PRUEBA DE HABILIDADES CCNA 2020

DIEGO FERNANDO NUÑEZ GALEANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
FACULTAD DE INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
IBAGUE-JULIO
2020

PRUEBA DE HABILIDADES CCNA 2020

DIEGO FERNANDO NUÑEZ GALEANO

Trabajo de grado para optar por el título de Ingeniero en Sistemas

PAULITA FLOR SALAZAR
Directora de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
FACULTAD DE INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
IBAGUE-JULIO
2020

Nota de Aceptación

_____

_____

_____

_____

Jurado

_____

Jurado

_____

Jurado

Ibagué, Tolima 10, 7, 2020

DEDICATORIA

Dedico este trabajo primero que todo a Dios por darme la fortaleza para sacar el trabajo de grado adelante, también a todas aquellas personas que Tienen una edad avanzada y que Quieran superarse y adquirir Cada día nuevos conocimientos Para el progreso de sus vidas Y de sus familias.

AGRADECIMIENTOS

Mi primero que todo agradecer a Dios por todas sus bendiciones durante este proceso de aprendizaje, a mis Padres a mi esposa Diana Yaneth Montes a mis hijos Juan Diego y Danna Sofia que han sido mi gran motivación para sacar este proyecto adelante y darles un mejor futuro, también por su apoyo y paciencia durante estos casi 5 años, y por último y especial a mi tía Ángela Nuñez que siempre ha estado apoyándome en este proyectó de vida.

También quiero agradecer a la Universidad Nacional abierta y a distancia UNAD, a sus directivos y profesores por la organización del programa de Ingeniería de Sistemas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL — Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad.

VLA N — Una red de área local virtual (VLA N) es una red de switch que es dividida en segmentos lógicamente por la función, el área, o la aplicación, sin consideración alguna hacia las ubicaciones físicas de los usuarios.

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

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

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

NAT (Network Address Translation): también llamado enmascaramiento de IP o **NAT**, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

Port Address Translation (PAT): es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet.

Open Shortest Path First (OSPF): es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF).

RESUMEN

En el presente proyecto de trabajo grado, fue la de desarrollar los escenarios propuestos, a las actividades educativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de aprendizaje y las habilidades que se adquirieren durante el curso, y que a través del cual se pondrá a prueba en los niveles de comprensión y solución de problemas relacionados con diversos aspectos de redes de ipv4 y Ipv6 en el mundo real. Hoy en dia puedo decir que tenemos tecnologías que nos permiten una comunicación real o instantánea con cualquier parte del mundo y esto es gracias a la capacidad que tiene las redes de comunicarsen entre si y donde nos permiten compartir voz, video y datos, tambien tenemos una infinidad de aplicaciones que nos permiten realizar transacciones de manera instantánea y esto es gracias a los dispositivos que actualmente estamos aprendiendo configurar y a identificar sus fallas, por eso están importante el curso de CCNA para el personal técnico como para los futuros ingenieros de sistemas o cualquier área de las comunicaciones.

ABSTRACT

In the present degree work project, it was to develop the proposed scenarios for the educational activities of the CCNA Deepening Diploma, which seeks to identify the degree of learning and the skills acquired during the course, and which through which You will be tested at levels of understanding and troubleshooting related to various aspects of IPv4 and IPv6 networking in the real world. Today I can say that we have technologies that allow us real or instant communication with any part of the world and this is thanks to the ability of networks to communicate with each other and where they allow us to share voice, video and data, we also have a infinity of applications that allow us to carry out transactions instantaneously and this is thanks to the devices that we are currently learning to configure and identify their failures, that is why the CCNA course is important for technical personnel as well as for future systems engineers or any area of communications.

INTRODUCCIÓN

El presente trabajo fue el desarrollo de investigar y analizar los principales procesos para la configuración y programación de los equipos Cisco en los diferentes ambientes propuestos. Por esta razón el diseño de redes y el saber adminístralas es un reto, la universidad Nacional abierta y a Distancia con este diplomado de profundización de Cisco, nos da la oportunidad de adquirir los conocimientos y las practicas necesarias para el mantenimiento y construcción de redes de comunicaciones. Los conceptos básicos, medios y operacionales de Ethernet son el fundamento de este curso. Al finalizar este curso seremos capaces de realizar configuraciones básicas en enrutadores y switches, además de implementar esquemas de direccionamiento IP en diferentes ambientes de la vida real.

OBJETIVOS

GENERAL

Fortalecer el conocimiento es necesario para configurar y solucionar problemas de enrutadores y switch y de resolver inconvenientes comunes con redes IPv4 e IPv6. Además de desarrollar el conocimiento y las habilidades necesarias para implementar una red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación y de enrutamiento.

ESPECIFICOS

- Aprender a configurar y verificar los comandos de enrutamiento básicos para el manejo de redes ipv4 y ipv6.

- Fortalecer los conocimientos y habilidades para el manejo de fallas de los dispositivos como router y Switch y determinar sus posibles soluciones.

PLANTEAMIENTO DEL PROBLEMA

DEFINICION DEL PROBLEMA

El presente trabajo pretende responder la importancia que tiene hoy en día las telecomunicaciones en las grandes, medianas y pequeñas empresas las cuales se desarrollan en un ambiente de constante cambio tecnológico, es por eso la importancia de analizar los diferentes factores que se manifiestan alrededor de ellas al momento de implementar nuevas estrategias para generar una ventaja competitiva en el entorno de las telecomunicaciones, es aquí donde las empresas deben realizar un análisis estratégico de su entorno tecnológico y donde el personal este altamente capacitado para resolver las fallas de Networking.

