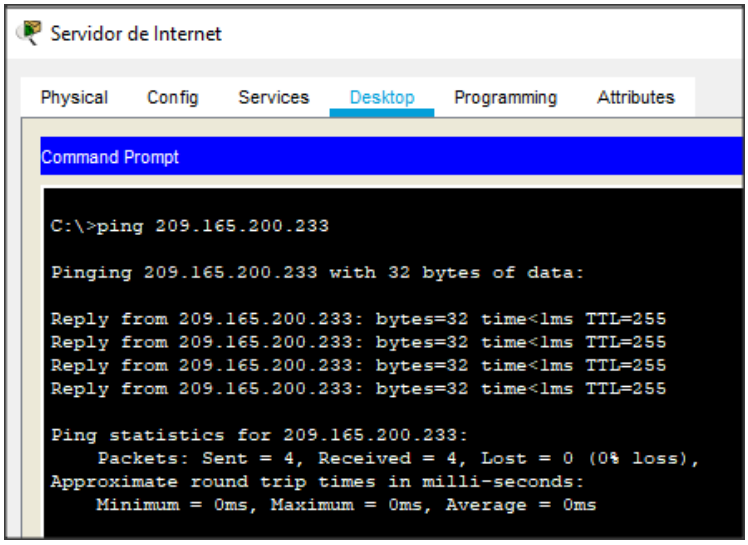


R2 – R3, S0/0/1 (172.16.2.1)

Figura 3 Evidencias de Ping R2 - R3

PC Internet – Gateway Predeterminado

Figura 4 Evidencia de Ping PC Internet - Gateway



Parte 3 configurar la seguridad del switch las vlan y el routing entre vlan

PASO 1 CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Análisis y resultados:

logramos crear cada una de las VLAN en este caso nombramos cada una de las VLAN con su descripción, asignamos la dirección IP a la VLAN de administración 192.168.99.2 y asignamos el Gateway predeterminado para esta VLAN con la dirección 192.168.99.1 como primera dirección ip de la red, configurarnos los puertos F0/3 y F0/5 como puertos o interfaces troncales para la comunicación punto a punto entre el R1 y el S3 y el trafico de las VLAN.

Los puertos adicionales se configuran como puertos de acceso, asignamos la interfaz F0/6 a la VLAN 21 que va hacia el PCA y posterior apagamos todo el rango de puertos que no se están usando.

Paso 2 configurar s3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config)#interface vlan99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Análisis y resultados:

logramos crear cada una de las VLAN en este caso nombramos cada una de las VLAN con su descripción, asignamos la dirección IP a la VLAN de administración 192.168.99.3 y asignamos el Gateway predeterminado para esta VLAN con la dirección 192.168.99.1 como primera dirección ip de la red, configurarnos el puerto F0/3 como puerto o interfaz troncal.

Los puertos adicionales se configuran como puertos de acceso, asignamos la interfaz F0/18 a la VLAN 18 que va hacia el PC-C

y posterior apagamos todo el rango de puertos que no se están usando.

PASO 3 CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

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

Análisis y resultados:

Configuramos cada una de las VLAN en la interfaz go/1 esto lo logramos aplicando el protocolo 802.1Q sobre el R1, con esto podemos usar la interfaz del router como acceso a todas las VLAN que creamos a través del puerto troncal del S1

PASO 4 VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Análisis y resultados:

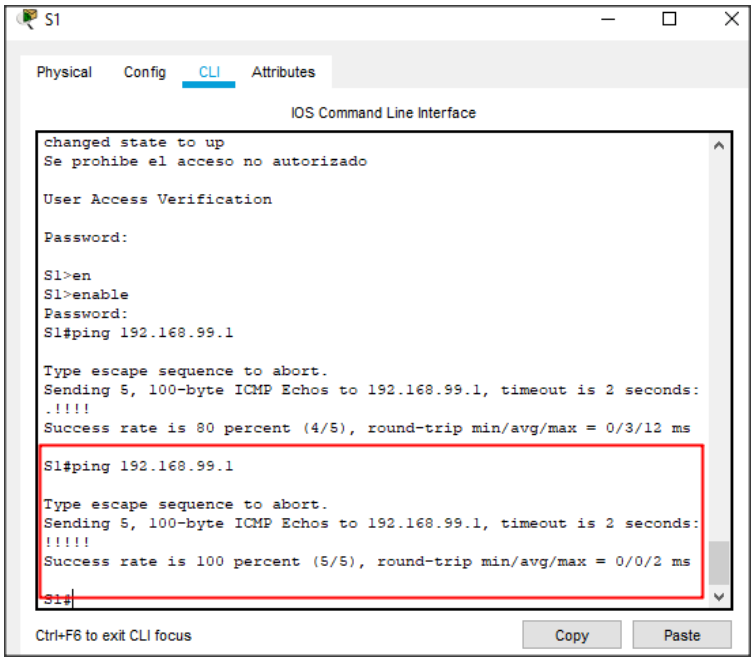
Realizamos las pruebas de comunicación de forma exitosa lo que nos garantiza que los switches se están viendo con las VLAN del router 1

A continuación, se documentan los resultados:

Evidencias de Conectividad

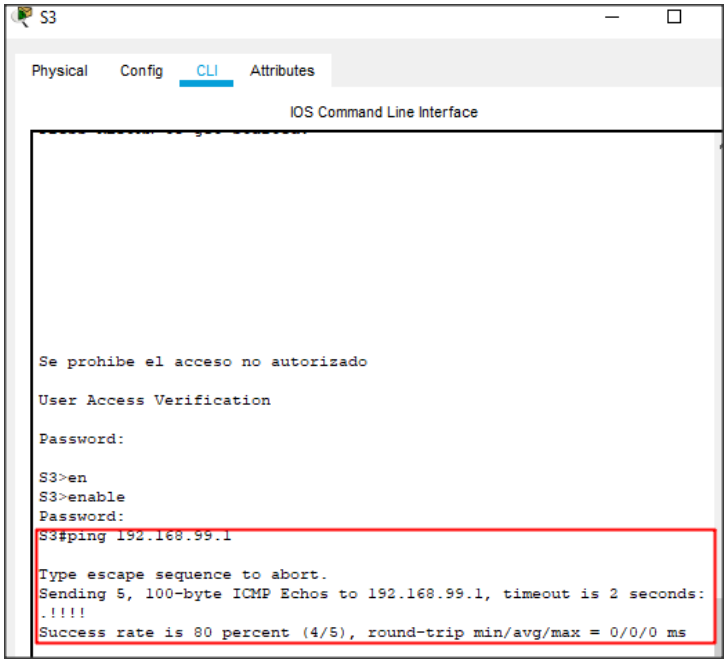
Ping S1 – R1 (Dirección VLAN 99)

Figura 5 Evidencia de Ping S1 - R1



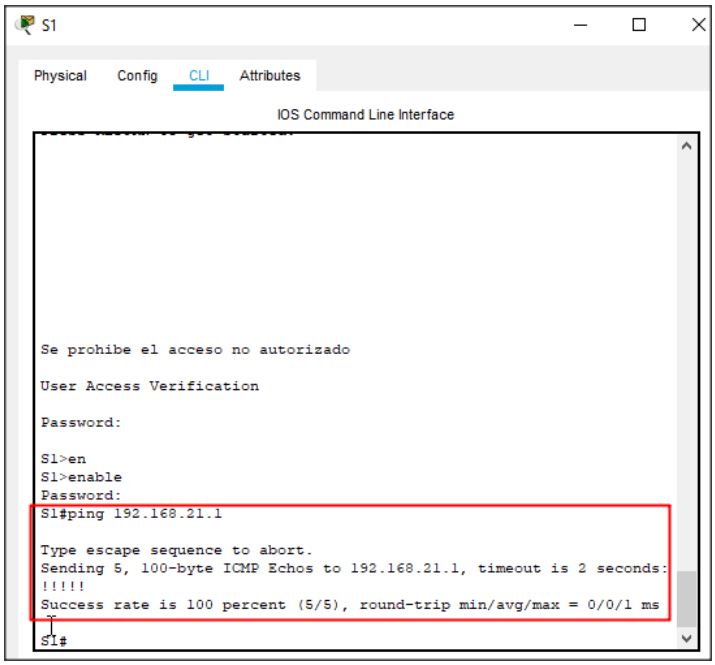
Ping S3 – R1 (Dirección VLAN 99)

Figura 6 Evidencia de Ping S3 - R1 VLAN 99



Ping S1 – R1 (Dirección VLAN 21)

Figura 7 Evidencia de Ping S1 - R1 VLAN 21



Ping S3 – R1 (Dirección VLAN 23)

Figura 8 Evidencia de Ping S3 - R1 VLAN 23

PARTE 4 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

PASO 1 CONFIGURAR RIPV2 EN EL R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 171.16.1.0 R1(config-router)#network 171.168.21.0 R1(config-router)#network 171.168.23.0 R1(config-router)#network 171.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99

Desactive la sumarización automática	R1(config-router)#no auto-summary

PASO 2 CONFIGURAR RIPV2 EN EL R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2 R2(config-router)#do show ip route connected
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

PASO 3 CONFIGURAR RIPV2 EN EL R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2 R3(config-router)#do show ip route connected
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summar

Análisis y resultados:

En este paso logramos activar el protocolo de RIPV2 en cada uno de los routers declarando cada una de sus redes directamente conectadas posterior realizamos la prueba de funcionamiento del protocolo asignando IP estáticas a los PC y confirmando comunicación o enrutamiento con cada uno de los dispositivos.

PASO 4 VERIFICAR LA INFORMACIÓN DEL RIP

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

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R3#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R3#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#show run | section router rip

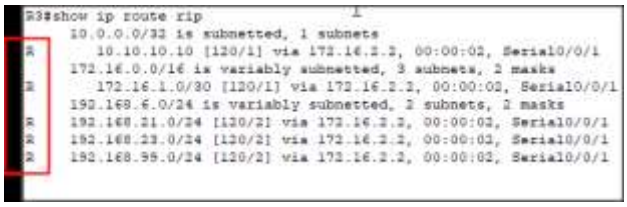
Análisis y resultados: se ejecutan cada uno de los comandos confirmando la información del protocolo configurado, las rutas de RIP

show ip protocols R3

Figura 9 Verificación de protocolo RIPV2

show ip route RIP

Figura 10 Show IP Route RIP



show run | section router rip

Figura 11 Verificación RIP R3

```
R3#show run | section router rip
router rip
 version 2
 passive-interface Loopback4
 passive-interface Loopback5
 passive-interface Loopback6
 network 172.16.0.0
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.6.0
 no auto-summary
R3#
```

PARTE 5 IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool **Cont** R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool **ENGNR** R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Análisis y resultados:

Volvemos sobre R1 y lo configuramos como servidor DHCP, realizamos la exclusión de las 20 primeras direcciones IP de cada VLAN para que no hagan parte del Pool de direcciones para asignación automática con esto posteriormente logramos la configuración del Pool de direccionamiento aplicado a las VLAN de contabilidad e ingeniería.

PASO 2 CONFIGURAR NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (PT no soporta este comando)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http server authentication local (PT no soporta este comando)
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Análisis y resultados:

Configuramos el servicio NAT para lograr navegación web hacia el servidor de internet.

