IDENTIFICACIÓN Y APLICACIÓN DE SOLUCIÓN A SITUACIÓN DE PROBLEMAS DE NETWORKING

EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA

MARIELA MARGARITA CAMPO HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS
INGENIERÍA DE SISTEMAS
VALLEDUPAR
2020

IDENTIFICACIÓN Y APLICACIÓN DE SOLUCIN A SITUACIÓN DE PROBLEMAS DE NETWORKING

EVALUACIÓN – PRUEBA DE HABILIDADES PRACTICAS CCNA

MARIELA MARGARITA CAMPO HERRERA

DIPLOMADO DE PROFUNDIZACIÓN CISCO
DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WLAN

TUTOR
HÉCTOR JULIÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS
INGENIERÍA DE SISTEMAS
VALLEDUPAR
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, 22 de mayo de 2020

El presente trabajo está dedicado a mi familia por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

AGRADECIMIENTOS

Agradezco a Dios por bendecir mi vida, por guiarme a lo largo de mi existencia, por ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mi madre: Martha Herrera, por ser la principal promotora de este sueño, por confiar y creer en mis expectativas, por los consejos, y principios que me ha inculcado.

Agradezco a docentes de la Escuela de Ingeniería de la Universidad Nacional abierta y a distancia Unad , por haber compartido sus conocimientos a lo largo de la preparación de mi profesión, de manera especial.

CONTENIDO

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL - Access Control List. Lista de Control de Acceso. Un ACL es una lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto. Un ACL define cuales usuarios y cuales grupos pueden accesar y que tipo de operaciones pueden realizar una vez dentro. Estas operaciones usualmente incluyen lectura, escritura y ejecución. Por ejemplo, si un ACL especifica un acceso de solo-lectura para un usuario sobre un archivo, el usuario podra abrir el archivo, pero no podra grabar encima o ejecutar el archivo. Las listas de control de acceso proporcionan un buen método para manejar los permisos de los archivos y carpetas. Son usadas por la mayoría de los sistemas operativos, incluyéndo Windows, Mac y Unix.

CISCO: Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

DHCP: Siglas del inglés "Dynamic Host Configuration Protocol." Protocolo Dinámico de Configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

NAT: Network Address Translation o Network Address Translator es la traducción de IPs privados de una red en IP públicos, para que la red pueda enviar paquetes al exterior, y viceversa.

IP: Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10.

IPv4: IPv4 es la cuarta revisión del Protocolo de Internet y la más usada hoy en día. Usa direcciones de 32 bits, con el formato "111.111.111.111." Cada sección puede contener un numero de 0 hasta 255, lo cual da un total de 4,294,967,296 (2^32) direcciones IP posibles.

IPv6: Con el crecimiento exponencial de las computadoras, el sistema de direcciones IP, IPv4, se va a quedar sin direcciones IP. Entra en acción IPv6, también llamado IPng (IP Next Generation - IP de Nueva Generación); es la siguiente versión planificada para el sistema de direcciones IP.

RESUMEN

El desarrollo del presente contenido, está basado en la evaluación de prueba de habilidades prácticas CCNA, desde el cual se selecciona un escenario de una pequeña empresa, para establecer la configuración de red, de una pequeña empresa, la cual tiene oficinas en 3 ciudades distintas. La metodología que se aplica, es de tipo mixto, porque se cualifica, cuantifica y se miden los procesos, para saber cómo se aplican los protocolos administrativos y las políticas de seguridad, que conlleven a evitar ataques de equipos remotos y se evite infiltración dentro de los bancos de datos de información y su servidor, y en específico la parte de la información manejada dentro de los equipos de cómputo de la empresa; Se concluye que todo este proceso se establece con los protocolos adecuados desde los cuales se identifican las líneas de acceso remoto y todo los procesos que permiten el control de acceso a los equipos de la empresa, así mismo, se hace un proceso de verificación de las redes nativas NAT y de los protocolos dinámicos de configuración de host para asignar direcciones dinámicas DHCP a diferentes computadoras, en este caso 3 y se puede hacer un proceso de traducción de IPs privados, estando en una red pública, lo que le permite tener un adecuado nivel de seguridad.

PALABRAS CLAVE: Configuración, IP, políticas administrativas, protocolo, redes nativas, seguridad.

1. INTRODUCCIÓN

El desarrollo de la actividad final de prueba del diplomado denominado PRUEBA DE HABILIDADES PRÁCTICAS CCNA, constituye un elemento práctico que, contribuye a reconocer las habilidades adquiridas y la construcción de conocimientos, dentro del contexto de las redes y la forma de, cómo se puede lograr colocar en práctica todo este tipo de habilidades.

De igual manera se realiza la configuración de los servidores DHCP, dentro de los cuales existe un protocolo de configuración que se trabaja de forma predeterminada desde su paquetes los cuales no pasan a través de los enrutadores por lo que necesita un agente de transmisión DHCP el cual recibe en cualquier tipo de difusión DHCP dentro de la subred y realiza el reenvío hacia la dirección IP específica en una subred distinta.

En esta forma se identifican las redes de los datos que se usan dentro de los procesos diarios y lo que permite que exista una apropiación de los conocimientos desde redes locales hasta las grandes redes a nivel interglobal. Todo este proceso se puede desarrollar, desde una pequeña oficina o bien dentro de una empresa, industria o centros de educación superior o colegios que requieren manejar grandes flujos de datos entre un conjunto mayor de equipos de comunicación y computadoras.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Identificar y aplicar una solución a un caso o situación estudio de problema de Networking

2.2 OBJETIVOS ESPECÍFICOS

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en Switch, elaboración de Vlans e inter Vlan Routing.
- Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación. Configurar y verificar listas de control de acceso ACL.
- Verificar conectividad entre los dispositivos de una topología.

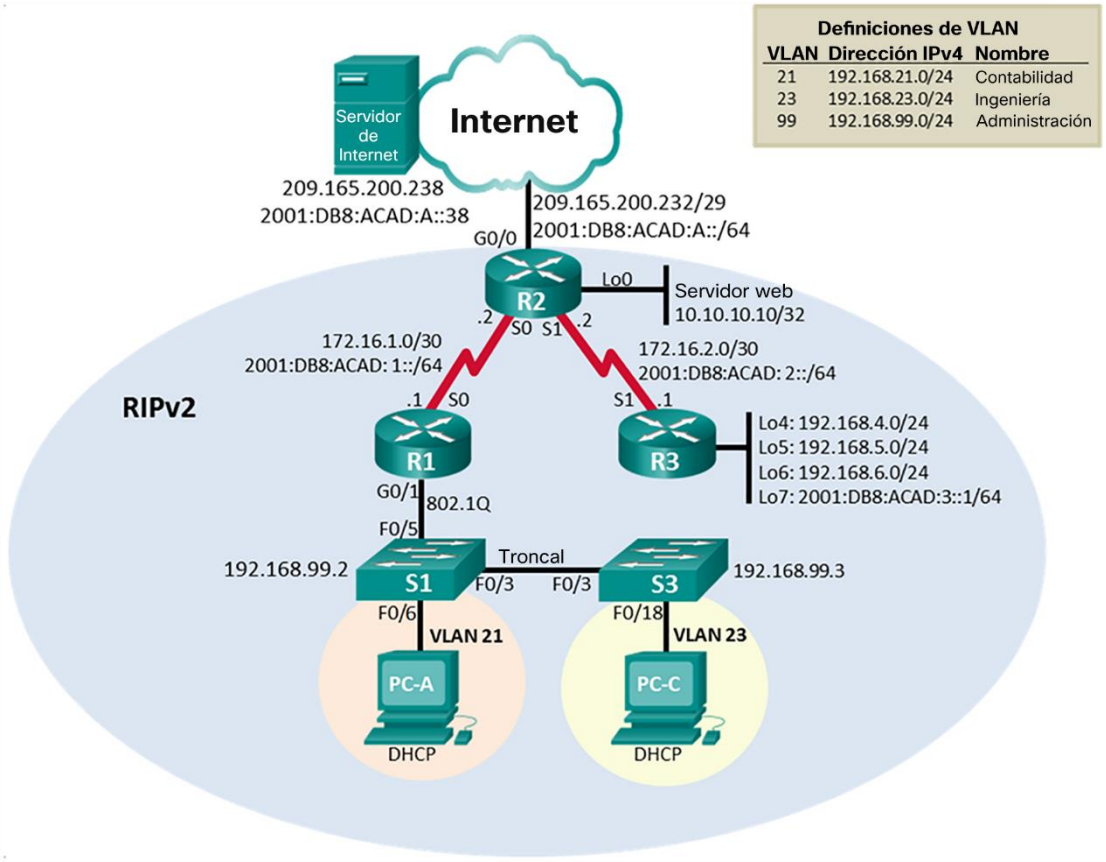
3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

3.1.1 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.

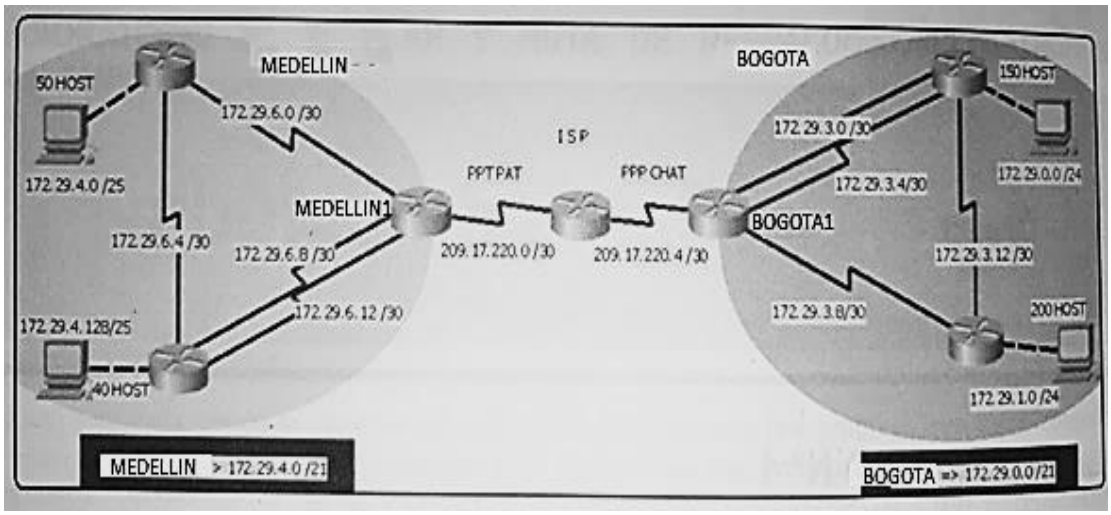
Figura 1 Topología escenario 1



3.1.2 Escenario 2

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

Figura 2 Topología de red



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.

3.2 JUSTIFICACIÓN

Buscar soluciones en particular en un escenario que, requiere de las experiencias técnicas, para programar una red; teniendo en cuenta que el propósito, es darle solución a una problemática que requiere en el configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches; en cuanto a la disposición de los diferentes elementos que se deben configurar que comprende los protocolos de routing dinámico y la configuración del server DHCP, la dirección de red de traslación NAT, así como la lista de control de acceso ACL, que se pueden desarrollar en la estructura de configuración para router, a fin de buscar que se

establezcan protocolos de seguridad de la red, con la implementación de políticas tanto de entrada como de salida de paquetes, para acceso de equipos de manera concreta y en forma específica, sin que haya flujo de información hacia otros centros y equipos en diferentes redes.

4. MARCO TEÓRICO

Operar una red que emplea dos protocolos de Internet, IPv4 e IPv6, generalmente implica que la configuración de red necesita ser replicada para el IPv6 recién implementado, es decir, la red debe configurarse para que IPv6 pueda operar como IPv4. Esta configuración de red no solo incluye aspectos como la habilitación del enrutamiento IPv6 y la incorporación de información IPv6 en el sistema de nombres de dominio, sino también el cumplimiento de las políticas de seguridad de la red a través del filtrado de paquetes[1].

En los escenarios más comunes, las políticas de seguridad de IPv6 reflejan sus contrapartes de IPv4. Después de todo, tanto IPv4 como IPv6 son solo protocolos de internet.

Por lo tanto, incluyen algunos problemas específicos del protocolo y políticas de seguridad, como los que especifican qué servicios de red están expuestos en la red pública, y tienden a ser independientes del protocolo subyacente de la capa de red. En general, no hay razón para que un servidor de red ofrezca un servicio sobre un protocolo de internet y no sobre el otro.

4.1 CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD

Uno podría esperar que las políticas de seguridad aplicadas a través de reglas de filtrado de paquetes basadas en la información de la capa de transporte, como permitir paquetes entrantes destinados al puerto 80, se especifiquen de manera de red independiente de la capa. Sin embargo, muchos dispositivos de red, incluidos dispositivos de seguridad, generalmente requieren que una regla de filtrado no solo especifique la información relevante de la capa de transporte, como los números de puerto de protocolo de transporte, sino también el protocolo de capa de red específico para el cual se debe aplicar la regla, como IPv4 o IPv6[2].

Esto significa que en los escenarios de doble pila más comunes, cada política de filtrado para un número de puerto específico dará como resultado dos reglas de

[1] Gont, F.. Qué hacer cuando las políticas de IPv4 e IPv6 discrepan. (2018, August 27 disponible en https://searchdatacenter.techtarget.com/es/consejo/Que-hacer-cuando-las-politicas-de-IPv4-e-IPv6-discrepan

[2]PAVÓN, Belén Colmenar; TELEMÁTICA, E. T. T. Diseño de una red WAN para una compañía nacional. *UOC, Integración de redes telemáticas ETT Telemática*, 2012.

filtrado separadas: una para el caso de IPv4 y otra para el caso de IPv6. Como resultado, no sería difícil esperar que, en ocasiones, los administradores simplemente no logren duplicar dichas reglas; por lo tanto, pueden producirse desajustes en las políticas de filtrado de paquetes para IPv4 e IPv6[3].