JUSTIFICACION

La práctica de habilidades de CCNA de cisco es desarrollada con el fin de medir los conocimientos de los estudiantes durante este proceso de enseñanza en el cual los escenarios planteados son importantes para medir la capacidad, de resolver fallas y responder al creciente número personal capacitado en el área de las telecomunicaciones. A medida que nuestra dependencia de las redes continúa creciendo, las tecnologías que nos rodea están evolucionando. Las redes de routing y switching básicas han madurado en redes convergentes de voz, video y datos, donde las organizaciones dependen de personal capacitado cada vez más para la administración el diseño e implementar nuevos retos.

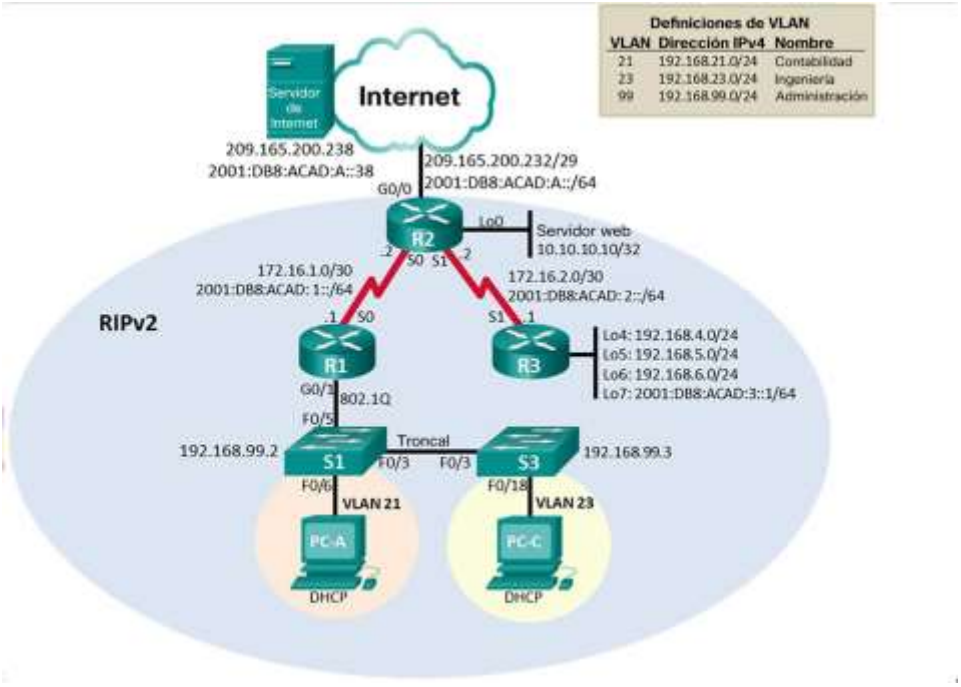
Desarrollo de los Escenarios Propuestos Para la Prueba de Habilidades

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 Topología Escenario 1



Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches

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

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

Tabla 1 Configuración básica del software del routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	**S1#Erase startup-config**
Volver a cargar todos los routers	**S1#reload**
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**S1#Erase startup-config** **S1#Delete flash:valn.dat**
Volver a cargar ambos switches	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**S1#show vlan brief**

Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

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

Tabla 2 Configurar la computadora de Internet según topología

Elemento o tarea de configuración	Especificación
Dirección IPv4	Se ingresa al servidor en la pestaña desktop y ubicamos Configuración ip, buscamos la casilla ipv4. Ingresamos la ruta. 209.165.200.238
Máscara de subred para IPv4	Buscamos la casilla de subred Mask Introducimos la ruta. 255.255.255.0

Gateway predeterminado	En la misma ventana, buscamos la pestaña o casilla Default Gateway Ingresamos la ruta 209.165.200.233
Dirección IPv6/subred	En la misma venta, buscamos la ventana IPV6 address ingresamos la ip. 2001:CB8:ACAD:A::38
Gateway predeterminado IPv6	En la misma venta, buscamos la casilla Gateway de IPV6 ingresamos la ruta. 2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Configurar R1

Tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuración básica de R1

Elemento o tarea de configuración	Especificación Se ingresan los siguientes comandos para configuración básica del Router 1 y se configura el puertos S0/0/0 con la ipv4 y ipv6 y se configura las rutas predeterminadas.
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router# Router(config)#hostname R2 R2(config)#exit
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#exit
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD	R1#config term R1(config)# banner motd # Se prohíbe el acceso no autorizado # R1(config)# exit

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama. R1(config)#Interface s0/0/0 R1(config)#ip address 172.16.1.1 255.255.255.252 R1(config)#clock rate 128000 R1(config)#no shutdown R1(config)#exit topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de R1(config)#interface s0/0/0 R1(config)#ipv6 enable R1(config)#ip address 2001:db8:acad:1::1/64 **R1(config)#clock rate 12800** **R1(config)#no shutdown** R1(config)#exit topología para conocer la información de direcciones 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 R1(config)#interface serial 0/0/0 R1(config-if)#ip address 0.0.0.0 0.0.0.0 R1(config-if)#exit Configurar una ruta Ipv6 predeterminada de S0/0/0 R1(config)#interface Serial0/0/0 R1(config-if)#ipv6 address ::/0 R1(config-if)#exit
Guardar Configuración	R1#copy running-config startup-config

Nota: Todavía no configure G0/1.

Configurar R2

La configuración del R2 incluye las siguientes tareas:

Se ingresan los siguientes comandos para la configuración básica del Router 2, y se configura los puertos S0/0/0, S0/0/1, G0/0 con la ipv4 y ipv6 y se configura las rutas predeterminadas.

