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

JUAN PABLO HERNANDEZ HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. CEAD IBAGUÉ
2020

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

JUAN PABLO HERNANDEZ HERNANDEZ

INFORME FINAL PARA OPTAR POR EL TÍTULO DE INGENIERO ELECTRÓNICO

DOCENTE
HÉCTOR JULIÁN PARRA MOGOLLÓN
DIPLOMADO DE PROFUNDIZACIÓN CISCO

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA . CEAD IBAGUÉ
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Ibagué 15 de mayo de 2020

Dedico el presente trabajo a la escuela de ciencias básicas de tecnología e ingeniería, por el aprendizaje obtenido, a través de las temáticas, en las unidades del curso y de los elementos de interacción multimedia, que me permiten obtener dicho conocimiento en el campo de la conexión y gestión de redes, empleando el uso de la plataforma netacad cisco, para la obtención del previo conocimiento.

AGRADECIMIENTOS

Para el desarrollo de la presente actividad, brindo especial agradecimiento al grupo de trabajo que conforma la escuela de ciencias básicas, tecnología e ingeniería, por la orientación brindada, para llevar acabo, el desarrollo del curso de diplomado de profundización cisco, e integrantes que conforman el programa de ingeniería electrónica.

Como otro proceso importante de mi formación, brindo agradecimientos, al grupo de estudiantes que participaron, llevando a cabo la actividad de aprendizaje, que, mediante el acompañamiento con cada uno de ellos, logre obtener los previos conocimientos desarrollados en la plataforma, evidenciando mis resultados, en el presente trabajo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

comandos: es una orden o instrucción, que dicha persona o usuario entrega a dicho sistema informático, a través de línea de ordenes o llamada.

c*onectividad*: es la capacidad de crear un vínculo, es la capacidad de conectarse a una red de internet y otros equipos.

Enrutamiento: es el proceso que permite que los paquetes ip que son enviados por el host origen puedan llegar al host destino.

Gateway: es un dispositivo que actúa como interfaz de conexión entre aparatos, dispositivos, que hace posible compartir recursos a partir de dos o más equipos u ordenadores.

Protocolo: definido como un conjunto de normas y pautas para guiar una conducta o una acción, standard que especifican el método de enviar y recibir datos e información entre varios ordenadores.

Red: característica organizada en ciertos patrones que comparten información, documentos, donde esta misma puede ser dividida, dado su alcance y el método de conexión.

Router: elementos empleados para realizar la respectiva conexión entre computadoras u ordenadores, a través de una red, buscando establecer la ruta para determinados paquetes de datos.

Subred: es un modo de ampliar el espacio para direcciones y reducir las tablas de enrutamiento, haciéndose más manejable administrativamente.

Topología: es el mapa físico de una red que se expresa para intercambiar datos información, diseñada desde el punto de vista físico y lógico.

RESUMEN

La actividad a desarrollar, presenta dos escenarios para establecer una previa conexión con cada uno de los elementos o sedes que estos solicitan, empleando los componentes de red, hasta los equipos de cómputo para el usuario final. Con ello, estableceremos las previas rutas mediante el uso de los comandos empleados para llevar a cabo dicha conexión. Cabe mencionarse que en este mismo se realizara la topología, para proyectar el diagrama de los routers, cableados o conexiones de puertos, hasta los elementos finales que son los equipos o pc ,creando conectividad de redes de empresas, por diferentes departamentos.

Con ello, se consolidará la obtención de los códigos que permiten realizar distintas funciones, al ejecutar y terminar procesos para que la conexión de dispositivos se lleve a cabo, hasta lograr la obtención de red en oficinas, equipos, grupos, empresas, entre otros, facilitando la conectividad, e interacción multimedia entre ellos.

En base de lo anterior, se evidenciara el aprendizaje logrado, al desarrollar cada uno de los ítems solicitados en la actividad, mostrando la solución de los dos escenarios y diagramas, empleado la utilización del simulador de redes packet tracer, contando con el paso a paso de la presente actividad para ejecutar dichos códigos con su respectiva función, anexando también, una serie de tablas que nos permitirá consolidar, dichos comandos, para generar conectividad de equipos según sea requerido por la empresa o la topología de los dos escenarios que deben proyectar su objetivo y propósito de trabajo sea, este entre sedes hasta capitales de una misma empresa.

PALABRAS CLAVE:

Enrutamiento, topologías de red, comandos.

1. INTRODUCCIÓN

Para el desarrollo de esta fase de trabajo, se realiza los procesos de enrutamiento, dirección y conexión de dispositivos de red, que permiten proyectar la topología de dos escenarios propuestos y por los cuales se establecerán las previas direcciones a través de comandos obtenidos para conectar en una sola red los dispositivos en diferentes oficinas o distancia de esta misma. Cabe mencionarse que se trabajaran en el primer escenario de tres dependencias que son contabilidad, ingeniería y administración, seguido por el escenario donde se unirán sectores de la empresa en Medellín y Bogotá como una sola dependencia.

Esto se demostrará a través de los códigos y enrutamiento en el simulador de cisco packet tracer, proyectando la previa solución de estos dos escenarios y evidenciando de los conocimientos obtenidos en la temática de diplomado de profundización cisco.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Mediante la actividad propuesta se proyectará en demostrar de los conocimientos obtenidos, en cisco packet tracer, a fin de generar solución, de dos escenarios que necesitan realizar una conexión de red en sus diferentes dependencias teniendo en cuenta sus especificaciones, para su modo de trabajo en una sola unidad.

2.2 OBJETIVOS ESPECÍFICOS

Determinar los elementos o dispositivos que serán empleados para realizar la conexión solicitada en los dos escenarios.

Generar los códigos de seguridad, de conexión y enrutamiento entre otros, a fin de que estos funcionen como una sola unidad.

Realizar la previa configuración de protocolos, vlan, direcciones, para la integración de red de los equipos.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Se encuentran dos escenarios por los cuales el primero consta de generar conectividad ipv4 y ipv6, teniendo en cuenta la seguridad y enrutamiento en las distintas áreas de trabajo, que son administración, ingeniería y contabilidad, configurando dichas redes por vlan, Nat, detallando cada área de trabajo a través de la topología de red.

El segundo escenario, se proyecta en conectar distintas sedes de la empresa, a través de las dos ciudades, como una sola unidad de trabajo de modo que todos los equipos trabajen a través de una sola red, para que la empresa se unifique a través de la red, cumpliendo igualmente con los protocolos de enrutamiento y topología.

3.2 JUSTIFICACIÓN

La problemática anteriormente planteada, se solucionará debido a que es un entorno donde se evidenciaran de los conocimientos obtenidos a través del programa de diplomado de profundización cisco, plasmando mediante códigos y rutas para lograr establecer conexiones de red, entre equipos sean de diferentes dependencias, para crear un campo laboral de conexión multimedia más productivo.

Este proyecto se lleva a cabo mediante la construcción topológica de los dos escenarios, que permiten ver e identificar los elementos necesarios para su funcionamiento y tipo de enrutamiento, para crear dicha comunicación de equipos. Con lo mencionado, empleamos el programa packet tracer, que permite evidenciar los códigos empleados y mapa de dichos entornos descritos en el proceso de trabajo.

4. MARCO TEÓRICO

En la actualidad, la gestión de redes cumple un papel fundamental en la vida cotidiana de cada persona, organización social entre otras, por las que se hace necesario la conectividad, para gestionar trabajos, funciones, labores entre otras, que requieran agilidad en la transmisión de la información de cualquier tipo de formato, por ejemplo: audios, documentos, videos, Imágenes y archivos, con su respectivo tipo de formato o extensión.

Cabe mencionar que estos mismos deben ser distribuidos, en las respectivas redes dirigidas por lo que se hace necesario el enrutamiento, cumpliendo la función de dirigir dichos elementos a los equipos de destino que el remitente solicito este mismo y viceversa, además de ser compartido con usuarios específicos.

Como otro proceso fundamental, es la protección de archivos y respectivas redes, para determinar el acceso a cierto personal autorizado, sean esta de tipo de redes corporativas, con determinada función. Por lo tanto, el proceso de gestión de redes cumple un proceso fundamental para la gestión multimedia de la sociedad.

Paul Mockapetris y Jon Postel (1983), crearon el sistema de nombres de dominio dns y las extensiones o las denominaciones .com, .org, y .gov, que son elementos principales y características de lo que hoy conocemos como Internet.

Tim Berners Lee (1990) que a principio de los ’90 inventó el sistema de links, resultando fundamental para el crecimiento de la conexión de redes.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Para llevar a cabo la creación de los diagramas de conexión, se emplea el software cisco packet tracer versión 7.1

5.2 METODOLOGÍA

Identificado el procedimiento a realizar para configurar la conexión, se hace necesario la obtención de comandos que permiten ejecutar acciones al realizar la topología de la red, con ello podremos dirigir el tipo de conexión destinada para cada equipo y que dominio se tiene dependiendo de la red asignada.

Se especifican algunos principios necesarios:

Software de aplicación: formado por programas que se comunican con usuarios de la red y estos permiten compartir información, como documentos, imágenes, videos, y además de recursos como impresoras, unidades de cd, tipo de software de aplicación que se nombra cliente-servidor.

Software de red: este se basa en programas informáticos que establecen protocolos o normas para que los ordenadores o los equipos se comuniquen entre ellos. Se aplican enviando y recibiendo grupos de datos formateados llamados paquetes.

Protocolos: es efectúan conexiones entre las aplicaciones de la red, dirige el movimiento de paquetes a través de red física y minimiza las probabilidades de un choque entre los paquetes enviados simultáneamente.

El hardware de red: formado por los componentes, materiales que unen a las computadoras, los componentes importantes son los medios de transmisión que transportan las señales de los ordenadores como cables o fibra óptica, y el adaptador de red, permitiendo acceder al medio que conecta a los computadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otros ordenadores.

