SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE LA TECNOLOGIA “CISCO”

PRESENTADO POR:

HECTOR FABIO VALLECILLA ARCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

VALLE DEL CAUCA

PALMIRA

2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE LA TECNOLOGIA “CISCO”

PRESENTADO POR:

HECTOR FABIO VALLECILLA ARCO

TRABAJO DE GRADO:

INFORME FINAL DEL DIPLOMADO PARA OPTAR POR EL TITULO DE INGENIERIA EN ELECTRONICA

TUTOR

HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

VALLE DEL CAUCA

PALMIRA

2020

Nota de aceptación:

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Zarzal-Valle del Cauca 22 de mayo del 2020

DEDICATORIA A MIS PADRES

Este trabajo de grado esta dedicado principalmente a DIOS, a mis PADRES LIBIA ARCO Y ARCADIO VALLECILLA por ayudarme a completar este proceso de aprendizaje y alcanzar una meta propuesta en mi vida.

AGRADECIMIENTO

Quiero espresar mi gratitud a DIOS, que con su grande bendicion llena siempre mi vida, a mis padres que han sabido darme su ejemplo. Tambien quiero agradecer a la universidad nacional abierta y adistancia, directivos y profesores de este programa academico, por todas las oportunidades adquiridas en estos años que enriquecen mi conocimiento.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Comprender el papel tan importante que desempeñan las telecomunicaciones en el desarrollo del mundo actual, es por esto que entender como es el funcionamiento a través de las redes de información es visto por la universidad nacional abierta y a distancia UNAD como base fundamental en desarrollo académico de los próximos ingenieros electrónicos, es por esto que en convenio con CISCO Networking Academy, han puesto a disposición el diplomado: “CISCO diseño e implementación de redes LAN-WAN”, donde el estudiante dispone de dos módulos, el primero bajo el título de CCNA1: Switching y routing: Introducción a redes, se enfoca en brindar la capacidad al estudiante de construir redes LAN simples, realizar configuraciones básicas para enrutadores e interruptores, e implementar esquemas de direccionamiento IP, el segundo CCNA2: Routing y switching: Principios básicos de routing y switching, ese encamina en presentar herramientas para configurar y solucionar problemas de enrutadores y cambia y resuelve problemas comunes con RIPv1, RIPv2, área única y área múltiple OSPF, LAN virtuales y enrutamiento entre VLAN en ambas redes IPv4 e IPv6, es por esto que como complemento y evaluación se dispone de la prueba de habilidades prácticas, la cual se desarrolla en este documento y que pretende demostrar al estudiante las habilidades desarrolladas.

PALABRAS CLAVE

COMANDO PING, COMANDO SHOW IP ROUTER, PROTOCOLO RIPV2, PROTOCOLO OSPF, CONFIGURACION IPV4, CONFIGURACION IPV6, CONFIGURACION DHCP

1. INTRODUCCIÓN

La Prueba de habilidades prácticas forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking en el cual se aplicará enrutamiento, parámetros de seguridad y acceso en diferentes dispositivos en la red, además de las configuraciones OSPF, RIP ver 2.0, implementación DHCP, NAT, verificación de ACL.

El desarrollo del trabajo de realizo en el simulador packet tracer en donde se evidencia en un informe la solución de los diferentes escenarios que a su vez relacionan mucho con problemas encontrados en la vida cotidiana y nos sirve para afrontarlos con seguridad por el gran conocimiento adquirido.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Solucionar dos estudios de caso bajo el uso de la tecnologia “cisco” colocando en practica las habilidades y conocimientos adquiridos durante el curso.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Configurar dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en los Router y demás políticas necesarias
- Realizar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing, de DHCP, NAT, RIP Ver2 y demás permitiendo dar solución a ciertos problemas.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICION DEL PROBLEMA

Busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado dando solucion a los 2 escenarios.
En el escenario 1 comprende en configurar los diferentes dispositivos que admita conectividad en ipv4, ipv6,seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. En el escenario 2 como administrador de red se 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. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

3.2 JUSTIFICACION

El desarrollo de este trabajo se aprende configurarlos diversos dispositivos como router, swiches, pc dando uso a los diferentes comandos de verificacion. Se es muy familiar el desarrollo de los diferentes escenarios y creacion de topologias de red ya que no enfoca a la solucion de problemas y a reforzar la seguriadad en los equipos.

4. DESARROLLO DEL PROYECTO

4.1 ESCENARIO 1

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

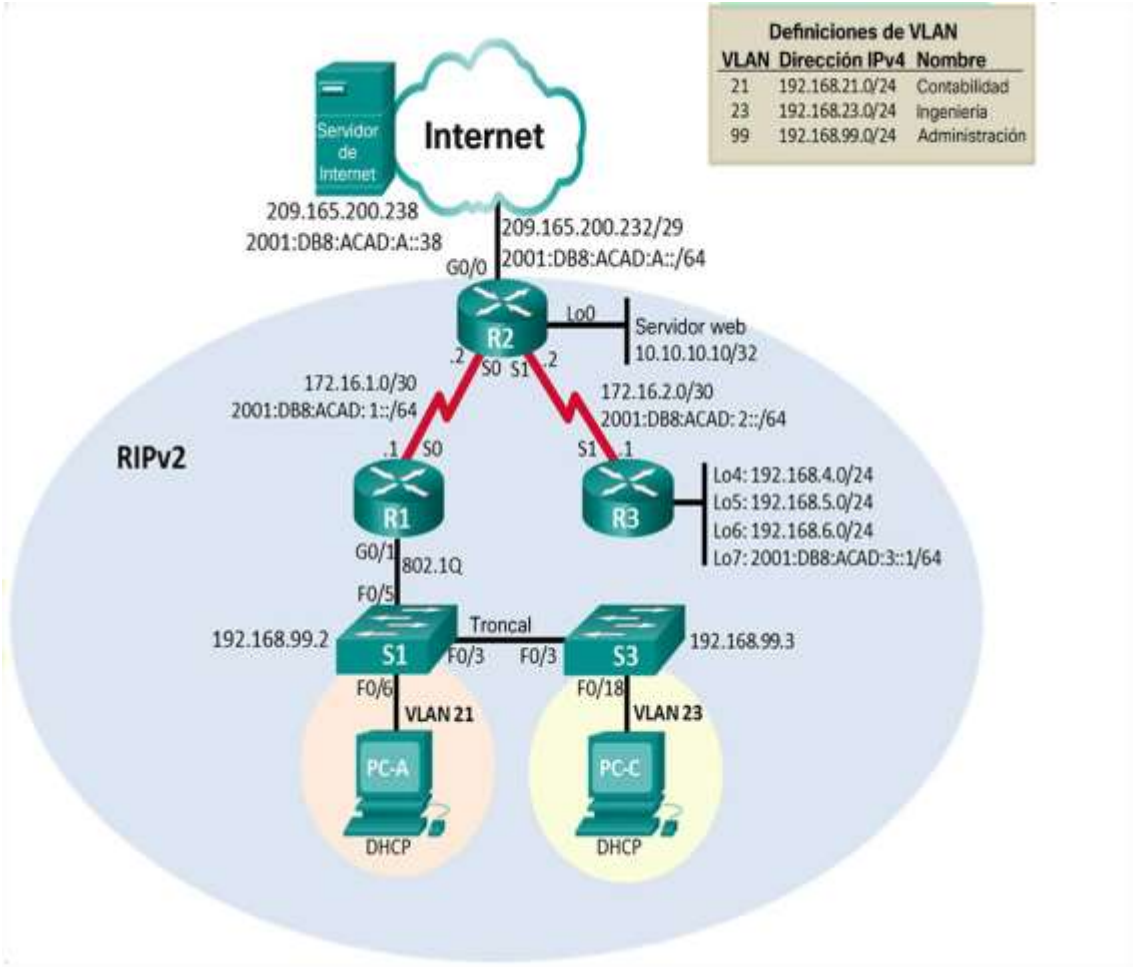

Figura 1. topologia escenario 1

TOPOLOGIA PACKET TRACER

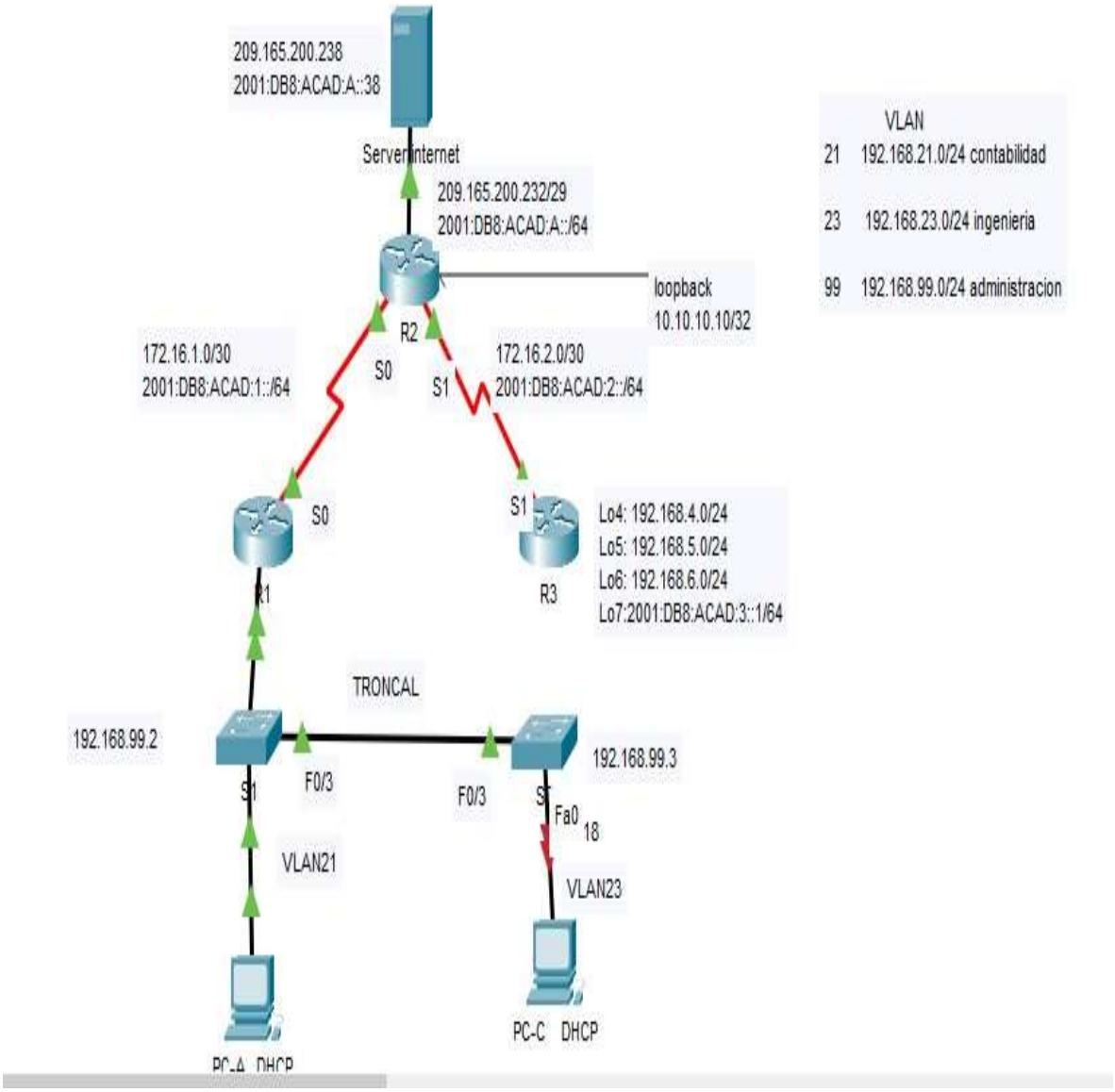

Figura 2. Topologia escenario 1 packet tracer

Parte 1: Inicializar dispositivos

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 1. Configuracion inicial

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**
Volver a cargar ambos switches	**#reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**#show vlan brief**

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

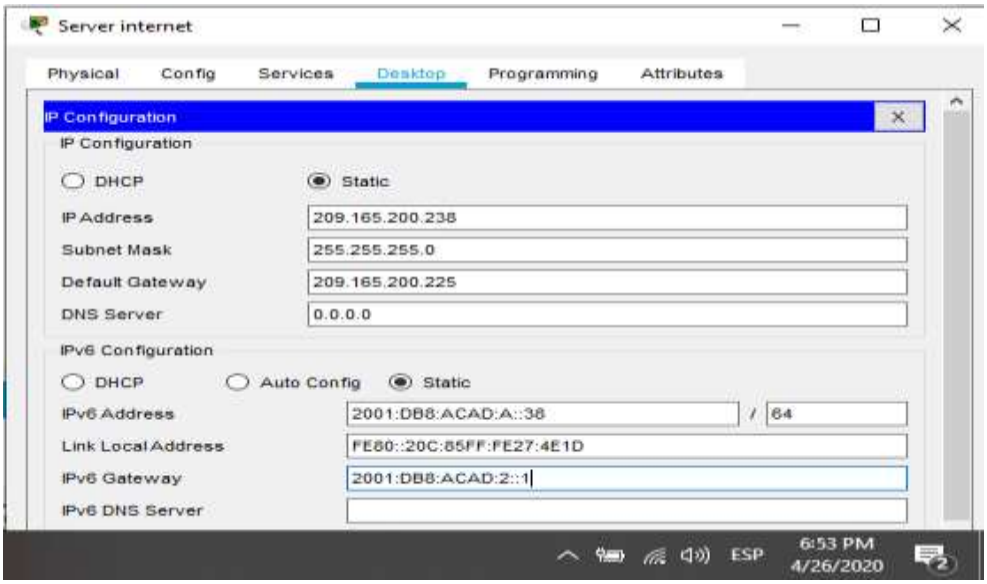

Figura 3. configuracion PC internet

Tabla 2 configuracion computadora internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	**209.165.200.238**
Máscara de subred para IPv4	**255.255.255.0**
Gateway predeterminado	**209.165.200.225**
Dirección IPv6/subred	**2001:DB8:ACAD:A::38**
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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuracion en R1 claves- interfaces

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**No ip domain-lookup**
Nombre del router	**R1**
Contraseña de exec privilegiado cifrada	**class**
Contraseña de acceso a la consola	**cisco**
Contraseña de acceso Telnet	**cisco**
Cifrar las contraseñas de texto no cifrado	**Service password-encryption**
Mensaje MOTD	**#Se prohíbe el acceso no autorizado!#**
Interfaz S0/0/0	**Establezca la descripción R1-R2** **Establecer la dirección IPv4 1712.16.1.1 255.255.255.252** **Establecer la dirección IPv6 2001:DB8:ACAD:1::1/64** **Establecer la frecuencia de reloj en 128000** **Activar la interfaz**
Rutas predeterminadas	**Configurar una ruta IPv4 predeterminada de S0/0/0** **Configurar una ruta IPv6 predeterminada de S0/0/0**

Comandos configuracion R1

Router#config t

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd #Se prohibe el acceso no autorizado!#

R1(config)#ipv6 unicast-routing

R1(config)#interface serial 0/0/0

R1(config-if)#ip address 172.16.1.1 255.255.255.252

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

R1(config-if)#clock rate 128000

R1(config-if)#description R1-R2

R1(config-if)#no shutdown

R1(config)#ipv6 route ::/0 serial 0/0/0

R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0

Nota: Todavía no configure G0/1

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4 Configuracion en R2 claves- interfaces

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**#No ip domain-lookup**
Nombre del router	**#hostname R2**
Contraseña de exec privilegiado cifrada	**class**
Contraseña de acceso a la consola	**cisco**
Contraseña de acceso Telnet	**cisco**
Cifrar las contraseñas de texto no cifrado	**#Service password-encryption**

Habilitar el servidor HTTP	**#Ip http secure-server**
Mensaje MOTD	**#Se prohíbe el acceso no autorizado!#**
Interfaz S0/0/0	Establezca la descripción **R2-R1** Establezca la dirección IPv4 Utilizar la siguiente dirección disponible en la subred. **172.16.1.2 255.255.255.252** Establezca la dirección IPv6. **20001:DB8:ACAD:1::1/64** Activar la interfaz
Interfaz S0/0/1	Establecer la descripción **R2-R3** Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.**172.16.2.1 255.255.255.255** Establezca la dirección IPv6. **2001:DB8:ACAD:2::1/64** Establecer la frecuencia de reloj en **128000.** Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. **R2-internet** Establezca la dirección IPv4 Utilizar la primera dirección disponible en la subred.. **209.165.200.233 255.255.255.248** Establezca la dirección IPv6. **2001:DB8:ACAD:A::1/64** Activar la interfaz
Interfaz loopback 0 G0/01 (servidor web simulado)	Establecer la descripción.**R2-web server** Establezca la dirección IPv4. **10.10.10.1 255.255.255.0**
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Comandos configuracion R2

Router#config t

Router(config)#no ip domain-lookup

Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #Se prohibe el acceso no autorizado!#
R2(config)#ip http server
R2(config)#ipv6 unicast-routing
R2(config)#interface serial 0/0/0
R2(config-if)#description R2-R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R2(config-if)#no shutdown
R2(config-if)#interface serial 0/0/1
R2(config-if)#description R2-R3
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#interface g0/0
R2(config-if)#description R2-Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
R2(config-if)#interface g0/1

R2(config-if)#description R2-Web server

R2(config-if)#ip address 10.10.10.1 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#

R2(config)#ipv6 route ::/0 g0/0

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configuracion en R3 claves- interfaces

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**#No ip domain-lookup**
Nombre del router	**# hostname R3**
Contraseña de exec privilegiado cifrada	**class**
Contraseña de acceso a la consola	**cisco**
Contraseña de acceso Telnet	**cisco**
Cifrar las contraseñas de texto no cifrado	**#Service password-encryption**
Mensaje MOTD	**#Se prohíbe el acceso no autorizado!#**
Interfaz S0/0/1	Establecer la descripción R3-R2 Establezca la dirección IPv4. **172.16.2.2 255.255.255.252**Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. **2001:DB8:ACAD:2::1/64**Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

Interfaz loopback 4	Establezca la dirección IPv4. **192.168.4.1 255.255.255.0** Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4.**192.168.5.1 255.255.255.0** Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4.**192.168.5.1 255.255.255.0** Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. **2001:DB8:ACAD:3::1/64** Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Comandos configuracion R3

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#no ip domain-lookup

Router(config)#hostname R3

R3(config)#enable secret class

R3(config)#line console 0

R3(config-line)#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 serial 0/0/1

R3(config-if)#exit

R3(config)#ipv6 unicast-routing

R3(config)#interface serial 0/0/1

R3(config-if)#description R3-R2

R3(config-if)#ip address 172.16.2.2 255.255.255.252

R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64

R3(config-if)#no shutdown

R3(config-if)#

R3(config)#interface lo4

R3(config-if)#ip address 192.168.4.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config-if)#interface lo5

R3(config-if)#ip address 192.168.5.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config-if)#interface lo6

R3(config-if)#ip address 192.168.6.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#ipv6 unicast-routing

R3(config-if)#interface lo7

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

R3(config-if)#no shutdown

R3(config-if)#exit

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6 Configuracion S1- claves

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**#no ip domain-lookup**
Nombre del switch	**#hostname S1**
Contraseña de exec privilegiado cifrada	**#enable secret class**
Contraseña de acceso a la consola	**#line console 0** **#password cisco**
Contraseña de acceso Telnet	**#line vty 0 4** **#password cisco**
Cifrar las contraseñas de texto no cifrado	**#service password-encryption**
Mensaje MOTD	**#banner motd# Se prohíbe el acceso no autorizado!#**

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7 Configuracion S3- claves

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	**#no ip domain-lookup**
Nombre del switch	**#hostname S1**
Contraseña de exec privilegiado cifrada	**#enable secret class**

Contraseña de acceso a la consola	**#line console 0** **#password cisco**
Contraseña de acceso Telnet	**#line vty 0 4** **#password cisco**
Cifrar las contraseñas de texto no cifrado	**#service password-encryption**
Mensaje MOTD	**#banner motd# Se prohíbe el acceso no autorizado!#**

Paso 7: Verificar la conectividad de la red

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

Tabla 8 Verificacion conectividad R1-R2-R3

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Successful (exitoso)
R2	R3, S0/0/1	172.16.2.2	Successful (exitoso)
PC de Internet	Gateway predeterminado	209.165.200.225	Successful (exitoso)

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

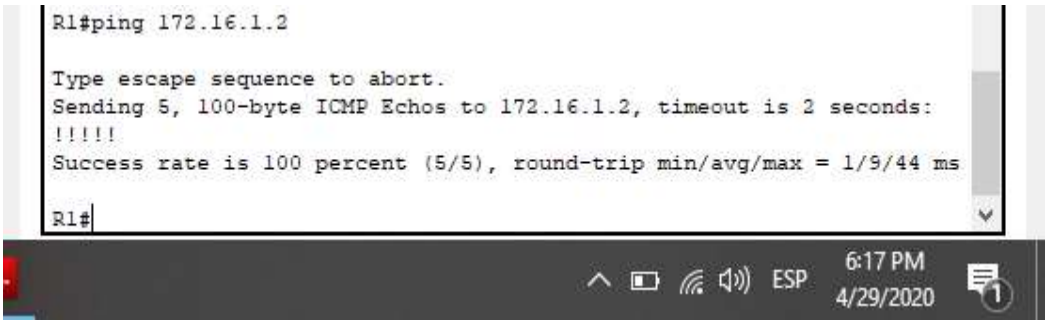

Figura 4. Ping R1-R2

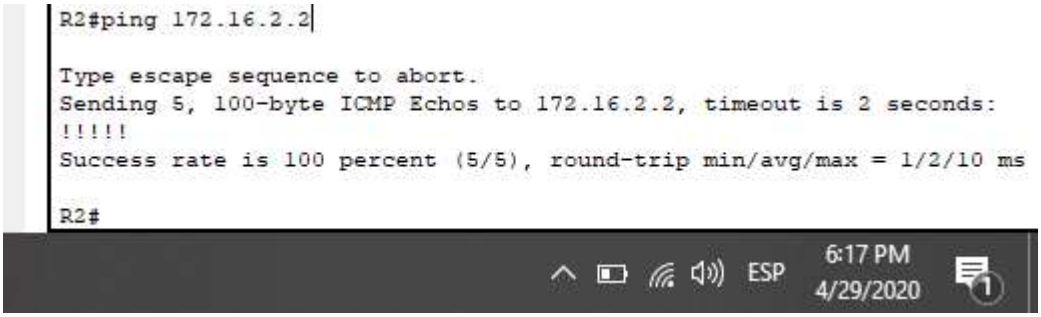

Figura 5. Ping R2-R3

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Configuracion S1- VLAN

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

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 **192.168.99.2**
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. **192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	**#interface range**

Comandos configuracion S1

S1#config t

S1(config)#vlan 21

S1(config-vlan)#name Contabilidad

S1(config-vlan)#vlan 23

S1(config-vlan)#name Ingenieria

S1(config-vlan)#vlan 99

S1(config-vlan)#name Administracion

S1(config-vlan)#exit

S1(config)#interface vlan 99

S1(config-if)#ip address 192.168.99.2 255.255.255.0

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.99.1

S1(config)#interface f0/3

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#exit

S1(config)#interface f0/5

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#exit

S1(config)#

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface range f0/1-2, f0/4-23, g0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#interface f0/6

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 21

S1(config-if)#interface range f0/1-2, f0/4, f0/7-23, g0/1-2

S1(config-if-range)#shutdown

Figura 6. Configuracion S1-VLAN

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10 Configuracion S3-VLAN

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.
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 **192.168.99.3**
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. **192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	**#interface range**

Comandos configuracion S3

S3#conf t

S3(config)#vlan 21

S3(config-vlan)#name Contabilidad

S3(config-vlan)#vlan 23

S3(config-vlan)#name Ingenieria

S3(config-vlan)#vlan 99

S3(config-vlan)#name Administracion

S3(config-vlan)#interface vlan 99

S3(config-if)#

S3(config-if)#ip address 192.168.99.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.99.1

S3(config)#interface f0/3

S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 1

S3(config-if)#interface f0/18

S3(config-if)#switchport mode access

S3(config-if)#switchport access vlan 21

S3(config-if)#exit

S3(config)#interface range f0/1-2, f0/4-17, f0/17-24, g0/1-2

S3(config-if-range)#switchport mode access

S3(config-if-range)#shutdown

S3(config-if-range)#exit

S3(config)#exit

Figura 7. configuracion S3-VLAN

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuracion R1-VLAN

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
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

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
Activar la interfaz G0/1	

Comandos configuracion R1

R1#config t

R1(config)#interface g0/1

R1(config-if)#exit

R1(config)#interface g0/1.21

R1(config-subif)#description LAN_C

R1(config-subif)#description LAN_Contabilidad

R1(config-subif)#encapsulation dot1q 21

R1(config-subif)#ip address 192.168.21.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface g0/1.23

R1(config-subif)#description LAN_Ingenieria

R1(config-subif)#encapsulation dot1q 23

R1(config-subif)#ip address 192.168.23.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface g0/1.99