Tabla 4 Configuración básica del router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	R2(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2(config)#exit
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#end
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2#config term R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP	No tiene la opción para la configuración del comando
Mensaje MOTD	R2#config term R2(config)#banner motd # Se prohíbe el acceso no autorizado # R2(config)#exit
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config)#Interface s0/0/0 R2(config)#ip address 172.16.1.2 255.255.255.252 R2(config)#clock rate 128000 R2(config)#no shutdown R2(config)#exit Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config)#interface s0/0/0

	R2(config)#ipv6 enable R2(config)#ip address 2001:db8:acad:1::2/64 R2(config)#clock rate 12800 **R2(config)#no shutdown** R2(config)#exit R2#
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config)#interface s0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 **R2(config-if)#no shutdown** R2(config-if)#exit Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. R2(config)#interface s0/0/1 R2(config-if)#ipv6 enable R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 **R2(config-if)#clock rate 128000** **R2(config-if)#no shutdown** R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 Bad mask /29 for address 209.165.200.232 R2(config-if)#no shutdown R2(config-if)#exit Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)#interface loopback 0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)# interface G0/0 R2(config)# ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)# exit Configure una ruta IPv6 predeterminada de G0/0. R2(config)# interface G0/0 R2(config)# ipv6 route ::/0 G 0/0 R2(config)# exit R2#

Configurar R3

La configuración del R3 incluye las siguientes tareas:

Ingresamos los siguientes comandos para la configuración básica del R3, y se configuran las direcciones loopbak 4, 5, 6, 7 y se configura el puerto S0/0/1 con ipv4 y ipv6.

Tabla 5 Configuración básica del router

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
Nombre del router	R3(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#exit
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3#config term R3(config)#service password-encryption R3(config)#exit
Mensaje MOTD	R3(config)# banner motd # Se prohíbe el acceso no autorizado #

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config)#interface s0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 **R3(config-if)#clock rate 128000** **R3(config-if)#no shutdown** R3(config-if)#exit Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface s0/0/1 R3(config-if)# ipv6 enable R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 **R3(config-if)#clock rate 128000** **R3(config-if)#no shutdown** R3(config-if)#exit R3(config)# Activar la interfaz No shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface looback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface looback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface looback 4 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface looback 7 R3(config-if)#ipv6 addres 2001:DB8:ACAD:3::1/64 R3(config-if)#exit

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se ingresa los siguientes comandos para la configuración básica del Switch 1, que son para la parte de seguridad para que solamente las personas autorizadas puedan ingresar.

Tabla 6 Configuración básica del Switch 1

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

Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Se ingresan los siguientes comandos para configuración básica del Switch 3

Tabla 7 Configuración básica del Switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)# no ip domain-lookup S3(config)#exit
Nombre del switch	Switch(config)# hostname S3

	S3#exit
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#exit
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)# banner motd # Se prohíbe el acceso no autorizado #

Verificar la conectividad de la red

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

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

Tabla 8 Comprobación de conectividad entre los dispositivos de red.