Se puede esperar que las políticas de seguridad se apliquen más a fondo en el mundo IPv4 como resultado de que los sitios no duplican/reflejan las reglas de filtrado de paquetes para IPv6 cuando se implementa el protocolo. Sin embargo, presenté una investigación en la conferencia de seguridad Hack In Paris 2018 que indica que las suposiciones y la lógica antes mencionadas no se aplican en el mundo real.

4.2 POLÍTICAS DE SEGURIDAD PARA IPV4 E IPV6

El estudio evaluó esencialmente las políticas de seguridad IPv4 e IPv6 de una gran cantidad de servidores web con el objetivo de identificar posibles desajustes entre los dos. Cada uno de los servidores web se escaneó en puertos en cada una de sus direcciones IPv4 e IPv6 y se compararon los resultados de los escaneos de puertos.

Los resultados del escaneo del puerto se ilustran en el gráfico de barras anterior e indican, para cada puerto abierto, si el número de puerto se abrió solo a través de IPv4, solo a través de IPv6 o en ambos, IPv4 e IPv6.

Para hacer más evidentes las diferencias en las políticas de filtrado, la siguiente figura ilustra la frecuencia de discrepancias de políticas para cada número de puerto; es decir, el porcentaje de sitios escaneados por puerto que exhibieron un puerto abierto solo a través de IPv4 o IPv6, pero no en ambos protocolos de internet.

Lo interesante de los resultados del escaneo de puertos es que, si bien hay discrepancias evidentes en las políticas de seguridad aplicadas para IPv4 frente a las políticas aplicadas para IPv6, no se puede argumentar realmente que las políticas de uno de los protocolos de internet sean más permisivas que las aplicadas al otro. De hecho, el estudio muestra que las políticas parecen depender de los

[3] ROSERO MUÑOZ, Marcelo Alejandro. *Diseño y configuración de una red LAN-WAN, utilizando direccionamiento y servicios IPV6*. 2017. Tesis de Licenciatura. CIENCIAS DE LA INGENIERÍA E INDUSTRIAS FACULTAD: INGENIERÍA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN.

números de puertos en cuestión, con algunos puertos que son más abiertos a través de IPv4, mientras que otros son más abiertos a través de IPv6[4].

Finalmente, para los servidores que estaban disponibles en múltiples direcciones IPv4 y múltiples direcciones IPv6, el estudio también encontró que, si bien prácticamente no existían discrepancias de política para diferentes direcciones IPv4 en el mismo servidor, había un pequeño porcentaje de desajustes entre las diferentes direcciones IPv6 del mismo sitio web

4.3 IMPLICACIONES PARA LOS PEN TESTERS

Al evaluar qué servicios ofrece un servidor determinado, no es inusual que los pen testers escaneen un servidor a través de cualquiera de las direcciones, pero no sobre todas ellas.

En función de los desajustes de política encontrados para IPv4 e IPv6, y para diferentes direcciones IPv6 en los mismos servidores, está claro que al evaluar qué servicios ofrece un servidor, el servidor en cuestión debe escanearse por puertos en todas las direcciones IPv4 e IPv6 disponibles.

Políticas de seguridad más homogéneas

Una conclusión obvia para los administradores de red y seguridad es que las políticas de seguridad deberían aplicarse de for ma más homogénea a IPv4 e IPv6, y que la aplicación de políticas de seguridad en ambos protocolos de internet debería formar parte de los procedimientos normales de operación y administración.

También es recomendable que los sitios que actualmente no son compatibles con IPv6 apliquen políticas de filtrado de paquetes IPv6 que sean similares a las aplicadas a las contrapartes de IPv4. De esta manera, cuando IPv6 finalmente se implemente en esos sitios, los servidores y otros elementos de la red no serán tomados por sorpresa[5].

[4] PALIZA, Félix F. Alvarez. GUÍA PARA EL DISEÑO DE REDES EMPRESARIALES.(TRANSICIÓN IPv4-IPv6).
[5] BAUTISTA, Dewar Willmer Rico; CÁRDENAS, Yurley Constanza Medina; JAIMES, Luz Marina Santos. IPSec de IPv6 en la universidad de Pamplona. *scientia et Technica*, 2008, vol. 14, no 39, p. 320-325.

Estudios recientes han indicado que las discrepancias entre las políticas de seguridad IPv4 e IPv6 son bastante comunes. Los administradores de redes y seguridad deben tomar medidas para garantizar que las políticas aplicadas a ambos protocolos sean homogéneas. Estas discrepancias comunes garantizan que, al escanear un sitio en un puerto como parte de una prueba de penetración, por ejemplo, todas las direcciones disponibles deben estar sujetas a escaneos de puertos, ya que los resultados para diferentes direcciones y diferentes protocolos de internet pueden diferir.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Dispositivos Requeridos

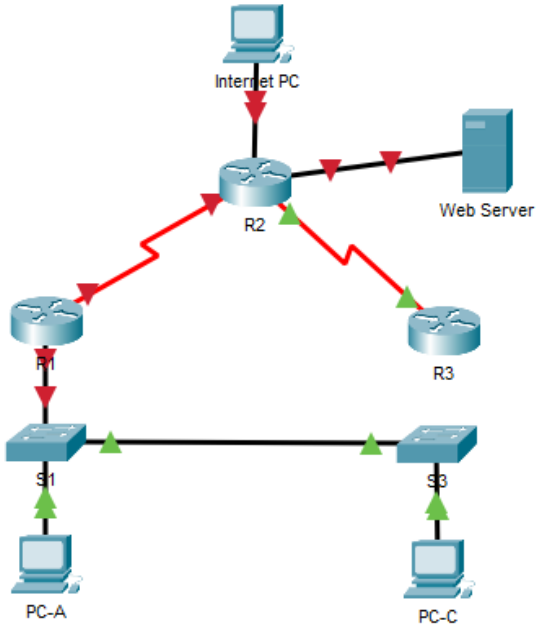
- 3 Routers (Cisco 1841) con 2 puertos FastEthernet, 2 puertos Seriales
- 2 Switches (Cisco 2960)
- 1 Servidor (Genérico PT)
- 3 PCs con sistema operativo Windows 7, con tarjeta de red
- Cables Serial y Ethernet

Tabla 1 Direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

	Dirección IP (Ip Address)	**Mascara de Red (Subnet Mask)**	**Puerta de Enlace Predeterminado (Default Gateway)**	**Direccion IPv6 (IPv6 Address)**	**Puerta de Enlace IPv6 (IPv6 Gateway)**
Internet Server	209.165.200.230	255.255.255.248	209.165.200.255	2001:DB8:ACAD:2::30/64	2001:DB8:ACAD:2::1
R1 to R2 S0/0/0	172.31.21.1	255.255.255.252		2001:DB8:ACAD:12::1/64	
R2 to R1 S0/0/1	172.31.21.2	255.255.255.252		2001:DB8:ACAD:12::2/64	
R2 to R3 S0/0/0	172.31.23.2	255.255.255.252		2001:DB8:ACAD:23::2/64	
R2 to Internet Server G0/0	209.165.200.225	255.255.255.248		2001:DB8:ACAD:2::1/64	
R2 Lo0 Web Server	10.10.10.10	255.255.255.255	0.0.0.0.0.0.0.0 G0/0	::/0 G0/0	
R3 to R2 S0/0/1	172.31.23.1	255.255.255.252		2001:DB8:ACAD:23::1/64	
R3 Lo4	192.168.4.1	255.255.255.0	0.0.0.0.0.0.0.0 S0/0/1	::/0 S0/0/1	
R3 Lo5	192.168.5.1	255.255.255.0	0.0.0.0.0.0.0.0 S0/0/1	::/0 S0/0/1	
R3 Lo6	192.168.6.1	255.255.255	0.0.0.0.0.0.0.0 S0/0/1	::/0 S0/0/1	
S1 Vlan 30, Vlan 40 Vlan 200	192.168.99.2	255.255.255.0			
S3 Vlan	192.168.99.3	255.255.255.0			

30, Vlan 40 Vlan 200					
R1 G0/0.30	192.168.30.1	255.255.255.0			
R1 G0/0.40	192.168.40.1	255.255.255.0			
R1 G0/0.200	192.168.200.1	255.255.255.0			

Figura 3 Diseño en Packet Trece escenario 1



5.2 METODOLOGÍA

5.2.1 Desarrollo de solución escenario 1

5.2.1.1 Parte 1: Inicializar dispositivos

5.2.1.1.1 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.

Tabla 2 Configuración inicial routers 1, 2 y 3 y los switches S1 y S3

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	**R1** Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router# **R2** Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router# **R3** Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router#
Volver a cargar todos los routers	**R1** Router#reload Router#reload Proceed with reload? [confirm] System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1) Initializing memory for ECC .. C1841 processor with 524288 Kbytes of main memory

	Main memory is configured to 64 bit mode with ECC enabled Readonly ROMMON initialized Self decompressing the image : #### [OK] Restricted Rights Legend Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013. cisco Systems, Inc. 170 West Tasman Drive San Jose, California 95134-1706 Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Wed 18-Jul-07 04:52 by pt_team Image text-base: 0x60080608, data-base: 0x6270CD50 This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

	Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please contact us by sending email to export@cisco.com. Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory. Processor board ID FTX0947Z18E M860 processor: part number 0, mask 49 2 FastEthernet/IEEE 802.3 interface(s) 1 Gigabit Ethernet/IEEE 802.3 interface(s) 2 Low-speed serial(sync/async) network interface(s) 191K bytes of NVRAM. 63488K bytes of ATA CompactFlash (Read/Write) Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Wed 18-Jul-07 04:52 by pt_team **R2** Router#reload **R3** Router#reload

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**S1** Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram **S3** Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar ambos switches	**S1** Switch# reload **S3** Switch# reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show flash **S1** Switch# show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) **S3** Switch# show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch>

5.2.1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

5.2.1.2.1 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):

Tabla 3 Configuración computadora de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::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.

5.2.1.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4 Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>ENABLE Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R1 Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	class R1(config)#enable secret class R1(config)#
Contraseña de acceso a la consola	cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit

	R1(config)#
Contraseña de acceso Telnet	cisco R1(config)#line vty 0 4 R1(config-line)#pass % Incomplete command. R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd #Se prohbe el acceso no autorizado!#
Interfaz S0/0/0	Establezca la descripción R1(config)#interface s0/0/0 %Invalid interface type and number R1(config)#interface s0/1/1 R1(config-if)#description conexion de R1 - R2
Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones	R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones	R1(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config-if)#clock rate 128000 R1(config-if)#
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ipv6 route ::/0 s0/1/1 R1(config)#

Nota: Todavía no configure G0/1.

5.2.1.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 5 Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	R2 Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	class R2(config)#enable secret class
Contraseña de acceso a la consola	cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	cisco R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#banner motd #Se prohibe el acceso no autorizado!# R2(config)#
Interfaz S0/0/0	Establezca la descripción R2(config)#interface s0/1/1 R2(config-if)#description conexion de R2 - R1
Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.	R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#no shutdown

	%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down R2(config-if)#
Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
Activar la interfaz	
Interfaz S0/0/1	Establecer la descripción R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R2(config)#interface s0/0/1 R2(config-if)#description conexion de R2 - Internet R2(config-if)#ip address 209.165.200.229 255.255.255.248
Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#NO SHUTDOWN R2(config-if)#EXIT
Establecer la frecuencia de reloj en 128000.	
Activar la interfaz	
Interfaz G0/0 (simulación de Internet)	Establecer la descripción.
Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R2(config)#interface loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)#description servidor web simulado

Establezca la dirección IPv4. Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0.	R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#

Configure una ruta IPv6 predeterminada de G0/0.

