SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SANDRA JOHANNA CAICEDO SERRANO

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNA
RAGONVALIA
2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

SANDRA JOHANNA CAICEDO
SERRANO

TRABAJO DE GRADO PRESENTADO PARA
OPTAR EL TÍTULO DE INGENIERÍA DE
SISTEMAS

TUTOR
ING. GUSTAVO ADOLFO RODRÍGUEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNA
RAGONVALIA
2020

NOTA DE ACEPTACIÓN

Firma del presidente de jurado

Firma del jurado

Firma del jurado

Ragonvalia, 07 de julio de 2020

DEDICATORIA

El presente trabajo lo dedico principalmente a Dios por darme las fuerzas para continuar con este proceso, a mis hijos padres y hermanos, por su amor trabajo y sacrificio en todos estos años, gracias a ustedes que han sido el motor para lograr llegar hasta donde estoy y convertirme en quien soy.

AGRADECIMIENTOS

Especialmente doy gracias a Dios por permitirme tener esta significativa experiencia, gracias a la universidad por permitirme y darme la oportunidad de convertirme en profesional, gracias a tutores y compañeros que hicieron parte de este proceso de aprendizaje integral de formación

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

ROUTER: Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet

PROTOCOLO: Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales

ENCAPSULAMIENTO: Es el proceso en el que los datos, que se encuentran dispuestos para ser enviados a través de una red, se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red.

ENRUTADOR: Dispositivo de red que dirige o enruta paquetes a través de las redes. Un enrutador funciona con una dirección de mensajes IP, a fin de determinar la mejor ruta hacia su destino.

IP: Es un direccionamiento utilizado para identificar un dispositivo en la red.

INTERNET: Es la interconexión global de millones de redes y computadoras, para formar una red de área extensa

INTERFAZ: La conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro.

ENRUTAMIENTO: Proceso utilizado para determinar la mejor ruta y hacer avanzar la información a lo largo de esa ruta, a partir de una red fuente o segmento de red, hacia una dirección de red de destino.

ETHERNET: Tecnología compartida de red sobre la cual todas las estaciones de trabajo de una red comparten al ancho de banda disponible, el cual puede ir desde 10 Mbps a 1 Gbps. Ethernet es el método de acceso utilizado comúnmente para redes de áreas pequeñas.

CAPA DE TRANSPORTE: Capa 4 del modelo OSI; proporciona control de un extremo a otro para transferencia de la información a través de la red.

CAPA FÍSICA: Capa 1 del modelo OSI; Esta capa define la manera como la corriente eléctrica de bits se transporta a través del hardware y los dispositivos mecánicos de la red.

CLIENTE / SERVIDOR: Tipo de red que incluye un servidor y clientes la autorización para acceder a los recursos de la red se administra por medio de un administrador central de la red.

CLIENTE: Estación de trabajo de una red que solicita y recibe servicios de un servidor de red. Los clientes de red solicitan los servicios del servidor de la red

INTERFERENCIA: Ruido no deseado del canal de comunicación.

ISO (Organización Internacional para la Normalización): Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking..

COMPUTADORA AISLADA: Computadora que no está conectada a otras computadoras y como resultado no puede compartir recursos, a no ser a través de una red de patines.

CONCENTRADOR (HUB): Dispositivo de red que se utiliza para conectar una o más estaciones de trabajo a una red.

CONECTIVIDAD: Es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.

CONECTOR BNC: Conector utilizado para cable coaxial delgado y grueso.

HTTP: Protocolo de transferencia de hipertexto, un protocolo de red que se usa para recuperar páginas web desde un servidor web

DATAGRAMA: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información de la Internet. Los términos trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

DNS (sistema de nombres de dominio): Es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.

FIBRA ÓPTICA: Tipo de cable de red que utiliza delgados filamentos de vidrio para transportar información digital que ha sido transformada en impulsos de luz. Es muy

costoso, difícil de trabajar y ciertamente no vale la pena el esfuerzo para una red de área pequeña.

MASCARA DE DIRECCIÓN: Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host.

MÁSCARA DE SUBRED: Máscara de dirección de 32 bits que se usa en IP para indicar los bits de una dirección IP que se utilizan para la dirección de subred.

FIREWALL: Router o servidor de acceso o varios routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de acceso, así como otros métodos para garantizar la seguridad de la red privada.

CABLE COAXIAL: Tipo de cable de red muy semejante al utilizado para conectar su aparato de televisor al decodificador de cable.

CAPA DE APLICACIÓN: Capa 7 del modelo OSI; proporciona autenticación, privacidad y restricción de información a los usuarios.

CAPA DE RED: Capa 3 del modelo OSI; define la manera como se enruta la información a una dirección destino

PING: Comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

PUERTO: Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

DHCP (Protocolo de configuración dinámica de host): De tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

DIRECCIÓN MAC (Protocolo de acceso a medios): Dirección física de un nodo. La dirección MAC es la única que se “graba” electrónicamente de manera permanente en los adaptadores de red, entre ellos las tarjetas de red (NIC), por parte de los fabricantes. La dirección MAC se utiliza para identificar exclusivamente cada nodo unido a la red

FTP (Protocolo de transferencia de archivos): Protocolo de aplicación, parte de la pila de protocolo TCP/IP utilizado para la transferencia de archivos entre nodos de red.

HOST: Sistema informático en una red. Similar al término nodo, salvo que host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers..

MODELO OSI: Modelo de referencia de interconexión de sistemas abiertos, un estándar que define las diversas funciones denominadas capas, que un paquete de red transmite al trasladarse desde una fuente hasta su destino. El modelo OSI de siete capas se aplica tanto a las redes locales como a las extensas, entre ellas Internet.

VLAN: Procedimiento para establecer redes lógicas de una forma independiente dentro de una misma red física.

CAPA DE PRESENTACIÓN: Capa 6 del modelo OSI; administra la conversación de la información entrante y saliente de un formato de datos a otro.

NAT: Protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.

OSPF: Protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-estado.

PUERTOS TRONCALES: Enlace punto a punto para enviar y recibir el tráfico entre routers o switches.

RED: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat..

TOPOLOGÍA FÍSICA: Disposición de cada uno de los dispositivos o hardware dentro de una red.

TOPOLOGÍA LÓGICA: Es la forma que utilizan los hosts para comunicarse a través de una red.

TOPOLOGÍA: Cadena de comunicación usada por los nodos que conforman una red para comunicarse.

TRAZAS: La traza de un algoritmo (o programa) indica la secuencia de acciones (instrucciones) de su ejecución, así como, el valor de las variables del algoritmo (o programa) después de cada acción (instrucción)

RESUMEN

A través de este trabajo se busca que los estudiantes profundicemos en este campo emergente de las Redes de tal forma que estemos en capacidad de responder a la demanda creciente de personal especializado en el área de tecnologías de la información, acompañado de un alto componente practico, mediante el uso de herramientas de simulación y laboratorios remotos

INTRODUCCIÓN

Las redes de datos que normalmente utilizamos en nuestra vida diaria transforman desde redes locales hasta grandes internet Work globales. Mientras que en casa un usuario puede tener un router y dos o mas computadoras, en una empresa posiblemente necesitan varios routers y switches para atender las necesidades de comunicación de datos de cientos o hasta miles de computadoras.

Se realizara el desarrollo de los escenarios expuestos, analizaremos cada uno de los contenidos y entraremos en consenso y debate con sus partes, dando así las pautas del paso a paso en cada una de las practicas realizadas individualmente, contamos con material de consulta en la plataforma Cisco con el fin de resolver inquietudes y novedades en cada uno delos puntos a resolver, se cuenta con el apoyo del tutor de curso, de la mano con la directora del diplomado, quienes establecerán las pautas y resolverán las posibles dudas e inquietudes.

A través de este trabajo se procura dar a conocer los contenidos asimilados durante el diplomado mediante el cual se aplicará el enrutamiento, parámetros de seguridad y acceso a distintos dispositivos en la red, sin pasar por alto las configuraciones OSPF, RIP, NAT, verificación de ACL. Las cuales se implementan en routers para mayor seguridad de una red o ampliar políticas de entrada y salida de paquetes para equipos específicos, así mismo se realiza la configuración de servidores DHCP, siendo este un protocolo de propagación que funciona de manera predeterminada en donde sus paquetes no atraviesan por medio de enrutadores. La función de un agente de trasmisión DHCP es recibir cualquier difusión DHCP de la subred y reenviar a la dirección IP determinada en una subred diferente.

Es importante destacar el grado de importancia que tiene el simulador Cisco Packet Tracer ya que, sin la ejecución de este, la interpretación de grado de análisis seria nulos, a pesar de que algunos comandos no los permite ejecutar, es significativo terne presente que la visión que brinda nos admite adquirir conocimientos y desarrollar si se quiere la crítica necesaria para inferir en decisiones de implementación y diseño en una red

OBJETIVOS

OBJETIVO GENERAL

Fortalecer los conocimientos precisos para el diseño de redes mediante el uso del modelo ordenado, con el fin de perfeccionar el beneficio de la red y reunir de carácter conveniente el uso de las tecnologías y protocolos de intercambio y enrutamiento.

OBJETIVOS ESPECÍFICOS

- Utilizar herramientas de la simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que accedan a ejecutar un estudio sobre la conducta de diversos protocolos y métricas de enrutamiento, valorando la conducta de enrutadores, a través de comandos de dirección de tablas de enrutamiento, bajo el uso de protocolos de resultante distancia y estado de vínculo.

- Manejar comandos de configuración avanzada de routers, realizando RIP y enrutamiento estático; bajo un plan de direccionamiento IP sin clase, para dar procedimientos de red y conectividad escalables, mediante el uso de principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

PLANTEAMIENTO DEL PROBLEMA

DEFENICION DEL PROBLEMA

El presente trabajo articula en su contenido diversas temáticas que permiten abordar el núcleo problemático: gestión de sistemas y servicio de telecomunicaciones en función del núcleo integrador problemático: las telecomunicaciones como herramienta para la complejidad global con visión socio humanística, en donde hay un aprendizaje mediante la creación de una red empresarial eficaz y escalable; así como a través de instalar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de una red convergente

JUSTIFICACION

Es importante estar en la capacidad de solucionar problemas responder a la demanda creciente de personal especializado en el área de las tecnologías de la información, acompañado de un alto componente practico, mediante el uso de herramientas de simulación y laboratorios remotos.

Para este fin contamos con una herramienta de gran experiencia efectiva como la configuración de sistemas operativos de red, protocolos de comunicación, mecanismos de acceso al medio y características de la capa de red, la capa de trasporte, asignación de direcciones IP, subnetting y capa de aplicación.

Además, analizamos la forma adecuada de diseñar y configurar soluciones soportadas en el uso de dispositivos de conmutación acorde con la topología de red requeridas bajo el uso de protocolos basadas en STP y VLANs bajo una arquitectura jerárquica

Por otra parte, contamos con la orientación para utilizar el enrutamiento estático, enrutamiento dinámico, enrutamiento de protocolos de estado enlace, listas de acceso, adignacion dinámica de direcciones IP y traducciones de direcciones IP mediante NAT

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.

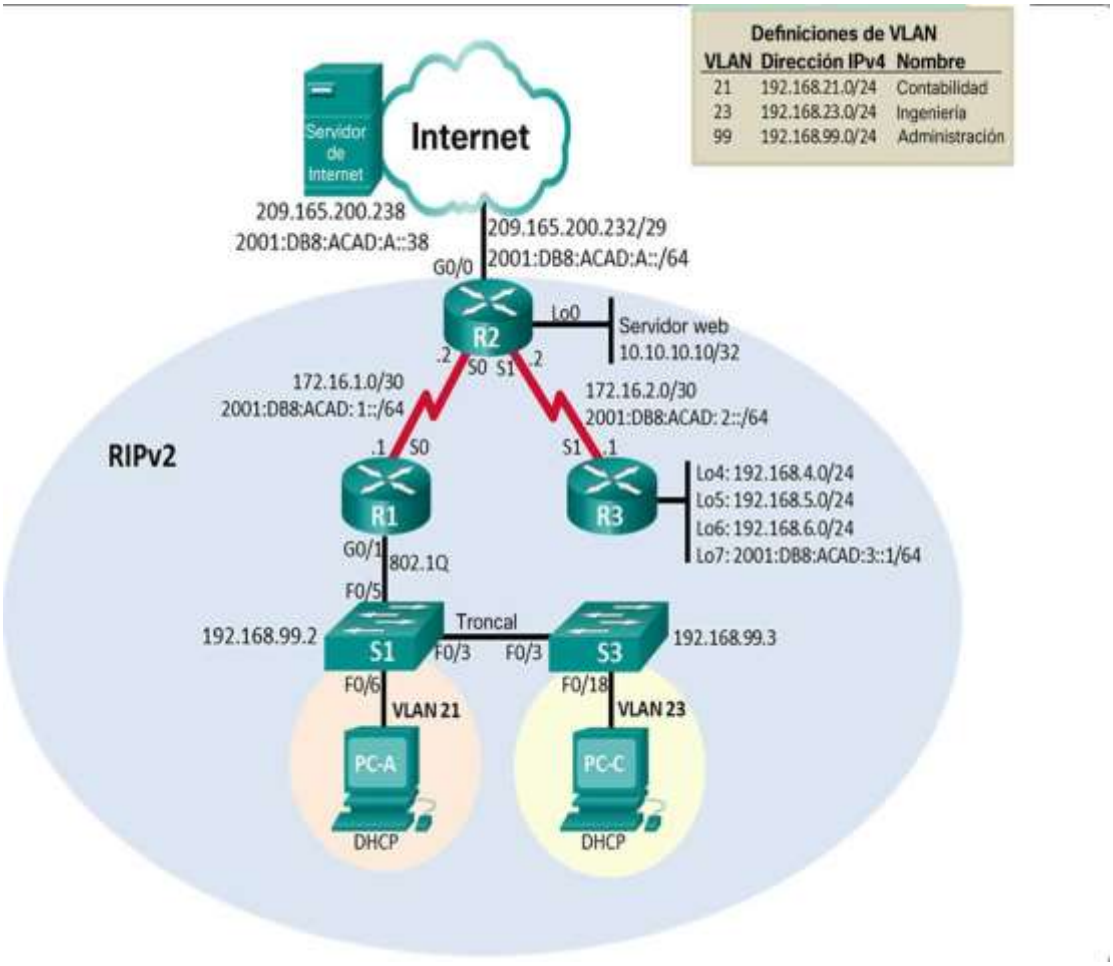

Figura 1. escenario 1

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.