PASO 3 VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTATICA

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet Tracer no soporta el comando ip http server en r2 para activar el servidor web, en el entorno real debe funcionar y solicitar la autenticación de nombre de usuario y password para ingresar.

Análisis y resultados:

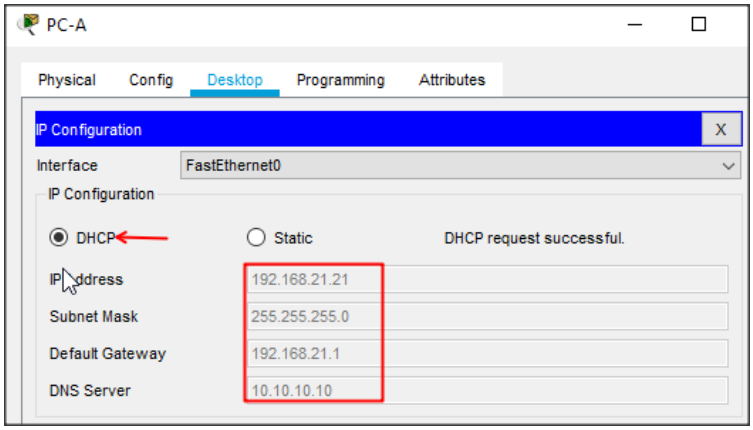
a través de la activación del servicio de DHCP en R1 realizamos las pruebas de asignación dinámica hacia los hosts de manera satisfactoria confirmando la asignación dinámica de direcciones IP.

Respecto a las pruebas de NAT y el servicio http, packet tracer no soporta el comando ip http server para activar el servidor web en un entorno real si se soporta y debe funcionar, así como solicitar la autenticación de nombre de usuario y password creadas en la base de datos en R2.

A continuación se documentan las respectivas pruebas:

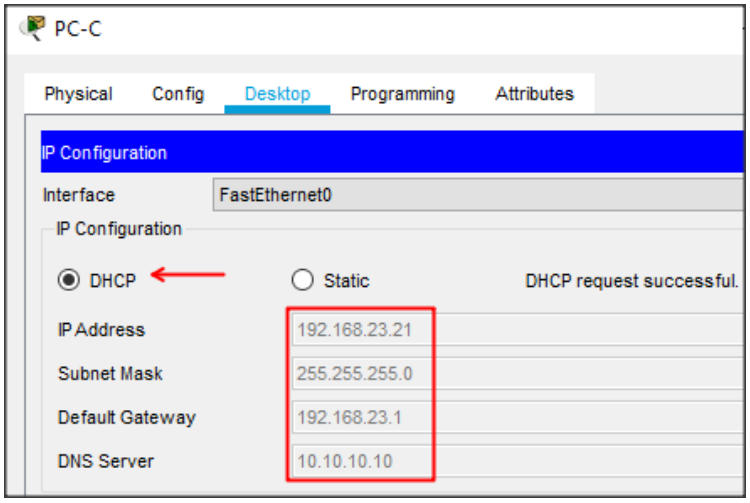
Direccionamiento DHCP PC-A

Figura 12 Verificacion DHCP PC-A



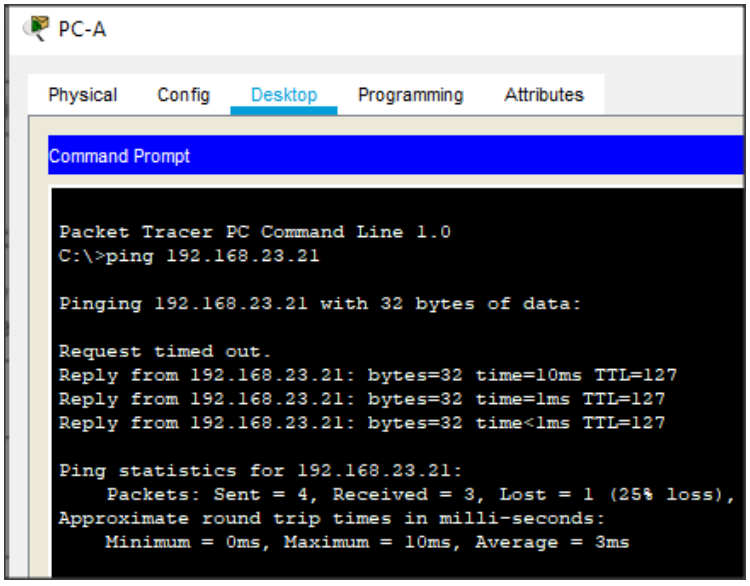
Direccionamiento DHCP PC-C

Figura 13 Verificación DHCP PC-C



verificación de ping PCA – PC-C

Figura 14 Verificación Ping PCA - PC-C



PARTE 6 CONFIGURAR NTP

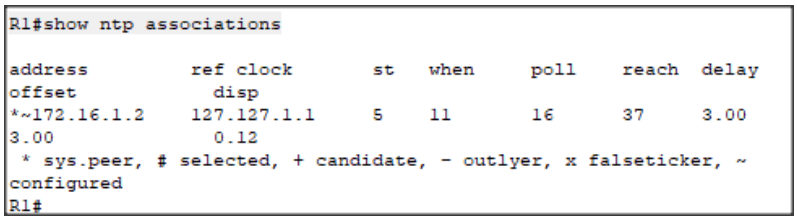
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 9:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Análisis y resultados:

Como resultado a la configuración de R2 como server principal de NPT y R1 como cliente verificamos que R1 toma la configuración cliente desde R2

NPT en R1

Figura 15 Verificación NPT R1



```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay
offset            disp
*~172.16.1.2    127.127.1.1     5    11       16      37     3.00
3.00              0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
R1#
```

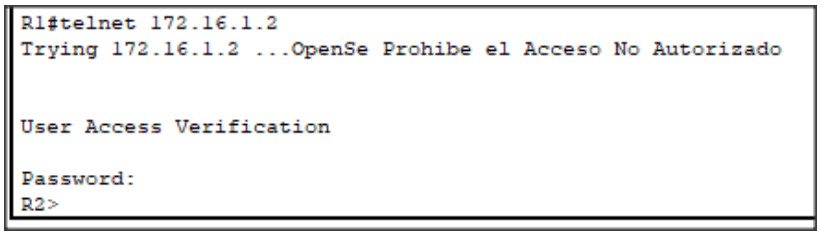
PARTE 7 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Exitoso

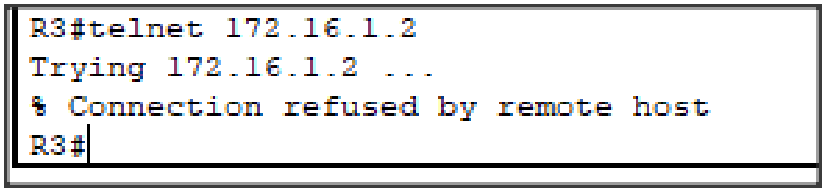
ACL R2

Figura 16 Verificación ACL R2



ACL R3

Figura 17 Verificación ACL R3



Análisis y Resultados:

Creamos la lista de acceso en R2 permitiendo la conexión del host R1 y denegamos todos los demás, además aplicamos la Access list a las líneas VTY con el fin de no permitir las conexiones entrantes por telnet hacia el dispositivo, como resultado obtenemos la conexión refutada por telnet de todos los dispositivos excepto del R1 el cual lo permitimos.

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-lists
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters (PT no soporta este comando)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translation
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

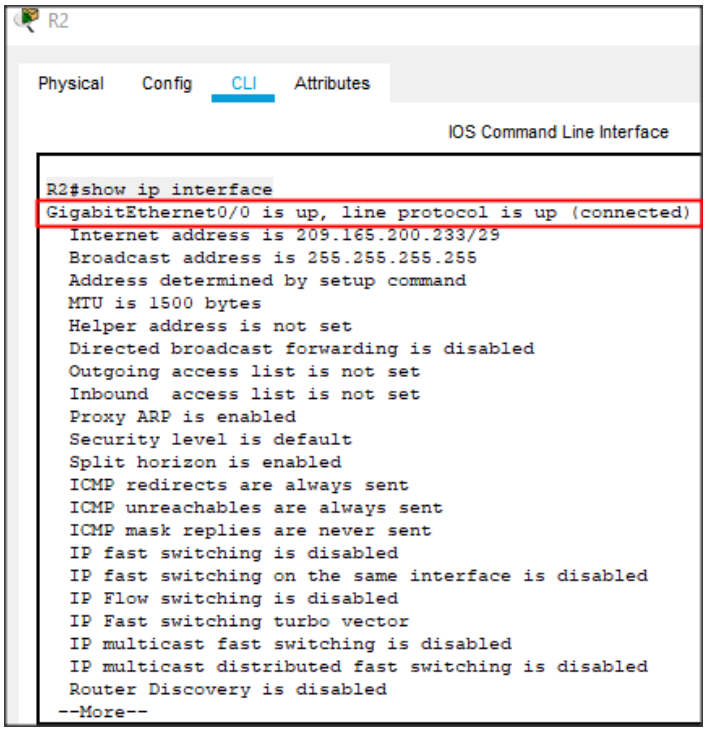
Show ip access-lists r2

Figura 18 Show IP access-list R2

```
R2#show ip access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))
```