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

Figura 2 Ping de conectividad de R1 a R2

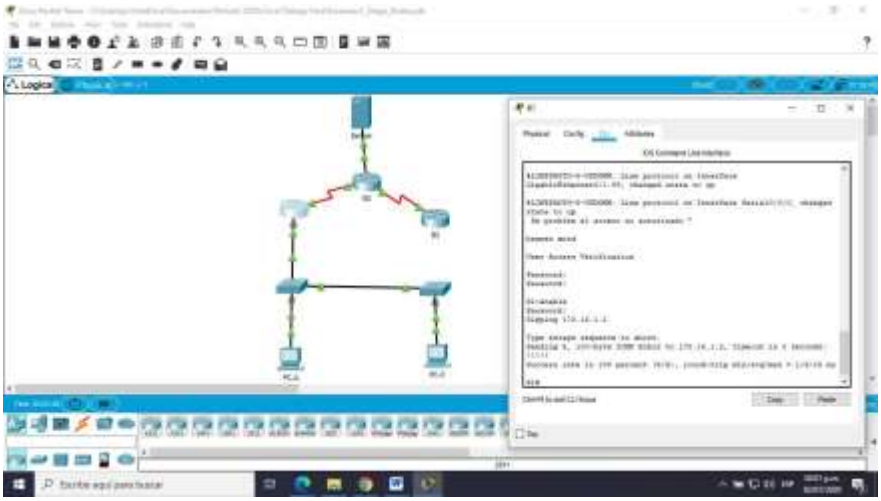


Figura 3 Conectividad de R2 a R3

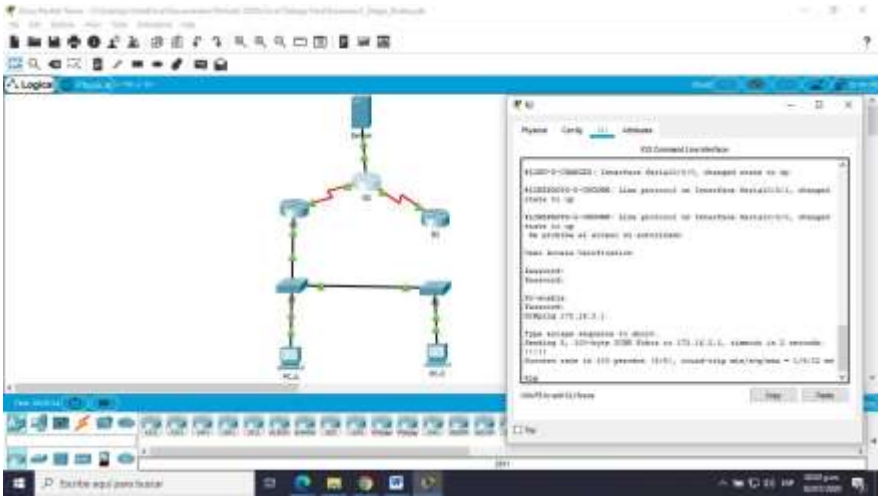
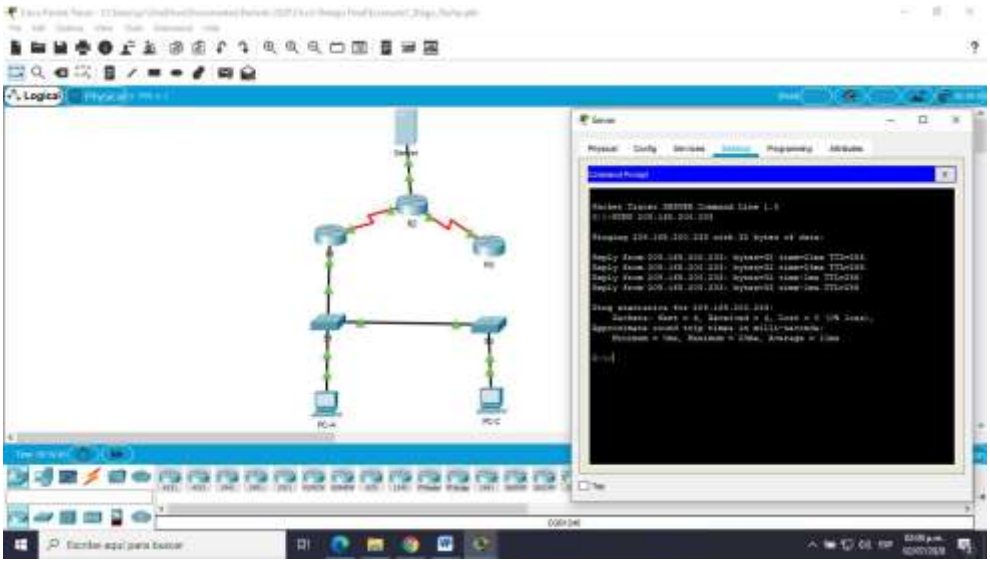


Figura 4 Conectividad servidor de internet a Gateway predeterminado



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

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

La configuración del S1 incluye las siguientes tareas:

Se ingresan los siguientes comandos para la creación de las vlan y seguridad de los puertos de Switch

Configurar S1

Tabla 9 Crear vlan en el switch 1 y direccionamiento

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)#name Contabilidad S1(config)#vlan 23 S1(config)#name Ingenieria S1(config)#vlan 99} S1(config)#name Administration

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config-if)# ip default-Gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)# switchport trunk native vlan 1 S1(config-if)# end
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface range f0/6 S1(config-if)# switchport mode access S1(config-if)# switchport access vlan 21 S1(config-if)# end
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Se ingresan los siguientes comandos para la configuración de seguridad del Switc3, crear trunk al puerto 3 del switch, crear vlan y asignar al puerto 18 del switch

Tabla 10 Seguridad del Switch 3 de vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S1(config)#vlan 21 S1(config)#name Contabilidad S1(config)#vlan 23 S1(config)#name Ingenieria S1(config)#vlan 99} S1(config)#name Administration
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 S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.3 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el Gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range R3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 R3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)# switchport mode access S3(config-if)# switchport access vlan 23 S3(config-if)# end
Apagar todos los puertos sin usar	R3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 R3(config-if-range)#shutdown

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Los siguientes comandos para la configuración de las Subinterfaces del R1 y asignar direccionamiento ip.

Tabla 11 Configuración de las subinterfaces de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz 1(config)#int g0/1.21 R1(config-subif)#description vlan 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz 1(config)#int g0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz 1(config)#int g0/1.99 R1(config-subif)#description vlan 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Verificar la conectividad de la red

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

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

Tabla 12 Verificar conectividad entre Switch y Routers

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

Figura 5 Ping de S1 entre vlan 99 y 21

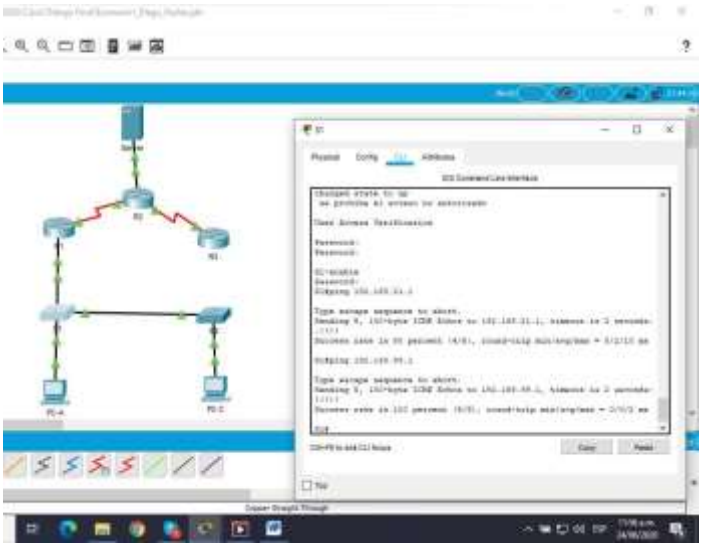
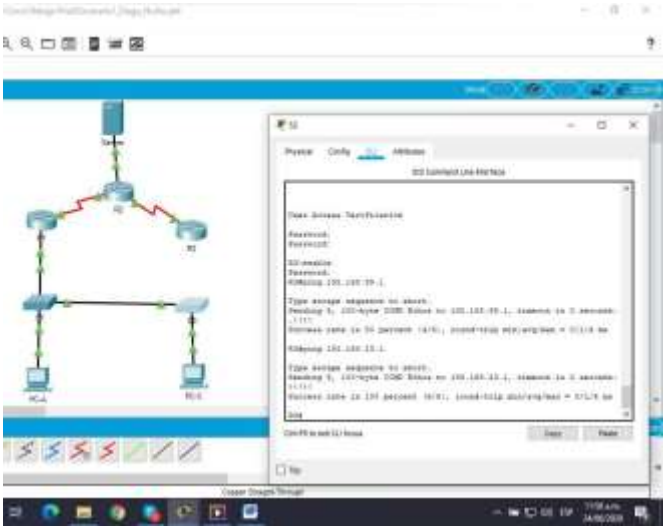