5.2.1.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 6 Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain.lookup ^ % Invalid input detected at '^' marker. Router(config)#no ip domain-lookup Router(config)#hostname R3 R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#passord cisco ^ % Invalid input detected at '^' marker. R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#service password-encryption R3(config)#banner motd #Se prohibe el acceso no autorizado!# R3(config)#interface s0/0/1 R3(config-if)#description conexion de R3 - R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252
Nombre del router	
Contraseña de exec privilegiado cifrada	
Contraseña de acceso a la consola	
Contraseña de acceso Telnet	
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	
Interfaz S0/0/1	
Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.	
Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	
Activar la interfaz	
Interfaz loopback 4	
Interfaz loopback 5	
Interfaz loopback 6	
Interfaz loopback 7	
Rutas predeterminadas	

	R3(config-if)#no shutdown R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up R3(config-if)#interface s0/0/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#ip route 0.0.0.0 0.0.0.0 255.255.255.255 R3(config)#description conexion de R3-internet ^ % Invalid input detected at '^' marker. R3(config)#description conexion de R3 - internet ^ % Invalid input detected at '^' marker. R3(config)#ip address 209.165.200.230 255.255.255.248 ^ % Invalid input detected at '^' marker. R3(config)#interface s0/0/1 R3(config-if)#ip address 209.165.200.230 255.255.255.248 R3(config-if)#ipv6 address 2001:DB8:ACAD:A::3/64 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface loopback 0 R3(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R3(config-if)#interface loopback 4 R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config-if)#interface loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config-if)#interface loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#interface loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

	R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1

5.2.1.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 7 Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain.lookup ^ % Invalid input detected at '^' marker. Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada class	S1(config)#enable secret class
Contraseña de acceso a la consola cisco	S1(config)#line console 0 S1(config-line)#passwor cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado cisco	S1(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S1(config)#banner motd #Se prohibe el acceso no autorizado# S1(config)#

5.2.1.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 8 Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada class	S3(config)#enable secret class
Contraseña de acceso a la consola cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado cisco	S3(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S3(config)#banner motd #Se prohibe el acceso no autorizado# S3(config)#

5.2.1.2.7 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:

Tabla 9 Verificación de conexión de red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	Perfecto
R2	R3, S0/0/1	172.16.2.1	Perfecto
PC de Internet	Gateway predeterminado	10.10.10.10	Perfecto

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

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

5.2.1.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 10 Tareas de configuración S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config-if)#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.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología 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	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa 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	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range 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 S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
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

5.2.1.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 11 Tareas de configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada 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	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#int f0/3 S3(config-if)#switch mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config-if-range)#switchport mode access 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

5.2.1.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12 Tareas de configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz 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	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz 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	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz 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

5.2.1.3.4 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:

Tabla 13 Verificación de conectividad de red

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

5.2.1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2

5.2.1.4.1 Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 Configuración RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router OSPF R1(config-router)#version 2 R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive- interface g0/1.21 R1(config-router)#passive- interface g0/1.23 R1(config-router)#passive- interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto- summary

5.2.1.4.2 Paso 2: Configurar RIPv2 en el R2

Tabla 15 Configuración RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router OSPF R2(config-router)#version 2 R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 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
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. 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

5.2.1.4.3 Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 16 Configuración RIPv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router OSPF R3(config-router)#version 2 R3(config-router)#do show ip route connected C 172.16.2.0/30 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
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 72.16.2.0 R3(config-router)#network 72.16.4.0 R3(config-router)#network 72.16.5.0 R3(config-router)#network 72.16.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive- interface loopback 4 R3(config-router)#passive- interface loopback 5 R3(config-router)#passive- interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto- summary

5.2.1.4.4 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:

Tabla 17 Verificación de información de RIP

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

¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run, luego dirigirse a la sesión de rip

5.2.1.5 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Configuración de R1 servidor DHCP – VLAN 21 y 23

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.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com

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

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configuración NAT estática y dinámica R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet tracer no soporta los comandos de habilitación del servidor HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

5.2.1.5.3 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.

Tabla 20 Verificación protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para el PC-A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	El resultado es satisfactorio para el PC-A
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	El resultado es satisfactorio
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**	Los PC no tienen comunicación a internet utilizando el comando http server porque en Packet Tracer es soportado a para activar el servidor web en R2. Pero si utilizamos la Dirección IP del servidor web en el navegador PC-A y PC-C tenemos acceso a internet.

5.2.1.6 Parte 6: Configurar NTP

Tabla 21 Configuración NTP

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#clock set 23:52:00 20 may 2020**.**
Aplicar la ACL con nombre a las líneas VTY	Packet tracer no soporta este comando
Permitir acceso por Telnet a las líneas de VTY	Servidor: **R2 Packet tracer no soporta este comando**
Verificar que la ACL funcione como se espera	

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

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

Tabla 22 Restricción 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
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN- MGT in Packet tracer no soporta el commando “imput”
Verificar que la ACL funcione como se espera	La pruebas es satisfactoria

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

Tabla 23 Introducción del comando CLI

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-list
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. **Show ip nat translations**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations

5.2.2 Desarrollo de solución escenario 2

Desarrollo
Como trabajo inicial se debe realizar lo siguiente.
• Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).
• Realizar la conexión física de los equipos con base en la topología de red

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

```
Router>enable
Router# configure terminal
Router(config)#hostname ISP  ISP(config)#int s0/0/0
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000  ISP(config-if)# no shutdown
ISP(config-if)#int s0/0/1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000  ISP(config-if)#no shutdown
```

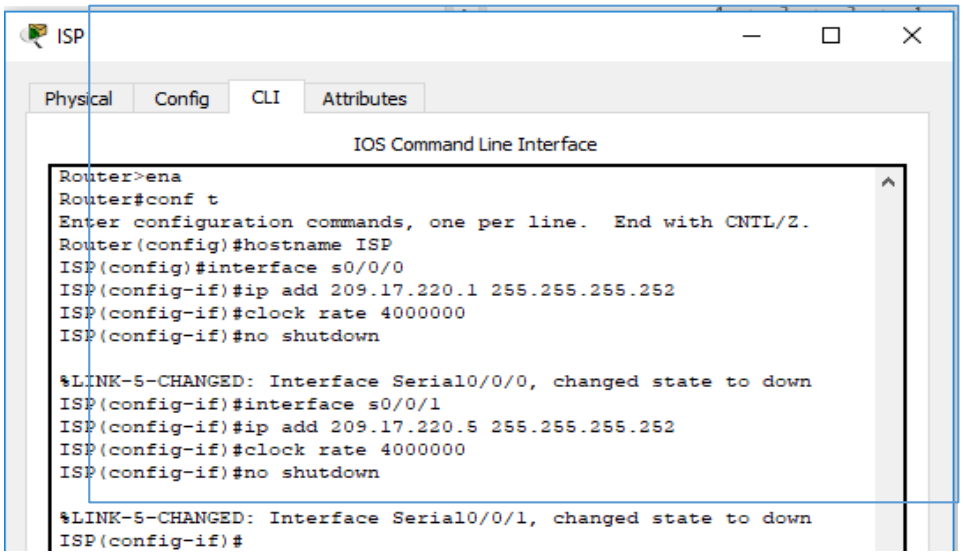


Figura 4 Configuración del direccionamiento IP en ISP.

5.2.4.4.2 Configuración IP Router (MEDELLIN1) Configuramos todas las interfaces Router>enable

Router#configure terminal
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#interface s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000 MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown

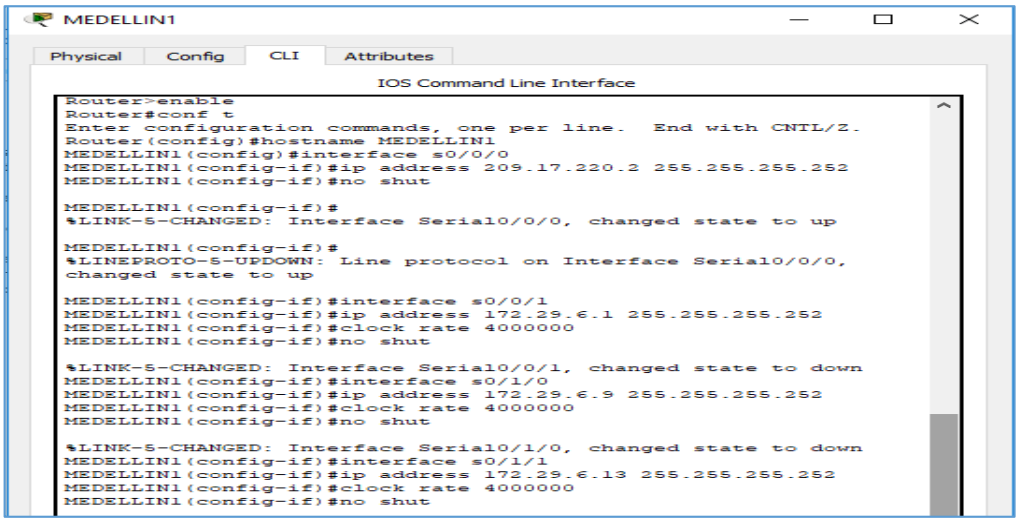


Figura 5 Configuración del direccionamiento IP en Medellín1.

Configuración IP Router (MEDELLIN2)
Configuramos todas las interfaces. Router>enable
Router#configure terminal
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#interface s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#interface s0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 4000000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#interface g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown

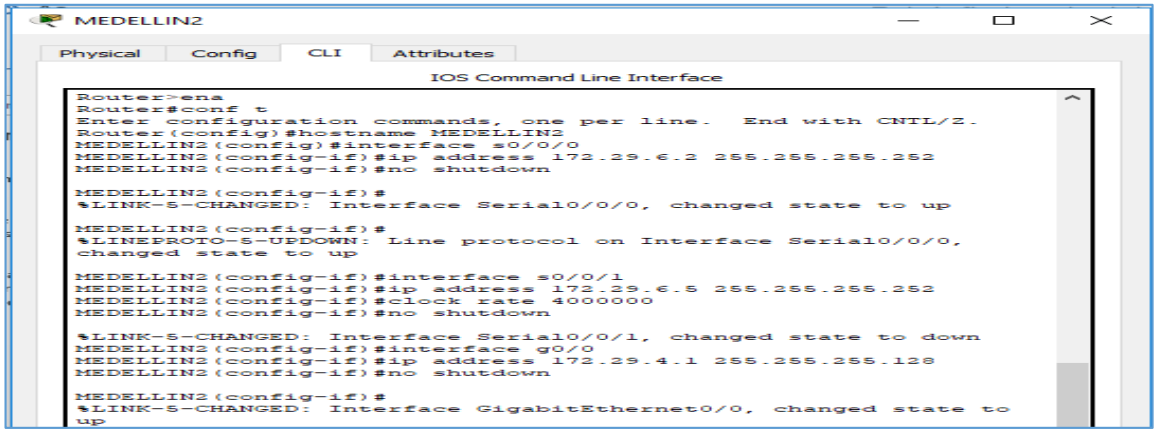


Figura 6 Configuración del direccionamiento IP en Medellín2

Configuración IP Router (MEDELLIN3)
Configuración interfaces
Router>enable Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#interface s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface s0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface s0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface g0/0
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shutdown

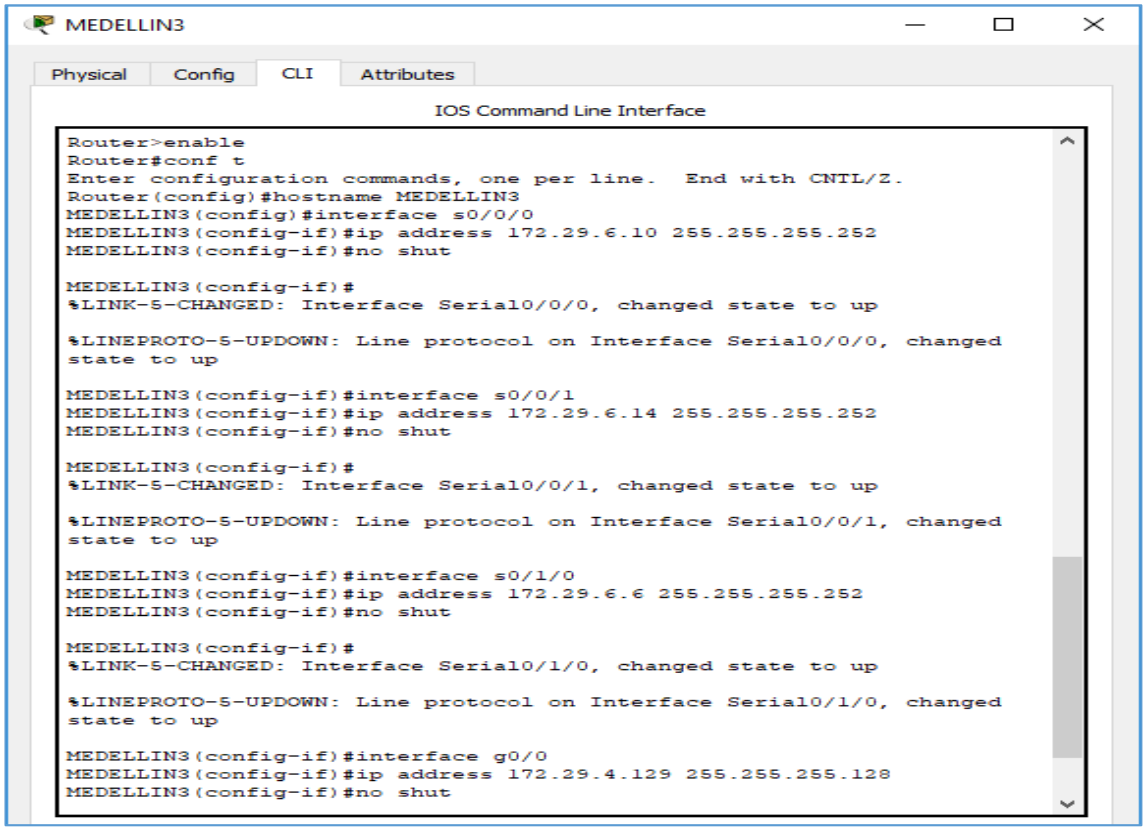


Figura 7 Configuración del direccionamiento IP en Medellín3

Configuración IP Router (Bogota1) Configuramos todas las interfaces
Router>enable Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown

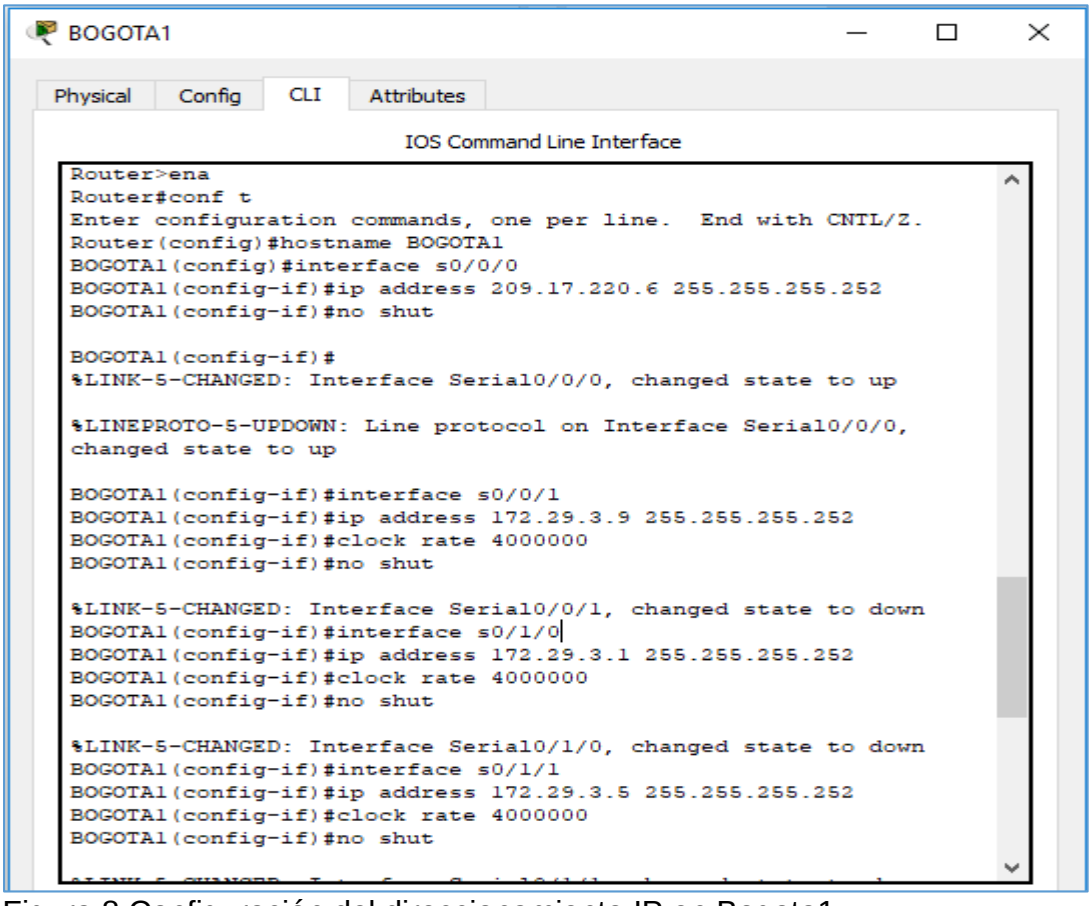


Figura 8 Configuración del direccionamiento IP en Bogota1.

Configuración IP Router (Bogota2) Configuramos todas las interfaces

Router>enable Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#interface s0/0/0
BOGOTA2(config-if)#ip add 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#interface s0/0/1
BOGOTA2(config-if)#ip add 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 4000000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#interface g0/0
BOGOTA2(config-if)#ip add 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown

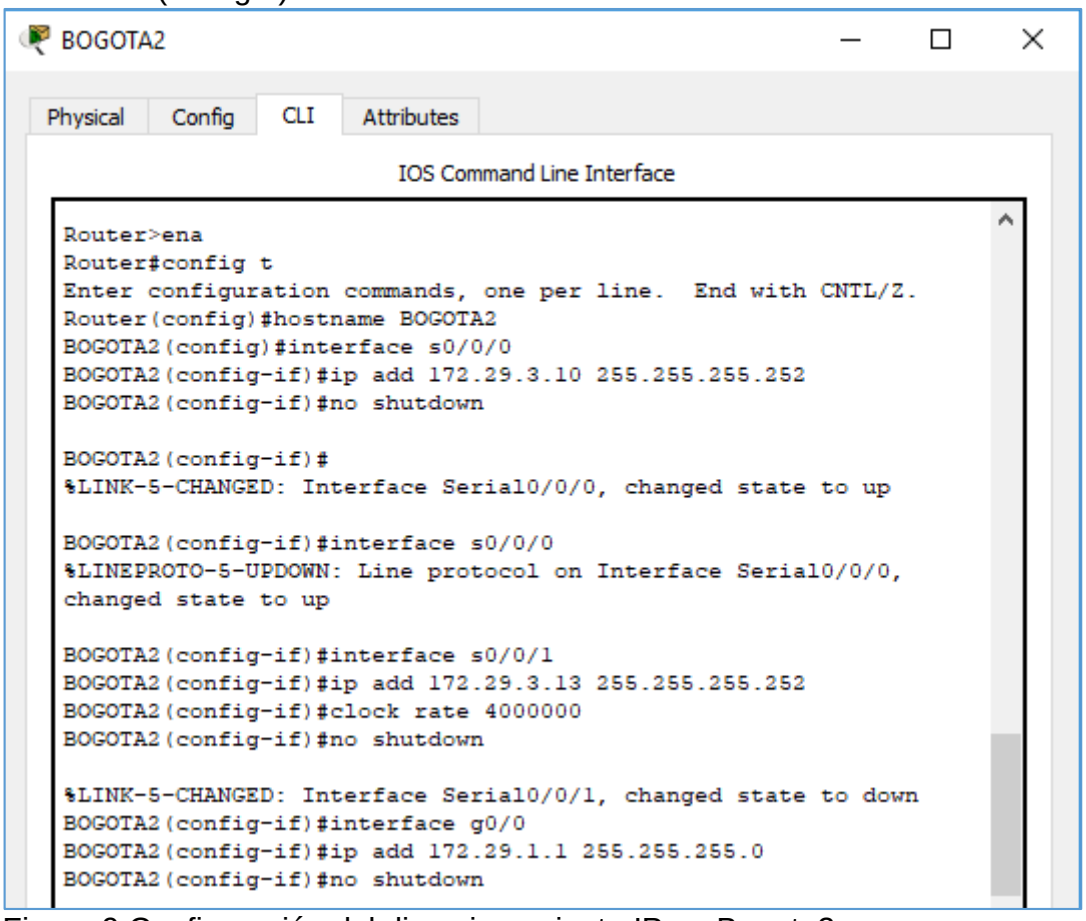


Figura 9 Configuración del direccionamiento IP en Bogota2

Configuración IP Router (Bogota3) Configuramos todas las interfaces
Router>enable Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname BOGOTA3
BOGOTA3(config)#interface s0/0/0
BOGOTA3(config-if)#ip add 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#interface s0/0/1
BOGOTA3(config-if)#ip add 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown BOGOTA3(config)#int s0/1/0
BOGOTA3(config-if)#ip add 172.29.3.14 255.255.255.252
BOGOTA3(config-if)# no shutdown BOGOTA3(config-if)#interface g0/0
BOGOTA3(config-if)#ip add 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown

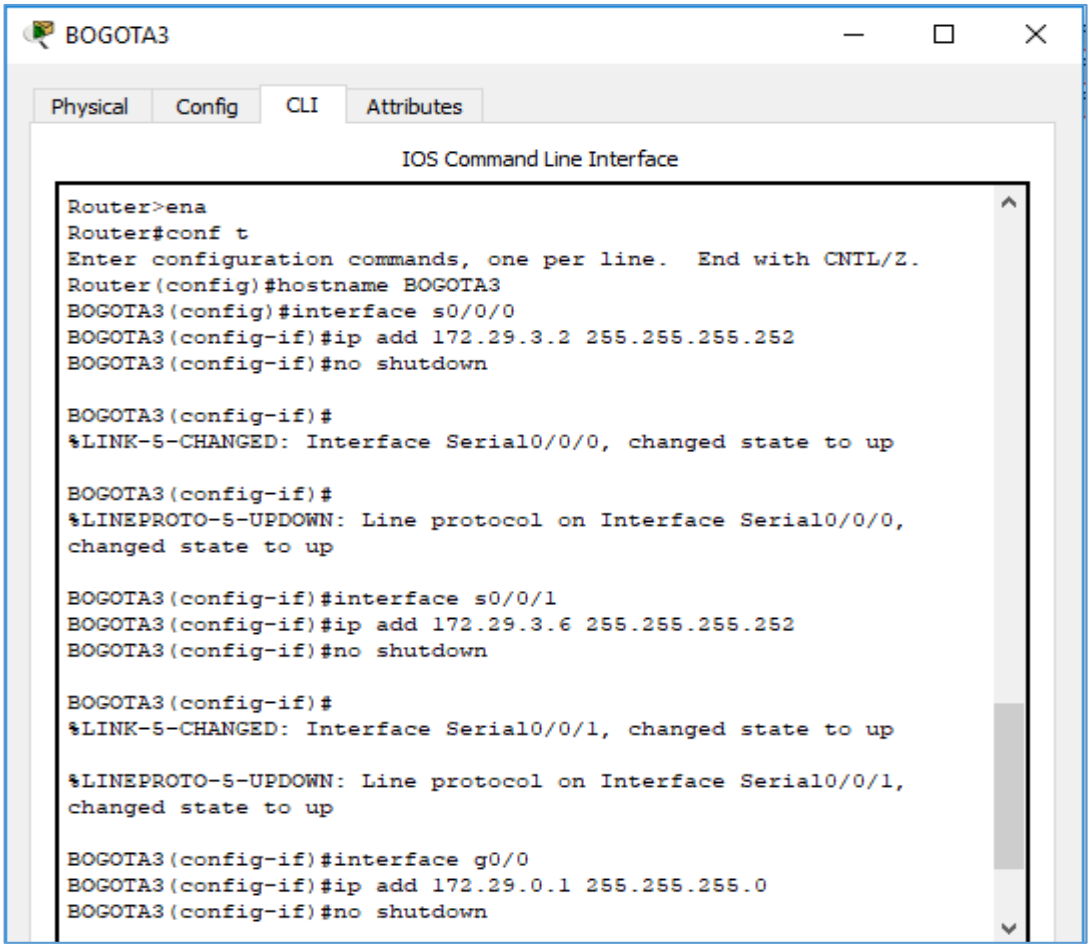


Figura 10 Configuración del direccionamiento IP en Bogota3.

5.2.2.1 Parte 1: Configuración del enrutamiento

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

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.

MEDELLIN1>enable MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router OSPF
MEDELLIN1(config-router)#version 2
MEDELLIN1(config-router)#no auto-summary
MEDELLIN1(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, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
MEDELLIN1(config-router)#network 172.29.6.0
MEDELLIN1(config-router)#network 172.29.6.8
MEDELLIN1(config-router)#network 172.29.6.12
MEDELLIN1(config-router)#passive-interface s0/0/0
MEDELLIN2>enable
MEDELLIN2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#router OSPF
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#no auto-summary
MEDELLIN2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
MEDELLIN2(config-router)#network 172.29.4.0
MEDELLIN2(config-router)#network 172.29.6.0
MEDELLIN2(config-router)#network 172.29.6.4
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#
Configuración de protocolo OSPF Router Medellin3
MEDELLIN3>enable
MEDELLIN3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#route OSPF
MEDELLIN3(config-router)#version 2
MEDELLIN3(config-router)#no auto-summary
MEDELLIN3(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1

MEDELLIN3(config-router)#network 172.29.4.128
MEDELLIN3(config-router)#network 172.29.6.4
MEDELLIN3(config-router)#network 172.29.6.8
MEDELLIN3(config-router)#network 172.29.6.12
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#

Configuración de protocolo OSPF Router Bogota1

Se ejecutan los siguientes comandos:

BOGOTA1>enable
BOGOTA1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#router OSPF
BOGOTA1(config-router)#version 2
BOGOTA1(config-router)#no auto-summary
BOGOTA1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
BOGOTA1(config-router)#network 172.29.3.0
BOGOTA1(config-router)#network 172.29.3.4
BOGOTA1(config-router)#network 172.29.3.8
BOGOTA1(config-router)#passive-interface s0/0/0

Configuración de protocolo OSPF Router Bogota2

BOGOTA2>enable BOGOTA2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#router OSPF
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#no auto-summary
BOGOTA2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
BOGOTA2(config-router)#network 172.29.1.0
BOGOTA2(config-router)#network 172.29.3.8
BOGOTA2(config-router)#network 172.29.3.12
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#

Configuración de protocolo OSPF Router Bogota3

Se ejecutan los siguientes comandos.

BOGOTA3>enable BOGOTA3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#router OSPF
BOGOTA3(config-router)#version 2
BOGOTA3(config-router)#no auto-summary
BOGOTA3(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0

BOGOTA3(config-router)#network 172.29.0.0
BOGOTA3(config-router)#network 172.29.3.0
BOGOTA3(config-router)#network 172.29.3.4
BOGOTA3(config-router)#network 172.29.3.12
BOGOTA3(config-router)#passive-interface g0/0

Configuración de enrutamiento de la ruta por defecto hacia ISP y redistribución por OSPF.

Los routers Bogota1 y Medellín1 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.

Router MEDELLIN1

MEDELLIN1>enable MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#route OSPF
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#

Router BOGOTA1

BOGOTA1>enable BOGOTA1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#route OSPF
BOGOTA1(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.

Para este caso se empiezan asignar rutas estáticas que le permitan a ISP acceder a las redes internas de Bogotá y Medellín, con la utilización de la subred base más la sumarización de las subredes, para lo cual se realiza la sumarización por separado de las subredes de Medellín y Bogotá de la siguiente manera.

Tabla 24 Tabla de sumarización de las subredes Medellín y Bogotá.