Primero se inicializan los dispositivos, se ejecuta la eliminación de las configuraciones de Vlan anteriores, se reinician y se vuelven a cargar los dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Introducimos el siguiente código Router# erase startup-config
Volver a cargar todos los routers	Introducimos el código: Router# reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para eliminar introducimos Router# erase startup-config delete vlan.dat
Volver a cargar ambos switches	Router#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Para verificar introducimos Router#show flash

Tabla 1. Configuración básica de routers y switches

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):

Se realiza la configuración grafica mediante interfaz de lo que es el servidor de internet donde le asignamos la dirección ipv4, la dirección ipv6 mascara de subred, Gateway predeterminado y la DNS.

Elemento o tarea de configuración	Especificación
Dirección IPv4	Se ingresa al server en la pestaña desktop y ubicamos la IP configuración buscamos la casilla del IPV4 e introducimos la ruta 209.165.200.238
Máscara de subred para IPv4	Se ingresa al server en la pestaña desktop y ubicamos la IP configuración buscamos la casilla de subred Mask e introducimos la ruta 255.255.255.248
Gateway predeterminado	Se ingresa al server en la pestaña desktop y ubicamos la IP configuración buscamos la casilla del Default Gateway e introducimos la ruta 209.165.200.233
Dirección IPv6/subred	Se ingresa al server en la pestaña desktop y ubicamos la IP configuración buscamos la casilla del IPV6 Address e introducimos la ruta 2001:db8:acad:a::38/64
Gateway predeterminado IPv6	Se ingresa al server en la pestaña desktop y ubicamos la IP configuración buscamos la casilla de Gateway de IPV6 e introducimos la ruta 2001:db8:acad:a::1

Tabla 2 configuración del servidor de internet según la topología

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:

Se configuran los routers con su información básica, se les asigna un nombre para diferenciarlos, se configura el acceso a consola y el acceso a telnet y determinamos las contraseñas para consola y acceso privilegiado para cuando ingrese por consola haya algún tipo de seguridad de igual forma se establece la dirección ipv4 la direccion ipv6, se configura la ruta predeterminada, se enciende la frecuencia de reloj y se activan las interfaces

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Router# config term Router(config)# no ip domain-lookup
Nombre del router	Se ingresa el código: Router(config)# hotsnameR1
Contraseña de exec privilegiado cifrada	Se ingresa el código: R1(config)# enable secret class
Contraseña de acceso a la consola	Se ingresa el código: R1(config)# line console 0 R1(config-line)# password cisco R1(config-line)# login
Contraseña de acceso Telnet	Se ingresa el código: R1(config-line)# Line vty 0 15 R1(config-line)# Password cisco R1(config-line)# login
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: R1(config-line)# service password -encryption
Mensaje MOTD	Se ingresa el código: R1(config)# Banner motd # unauthorized Access is prohibit!#.

Interfaz S0/0/0	Establezca la descripción se hace con este código: R1(config)# int s0/0/0 R1(config-if)# description connection to R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones es: R1(config-if)#ip address 172.16.1.1255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones es: R1(config-if)# ipv6 address 2001:db8:acad:1::1/64 Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config-if)# clock rate 128000 R1(config-if)# no shutdown R1(config-if)# exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 El código es: R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 El código es: R1(config)# ipv6 route ::/0 s0/0/0

Tabla 3 Configuración básica Router 1

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Se configuran los routers con su información básica, se les asigna un nombre para diferenciarlos, se configura el acceso a consola y el acceso a telnet y determinamos las contraseñas para consola y acceso privilegiado para cuando ingrese por consola haya algún tipo de seguridad de igual forma se establece la dirección ipv4 la direccion ipv6, se configura la ruta predeterminada, se enciende la frecuencia de reloj y se activan las interfaces

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Router# config term Router(config)# no ip domain-lookup
Nombre del router	Se ingresa el código: Router(config)# hotsname R2
Contraseña de exec privilegiado cifrada	Se ingresa el código: R2(config)# enable secret class
Contraseña de acceso a la consola	Se ingresa el código: R2(config)# line console 0 R2(config-line)# password cisco R2(config-line)# login
Contraseña de acceso Telnet	Se ingresa el código: R2(config-line)# line vty 0 15 R2(config-line)# password cisco R2(config-line)# login
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: R2(config-line)# service password-encryption
Habilitar el servidor HTTP	Se ingresa el código: R2(config)# ip http server
Mensaje MOTD	Se ingresa el código: R2(config-line)# banner motd #unauthorized Access is prohibit!#
	Establezca la descripción

Interfaz S0/0/0	R2(config)# int s0/0/0 R2(config-if)# descrption connection to R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config-if)# ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config-if)# ipv6 address 2001: cb8: acad:1::2/64 R2(config-if)# no shutdown R2(config-if)# exit
Interfaz S0/0/1	Establecer la descripción R2(config)# int s0/0/1 R2(config-if)# description connection to R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)# ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)# ipv6 address 2001:bd8: acad:2::2/64 Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config-if)# clock rate 128000 R2(config-if)# no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config)# Int fa 0/0 R2(config-if)# Description connection to R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)# Ip address 209.165.200.233

	255.255.255.248 Establezca la dirección IPv6. R2(config-if)# Ipv6 address 2001:db8: acad:a::1/64 Utilizar la primera dirección disponible en la subred. Activar la interfaz R2 (config-if) # no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config-if)# Int loopback 0 changed state to up R2(config-if)# Int loopback 0 changed R2(config-if)# Ip address 10.10.10.10 255.255.255.255 R2(config-if)# Description connection simuled web server R2(config-if)# exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)# Ip route 0.0.0.0 0.0.0.0 fa 0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)# Ip route ::/0 fa0/0

Tabla 4 Configuración básica Router 2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Se configuran los routers con su información básica, se les asigna un nombre para diferenciarlos, se configura el acceso a consola y el acceso a telnet y determinamos las contraseñas para consola y acceso privilegiado para cuando ingrese por consola haya

algún tipo de seguridad de igual forma se establece la dirección ipv4 la direccion ipv6, se configura la ruta predeterminada, se enciende la frecuencia de reloj y se activan las interfaces

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Router# Conf term
Nombre del router	Se ingresa el código: Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	Se ingresa el código: R3(config)# enable secret class
Contraseña de acceso a la consola	Se ingresa el código: R3(config)# line console 0 R3(config-line)# password cisco R3(config-line)# login
Contraseña de acceso Telnet	Se ingresa el código: R3(config-line)# line vty 0 15 R3(config-line)# password cisco R3(config-line)# login
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: R3(config-line)# Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. Se ingresa el código: R3(config)# banner motd #unauthorized Access is prohibit!#
	Establecer la descripción R3(config)# Int 0/0/1 R3(config-if)# Description connection to R3

Interfaz S0/0/1	Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config-if)# Ip address 172.16.2.1 255.255.255.255 Establezca la dirección IPv6. R3(config-if)# Ipv6 address 2001:db8:acad:2::1/64 Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config-if)# no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# Int loopback 4 R3(config-if)# Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# Int loopback 5 R3(config-if)# Ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)# Int loopback 6 R3(config-if)# Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)# Int loopback 7 R3(config-if)# Ip address 2001:db8:acad:3::1/64 R3(config-if)# Exit R3(config)# Ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)# Ipv6 route ::/0 s0/0/1 R3(config)# exit

Tabla 5 Configuración básica Router 3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se configuran los switch con su información básica, se les asigna un nombre para diferenciarlos, se configura el acceso a consola y el acceso a telnet y determinamos las contraseñas para consola y acceso privilegiado para cuando ingrese por consola haya algún tipo de seguridad de igual forma se establece la dirección ipv4 la direccion ipv6, se configura la ruta predeterminada, se enciende la frecuencia de reloj y se activan las interfaces

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Switch# conf term
Nombre del switch	Se ingresa el código: Switch# hostname S1
Contraseña de exec privilegiado cifrada	Se ingresa el código: S1(config)# enable secret class
Contraseña de acceso a la consola	Se ingresa el código: S1(config)# line console 0 S1(config-line)# Password cisco S1(config-line)# login
Contraseña de acceso Telnet	Se ingresa el código: S1(config-line)# line vty 0 15 S1(config-line)# password cisco S1(config-line)# login
Cifrar las contraseñas de texto no cifrado	Se ingresa el código: S1(config-line)# Service password-encryption
	Se prohíbe el acceso no autorizado.

Mensaje MOTD	Se ingresa el código: S1(config)# banner motd #unauthorized Access is prohibit!#

Tabla 6 configuración Switche 1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Se configuran los switch con su información básica, se les asigna un nombre para diferenciarlos, se configura el acceso a consola y el acceso a telnet y determinamos las contraseñas para consola y acceso privilegiado para cuando ingrese por consola haya algún tipo de seguridad de igual forma se establece la dirección ipv4 la direccion ipv6, se configura la ruta predeterminada, se enciende la frecuencia de reloj y se activan las interfaces

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ingresa el código: Switch# conf term
Nombre del switch	Se ingresa el código: Switch(config)# hostname S3
Contraseña de exec privilegiado cifrada	Se ingresa el código: S3(config)# enable secret class
Contraseña de acceso a la consola	Se ingresa el código: S3(config)# line console 0 S3(config-line)# password cisco S3(config-line)# login
Contraseña de acceso Telnet	Se ingresa el código: S3(config-line)# Line vty 0 15 S3(config-line)# Password cisco S3(config-line)# Login

Cifrar las contraseñas de texto no cifrado	Se ingresa el código: S3(config-line)# Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. Se ingresa el código: S3(config)# banner motd #unauthorized Access is prohibit!#

Tabla 7 Configuración Switche 3

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:

Se realizan los diferentes Pruebas de conectividad pings para determinar si hicimos la configuración de acuerdo a lo que nos piden, de las conexiones de los cuales son éxitos y responden de una manera excelente

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	SI
R2	R3, S0/0/1	172.16.2.1	SI
PC de Internet	Gateway predeterminado	209.165.200.233	SI

Tabla 8 verificación de la red

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

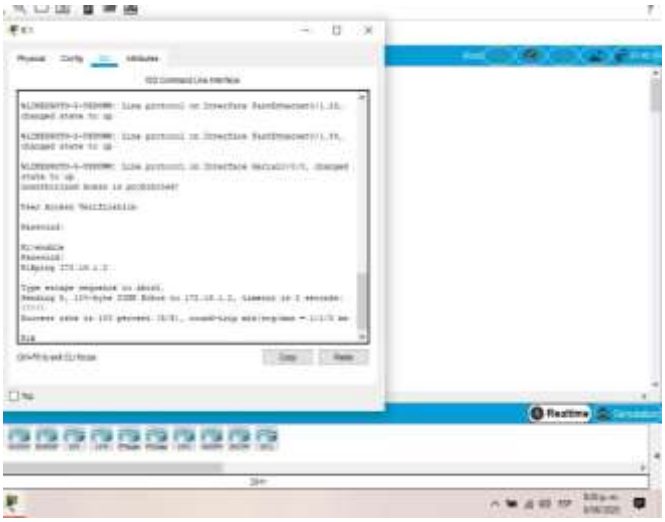

Figura 2 verificación de ping R1 a R2

Figura 3 verificación de ping R2 a R3

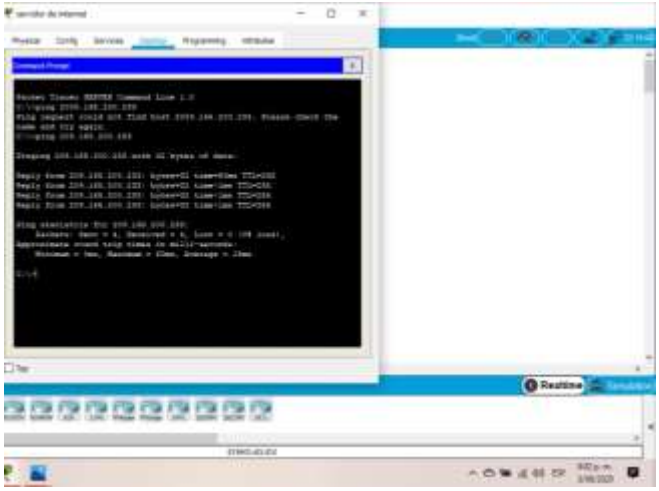

Figura 4 verificación de ping pc de internet

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

Como parte inicial definimos la Vlan que sin la 21 d econtabilidad la 23 de ingeniería y la 99 de administración posteriormente definimos la vlan 1 como la vlan nativa y configuramos la asignacion de direccionamiento ip y le gateway predeterminado seguidamente forzamos la troncal de la interfaz de igual forma configuramos el resto de puertos como puertos de acceso y por ultimo apagamos todos los puertos de acceso que no se están utilizando