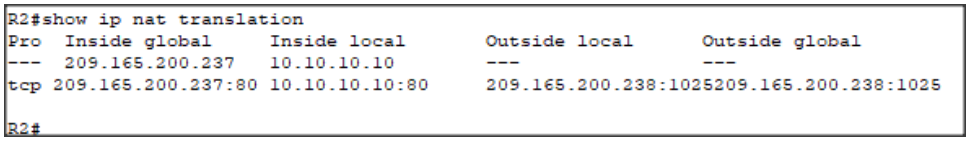
Show ip interface R2

Figura 19 Show IP Interface R2



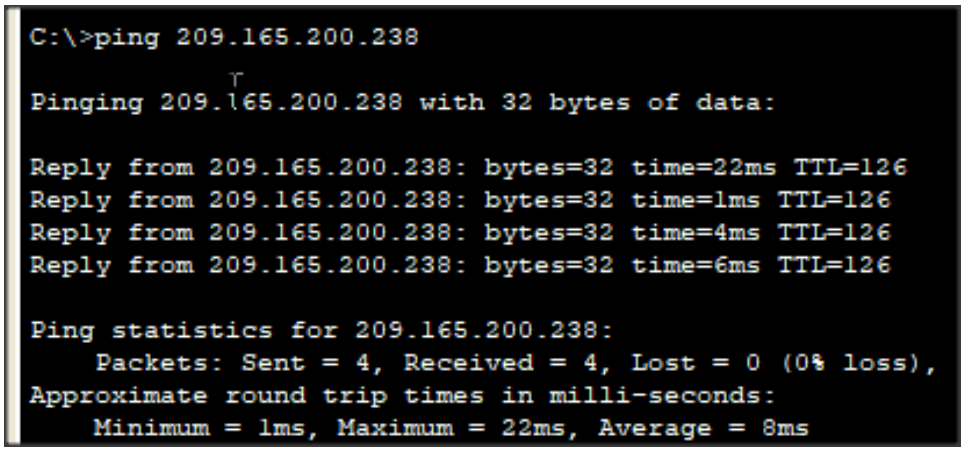
Show ip nat translation

Figura 20 Show IP Nat Translation



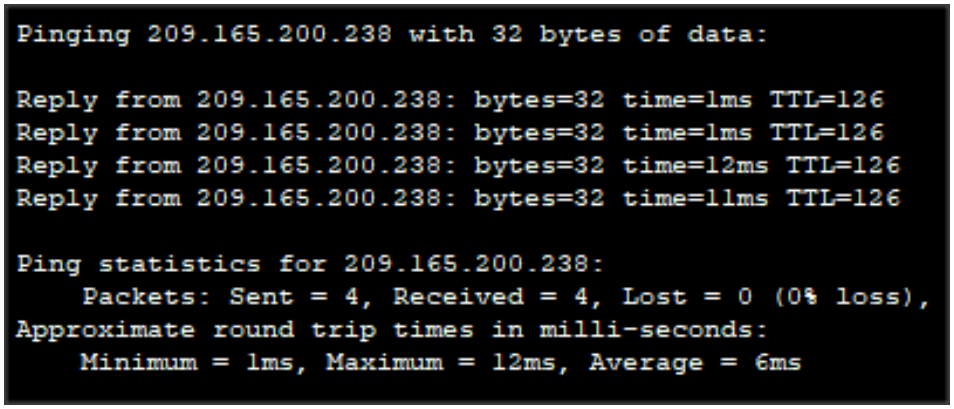
PC-A a Servidor de Internet

Figura 21 Ping PC-A - Servidor de Internet



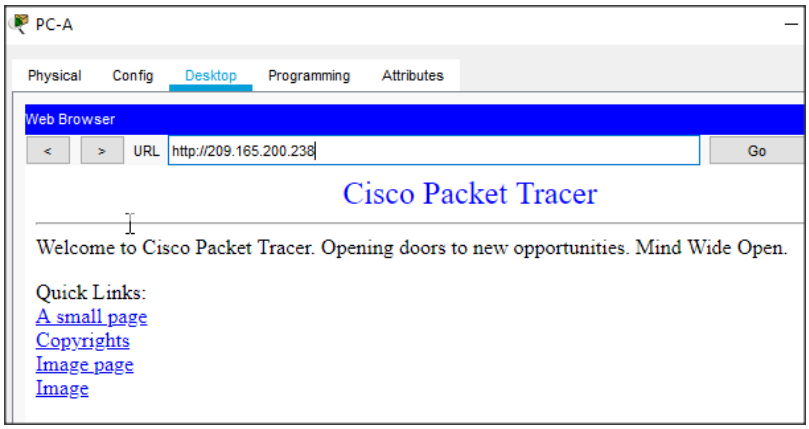
PC-C a Servidor de Internet

Figura 22 Ping PC-C - Servidor de Internet



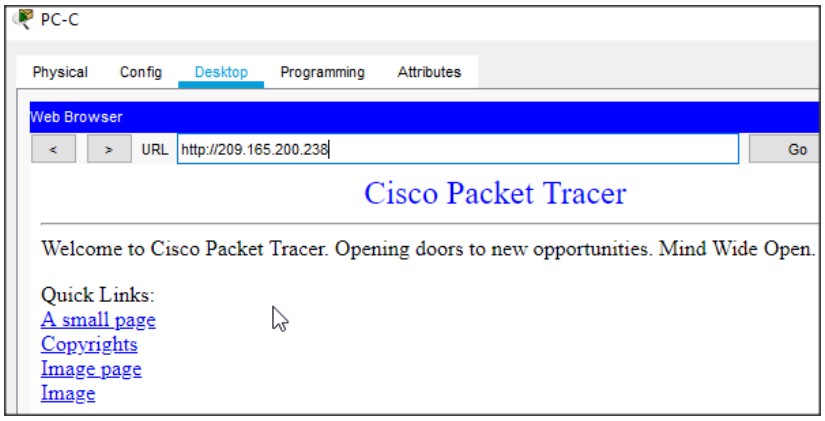
Servidor web - PC-A

Figura 23 Acceso a servidor web desde PC-A



Servidor web desde PC-C

Figura 24 Acceso a servidor web desde PC-C



Show ip translation posterior a los ping y accesos anteriores

Figura 25 Show IP Translation R2

```
R2#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.233:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1025192.168.23.21:1025 200.165.200.238:80 200.165.200.238:80
tcp 209.165.200.234:1026192.168.23.21:1026 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1025209.165.200.238:1025
```

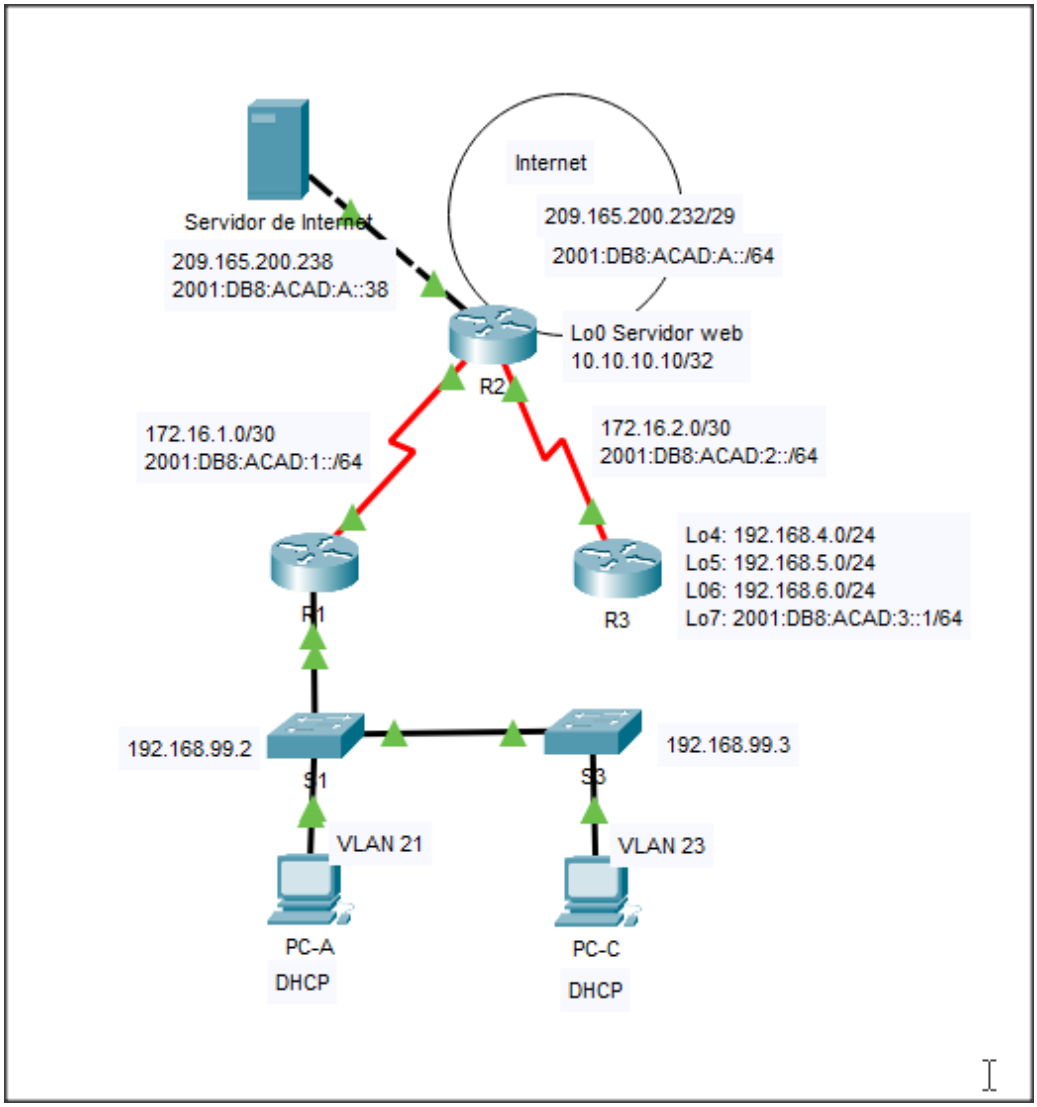
Clear ip translation R2

Figura 26 Clear IP Traslation R2

```
R2#clear ip nat translation *
R2#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
```

TOPOLOGÍA FINAL ESCENARIO 1 [PACKET TRACER]

Figura 27 Topología Final Escenario 1 [William Vargas A]



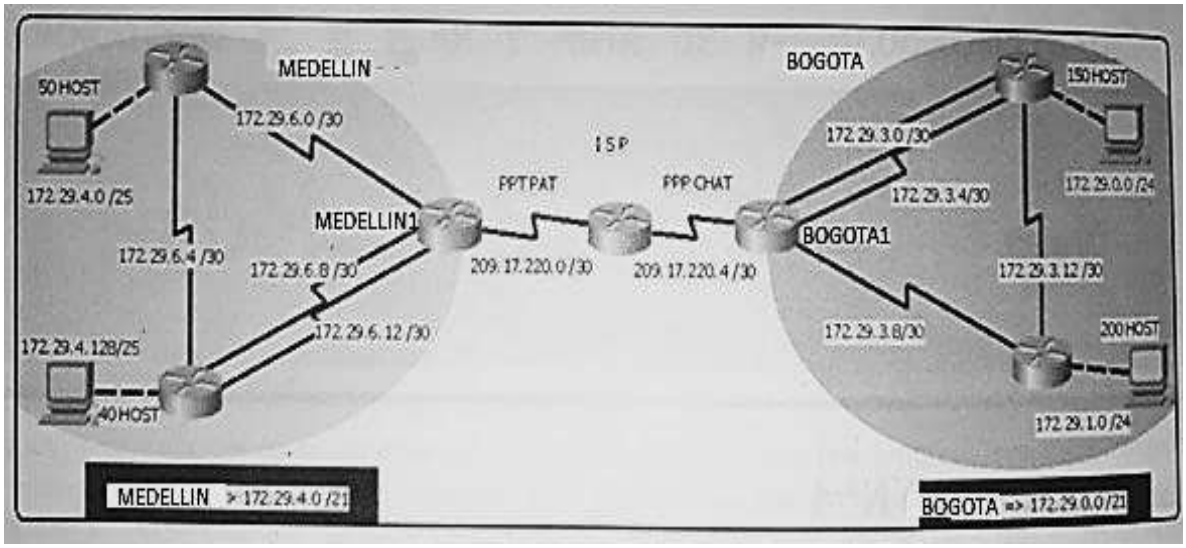
Resultado Topología Final: Finalmente, como resultado obtenemos la funcionalidad de todos los servicios en la red del escenario 1, tenemos enrutamiento RIPV2 aplicado a toda la red, servicio de DHCP hacia los hosts desde el router 1, enrutamiento a través de las VLAN 21 y 23, la traducción de las direcciones NAT hacia el servidor de internet y las listas de control de acceso permitidas desde el R2 hacia el R1 y denegadas para los demás dispositivos, y por ultimo la aplicación del protocolo de tiempo NTP en R2 como server y R1 como Cliente.