R1(config-subif)#description LAN_Administracion

R1(config-subif)#encapsulation dot1q 99

R1(config-subif)#ip address 192.168.99.1 255.255.255.0

R1(config-subif)#exit

R1(config)#interface g0/1

R1(config-if)#no shutdown

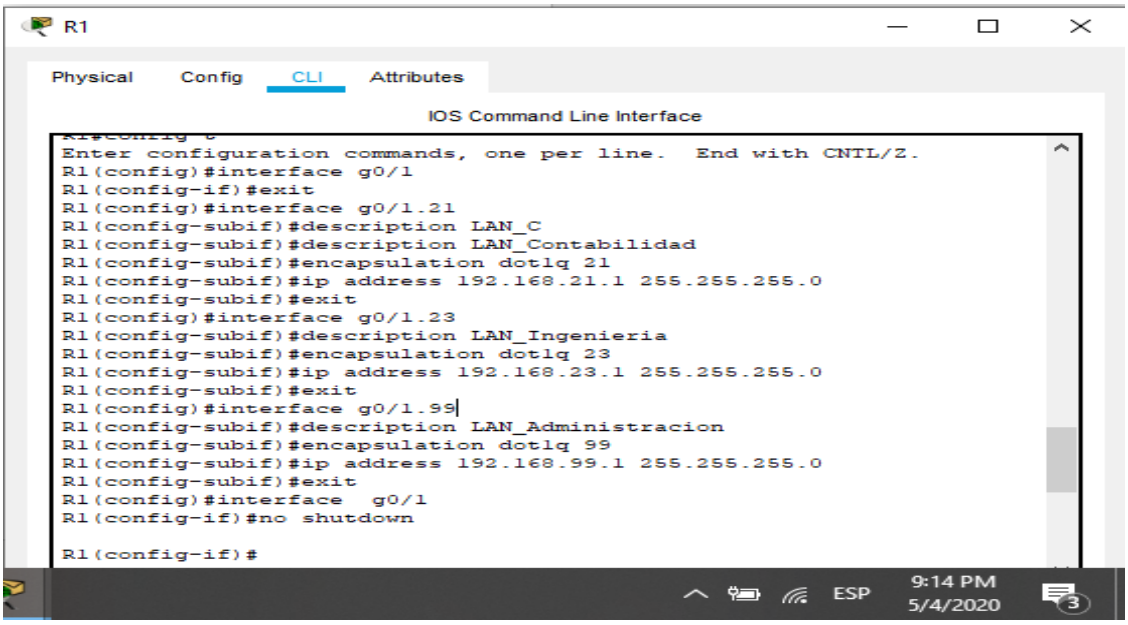

Figura 8. configuracion R1-VLAN

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 12 Verificacion conectividad switches-R1

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Successful(exitoso)
S3	R1, dirección VLAN 99	192.168.99.1	Successful(exitoso)
S1	R1, dirección VLAN 21	192.168.21.1	Successful(exitoso)
S3	R1, dirección VLAN 23	192.168.23.1	Successful(exitoso)

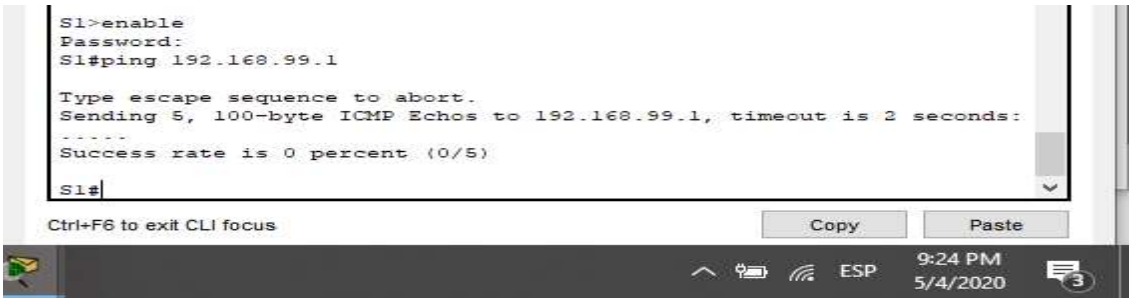

Figura 9. Ping S1-R1 VLAN99

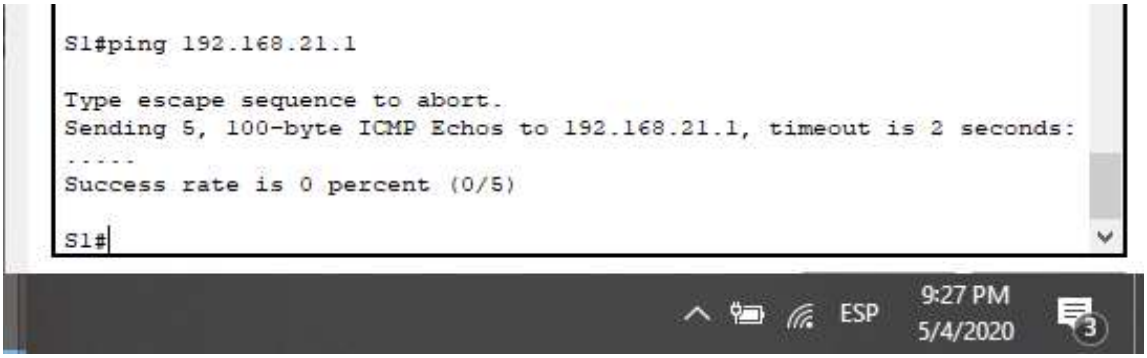

Figura 10. Ping S1-R1 VLAN21

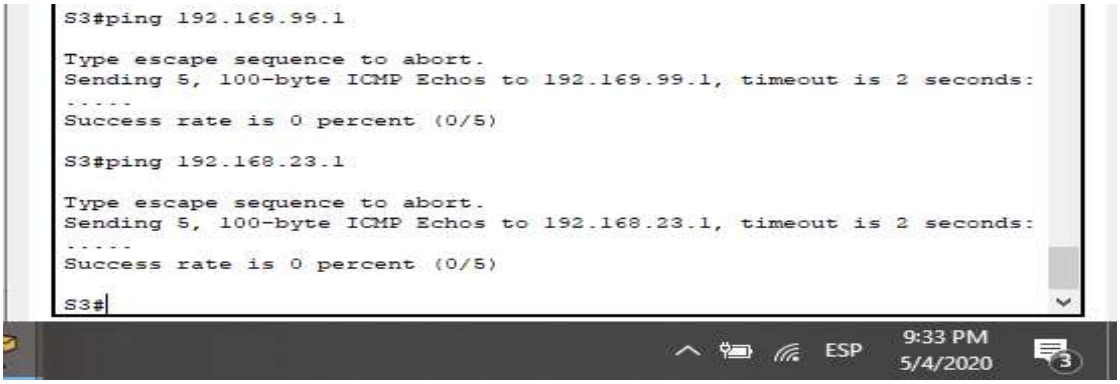

Figura 11. Ping S3-R1 VLAN99 S3-R1 VLAN23

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 configuracion RIPV2-R1

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	**#route rip** **#version 2**
Anunciar las redes conectadas directamente	**S0/0/0 172.16.1.0** **G0/1.21 192.168.21.0** **G0/1.23 192.168.23.0** **G0/1.99 192.168.99.0**
Establecer todas las interfaces LAN como pasivas	**#passive-interface**
Desactive la sumarización automática	**#no auto-summary**

Figura 12. Configuracion RIPV2-R1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 configuracion RIPV2-R2

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	**#route rip** **#version 2**
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. **S0/0/0 172.16.1.0** **S0/0/1 172.16.2.0** **G0/1 10.10.10.0**
Establecer la interfaz LAN (loopback) como pasiva	**#passive-interface**
Desactive la sumarización automática.	**#No auto-summary**

Figura 13. Configuracion RIPV2-R2

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. configuracion RIPV2-R3

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	**#version 2**
Anunciar redes IPv4 conectadas directamente	**S0/0/1 172.16.2.2** **Lo4 192.168.4.1** **Lo5 192.168.5.1** **Lo6 192.168.6.1**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	**#passive-interface**
Desactive la sumarización automática.	**#no auto-summary**

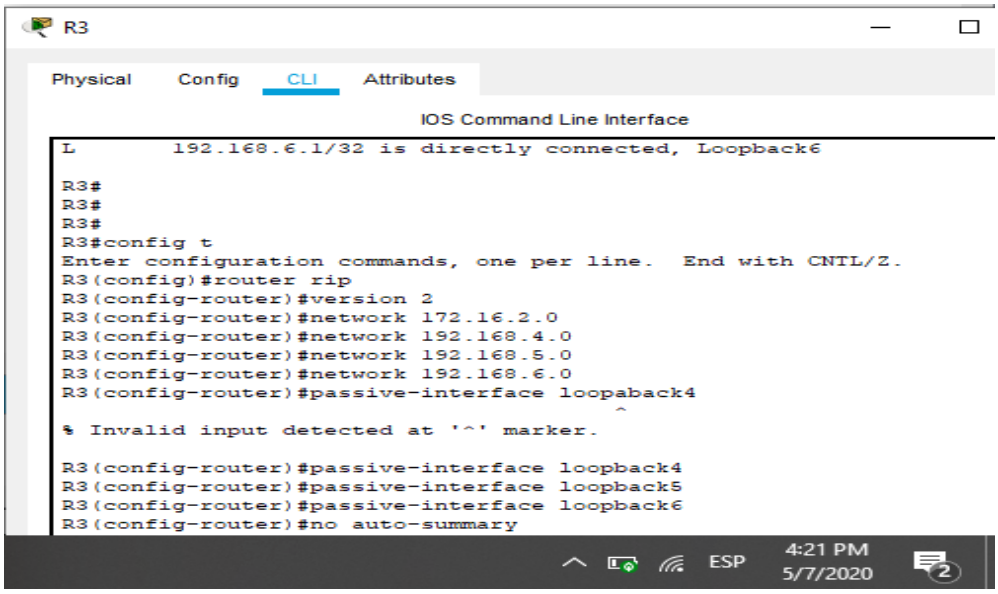

Figura 14. Configuracion RIPV2-R3

Paso 4: Verificar la información de RIP

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

Tabla 16 verificacion informacion 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**
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**#show ip protocols**

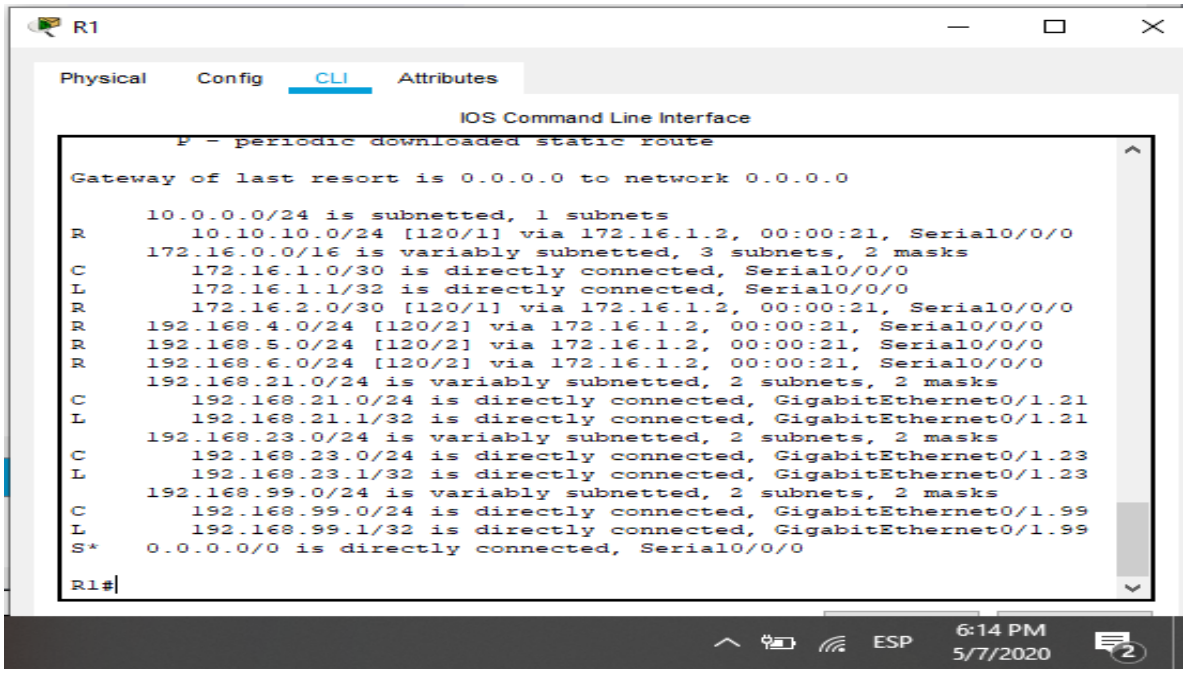

Figura 15. verificacion RIP -R1

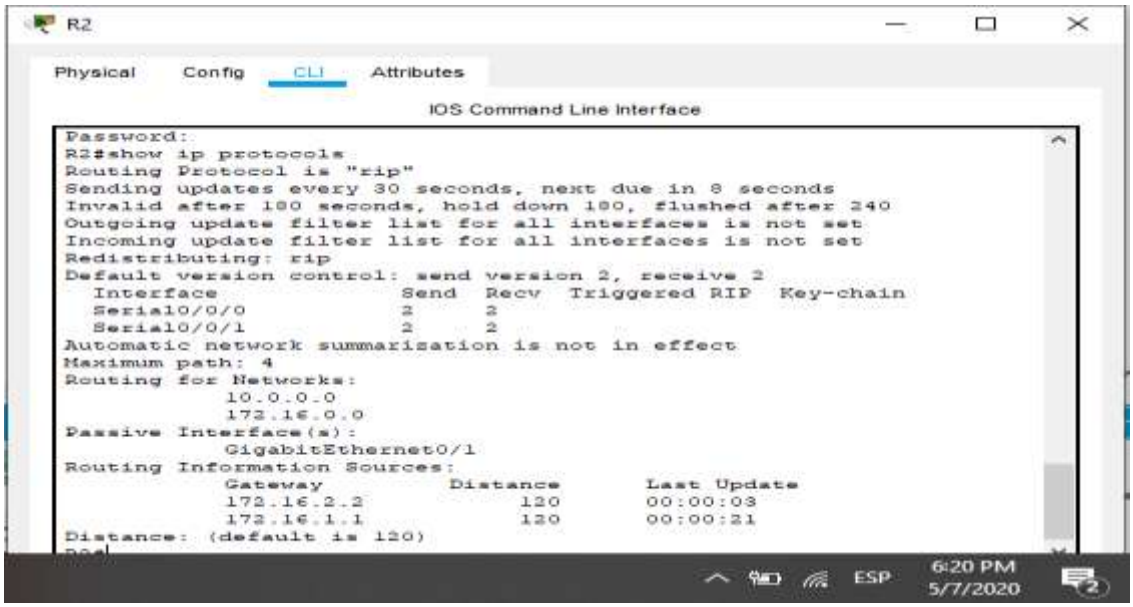

Figura 16. . Verificacion RIP-R2

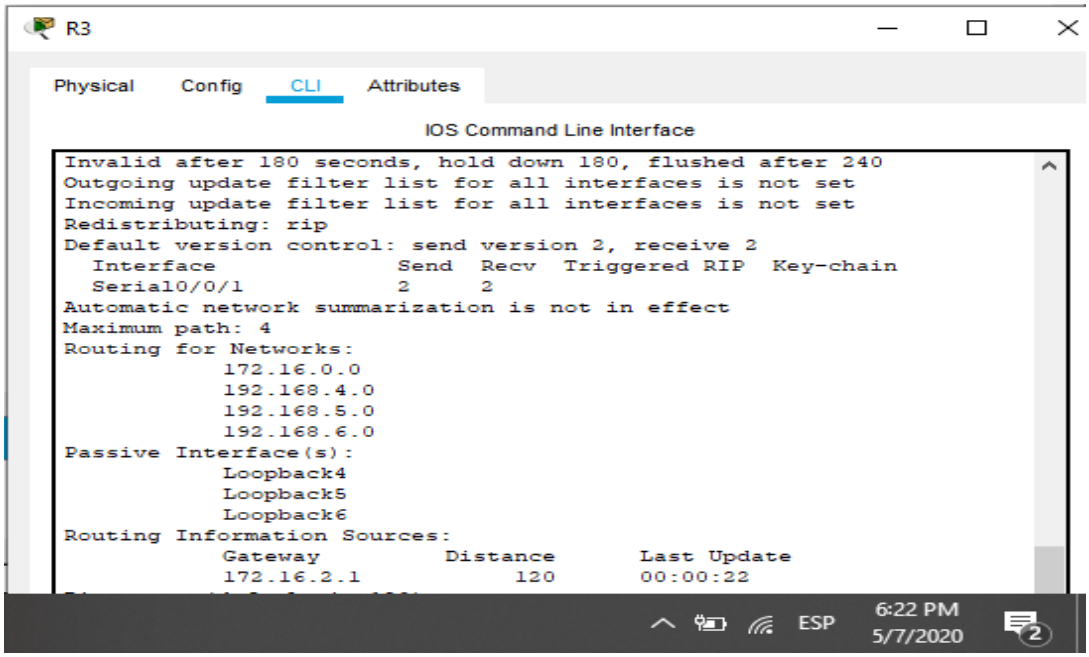

Figura 17. Verificacion RIP- R3

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17.Configuracion DCHP en R1

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	**192.168.21.1 192.168.21.20**
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	**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
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