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)# Vlan 21 S1(config-vlan)# Name accounting S1(config)# Vlan 23 S1(config-vlan)# Name engineering S1(config)# Vlan 99 S1(config-vlan)# Name administration S1(config-vlan)# exit
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 Ingresamos el código: S1(config)# Int vlan 99 S1(config-if)# Ip address 192.168.99.2 255.255.255.0

	S1(config-if)# no shutdown S1(config-if)# exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ingresamos el código: S1(config)# ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Ingresamos el código: S1(config)# Int f 0/3 S1(config-if)# Switchport mode trunk S1(config-if)# Switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa Ingresamos el código: S1(config)# Int f 0/5 S1(config-if)# Switchport mode trunk S1(config-if)# Switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Ingresamos el código: S1(config-if)# Int range f 0/1-2, f 0/4, f 0/7-24, g 0/1-2 S1(config-if-range)# no shutdown
Asignar F0/6 a la VLAN 21	Ingresamos el código: S1(config-if-range)# Int f 0/6 S1(config-if)# Switchport mode Access vlan 21
Apagar todos los puertos sin usar	Ingresamos el código:

	S1(config-if)# Inte range f 0/1-2, f 0/4, f 0/7-24, g 0/1-2 S1(config-if-range)# no shutdown

Tabla 9 Seguridad de switches 1 de VLAN

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Como parte inicial definimos la Vlan que sin la 21 d econtabilidad la 23 de ingeniería y la 99 de administración posteriormente definimos la vlan 1 como la vlan nativa y configuramos la asignacion de direccionamiento ip y le gateway predeterminado seguidamente forzamos la troncal de la interfaz de igual forma configuramos el resto de puertos como puertos de acceso y por ultimo apagamos todos los puertos de acceso que no se están utilizando

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#Vlan 21 S3(config-vlan)#Name accounting S3(config)#Vlan 23 S3(config-vlan)#name engineering S3(config)#Vlan 99 S3(config-vlan)#name administration exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#Ip address 192.168.99.3 255.255.255.0 S3(config)#No shutdown
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.

	Ingresamos el código: S3(config)#Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Ingresamos el código: S3(config)#Int f 0/3 S3(config-if)#Switchport mode trunk S3(config-if)#Switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Ingresamos el código: S3(config-if)#Int range f 0/1-2, f 0/4-24 , f 0/7-24, g 0/1-2
Asignar F0/18 a la VLAN 21	Ingresamos el código: S3(config)#Int f 0/18 S3(config-if)#Switchport mode Access vlan 23
Apagar todos los puertos sin usar	Ingresamos el código: S3(config-if)#Inte range f 0/1-2, f 0/4-17, f 0/19-24, g 0/1-2 S3(config-if-orange)# No shutdown

Tabla 10 Seguridad de switches 3 de VLAN

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

En este caso son spide realizar La configuración de la subinterfaz de la vlan 21 para ellos seleccionamos la dirección ip que vamos a utilizar con su respectiva mascara de subred, seleccionamos un descripción de la vlan y procedemos a ejecutar el encapsulamiento y por ultimo activamos la interface

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Introducimos el código: R1# conf term R1(config)# Int fa /1.21 R1(config-if)# Drescription vlan 21 Asignar la primera dirección disponible a esta interfaz Introducimos el código: R1(config-subif)# Encaptulation dot1q 21 R1(config-subif)# Ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Introducimos el código: R1(config-subif)# Int fa /1.23 R1(config-subif)# Drescription vlan 23 Asignar la primera dirección disponible a esta interfaz Introducimos el código: R1(config-subif)# Encaptulation dot1q 23 R1(config-subif)# Ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Introducimos el código: R1(config-subif)# Int fa /1.99 R1(config-subif)# Drescription vlan 99 Asignar la primera dirección disponible a esta

	interfaz Introducimos el código: R1(config-subif)# Encaptulation dot1q 99 R1(config-subif)# Ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	Introducimos el código: R1(config-subif)# Int fa /1.99 R1(config-subif)# Drescription vlan 99 R1(config-subif)# Int fa 0/1 R1(config-if)# No shutdown

Tabla 11 Configuración del Router de la interfaz

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:

Vamos a verificar la conectividad de la red con ping de lo cual los resultados son satisfactorios

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

Tabla 12 Verificación la conectividad de la red

Figura 5 resultado de ping en S1 vlan 99

Figura 6 resultado ping S3 vlan 99

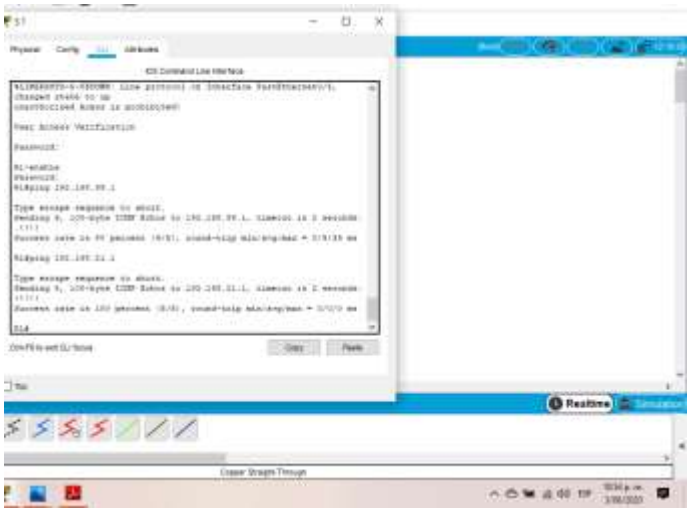

Figura 7 resultado ping S1 vlan 21

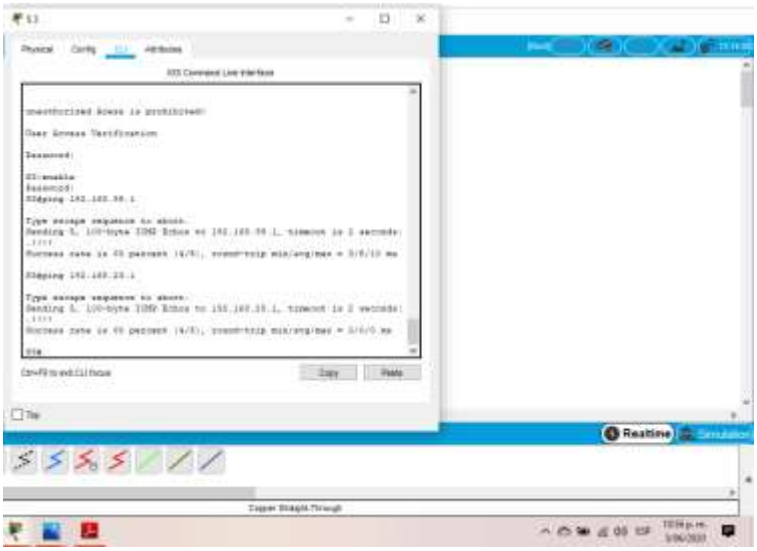

Figura 8 resultado ping S3 vlan 23

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Principalmente asignamos las redes conectadas directamente, luego establecemos establecemos todas las interfaces como pasivas y desactivamos la sumatización automática

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Introducimos el código: R1(config)# router rip R1(config-router)# Versión 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. Introducimos el código: R1(config-router)# Do show ip route connected R1(config-router)# Network 172.16.1.0 R1(config-router)# Network 172.168.21.0

	R1(config-router)# Network 172.168.23.0 R1(config-router)# Network 172.168.99.0
Establecer todas las interfaces LAN como pasivas	Introducimos el código: R1(config-router)# Pasive interface fa 0/1.21 R1(config-router)# Pasive interface fa 0/1.23 R1(config-router)# Pasive interface fa 0/1.29
Desactive la sumarización automática	Introducimos el código: R1(config-router)# No auto-summary

Tabla 13 Configurar el protocolo de routing 1, dinámico RIPv2

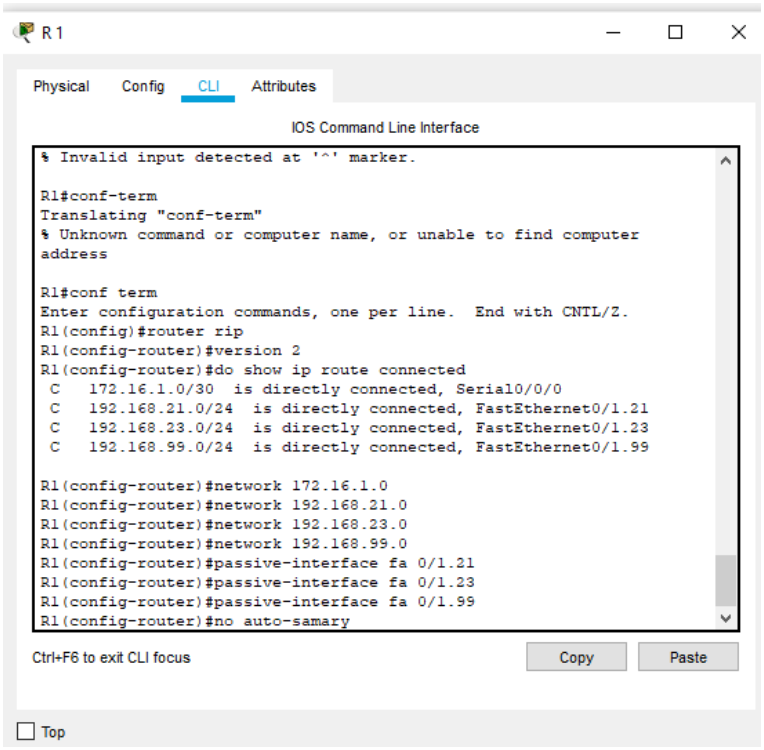

Figura 9 resultados de do show ip route connected R1

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Principalmente asignamos las redes conectadas directamente, luego establecemos establecemos todas las interfaces como pasivas y desactivamos la sumatización automática

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Introducimos el código: R2(config)# router rip R2(config)# Versión 2
Anunciar las redes conectadas directamente	Introducimos el código: Do show ip route connected R2(config-router)# Network 10.10.10.10 R2(config-router)# Network 172.16.1.0 R2(config-router)# Network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	Introducimos el código: R2(config-router)# Pasive interface loopback 0
Desactive la sumarización automática.	Introducimos el código: R2(config-router)# No auto-summary

Tabla 14 Configurar el protocolo de routing 2, dinámico RIPv2

Figura 10 resultados de do show ip route connected R2

Paso 3: Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Principalmente asignamos las redes conectadas directamente, luego establecemos establecemos todas las interfaces como pasivas y desactivamos la sumatización automática

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Introducimos el código: R3(config)# router rip R3(config)# Versión 2
Anunciar redes IPv4 conectadas directamente	Introducimos el código: R3(config-router)# Do show ip route connected R3(config-router)# Network 172.16.2.0 R3(config-router)# Network 172.168.4.0 R3(config-router)# Network 172.168.5.0 Network 172.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Introducimos el código: R3(config-router)# Pasive interface loopback 4 R3(config-router)# Pasive interface loopback 5 R3(config-router)# Pasive interface loopback 6
Desactive la sumarización automática.	Introducimos el código: R3(config-router)# No auto-summary R3(config-router)# end

Tabla 15 Configurar el protocolo de routing 3, dinámico RIPv2

Figura 11 resultados de do show ip route connected 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:

Iniciamos con el comando show ip protocols el cual nos muestra la ID del proceso,el comando show ip route rip nos muestra las rutas RIP y el comando show run nos muestra la sección de RIP