Medellín	**172**	**29**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**172.29.4.0/25**
	172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	**172.29.4.128/25**
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	**172.29.6.4/30**
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	**172.29.6.8/30**
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	**172.29.6.12/30**
	172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	**172.29.6.0/30**
	172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	**172.29.4.0/22**
Bogotá	172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**172.29.0.0/24**
	172	29	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	**172.29.1.0/24**
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	**172.29.3.12/30**
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	**172.29.3.8/30**
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	**172.29.3.0/30**
	172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	**172.29.3.4/30**
	172	**29**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**172.29.0.0/22**

Después de realizada la sumarización se ejecutan los siguientes comandos en el Router ISP.

ISP>enable ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6

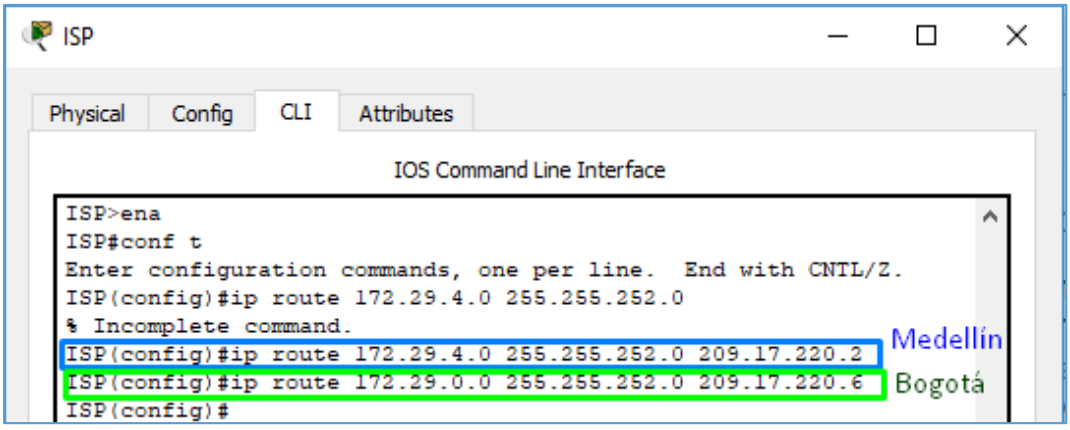


Figura 11 Configuración IP estáticas ISP para acceso a Medellín y Bogotá.

5.2.2.2 Parte 2: Tabla de Enrutamiento.

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

Se verifica que los pin funcionen entre los router

Ruta BOGOTA3 - MEDELLIN2

BOGOTA3#ping 172.29.3.1
BOGOTA3#ping 209.17.220.5
BOGOTA3#ping 209.17.220.2
BOGOTA3#ping 172.29.6.2

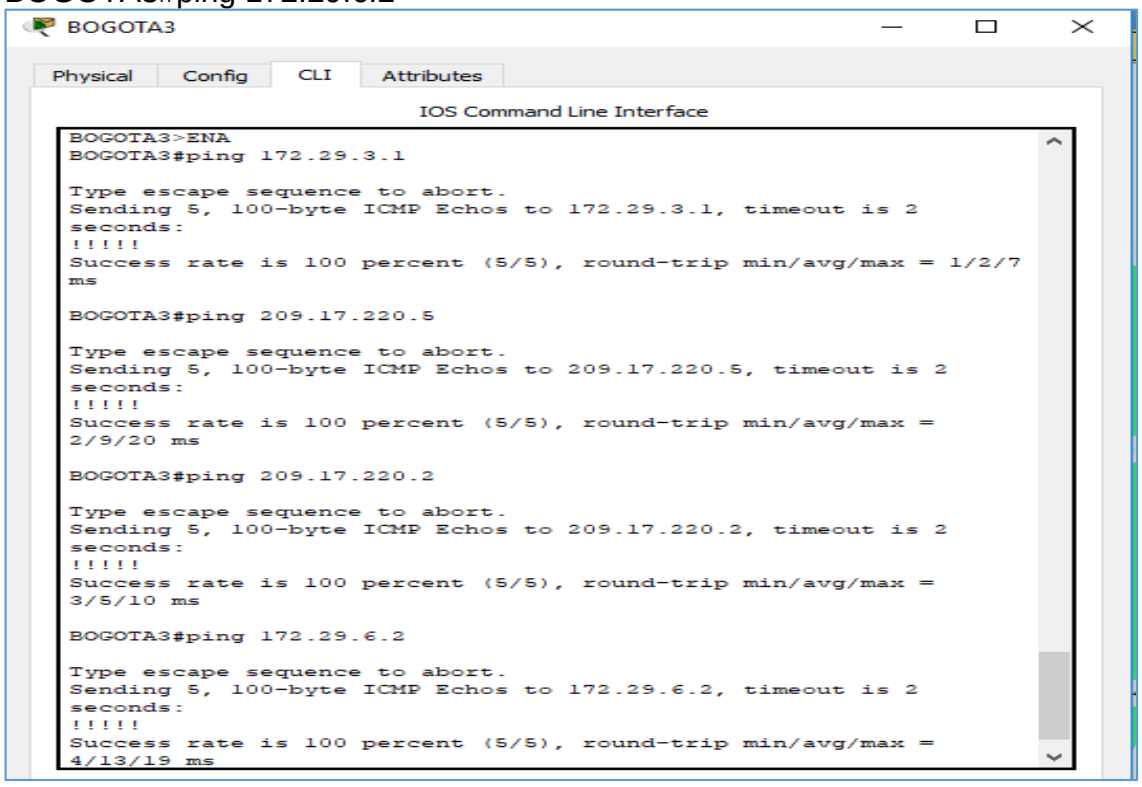


Figura 12 Ping ruta Bogota3 - Medellin2.
Ruta BOGOTA2-MEDELLIN3

BOGOTA2#ping 172.29.3.9
BOGOTA2#ping 209.17.220.5
BOGOTA2#ping 209.17.220.2
BOGOTA2#ping 172.29.6.9

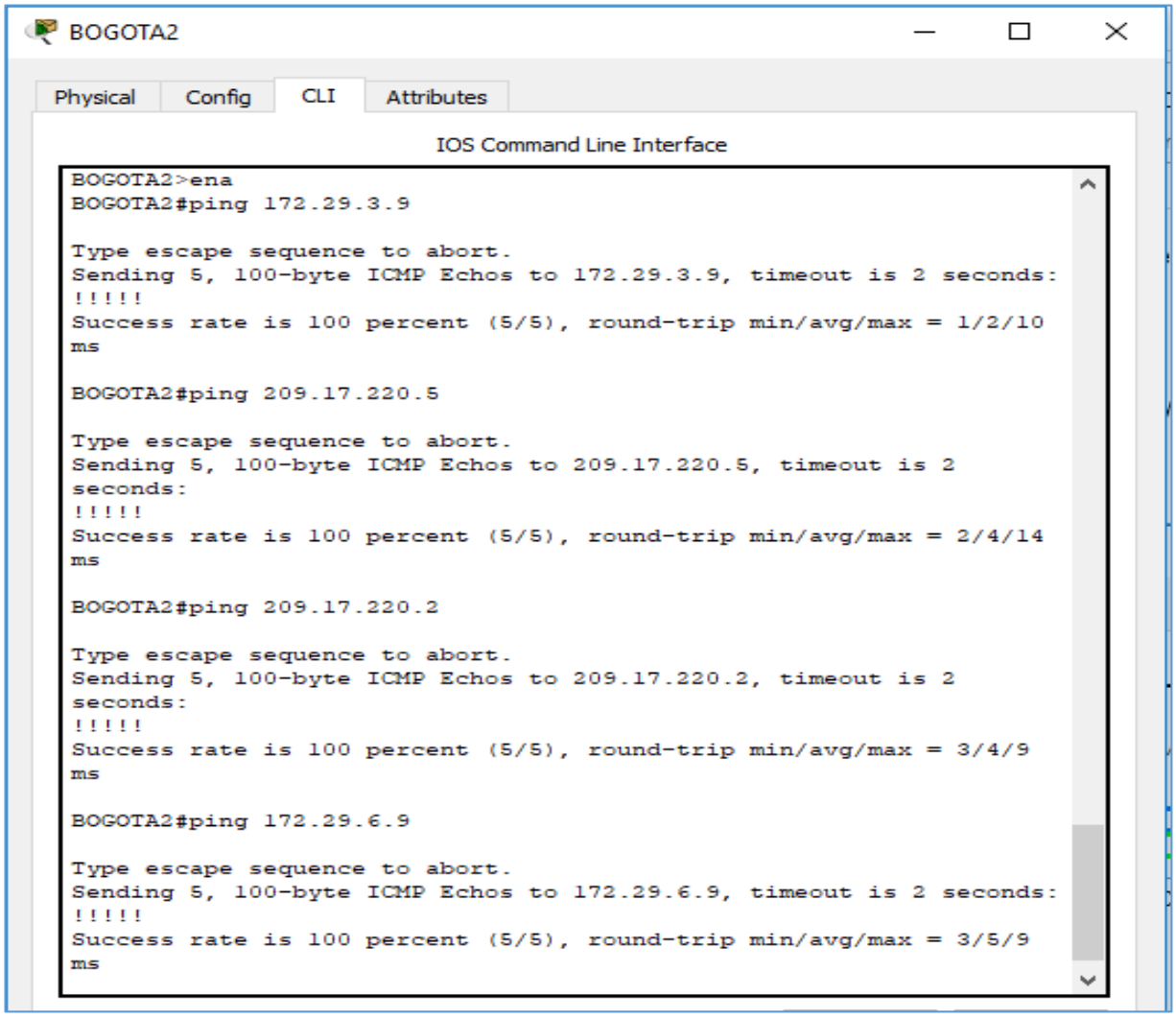


Figura 13 Ping ruta Bogota2 – Medellin3.

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

Se realiza para los que tienen asignado dos seriales conectados en el mismo Router, donde tiene diferentes opciones para llevar la carga de internet. Para visualizar se ejecuta el comando show ip route, que nos permite observar que no hay balanceo de carga.

Estos se presentan en los router MEDELLIN3 Y BOGOTA2, donde las conexiones dobles nos permiten balancear la información.

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.

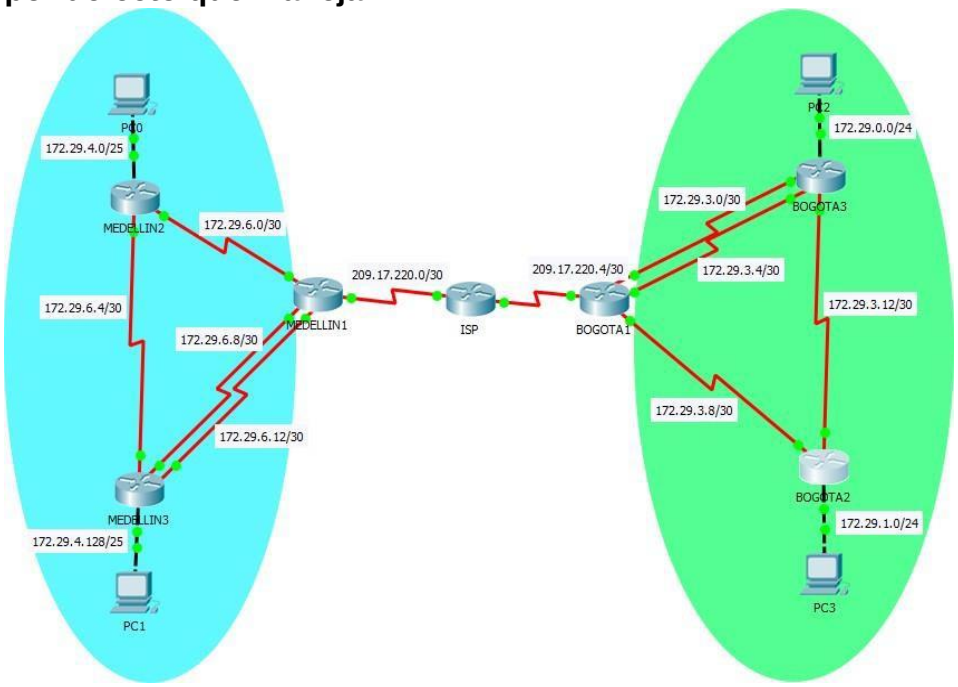


Figura 14 Verificación de similitud en router Bogota1 y Medellin1.

BOGOTA1 Y MEDELLIN1 Son redes similares en el número de conexiones que estos se encuentran pero además están conectadas al ROUTER ISP.

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

Se ejecuta el comando show ip route para visualizar las redes.

Podemos verificar por el comando show ip route las redes conectadas por OSPF EN LOS ROUTERS MEDELLIN2 Y BOGOTA3.