Figura 6 Ping de S1 entre Vlan 99 y 23



Configurar el protocolo de routing dinámico RIPv2

Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Los siguientes comandos son para la configuración del protocolo routing Ripv2 en R1, R2 Y R3 anunciar las redes conectadas y estableces las interfaces ´pasivas.

Tabla 13 Configurar protocolo routing dinámico RIPV2 EN R1

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	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
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#
Desactive la sumarización automática	R1(config-router)#no auto-summary R1(config-router)#exit

Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configurar protocolo routing dinámico RIPV2 EN R2

Elemento o tarea de configuración	**Especificación** Se ingresan los siguientes comandos para configuración del protocolo routing Ripv2 en R2
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0 R2(config-router)#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	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configurar protocolo routing dinámico RIPV2 EN R3

Elemento o tarea de configuración	Especificación Se ingresan los siguientes comandos para configuración del protocolo routing Ripv2 en R3
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 172.16.4.0 R3(config-router)#network 172.16.5.0 R3(config-router)#network 172.16.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary R3(config-router)#end

Verificar la información de RIP

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

Tabla 16 Verificación de la configuración RIP

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

Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configurar DHCP y NAT para IPv4 en R1

Elemento o tarea de configuración	Especificación Se ingresan lo siguientes comandos para configurar DHCP Y NAT para R1
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el Gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio ccna-sa.com Establecer el Gateway predeterminado R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit

Configurar la NAT estática dinámica en el R2

Configuración en R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configurar NAT estática y dinámica en el R2

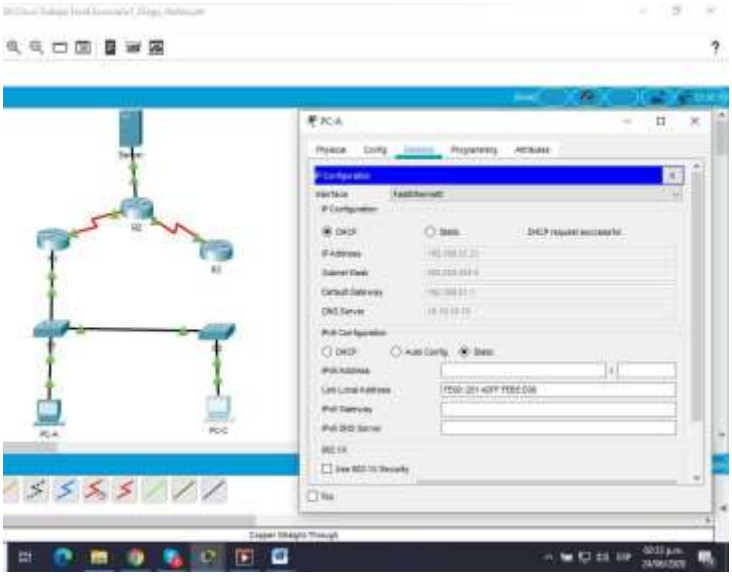
Elemento o tarea de configuración	**Especificación** Se ingresan los siguientes comandos para configurar NAT estática y dinámica en el R2
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R1#config term R1(config)#user webuser privilege 15 secret cisco12345 R1(config)#exit
Habilitar el servicio del servidor HTTP	**No se puede configurar este comando en Packet - Tracer**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**No se puede configurar este comando en Packet - Tracer**
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237** **R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237**
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside 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 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