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

Tabla 16 Verificar la información de RIP

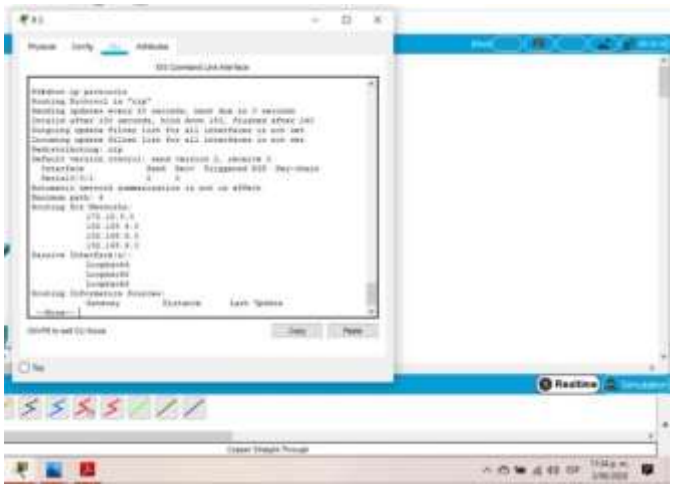

Figura 12 show ip protocols

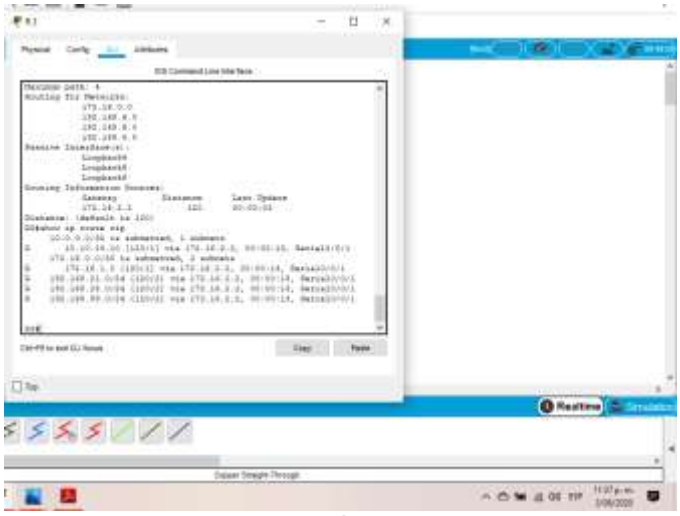

Figura 13 verificación ip route rip en R1

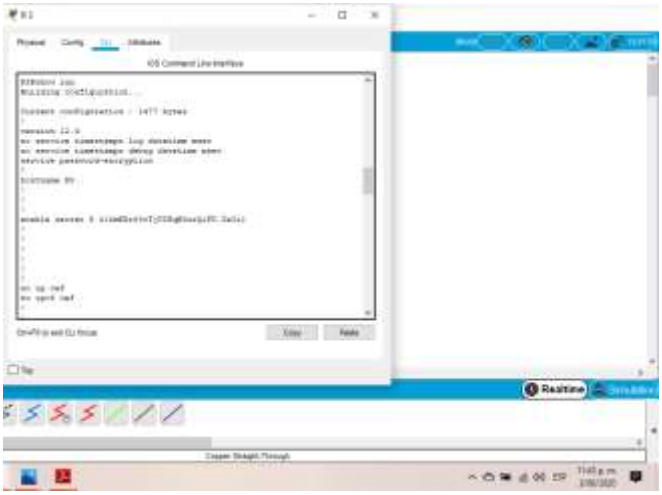

Figura 14 verificación show run en R1

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:

Primeramente reservamos las primeras 20 direcciones creamos el pool DHCP para la vlan donde establecemos el geteway predeterminado

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)# Ip dhcp excluded-address 192.168.21.1 192.168.1.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)# Ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado Introducimos le siguiente código: R1(config)# Ip dhcp pool ACCT R1(dhcp-config)# Networ 192.168.21.0 255.255.255.0 R1(dhcp-config)# Default-router 192.168.21.1 R1(dhcp-config)# Dns-server 10.10.10.10 R1(dhcp-config)# Domain-name ccna-san.com
	Nombre: ENGNR 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	Introducimos le siguiente código: R1(dhcp-config)# Ip dhcp pool ENGNR R1(dhcp-config)# Networ 192.168.23.0 255.255.255.0 R1(dhcp-config)# Default-router 192.168.23.1 R1(dhcp-config)# Dns-server 10.10.10.10 R1(dhcp-config)# Domain-name ccna-san.com

Tabla 17 implementar DHCP y NAT para IPv4 en el Router 1

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)# Username wubuser privilege is secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)# Ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# Ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237 R2(config)# Ip inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	Introducimos le siguiente código: R2(config)# Int fa 0/0 R2(config-if)# Ip nat autside R2(config-if)# Int s 0/0/0

	R2(config-if)# Ip nat autside R2(config-if)# Int s 0/0/1 R2(config-if)# Ip nat autside R2(config-if)# Exit
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 Introducimos le siguiente código: R2(config)# access-list 1 permit 192.168.21.0 0.0.0.255 R2(config-if)# access-list 1 permit 192.168.23.0 0.0.0.255 R2(config-if)# access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236 R2(config-if)# Ip nat pool internet 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config-if)# Ip nat inside sourse-list 1 pool internet

Tabla 18 configurar la 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.

Configuramos en el R1 para que no suministre automatíceme la dirección ip para los dos dispositivos para el pc a y pc c y hay tenemos la prueba que los equipos toman automáticamente la dirección ip del router

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	192.168.22.21 255.255.255.0 192.168.21.1 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	192.168.23.21 255.255.255.0 192.168.23.1 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.	Ping 192.168.23.21
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	http://209.165.200.237

Tabla 19 Verificar el protocolo DHCP y la NAT estática

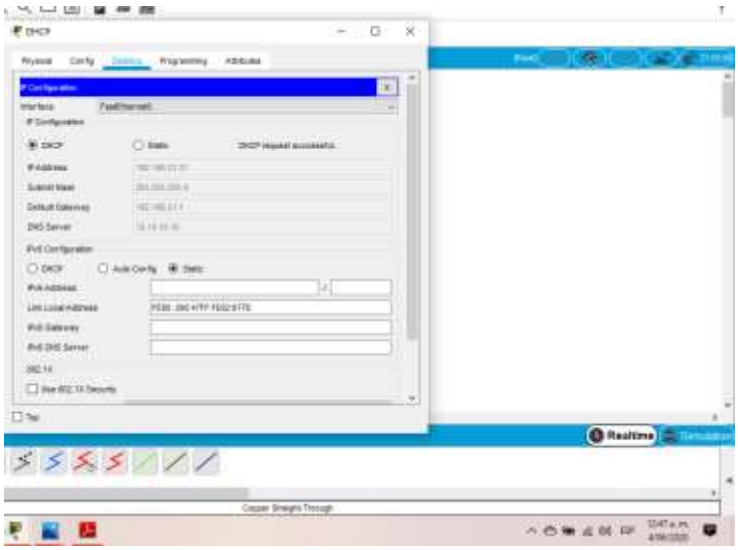

Figura 15 verificación protocolo DHCP pc-a

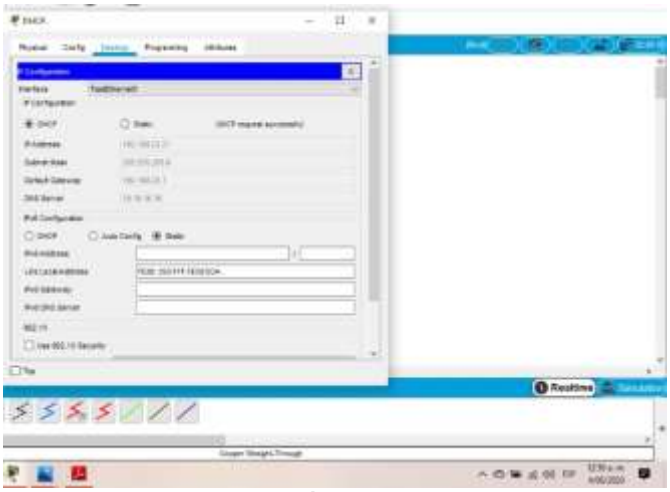

Figura 16 verificación protocolo DHCP pc-c

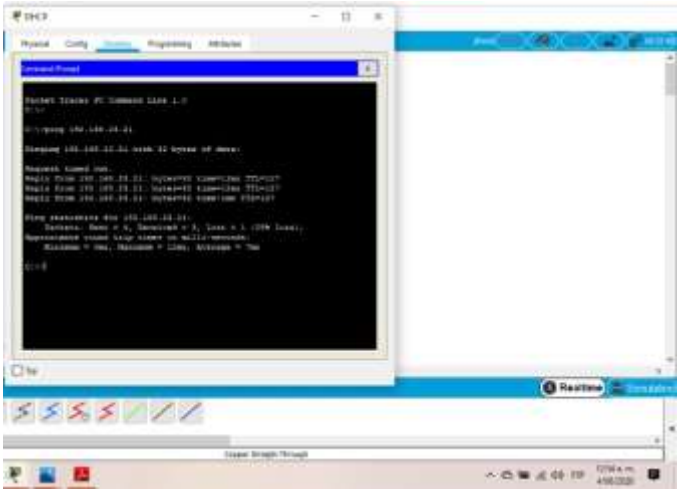

Figura 17 resultados de ping pc-a a pc-c

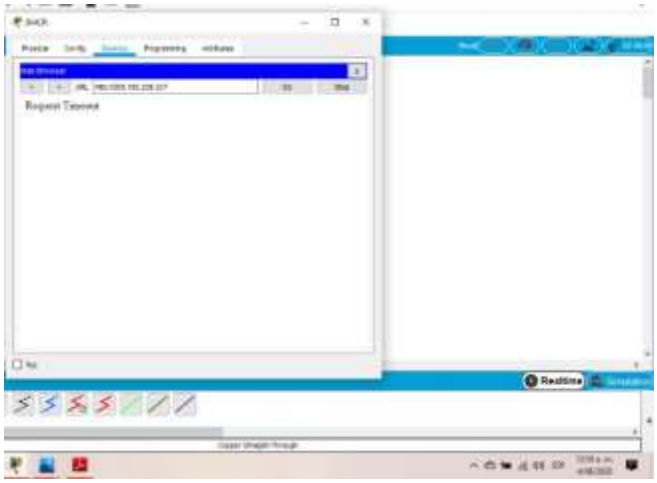

Figura 18 navegador web

PARTE 6: CONFIGURAR NTP

Nos solicita que ajustemos la fecha y la hora en R2 con el comando Clook set ajustamos la hora e ingresamos la fecha solicitada y establecemos el router como maestro en nttp en estrato 5

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#Clook set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R1(config)# Ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2 R1(config-if)# Ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config-if)# Ntp update-calendar R1(config-if)# end
Verifique la configuración de NTP en R1.	R1#Show ntp associations

Tabla 20 Configurar NTP

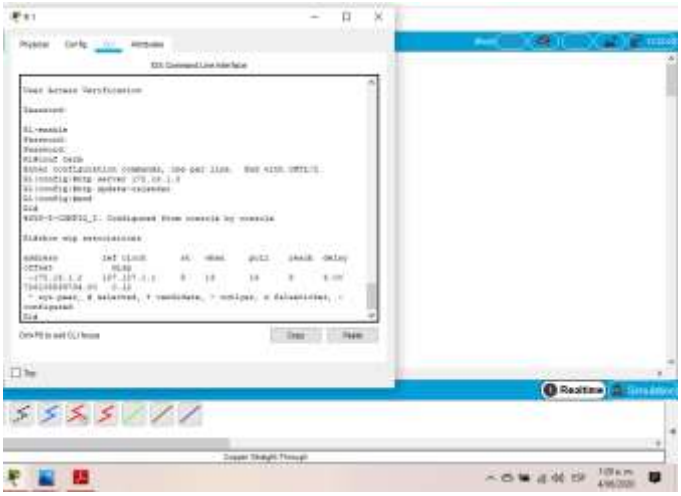

Figura 19 verificacion show ntp association en R1

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL

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

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 R3(config)# ip Access-list standard ADMIN- MGT R3(config)# permit host 172.16.1.1 R3(config)# exit
Aplicar la ACL con nombre a las líneas VTY	R3 (config)# Line vty 0 15 R3 (config-line)# access-class ADMIN-MGT
Permitir acceso por Telnet a las líneas de VTY	R3(config-line)# Trasnport input telnet R3(config-line)#end
Verificar que la ACL funcione como se espera	R3(config)# telnet 172.16.1.2

Tabla 21 Configuración y verificación las listas de control de acceso (ACL)

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

Finalmente hacemos la verificación del comando ping del pc a al pc a viendo que son correctos y de internet pc al servidor web en este caso vemos que le comando ping funciona y que al intentar acceder del pc de internet al servidor web vemos que nos carga correctamente la interfaz

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#Show access-list *Figura 19*
Restablecer los contadores de una lista de acceso	R2#Clear ip Access-list countrs *Figura 2*