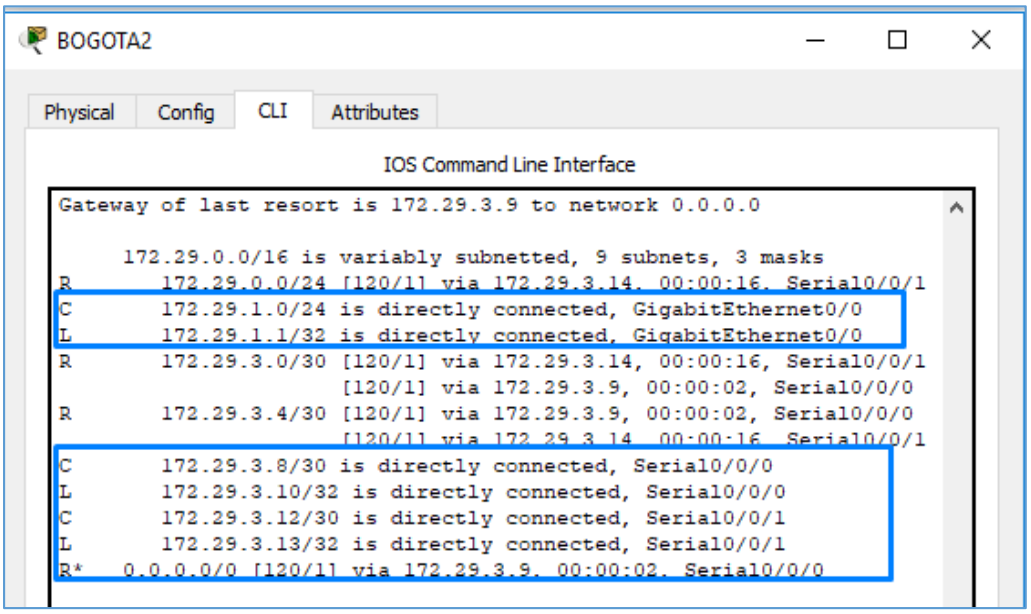


Figura 15 Redes conectadas directamente y recibidas por OSPF en Bogota2.

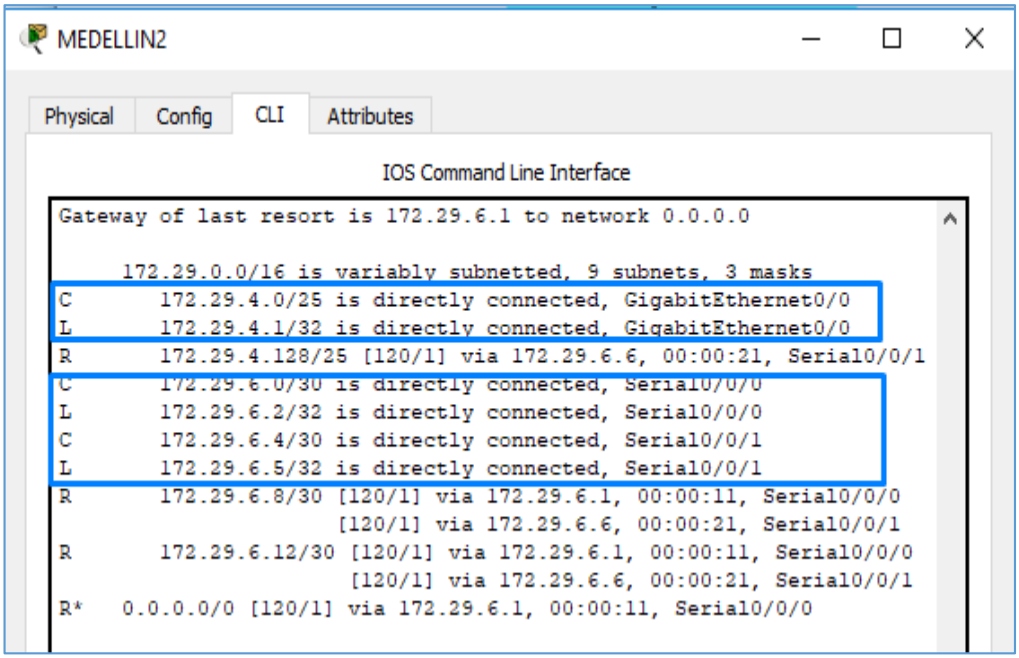


Figura 16 Redes conectadas directamente y recibidas por OSPF en Medellin2.

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

Estas son las especificadas en el punto b, donde se halla más de una ruta para acceder a internet.

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

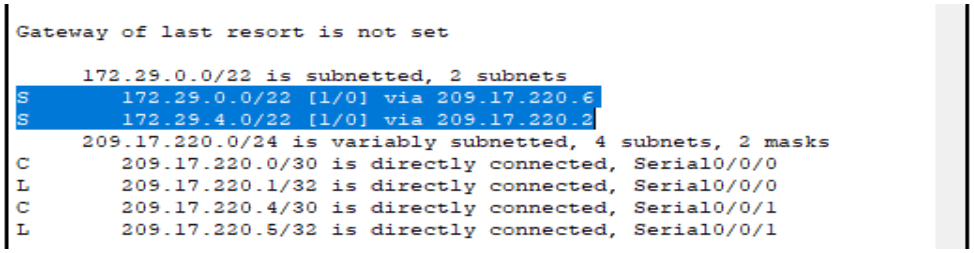


Figura 17 Verificación de rutas estáticas en ISP.

5.2.2.3 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.

Tabla 25 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

Fueron tenidas en cuenta en la configuración del protocolo OSPF en cada router al inicio de la configuración.

BOGOTA1(config-router)#passive-interface s0/0/0
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA3(config-router)#passive-interface g0/0
MEDELLIN1(config-router)#passive-interface s0/0/0
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#passive-interface g0/0

5.2.2.4 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.

Fueron tenidas en cuenta en la configuración del protocolo OSPF en cada router, como se evidencia en los pantallazos de la configuración inicial.

5.2.2.4.1 Configuración del Direccionamiento IP

Realización de la conexión física de los equipos con base en la topología de red.

5.2.2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Se ejecuta los siguientes comandos en ISP ISP>enable
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username MEDELLIN1 password cisco ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco

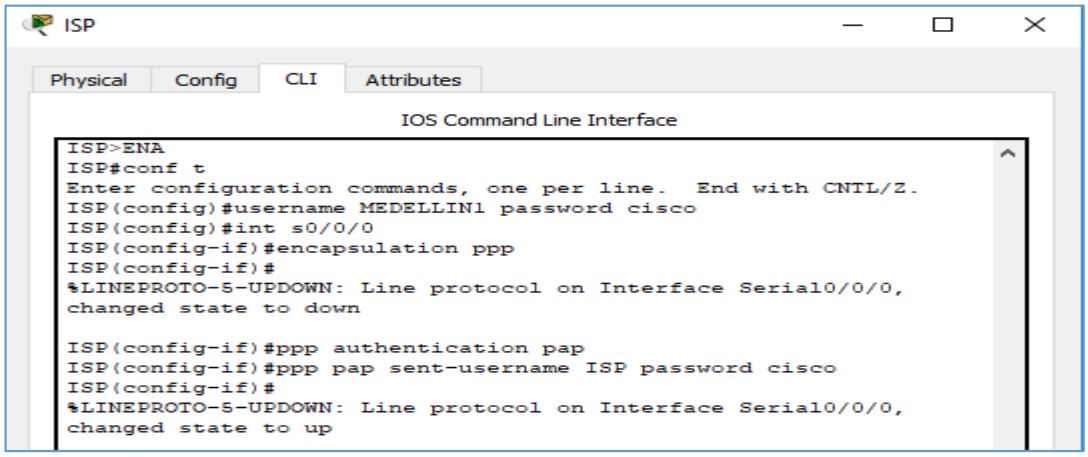


Figura 18 Configuración con la autenticación PAP en ISP.

Se ejecuta los siguientes comandos en MEDELLIN1
MEDELLIN1>enable
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.

MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username
MEDELLIN1 password cisco

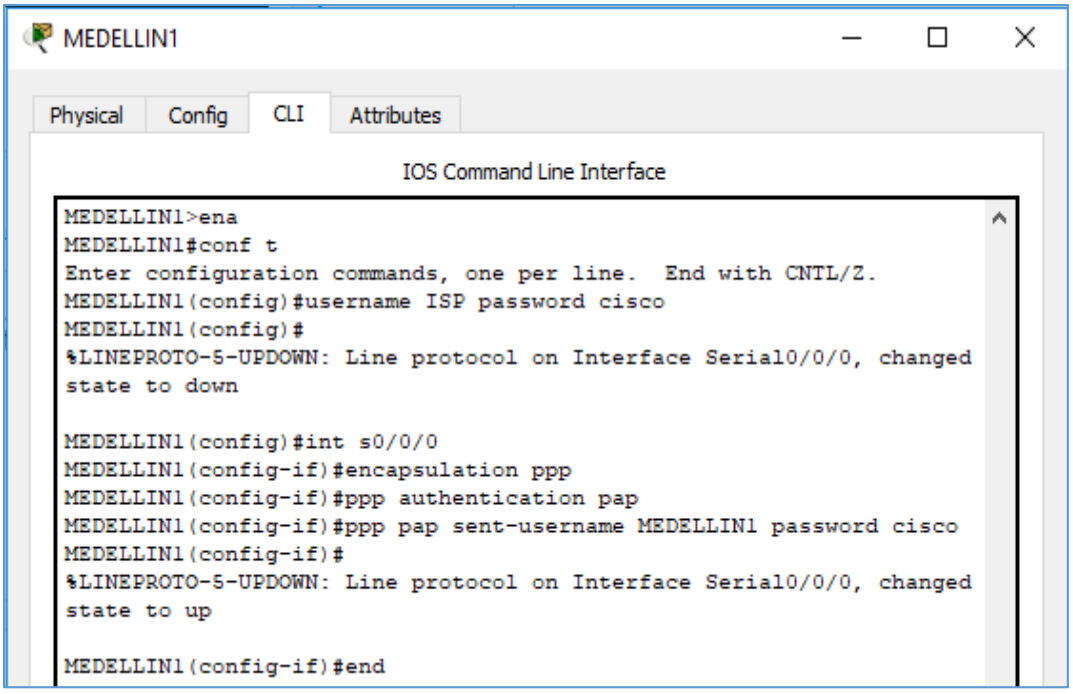


Figura 19 Configuración con la autenticación PAP en Router MEDELLIN1.

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

Se ejecutan los siguientes comandos en ISP
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap

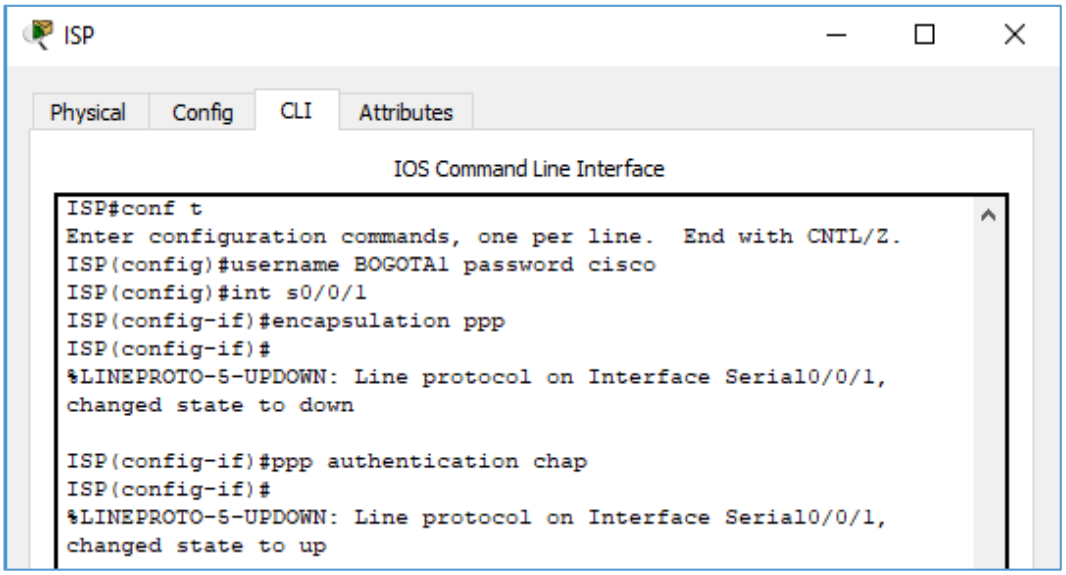


Figura 20 Configuración con la autenticación CHAP en Router ISP.

Se ejecutan los siguientes comandos en BOGOTA1

BOGOTA1>ena
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap

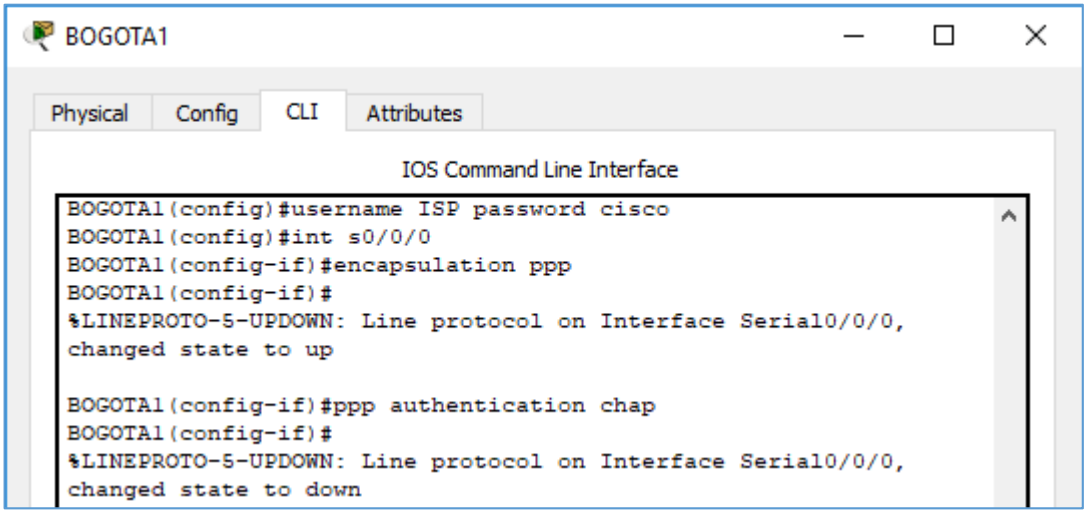


Figura 21 Configuración con la autenticación CHAP en Router BOGOTA1

5.2.2.6 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.

```
MEDELLIN1#ping 209.17.220.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (0/5), round-trip min/avg/max = 2/4/8
ms
```

Figura 22 Ping falla Medellin1 a Bogota1.