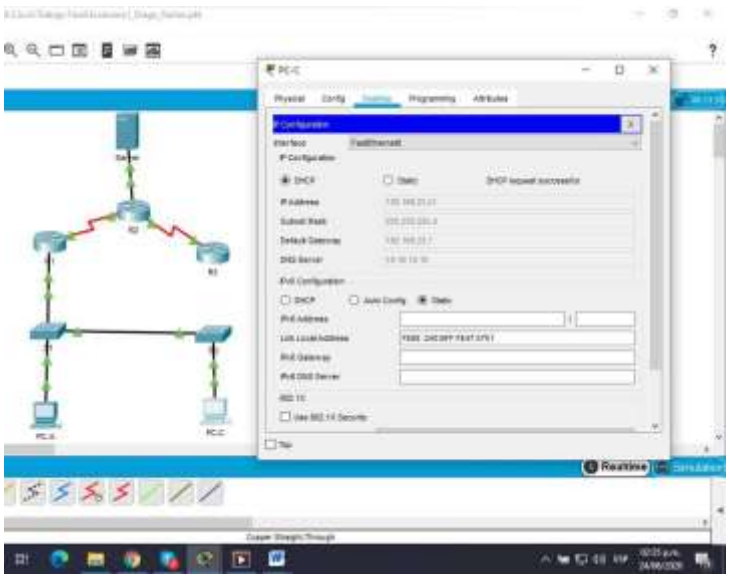
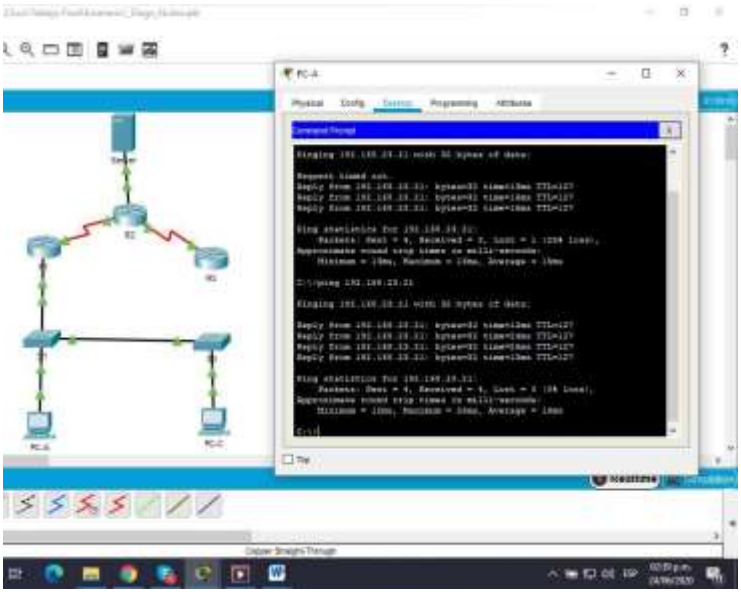
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233 – 209.165.200.236** **R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	**R2(config)#ip nat inside source list 1 pool INTERNET**

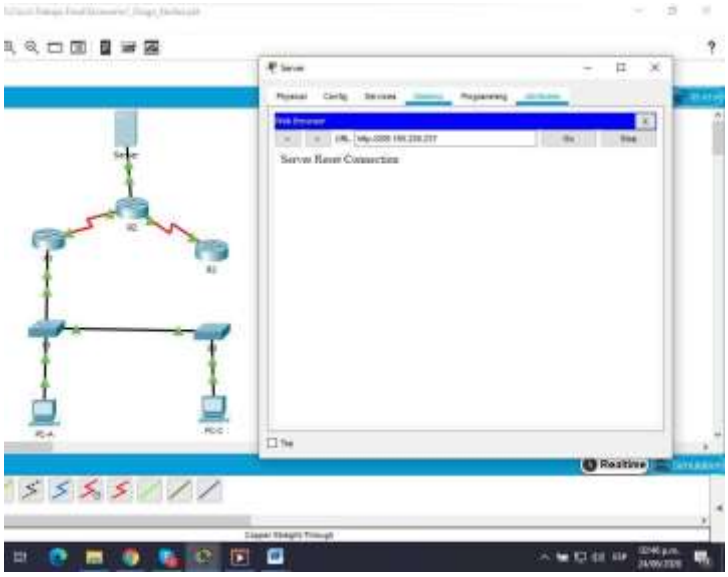
Verificar el protocolo DHCP y la NAT estática

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

Tabla 19 Verificar el protocolo DHCP y la NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Figura 7 PCA con conectividad DHCP* 

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura 8 PCC con conectividad DHCP* 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	*Figura 9 Ping de PCA entre PC-C* 

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	*Figura 10 Conectividad deL servidor, no se ejecuta por no poder configurar HTTP en el R2*  No nos muestra nada, ya que cuando fuimos a configurar HTTP en R2 el comando no lo soporta Packet-Tracer.