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#Show ip interface *Figura 21*
¿Con qué comando se muestran las traducciones NAT?	PC-A Ping: 209.165.200.238 *Figura 22* PC-C Ping: 209.165.200.238 *Figura 23* PC-C http://209.163.200.238 *Figura 24* PC-A http://209.165.200.238 *Figura 25* R2#Show ip nat translations *Figura 26*
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#Clear ip nat trnslations* *Figura 27*

Tabla 22 *comando CLI*

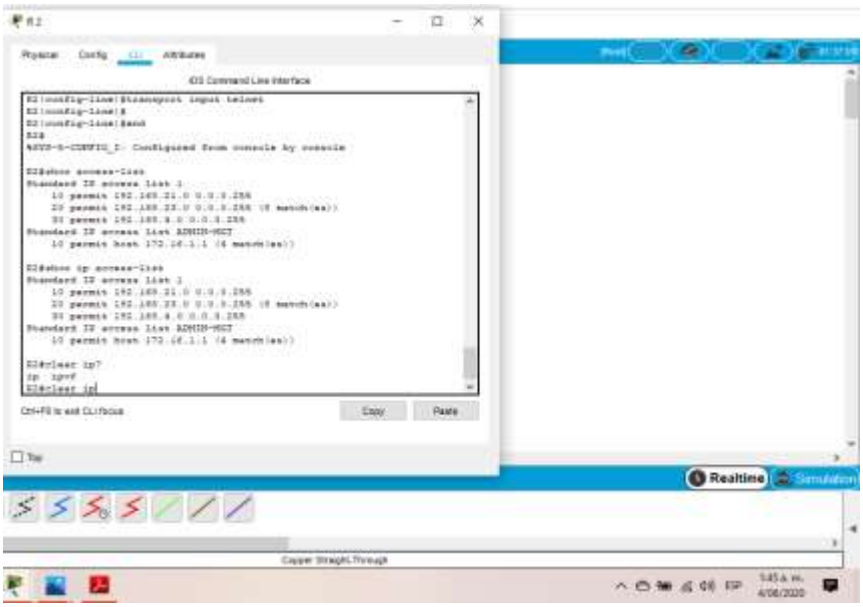

figura 20 verificación de show access-list R2

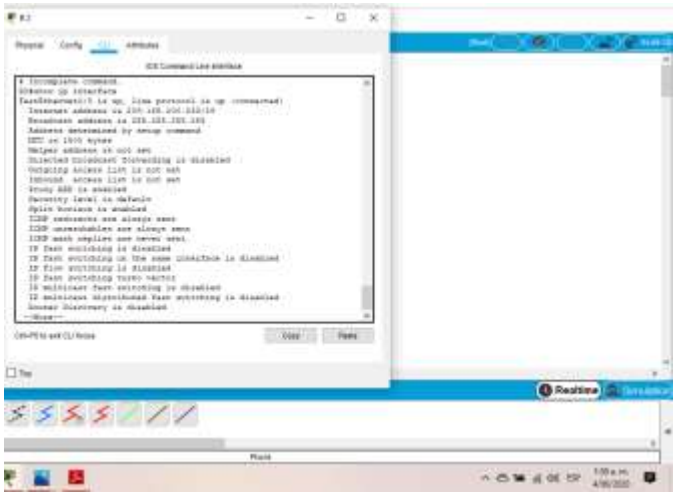

figura 21 verificación show ip interface

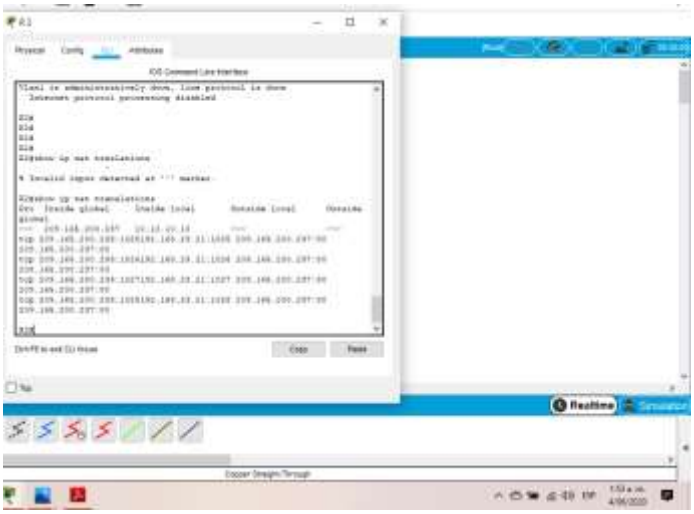

Figura 22 show ip nat trnslations

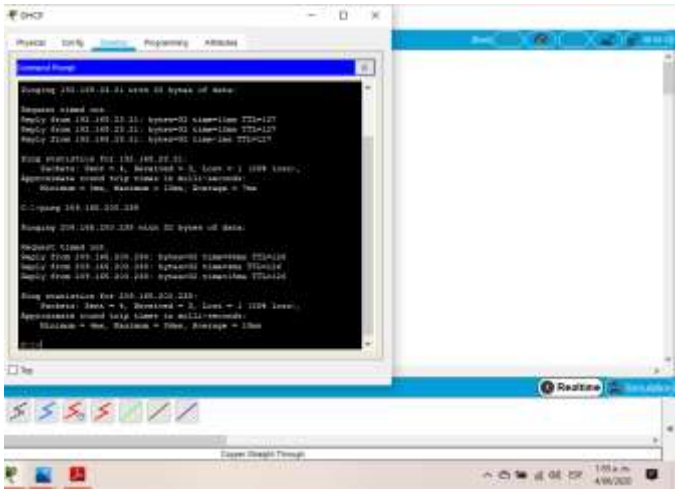

Figura 23 verificación de DHCP ping a pc-a

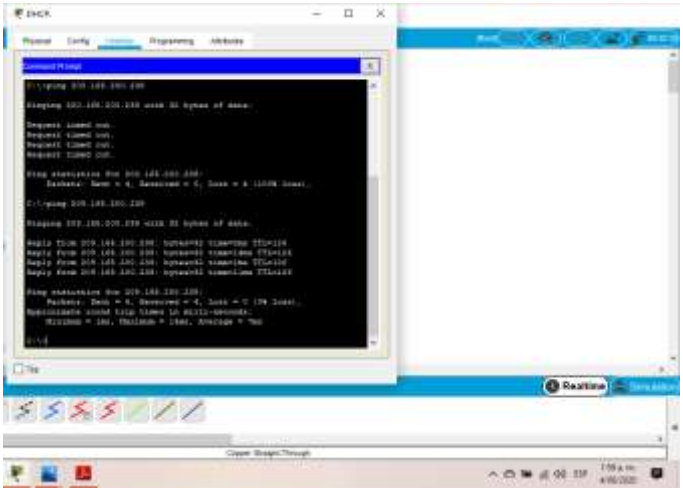

Figura 24 verificación de DHCP ping a pc-c

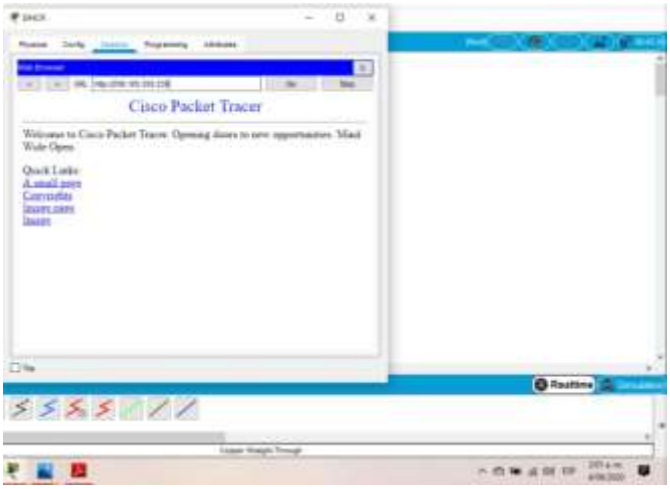

Figura 25 verificacion DHCP Traduccion pc-c

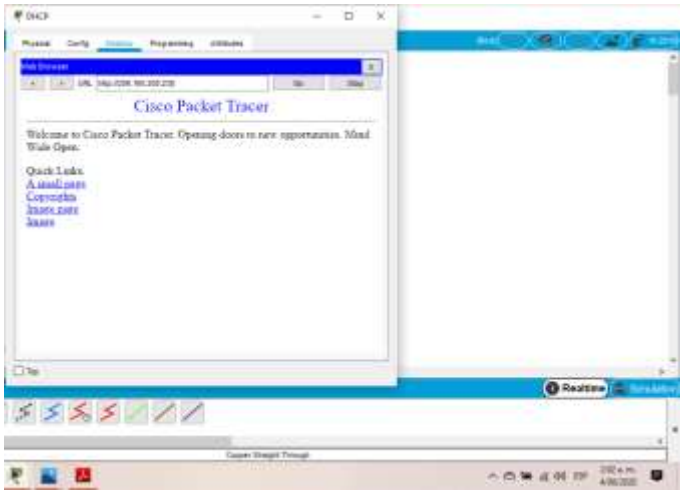

Figura 26 verificacion DHCP Traduccion pc-a

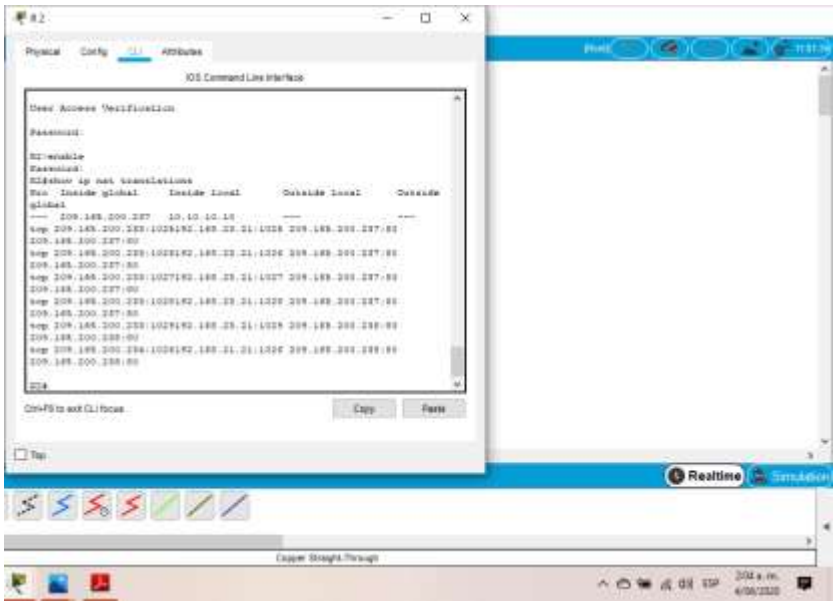

Figura 27 verificación Show in nat translations

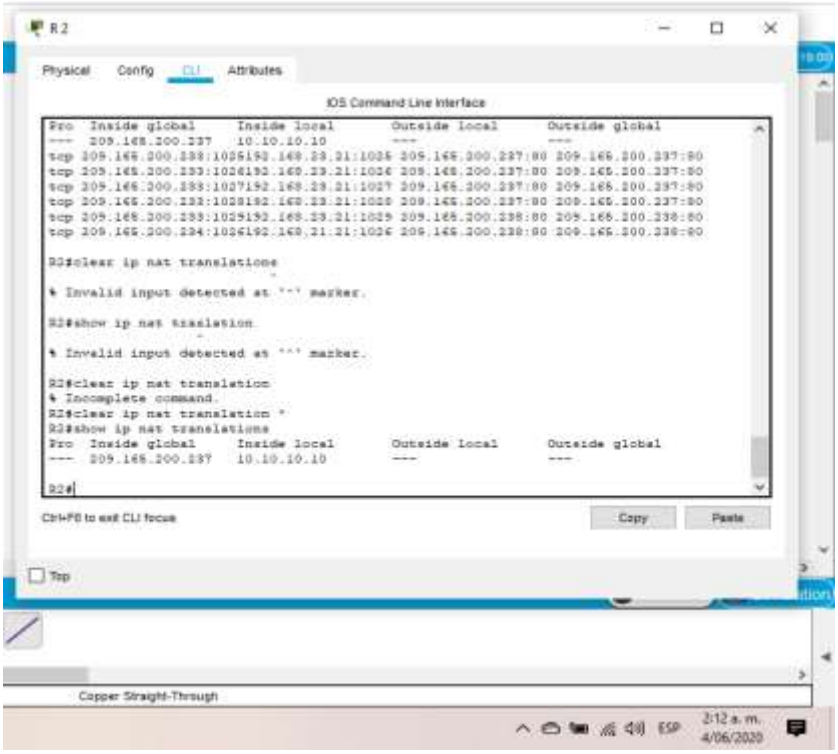

Figura 28 verificación claer ip nat translations

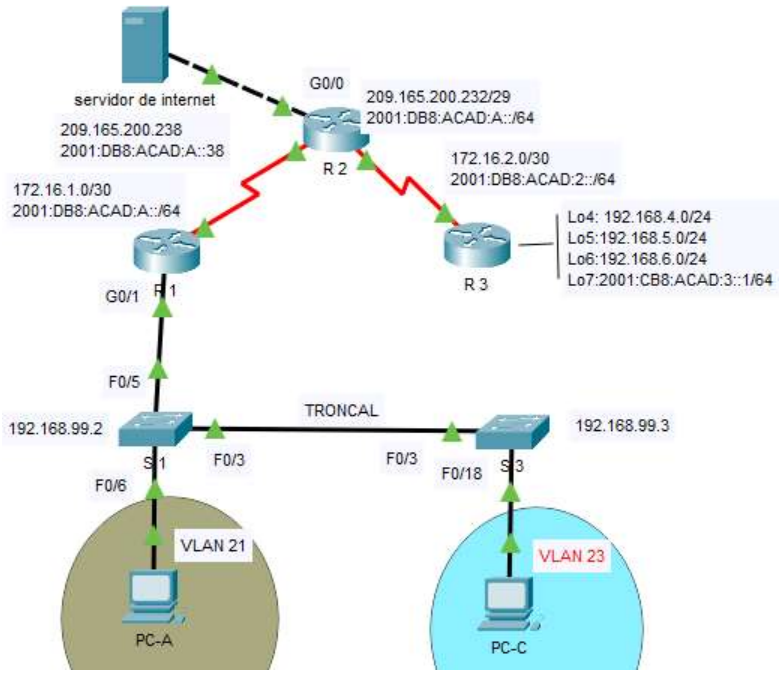

FIGURA 29. Final de la topología escenario 1

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

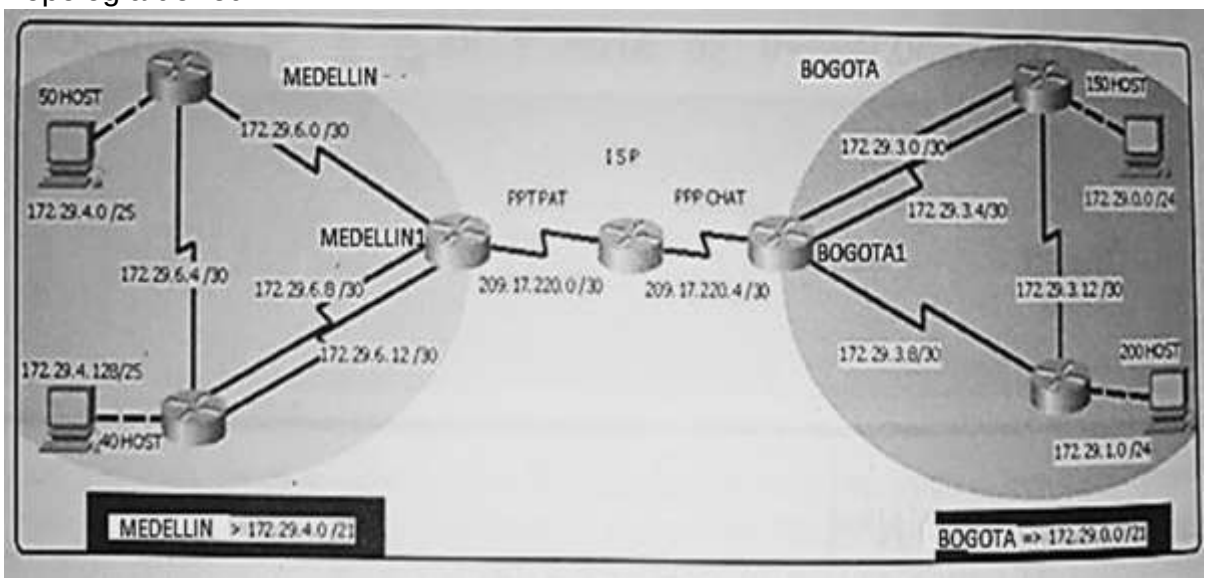

Figura 30. Escenario 2

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).

Habilitamos el terminal de configuraciones agregamos el nombre del dispositivo establecemos la contraseña exel privilegiado nos logueamos y finalmente hacemos la asignación de las contraseñas luego creamos un banner para prohibir el acceso no autorizado

Dispositivo	Configuración Básica
Bogotá 1	Router#conf term Router (config)# ip domian-lookup Router (config)# hostname BOGOTA 1 BOGOTA1(config)# service password-encryption BOGOTA1(config)# enable secret class BOGOTA1(config)# banner motd "Access restringido" BOGOTA1(config)# line console 0 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#line vty 0 15 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login
Bogotá 2	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname BOGOTA 2 BOGOTA2(config)# service password-encryption BOGOTA2(config)# enable secret class BOGOTA2(config)# banner motd "Access restringido" BOGOTA2(config)# line console 0 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login BOGOTA2(config-line)#line vty 0 15 BOGOTA2(config-line)#password cisco BOGOTA2(config-line)#login
Bogotá 3	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname BOGOTA3 BOGOTA3(config)# service password-encryption BOGOTA3(config)# enable secret class BOGOTA3(config)# banner motd "Access restringido" BOGOTA3(config)# line console 0

	BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login BOGOTA3(config-line)#line vty 0 15 BOGOTA3(config-line)#password cisco BOGOTA3(config-line)#login
Medellín 1	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname MEDELLIN1 MEDELLIN1(config)# service password-encryption MEDELLIN1(config)# enable secret class MEDELLIN1(config)# banner motd "Access restringido" MEDELLIN1(config)# line console 0 MEDELLIN1(config-line)#password cisco MEDELLIN1 (config-line)#login MEDELLIN1 (config-line)#line vty 0 15 MEDELLIN1 (config-line)#password cisco MEDELLIN1 (config-line)#login
Medellín 2	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname MEDELLIN2 MEDELLIN2(config)# service password-encryption MEDELLIN2(config)# enable secret class MEDELLIN2(config)# banner motd "Access restringido" MEDELLIN2(config)# line console 0 MEDELLIN2(config-line)#password cisco MEDELLIN2 (config-line)#login MEDELLIN2 (config-line)#line vty 0 15 MEDELLIN2 (config-line)#password cisco MEDELLIN2 (config-line)#login
	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname MEDELLIN3 MEDELLIN3(config)# service password-encryption MEDELLIN3(config)# enable secret class MEDELLIN3(config)# banner motd "Access restringido"

Medellín 3	MEDELLIN3(config)# line console 0 MEDELLIN3(config-line)#password cisco MEDELLIN3 (config-line)#login MEDELLIN3 (config-line)#line vty 0 15 MEDELLIN3 (config-line)#password cisco MEDELLIN3 (config-line)#login
ISP	Router:enable Router:conf term Router (config)# ip domian-lookup Router (config)# hostname ISP ISP(config)# service password-encryption ISP(config)# enable secret class ISP(config)# banner motd "Access restringido" ISP(config)# line console 0 ISP(config-line)#password cisco ISP(config-line)#login ISP(config-line)#line vty 0 15 ISP(config-line)#password cisco ISP(config-line)#login

Tabla 23 configuración básica de dispositivos

• Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Realizamos el direccionamiento ip en todos los dispositivos