ESCENARIO 2

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

Topología de Red

Figura 28Topologia de Red 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 fisica de los equipos con base en la topología de red

CONFIGURACION INICIAL DE ROUTERS (CONTRASEÑAS, NOMBRES)

```
Router(config)#no ip-domain-lookup
Router(config)#hostname RMED1
RMED1(config)#line con 0
RMED1(config-line)#password cisco
RMED1(config-line)#login
RMED1(config-line)#exit
RMED1(config)#enable secret class
RMED1(config)#line vty 0 15
RMED1(config-line)#password cisco
RMED1(config-line)#login
RMED1(config-line)#service password-encryption
RMED1(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Router(config)#no ip domain-lookup
Router(config)#hostname RBOG02
RMED02(config)#line con 0
RMED02(config-line)#password cisco
RMED02(config-line)#login
RMED02(config-line)#exit
RMED02(config)#enable secret class
RMED02(config)#line vty 0 4
RMED02(config-line)#password cisco
RMED02(config-line)#login
RMED02(config-line)#service password-encryption
RMED02(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
RMED02(config)#

Router(config)#no ip domain-lookup
Router(config)#hostname RMED3
RMED3(config)#line con 0
RMED3(config-line)#password cisco
RMED3(config-line)#login
```

```
RMED3(config-line)#exit
RMED3(config)#enable secret class
RMED3(config)#line vty 0 15
RMED3(config-line)#password cisco
RMED3(config-line)#login
RMED3(config-line)#service password-encryption
RMED3(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Router(config)#no ip domain-lookup
Router(config)#hostname RBOG1
RBOG1(config)#enable secret class
RBOG1(config)#line con 0
RBOG1(config-line)#password cisco
RBOG1(config-line)#login
RBOG1(config-line)#line vty 0 15
RBOG1(config-line)#password cisco
RBOG1(config-line)#login
RBOG1(config-line)#service password-encryption
RBOG1(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Router(config)#no ip domain-lookup
Router(config)#hostname RBOG2
RBOG2(config)#enable secret class
RBOG2(config)#line con 0
RBOG2(config-line)#password cisco
RBOG2(config-line)#login
RBOG2(config-line)#line vty 0 15
RBOG2(config-line)#password cisco
RBOG2(config-line)#login
RBOG2(config-line)#service password-encryption
RBOG2(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#service password-encryption
ISP(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
```

Analisis y resultados: Como primera medida en la red ejecutamos la configuracion basica de todos los routers respecto a la seguridad de acceso, definicion de los nombres de los dispositivos y encriptacion de las contraseñas.

CONFIGURAR LA TOPOLOGÍA DE RED, DE ACUERDO CON LAS SIGUIENTES ESPECIFICACIONES.

Tabla de Enrutamiento

Dispositivo	Interfaz	Dirección IP	Máscara de red	Máscara Wilcard	Gateway Predeterminado
Medellin1	S0/0/0	172.29.6.9	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.13	255.255.255.252	0.0.0.3	NA
	S0/1/1	209.17.220.1	255.255.255.252	0.0.0.3	NA
Medellin2	S0/0/0	172.29.6.5	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.2	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.1	255.255.255.128	0.0.0.127	NA
Medellin3	S0/0/0	172.29.6.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.10	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.129	255.255.255.128	0.0.0.127	NA
ISP	S0/0/0	209.17.220.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	209.17.220.5	255.255.255.252	0.0.0.3	NA
Bogota1	S0/0/0	209.17.220.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.9	255.255.255.252	0.0.0.3	NA
	S0/1/1	172.29.3.5	255.255.255.252	0.0.0.3	NA
Bogota2	S0/0/0	172.29.3.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.13	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.6	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.0.1	255.255.255.0	0.0.0.255	NA
Bogota3	S0/0/0	172.29.3.10	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.1.1	255.255.255.0	0.0.0.255	NA

PC1_Med	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.1
PC2_Med	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.129
PC1_Bog	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.0.1
PC2_Bog	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.1.1

Analisis y resultados:

Definimos a traves de la tabla las direcciones IP a asignar en cada uno de los dispositivos teniendo en cuenta los segmentos de red presentados en la topologia en relacion a la red principal de cada sitio. Esta tabla es el insumo para la configuracion del enrutamiento en los dispositivos.

CONFIGURACIÓN RED ROUTERS

RMED 1 – Router Medellin 1

RMED1(config)#int s0/0/0
RMED1(config-if)#description conexion a RMED3
RMED1(config-if)#ip add 172.29.6.9 255.255.255.252
RMED1(config-if)#clock rate 128000
RMED1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RMED1(config-if)#exit
RMED1(config)#int s0/0/1
RMED1(config-if)#description conexion a RMED2
RMED1(config-if)#ip add 172.29.6.1 255.255.255.252
RMED1(config-if)#clock rate 128000
RMED1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
RMED1(config-if)#exit
RMED1(config)#int s0/1/0
RMED1(config-if)#description conexion a RMED3
RMED1(config-if)#ip add 172.29.6.13 255.255.255.252
RMED1(config-if)#clock rate 128000
RMED1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
RMED1(config-if)#exit
RMED1(config)#int s0/1/1
RMED1(config-if)#description conexion a ISP

RMED1(config-if)#ip add 209.17.220.1 255.255.255.252
RMED1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
RMED1(config-if)#exit

Análisis y resultados:

Configuración del enrutamiento y activación de las 4 interfaces del router medellin 1 que tiene conexión con los router Medellín 2 y 3 y la conexión al router ISP.

RMED 2 – Router Medellin 2

RMED2(config)#int s0/0/0
RMED2(config-if)#description conexion a RMED3
RMED2(config-if)#ip add 172.29.6.5 255.255.255.252
RMED2(config-if)#clock rate 128000
RMED2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RMED2(config-if)#exit
RMED2(config)#int s0/0/1
RMED2(config-if)#description conexion a RMED1
RMED2(config-if)#ip add 172.29.6.2 255.255.255.252
RMED2(config-if)#no shutdown

RMED2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

RMED2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

RMED2(config-if)#exit
RMED2(config)#int g0/0
RMED2(config-if)#description conexion a PC1_MED
RMED2(config-if)#ip add 172.24.4.1 255.255.255.128
RMED2(config-if)#no shutdown

RMED2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Análisis y resultados:

Obtenemos la configuración del enrutamiento de las 3 interfaces del router medellin 2 el cual tiene conexión serial con el router medellin 1, medellin 2 y la conexión ethernet a los host de la red PC1_Med

RMED-3 – Router Medellin 3

```
RMED3(config)#int s0/0/0
RMED3(config-if)#description conexion a RMED2
RMED3(config-if)#pi add 172.29.6.6 255.255.255.252
               ^
% Invalid input detected at '^' marker.

RMED3(config-if)#ip add 172.29.6.6 255.255.255.252
RMED3(config-if)#no shutdown

RMED3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

RMED3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

RMED3(config-if)#exit
RMED3(config)#int s0/0/1
RMED3(config-if)#description conexion a RMED1
RMED3(config-if)#ip add 172.29.6.10 255.255.255.252
RMED3(config-if)#no shutdown

RMED3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

RMED3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up

RMED3(config-if)#exit
RMED3(config)#int s0/1/0
RMED3(config-if)#description conexion a RMED1
RMED3(config-if)#ip add 172.29.6.14 255.255.255.252
RMED3(config-if)#no shutdown

RMED3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

RMED3(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

RMED3(config-if)#exit
RMED3(config)#int g0/0
RMED3(config-if)#description conexion a PC2_MED
RMED3(config-if)#ip add 172.29.4.129 255.255.255.128
RMED3(config-if)#no shutdown

RMED3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Análisis y resultados:

Obtenemos la configuración del enrutamiento de las 4 interfaces del router medellin 3 el cual tiene conexión serial con los routers medellin 1 (conexión de entrada y salida), medellin 2 y la conexión ethernet a los host de la red PC2_Med

ISP – Router ISP

SP(config)#int s0/0/0
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

ISP(config-if)#exit
ISP(config)#int s0/0/1
ISP(config-if)#description conexion a RBOG1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
ISP(config-if)#exit
ISP(config)#exit

Análisis y resultado:

Configuración y direccionamiento IP de las 2 interfaces de conexión serial del router ISP que tiene conexión con los routers principales de la red de Bogota y la red de Medellin.

RBOG1 – Router Bogota 1

```
RBOG1(config)#int s0/0/0
RBOG1(config-if)#description conexion a ISP
RBOG1(config-if)#ip add 209.17.220.6 255.255.255.252
RBOG1(config-if)#no shutdown

RBOG1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

RBOG1(config-if)#exit
RBOG1(config)#int s0/0/1
RBOG1(config-if)#description conexion a RBOG2
RBOG1(config-if)#ip add 172.29.3.1 255.255.255.252
RBOG1(config-if)#clock rate 128000
RBOG1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
RBOG1(config-if)#
RBOG1(config-if)#exit
RBOG1(config)#int s0/1/0
RBOG1(config-if)#description conexion a RBOG3
RBOG1(config-if)#ip add 172.29.3.9 255.255.255.252
RBOG1(config-if)#clock rate 128000
RBOG1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
RBOG1(config-if)#exit
RBOG1(config)#int s0/1/1
RBOG1(config-if)#description conexion a RBOG2
RBOG1(config-if)#ip add 172.29.3.5 255.255.255.252
RBOG1(config-if)#clock rate 128000
RBOG1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
RBOG1(config-if)#exit
```

Análisis y resultados:

Configuramos el direccionamiento IP y la activación de las 4 interfaces de uso del router Bogotá 1 el cual tiene comunicación serial con los routers de ISP, Router Bogota 2 y Router Bogota 3.

RBOG2 – Router Bogota 2

```
RBOG2(config)#int s0/0/0
RBOG2(config-if)#description conexion a RBOG1
RBOG2(config-if)#ip add 172.29.3.2 255.255.255.252
RBOG2(config-if)#no shutdown

RBOG2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

RBOG2(config-if)#exit
RBOG2(config)#int s0/0/1
RBOG2(config-if)#description conexion a RBOG3
RBOG2(config-if)#ip add 172.29.3.13 255.255.255.252
RBOG2(config-if)#clock rate 128000
RBOG2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
RBOG2(config-if)#exit
RBOG2(config)#int s0/1/0
RBOG2(config-if)#description conexion a RBOG1
RBOG2(config-if)#ip add 172.29.3.6 255.255.255.252
RBOG2(config-if)#no shutdown