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.

```
MEDELLIN1>ena
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
```

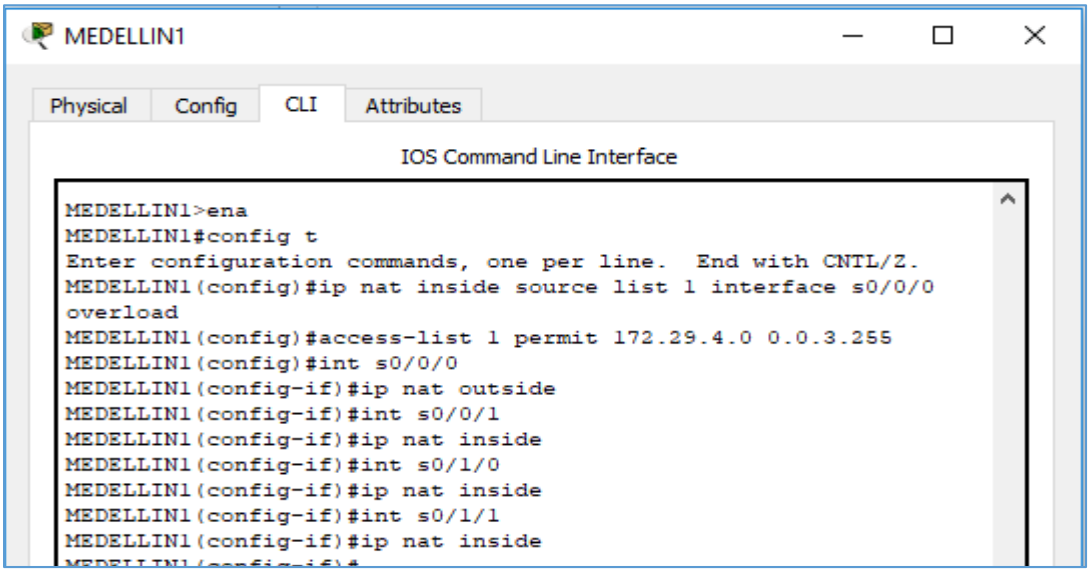


Figura 23 Activación de la PAT en Medellin1.

BOGOTA1>ena
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#

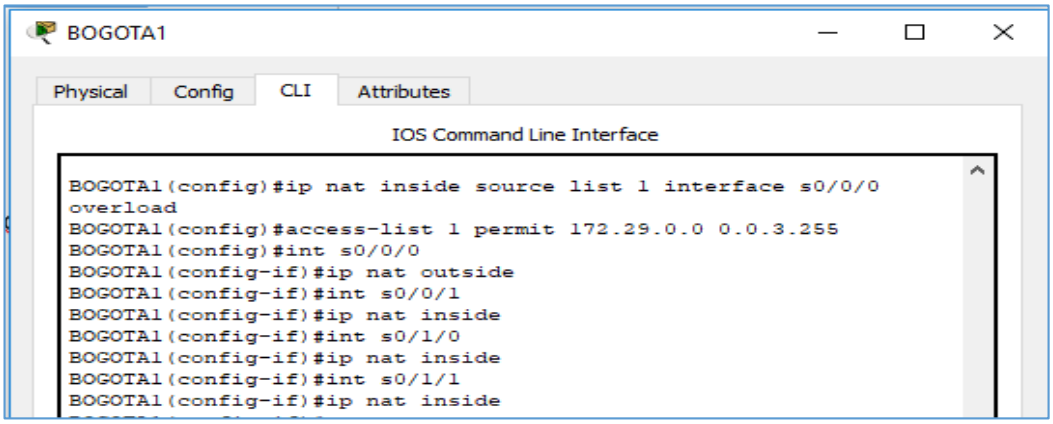


Figura 24 Activación de la PAT en Bogota1.

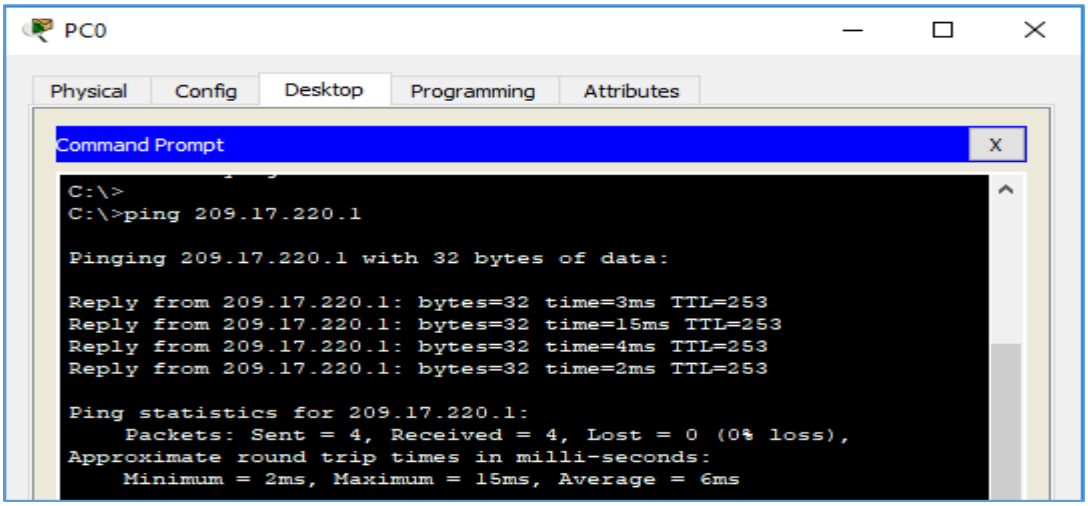


Figura 25 Ping ISP desde PC0.

Ejecución del comando show ip nat translation

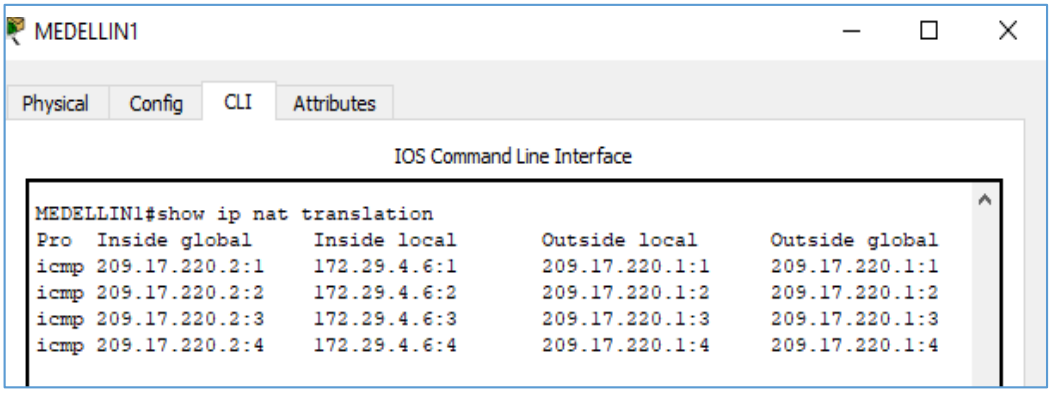


Figura 26 Indica la traducción de direcciones de puerto en Medellin1

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.

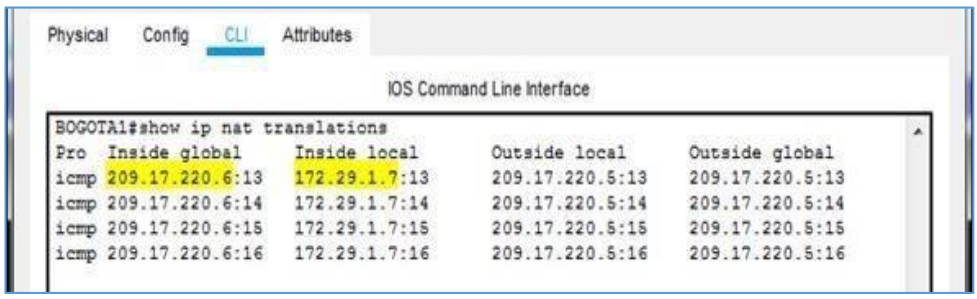


Figura 27 Indica la traducción de direcciones de puerto en Bogota1.

5.2.2.7 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.

Configuración DHCP en MEDELLIN2
MEDELLIN2>ena
MEDELLIN2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 MED2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MED3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit

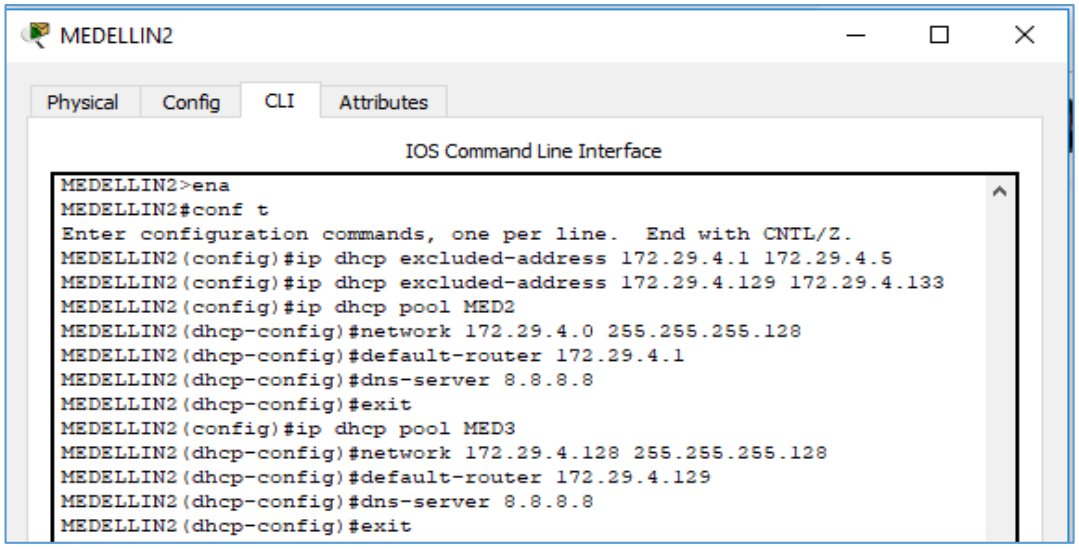


Figura 28 Configuración DHCP en Medellin2.

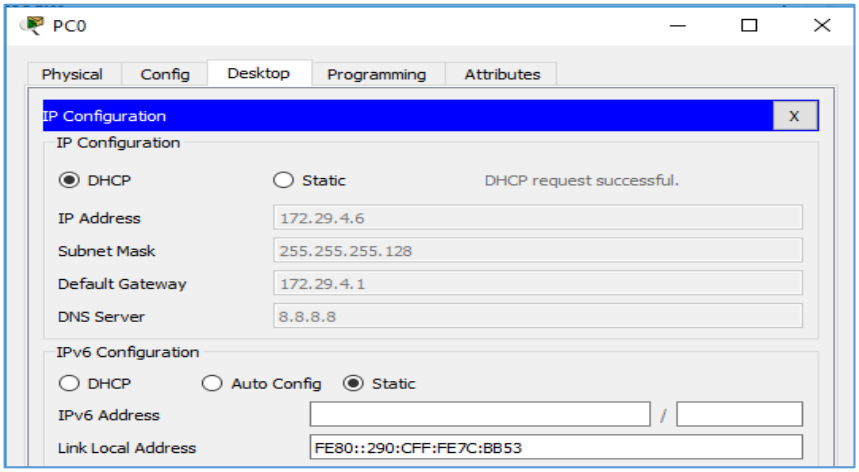


Figura 29 Asignación dirección IP a la PC0.

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

Creación de direccionamiento a MEDELLIN3.
MEDELLIN3>ena
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5

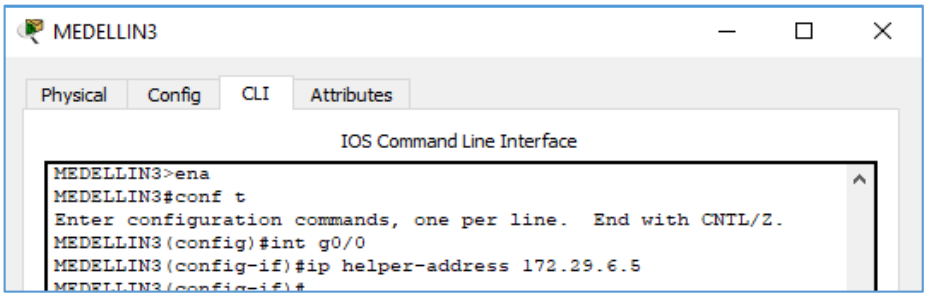


Figura 30 Configuración Medellin3.

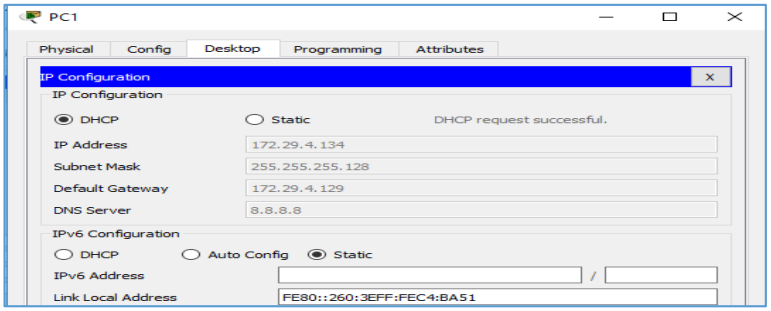


Figura 31 Asignación dirección IP a la PC1.