Dispositivo	Interfaz	Conexión a	Dirección IP	Máscara de Subred	Gateway Predeterminado
Bogotá 1	S0/0/0	ISP	209.17.220.6	255.255.255.252	N.A
	S0/0/1	Bogotá 2	172.29.3.9	255.255.255.252	N.A
	S0/1/0	Bogotá 3	172.29.3.1	255.255.255.252	N.A
	S0/1/1	Bogotá 2	172.29.3.5	255.255.255.252	N.A
Bogotá 2	S0/0/0	Bogotá 1	172.29.3.10	255.255.255.252	N.A
	S0/0/1	Bogotá 3	172.29.3.13	255.255.255.252	N.A
	G0/0	Bogotá - LAN1	172.29.1.1	255.255.255.252	N.A
Bogotá 3	S0/0/0	Bogotá i1	172.29.3.2	255.255.255.252	N.A
	S0/0/1	Bogotá 2	172.29.3.6	255.255.255.252	N.A
	S0/1/0	Bogotá 2	172.29.3.14	255.255.255.252	N.A
	G0/0	Bogotá - LAN2	172.29.0.1	255.255.255.252	N.A
Medellín 1	S0/0/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellín 2	172.29.6.1	255.255.255.252	N.A
	S0/1/0	Medellín 3	172.29.6.9	255.255.255.252	N.A

	S0/1/1	Medellín 3	172.29.6.13	255.255.255.252	N.A
Medellín 2	S0/0/0	Medellín 1	174.29.6.2	255.255.255.252	N.A
	S0/0/1	Medellín 3	172.29.6.5	255.255.255.252	N.A
	G0/0	Medellín - LAN1	172.29.4.1	255.255.255.128	
Medellín 3	S0/0/0	Medellín 2	172.29.6.10	255.255.255.252	N.A
	S0/0/1	Medellín 2	172.29.6.14	255.255.255.252	N.A
	S0/1/0	Bogotá 1	172.29.6.6	255.255.255.252	N.A
	G0/0	Medellín - LAN2	192.168.2.1	255.255.255.128	N.A
ISP	S0/0/0	Bogotá 1	209.17.220.1	255.255.255.252	N.A
	S0/0/1	Bogotá 1	209.17.220.5	255.255.255.252	N.A
PC-3 Bogotá - LAN1	Fa0	Bogotá 2	DHCP	255.255.255.0	172.29.1.1
PC-2 Bogotá - LAN2	Fa0	Bogotá 3	DHCP	255.255.255.0	172.29.0.1
PC-0 Medellín - LAN1	Fa0	Medellín 2	DHCP	255.255.255.128	172.29.4.1
PC-1 Medellín - LAN2	Fa0	Medellín 3	DHCP	255.255.255.128	172.29.4.129

Tabla 24 Especificación para configurar topología de red

Posteriormente configuramos el direccionamiento ipv4, ingresamos a la interfaz le agregamos una descripción configuramos la dirección ip y la mascara de subred se enciende la frecuencia del reloj y activamos la interface

Dispositivo	Configuración Direccionamiento IP
Bogotá 1	BOGOTA1#conf term BOGOTA1(config)#int s0/0/0 BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shutdown BOGOTA1(config)#int s0/0/1 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#clock rate 4000000 BOGOTA1(config-if)#no shutdown BOGOTA1(config)#int s0/1/0 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 4000000 BOGOTA1(config-if)#no shutdown

	BOGOTA1(config)#int s0/1/1 BOGOTA1(config-if)# ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)# clock rate 4000000 BOGOTA1(config-if)# no shutdown
Bogotá 2	BOGOTA2#conf term BOGOTA2(config)#int s0/0/0 BOGOTA2(config-if)# ip address 172.29.3.10 255.255.255.252 BOGOTA2(config-if)# no shutdown BOGOTA2(config)#int s0/0/1 BOGOTA2(config-if)# ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)# clock rate 4000000 BOGOTA2(config-if)# no shutdown BOGOTA2(config)#int g0/0 BOGOTA2(config-if)# ip address 172.29.1.1 255.255.255.252 BOGOTA2(config-if)# no shutdown
Bogotá 3	BOGOTA3#conf term BOGOTA3(config)#int s0/0/0 BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config)# int s0/0/1 BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config)# int s0/1/0 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shutdown BOGOTA3(config)# int g0/0 BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.252 BOGOTA3(config-if)# no shutdown
	MEDELLIN1conf term MEDELLIN1(config)# int s0/0/0 MEDELLIN1 (config-if)# ip address 209.17.220.2 255.255.255.252 MEDELLIN1 (config-if)# no shutdown

Medellín 1	MEDELLIN1(config)# int s0/0/1 MEDELLIN1 (config-if)# ip address 172.29.6.1 255.255.255.252 MEDELLIN1 (config-if)# clock rate 4000000 MEDELLIN1 (config-if)# no shutdown MEDELLIN1(config)# int s0/1/0 MEDELLIN1 (config-if)# ip address 172.29.6.9 255.255.255.252 MEDELLIN1 (config-if)# clock rate 4000000 MEDELLIN1 (config-if)# no shutdown MEDELLIN1(config)# int 0/1/1 MEDELLIN1 (config-if)# ip address 172.29.6.13 255.255.255.252 MEDELLIN1 (config-if)# clock rate 4000000 MEDELLIN1 (config-if)# no shutdown
Medellín 2	MEDELLIN2#conf term MEDELLIN2(config)# int s0/0/0 MEDELLIN2 (config-if)# ip address 174.29.6.2 255.255.255.252 MEDELLIN2 (config-if)# no shutdown MEDELLIN2(config)# int 0/0/1 MEDELLIN2 (config-if)# ip address 172.29.6.5 255.255.255.252 MEDELLIN2 (config-if)# clock rate 4000000 MEDELLIN2 (config-if)# no shutdown MEDELLIN2(config)# int g0/0 MEDELLIN2 (config-if)# ip address 172.29.4.1 255.255.255.128 MEDELLIN2 (config-if)# clock rate 4000000 MEDELLIN2 (config-if)# no shutdown
Medellín 3	MEDELLIN3#conf term MEDELLIN2(config)# int s0/0/0 MEDELLIN3 (config-if)# ip address 172.29.6.10 255.255.255.252 MEDELLIN3 (config-if)# no shutdown MEDELLIN3(config)# int s0/0/1 MEDELLIN3 (config-if)# ip address 172.29.6.14 255.255.255.252 MEDELLIN3 (config-if)# no shutdown MEDELLIN3(config)# int s0/1/0 MEDELLIN3 (config-if)# ip address 172.29.6.6 255.255.255.252