RBOG2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to up

RBOG2(config-if)#exit
RBOG2(config)#int g0/0
RBOG2(config-if)#description conexion a PC1_BOG
RBOG2(config-if)#ip add 172.29.0.1 255.255.255.0
RBOG2(config-if)#no shutdown
```

RBOG2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Análisis y resultado:

Configuración de direccionamiento IP y activación de las 4 interfaces de uso para el router Bogota 2 el cual tiene comunicación serial con los routers Bogota 1 y Bogota 3 y comunicación ethernet con la red de host PC1:Bog

RBOG2(config-if)#exit

RBOG3 – Router Bogota 3

RBOG3(config)#int s0/0/0
RBOG3(config-if)#description conexion a RBOG1
RBOG3(config-if)#ip add 172.29.3.10 255.255.255.252
RBOG3(config-if)#no shutdown

RBOG3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

RBOG3(config-if)#exit
RBOG3(config)#int s0/0/1
RBOG3(config-if)#description conexion a RBOG2
RBOG3(config-if)#ip add 172.29.3.14 255.255.255.252
RBOG3(config-if)#no shutdown

RBOG3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

RBOG3(config-if)#exit
RBOG3(config)#int g0/0
RBOG3(config-if)#description conexion a PC2_BOG
RBOG3(config-if)#ip add 172.29.1.1 255.255.255.0
RBOG3(config-if)#no shutdown

RBOG3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

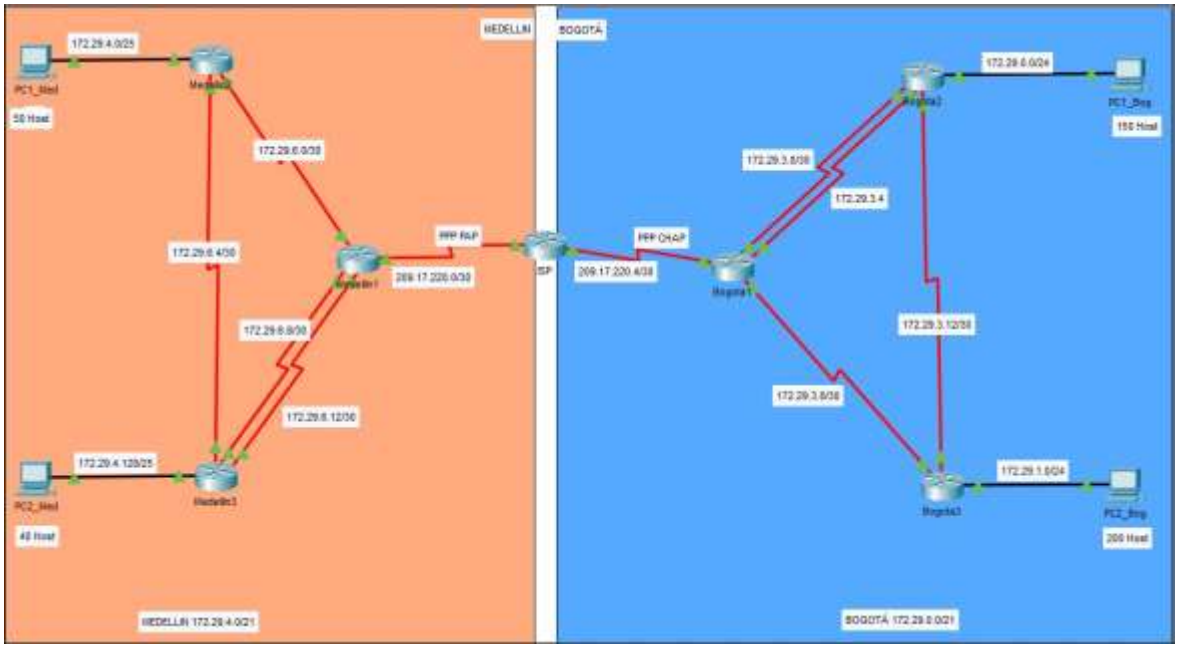
RBOG3(config-if)#

Analisis y resultados:.

Configuramos el direccionamiento IP y la activacion de las 3 interfaces del router Bogota 3 el cual tiene conexion serial con los routers Bogota 1 y Bogota 2 y conexion ethernet con los host PC2_Bog

Finalmente en este paso la topología nos debe quedar interconectada Figura29

Figura 29 Topología de red conectada en Packet Tracer Escenario 2



PARTE 1 CONFIGURACIÓN DEL ENRUTAMIENTO

a. **Configurar el enrutamiento en la red usando el protocolo OSPF versión 1, declare la red principal, desactive la sumarización automática.**

RMED1(config)#router ospf 1
RMED1(config-router)#router-id 1.1.1.1
RMED1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/1/0
C 209.17.220.0/30 is directly connected, Serial0/1/1
RMED1(config-router)#network 172.29.6.0 0.0.0.3 area 0

RMED1(config-router)#network 172.29.6.8 0.0.0.3 area 0
RMED1(config-router)#
01:32:17: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to FULL, Loading Done
RMED1(config-router)#network 172.29.6.12 0.0.0.3 area 0
RMED1(config-router)#
01:32:48: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from LOADING to FULL, Loading Done
RMED1(config-router)#network 209.17.220.0 0.0.0.3 area 0
RMED1(config-router)#exit
Packet Tracert no soporta el comando de sumarizar las rutas en OSPF

RMED2(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/0
RMED2(config-router)#router-id 2.2.2.2
RMED2(config-router)#network 172.29.4.0 0.0.0.127 area 0
RMED2(config-router)#network 172.29.6.0 0.0.0.3 area 0
RMED2(config-router)#network 172.29.6.4 0.0.0.3 area 0
RMED2(config-router)#
01:50:31: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
01:50:37: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to FULL, Loading Done

RMED3(config)#router ospf 1
RMED3(config-router)#router-id 3.3.3.3
RMED3(config-router)#do show ip route connected
C 172.29.6.4/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0
RMED3(config-router)#network 172.29.4.128 0.0.0.127 area 0
RMED3(config-router)#network 172.29.6.4 0.0.0.3 area 0
RMED3(config-router)#network 172.29.6.8 0.0.0.3 area 0
RMED3(config-router)#network 172.29.6.12 0.0.0.3 area 0
RMED3(config-router)#

RBOG1(config)#router ospf 1
RBOG1(config-router)#router-id 4.4.4.4
RBOG1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/1

```
C    172.29.3.8/30 is directly connected, Serial0/1/0
C    209.17.220.4/30 is directly connected, Serial0/0/0
RBOG1(config-router)#network 172.29.3.0 0.0.0.3 area 0
RBOG1(config-router)#
01:58:28: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING
to FULL, Loading Done
RBOG1(config-router)#network 172.29.3.4 0.0.0.3 area 0
RBOG1(config-router)#
01:59:10: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/1 from LOADING
to FULL, Loading Done
RBOG1(config-router)#network 172.29.3.8 0.0.0.3 area 0
RBOG1(config-router)#network 209.17.220.4 0.0.0.3 area 0
RBOG1(config-router)#exit


RBOG2(config)#router ospf 1
RBOG2(config-router)#router-id 5.5.5.5
RBOG2(config-router)#do show ip route connected
C    172.29.3.0/30 is directly connected, Serial0/0/0
C    172.29.3.4/30 is directly connected, Serial0/1/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
RBOG2(config-router)#network 172.29.0.0 0.0.0.255 area 0
RBOG2(config-router)#network 172.29.3.0 0.0.0.3 area 0
RBOG2(config-router)#network 172.29.3.4 0.0.0.3 area 0
RBOG2(config-router)#network 172.29.3.12 0.0.0.3 area 0


RBOG3(config)#router ospf 1
RBOG3(config-router)#router id 6.6.6.6
RBOG3(config-router)#router-id 6.6.6.6
RBOG3(config-router)#do show ip route connected
C    172.29.3.8/30 is directly connected, Serial0/0/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
RBOG3(config-router)#network 172.29.1.0 0.0.0.255 area 0
RBOG3(config-router)#network 172.29.3.8 0.0.0.3 area 0
RBOG3(config-router)#
01:58:20: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/0 from LOADING
to FULL, Loading Done
RBOG3(config-router)#network 172.29.3.12 0.0.0.3 area 0
RBOG3(config-router)#
01:59:10: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING
to FULL, Loading Done
RBOG3(config-router)#exit
```

```
ISP(config)#router ospf 1
ISP(config-router)#router-id 7.7.7.7
ISP(config-router)#do show ip route connected
C   209.17.220.0/30  is directly connected, Serial0/0/0
C   209.17.220.4/30 is directly connected, Serial0/0/1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)#
02:10:53: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING
to FULL, Loading Done
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#
02:11:24: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

Analisis y resultados:

Generamos un ID a cada router donde vamos a aplicar el OSPF, posteriomente declaramos las redes que van a participar en el OSPF iniciando con la red principal utilizando el modelo wilcard y especificamos el area como area 0 por defecto para todos los routers con esto como resultado ya tenemos aplicado el protocolo OSPF en nuestros routers.

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.

```
RMED1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
RMED1(config)#router ospf 1
RMED1(config-router)#default-information originate
RMED1(config-router)#exit
```

```
RBOG1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
RBOG1(config)#router ospf 1
RBOG1(config-router)#default-information originate
RBOG1(config-router)#exit
```

Analisis y resultado:
Obtenemos la configuracion de enrutamiento desde el router medellin1 hasta la interface serial 0 del ISP y el router bogota1 hasta la interface serial 1 de ISP.

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.

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

Analisis y resultado:

Obtenemos la configuracion de la ruta estatica desde el router ISP al router medellin 1 con direccion ip 209.17.220.1 y al router bogota 1 con direccion ip 209.17.220.6

PARTE 2: TABLA DE ENRUTAMIENTO

.

- **a.** Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas. **(Se cumple)**
- **b.** Verificar el balanceo de carga que presentan los routers. **(Se cumple)**
- **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. **(Se cumple)**
- **d.** Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF. **(Se cumple)**
- **e.** Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto. **(Se cumple)**
- **f.** El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas. **(Se cumple)**

Analisis y resultados:

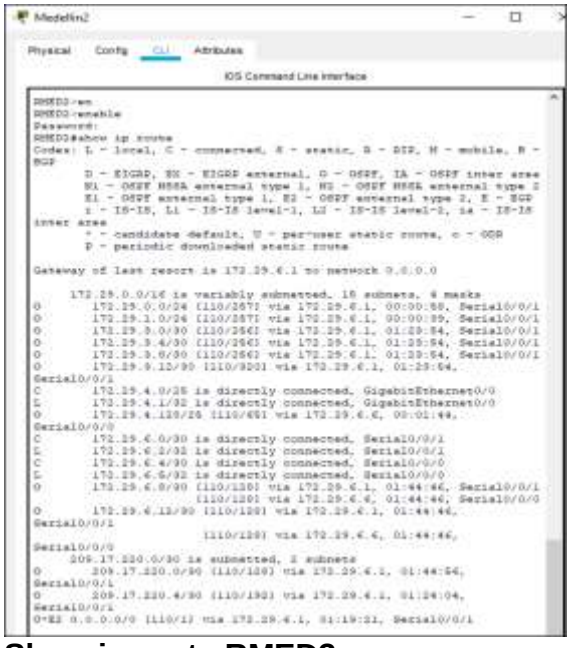
En el registro de imágenes siguientes podemos ver el cumplimiento de cada uno de los puntos solicitados en la revisión de la tabla de enrutamiento la cual se genera en cada router a traves del comando show ip route.