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

Creación del direccionamiento en Bogota2

BOGOTA2>ena
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 BOG2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8 BOGOTA2(dhcp-config)#ip dhcp pool BOG3 BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8

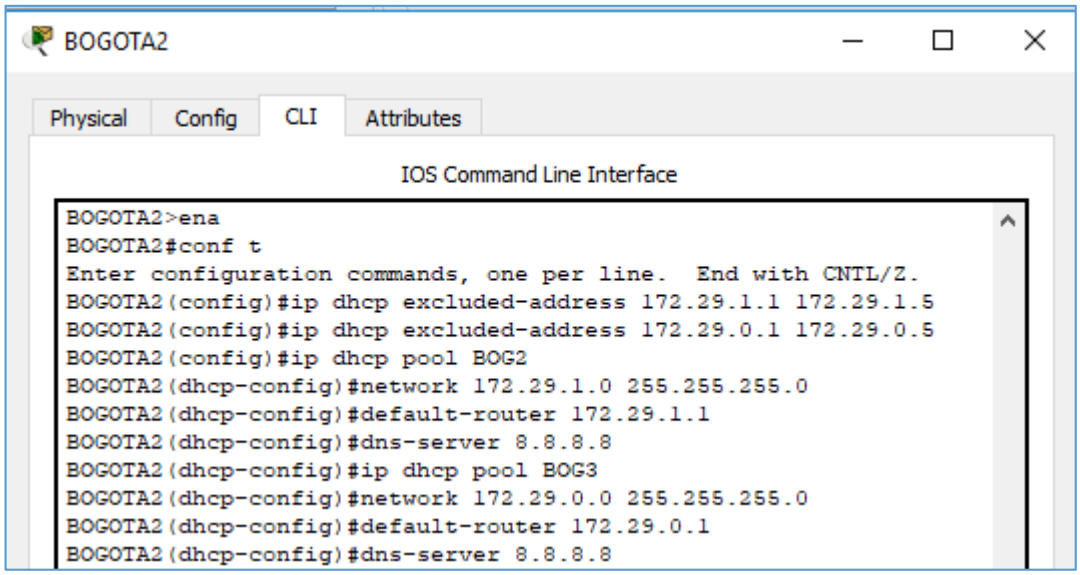


Figura 32 Configuración DHCP en Bogota2.

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

Creación de direccionamiento en Bogotá3.
BOGOTA3>ena
BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13

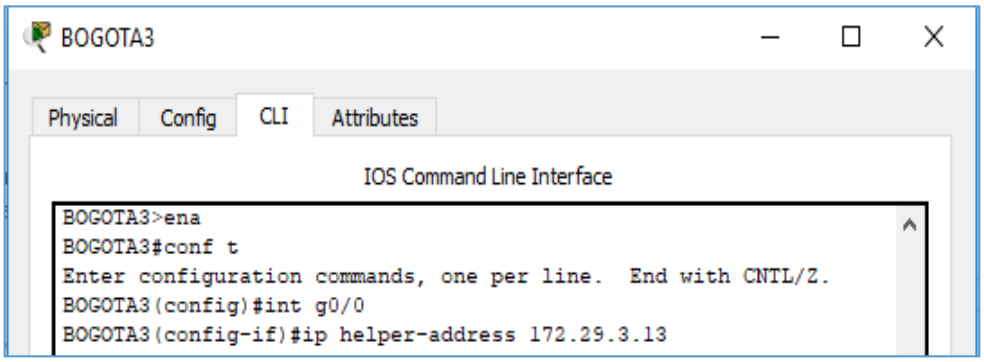


Figura 33 Configuración Bogota3.

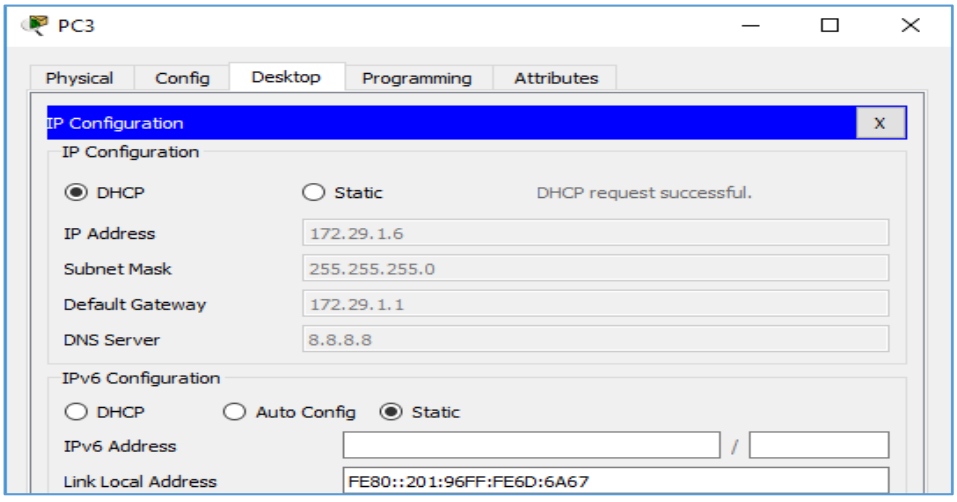


Figura 34 Asignación dirección IP a la PC3.

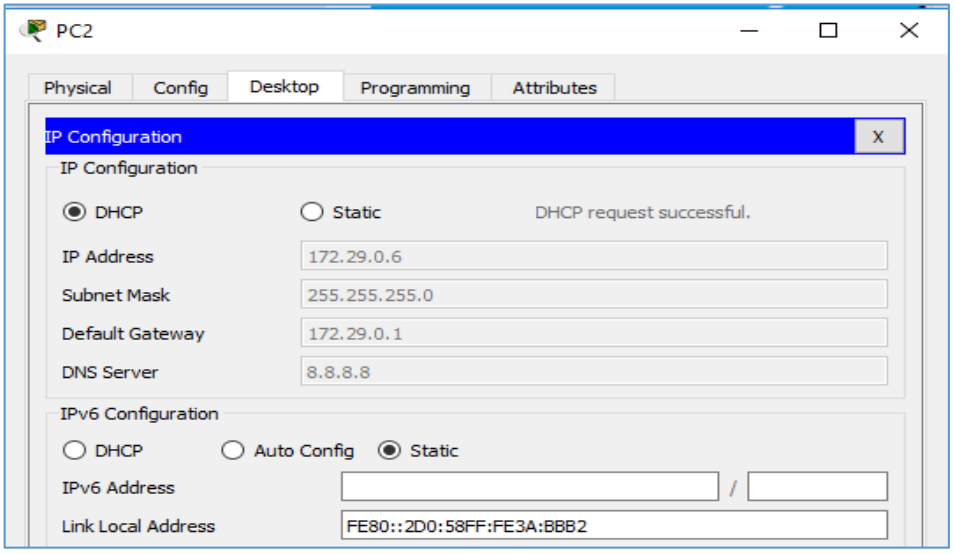


Figura 35 Asignación dirección IP a la PC2.

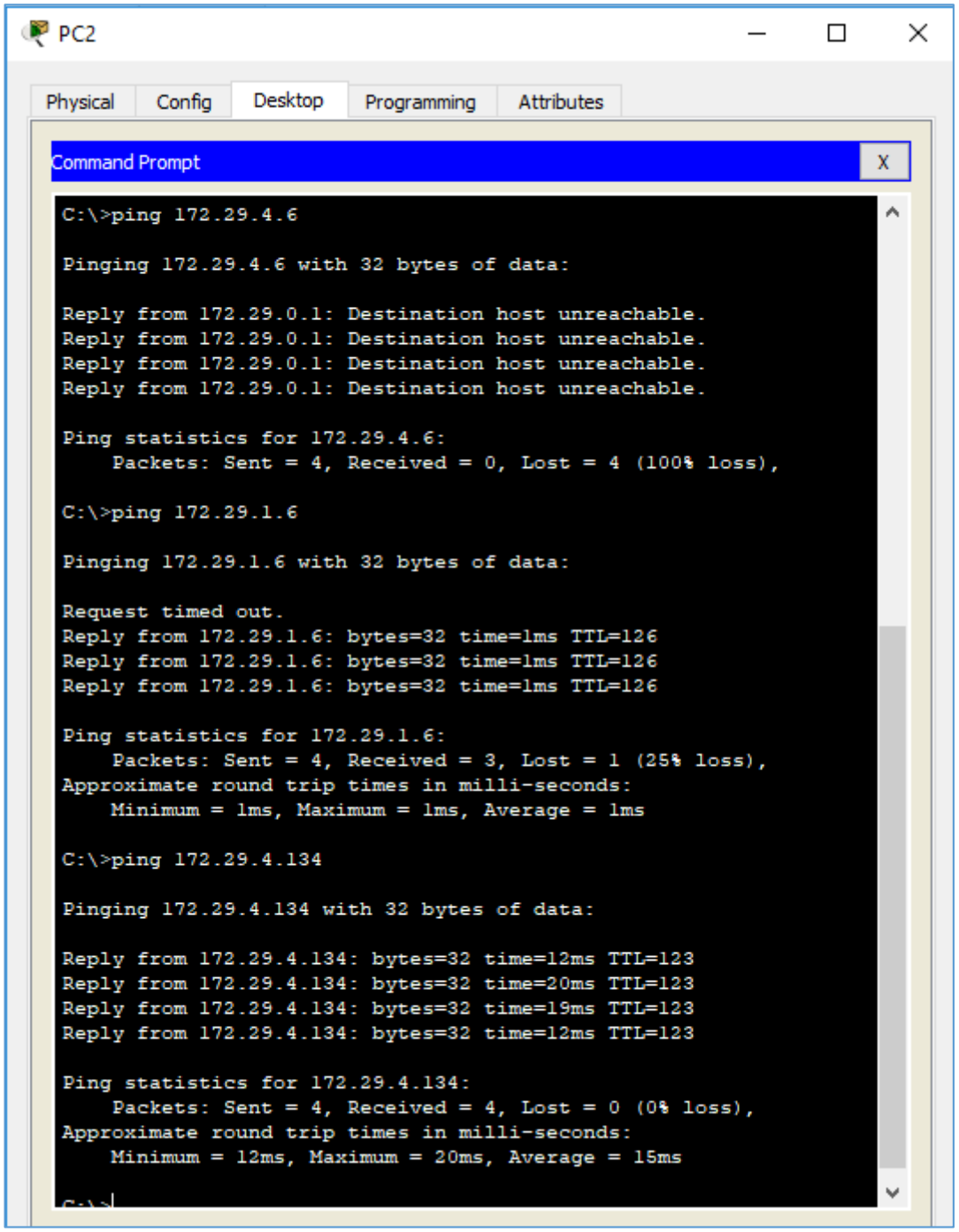


Figura 36 Ping puntos de extremo a extremo.

CONCLUSIONES

El desarrollo de esta prueba final de habilidades en CCNA, permite concluir que se pueden aplicar los conocimientos adquiridos dentro del tiempo del diplomado. Teniendo en cuenta que la EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA, requiere de tener concepciones claras, desde el autoaprendizaje, toda vez que los elementos teóricos se debieron asimilar de manera personal, sin embargo, se cumple la meta de haber elaborado una programación de una pequeña red, desde la orientación del programa y de los criterios aprendidos.

Todos estos aspectos se aplicaron en el desarrollo de las actividades que hicieron parte de la resolución del problema plantea, estableciendo los parámetros y funciones de verificación de una conexión entre dispositivos, la cual es proporcionada en la configuración inicial de la topología; así mismo, se configuró la ACL de los Routers, esto con el objetivo de reducir los posibles ataques desde equipos en forma remota, pero además, se logró la verificación de la funcionalidad de los procesos aplicados.

RECOMENDACIONES

Las condiciones de desarrollo de la evaluación de la prueba de habilidades, pese a que es un medio de reconocer las habilidades y conocimientos aprendidos, es recomendable que al momento de seleccionar los procesos, exista un mecanismo de propiciar el aprendizaje más que de identificar qué nota o calificación se puede lograr.

BIBLIOGRAFÍA

BAUTISTA, Dewar Willmer Rico; CÁRDENAS, Yurley Constanza Medina; JAIMES, Luz Marina Santos. IPSec de IPv6 en la universidad de Pamplona. scientia et Technica, 2008, vol. 14, no 39, p. 320-325.

Gont, F.. Qué hacer cuando las políticas de IPv4 e IPv6 discrepan. (2018, August 27 disponible en https://searchdatacenter.techtarget.com/es/consejo/Que-hacer-cuando-las-politicas-de-IPv4-e-IPv6-discrepan

PALIZA, Félix F. Alvarez. GUÍA PARA EL DISEÑO DE REDES EMPRESARIALES.(TRANSICIÓN IPv4-IPv6).

PAVÓN, Belén Colmenar; TELEMÁTICA, E. T. T. Diseño de una red WAN para una compañía nacional. UOC, Integración de redes telemáticas ETT Telemática, 2012.

ROSERO MUÑOZ, Marcelo Alejandro. Diseño y configuración de una red LAN-WAN, utilizando direccionamiento y servicios IPV6. 2017. Tesis de Licenciatura. CIENCIAS DE LA INGENIERÍA E INDUSTRIAS FACULTAD: INGENIERÍA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN.