DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WLAN
TRABAJO DE GRADO HABILIDADES PRÁCTICAS CCNA

WILLY YESID DUARTE RAGUA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS E INGENIERÍA (ECBTI)

DIPLOMADO DE PROFUNDIZACIÓN CISCO

CÚCUTA, NORTE DE SANTANDER

MAYO 2020

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WLAN
TRABAJO DE GRADO HABILIDADES PRÁCTICAS CCNA

INFORME FINAL PARA OPTAR POR EL TÍTULO DE INGENIERO DE SISTEMAS

TUTOR

ING. HÉCTOR JULIÁN PARRA MOGOLLÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS E INGENIERÍA (ECBTI)
DIPLOMADO DE PROFUNDIZACIÓN CISCO
CÚCUTA, NORTE DE SANTANDER
MAYO 2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cúcuta, 26 de mayo de 2020

Este trabajo lo quiero dedicar a Dios primeramente y a mi familia, mi esposa e hijos que me han apoyado durante el proceso formativo como Ingeniero de Sistemas.

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

Un agradecimiento a todas las autoridades y personal que hacen la Unidad Abierta y a Distancia UNAD, por confiar en mí, abrirme las puertas de la Universidad y permitirme realizar todo el proceso formativo e investigativo dentro de su establecimiento educativo.

De igual manera mis agradecimientos al Tutor Ing. Vicente Ortiz por su acompañamiento y consejo en el proceso de inscripción y homologación de los cursos, a la Ingeniera Claudia Mariño por su acompañamiento en los procesos administrativos; quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Finalmente quiero expresar mi más grande y sincero agradecimiento al ingeniero Héctor Julián Parra, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

CONTENIDO

Pág

LISTA DE TABLAS

Pág

LISTA DE FIGURA

Pág

GLOSARIO

IP: Protocolo de Internet. Protocolo de capa de red en el stack TCP/IP que brinda un servicio de internetworking sin conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad.

IPv6: Protocolo de capa de red para trabajos de Internet conmutados por paquetes. Sucesor de IPv4 para uso general en Internet.

Algoritmo: Regla o proceso bien definido para llegar a la solución de un problema. En networking, suelen usarse los algoritmos para determinar el mejor camino para el tráfico desde un origen en particular a un destino en particular.

Cable: Medio de transmisión de cable de cobre o fibra óptica envuelto en una cubierta protectora.

Contiguo: Constante o adyacente. En cuanto a las redes contiguas, la palabra contiguo significa bloques de redes que son jerárquicas por naturaleza.

Convergencia: Velocidad y capacidad de un grupo de dispositivos de internetwork que ejecutan un protocolo de enrutamiento específico para coincidir con la topología de una internetwork después de un cambio en esa topología.

Dirección IP con clase: En los primeros tiempos de IPv4, las direcciones IP estaban divididas en 5 clases, particularmente Clase A, Clase B, Clase C, Clase D y Clase E.

Dominio: Parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3.

Flash: Tecnología desarrollada por Intel y cuya licencia le ha sido otorgada a otras empresas de semiconductores. La memoria Flash es un almacenamiento no volátil que se puede borrar y reprogramar de forma eléctrica. Permite que las imágenes de software se guarden, arranquen y rescriban según sea necesario.

Gateways: Dispositivo de una red que sirve como punto de acceso a otra red. El gateway predeterminado es utilizado por un host cuando la dirección de destino de un paquete IP pertenece a algún lugar fuera de la subred local. Un router es un buen ejemplo de un gateway predeterminado.

Hosts: Sistema de computación en una red. Es similar al nodo, salvo que el host generalmente indica un sistema de computación, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluidos servidores de acceso y routers.

Loopback: 127.0.0.1 es una dirección IP disponible en todos los dispositivos para ver si la tarjeta NIC de ese dispositivo funciona. Si se envía algo a 127.0.0.1, hace un loop back en sí misma y por consiguiente envía los datos a la NIC de ese dispositivo. Si se obtiene una respuesta positiva a un ping 127.0.0.1, se sabe que la tarjeta NIC funciona correctamente.

RAM: Memoria volátil que puede ser leída y escrita por un microprocesador.

ROM: Memoria no volátil que un microprocesador puede leer, pero no escribir.

ATM: Modo de transferencia asíncrona. El estándar internacional del relay de celda en el cual se transmiten múltiples tipos de servicios (como voz, video o datos) en celdas de una longitud fija (53 bytes). Las celdas de longitud fija permiten que se produzca el procesamiento de las celdas en el hardware, por consiguiente, se reducen los retardos en el tránsito. La ATM está diseñada para sacar provecho de los medios de transmisión de alta velocidad, como son E3, SONET y T3.

Modo Setup: Cuando un router de Cisco se inicia y no encuentra un archivo de configuración en NVRAM ingresa en el modo setup. El modo setup es un diálogo de preguntas que el administrador debe contestar para establecer una configuración básica para la funcionalidad del router.

VLSM: máscara de subred de longitud variable. Capacidad para especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes con mayor frecuencia se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

RIP: Protocolo de información de enrutamiento. IGP suministrado con los sistemas UNIX BSD. El IGP más común de Internet. El RIP usa el conteo de saltos como métrica de enrutamiento.

Protocolo vector ruta: Un protocolo vector ruta es un protocolo de enrutamiento que marca y muestra la ruta que toma la información actualizada a medida que se esparce por la red. BGP es un usuario de ese tipo de protocolo porque verifica por qué sistema autónomo pasó la actualización para verificar los bucles.

NVRAM: Memoria de acceso aleatorio no volátil. Memoria de acceso aleatorio que, cuando la computadora se apaga, el contenido de la NVRAM permanece allí.

WAN: Red de comunicación de datos que sirve a los usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión proporcionados por proveedores comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

LAN: El término Red de área local (LAN) hace referencia a una red local, o a un grupo de redes locales interconectadas, que están bajo el mismo control administrativo. En las primeras épocas del networking, las LAN se definían como pequeñas redes que existían en una única ubicación física. A pesar de que las LAN pueden ser una única red local instalada en una vivienda u oficina pequeña, la definición de LAN ha evolucionado y ahora incluye redes locales interconectadas compuestas por muchos cientos de hosts, instaladas en múltiples edificios y ubicaciones.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red. Ocasionalmente, se denomina gateway (aunque esta definición de gateway está cayendo más en desuso).

Ruta sumarizada: La sumarización de ruta reduce el número de rutas que el router debe mantener. Es un método para representar una serie de números de red en una única dirección sumarizada.

RESUMEN

La concepción, gestión y administración de las redes de comunicación, sean LAN, MAN ó WAN hacen parte de la cotidianidad y son parte sumamente importante para el desarrollo y sostenibilidad de las áreas de comunicaciones y flujo de información; en todas las instituciones o empresas que hoy dependen del flujo, disponibilidad, veracidad y seguridad de su activo más importante, la información.

Los sistemas de comunicación día a día van en un crecimiento y desarrollo considerable, por esto se hace importante que se definan estándares y reglas para un uso adecuado de los sistemas de administración, con el objetivo de optimizar el uso de los recursos que pone a disposición de sus usuarios una empresa enfocándose en la meta de obtener el mayor rendimiento y productividad posibles.

Con estos antecedentes el presente Informe final para optar por el título de Ingeniero de Sistemas se desarrolla con la herramienta PACKET TRACER, y con los contenidos del módulo DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN, considerando tecnologías de alta velocidad para redes y sistemas de comunicación, además realiza un análisis de la herramienta de administración y monitoreo de equipos activos y recursos de red que se pueden implementar según los requerimientos que se puedan presentar.

El primer capítulo Fundamentos de Networking comprende un estudio de las principales tecnologías de alta velocidad para las redes de comunicación, tendencias, características principales, ventajas y desventajas y su evolución a lo largo de la historia.

El segundo capítulo Modelo OSI y Direccionamiento IP presenta El Protocolo de control de transmisión (TCP) es un protocolo utilizado para todos los nodos conectados a internet de manera que estos se puedan comunicar entre sí de manera fiable. Se trata de un protocolo orientado a la conexión que junto con el protocolo IP ha servido de base para el modelo TCP/IP, utilizado desde antes de que se estableciera el Modelo OSI (Interconexiones de Sistemas Abiertos) y por esta razón el modelo TCP/IP ha sido comparado con el modelo OSI.

El tercer capítulo Configuración de Sistemas de red soportados en VLANs se muestra la a importancia de las prácticas de las tecnologías de la información y de las comunicaciones actualmente están relacionados de alguna manera y el conocimiento de la estructura y las herramientas de los sistemas o TIC, además de comprender y aplicar cada una de las temáticas abordada en la unidad, fortaleciendo el desarrollo de competencias en el área del saber especifico orientadas a la configuración de los sistemas de red soportados en VLANs

El cuarto capítulo Enrutamiento en soluciones de red se conoce el enrutamiento estático como la solución para redes pequeñas por su seguridad y por la economía de sus recursos; no consume ancho de banda, no hace trabajar a la CPU del router y es fácil de configurar. Frente a lo que ocurre cuando se configura una red con protocolos de enrutamiento dinámico, la configuración de rutas estáticas exige la intervención del administrador cada vez que se producen cambios en esta, por este motivo lo normal es que en las mayorías de las redes se utilicen tanto rutas estáticas (configuradas manualmente) como protocolos de enrutamiento dinámico que veremos más adelante y que “aprenden” y establecen nuevas rutas a medida que la red cambia.

PALABRAS CLAVE: Rendimiento de red, escalabilidad, disponibilidad, seguridad.

1. INTRODUCCIÓN

La prueba de Habilidades del Diplomado de Profundización CISCO, pretende por medio de 2 Escenarios planteados desarrollar de manera practica y de manera evaluativa los conceptos y experiencias aprendidas a través del curso; se pondrá en práctica la temática estudiada y en el cómo lo ponemos en práctica en la vida laboral.

Por medio del uso de la herramienta PACKET TRACER pretendo mostrar el desarrollo y respuesta a los escenarios planteados.