Show ip route – RMED1

Figura 30 Tabla de enrutamiento RMED1

Show ip route – RMED2

Figura 31 Tabla de enrutamiento RMED2



Show ip route RMED3

Figura 32 Tabla de enrutamiento RMED3

Show ip route RBOG1

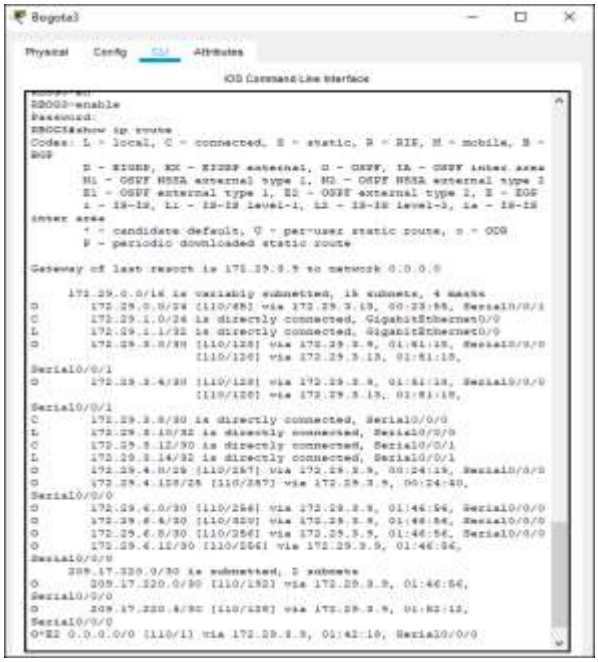
Figura 33 Tabla de enrutamiento RBOG1

Show ip route RBOG2

Figura 34 Tabla de enrutamiento RBOG2

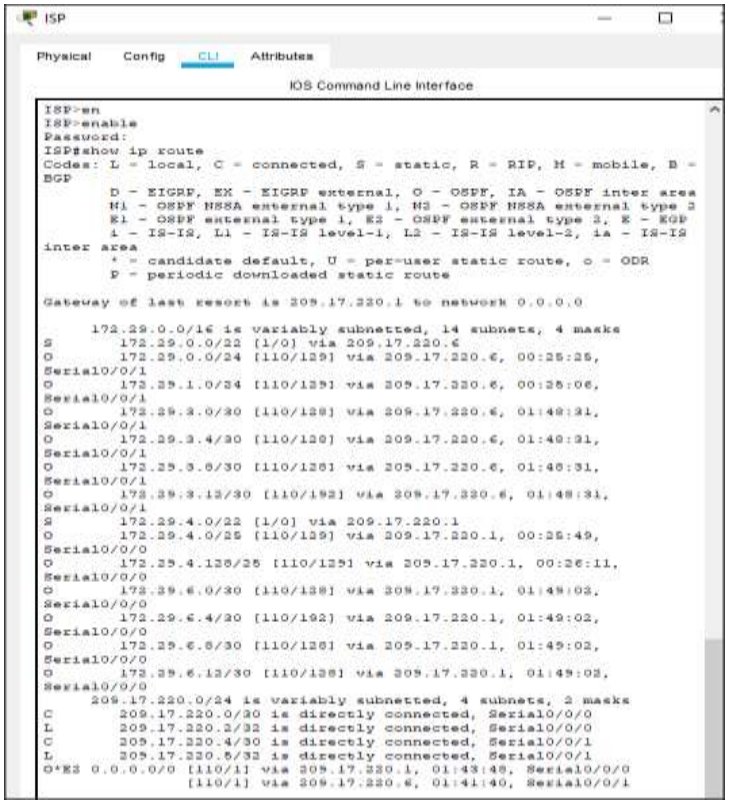
Show ip route RBOG3

Figura 35 Tabla de enrutamiento RBOG3



Show ip route ISP

Figura 36 Tabla de enrutamiento Router ISP



PARTE 3 DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF

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

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Bogotá 1

RBOG1(config)#router ospf 1
RBOG1(config-router)#passive-interface s0/1/1
RBOG1(config-router)#
04:06:43: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Bogotá 2

RBOG2(config)#router ospf 1
RBOG2(config-router)#passive-interface s0/1/0
RBOG2(config-router)#passive-interface g0/0
RBOG2(config-router)#exit

Bogotá 3

RBOG3(config)#router ospf 1
RBOG3(config-router)#passive-interface g0/0
RBOG3(config-router)#exit

Medellin 1

RMED1(config)#router ospf 1
RMED1(config-router)#passive-interface s0/1/0
RMED1(config-router)#
04:13:59: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Medellin 2

RMED2(config)#router ospf 1
RMED2(config-router)#passive-interface g0/0
RMED2(config-router)#exit

Medellin 3

RMED3(config)#router ospf 1
RMED3(config-router)#passive-interface g0/0

RMED3(config-router)#exit

Análisis y resultados:

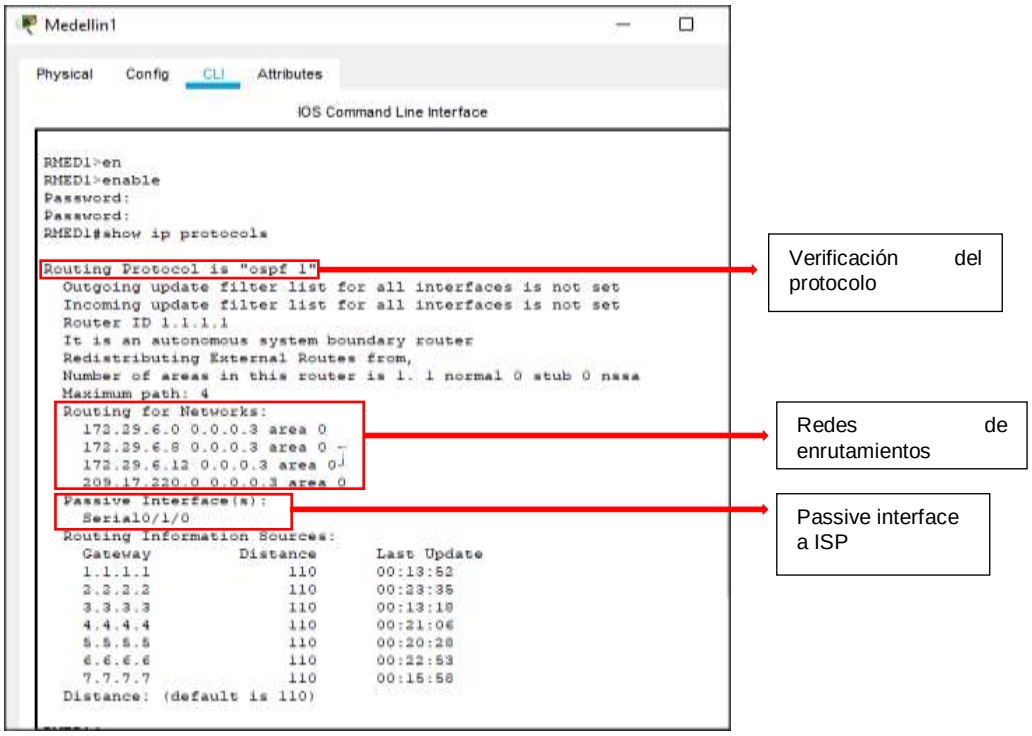
A través del comando passive-interface deshabilitamos las interfaces de las cuales no vamos hacer uso con el fin de evitar por estas la propagación del protocolo OSPF.

PARTE 4 VERIFICACIÓN DEL PROTOCOLO OSPF

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

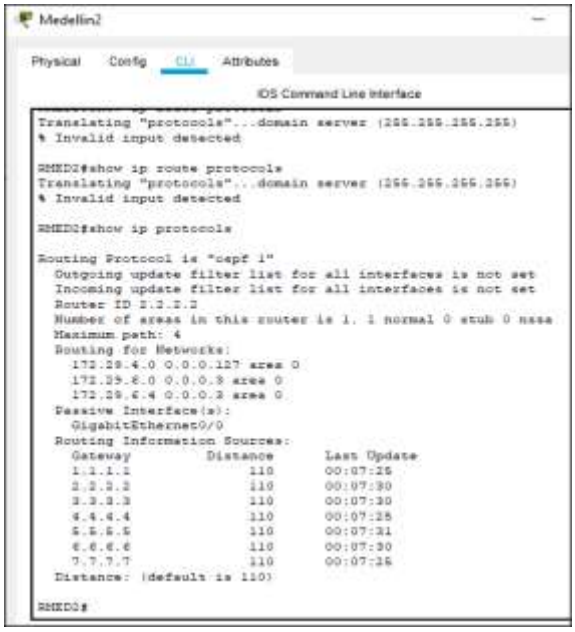
Show ip route protocols en RMED1

Figura 37 Verificación Protocolo OSPF RMED1



Show ip route protocols en RMED2

Figura 38 Verificación del Protocolo OSPF RMED2

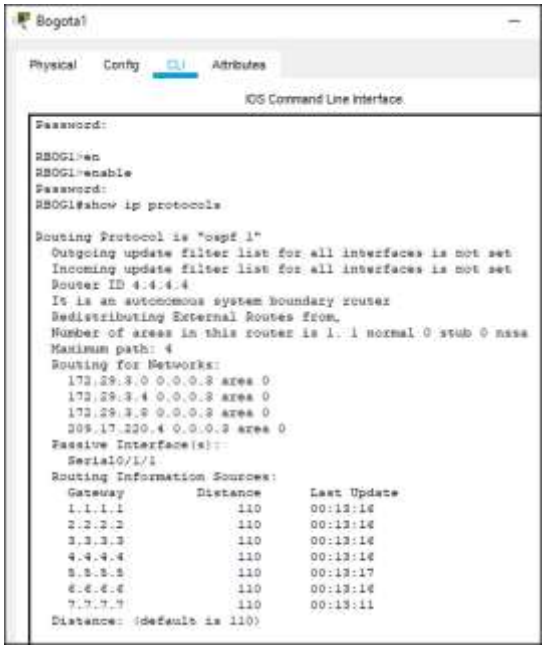


Show ip route protocols en RMED3

Figura 39 Verificacion Protocolo OSPF RMED3

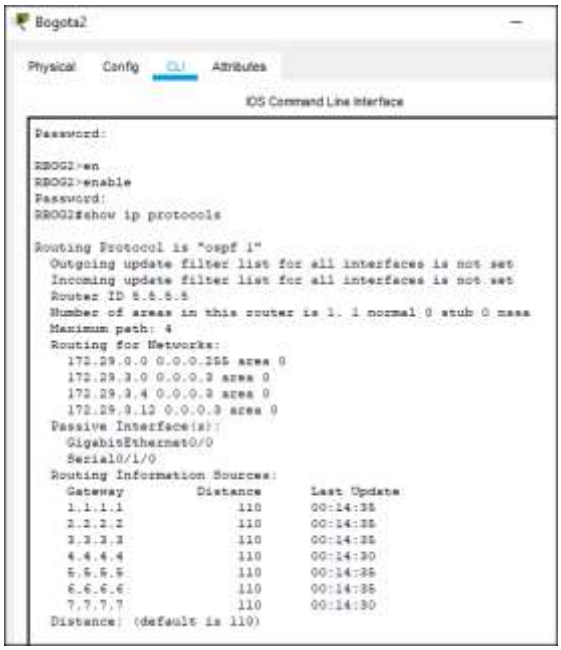
Show ip route protocols en RBOG1

Figura 40 Verificacion Protocolo OSPF RBOG1



Show ip route protocols en RBOG2

Figura 41 Verificacion del Protocolo OSPF RBOG2

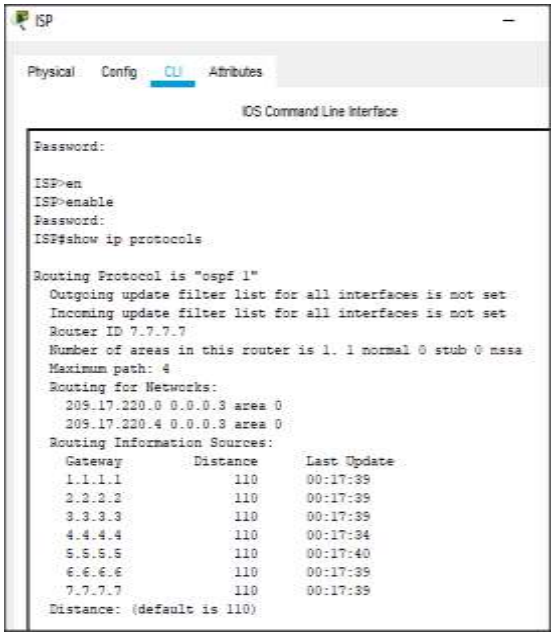


Show ip route protocols en RBOG3

Figura 42 Verificacion Protocolo OSPF RBOG3

Show ip route protocols en ISP

Figura 43 Verificacion Protocolo OSPF Router ISP



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.