6 DESARROLLO DEL PROYECTO

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

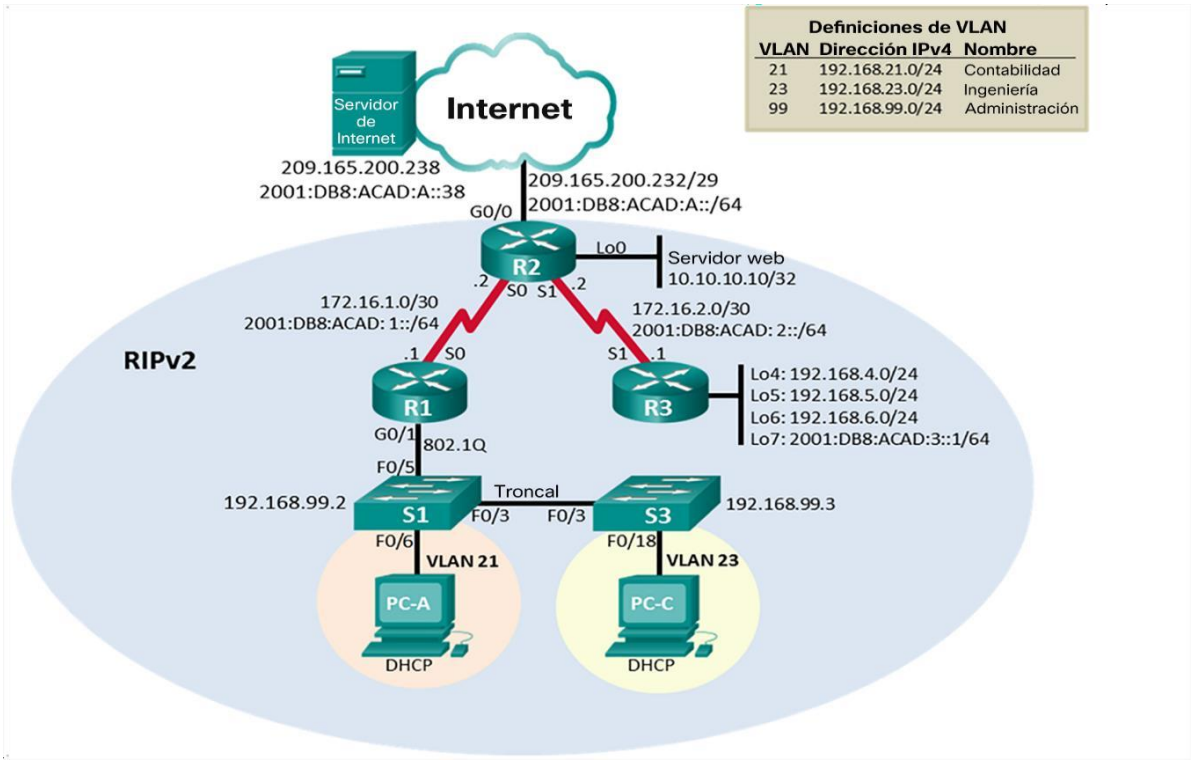

Figura 1. diagrama escenario 1

Parte 1: Inicializar dispositivos

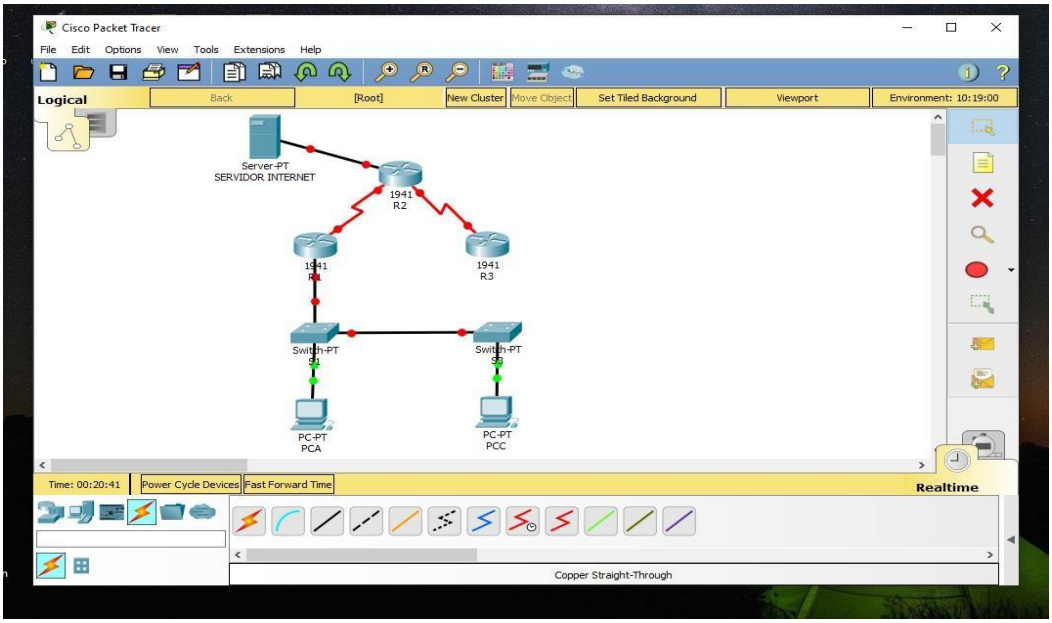

Figura 2. topología y conexión escenario 1

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.

Identificamos los principales comandos para poder llevar a cabo, el desarrollo del escenario 2 a través de la siguiente tabla:

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config enable
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	delete vlan.adt
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 show vlan brief dir flash:

Tabla 1.comandos principales

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):

Configuramos inicialmente, el servidor de internet donde las direcciones en (destock- ip configuration) se ingresaron como se diligencio en la tabla:

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	8.8.8.8
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2.Configuración servidor internet

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

Los comandos anexos en la tabla a ejecutar, nos servirán para crear las políticas de acceso, direccionamiento, y de seguridad, adjunto a la tabla agregamos la configuración para R1:

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Cisco Line con 0 Enable password cisco
Contraseña de acceso Telnet	Cisco Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. Banner motd % acceso no autorizado.%

Interfaz S0/0/0	Establezca la descripción Inteface s0/0/0 Description conexión a R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección Ipv6 Consultar el diagrama de topología para conocer la información de direcciones ip address 192.168.21.0 255.255.252.0 Establecer la frecuencia de reloj en 128000 Clock rate 128000 Activar la interfaz No shutdown
Rutas predeterminadas	Configurar una ruta Ipv4 predeterminada de S0/0/0 Configurar una ruta Ipv6 predeterminada de S0/0/0 Ip route 0.0.0.0 0.0.0.0 s0/0/0

*Tabla 3.*configuración R1

Comandos utilizados

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
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 %"acceso no permitido"%
```

R1(config)#int g0/0
R1(config-if)#description R1-R2
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

Los comandos anexos en la tabla a ejecutar, nos servirán para crear las políticas de acceso, direccionamiento, y de seguridad, adjunto a la tabla, agregamos la configuración para R2:

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	hostname R2
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Cisco Line con 0 Password cisco login
Contraseña de acceso Telnet	Cisco Line vty 0 4 Password cisco login
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. Banner motd % acceso no autorizado%

Interfaz S0/0/0	Establezca la descripción Interface s0/0/0 Description conexión a R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Ip address 192.168.21.0 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz No shutdown
Interfaz S0/0/1	Establecer la descripción Interface s0/0/1 Description conexión a R1 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Ip address 192.168.23.0 255.255.255.252 Establecer la frecuencia de reloj en 128000. Clock rate 128000 Activar la interfaz No shutdown

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Description conexión a servidor www Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Ip address 10.10.10.10 255.255.255.0 Activar la interfaz No shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Description conexión a servidor www Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. Ip route 0.0.0.0 0.0.0.0 g0/0

Tabla 4. Configuración R2

Comandos utilizados en la tabla

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 %" acceso no permitido"%
R2(config)#int g0/1
```

R2(config-if)#description R2-R1
R2(config-if)#ip address 172.16.2.0 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Paso 4: Configurar R3

Se configuro los comandos a ejecutar para generar política de acceso, direccionamiento en cada uno de los routers R1, R3, Pc Internet y Web Server, añadiendo seguridad, además de loopback 4,5,6 y 7.

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Cisco Line con 0 Password cisco login
Contraseña de acceso Telnet	Cisco Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Service password encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. Banner motd % acceso no autorizado%

Interfaz S0/0/1	Establecer la descripción Interface s0/0/1 Description conexión a R3 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Interface l04 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Ip address 192.168.99.0 255.255.255.0 Activar la interfaz No shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface l04 Ip address 192.168.21.0 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface l05 Ip address 192.168.23.0 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface l06 Ip address 192.168.99.0 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	Ip route 0.0.0.0 0.0.0.0 s0/0/1

Tabla 5. configuración R3

Comandos utilizados para R3

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-lookup
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 %"acceso no permitido"%
R3(config)#int s0/1
%Invalid interface type and number
R3(config)#int g0/1
R3(config-if)#description R3-R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
R3(config-if)#int lo4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config-if)#ip address 192.168.21.0 255.255.255.0
Bad mask /24 for address 192.168.21.0
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#int lo5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R3(config-if)#int lo6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#int lo7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
```

Paso 5: Configurar S1

Creamos la configuración inicial de seguridad, para los swich en los commandos adjuntos despues de la tabla, segun los datos que solicita para su acceso.

La configuración del S1 incluye las siguientes tareas:

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	Cisco Line con 0 Password cisco login
Contraseña de acceso Telnet	Cisco Line vty 0 4 Password login
Cifrar las contraseñas de texto no cifrado	Service password encryption
Mensaje MOTD	Banner motd % aceeso no autorizado%

Tabla 6. configuración del s1

Comando utilizado

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %"acceso no autorizado"%
S1(config)#exit
```

%SYS-5-CONFIG_I: Configured from console by console

Paso 6: Configurar el S3

Creamos la configuración inicial de seguridad, para los swich en los comandos adjuntos después de la tabla, según los datos que solicita para su acceso

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Cisco Line con 0 Password cisco login
Contraseña de acceso Telnet	Cisco Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Service password encryption
Mensaje MOTD	Banner motd % acceso no autorizado%

Tabla 7. configuración s3

Comando utilizado

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd %"acceso no autorizado"%
S3(config)#exit
```

%SYS-5-CONFIG_I: Configured from console by console

Paso 7: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.031.21.2	5/5
R2	R3, S0/0/1	172.16.23.2	5/5
PC de Internet	Gateway predeterminado	209.165.200.225	5/5

Tabla 8. prueba direcciones ip dependencias

Mediante el comando ping observamos la conexión de los distintos routers, con el objetivo de que las tres dependencias como contabilidad, ingeniería y administración se encuentren habilitadas, además de que se encuentran con su respectiva seguridad o clave de acceso.

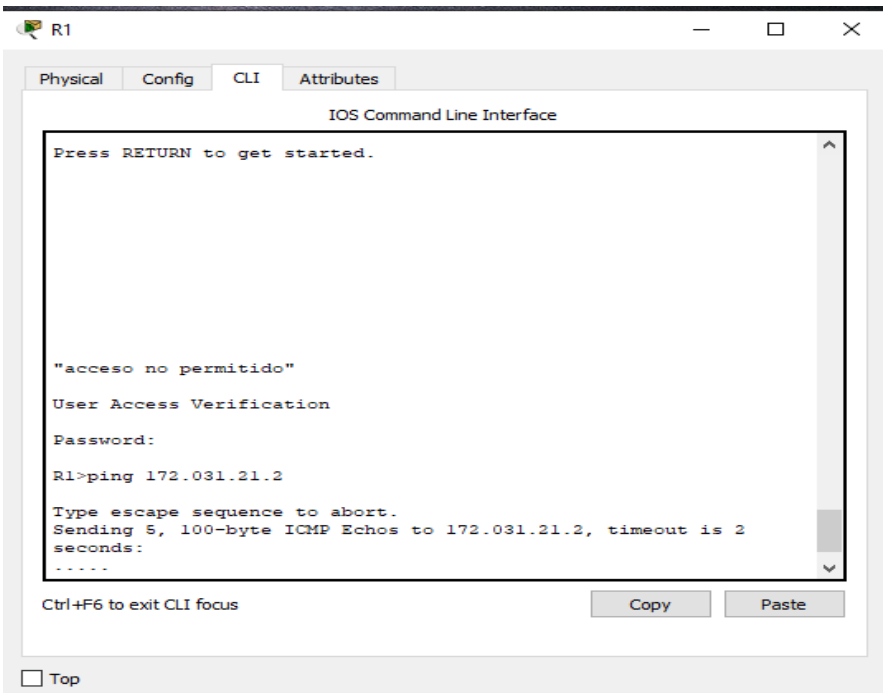

Figura 3. prueba conectividad R1

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

Paso 1 Configurar S1

Para esta configuración creamos las vlan o las redes solicitadas de las tres dependencias en un solo modulo a fin de que sea una misma red física, por lo que asignaremos los comandos para los switches s1 y s3 adjuntos en las tablas y códigos respectivos:

La configuración del S1 incluye las siguientes tareas:

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 Enable Configure terminal Vlan 21 Name contabilidad Vlan 23 Name ingeniería Vlan 99 Name administracion
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología Interface vlan 99 Ip address 192.168.99.0 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ip default-gateway 192.168.99.0
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Interface fa 0/3 Swichport mode trunk Swichport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa Interface fa0/5 Switchport mode trunk Switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Interface range fa0/1-2, fa0/4, fa0/6-24, g0/1-2 Switchport mode access
Asignar F0/6 a la VLAN 21	Interface fa0/6 Swichport mode Access Swichport access vlan 31
Apagar todos los puertos sin usar	Interface range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 shutdown

Tabla 9. configuración seguridad y routing de s1

Comandos de s1

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#vlan 30
S1(config-vlan)#exit
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name administracion
S1(config-vlan)#vlan 99
S1(config-vlan)#name LAN_S1_S3
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#
```