También en esta actividad del curso de profundización CISCO, nos permitirá desarrollar las actividades correspondientes para resolver los casos de estudio para el curso CCNA nivel 1 denominado aspectos básicos del Networking y para el curso CCNA nivel 2 denominado conceptos y protocolos de enrutamiento. Con este fin, se pretende la solución óptima de la totalidad de los puntos de las prácticas, se entregarán los productos generados en el diseño del Packet Tracer para la revisión del tutor a través de la Plataforma Virtual del curso.
Siendo así mejoraremos la comprensión acerca de las temáticas de este curso, su alcance y composición, facilitando el aprendizaje, generando así motivación que me lleve a realizar un trabajo a con excelencia cumpliendo así el reto formación de lo propuesto inicialmente como lo son las redes de computadores y las telecomunicaciones.

2. PLANTEAMIENTO DEL PROBLEMA

2.1. DEFINICION

Siendo las redes de comunicación un elemento importante en la administración de la información, está siendo relativamente desaprovechada por las empresas cuya sostenibilidad depende del flujo de la información relacionada con su ejercicio productivo. Por tanto, al no utilizarse el máximo de potencial en los sistemas de comunicación, se limita el rendimiento y la productividad de las empresas que de ello depende.

Por tanto, surge el siguiente interrogante: ¿De qué manera, plantear una solución tecnológica a los escenarios focalizados para optimizar su rendimiento y productividad?

El desarrollo de esta práctica, desde el planteamiento del escenario No. 1 como un problema, en el cual se expone el caso de un requerimiento de plantear una pequeña red, en la que se pretende administrar 3 puntos (routers), distribuidas en lugares diferentes, en donde se hace necesario configurar e interconectar entre si cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP en admisión de ipv4 e ipv6, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red; esto pretendió administrar de manera segura y sectorizada por medio de las VLAN, como lo son la Contabilidad, Ingeniería y administración, proveyendo así un sistema de comunicación estable y seguro, donde el flujo de información este garantizado y a su vez esta información este segura según los protocolos establecidos.

A su vez, dentro del escenario No. 2 planteado para una empresa que posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el administrador de la red, configura e implementa un esquema de comunicación y conexión de dispositivos entre sí, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red; garantizando de igual manera el flujo correcto de la información por medio de la conexión estable y segura de los dispositivos interconectados, pese a las distancias geográficas de las sucursales de la misma empresa.

En consecuencia, respondiendo a la pregunta planteada ¿De qué manera, plantear una solución tecnológica a los escenarios focalizados para optimizar su rendimiento y productividad? Se puede responder que con la ayuda del conocimiento aprendido en el curso de profundización CISCO, y con las experiencias adquiridas en los laboratorios a través de la herramienta software PACKET TRACER, se ha dado solución a cada planteamiento y mostrando a su vez el beneficio para aquellas empresas que a través de los requerimientos expuestos, se puede hacer la proyección de manera visual y practica

para ser puesta a consideración de un posible presupuesto de implementación y desarrollo en las áreas productivas de una empresa.

2.2. JUSTIFICACION

La práctica se lleva a cabo, con el fin de medir los conocimientos adquiridos durante el desarrollo del diplomado de profundización en CCNA, por medio de escenarios propuestos, exigiendo la implementación de una solución en donde se establezca la correcta configuración del direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario y la configuración e implementación correcta del protocolo de enrutamiento RIPv2 Y RIPv3 en los casos planteados.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Resolver los escenarios propuestos como trabajo final del curso de profundización UNAD CISCO CCNA CISCO aplicando los conceptos básicos aprendidos sobre las tecnologías y dispositivos de networking orientados correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

3.2 OBJETIVOS ESPECÍFICOS

- Reconocer la estructura de los modelos de capas OSI y TCP/IP, su importancia, el rol que desempeña cada nivel y su eficiencia a la hora de integrarse tecnológicamente en redes de computadores.
- Estudiar los aspectos básicos y elementos de las redes de telecomunicación y de las técnicas de conmutación, así como los principales protocolos y servicios de seguridad en redes.
- Analizar los conceptos relacionados con la arquitectura, funciones, componentes y modelos de Internet y otras redes de computadores.
- Configurar una prioridad de routers, RID y el enrutamiento OSPF.

4. Descripción de escenarios propuestos para la prueba de habilidades

4.1 Escenario 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

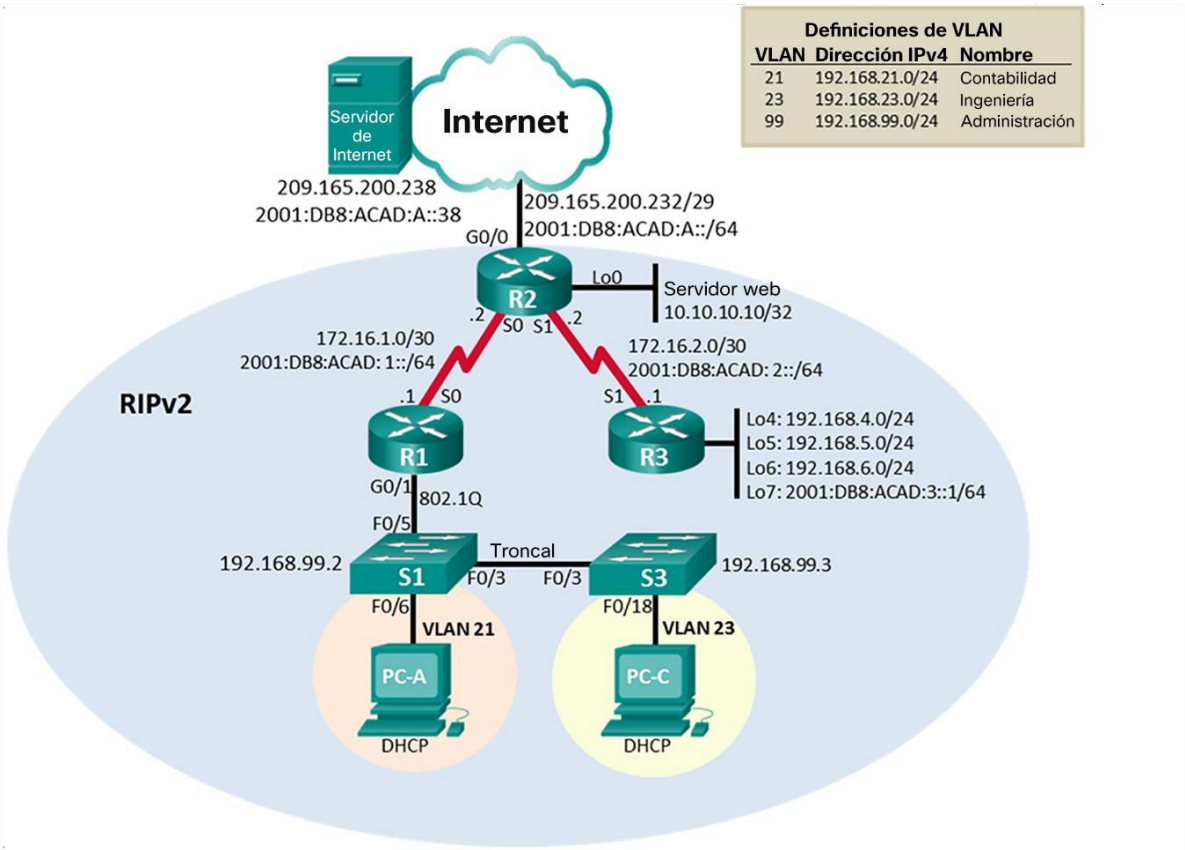


Figura 1 Propuesta del Escenario 1

4.1.1 Parte 1: Inicializar dispositivos

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

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

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

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	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 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	Dir flash

Tabla 1 Inicialización de Routers y Switches

R1:

R1#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

R1#reload

Proceed with reload? [confirm]

R2:

R2#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

R2#reload

Proceed with reload? [confirm]

R3:

R3#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

R3#reload

Proceed with reload? [confirm]

S1:

S1#Erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

S1#Delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

S3:

S3#Erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

S3#Delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm

4.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

4.1.2.1 Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2 Configuración IP de la Computadora de Internet

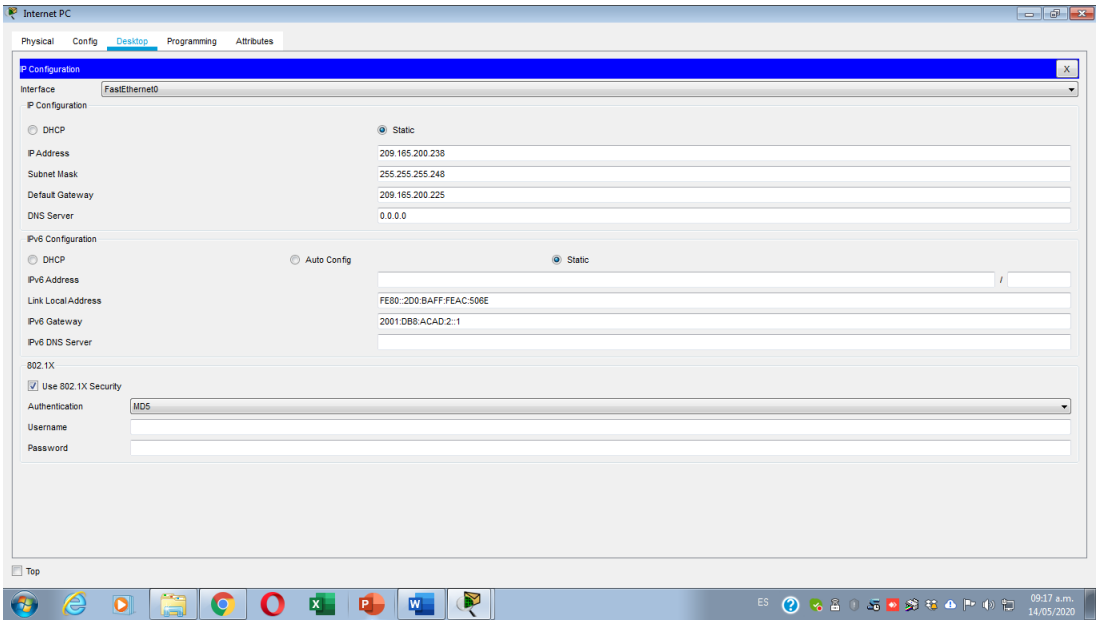


Figura 2 Direccionamiento IP del Servidor

4.1.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En Conf t No ip domain-lookup
Nombre del router	Hostname R1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Pass cisco
Contraseña de acceso Telnet	Line vty 0 4 Pass cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/0	Int s0/0/0 Description Connetion to R2 Ip add 172.16.1.1 255.255.255.252 Ipv6 add 20001:DB8:ACAD:1::/64 Clock rate 128000 No shutdown
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/0 Ipv6 route ::0/0 s0/0/0

Tabla 3 Configuración del Router 1

Nota: Todavía no configure G0/1.