Revisar Figura 37 a Figura 43 la base de datos de OSPF da respuesta a esta pregunta.

PARTE 5 CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

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

```
RMED1(config)#int s0/1/1
RMED1(config-if)#encapsulation ppp
RMED1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state
to down
04:54:09: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/1/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
RMED1(config-if)#no shutdown
RMED1(config-if)#exit
RMED1(config)#username ISP secret cisco
RMED1(config)#int s0/1/1
RMED1(config-if)#ppp authentication pap
RMED1(config-if)#ppp pap sent-username MEDELLIN password cisco
      RMED1(config-if)#exit
```

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

```
RBOG1(config)#int s0/0/0
RBOG1(config-if)#encapsulation ppp
RBOG1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to down
04:58:38: %OSPF-5-ADJCHG: Process 1, Nbr 7.7.7.7 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
RBOG1(config-if)#no shutdown
RBOG1(config-if)#exit
RBOG1(config)#username ISP secret cisco
RBOG1(config)#int s0/0/0
RBOG1(config-if)#ppp authentication chap
RBOG1(config-if)#exit
```

```
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/0/0
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#exit
ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap
        ISP(config-if)#exit
```

Análisis y resultados:

Se configura y prueba la autenticación de seguridad de los enlaces hacia el ISP con el fin de generar seguridad de acceso a los enlaces principales hacia el ISP.

PARTE 6 CONFIGURACIÓN DE PAT

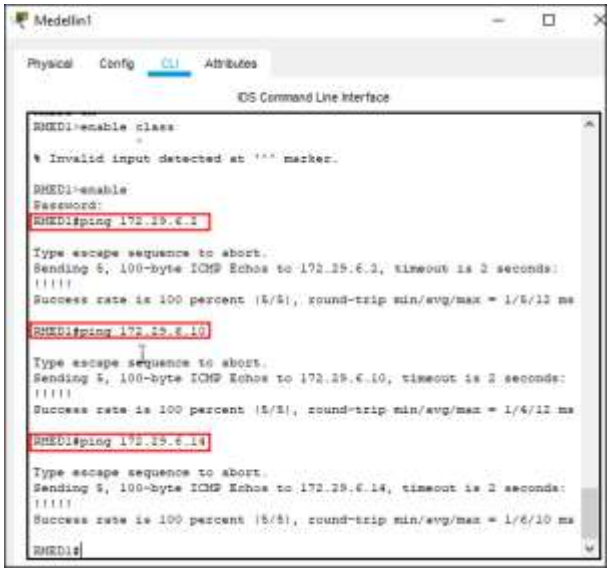
a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1. **(Se cumple)**
b. Después de verificar lo indicado 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 cumple figura 44).**
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 cumple figura 45).**

```
RMED1(config)#ip access-list standard host
RMED1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
RMED1(config-std-nacl)#exit
RMED1(config)#ip nat inside source list host interface s0/1/1 overload
RMED1(config)#int s0/0/0
RMED1(config-if)#ip nat inside
RMED1(config-if)#exit
RMED1(config)#int s0/0/1
RMED1(config-if)#ip nat inside
RMED1(config-if)#exit
RMED1(config)#int s0/1/0
RMED1(config-if)#ip nat inside
RMED1(config-if)#exit
RMED1(config)#int s0/1/1
RMED1(config-if)#ip nat outside
RMED1(config-if)#exit
RMED1(config)#exit
RMED1#
%SYS-5-CONFIG_I: Configured from console by console
RMED1#show ip nat translation

RBOG1(config)#ip access-list standard host
RBOG1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
RBOG1(config-std-nacl)#exit
RBOG1(config)#ip nat inside source list host interface s0/0/0 overload
RBOG1(config)#int s0/0/0
RBOG1(config-if)#ip nat outside
RBOG1(config-if)#exit
RBOG1(config)#int s0/0/1
RBOG1(config-if)#ip nat inside
RBOG1(config-if)#exit
RBOG1(config)#int s0/1/0
RBOG1(config-if)#ip nat inside
RBOG1(config-if)#exit
RBOG1(config)#int s0/1/1
RBOG1(config-if)#ip nat inside
RBOG1(config-if)#exit
RBOG1(config)#exit
RBOG1#
%SYS-5-CONFIG_I: Configured from console by console
RBOG1#show ip nat translation
```

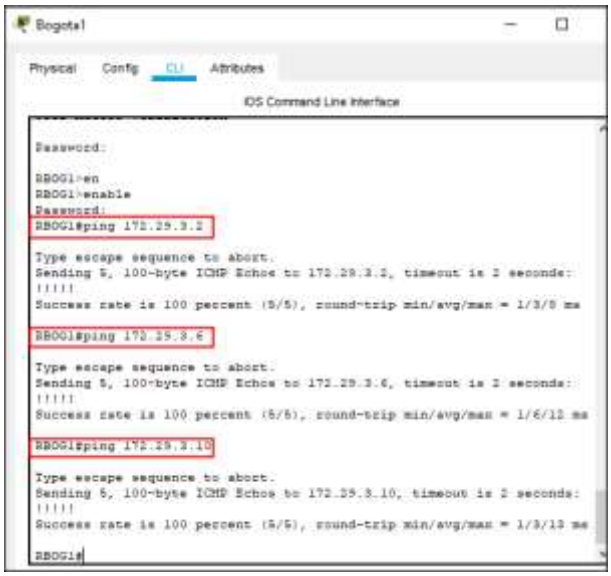
Ping RMED1 – RMED2 y RMED3

Figura 44 Ping Router RMED1 - RMED2 - RMED3



Ping RBOG1 – RBOG2 y RBOG3

Figura 45 Ping Router RBOG1 - RBOG2 - RBOG3



PARTE 7 CONFIGURACIÓN DEL SERVICIO DHCP

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

```
RMED2(config)#ip dhcp excluded-address 172.29.4.1
RMED2(config)#ip dhcp pool RMED2
RMED2(dhcp-config)#network 172.29.4.0 255.255.255.128
RMED2(dhcp-config)#default-router 172.29.4.1
RMED2(dhcp-config)#dns-server 8.8.8.8
RMED2(dhcp-config)#exit
RMED2(config)#ip dhcp excluded-address 172.29.4.29
RMED2(config)#ip dhcp pool RMED3
RMED2(dhcp-config)#network 172.29.4.128 255.255.255.128
RMED2(dhcp-config)#default-router 172.29.4.129
RMED2(dhcp-config)#dns-server 8.8.8.8
RMED2(dhcp-config)#exit
```

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

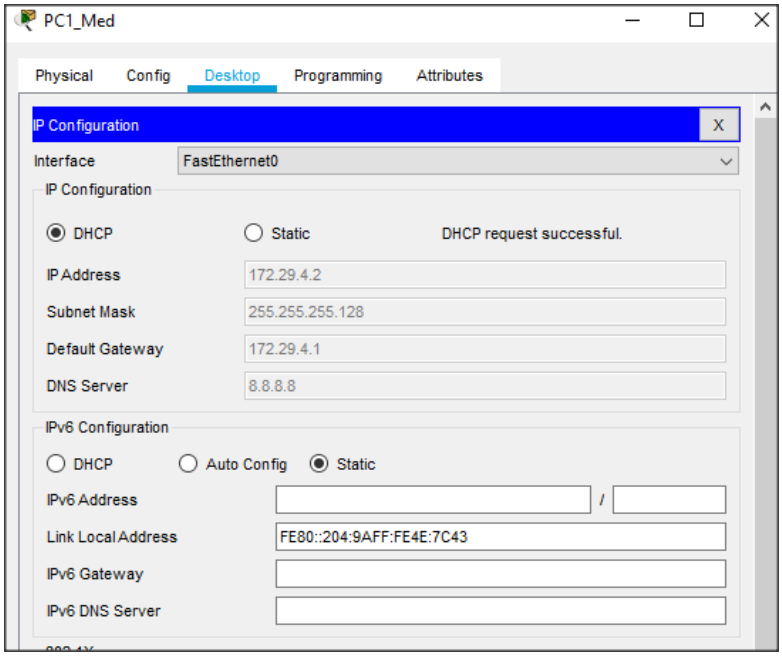
Análisis y resultados:

Como el servidor RMED3 tiene una red LAN conectada pero no realizara funciones de servidor DHCP, surge la necesidad de configurar “ip helper” el cual va permitir ser un router de transito para llegar al router con el ROL de DHCP. Utilizamos el comando ip helper-address para atrapar los broadcast y redireccionarlos hacia la IP del router de medellin2, se debe utilizar la dirección IP de la interfaz de salidad Medellin2 (S/0/0/0 – 172.29.6.5)

```
RMED3(config)#int g0/0
RMED3(config-if)#ip helper-address 172.29.6.5
RMED3(config-if)#exit
```