%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit

S1(config)#ip default-gateway 192.168.21.1

Configuración de los puertos troncales:

S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

Comandos para los puertos de acceso y de seguridad:

S1(config)#int range f0/1-2, f0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/2, f0/4-23, g0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit

Paso 2: Configurar el S3

Para esta configuración creamos las vlan o las redes solicitadas de las tres dependencias en un solo modulo a fin de que sea una misma red física, por lo que asignaremos los comandos para los switches s1 y s3 adjuntos en las tablas y códigos respectivos:

La configuración del S3 incluye las siguientes tareas:

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. Enable Configure terminal Vlan 21 Name contabilidad Vlan 23 Name ingeniería Vlan 99 Name administracion
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología Interface vlan 99 Ip address 192.168.99.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. ip default-gateway 192.168.99.0 255.255.255.0
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Interface fa0/3 Swichport mode trunk Switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Interface range fa0/1-2, fa0/4, fa0/6-24 Swichport mode access
Asignar F0/18 a la VLAN 21	Interface fa0/18 Swichport mode Access Swichport access vlan 33
Apagar todos los puertos sin usar	Interface range fa0/1-2, fa0/4-17, fa0/19- 24, g0/1-2 shutdown

Tabla 10. configuración vlan swich s3

Comandos para configurar s3

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
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)#name LAN_S1_S3
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.40.1
```

Ajustamos puertos troncales:

```
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
```

Ajustamos puertos de acceso y de seguridad:

```
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#shut
S3(config-if-range)#exit
S3(config)#int f0/1
S3(config-if)#no shut
S3(config-if)#switchport mode access
s3(config-if)#switchport access vlan 23
s3(config-if)#exit
```

Paso 3: Configurar R1

se procede en configurar su dirección ip , los datos respectivos a los vlan. Por lo que, de este modo, el router puede mantener separado, el tráfico de cada subinterfaz.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Interface g0/1.21 Encapsulation dotq1 21 Description LAN contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz Ip address 192.168.21.0 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Interface g0/1.23 Encapsulation dotq1 23 Description LAN ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz Ip address 192.168.23.0 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Interface g0/1.99 Encapsulation dotq1 99 Description LAN administracion Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz Ip address 192.168.99.0 255.255.255.0
Activar la interfaz G0/1	No shutdown

Tabla 11. Configuración y asignación vlan para R1

Comandos utilizados

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0.21
%Invalid interface type and number
R1(config)#int g0/0.21
R1(config-subif)#description contabilidad_LAN
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#
R1(config-subif)#ip add 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#in g0/0.23
R1(config-subif)#description ingenieria_LAN
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.
R1(config-subif)#int g0/0.99
R1(config-subif)#description administracion_RED
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.99
R1(config-subif)#description s1_s3_red
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0
R1(config-if)#no shut
```

Prueba configuración R1 comando no shut

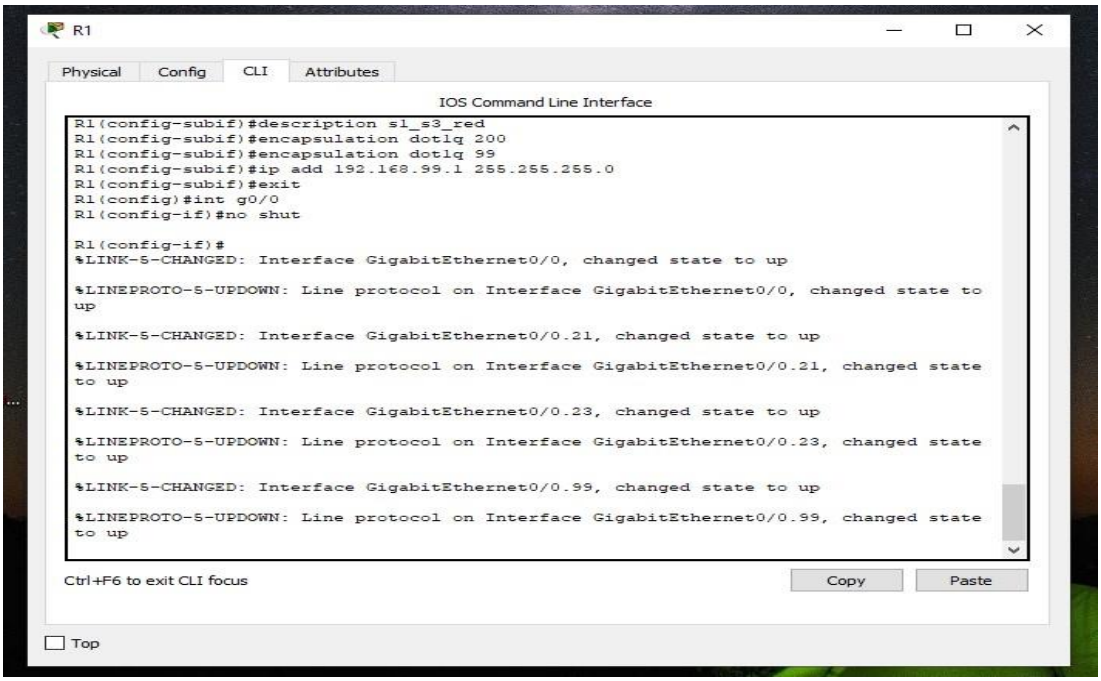

Figura 4. Configuración R1 subinterfaces

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.0	5/5
S3	R1, dirección VLAN 99	192.168.99.0	5/5
S1	R1, dirección VLAN 21	192.168.31.0	5/5
S3	R1, dirección VLAN 23	192.168.23.0	5/5

Tabla 12. Rutas para pruebas de conexión elementos

Utilizando el comando ping y las direcciones ip de cada una de las dependencias probamos la respectiva conexión de cada uno de los elementos.

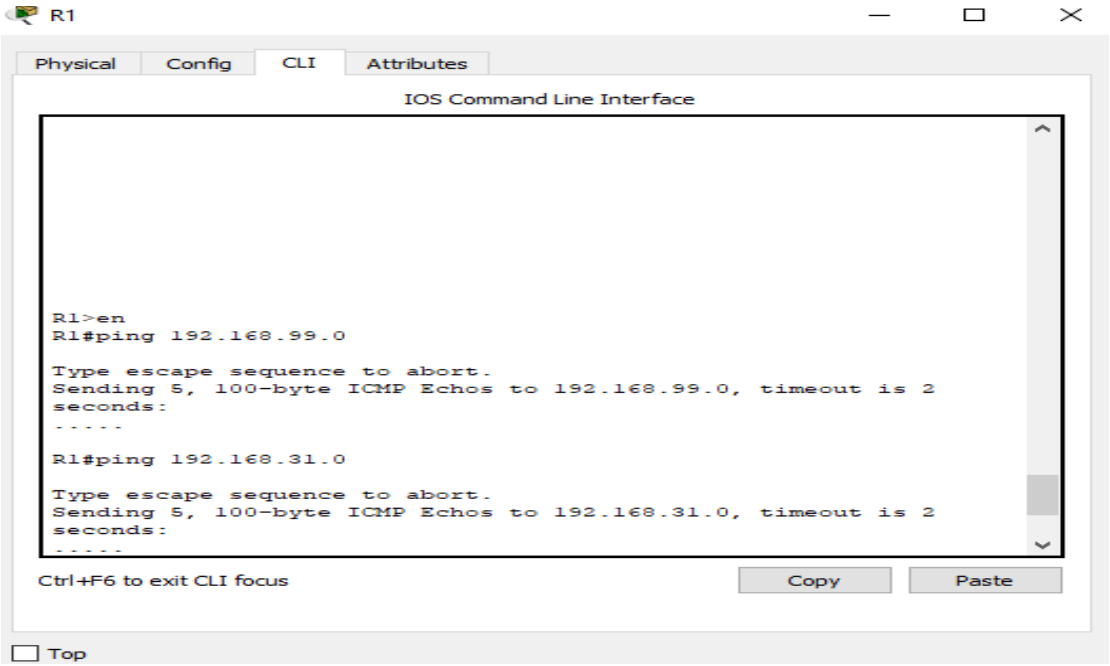

Figura 5. Prueba conexión de dispositivos entre dependencias

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Aplicamos el protocolo de ripv2 encaminando los router y estableciendo las puertas de enlace para la comunicación en las distintas áreas.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Enable Conf t Route ip
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. Network 172.16.12.0 0.0.0.3 area 0 Network 192.168.21.0 0.0.0.255 area 0 Network 192.168.23.0 0.0.0.255 area 0 Network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	Passive-interface g0/1.21 Passive-interface g0/1.23 Passive-interface g0/1.99
Desactive la sumarización automática	No auto-summary