4.1.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En Conf t No ip domain-lookup

Nombre del router	Hostname R2
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Pass cisco
Contraseña de acceso Telnet	Line vty 0 4 Pass cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Habilitar el servidor HTTP	Ip http server
Mensaje MOTD	Banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/0	Int s0/0/0 Description Connetion to R1 Ip add 172.16.1.2 255.255.255.252 Ipv6 add 20001:DB8:ACAD:2::/64 No shutdown
Interfaz S0/0/1	Int s0/0/0 Description Connetion to R3 Ip add 172.16.2.2 255.255.255.252 Ipv6 add 20001:DB8:ACAD:2::/64 Clock rate 128000 No shutdown
Interfaz G0/0 (simulación de Internet)	Int g0/0 Description Connetion to ISP Ip add 209.165.200.233 255.255.255.248 Ipv6 add 2001:DB8:ACAD:2::1/64 No shutdown
Interfaz loopback 0 (servidor web simulado)	Interface loopback 0 Ip add 10.10.10.12 255.255.255.252 No shutdown
Ruta predeterminada	description Connetion to Web Server ip route 0.0.0.0 0.0.0.0. g0/0 ipv6 router ::0/0 g0/0 end

Tabla 4 Configuración del Router 2

4.1.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En Conf t No ip domain-lookup
Nombre del router	Hostname R3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Pass cisco
Contraseña de acceso Telnet	Line vty 0 4 Pass cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $Se prohíbe el acceso no autorizado.$
Interfaz S0/0/1	Int s0/0/1 Description Connetion to R2 Ip add 172.16.2.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:1::/64 No shutdown
Interfaz loopback 4	Int loopback 4 Ip add 192.168.4.1 255.255.255.0 No shutdown
Interfaz loopback 5	Int l loopback 5 Ip add 192.168.5.1 255.255.255.0 No shutdown
Interfaz loopback 6	Int loopback 6 Ip add 192.168.6.1 255.255.255.0 No shutdown
Interfaz loopback 7	Int loopback 7 Ipv6 address 2001:DB8:ACAD:3::1/64 No shutdown

Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/1 Ipv6 route ::0/0 s0/0/0 end

Tabla 5 Configuración del Router 3

4.1.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En Conf t No ip domain-lookup
Nombre del switch	Hostname S1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Pass cisco login
Contraseña de acceso Telnet	Line vty 0 4 Pass cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $Se prohíbe el acceso no autorizado.$

Tabla 6 Configuración del Switch 1

4.1.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En Conf t No ip domain-lookup
Nombre del switch	Hostname S3

Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line con 0 Pass cisco login
Contraseña de acceso Telnet	Line vty 0 4 Pass cisco Login exit
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd $Se prohíbe el acceso no autorizado.$

Tabla 7 Configuración del Switch 3

4.1.2.7 Paso 7: Verificar la conectividad de la red

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

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

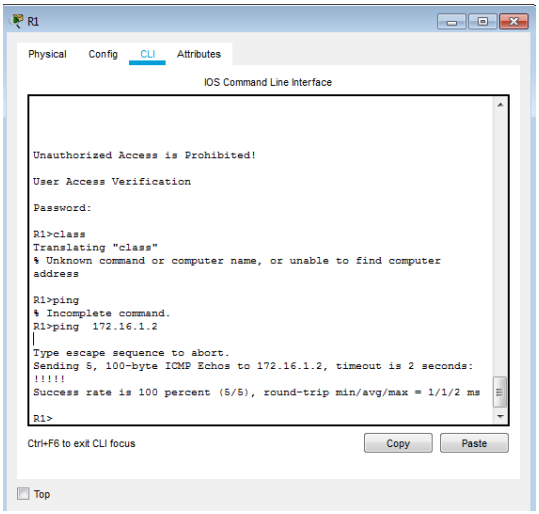
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.12.2	

Figura 3 Resultados ping de R1 a R2

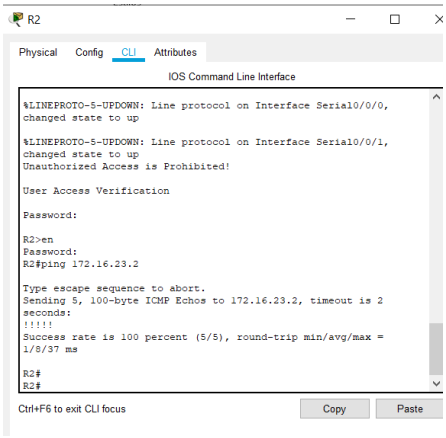
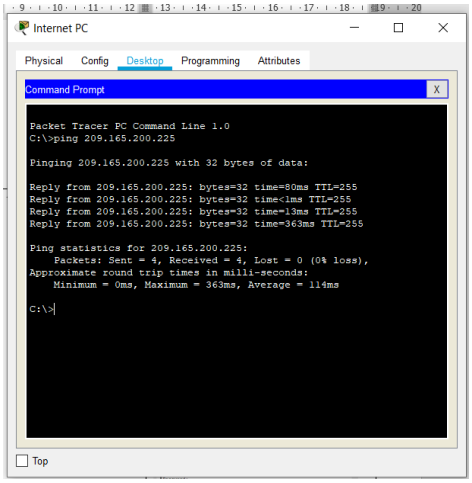
R2	R3, S0/0/1	172.16.23.2	 *Figura 4 Resultados ping de R2 a R3*
PC de Internet	Gateway predeterminado	200.165.200.225	 *Figura 5 Resultados ping Pc de Internet*

Tabla 8 Verificación la conectividad de la red

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

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

4.1.3.1 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	Vlan 21 Name Contabilidad Vlan 23 Name Ingenieria Vlan 99 Name Administracion
Asignar la dirección IP de administración.	Int vlan 99 Ip add 192.168.99.2 255.255.255.0 No shutdown
Asignar el gateway predeterminado	Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Int f0/3 switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Int f0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range fa0/1 - 2, fa0/4, fa0/6 - 24, g0/1 – 2 switchport mode access
Asignar F0/6 a la VLAN 21	Int fa0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	int range fa0/1 - 2, fa0/4, fa0/7 - 24, g0/1 – 2 shutdown

Tabla 9 Configuración de la seguridad del switch 1

4.1.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Vlan 21 Name Contabilidad Vlan 23 Name Ingeneria Vlan 99 Name Administracion
Asignar la dirección IP de administración	Int vlan 99 Ip add 192.168.99.3 255.255.255.0 No shutdown
Asignar el gateway predeterminado.	Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Int fa0/3 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range fa0/1 - 2, fa0/4, fa0/6 - 24, g0/1 – 2 switchport mode access
Asignar F0/18 a la VLAN 21	Int fa0/18 Switchport mode access Switchport access vlan 21
Apagar todos los puertos sin usar	int range fa0/1 - 2, fa0/4 - 17, fa0/19 - 24, g0/1 - 2 Shutdown

Tabla 10 Configuración de la seguridad del switch 3

4.1.3.3 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#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1 R1(config-if)#no shut R1(config-if)#exit R1(config)#int g0/1.21 R1(config-subif)#Encapsulation dot1q 21 R1(config-subif)#description LAN contabilidad R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#Encapsulation dot1q 23 R1(config-subif)#description LAN ingenieria R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#exit R1(config)#
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#Encapsulation dot1q 99 R1(config-subif)#description LAN administracion R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit R1(config)#
Activar la interfaz G0/1	Int g0/1 No shutdown

Tabla 11 Configuración de la seguridad del Router 1

4.1.3.4 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:

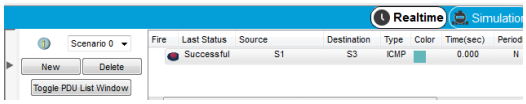
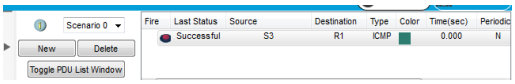
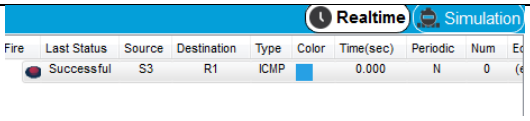
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	Ping 192.168.99.1	 *Figura 6 Resultados ping de S1 a R1*
S3	R1, dirección VLAN 99	Ping 192.168.99.1	 *Figura 7 Resultados ping de S3 a R1*
S1	R1, dirección VLAN 31	192.168.31.1	 *Figura 8 Resultados ping de S1 a R1por Vlan 31*
S3	R1, dirección VLAN 33	192.168.33.1	 *Figura 9 Resultados ping de S3 a R1por Vlan 33*

Tabla 12 Verificación la conectividad de la red despues de Seguridad

4.1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2

4.1.4.1 Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1>en Password: R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router rip R1(config-router)#version 2

Anunciar las redes conectadas directamente	R1(config-router)#do show ip route conne C 172.16.12.0/30 is directly connected, Serial0/0/0 C 192.168.31.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.33.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.31.0 R1(config-router)#network 192.168.33.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 13 Configuración de RIPv2 en el R1