Comandos configuracion R1 -DHCP

```
R1(config)#ip dhcp excluded-address 192.168.21.1  192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1  192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#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

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

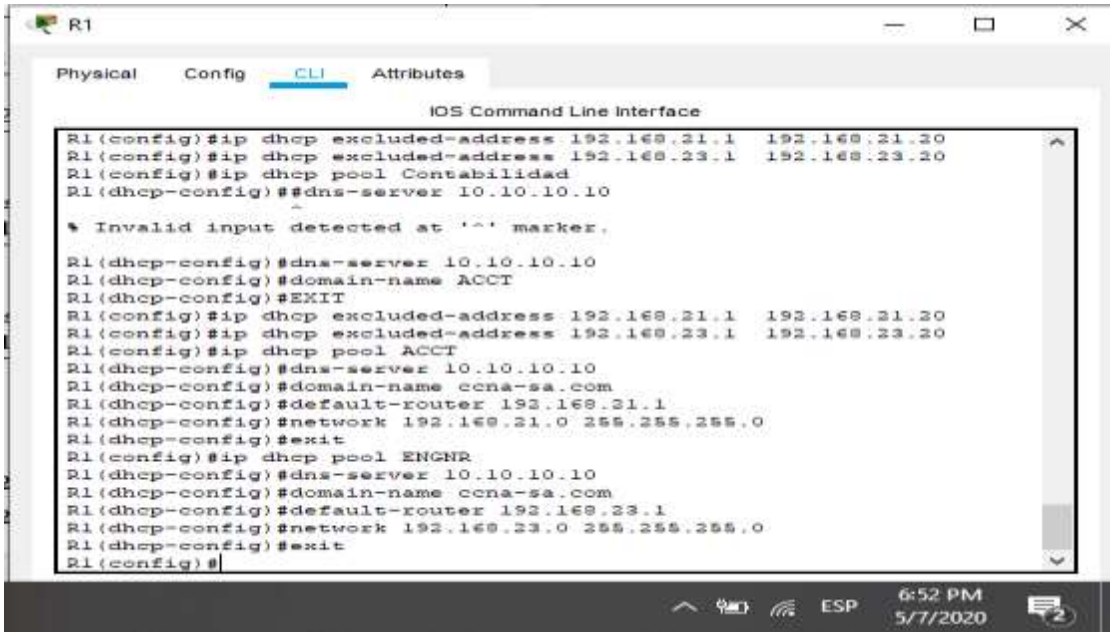

Figura 18. configuracion DCHP en R1

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18.Nat estatica y dinamica en R1

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**

Habilitar el servicio del servidor HTTP	**#Ip http server**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**#Ip http authentication local**
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
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**
Definir la traducción de NAT dinámica	

Comandos configuracion NAT -R1

R2(config)#user webuser privilege 15 secret cisco12345

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 g0/1

R2(config-if)#ip nat inside

R2(config-if)#exit

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

R2(config)#ip nat pool INTERNET 209.165.200.255 209.165.200.228 netmask 255.255.255.248

R2(config)#ip nat inside source list 1 pool INTERNET

R2(config)#

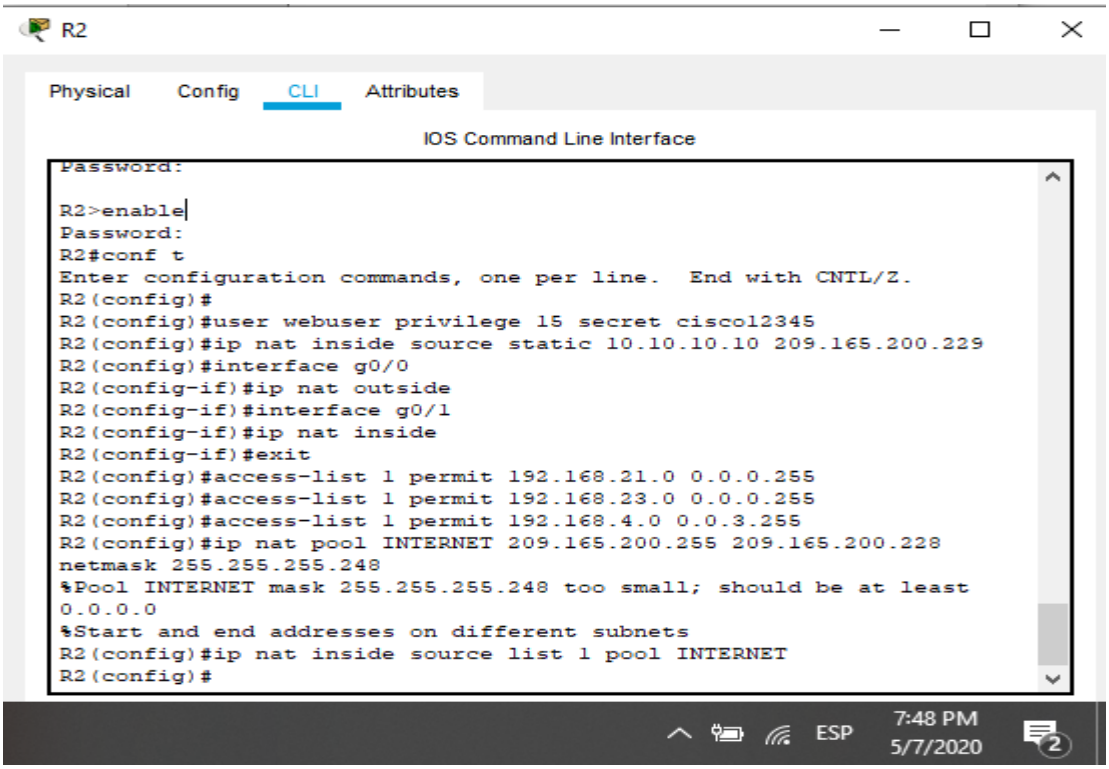

Figura 19. Nat estatica y dinamica en R1

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.

- Verificar que la PC-A haya adquirido información de IP del servidor de DHCP
- Verificar que la PC-C haya adquirido información de IP del servidor de DHCP
- Verificar que la PC-A pueda hacer ping a la PC-C

- Nota: Quizá sea necesario deshabilitar el firewall de la PC.

- 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

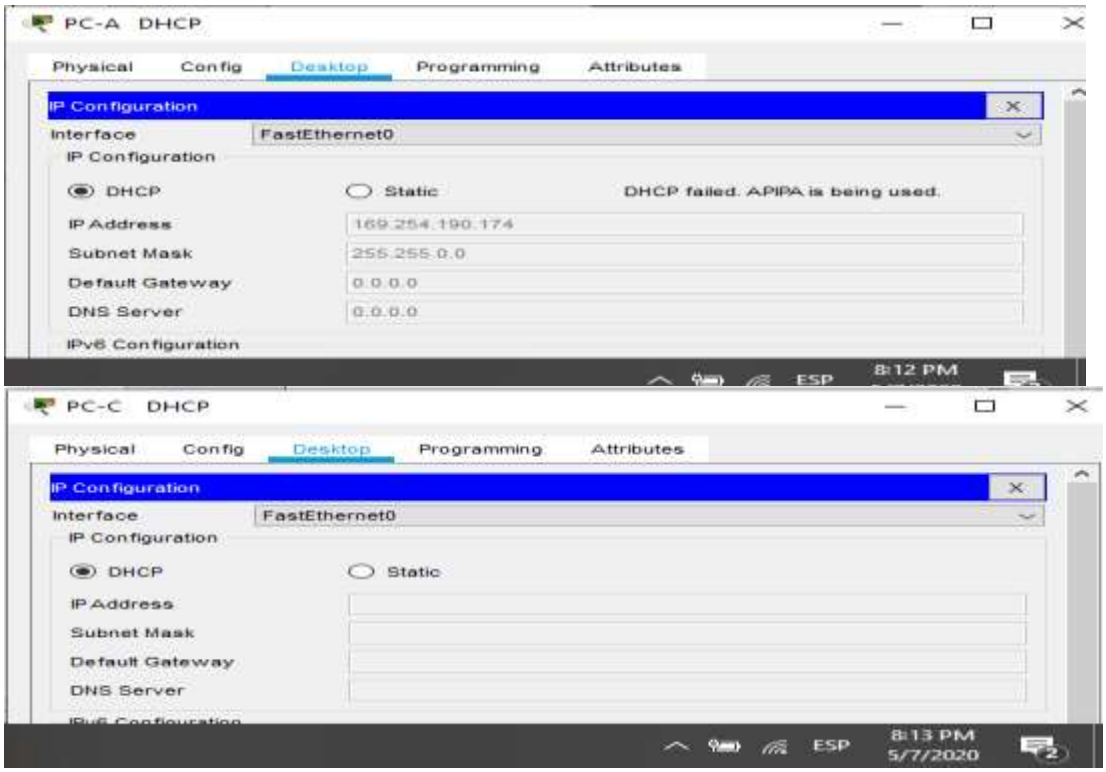

Figura 20.Configuracion PCA-PC_C en DHCP

Figura 21.Accede al sitio web desde el servidor internet

Parte 6: Configurar NTP

Tabla 19.Configuracion NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	**#ntp update-calendar**
Verifique la configuración de NTP en R1.	**#show ntp association #show ntp status**

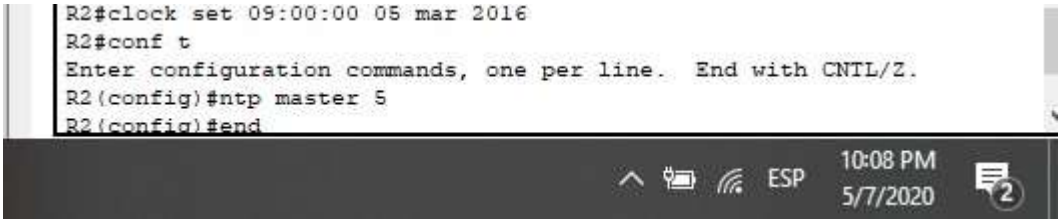

Figura 22.Configuracion NTP R1-R2, Fecha-Hora, Maestro.

Figura 23.Configuracion NTP R1- Actualizacion calendario

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

Paso 4: Restringir el acceso a las líneas VTY en el R2

Tabla 20.Acceso VTY en 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**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Comandos configuracion R2

R2#config t

R2(config)#ip access-list standard ADMIN-MGT

R2(config-std-nacl)#permit host 172.16.1.1

R2(config-std-nacl)#exit

R2(config)#line vty 0 4

R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#exit

R2(config)#

Paso 5: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 21.Verificacion -listas de acceso

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

show access-list

Figura 24.Verificacion – listas de acceso

#clear ip access-list counter

Figura 25.Verificacion – listas de acceso

#show run

Figura 26.Verificacion – listas de acceso

#show ip nat translation

Figura 27.Verificacion – listas de acceso

#clear ip nat translation

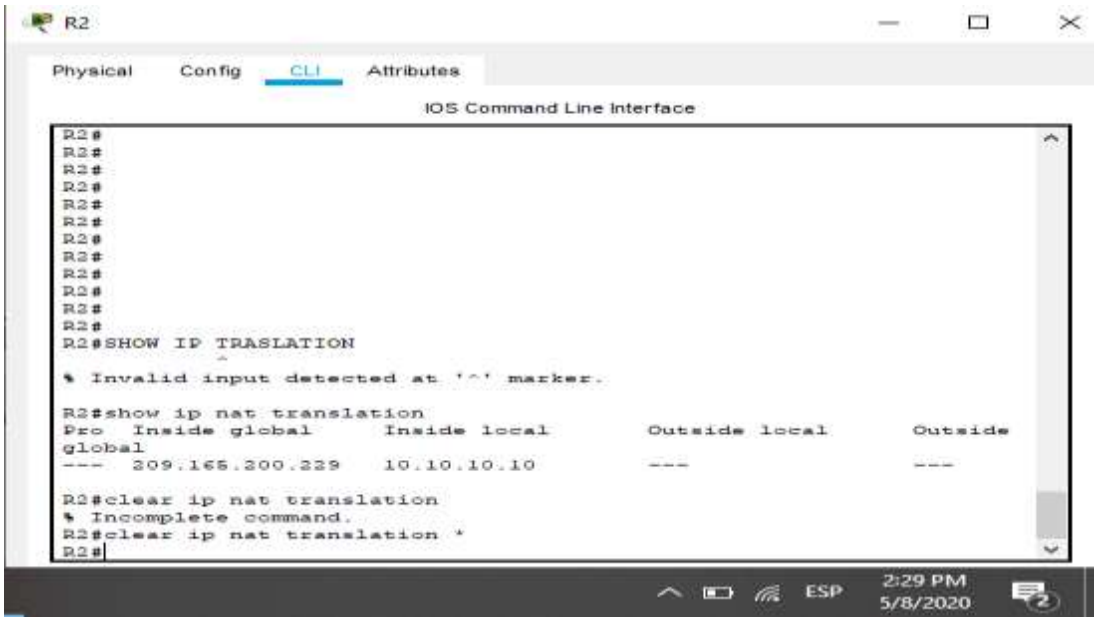

Figura 28.Verificacion – listas de acceso

4.2 ESCENARIO 2

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

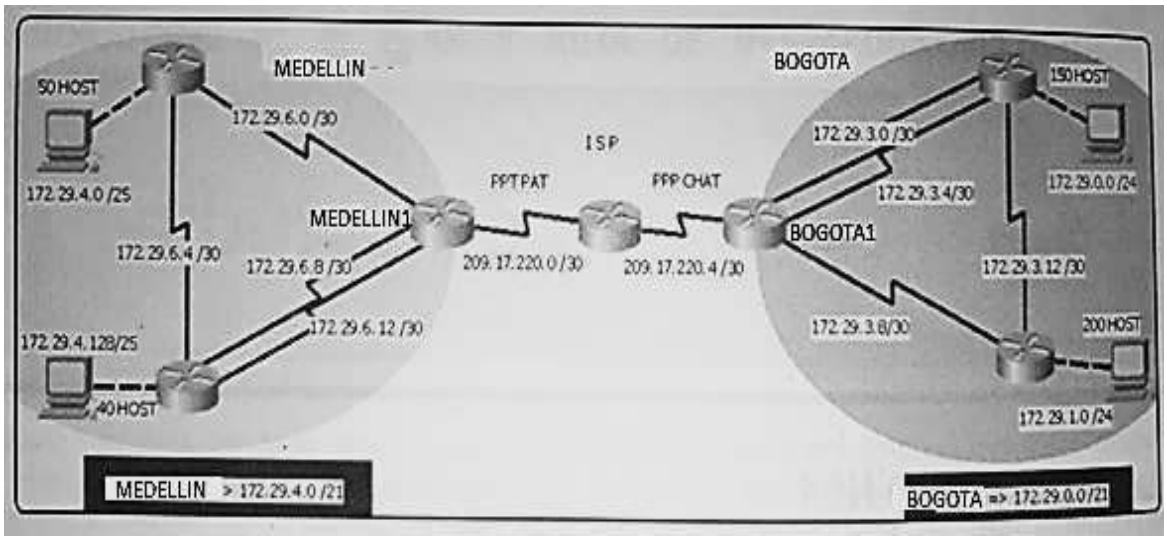

Figura 29.Topologia escenario 2

IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como ping, traceroute, show ip route, entre otros.

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.

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.

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.

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.

Parte 2: Tabla de Enrutamiento.

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

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.

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 22.Interfaces sin deshabilitacion OSPF

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

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 OSP 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.

Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Parte 6: Configuración de NAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

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.

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.

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

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

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

4.2.1 DESARROLLO DEL ESCENARIO 2

- 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

R// Desarrollo del diseño en Packet tracer con los equipos listos para su configuración, además se agregaron módulos con puerto serial adicional para realizar la configuración en ciertos router que exigen más de dos conexiones por cable serial.

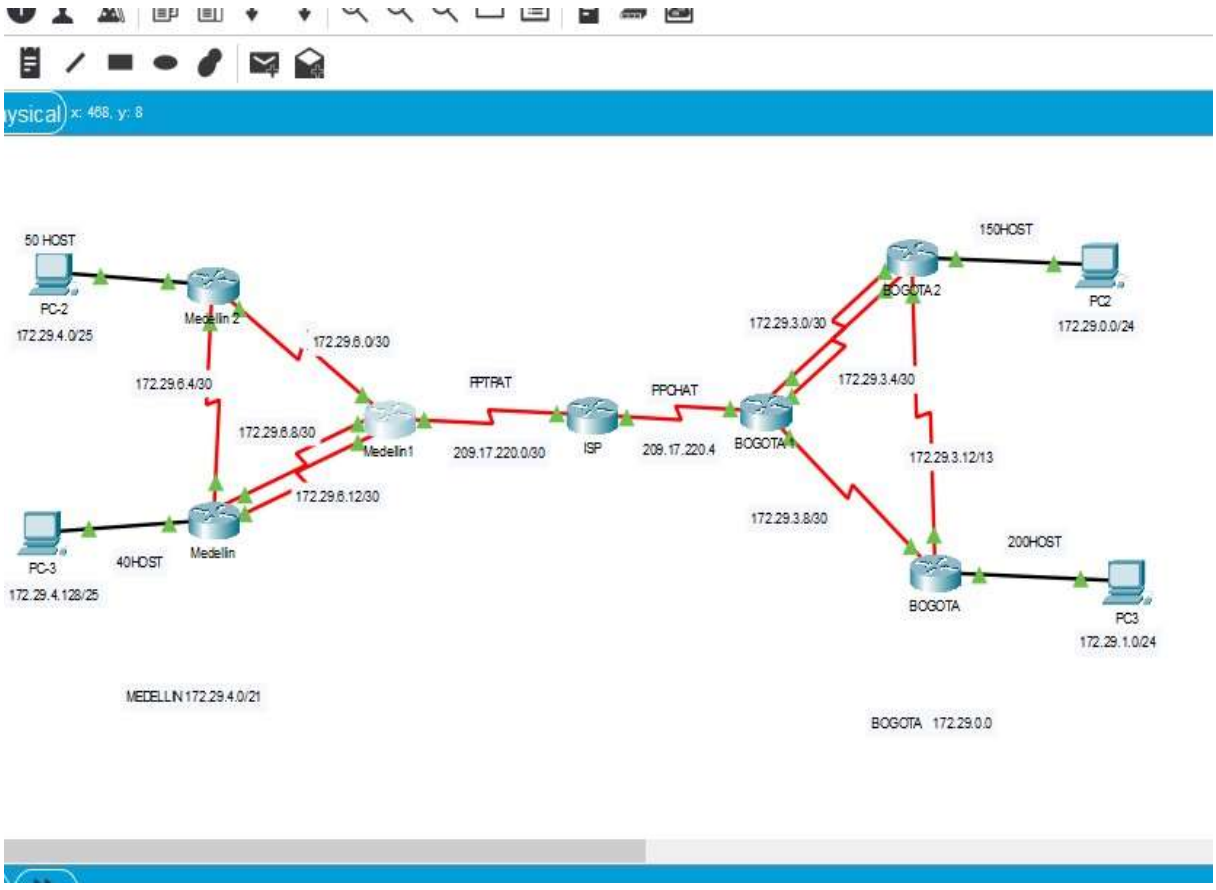

Figura 30.Topologia packet tracer escenario 2