Tabla 13. Configuración ripv2 en R1

Comando aplicado

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
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
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
```

Aplicamos do show ip route

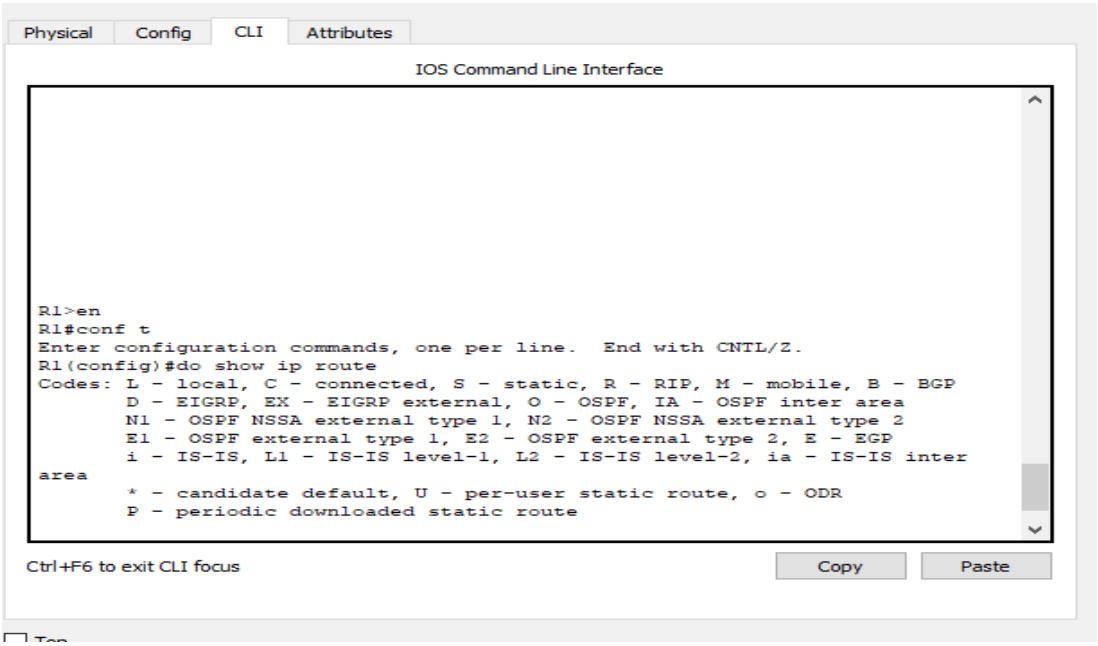

Figura 6. Configuración y función ripv2 en R1

Paso 2 Configurar RIPv2 en el R2

Aplicamos el protocolo de ripv2 encaminando los router y estableciendo las puertas de enlace para la comunicación en las distintas áreas.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Enable Conf t (config-router)#router rip
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	Passive-interface loopback g0/1
Desactive la sumarización automática.	(config-router)#no auto-summary

Tabla 14. configuración ripv2 en R2

Comando utilizado

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
R2(config-router)#network 172.16.1.0
R2(config-router)#network 192.168.21.0
R2(config-router)#network 192.168.23.0
R2(config-router)#network 192.168.99.0
R2(config-router)#passive-interface g0/1.21
R2(config-router)#passive-interface g0/1.23
R2(config-router)#passive-interface g0/1.99
R2(config-router)#no auto-summary

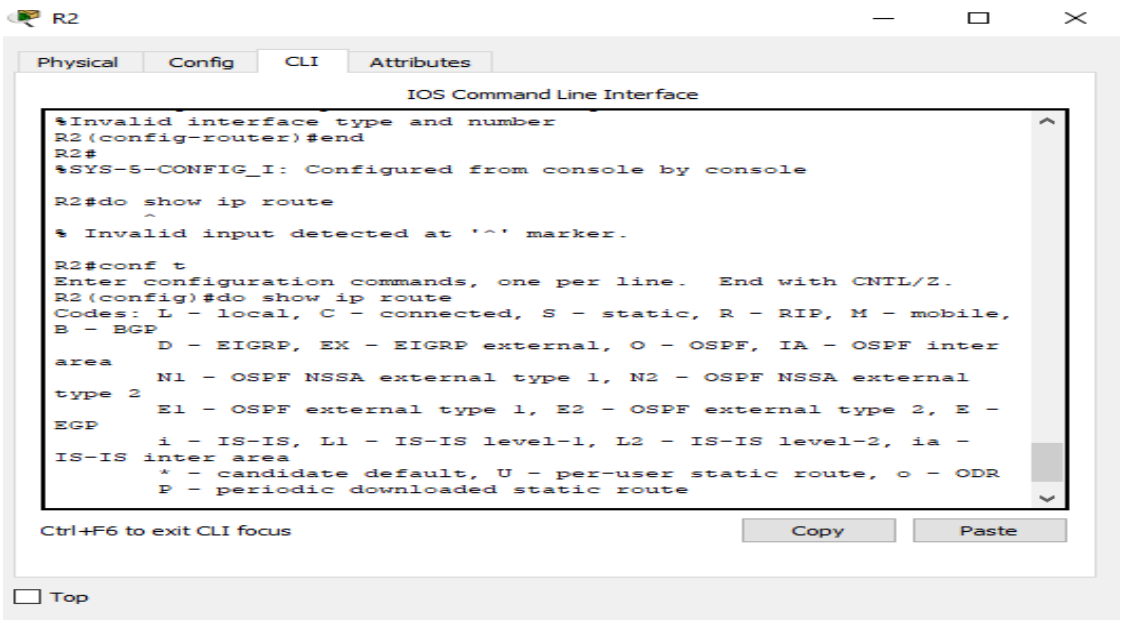

Figura 7 Configuración router R2

Paso 3: Configurar RIPv3 en el R3

Aplicamos el protocolo de ripv2 encaminando los router y estableciendo las puertas de enlace para la comunicación en las distintas áreas.

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Enable Conf t (config-router)#router rip
Anunciar redes IPv4 conectadas directamente	Network 172.16.12.0 0.0.0.3 area 0 Network 172.16.23.0 0.0.0.3 area 0 Network 10.10.10.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Passive-interface loopback 0
Desactive la sumarización automática.	(config-router)#no auto-summary

Tabla 15. configuración router R3

Comandos utilizados

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
R2(config-router)#network 172.16.1.0
R2(config-router)#network 192.168.21.0
R2(config-router)#network 192.168.23.0
R2(config-router)#network 192.168.99.0
R2(config-router)#passive-interface g0/1.21
R2(config-router)#passive-interface g0/1.23
R2(config-router)#passive-interface g0/1.99
R2(config-router)#no auto-summary

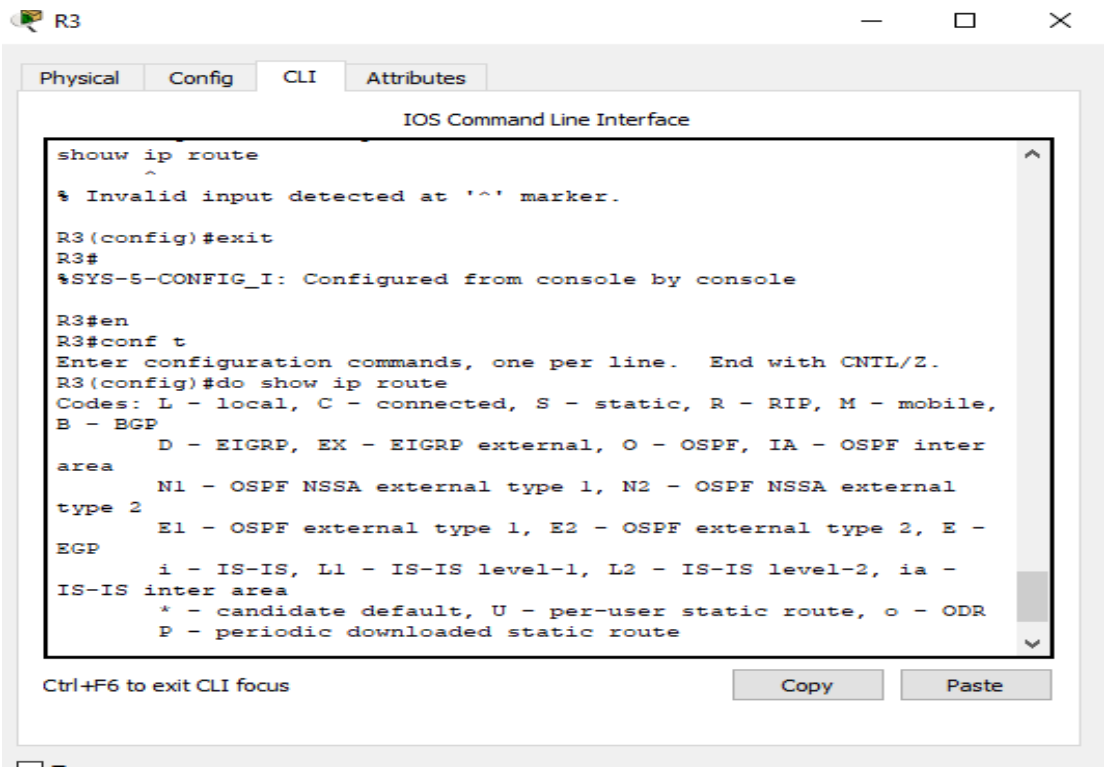

Figura 8. Configuración router R3

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:

Desarrollamos las siguientes preguntas, mostrando los comandos principales para la configuración de las direcciones de cada área, según dirección ip asignada o configurada.

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 interface
¿Qué comando muestra solo las rutas RIP?	Show ip route
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show running-config

Tabla 16. Desarrollo preguntas muestra de rutas

Parte 5: Implementar DHCP y NAT para IPv4

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

Mediante este protocolo configuramos el router R1 para establecer comunicación o union en base de las vlan 21 y 23 especificando en el código su respectiva dirección ip.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Enable Conf t 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	Enable Configure terminal Ip dchp exclude-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Ip dhcp pool ACCT Servidor DNS: 10.10.10.10 Dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com Domain-name ccna-sa.com Establecer el gateway predeterminado Default-router 192.168.23.1
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Ip dhcp pool ACCT Servidor DNS: 10.10.10.10 Dns-server 10.10.10.10 Nombre de dominio: ccna-sa.com Domain-name ccna-sa.com Establecer el gateway predeterminado Default-router 192.168.23.1