4.1.4.2 Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2>en Password: R2#conf t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#router rip R2(config-router)#version 2

Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config)#do show ip route conne C 10.10.10.0/24 is directly connected, GigabitEthernet0/1 C 172.16.1.0/30 is directly connected, Serial0/0/0 C 172.16.2.0/30 is directly connected, Serial0/0/1 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0 R2(config-router)#net 10.10.10.0 R2(config-router)#net 172.16.1.0 R2(config-router)#net 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 14 Configuración de RIPv2 en el R2

4.1.4.3 Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route conne C 176.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6 R3(config-router)#net 172.16.2.0 R3(config-router)#net 192.168.4.0 R3(config-router)#net 192.168.5.0 R3(config-router)#net 192.168.6.0 R3(config-router)# R3(config-router)#exit

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	no auto-summary

Tabla 15 Configuración de RIPv3 en el R2

4.1.4.4 Paso 4: Verificar la información de RIP

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

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

Tabla 16 Verificación de RIP

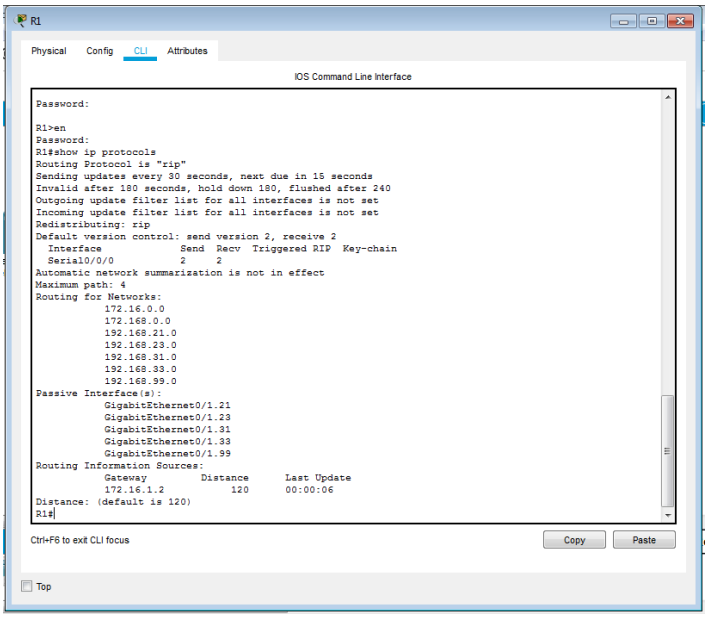


Figura 10 Verificación de RIP en R1

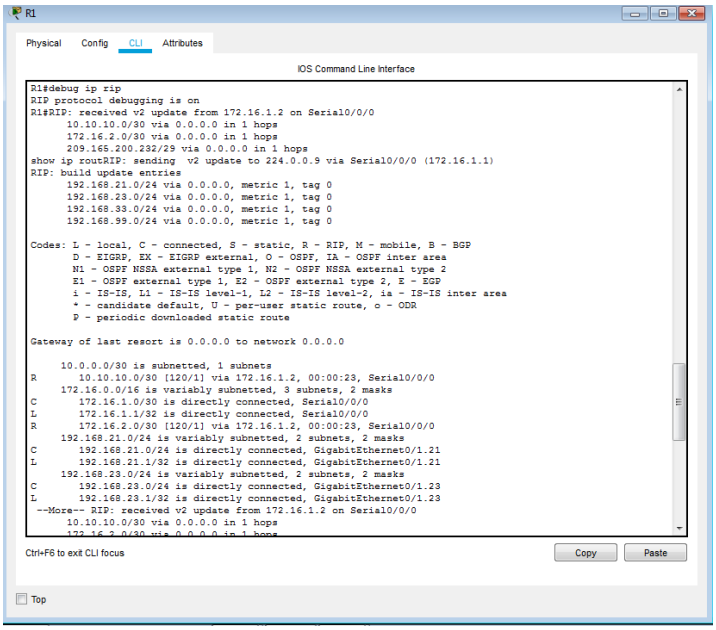


Figura 11 Verificación de Rutas Rip en R1

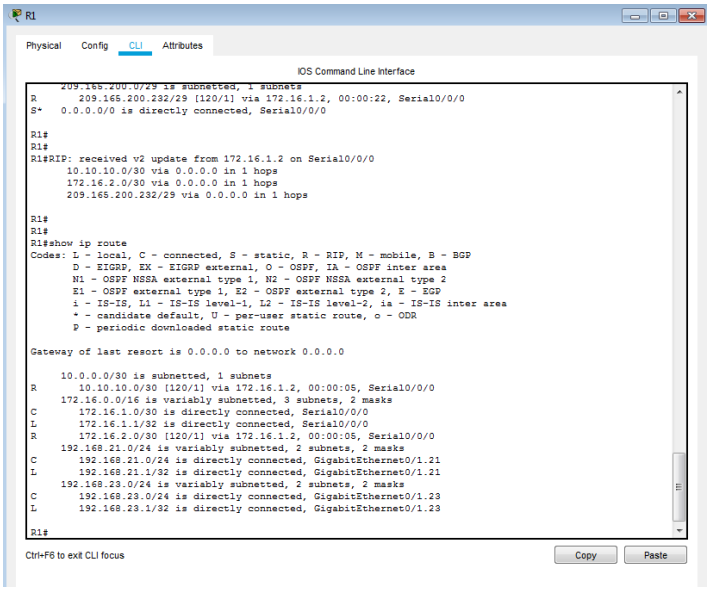


Figura 12 RIP de la configuración en ejecución en R1

4.1.5 Implementar DHCP y NAT para IPv4

4.1.5.1 Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

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

Tabla 17 Figura 6 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

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

La configuración del R2 incluye las siguientes tareas:

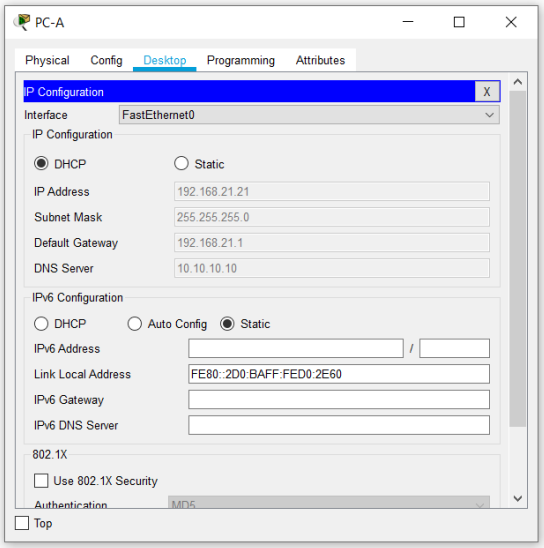
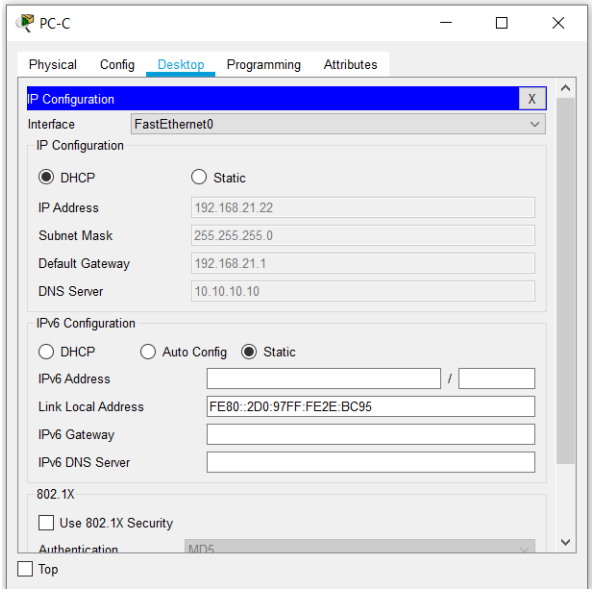
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#user webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#int g0/1 R2(config-if)#ip address 10.10.10.1 255.255.255.252 R2(config-if)#des Conectado al web server R2(config-if)#no shut R2(config-if)#
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config-if)#ip nat inside source static 10.10.10.2 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 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** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 18 Configuración de la NAT estática y dinámica en el R2

4.1.5.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Figura 13 Verificación de Asignación de IP por DHCP dinámica en PC- A*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Figura 14 Verificación de Asignación de IP por DHCP dinámica en PC- C*

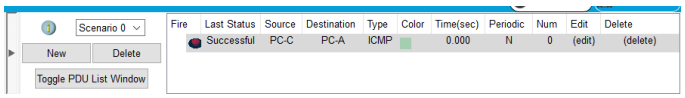
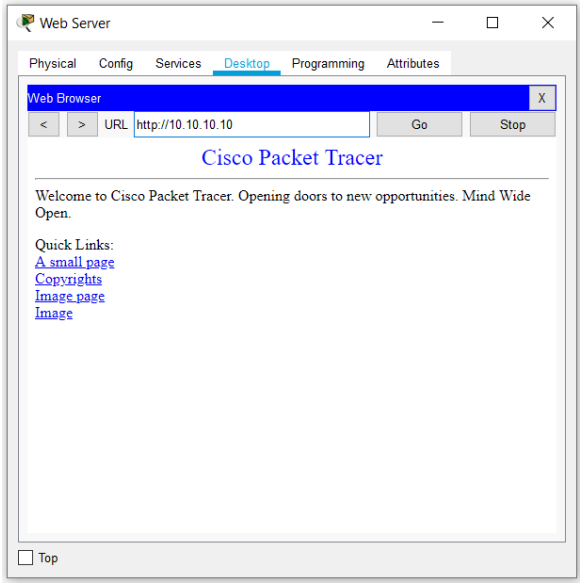
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Figura 15 Verificación de de ping PC - a a PC- C*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	 *Figura 16 Verificación de acceso al servidor Web*