	MEDELLIN3 (config-if)# no shutdown MEDELLIN3(config)# int g0/0 MEDELLIN3 (config-if)# ip address 172.29.4.129 255.255.255.128 MEDELLIN3 (config-if)# no shutdown
ISP	ISP(config)# conf term ISP(config)# int s0/0/0 ISP(config-if)# ip address 209.17.220.1 255.255.255.252 ISP(config-if)# clock rate 4000000 ISP(config-if)# no shutdown ISP(config)# int s0/0/1 ISP(config-if)# ip address 209.17.220.5 255.255.255.252 ISP(config-if)# clock rate 4000000 ISP(config-if)# no shutdown

Tabla 25 configuración direccionamiento IP

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

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

Seguidamente habilitamos el protocolo OSPF ingresamos al router ospf 1 creamos el id verificamos las rutas conectadas y de acuerdo a la cantidad de rutas debemos crear unas rutas en el área 0

Dispositivo	Configuración OSPF en los Routers
Bogotá 1	BOGOTA1#conf term BOGOTA1(config)# router ospf 1 BOGOTA1(config-router) router-id 1.1.1.1 BOGOTA1(config-router) network 172.29.3.0 0.0.0.3 area 0 BOGOTA1(config-router) network 172.29.3.4 0.0.0.3 area 0 BOGOTA1(config-router) network 172.29.3.8 0.0.0.3 area 0 BOGOTA1(config-router) passive-interface s0/0/0
Bogotá 2	BOGOTA2#conf term BOGOTA2(config)# router ospf 1 BOGOTA2(config-router) router-id 2.2.2.2 BOGOTA2(config-router) network 172.29.1.0 0.0.0.255 area 0 BOGOTA2(config-router) network 172.29.3.8 0.0.0.3 area 0

	BOGOTA2(config-router) network 172.29.3.12 0.0.0.3 area 0 BOGOTA2(config-router) passive-interface g0/0
Bogotá 3	BOGOTA3#conf term BOGOTA3(config)# router ospf 1 BOGOTA3(config-router) router-id 3.3.3.3 BOGOTA3(config-router) network 172.29.0.0 0.0.0.255 area 0 BOGOTA3(config-router) network 172.29.3.0 0.0.0.3 area 0 BOGOTA3(config-router) network 172.29.3.4 0.0.0.3 area 0 BOGOTA3(config-router) network 172.29.3.12 0.0.0.3 area 0 BOGOTA3(config-router) passive-interface g0/0
Medellín 1	MEDELLIN1#conf term MEDELLIN1(config)# router ospf 1 MEDELLIN1(config-router) router-id 11.11.11.11 MEDELLIN1(config-router) network 172.29.6.0 0.0.0.3 area 1 MEDELLIN1(config-router) network 172.29.6.8 0.0.0.3 area 1 MEDELLIN1(config-router) network 172.29.6.12 0.0.0.3 area 1 MEDELLIN1(config-router) passive-interface s0/0/0
Medellín 2	MEDELLIN2#conf term MEDELLIN2(config)# router ospf 1 MEDELLIN2(config-router) router-id 22.22.22.22 MEDELLIN2(config-router) network 172.29.4.0 0.0.0.127 area 1 MEDELLIN2(config-router) network 172.29.6.0 0.0.0.3 area 1 MEDELLIN2(config-router) network 172.29.6.4 0.0.0.3 area 1 MEDELLIN2(config-router) passive-interface g0/0
Medellín 3	MEDELLIN3#conf term MEDELLIN1(config)# router ospf 1 MEDELLIN2(config-router) router-id 33.33.33.33 MEDELLIN2(config-router) network 172.29.4.128 0.0.0.127 area 1 MEDELLIN2(config-router) network 172.29.6.4 0.0.0.3 area 1 MEDELLIN2(config-router) network 172.29.6.8 0.0.0.3 area 1 MEDELLIN2(config-router) network 172.29.6.12 0.0.0.3 area 1 MEDELLIN2(config-router) passive-interface g0/0

Tabla 26 configuración OSPF en los Routers

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Dispositivo	Configuración Ruta Distribuida en OSPF
Bogotá 1	BOGOTA1#conf term BOGOTA1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.5 BOGOTA1(config)# router ospf 1 BOGOTA1(config-router)# dafault-information originate
Medellín 1	MEDELLIN1# conf term MEDELLIN1(config)# ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)# router ospf 1 MEDELLIN1(config-router)# dafault-information originate

Tabla 27 configuración de ruta distribuida en 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.

Dispositivo	Configuración Rutas Estáticas Sumarizada a Sedes
ISP	ISP#conf term ISP(config)# ip route 172.29.4.0 255.255.252.0 209.17.220.2 ISP(config)# ip route 172.29.0.0 255.255.252.0 209.17.220.6

Tabla 28 configuración rutas estáticas sumariada a sedes

PARTE 2: TABLA DE ENRUTAMIENTO.

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

Se realiza la verificación de la subred de Medellín y Bogotá con satisfacción

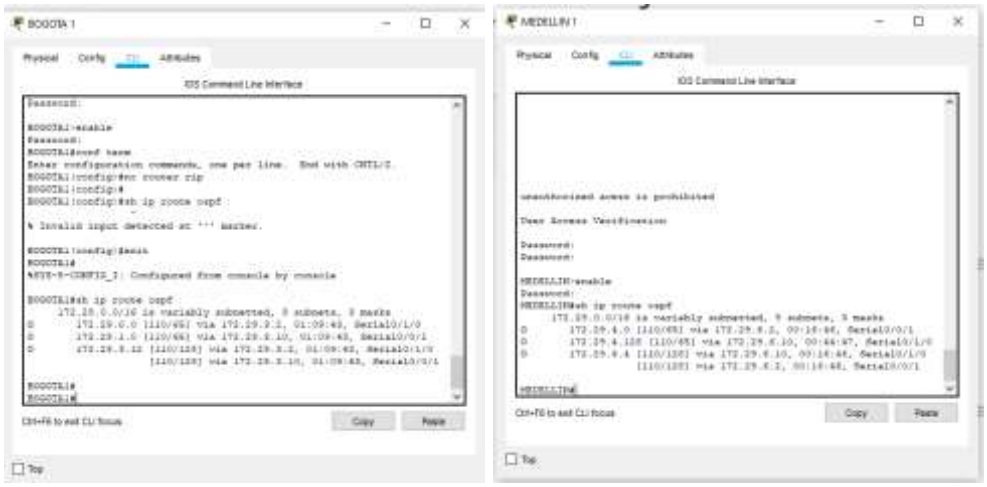

figura 31 verificación de la tabla de enrutamiento

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

Se observa que hay un balanceo de carga en el routers medellin2, en el cual recibe varias trayectorias

figura 32 verificación de balanceo de carga de Routers

f. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Se observa q la similitud en las rutas de las redes con sus rutas

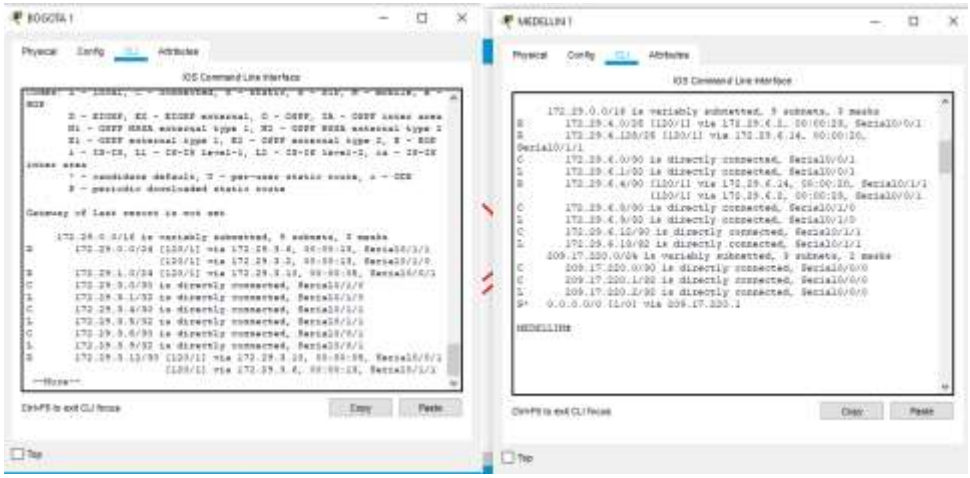

figura 2 similitud en la tabla de redes

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

   Se observa que las redes de los routers Medellín 2 y Bogotá 2 están conectadas y recibidas mediante OSPF

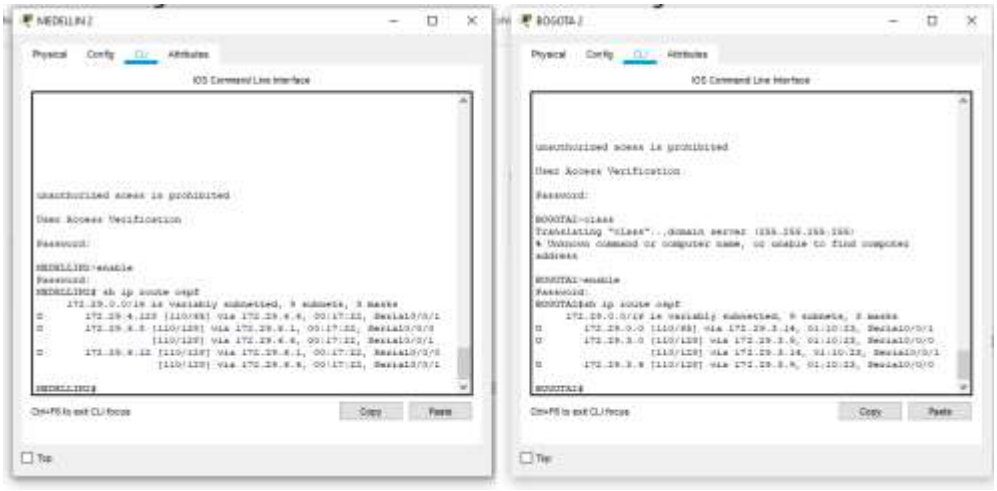

figura 3 redes conectadas directamente

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

   Se observan las 3 rutas de la red para mantener la red confiable

Figura 4 Visualización de rutas redundantes

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

Esto nos indica la ip de destino y la ip de donde tiene que ser enviado

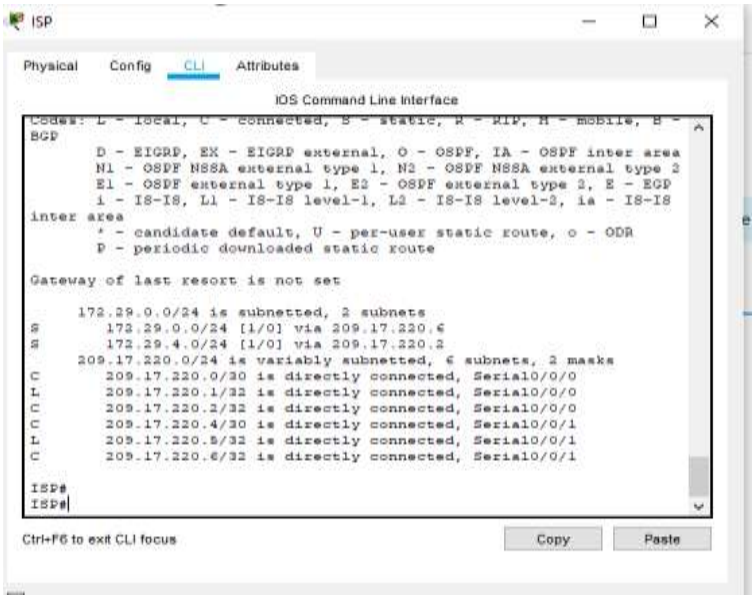

Figura 5 ISP indica sus rutas estáticas

PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

j. 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 29 interfaces que no necesitan desactivación

PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

k. 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.

Se observa la interface passive del router

Figura 37 verificación de passive interface

l. 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.

Se observa la base de datos RIP del router Bogotá 2 donde nos indica las rutas de red OSPF

figura 38 verificación base de datos OSPF en Routers

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.