Tabla 17. DHCP y NAT IPv4 para vlan 21, 23

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

En esta configuración, los equipos en la red, debe tener su correspondiente IP asignada para poder acceder a Internet, adjuntando dicho comando en la tabla .

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** User webuser privilege 15 secret cisco 12345
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** Ip nat inside static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	Interface g0/0 Ip nat outside Interface g0/1 Ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 Access-list 1 permit 192.168.21.0 0.0.0.255 Access-list 1 permit 192.168.23.0 0.0.0.255 Access-list 1 permit 192.168.99.0 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** Ip nat pool internet 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Ip nat source inside list 1pool internet

Tabla 18. Configuración NAT estática y dinámica en el R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	IP: 192.168.21.23 NETMASK: 255.255.255.0 GATEWAY:192.168.21.1 DNS-SERVER 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	IP: 192.168.23.23 NETMASK: 255.255.255.0 GATEWAY:192.168.23.1 DNS-SERVER 10.10.10.10
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	5/5
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**	Muestra página web

Tabla 19. Configuración dirección pcA

Mostramos el direccionamiento en servidores para los pc adjuntos, demostrando la conectividad de una a otra y ejecución con el comando ping, procedemos, en un uno de los servidores, a realizar la conectividad web.

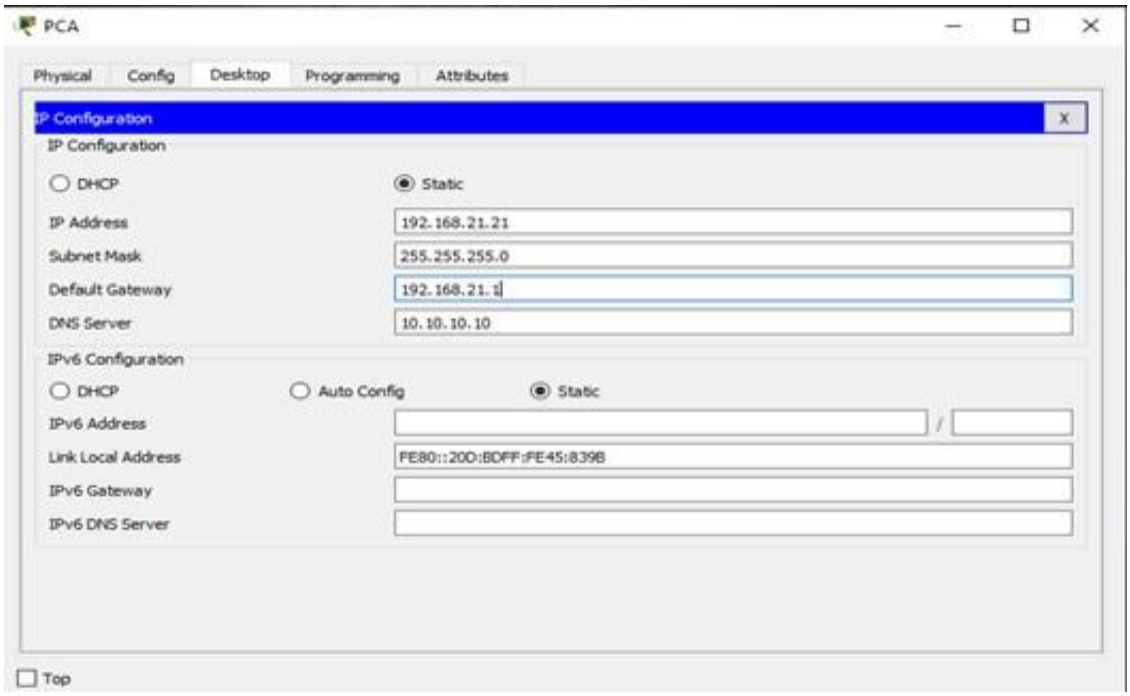

Figura 9. Direccionamiento dhcp PCA

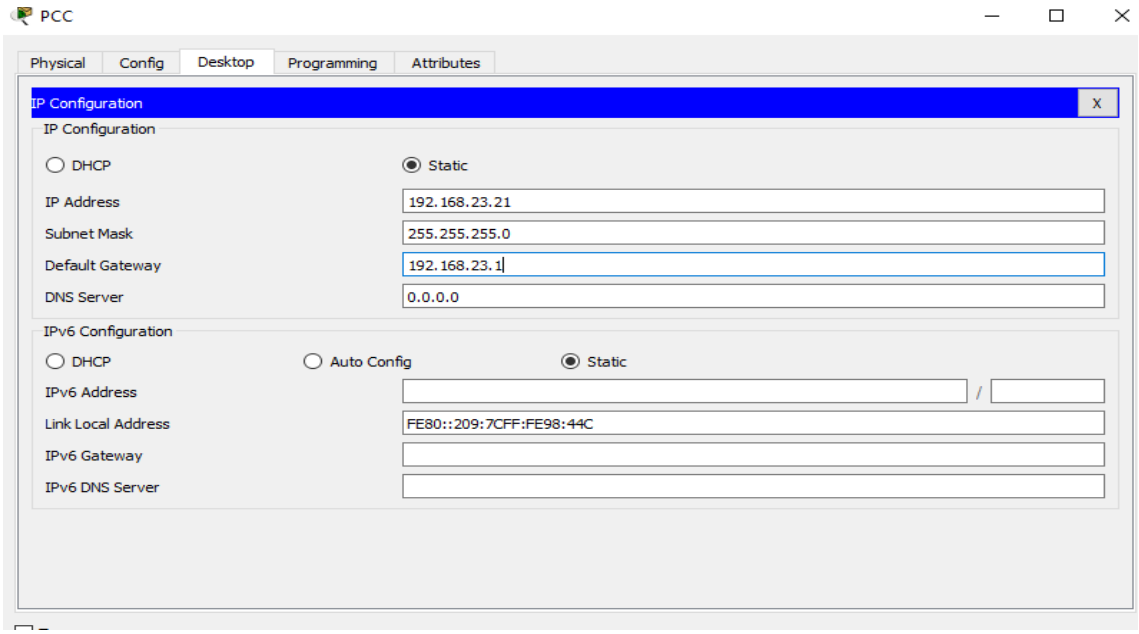

Figura 10. Direccionamiento dhcp pcc

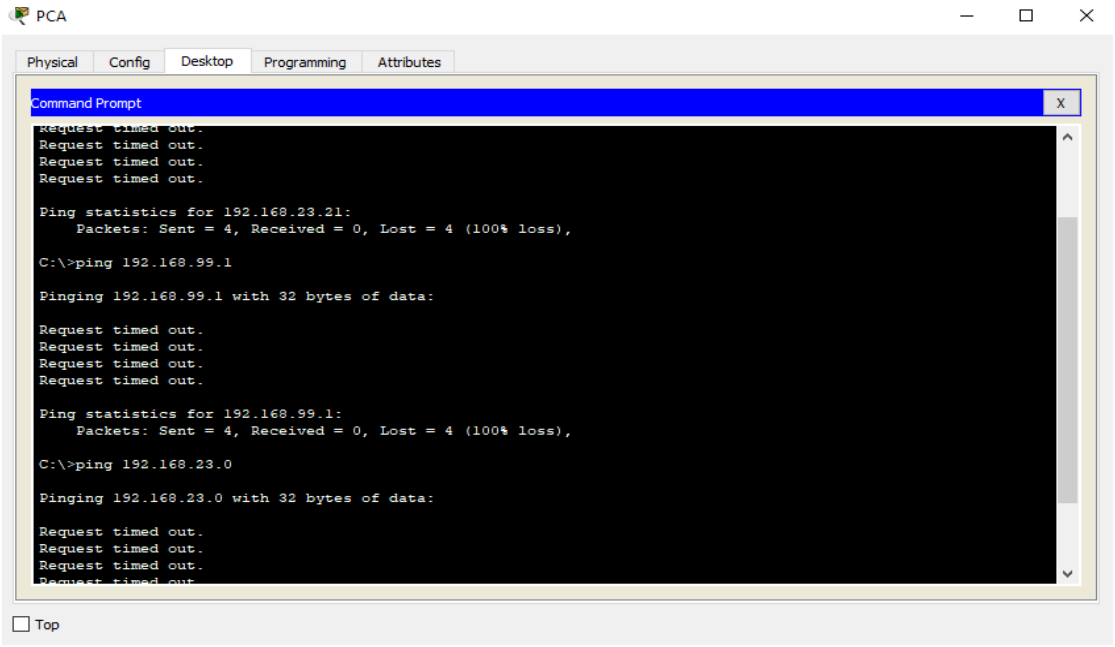

Figura 11. Ping pca a pcc

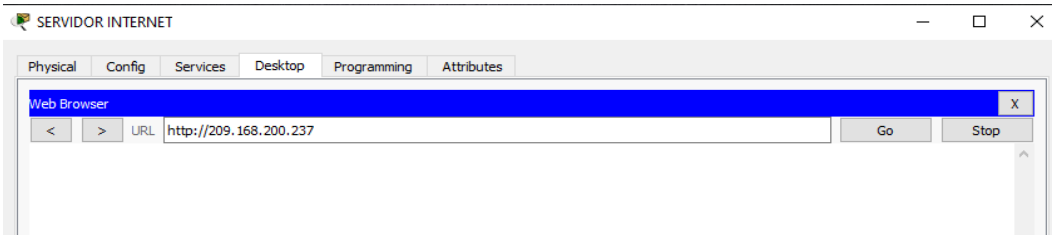

Figura 12. Conexión web servidor internet

Parte 6: Configurar NTP

Sincronizamos fecha hora a través de enrutamiento de paquetes aplicados en R1 y R2, mostrando los comandos utilizados

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.	Show clock *02.37 UTC Mar 5 2016
Verifique la configuración de NTP en R1.	R1(config)# ntp server

Tabla 20. Configuración fecha y horas routers

Comando utilizado R2

Router#clock set 09:00:25 ?
<1-31> Day of the month
MONTH Month of the year
Router#clock set 09:00:25 march ?
<1-31> Day of the month
Router#clock set 09:00:25 march 5 2016

Router#

Comando utilizado R1

Router#clock set 02:37:17 ?
<1-31> Day of the month
MONTH Month of the year
Router#clock set 02:37:17 march ?
<1-31> Day of the month
Router#clock set 02:37:17 march 5 2016

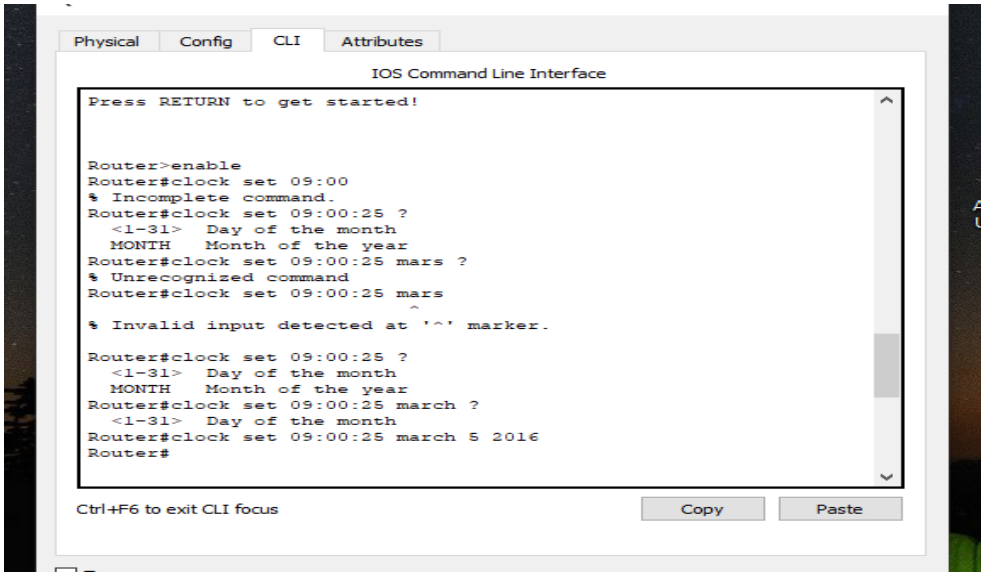

Figura 13. configuración fecha y hora para R1 y R2

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

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

Generamos los comandos adjuntos en la tabla, creando acceso en R2 por medio de Telnet, de este modo los switches admitirán las líneas de conexión vty

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** Enable Configure terminal Ip Access-list standard ADMIN-MGT permit Host 172.16.12.1
Aplicar la ACL con nombre a las líneas VTY	Line vty 04 Access-class ADMIN- MGT in
Permitir acceso por Telnet a las líneas de VTY	telnet 10.10.10.10
Verificar que la ACL funcione como se espera	telnet 172.16.23.2 connection refused for foreign host telnet 172.16.23.1 connection refused for foreign host

Tabla 21. restringir acceso

Commandos utilizados

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret cisco
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#loggin synchronous
R2(config-line)#exec-timeout 10
R2(config-line)#transport input telnet
R2(config-line)#exit
```