Tabla 19 Verificación del protocolo DHCP y la NAT estática

4.1.6 Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2>en Password: R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2#ntp master 5 ^ % Invalid input detected at '^' marker. R2#ntp master stratum 5 ^ % Invalid input detected at '^' marker. R2#

Configurar R1 como un cliente NTP.	Servidor: **R2** R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ntp server % Incomplete command. R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#exit
Verifique la configuración de NTP en R1.	R1#do show ntp status ^% Invalid input detected at '^' marker

Tabla 20 Configuración de NTP

4.1.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL)

4.1.7.1 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	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit R2(config)#

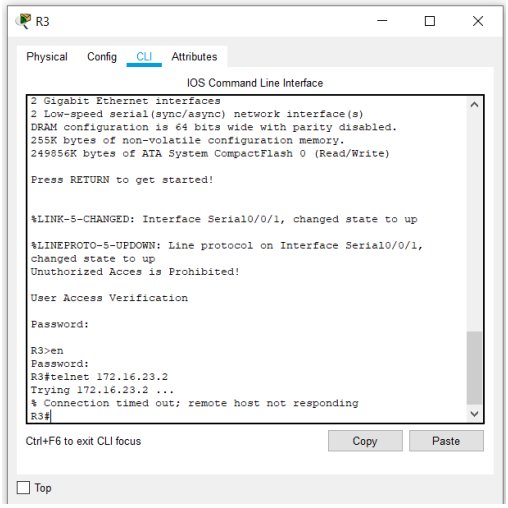
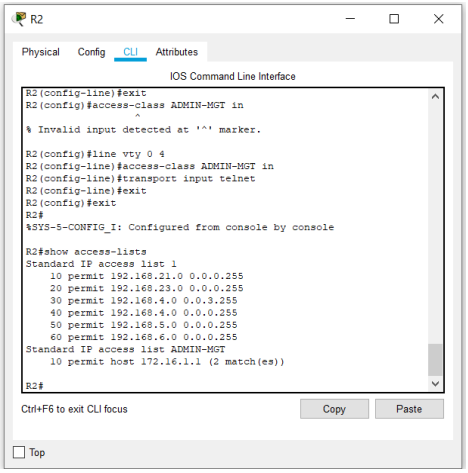
Verificar que la ACL funcione como se espera	 *Figura 17 Verificación de funcionamiento de ACL*

Tabla 21 Restricción del acceso a las líneas VTY en el R2

4.1.7.2 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	 *Figura 18 Verificación de lista de acceso en R2*
Restablecer los contadores de una lista de acceso	R1(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1(config)#interface Fa0/1 R1(config-if)#ip access-group 1 out

¿Con qué comando se muestran las traducciones NAT? 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 se 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.	R1(config)#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

Tabla 22 Verificación de Comandos y resultados

4.2 Escenario 2

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

Topología de red

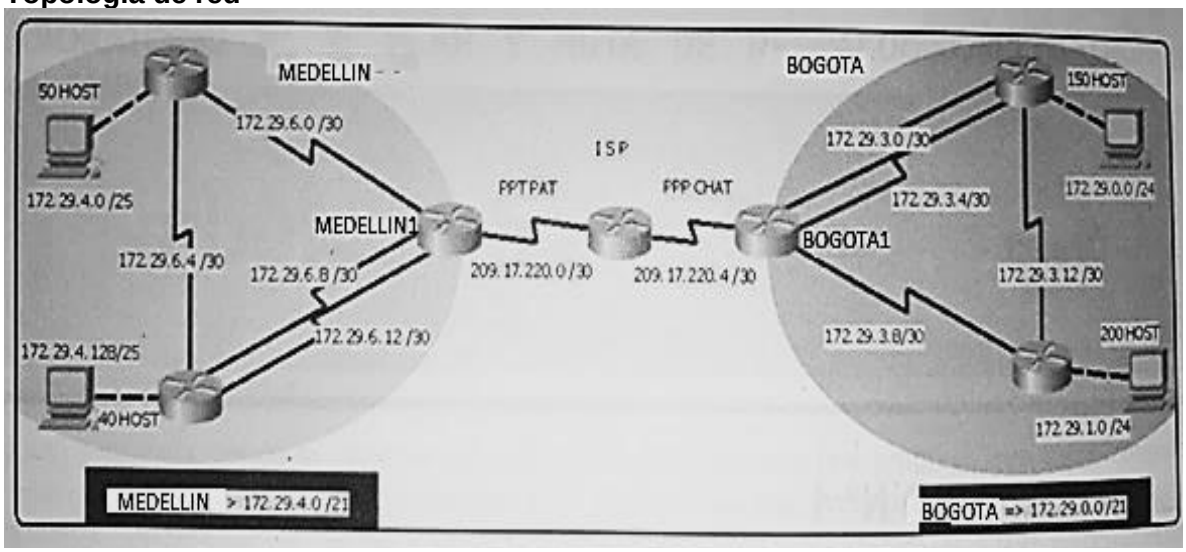


Figura 19 Planteamiento del Escenario 2

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

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

4.2.1 Parte 1: Configuración del enrutamiento

```
Router(config)#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#enable secret class
Router(config)#banner motd $Prohibido el acceso no autorizado!$
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)# Hostname ISP
```

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

Bogotá 1

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#no auto-summary
```

Medellin 1

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 2.2.2.2
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
```

MEDELLIN1(config-router)#no auto-summary

Bogotá 2

BOGOTA2(config)#router ospf 1

BOGOTA2(config-router)#router-id 3.3.3.3

BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 0

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 0

BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0

BOGOTA2(config-router)#no auto-summary

BOGOTA2(config-router)#passive-interface g0/0

Bogotá 3

BOGOTA3(config)#router ospf 1

BOGOTA3(config-router)#router-id 4.4.4.4

BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 0

BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 0

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 0

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0

BOGOTA3(config-router)#no auto-summary

BOGOTA3(config-router)#passive-interface g0/0

Medellin 2

MEDELLIN2(config)#router ospf 1

MEDELLIN2(config-router)#router-id 5.5.5.5

MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 0

MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0

MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.3 area 0

MEDELLIN2(config-router)#no auto-summary

MEDELLIN2(config-router)#passive-interface g0/0

Medellin 3

MEDELLIN3(config)#router ospf 1

MEDELLIN3(config-router)#router-id 6.6.6.6

MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.255 area 0

MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0

MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0

MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0

MEDELLIN3(config-router)#passive-interface g0/0

MEDELLIN3(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.

Bogotá 1

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0

BOGOTA1(config)#router ospf 1

BOGOTA1(config-router)#default-information originate

Medellin 1

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1

MEDELLIN1(config)#router ospf 1

MEDELLIN1(config-router)#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.