Dispositivo	Encapsulación y Autenticación PPP
Medellín 1	MEDELLIN1#conf term MEDELLIN1(config)# hostname MEDELLIN1 MEDELLIN1(config)# username ISP password cisco MEDELLIN1(config)# int s0/0/0 MEDELLIN1(config-if)# encapsulation ppp MEDELLIN1(config-if)# ppp encapsutalion pap MEDELLIN1(config-if)# ppp pap sent-username ISP password cisco
Bogotá 1	BOGOTA1#conf term BOGOTA1(config)# hostname BOGOTA1 BOGOTA1(config)# hostname ISP password cisco BOGOTA1 (config)# int s0/0/0 BOGOTA1 (config-if)# encaptulation ppp BOGOTA1 (config-if)# ppp authentication chat
	ISP#conf term

ISP	ISP(config)# hostname ISP ISP(config)# username MEDELLIN1 password cisco ISP(config)# int s0/0/0 ISP(config-if)# encapsulation ppp ISP(config-if)# ppp encapsutalion pap ISP(config-if)# ppp pap sent-username ISP password cisco ISP(config)# int s0/0/0 ISP(config-if)# username BOGOTA 1 password cisco ISP(config-if)# encapsulation ppp ISP(config-if)# ppp encapsutalion pap

Tabla 30 encapsulación y autenticación ppp

PARTE 6: CONFIGURACIÓN DE PAT.

m. 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.
n. 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.
o. 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
p. 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.

Dispositivo	Configuración PAT
Bogotá 1	ip nat inside source list 10 interface s0/0/0 overload access-list 10 permit 172.29.4.0 0.0.3.255 int s0/0/0 ip nat outside int s0/0/1 ip nat inside int s0/1/0 ip nat inside int s0/1/1

	ip nat inside
Medellín 1	ip nat inside source list 10 interface s0/0/0 overload access-list 10 permit 172.29.0.0 0.0.3.255 int s0/0/0 ip nat outside int s0/0/1 ip nat inside int s0/1/0 ip nat inside int s0/1/1 ip nat inside

Tabla 6 configuración pat de los dispositivos

Se observa ping satisfactorio de pc 2 a pc 3 con satisfacción luego observamos que por el proceso de traducción nat no puede llegar hasta el otro extremo como esta descrito en el enunciado

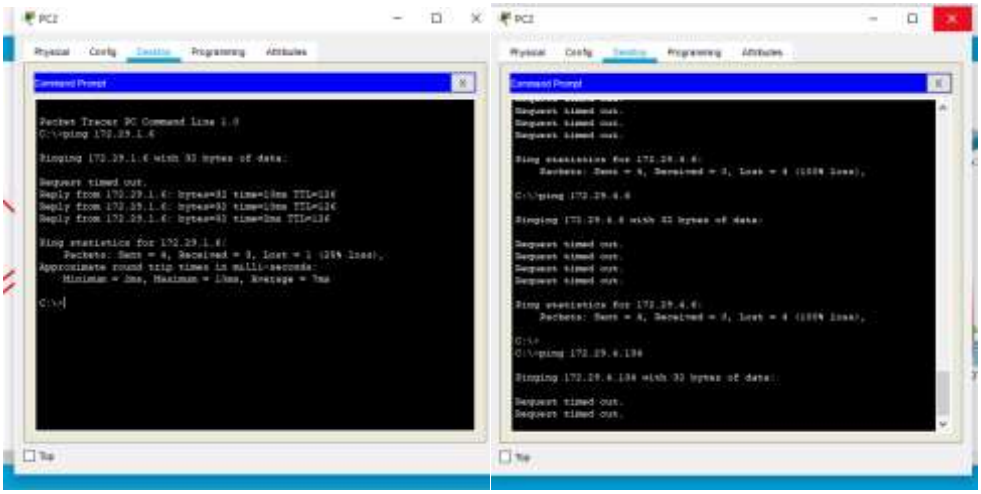

figura 39 verificación configuración nat

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.

Nos solicita excluir la dirección ip inicial agregamos la pool agregamos la red configuramos la red por defecto agregamos un DNS excluimos las direcciones ip y creamos la red para que tome el aquipo

Dispositivo	Configuración DHCP
Bogotá 2	BOGOTA2#conf term 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 BOGOTA 2 BOGOTA2(dhcp-config)#nerwork 172.29.1.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.1.1 BOGOTA2(dhcp-config)#dns-server 8.8.8.8 BOGOTA2(dhcp-config)#exit BOGOTA2(config)#ip dhcp pool BOGOTA 3 BOGOTA2(dhcp-config)#nerwork 172.29.0.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.29.1 BOGOTA2(dhcp-config)#dns-server 8.8.8.8 BOGOTA2(dhcp-config)#exit
Bogotá 3	BOGOTA3#conf term BOGOTA3(config)#int g0/0 BOGOTA3(config-if)#ip helper-address 172.29.3.13
Medellín 2	MEDELLIN2#conf term 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 MEDELLIN 2 MEDELLIN2(dhcp-config)#nerwork 172.29.4.0 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.1 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp pool MEDELLIN 3 MEDELLIN2(dhcp-config)#nerwork 172.29.4.128 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.129 MEDELLIN2(dhcp-config)#dns-server 8.8.8.8 MEDELLIN2(dhcp-config)#exit

Medellín 3	BOGOTA3#conf term BOGOTA3(config)#int g0/0 BOGOTA3(config-if)#ip helper-address 172.29.6.5

Tabla 32 configuración DHCP de los dispositivos

Nos indica que la interfaz de entrada y salida es s0/1/0

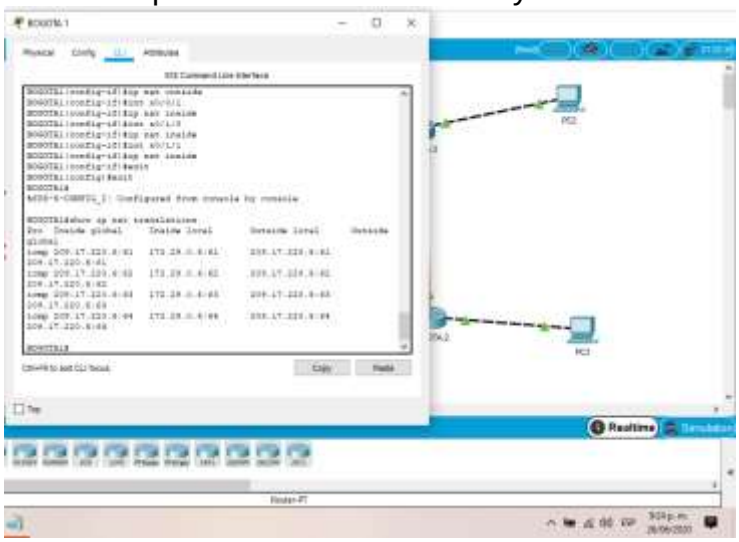

figura 40 verificación de nat

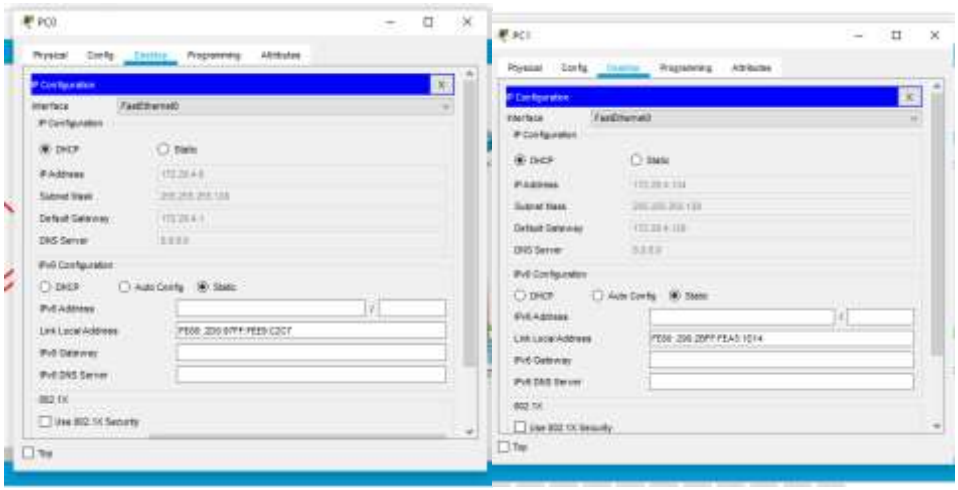

Figura 41 Configuración del servicio DHCP pc 0 pc 1

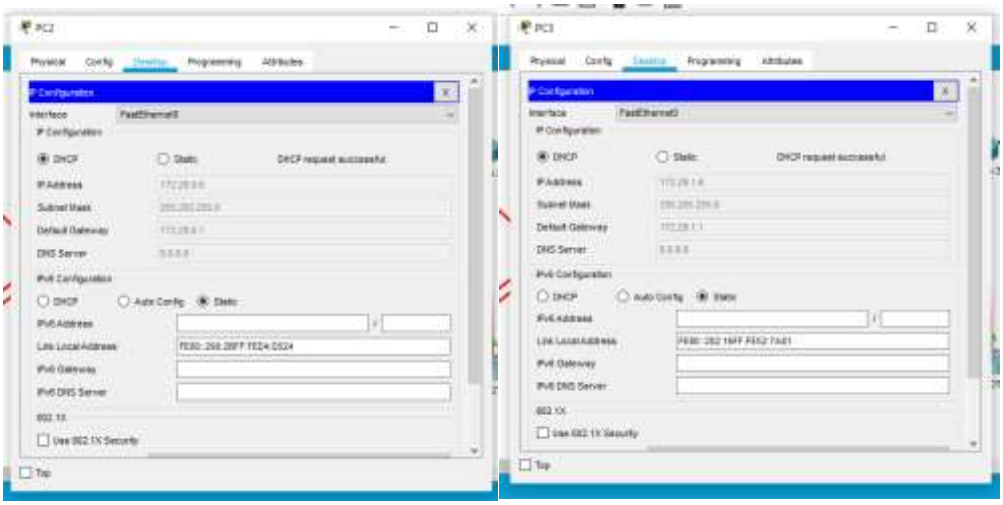

figura 42 Configuración del servicio DHCP pc 2 pc3

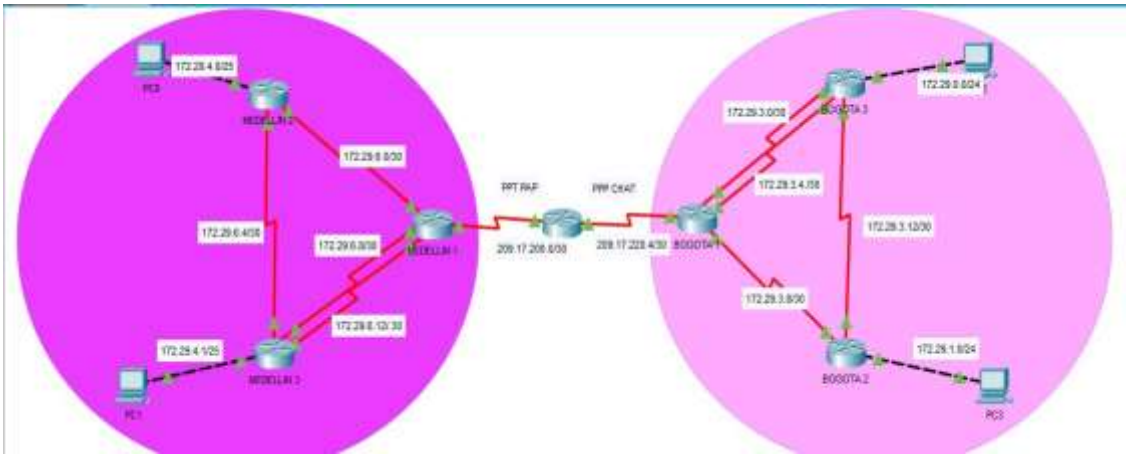

figura 43. Fin tipología escenario 2

CONCLUSIONES

Con el desarrollo de esta actividad de habilidades practica se realizaron diferentes tareas las cuales jugaron un papel importante para llegar a la solución de los ejercicios propuestos, mediante esto se ejecutaron funciones de verificación de una conexión entre los dispositivos dispuestos en la configuración inicial de la topología, se configura la ACL de los routers, cuyo fin es mitigar los ataques de manera remota, además de la verificación de la funcionalidad de las actividades ejecutadas anteriormente (ACL) cuya función es permitir el acceso de las direcciones IP específicas, dando seguridad de que únicamente el administrador de la computadora tenga permiso para acceder al router mediante o SSH.

En el segundo escenarios nos apoyamos en los conocimientos del primer escenario teniendo en cuenta que en el ejercicio vimos solo router y pc, y configuramos los router principal con características distintas y lo dividimos entre áreas.

BIBLIOGRAFÍA

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgTCtKY-7F5KIRC3

ANEXOS

Link del driver donde se encuentran los laboratorios de los escenarios 1 y 2:

https://drive.google.com/drive/folders/1VG3iEandf2KxXU80BofeEJ9hOhUWnOZ-?usp=sharing