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

Se resuelven las siguientes preguntas mostrando los comandos solicitados empleados en cisco

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 counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show running-config
¿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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation*

Tabla 22. Solución de preguntas para el comando CLI

Escenario 2

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

Topología de red

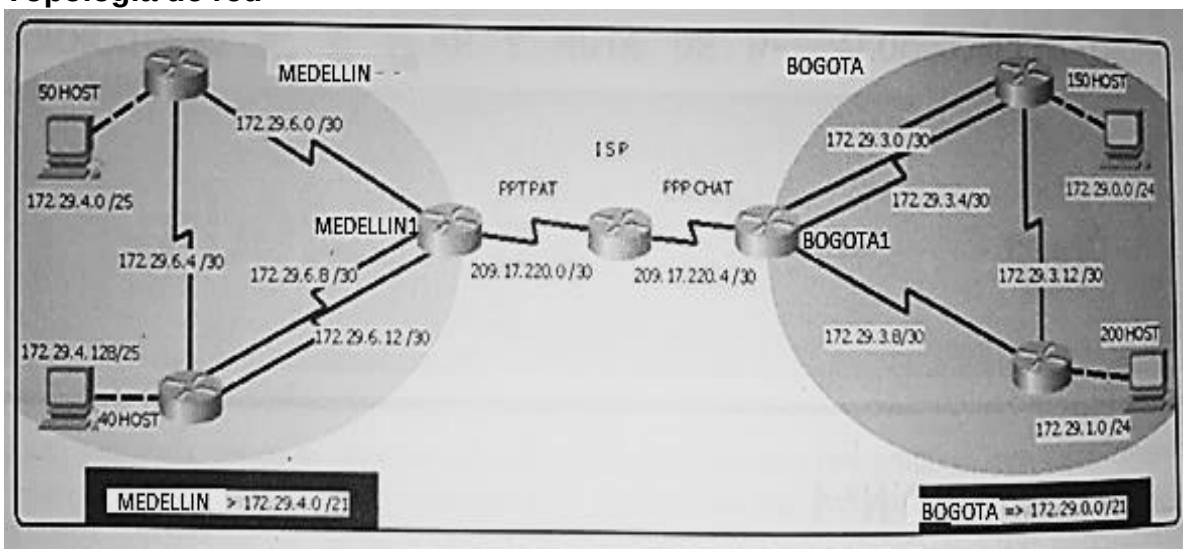

Figura 14.Diagrama escenario 2

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

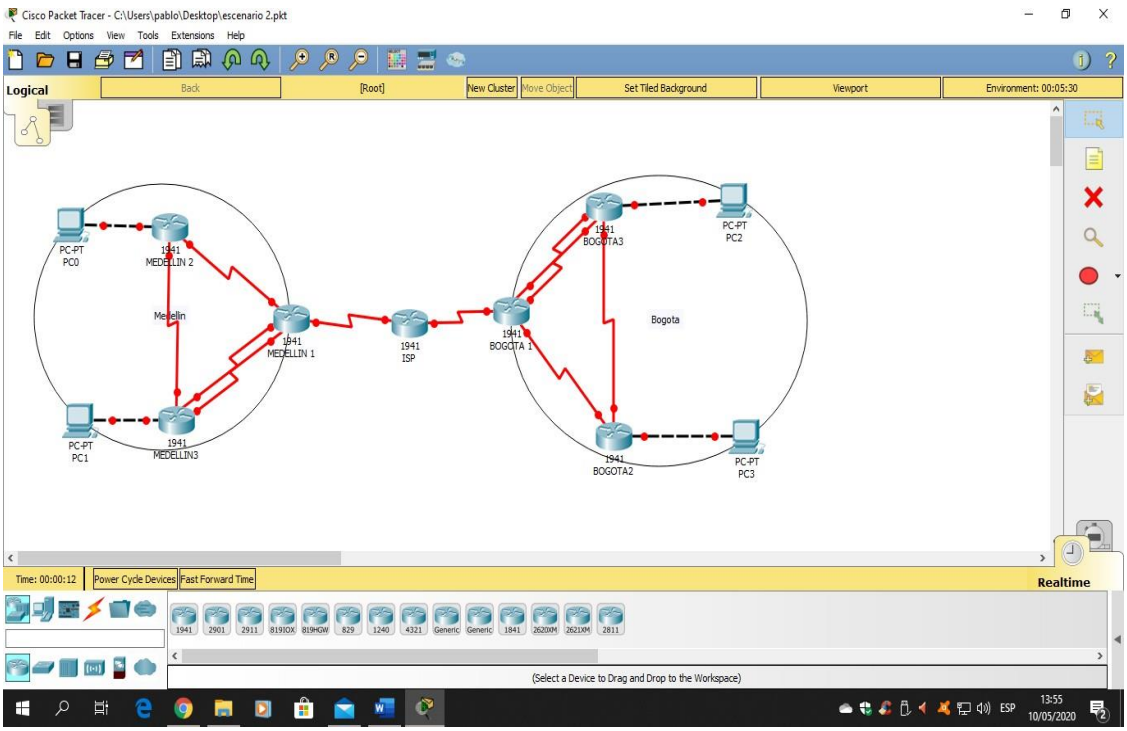

Figura 15.Topologia y conexión escenario 2

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

No ip domain-lookup
Service password-encryption
Enable secret class
Banner motd % acceso no autorizado %
Line console 0
Password cisco
Login
Line vty 0 15
Password cisco
Login

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.

Iniciamos configurando las ip de todos los Router, luego aplicamos el protocolo y desactivamos la sumarización automática. Esto mencioando anteriormente se aplica a todas las ciudades y sus distintas sedes, mediante los comandos configurados, en el punto b.

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.

Medellin 2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.0
Router(config-router)#network 172.29.4.0
Router(config-router)#no auto-summary
Router(config-router)#passive-interface g0/0
```

Medellin 1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#network 172.29.4.128
Router(config-router)#no auto-summary
Router(config-router)#passive-interface g0/0
```

Medellin 3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.29.6.4
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#network 172.29.4.128
Router(config-router)#no auto-summary
Router(config-router)#passive-interface g0/0
```

Bogota 1

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 209.17.220.4
Router(config-router)#network 172.29.3.8
Router(config-router)#network 172.29.3.4
Router(config-router)#network 172.29.3.0
Router(config-router)#no auto-summary
Router(config-router)#hostname BOGOTA1
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.6
BOGOTA1(config)#route rip
BOGOTA1(config-router)#default-information originate
```

Bogota 2

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.29.3.8
Router(config-router)#network 172.29.3.12
Router(config-router)#network 172.29.1.0
```

```
Router(config-router)#no auto-summary
Router(config-router)#passive-interface g0/0
Router(config-router)#
```

Bogota 3

```
outer>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 172.29.3.0
Router(config-router)#network 172.29.3.4
Router(config-router)#network 172.29.3.12
Router(config-router)#network 172.29.0.0
Router(config-router)#no auto-summary
Router(config-router)#passive-interface g0/0
```

Isp

```
ISP>en
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router rip
ISP(config-router)#version 2
ISP(config-router)#network 209.17.220.4
ISP(config-router)#network 209.17.220.0
ISP(config-router)#no auto-summary
ISP(config-router)#ip route 172.29.4.0 255.255.252.0 209.17.220.5
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5
```

c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

```
ISP#en
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.5
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5
ISP(config)#
```

Parte 2: Tabla de Enrutamiento.

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

Comprobamos mediante el comando ping las direcciones asignadas en las diferentes dependencias de Bogota y de Medellin.

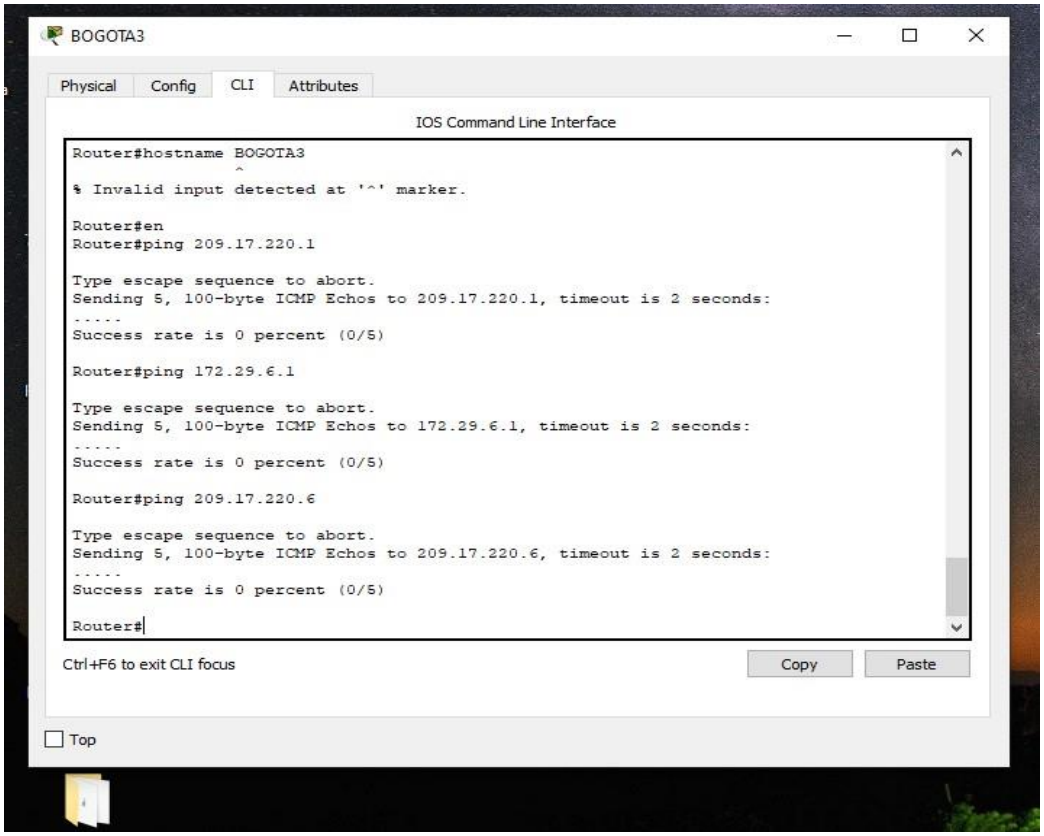

Figura 16. conexión de las rutas asignadas

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

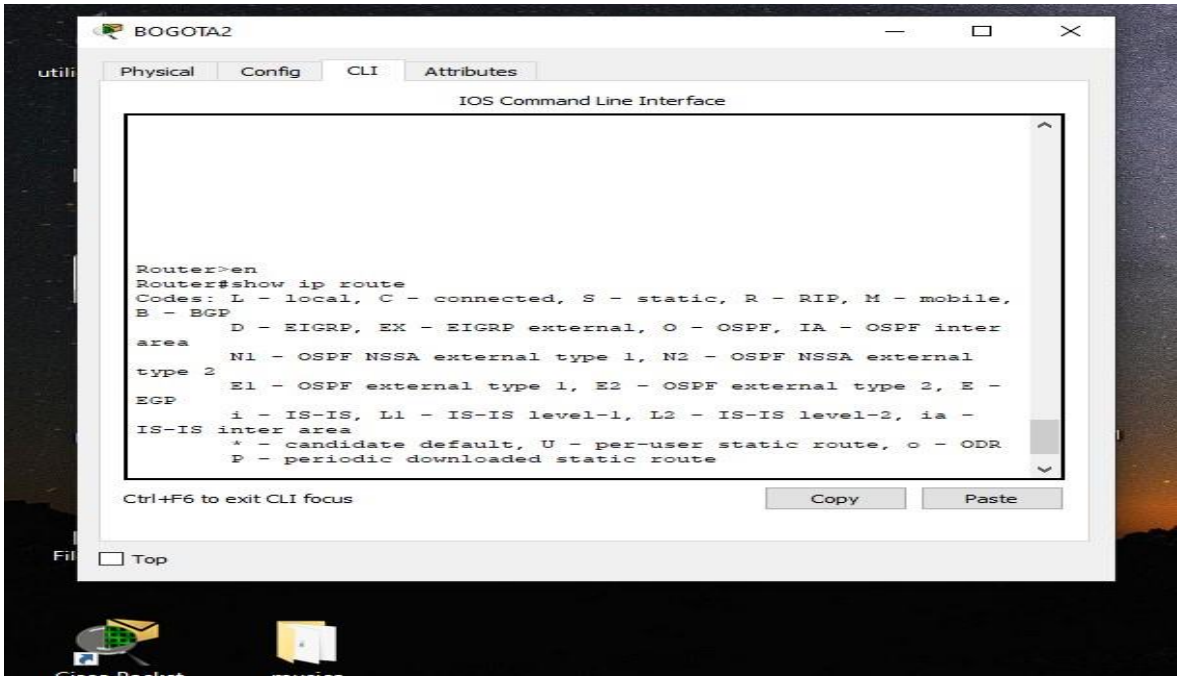

Figura 17. conexión establecida de los routers

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.

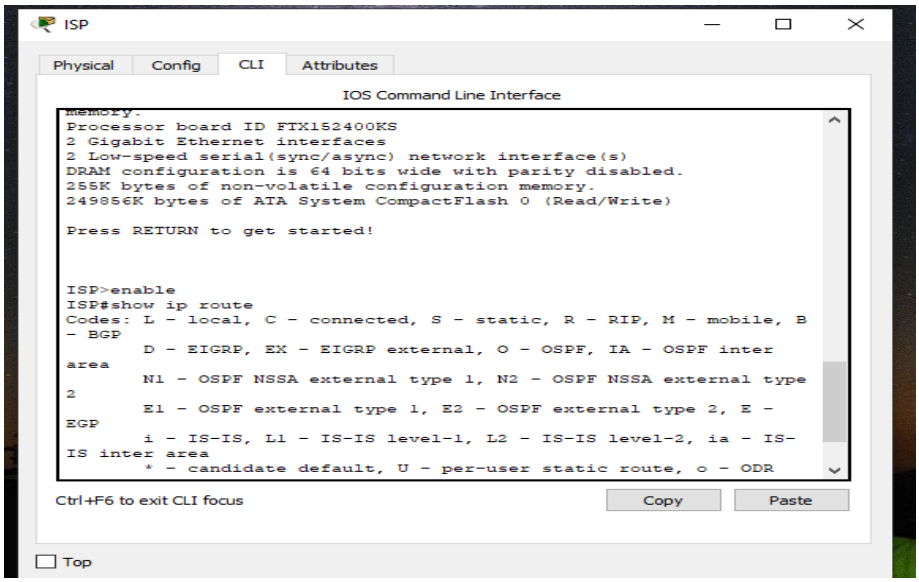

Figura 18. Configuracion rutas ISP

ISP#en
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.5
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Tabla 23. Tabla de interfaces por sedes

Bogotá 1