ISP(config)#ip route 172.29.4.0 255.255.252.0 serial0/0/1

ISP(config)#ip route 172.29.0.0 255.255.252.0 serial0/0/0

4.2.2 Parte 2: Tabla de Enrutamiento.

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

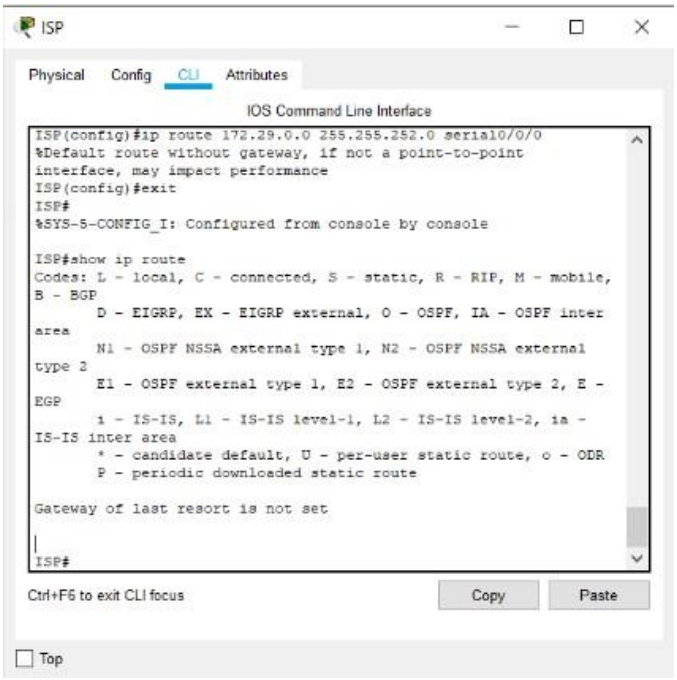


Figura 20 Verificación de la tabla de enrutamiento en ISP

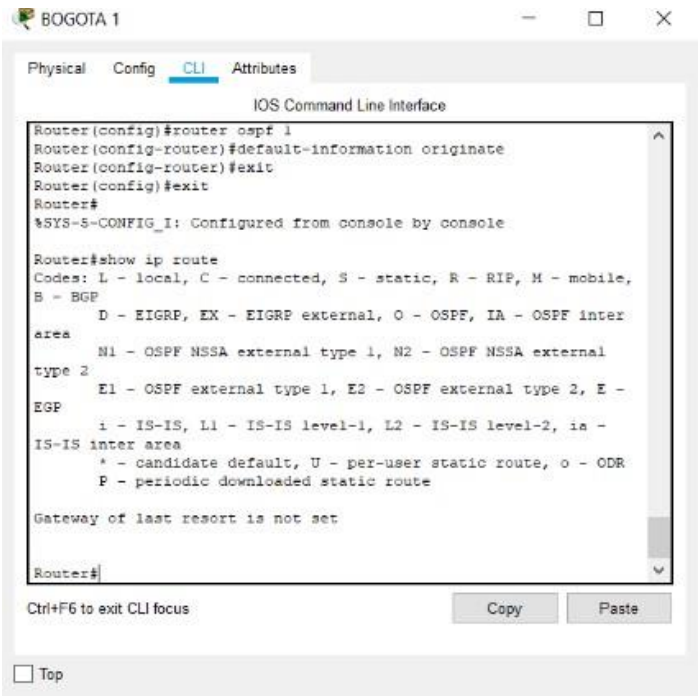


Figura 21 Verificación de la tabla de enrutamiento en Bogotá 1

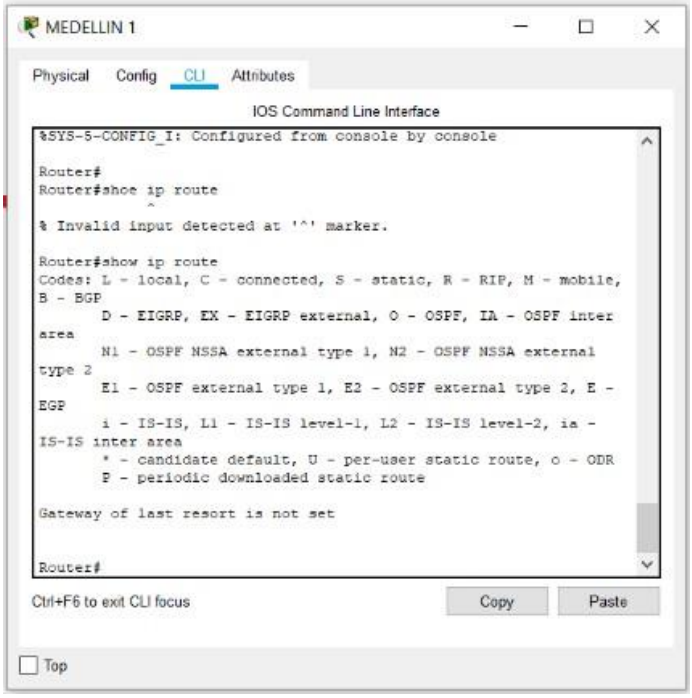


Figura 22 Verificación de la tabla de enrutamiento en MEDELLIN 1

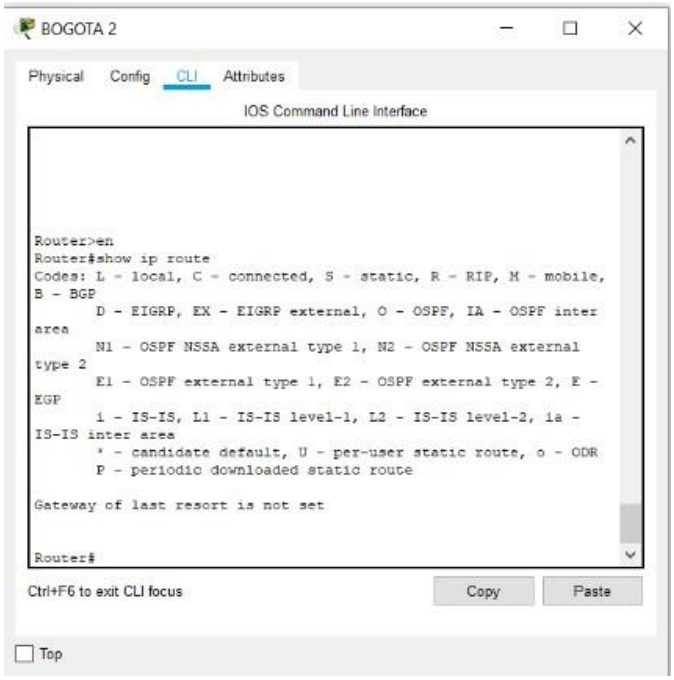


Figura 23 Verificación de la tabla de enrutamiento en BOGOTA 2

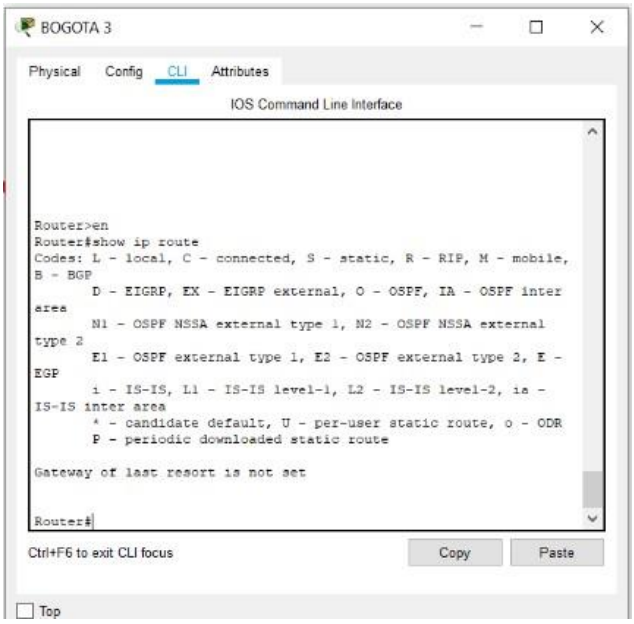


Figura 24 Verificación de la tabla de enrutamiento en BOGOTA 3

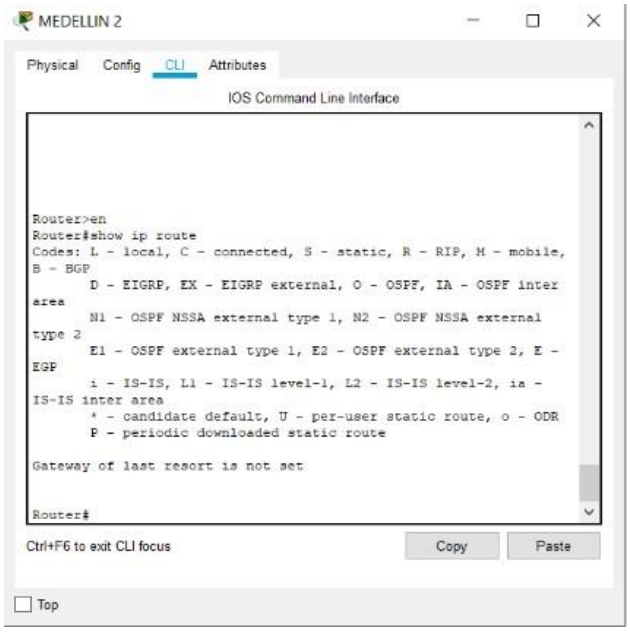


Figura 25 Verificación de la tabla de enrutamiento en MEDELLIN 2

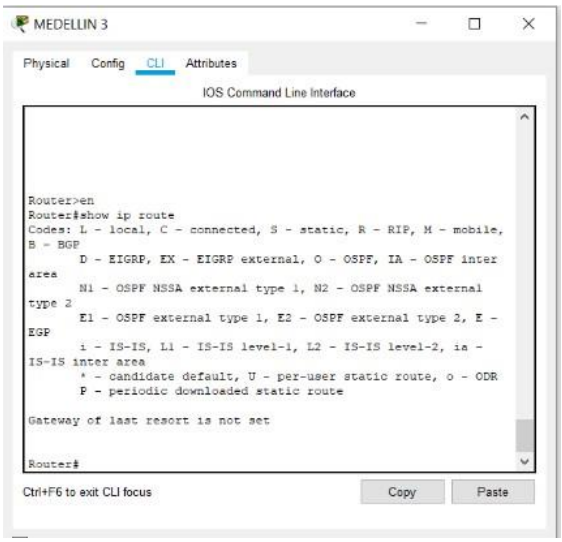


Figura 26 Verificación de la tabla de enrutamiento en MEDELLIN 3

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

ISP

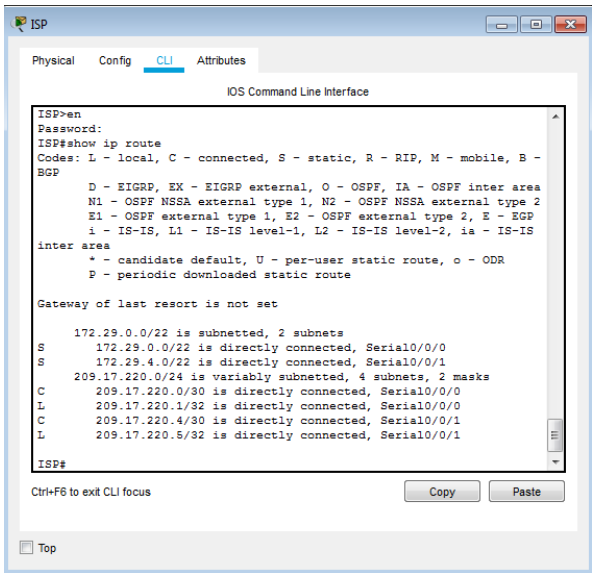


Figura 27 Verificación de la tabla de enrutamiento en ISP

Bogota 1

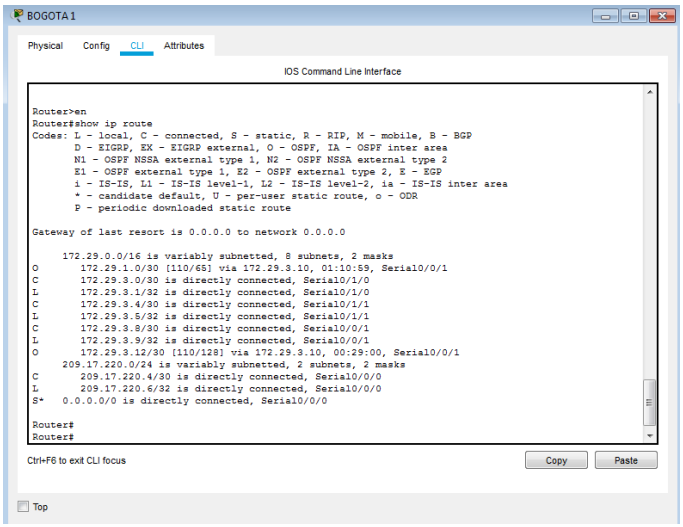


Figura 28 Verificación de la tabla de enrutamiento en BOGOTA 1

Bogota 2

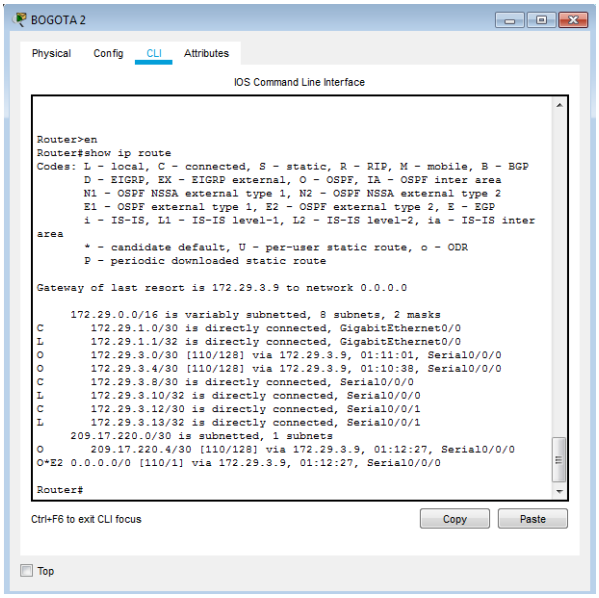


Figura 29 Verificación de la tabla de enrutamiento en BOGOTA 2

Bogota 3

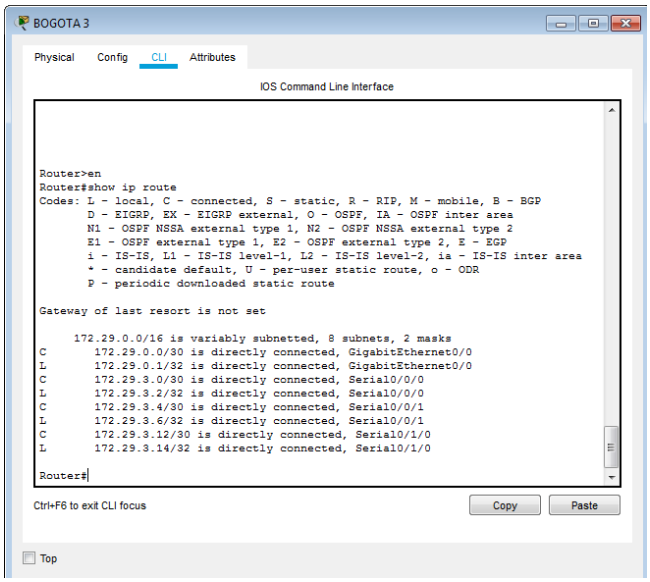


Figura 30 Verificación de la tabla de enrutamiento en BOGOTA 3

Medellin 1

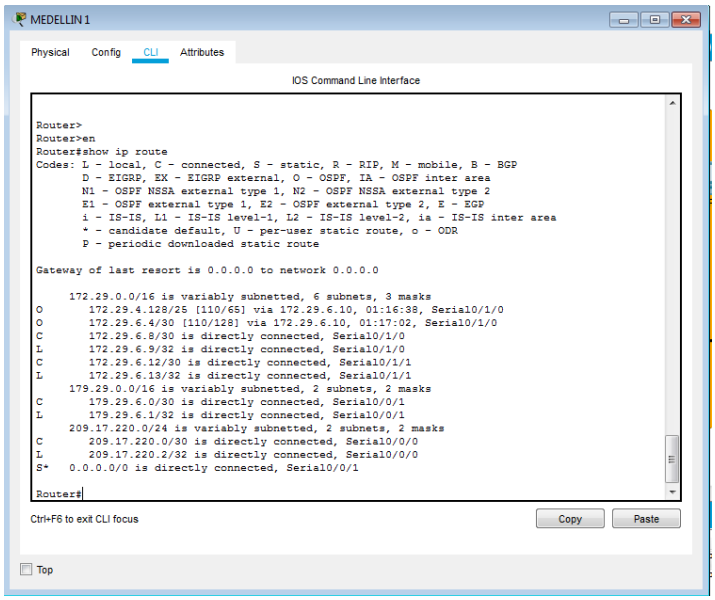


Figura 31 Verificación de la tabla de enrutamiento en MEDELLIN 1

Medellin 2

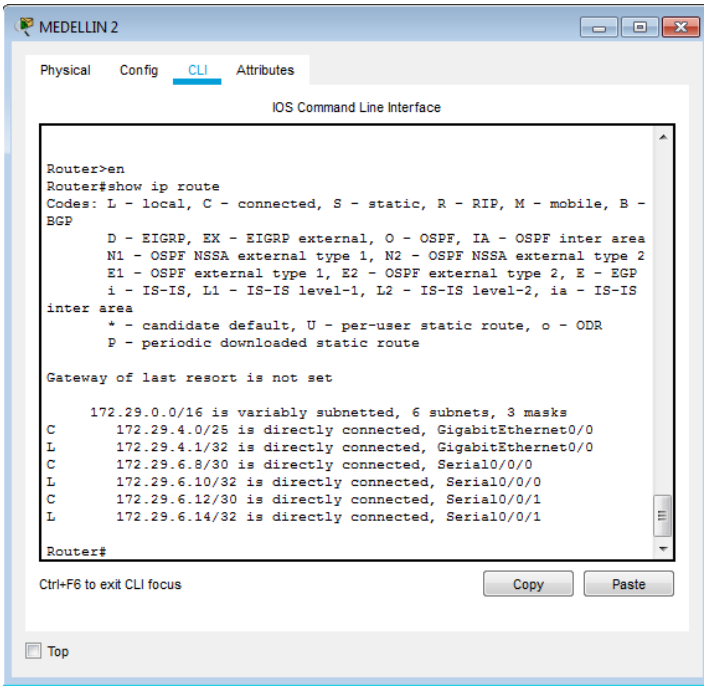


Figura 32 Verificación de la tabla de enrutamiento en MEDELLIN 2

Medellin 3

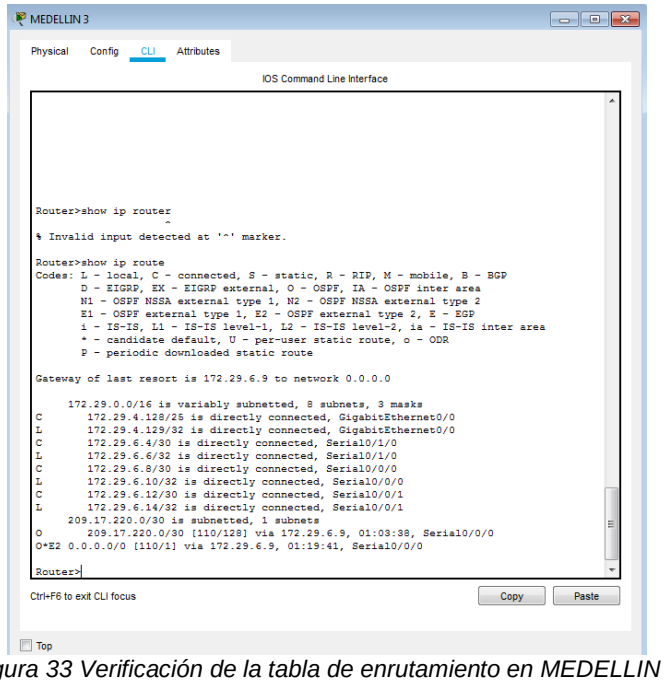


Figura 33 Verificación de la tabla de enrutamiento en MEDELLIN 3

4.2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Tabla 23 Interfaces de cada router que no necesitan desactivación