Parte 1: Configuración del enrutamiento

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

R// Comenzamos con figurando las ip de todos los Router después aplicamos el protocolo RIP versión 2 y desactivamos la sumarización automática:

Comandos ejecutados en el Router ISP:

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname ISP
ISP(config)# interface serial 0/0/0
ISP(config-if)#description ISP-Medellin1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config)#interface serial 0/0/1
ISP(config-if)#description ISP-Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
This command applies only to DCE interfaces
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#router ospf 1
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
ISP(config-router)# network 209.17.220.4 0.0.0.3 area 0
ISP(config-router)#exit

Comandos ejecutados en el Router MEDELLIN1

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin1
Medellin1(config)#interface serial 0/0/0
Medellin1(config-if)#description Medellin1-ISP
Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/1
Medellin1(config-if)#description Medellin1-Medellin
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/0/1
Medellin1(config-if)#description Medellin-Medellin1
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#interface serial 0/1/0
Medellin1(config-if)#description Medellin1-Medellin2
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
Medellin1(config-if)#clock rate 128000
Medellin1(config-if)#no shutdown
Medellin1(config-if)#exit
Medellin1(config)#router ospf 1
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#passive-interface serial 0/0/0
Medellin1(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN2:

Router(config)#hostname Medellin2
Medellin2(config)#interface serial 0/0/1
Medellin2(config-if)#description Medellin2-Medellin1
Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config)#interface serial 0/0/0
Medellin2(config-if)#description Medellin2-Medellin
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(config-if)#exit
Medellin2(config)#interface g0/0
Medellin2(config-if)#description Medellin2-PC2
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shutdown
Medellin2(config)#exit
Medellin2(config)#router ospf 1
Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0
Medellin2(config-router)#passive-interface g0/0
Medellin2(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN:

Router>ENABLE
Router#conf t
Router(config)#hostname Medellin
Medellin(config)#interface serial 0/0/1
Medellin(config-if)#description Medellin-Medellin1
Medellin(config-if)#ip addres 172.29.6.14 255.255.255.252
Medellin(config-if)#clock rate 128000
Medellin(config-if)#no shutdown
Medellin(config)#interface serial 0/0/0
Medellin(config-if)#description Medellin1-Medellin
Medellin(config-if)#ip addres 172.29.6.10 255.255.255.252
Medellin(config-if)#clock rate 128000
Medellin(config-if)#no shutdown
Medellin(config-if)#exit
Medellin(config)#interface serial 0/1/0
Medellin(config-if)#description Medellin-Medellin2
Medellin(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin(config-if)#clock rate 128000
Medellin(config-if)#no shutdown
Medellin(config)#interface g0/0
Medellin(config-if)#description Medellin-PC3
Medellin(config-if)#ip address 172.29.4.2 255.255.255.128
Medellin(config-if)#no shutdown
Medellin(config)#router ospf 1
Medellin(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin(config-router)#network 172.29.6.4 0.0.0.3 area 0
Medellin(config-router)#network 172.29.4.128 0.0.0.127 area 0
Medellin(config-router)#passive-interface g0/0
Medellin(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA1:

Router>ENABLE
Router#config t
Router(config)#hostname Bogota1
Bogota1(config)#interface serial 0/0/0
Bogota1(config-if)#description Bogota1-ISP
Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/0/1
Bogota1(config-if)#description Bogota1-Bogota2
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/1/0
Bogota1(config-if)#description Bogota2-Bogota1
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#interface serial 0/1/1
Bogota1(config-if)#description Bogota1-Bogota
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
Bogota1(config-if)#exit
Bogota1(config)#router ospf 1
Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota1(config-router)#passive-interface serial 0/0/0
Bogota1(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA2:

Router>enable
Router#conf t
Router(config)#hostname Bogota2
Bogota2(config)#interface serial 0/0/0
Bogota2(config-if)#description Bogota2-Bogota1
Bogota2(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config)#interface serial 0/0/1
Bogota2(config-if)#description Bogota1-Bogota2
Bogota2(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config)#exit
Bogota2(config)#interface serial 0/1/0
Bogota2(config-if)#description Bogota2-Bogota
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota2(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
Bogota2(config-if)#exit