```
BOGOTA1#en
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface s0/1
BOGOTA1(config-router)#
```

Bogotá 2

```
BOGOTA2#en
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface s0/1
BOGOTA2(config-router)#
```

Bogotá 3

```
BOGOTA3#en
BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface s0/1
BOGOTA3(config-router)#
```

Medellín 1

```
MEDELLIN1#en
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface s0/1
MEDELLIN1(config-router)#
```

Medellín 2

```
MEDELLIN2#en
MEDELLIN2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface s0/1
MEDELLIN2(config-router)#
```

Medellin 3

```
MEDELLIN3#en
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface s0/1
MEDELLIN3(config-router)#
```

Parte 4: Verificación del protocolo OSPF.

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

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

En las previas imágenes documentamos la conexión de cada uno solucionando los ítems a y b verificando enrutamiento en la red.

Medellín 1

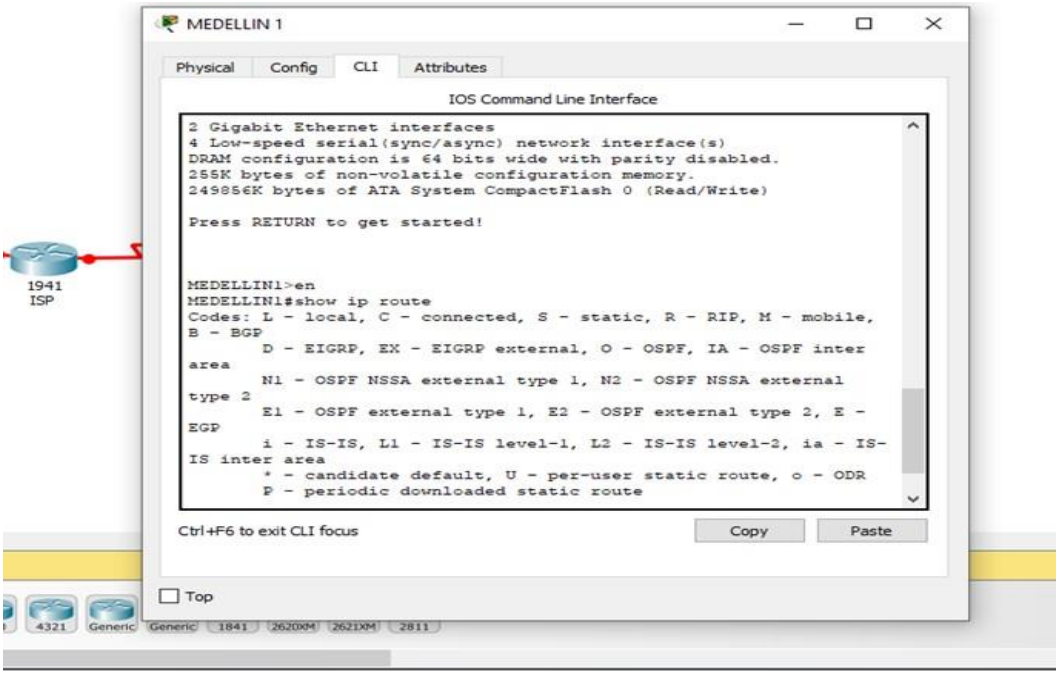

Figura 19. Verificación enrutamiento Medellín 1

Medellín 2

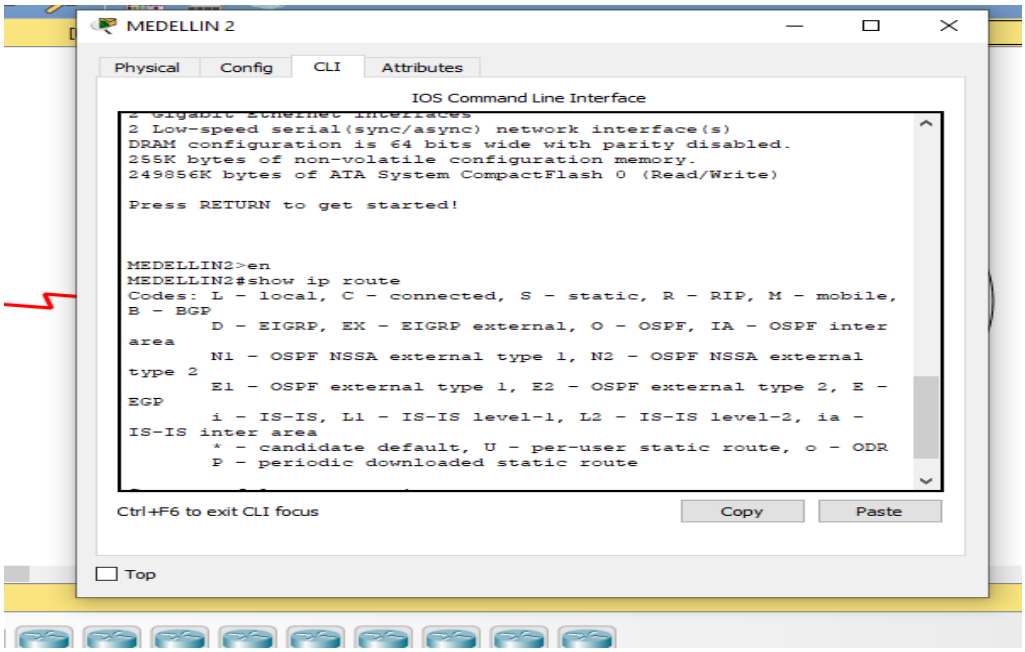

Figura 20. Verificación enrutamiento Medellín 2

Medellín 3

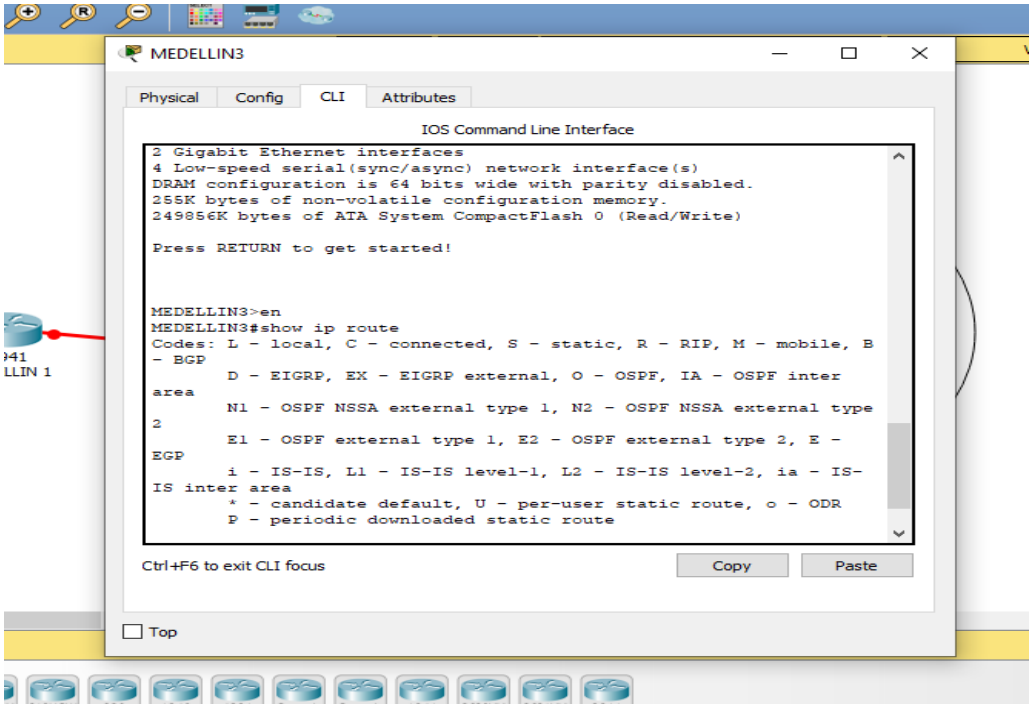

Figura 21 Verificación enrutamiento Medellín 3

Bogotá 1

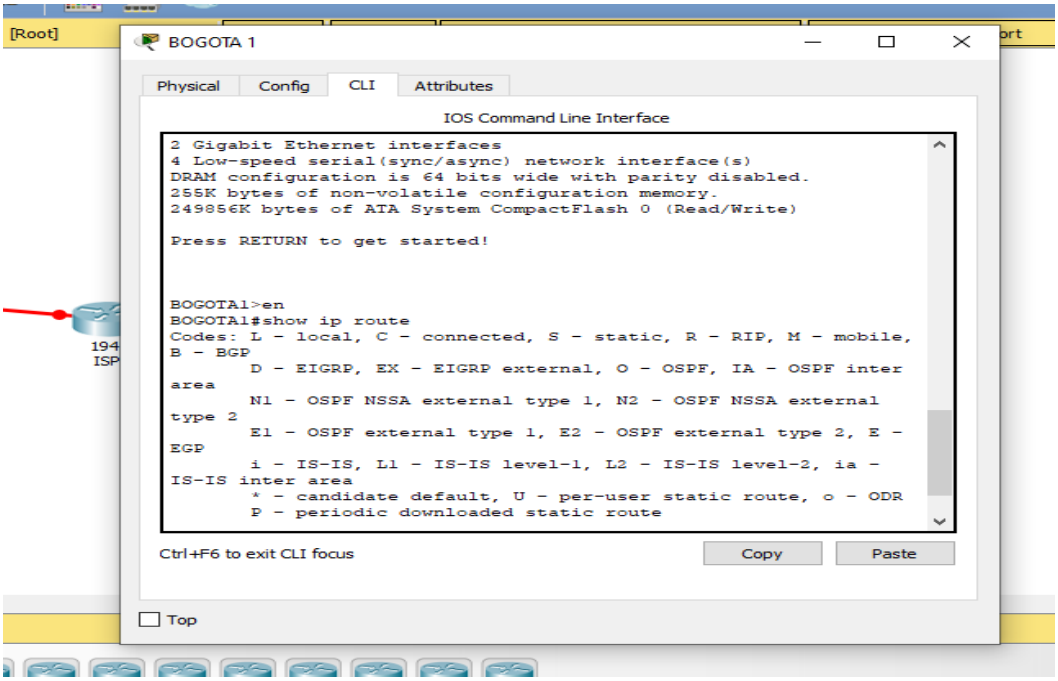

Figura 22. Verificación enrutamiento Bogotá 1

Bogotá 2

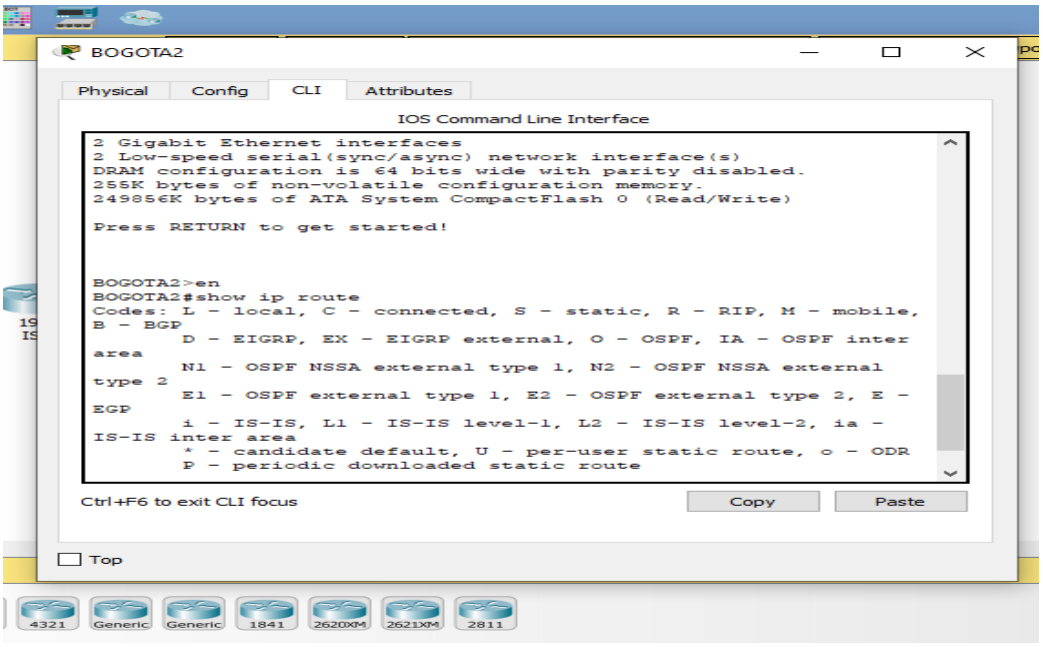

Figura 23. Verificación enrutamiento Bogotá 2

Bogotá 3

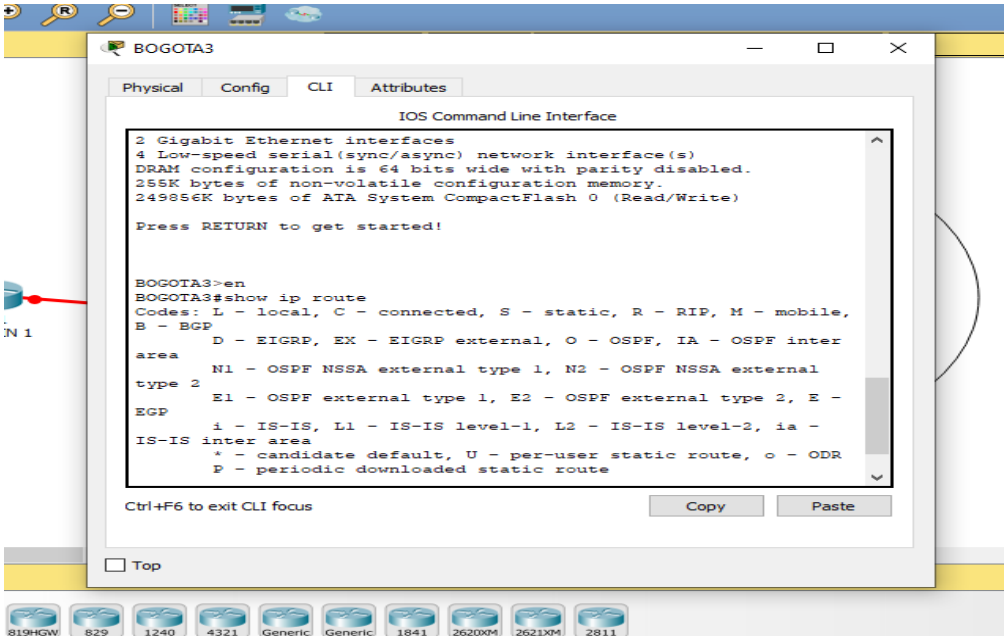

Figura 24. Verificación enrutamiento Bogotá 3

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Aplicamos la dirección principal, para las demás direcciones privadas internas aplicadas entre Medellín 1 - isp , pero asignando un puerto diferente a las demás

Isp