4.2.4 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.

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.

4.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#interface s0/0/1
ISP(config-if)#encapsulation PPP
ISP(config-if)#PPP authentication PAP
ISP(config-if)#PPP PAP sent-username ISP password cisco

MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#interface s0/0/1
MEDELLIN1(config-if)#encapsulation PPP
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
```

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

```
ISP(config)#username BOGOTA1 password cisco
ISP(config)#interface s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap


BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
```

4.2.6 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.

```
BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#interface s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit

MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/1 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#interface s0/0/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#interface s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#interface s0/1/1
MEDELLIN1(config-if)#ip nat inside
```

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.

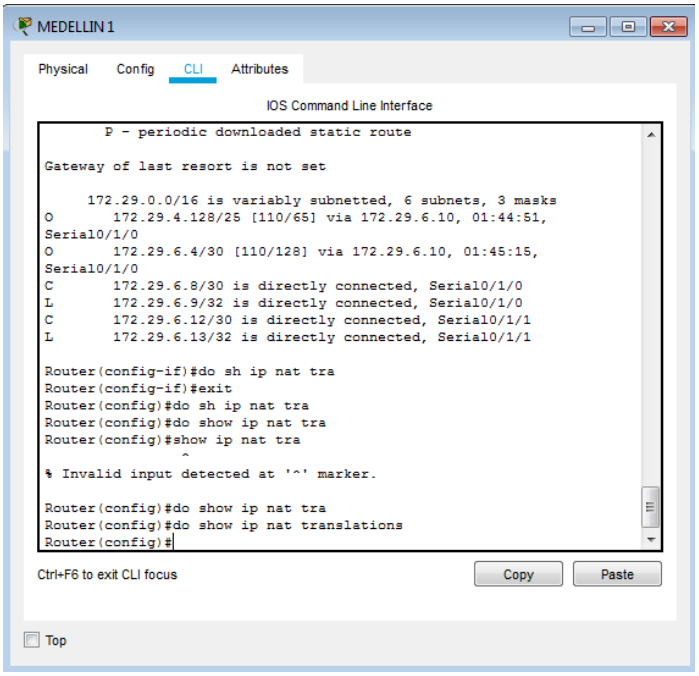


Figura 34 Comprobación y verificación que la traducción de direcciones

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.

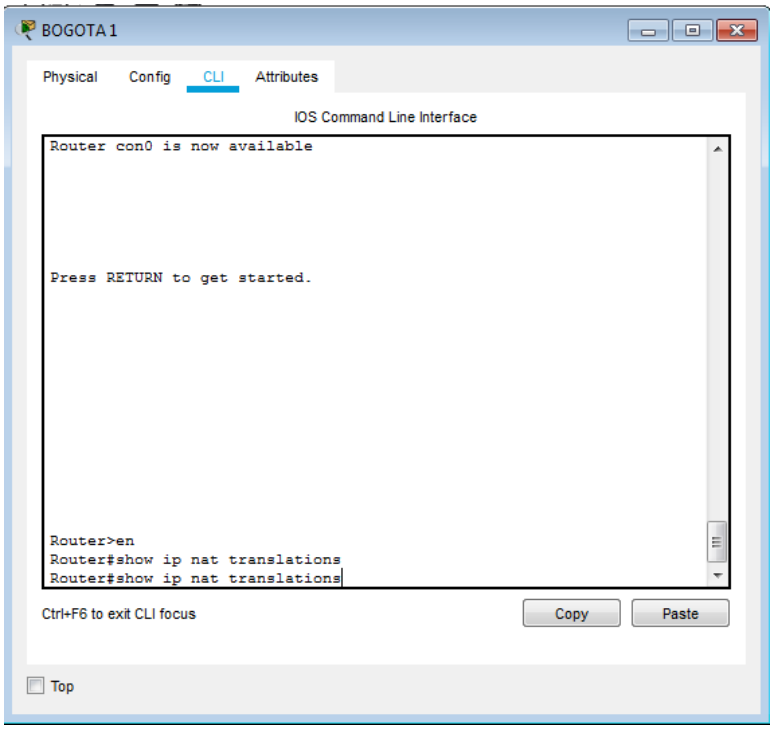


Figura 35 Comprobación y verificación que la traducción de direcciones en Bogotá 1

4.2.7 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.

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-route 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 7.7.7.7
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-route 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 7.7.7.7
MEDELLIN2(dhcp-config)#exit
```