Configurar NTP

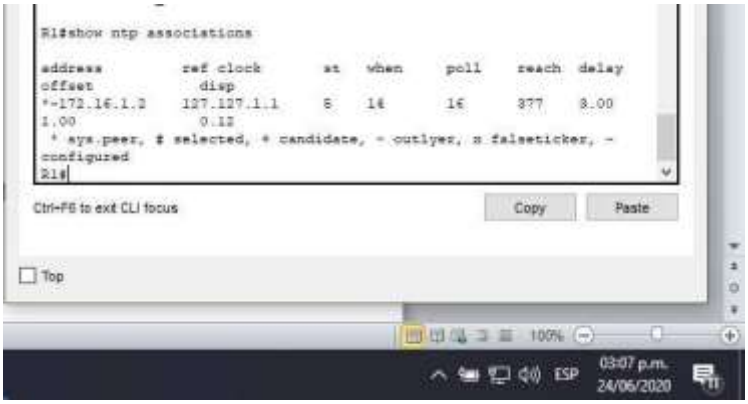
Configuración en R2 Y R1 para NTP

Los siguientes comandos para la configuración NTP en R1 Y R2

Tabla 20 Configuración NTP

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

Figura 11 Se verifica conectividad NTP en R1



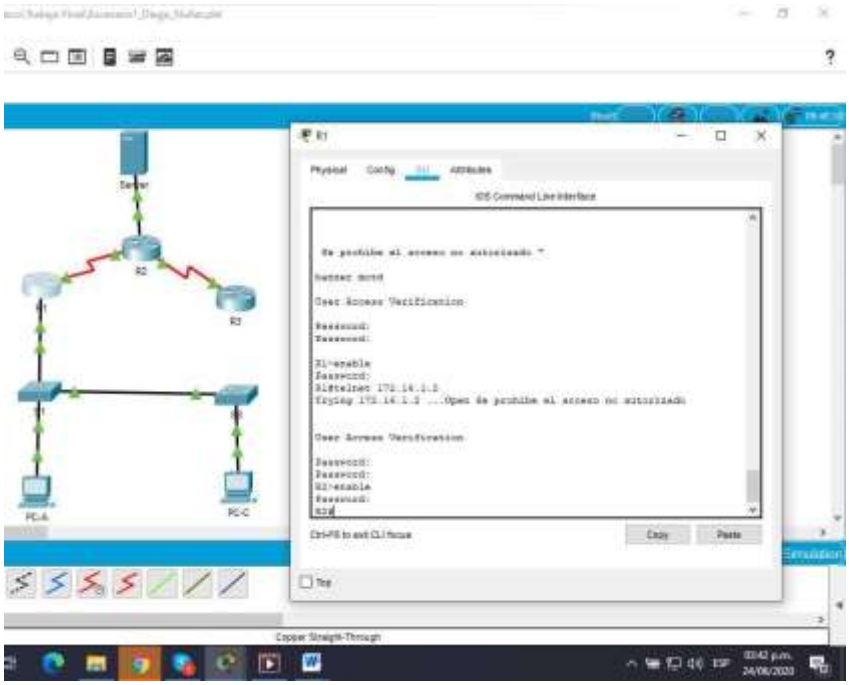
Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Tabla 21 Configuración y verificación las listas de control de acceso

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN- MGT**
Aplicar la ACL con nombre a las líneas VTY	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	Show access-list

Figura 12 Verificación que a ACL funcione



Introducir en el comando Cli lo adecuado que se necesita para mostrar lo siguiente

Tabla 22 Comando Cli

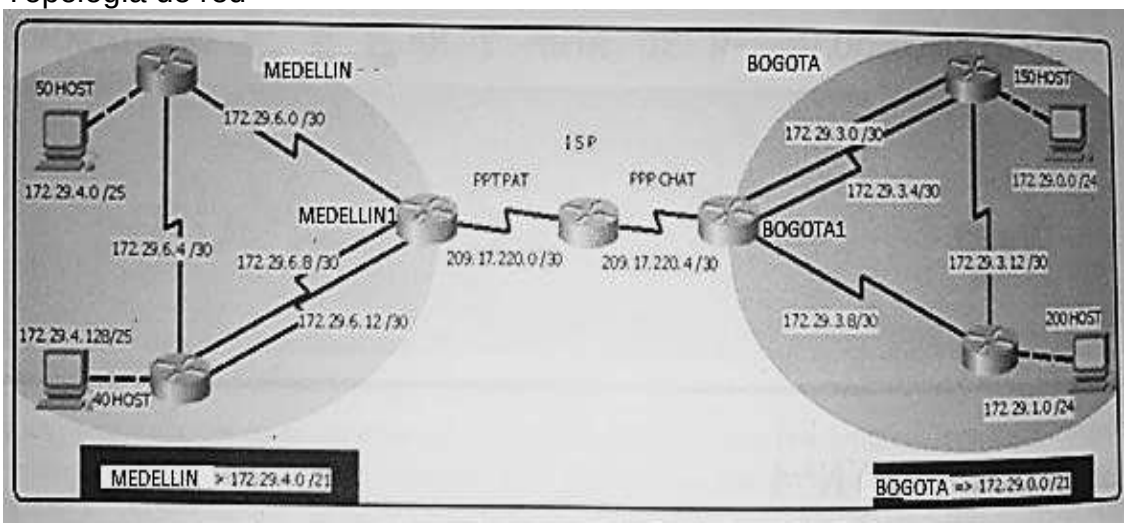
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#Show Access-list R2#Show Access-list 1
Restablecer los contadores de una lista de acceso	No soporta el comando
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface

¿Con qué comando se muestran las traducciones NAT?	R2#show ip net translations **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?	R2#clear ip nat translation *

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



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán 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 escenario 2

Como trabajo inicial se debe realizar lo siguiente.

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

Configuración básica de equipos y direccionamiento IP

Configuran los router con la configuración básica, y se agrega el direccionamiento

Tabla 23 Configuración de interfaces de los Routers y direccionamiento.

Dispositivos	Configuración basica de Routers
ISP	Router(config)#hostname ISP ISP(config)#interface s0/0/0 ISP(config-if)#description ISP A MEDELLIN ISP(config-if)#ip add 209.17.220.1 255.255.255.252 ISP(config-if)#clcok rate 128000 ISP(config-if)#no shutdown ISP(config-if)#exit ISP(config)#interface s0/0/1 ISP(config-if)#description ISP A BOGOTA ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown ISP(config-if)#exit ISP#copy running-config startup-config
Medellin	Router(config)#hostname Medellin Medellin(config)#interface s0/0/0 Medellin(config-if)#description Medellin A ISP Medellin(config-if)#ip address 209.17.220.2 255.255.255.252 Medellin(config-if)#clock rate 128000 Medellin(config-if)#no shutdown Medellin(config-if)#exit Medellin(config)#interface s0/1/1 Medellin(config-if)#description Medellin a Medellin 1 Medellin(config-if)#ip address 172.29.6.13 255.255.255.252 Medellin(config-if)#clock rate 128000 Medellin(config-if)# no shutdown Medellin(config-if)#exit Medellin(config)#interface s0/1/0 Medellin(config-if)#Description Medellin 1 a Medellin Medellin(config-if)#ip address 172.29.6.9 255.255.255.252 Medellin(config-if)#clock rate 128000 Medellin(config-if)#no shutdown Medellin(config-if)#exit Medellin(config)#interface s0/0/1