```
ISP>en
ISP#config 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
```

Medellin 1

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#username isp password cisco
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
```

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

Isp

```
ISP>en
ISP#config 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)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to
down
ISP(config-if)#
ISP(config-if)#ppp authentication chap
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Bogotá 1

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

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.

Con esta configuración crearemos ip externa a fin de comunicarse con las restantes:

```
MEDELLIN1>enable
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
MEDELLIN1(config-std-nacl)#exit
MEDELLIN1(config)#ip nat inside source list HOST interface g0/0 overload
MEDELLIN1(config)#int g0/0
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 s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
```

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.

Solución de los puntos b y c:

Medellin 1

```
MEDELLIN1>en
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip nat inside source list 1 interface g0/1/0 overload
%Invalid interface number (Slot is empty)
MEDELLIN1(config)#ip nat inside source list 1 interface s0/1/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#
```

Bogotá 1

```
BOGOTA1>en
BOGOTA1#config 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 s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
```

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.

Medellin 2

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-route 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#end
MEDELLIN2#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-route 172.29.4.129
```

```
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#
```

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

Habilitamos difusión paquetes de datos entre Medellín 3 y el destino Medellín 2.

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

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

Con esta configuración distribuiremos las redes de Bogotá 2 y 3 mediante su dirección generando conexión con Medellín 2, creando así vinculo en estas sedes

Comando utilizado:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-route 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-route 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#
```

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

A través del broadcast difundimos la información de datos de Bogotá 1 a Bogotá 2, así se puede transferir a otros nodos receptores.

Comando utilizado

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)
```

6.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO

El software cisco packet tracer, permite graficar y mostrar las previas conexiones de red, que se propusieron en los dos escenarios, por lo tanto, entendemos el enrutamiento y el objetivo de donde estos serán conectados.

Se establecen los protocolos de seguridad, para brindar acceso mediante contraseña así creando uno de los tipos de redes corporativas aplicadas a sectores de laborales como de dependencias laborales y sedes.

Conocemos los códigos o comandos necesarios para ejecutar el sistema de red, teniendo en cuenta el propósito y objetivo. Sea para el escenario 1 donde se realizó la conexión de sectores laborares, de administración, contabilidad e ingeniería y el escenario 2, donde unificamos las conexiones de una empresa en sus distintas sedes de Bogotá y Medellín, para que funcionen como un solo módulo de red.

Mediante la utilización del software también realizamos la configuración de los routers, que permiten al usuario final, laborar en su determinado sector, cumpliendo el protocolo destinado, o el permiso para ejecutar ciertas funciones integradas en una red.

CONCLUSIONES

Para el desarrollo del escenario uno, se comprende la temática, respecto a la configuración establecida. Destacando elementos importantes como lo es las subinterfaces, además de enlaces troncales, como unos de los componentes importantes para crear subredes en un mismo modulo o de las diferentes dependencias que se trabajaron, en direccionamiento de red en contabilidad, ingeniería y administración.

durante el proceso de trabajo en el escenario dos, se destaca términos importantes como lo es LAN, Vlan, logrando en ello, aplicar distintas redes independientes, en una sola red física, tal como se configuro las sedes de la misma empresa, en Medellín y Bogotá, como una sola organización, teniendo en cuenta los protocolos de seguridad.

En cada uno de los escenarios se configuro, cada uno de los elementos, obteniendo aprendizaje en el enrutamiento de cada uno, logrando conectar dependencias que trabajan en base a una sola red u organización.

RECOMENDACIONES

En el procedimiento, para el desarrollo de los escenarios, se recomienda utilizar cisco packet tracer versión 7.2 ya que esta permite verificar los punto a punto de las conexiones de los elementos, con indicador a través de colores, brindando seguridad en el cableado, y la eliminación de ciertos componentes no deseados de forma más accesible en su interfaz.

Es importante comprender el termino de las subinterfaces ya que, en base de este término, se trabajan distintos tipos y configuraciones de red, para llevar a cabo el proyecto de los escenarios propuestos, explicando en su teoría distintas redes para un módulo u organización, tal como se plantearon en las dependencias y sedes de dichos escenarios.

BIBLIOGRAFÍA

Auditoria grupo redes, “ configuración y conceptos básicos de switching”.(en línea).(13 mayo de 2020) disponible en: (http://auditoriagruporedes.blogspot.com/2018/11/configuracion-y-conceptos-basicos-de.html).

Calameo,” resumen de principio básicos de enrutamiento y routers”.(en línea).(13 mayo de 2020) disponible en: (https://es.calameo.com/books/00077688959361494ab8d).

DE ROUSE, Margaret “topología de red”.(en línea).(13 mayo de 2020) disponible en: (https://searchdatacenter.techtarget.com/es/definicion/Topologia-de-red).

Ecured, “ protocolos de red “.”en línea” (13 mayo de 2020) disponible en: (https://www.ecured.cu/Protocolos_de_red).

Ecured, “ ruteo “.”en línea” (13 mayo de 2020) disponible en: (https://www.ecured.cu/Ruteo).

Fernández, Raúl “ enrutamiento entre vlans con packet tracer ”.(en línea).(13 mayo 2020) disponible en: (https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-entre-vlans-con-packet-tracer).

Itesa.edu, “ introducción a redes conmutadas”.(en línea).(13 mayo de 2020) disponible en: (https://www.itesa.edu.mx/netacad/switching/course/module1/index.html#1.0.1.1).