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

MEDELLIN3(config)#interface g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.4.1

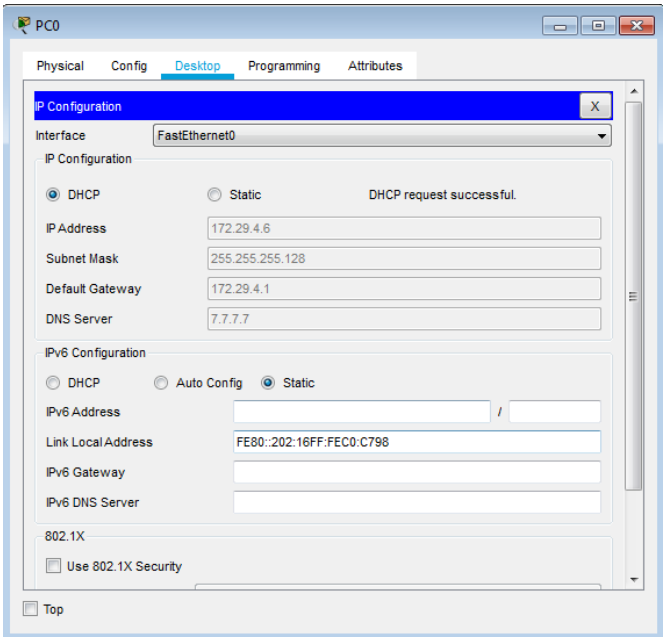


Figura 36 Verificación de asignación de ip por DCHP en el PC MEDELLIN 50 HOST

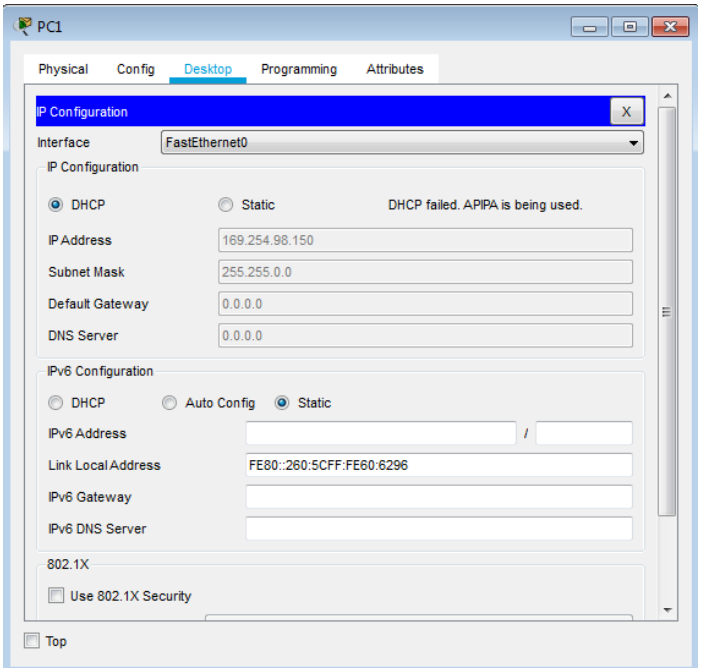


Figura 37 Verificación de asignación de ip por DCHP en el PC MEDELLIN 40 HOST

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

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-route 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 7.7.7.7
BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-route 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 7.7.7.7
BOGOTA2(dhcp-config)#exit
```

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

```
BOGOTA3(config)#interface g0/0
BOGOTA3(config-if)#ip helper-address 172.29.1.1
BOGOTA3(config-if)#exit
```

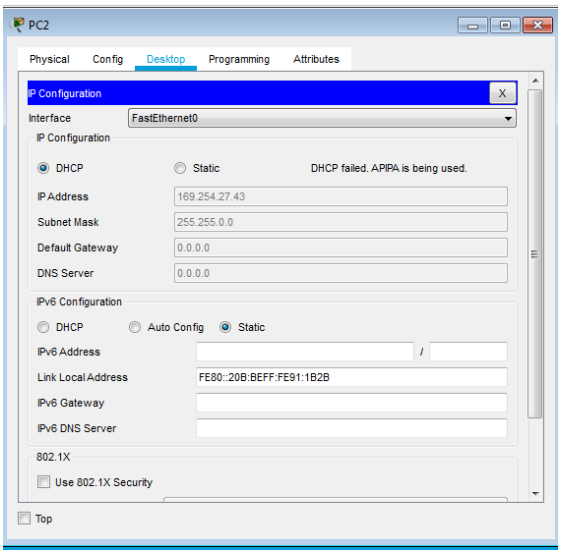


Figura 38 Verificación de asignación de ip por DCHP en el PC BOGOTA 150 HOST

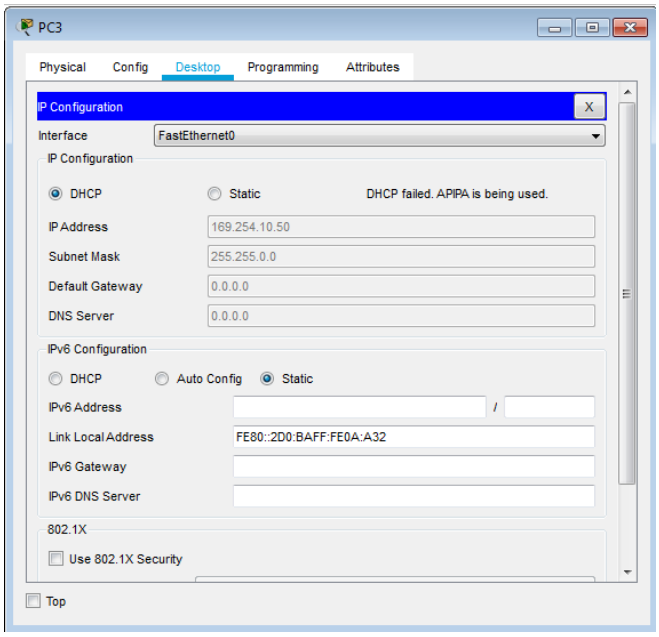


Figura 39 Verificación de asignación de ip por DCHP en el PC BOGOTA 200 HOST

CONCLUSIONES

En el desarrollo de esta prueba de Habilidades, se presenta de manera ordenada e ilustrativa de una forma de concebir los planteamientos necesarios para dar funcionamiento óptimo a los escenarios planteados, tratando siempre de mantener las buenas prácticas en las configuraciones e implementaciones de los materiales requeridos.
De igual manera se hacen las pruebas necesarias de verificación de conexiones y respuestas, y también de los cambios aplicados a medida del desarrollo del proceso de implementación; ejecutando funciones como la de verificar una conexión entre los dispositivos proporcionada en la configuración inicial de la topología.

En la explicación del paso a paso se dan las instrucciones para la resolución de los ejercicios, en los cuales se aplicó diferentes estructuras como, por ejemplo, se armó una topología simple mediante cableado LAN Ethernet, se accedió a diferentes routers Cisco para su configuración, utilizando los métodos de acceso de consola, también se visualizó la configuración predeterminada de cada componente, antes de configurar los parámetros básicos.

En el caso de la implementación del servidor para la asignación de la direcciones de red DHCP es muy se presenta la asignación de direcciones de red, por esto el servidor o como en este caso un router que hace las veces del servidor es esencial al momento de asignar direcciones de red a una gran cantidad de ordenadores y así evitar el trabajo de asignarlas manualmente.

BIBLIOGRAFÍA

Cisco Networking Academy, MODULO DE ESTUDIO CCNA1(Network Fundamentals). Recuperado de: http://www.mediafire.com/?9cq9h4jo23c1359

Cisco Networking Academy, MODULO DE ESTUDIO CCNA2 (Routing Protocols and Concepts). Recuperado de: http://www.mediafire.com/?5y052miul2vezhj

Cisco CCNA – configuración DHCP en un router. Recuperado de: http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-encisco-router/

Cisco CCNA - configuración troncal 802.1Q. En un switch recuperado de: https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-seriesswitches/24064- 171.html

CISCO. CCNA. Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

Reyes Reynaud, M, A. 2011. Calculo de Subredes de México. [Video] recuperado de: http://www.youtube.com/watch?v=Z7DM639rAmQ&list=PLaXGHu_K17nuWSyLNRtX7UvR2LcpTB K7P&index=5