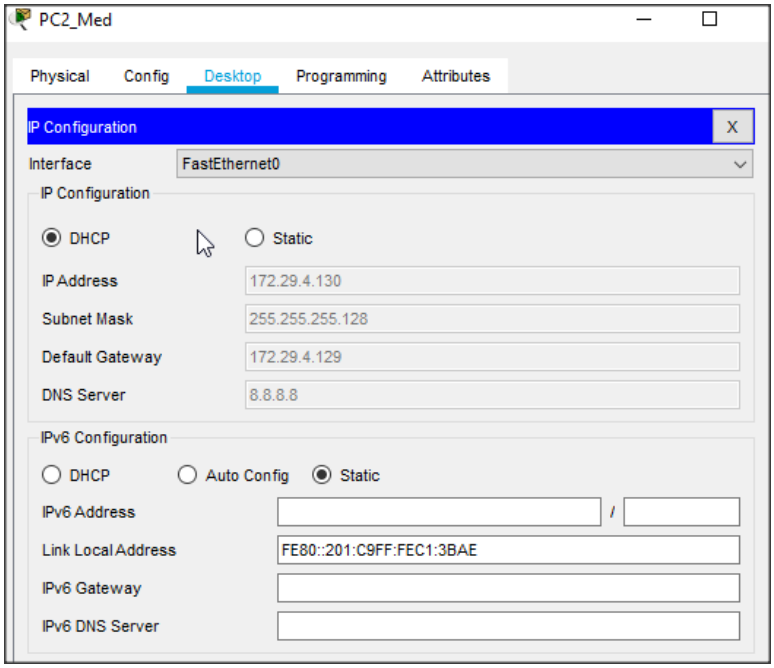
Direccionamiento DHCP PC1_Med

Figura 46 Verificación Direccionamiento DHCP PC1_MED



Direccionamiento DHCP PC2_Med

Figura 47 Verificacion de Direccionamiento DHCP PC2_MED



c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes Lan.

```
RBOG2(config)#ip dhcp excluded-address 172.29.0.1
RBOG2(config)#ip dhcp pool RBOG2
RBOG2(dhcp-config)#network 172.29.0.0 255.255.255.0
RBOG2(dhcp-config)#default-router 172.29.0.1
RBOG2(dhcp-config)#dns-server 8.8.8.8
RBOG2(dhcp-config)#exit
RBOG2(config)#ip dhcp excluded-address 172.29.1.1
RBOG2(config)#ip dhcp pool RBOG3
RBOG2(dhcp-config)#network 172.29.1.0 255.255.255.0
RBOG2(dhcp-config)#default-router 172.29.1.1
RBOG2(dhcp-config)#dns-server 8.8.8.8
RBOG2(dhcp-config)#exit
```

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

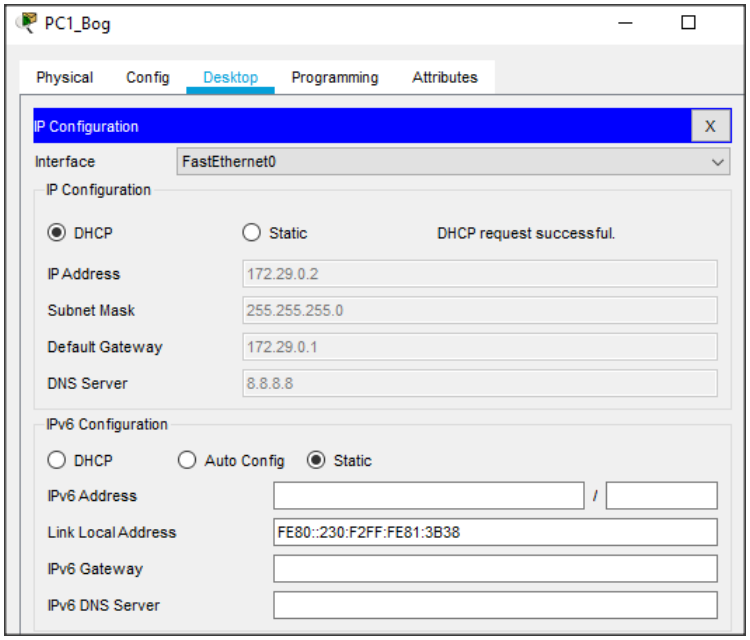
Análisis y Resultados:

Como el servidor RBOG3 tiene una red LAN conectada pero no realizara funciones de servidor DHCP, surge la necesidad de configurar “ip helper” el cual va permitir ser un router de transito para llegar al router con el ROL de DHCP. Utilizamos el comando ip helper-address para atrapar los broadcast y redireccionarlos hacia la IP del router de RBOG2, se debe utilizar la dirección IP de la interfaz de salidad Bogota2 (S/0/0/1 – 172.29.3.13)

```
RBOG3(config)#int g0/0
RBOG3(config-if)#ip helper-address 172.29.3.13
RBOG3(config-if)#exit
```

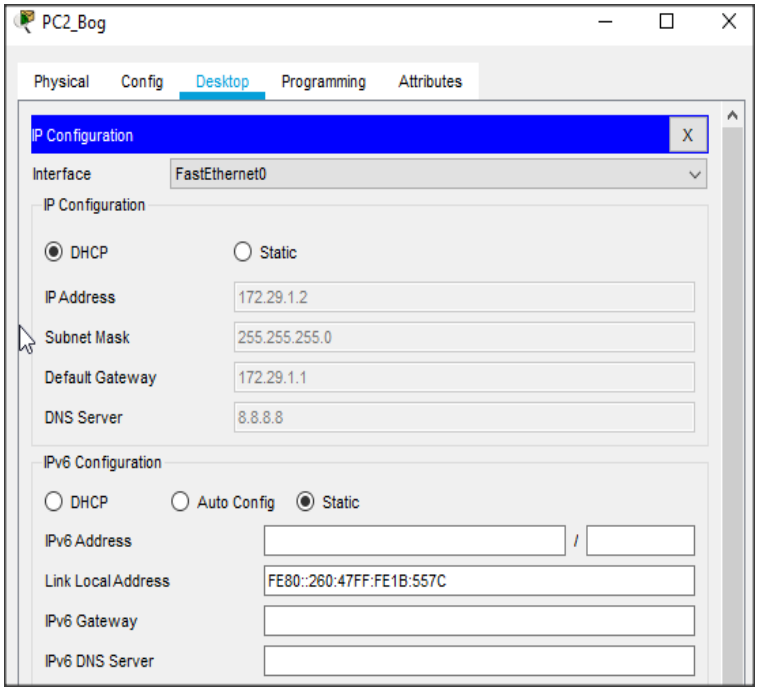
Direccionamiento DHCP PC1_Bog

Figura 48 Verificacion Direccionamiento DHCP PC1_BOG



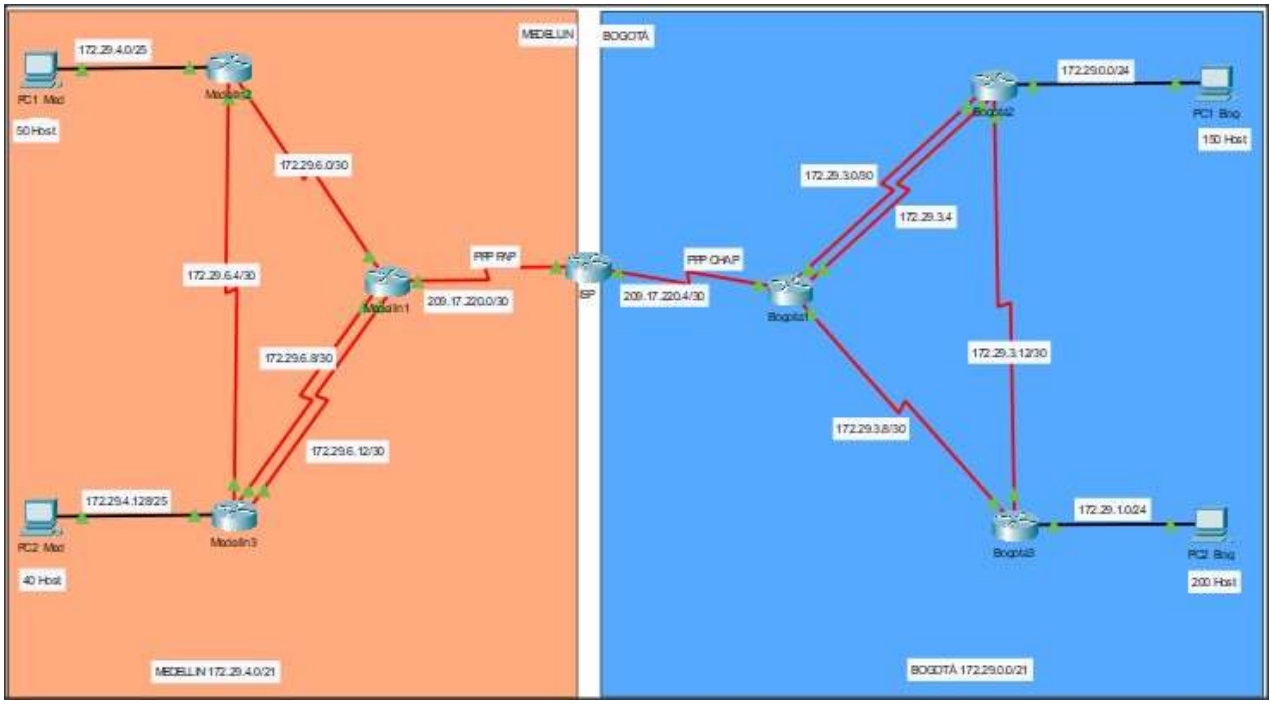
Direccionamiento DHCP PC2_Bog

Figura 49 Verificacion Direccionamiento DHCP PC2_BOG



TOPOLOGÍA FINAL ESCENARIO 2 [PACKET TRACER]

Figura 50 Topología Final Escenario 2 [William Vargas A]



Finalmente tenemos la topología desarrollada aplicando el protocolo OSPF por medio de un ISP que recibe los routers principales de las 2 redes y es el punto central de comunicación en cada enlace del ISP a los routers principales tenemos encapsulación PPP con autenticación con el fin de mantener seguridad en la red, obtuvimos los resultados satisfactorios en la aplicación de los servicios DHCP de cada uno de los routers principales de cada una de las sucursales a los host finales.

CONCLUSIONES

Durante el desarrollo de la prueba de habilidades podemos evidenciar que los 2 caso de estudio propuestos nos exponen 2 contextos diferentes que son aplicables para 2 protocolos principales de red que también son diferentes y debemos adquirir la habilidad y competencia para identificar según los requerimientos, infraestructura y necesidades de la red cual aplicar.

En el escenario 1 logramos evidenciar una red que no es muy extensa por decirlo de alguna manera una red pequeña que la podemos encontrar en nuestro ámbito profesional en una compañía pyme o no muy grande y podemos aplicar el protocolo RIPV2 el cual concluimos según el ejercicio es un protocolo de enrutamiento dinámico que nos permite utilizar a través de saltos como métricas el camino para enrutar los datos sin embargo aplica para este tipo de redes ya que su convergencia es lenta y puede tardar en recibir paquetes.

En el escenario 2 evidenciamos una red mucho mas extensa que la vamos a encontrar en un entorno de una compañía con una infraestructura mas grande y por ello aplicamos el protocolo OSPF el cual posee una convergencia más rápida, es un protocolo que puede encontrar caminos alternos de forma más inteligente en tiempos muy cortos a diferencia del RIPV2.

Es fundamental que como administradores de redes tengamos pleno conocimiento de las diferencias y funcionalidades de los protocolos a aplicar en principio estos 2 protocolos son dinámicos, pero además de esto evidenciamos un proceso ordenado para la administración o configuración de las redes en cualquier escenario y es garantizar la seguridad de la red por medio de la aplicación de autenticación y encapsulamiento de dispositivos y enlaces con el fin de evitar al máximo su vulnerabilidad. Ser prácticos y conocer la aplicación de VLANS en la red nos ayuda a optimizar procesos y recursos en la red de la misma manera.

BIBLIOGRAFIA

CISCO.DHCP. Principios de Enrutamiento y Conmutación. Recuperado……de.....https://static-course- assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de .https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO.OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado ……de.....https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

MODULO 3 CISCO CCNA. Exploration 3. Tipos de VLAN. Recuperado……de https://sites.google.com/site/paginamodulo3vlan/presentacion-de-las-vlan/tipos-de-vlan