Bogota2(config)#interface g0/0
Bogota2(config-if)#description Bogota2-PC0
Bogota2(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota2(config-if)#no shutdown
Bogota2(config)#router ospf 1
Bogota2(config-router)#network 172.29.3.0 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.3.4 0.0.0.3 area 0
Bogota2(config-router)#network 172.29.0.0 0.0.0.255 area 0
Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota2(config-router)#passive-interface g0/0
Bogota2(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA:

Router>ENABLE
Router#confi t
Router(config)#hostname Bogota
Bogota(config)#interface serial 0/0/1
Bogota(config-if)#description Bogota-Bogota1
Bogota(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota(config-if)#clock rate 128000
Bogota(config-if)#no shutdown
Bogota(config)#interface serial 0/0/0
Bogota(config-if)#description Bogota-Bogota2
Bogota(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota(config-if)#clock rate 128000
This command applies only to DCE interfaces
Bogota(config-if)#no shutdown
Bogota(config-if)#exit
Bogota(config)#interface g0/0
Bogota(config-if)#description Bogota-PC1
Bogota(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota(config-if)#no shutdown
Bogota(config)#router ospf 1
Bogota(config-router)#network 172.29.3.12 0.0.0.3 area 0
Bogota(config-router)#network 172.29.1.0 0.0.0.255 area 0
Bogota(config-router)#network 172.29.3.8 0.0.0.3 area 0
Bogota(config-router)#passive-interface g0/0
Bogota(config-router)# exit

d. 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.

R// **Comandos usados para la ruta estática en ISP:**

ISP(config)#ip route 172.29.0.0 255.255.255.252 serial 0/0/1
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 serial 0/0/1
ISP(config)#ip route 172.29.4.128 255.255.255.128 serial 0/0/0

Comandos usados para la ruta estática predeterminada hace la red de MEDELLIN:

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#exit

Comandos usados para la ruta estática predeterminada hace la red de BOGOTA:

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#exit

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 verifican en los dos routes principales de cada ciudad con el comando **show ip route.**

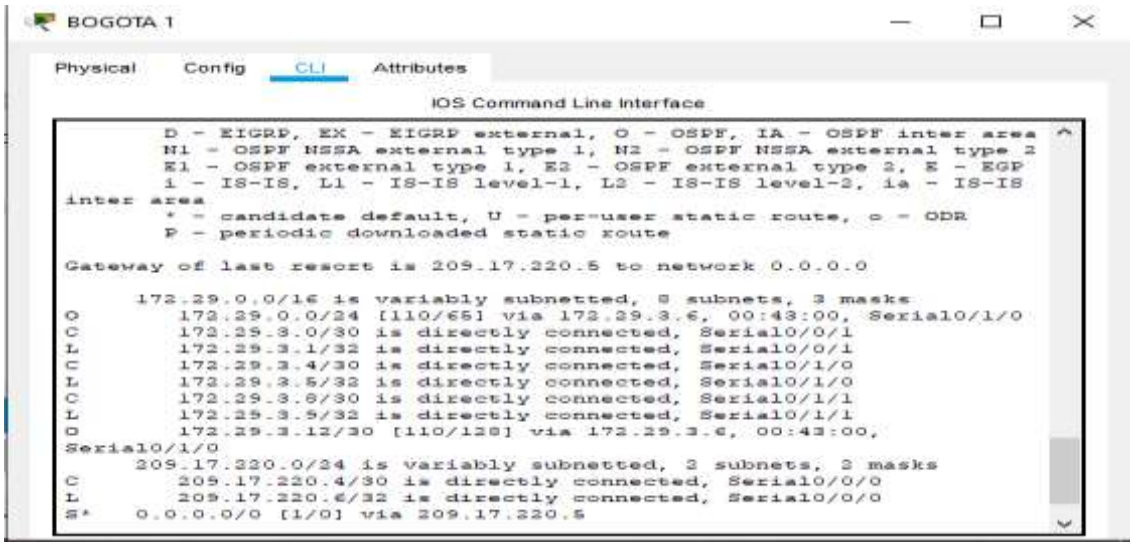

Figura 31.enrutamiendo Bogota 1

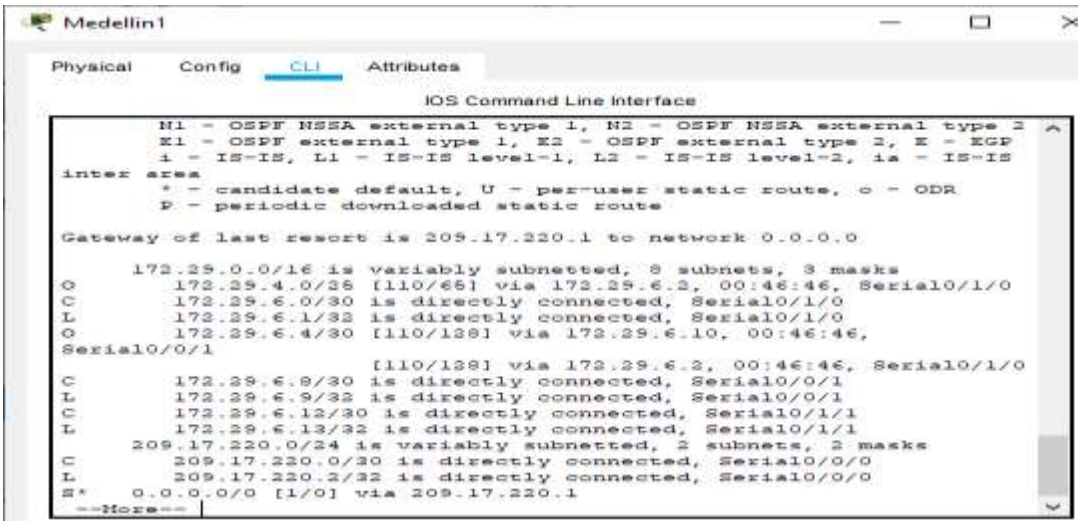

Figura 32.enrutamiento Medellin 1

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.

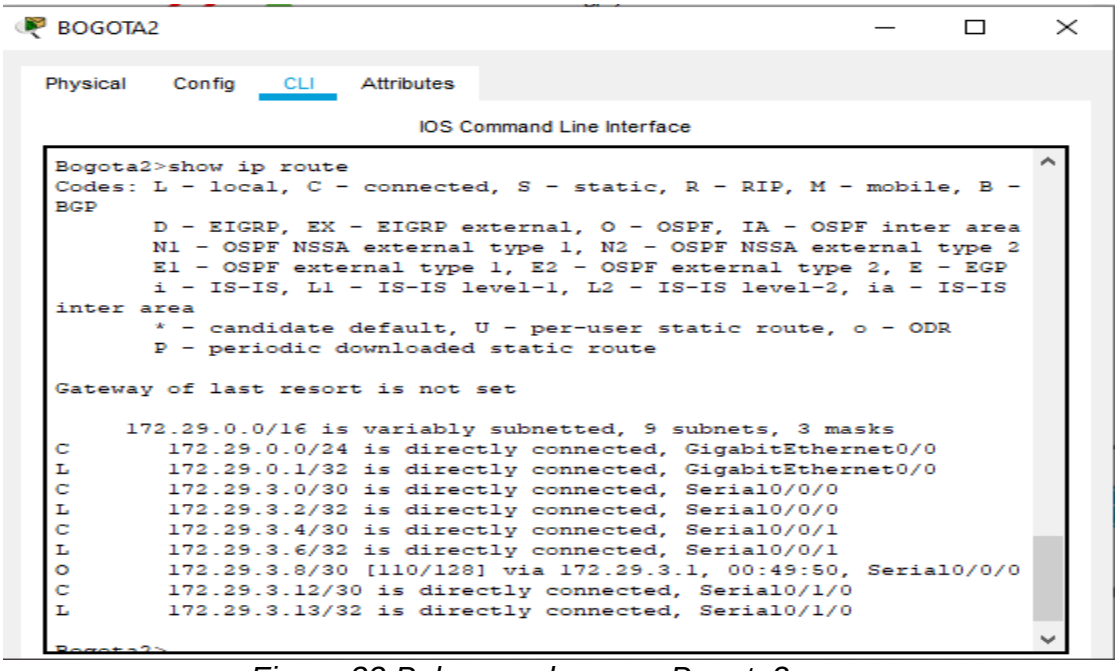

Figura 33.Balanceo de carga Bogota2

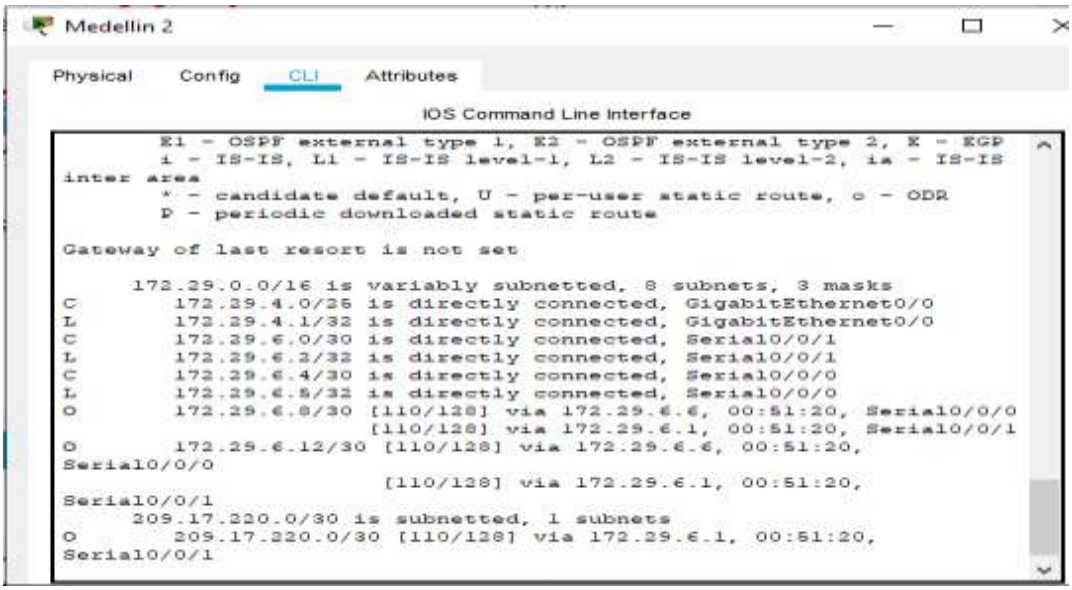

Figura 34.Balanceo de carga Medellin 2

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.

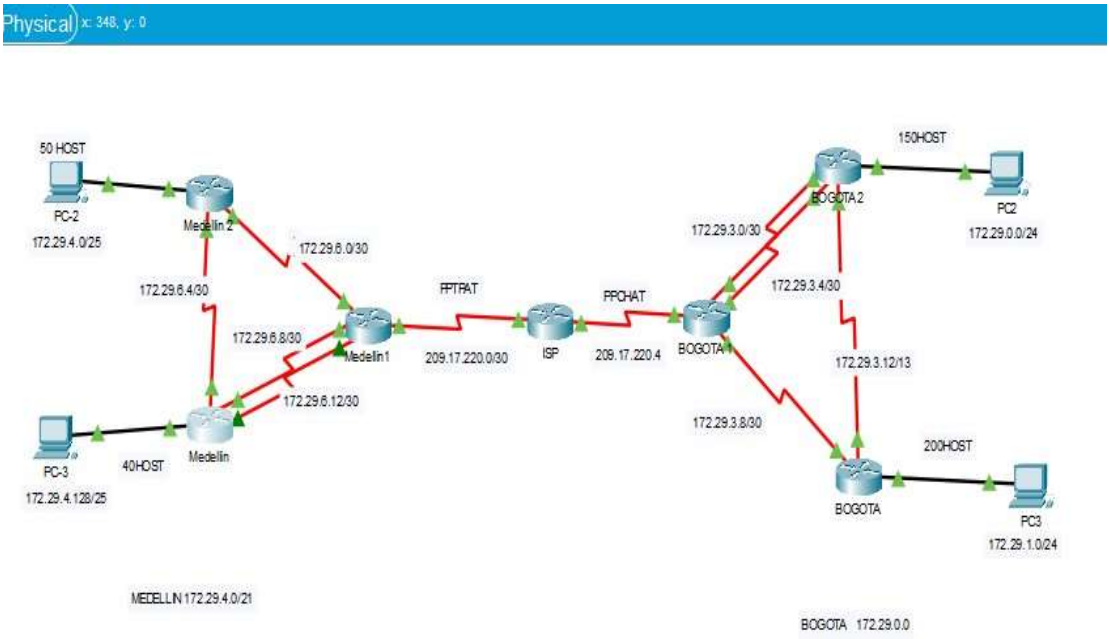

Figura 35.Similitud bogota1- medellin 1

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

R// en el paso anterior del item b se verifican con el comando show ip route

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

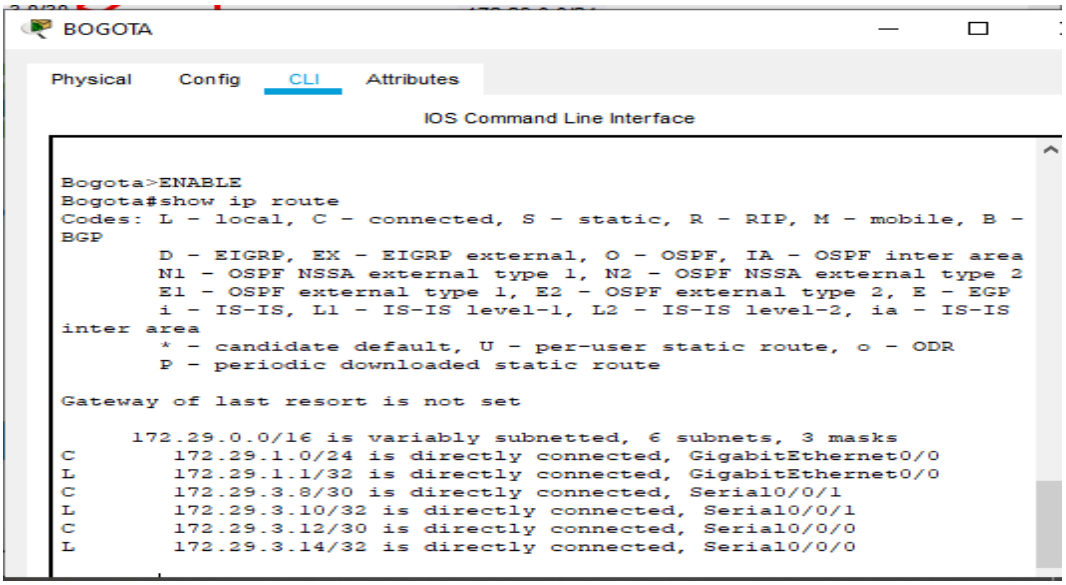

Figura 36.Rutas Redundantes bogota

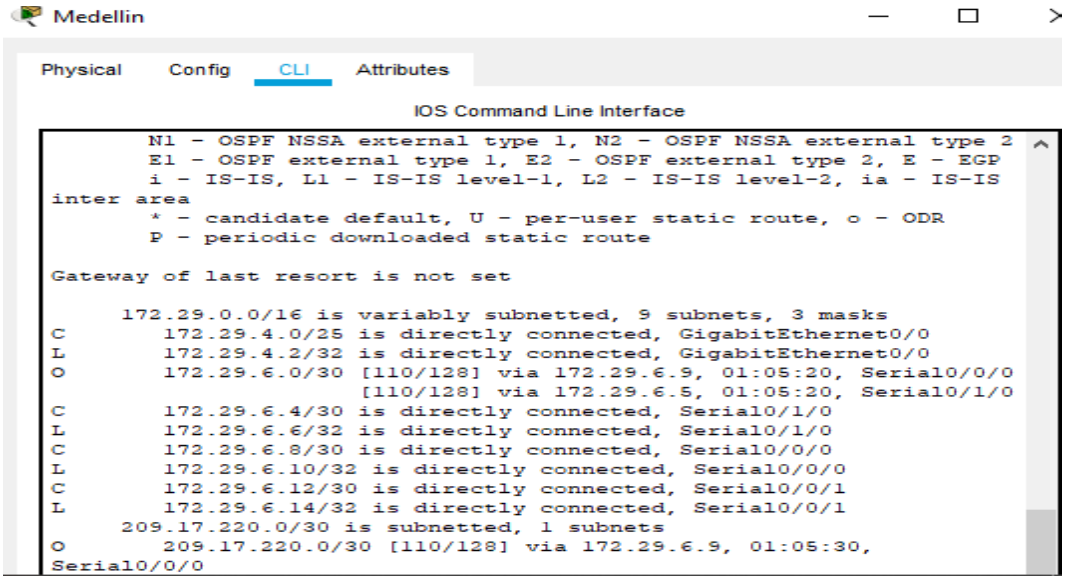

Figura 37.Rutas dedundantes Medellin

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

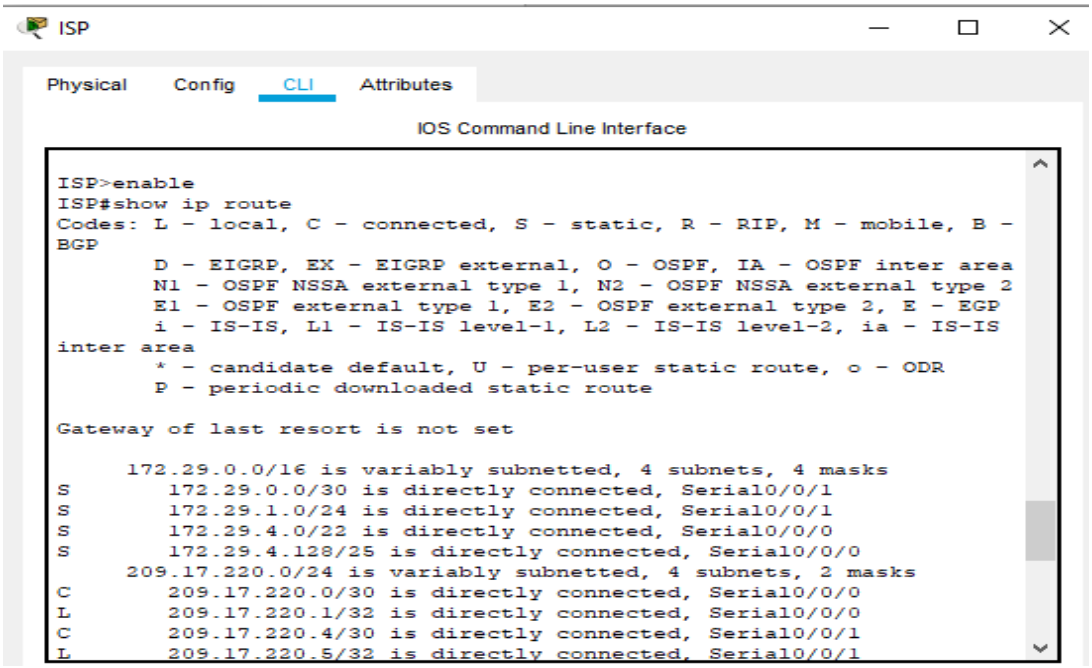

Figura 38.ISP rutas estaticas

Parte 3: Deshabilitar la propagacion 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.

R// Fueron tenidas en cuenta en la configuración del protocolo RIP 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.

Parte 4: Verificación del protocolo RIP.

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 RIP y las interfaces que participan de la publicación entre otros datos.
b. Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

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

Parte 5: Configurar encapsulamiento y autenticación PPP.

c. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAP.

.

Se ejecuta los siguientes comandos ISP:

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
ISP(config-if)#exit

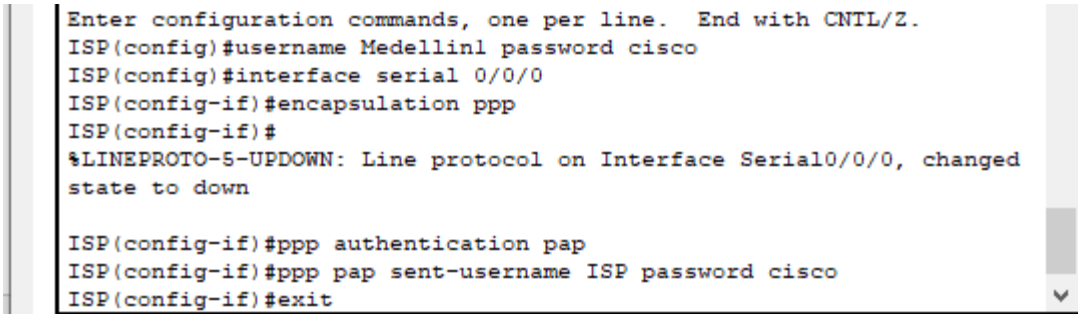

Figura 39.ISP Encapsulamiento y autenticacion ppp

Se ejecuta los siguientes comandos Medellin1

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)# ppp pap sent-username Medellin1 password cisco

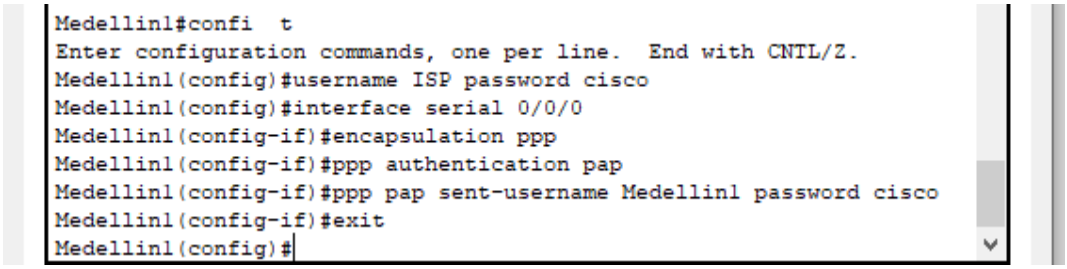

Figura 40.medellin1 Encapsulamiento y autenticacion ppp

D. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP

Se ejecuta los siguientes comandos ISP

ISP(config)#username Bogota1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap

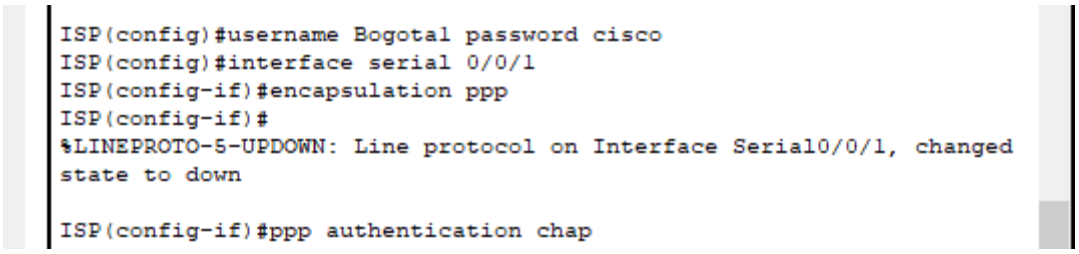

Figura 41.. ISP autenticacion CHAP

Se ejecuta los siguientes comandos Bogota1

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap

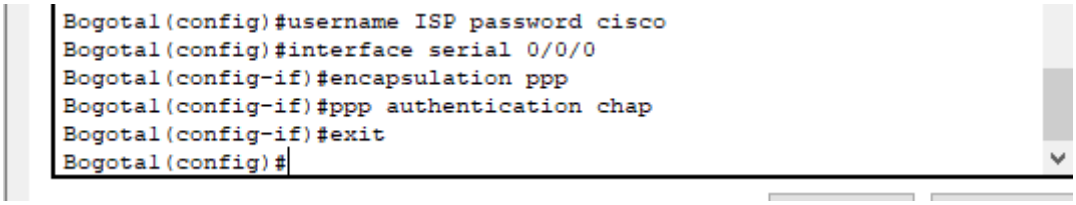

Figura 42.Bogota 1 autenticacion CHAP

Parte 6: Configuración de NAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

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 ladirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

R// Iniciamos con la configuración NAT en MEDELLIN1:

```
MEDELLIN1>en
MEDELLIN1#conf t
```

“Con este comando definidos la red de los PC’s que se desean que sean empleadas en el PAT”

```
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit
```

“Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP”

```
MEDELLIN1(config)#Ip nat inside source list HOST interface s0/0/0
overload
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat translation
```

Iniciamos con la configuración NAT en BOGOTA1:

```
BOGOTA1>en
BOGOTA1#conf t
```

“Con este comando definidos la red de los PC’s que se desean que sean empleadas en el PAT”

```
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
```

“Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP”

```
BOGOTA1(config)#Ip nat inside source list HOST interface s0/0/0 overload
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
```

```
BOGOTA1(config-if)#exit
BOGOTA1|(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1//0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#exit
BOGOTA1#show ip nat translation
```

Verificamos ping entre MEDELLIN2 y MEDELLIN1

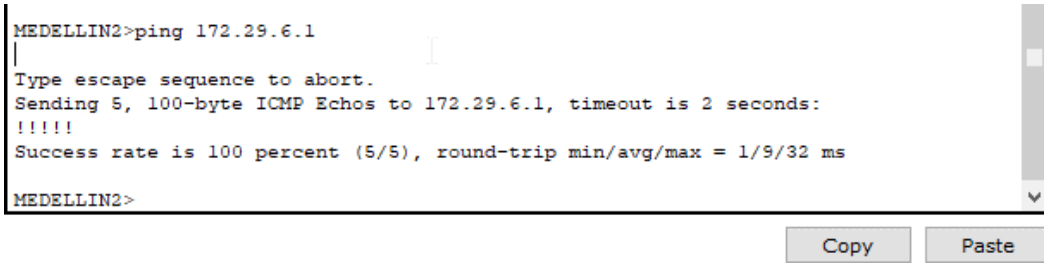

Figura 43.ping medellin2- medellin 1

Parte 7: Configuración del servicio DHCP.

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

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

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

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

R// Iniciamos configurando en DHCP en el Router MEDELLIN2

MEDELLIN2>en
MEDELLIN2#conf t
-Se definen que direcciones IP no deben ser entregadas por el DHCP debido a que estas ya están siendo utilizadas.
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(dhcp-config)#ip dhcp pool MEDELLIN2
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 8.8.4.4 MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN
-Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
-Definimos la dirección del Gateway para los Host.
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN2(dhcp-config)#exit

Continuamos configurando el DHCP, como el router MEDELLIN tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de MEDELLIN2:

MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#Int g0/0
MEDELLIN(config-if)#ip helper-addres
172.29.6.5 MEDELLIN(config-if)#exit

Iniciamos configurando en DHCP en el Router BOGOTA2

BOGOTA2>en
BOGOTA2#conf t
-Se definen que direcciones IP no deben ser entregadas por el DHCP debido a que estas ya están siendo utilizadas.

BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4
BOGOTA2(dhcp-config)#ip dhcp pool
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 8.8.4.4
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp pool BOGOTA
-Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
-Definimos la dirección del Gateway para los Host.
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
BOGOTA2(dhcp-config)#exit

Continuamos configurando el DHCP, como el router BOGOTA tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de BOGOTA2:

BOGOTA>en
BOGOTA#conf t
BOGOTA(config)#Int g0/0
BOGOTA(config-if)#ip helper-addres 172.29.3.13
BOGOTA(config-if)#exit

Verificamos que en el modo grafico del PC2 en la red de MEDELLIN, cuando le asignamos la configuración de ip por DHCP automáticamente le asigna una ip dentro del rango configurado anteriormente.

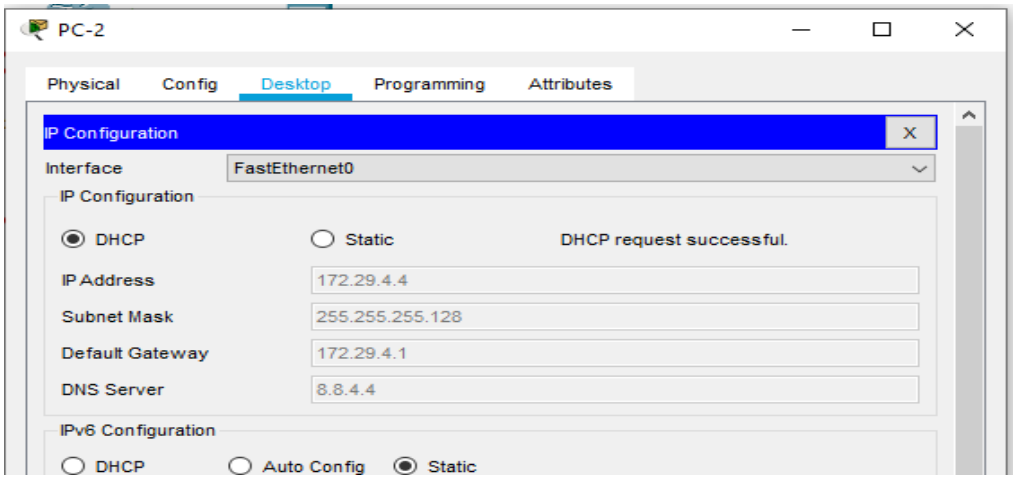

Figura 44.Configuracion de ip por DHCP- PC-2

Al estar el router en modo dhcp el router MEDELLIN2, le asigna aleatoriamente una ip al PC2, y podemos confirmar por un ping hacia el PC3 que la asignación es la correcta por que hay conectividad en la red, lo mismo sucede en la red de Bogota con el PC0 y el Router BOGOTA2

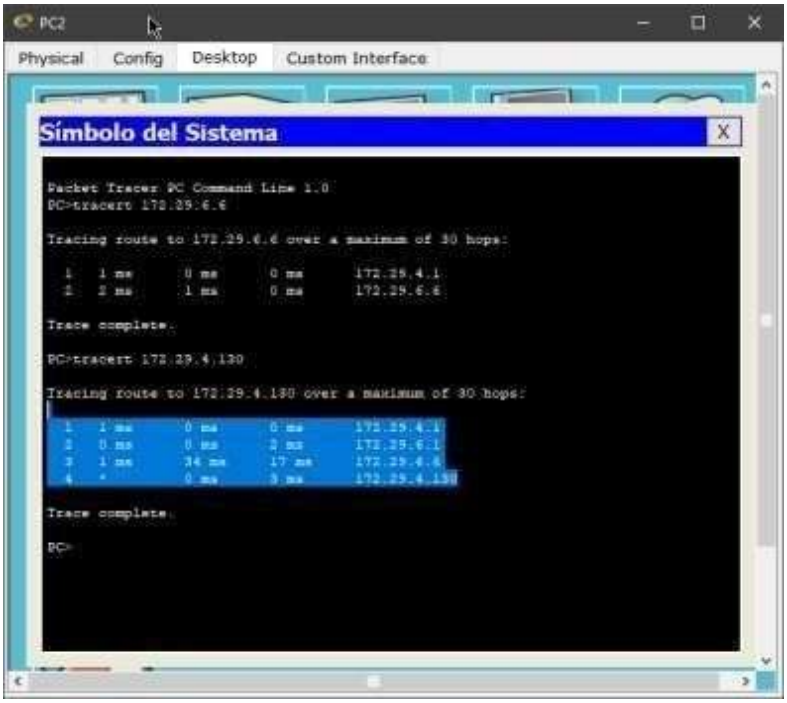

Figura 45.Tracert – ping de PC2 -PC3

- Por ultimo se asignan claves de seguridad a cada router, este paso se realiza de ultimo para agilizar el acceso a los router mientras se hacían los demás puntos.

R// Configuracion en Router ISP:

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

Configuracion en Router MEDELLIN1:

```
MEDELLIN1>en
MEDELLIN1#consf t
MEDELLIN1(config)#enable secret MEDELLIN1
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN1(config)#exit
```

Configuracion en Router MEDELLIN2:

```
MEDELLIN2>en
MEDELLIN2#conf t
MEDELLIN2(config)#enable secret MEDELLIN2
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
```

MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN2(config)#exit

Configuracion en Router MEDELLIN:

MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#enable secret MEDELLIN
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN(config)#exit

Configuracipon en Router BOGOTA1:

BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#enable secret BOGOTA1
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#line vty 0 4
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA1(config)#exit

Configuracipon en Router BOGOTA2:

```
BOGOTA2>en
BOGOTA2#conf t
BOGOTA2(config)#enable secret BOGOTA2
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA2(config)#exit
```

Configuracipon en Router BOGOTA:

```
BOGOTA>en
BOGOTA#conf  t
BOGOTA(config)#enable secret BOGOTA
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA(config)#exit
```

Ejemplo de la seguridad implementada en los router, aleatoriamente se selecciono Medellin1:

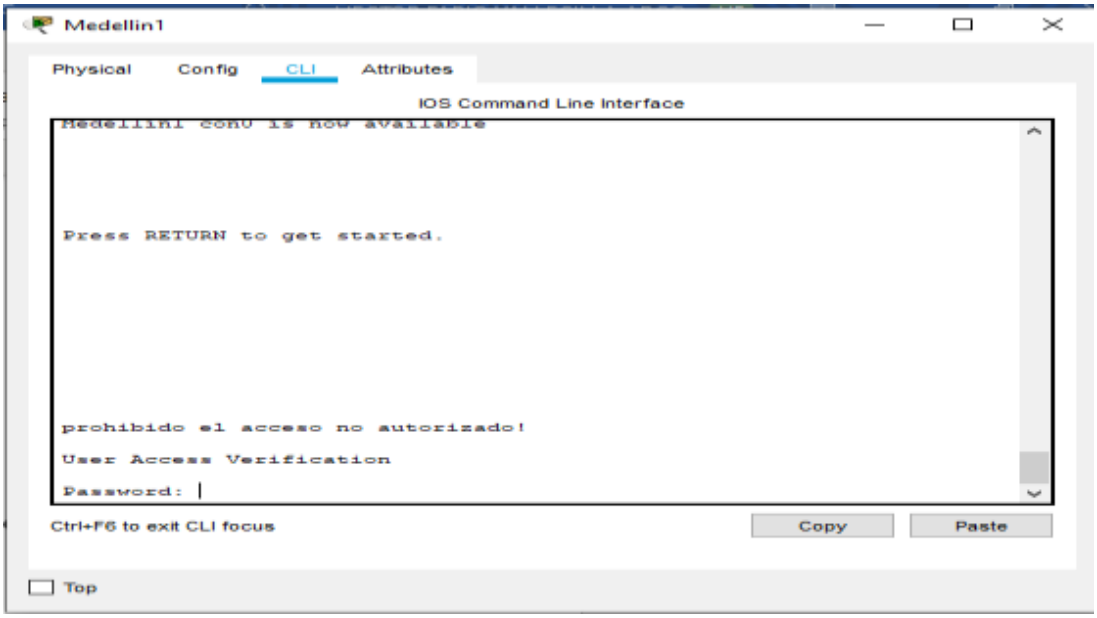

Figura 46.verificacion seguridad medellin1

5. CONCLUSIONES

Con el desarrollo del presente trabajo se adquiere conocimientos habilidades.Utilizando la herramienta de simulacion packet tracer el cual es muy practica, de facil comprension para la creacion de topologias de red y dar solucion a los escenarios propuestos. Durante la solucion de los ejercicios se logró realizar de manera gradual los procedimientos básicos para configuración de una red básica como compleja, donde se logra identificar, analizar y configurar dispositivos de red según las necesidades requeridas, durante toda la ejecucion de la asignatura. se debió tener presentes los elementos idóneos para la representación de la misma así como el especial cuidado en las asignaciones de las IP´s puesto que de allí deriva el éxito o el error al momento de realizar las respectivas pruebas.

Se consiguió llevar a cabo de manera exitosa protocolos de enrutamiento dinámico como OSPF y otros servicios como DHCP, listas de acceso, Nat y aseguramiento de dispositivos Cisco.

Se realizaron las debidas verificaciones de las configuraciones y conexiones con comandos ping, show ip route entre otros donde garantiza en funcionamiento de la red.

Finalmente el aprendizaje, destrezas y solucion de problemas adquiridas durante el DIPLOMADO CISCO llena de gran sastifacion ya que los procesos son muy similares a los que vemos en la vida laboral y hogares.

6. BIBLIOGRAFÍA

BARBOSA, Rodrigo. IP Helper y Relay Agent – Manteniendo un servidor DHCP en otra red.(en linea). (15 marzo de 2016). disponible en: https://www.seaccna.com/ip-helper-relay-agent/

Byspel. Configurar servidor DHCP en Packet Tracer.(en linea). (13 junio de 2017). Disponible en:https://byspel.com/configurar-servidor-dhcp-en-cisco-packet-tracer/

CALVO, Angel. RIP Cisco, aprende a configurar este protocolo facilmente. (en linea). (11 mayo de 2015). disponible en :https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-y- sencilla/

Colaboradores de Wikipedia. Máscara de red - Wikipedia, la enciclopedia libre. (en linea). (29 octubre 2014). Disponible en: https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

JUANSA, J. Solucionando errores TCP/IP. 4 – Uno de los blogs de Juansa. (en linea). (5 octubre de 2018). Disponible en :https://geeks.ms/juansa/2008/10/05/solucionando-errores-tcpip-4/

MARTINEZ, Victor. Configuración de RIPv2 (protocolo dinámico). (en linea). (25 febrero de 2013). Disponible en:http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/

MARTINEZ, Victor. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. (en linea). (16 agosto de 2016). disponible en:http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route- router-cisco/