	Medellin(config-if)#Description Medellin a Medellin 2 Medellin(config-if)#ip address 172.29.6.1 255.255.255.252 Medellin(config-if)#clock rate 128000 Medellin(config-if)#no shutdown Medellin(config-if)#end Medellin1#wr
Medellin1	Router(config)#hostname Medellin1 Medellin1(config)#interface s0/0/0 Medellin1(config-if)#Description Medellin_1 a Medellin Medellin1(config-if)#ip address 172.29.6.14 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#exit Medellin1(config)#interface s0/0/1 Medellin1(config-if)#Description Medellin a Medellin_1 Medellin1(config-if)#ip address 172.29.6.10 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#exit Medellin1(config)#interface s0/1/0 Medellin1(config-if)#Description Medellin_1 a Medellin2 Medellin1(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#exit Medellin1(config)#interface g0/0 Medellin1(config-if)#Description Medellin_1 a PC1 Medellin1(config-if)#ip address 172.29.4.129 255.255.255.128 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#end Medellin1#wr
Medellin2	Router(config)#hostname Medellin2 Medellin2(config)#interface s0/0/1 Medellin2(config-if)#Description Medellin2 a Medellin Medellin2(config-if)#no description Medellin2(config-if)#exit Medellin2(config)#interface s0/0/0 Medellin2(config-if)#Description Medellin 2 a Medellin Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252 Medellin2(config-if)#no shutdown Medellin2(config)#interface g0/0 Medellin2(config-if)#Description Medellin2 a PC2 Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128 Medellin2(config-if)#no shutdown Medellin2(config-if)#end Medellin2#wr
Bogota	Router(config)#hostname Bogota Bogota(config)#interface s0/0/0 Bogota(config-if)#Description Bogota a ISP Bogota(config-if)#ip address 209.17.220.6 255.255.255.252 Bogota(config-if)#clock rate 128000 Bogota(config-if)#no shutdown Bogota(config-if)#exit

	Bogota(config)#interface s0/0/1 Bogota(config-if)#Description Bogota a Bogota 2 Bogota(config-if)#ip address 172.29.31.1 255.255.255.252 Bogota(config-if)#no shutdown Bogota(config-if)#exit Bogota(config)#interface s0/1/0 Bogota(config-if)#Description Bogota 2 a Bogota Bogota(config-if)#ip address 172.29.3.5 255.255.255.252 Bogota(config-if)#no shutdown Bogota(config-if)#exit Bogota(config)#interface s0/1/1 Bogota(config-if)#Description Bogota a Bogota 1 Bogota(config-if)#ip address 172.29.3.9 255.255.255.252 Bogota(config-if)#no shutdown Bogota(config-if)#end Bogota#wr
Bogota_1	Router(config)#hostname Bogota_1 Bogota_1(config)#interface s0/0/0 Bogota_1(config-if)#description Bogota 1 a Bogota Bogota_1(config-if)#ip add 172.29.3.10 255.255.255.252 Bogota_1(config-if)#clock rate 128000 Bogota_1(config-if)#no shutdown Bogota_1(config-if)#exit Bogota_1(config)#interface s0/0/1 Bogota_1(config-if)#description Bogota 1 a Bogota 2 Bogota_1(config-if)#ip add 172.29.3.14 255.255.255.252 Bogota_1(config-if)#clock rate 128000 Bogota_1(config-if)#no shutdown Bogota_1(config-if)#exit Bogota_1(config)#interface g0/0 Bogota_1(config-if)#description Bogota 1 a PCC Bogota_1(config-if)#ip address 172.29.1.1 255.255.255.0 Bogota_1(config-if)#clock rate 128000 Bogota_1(config-if)#no shutdown Bogota_1(config-if)#exit Bogota_1#wr
Bogota_2	Router(config)#hostname Bogota_2 Bogota_2(config)#interface s0/0/0 Bogota_2(config-if)#description Bogota 2 a Bogota Bogota_2(config-if)#ip address 172.29.3.2 255.255.255.252 Bogota_2(config-if)#no shutdown Bogota_2(config-if)#exit Bogota_2(config)#interface s0/0/1 Bogota_2(config-if)#description Bogota a Bogota 2 Bogota_2(config-if)#ip address 172.29.3.6 255.255.255.252 Bogota_2(config-if)#no shutdown Bogota_2(config-if)#exit Bogota_2(config)#interface s0/1/1 Bogota_2(config-if)#Description Bogota 2 a Bogota 1 Bogota_2(config-if)#ip address 172.29.3.13 255.255.255.252 Bogota_2(config-if)#no shutdown Bogota_2(config-if)#exit Bogota_2(config)#interface g0/0

	Bogota_2(config-if)#Description Bogota a PCC Bogota_2(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota_2(config-if)#no shutdown Bogota_2(config-if)#exit Bogota_2#wr

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

Configuración del enrutamiento

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

Configuración de dispositivos a OSPF

Se configuran los dispositivos con OSPF el cual se usa para distribuir la información de ruteo dentro de un área.

Tabla 24 Configuración de protocolo OSPF a todos los router menos ISP

Dispositivos	Configuración OSPF en los Routers
Medellín	Medellin(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medellin(config)#router ospf 1 Medellin(config-router)#router-id 1.1.1.1 Medellin(config-router)#network 172.29.6.0 0.0.0.3 area 0 Medellin(config-router)#network 172.29.6.8 0.0.0.3 area 0 Medellin(config-router)#network 172.29.6.12 0.0.0.3 area 0 Medellin(config-router)#default-information originate Medellin(config-router)#end
Medellin1	Medellin1(config)#router ospf 1 Medellin1(config-router)#router-id 3.3.3.3 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0 Medellin1(config-router)#network 172.29.6.4 0.0.0.3 area 0 Medellin1(config-router)#network 172.29.4.128 0.0.0.127 area 0 Medellin1(config-router)#default-information originate Medellin1(config-router)#passive-interface g0/0 Medellin1(config-router)#end
Medellin2	Medellin2(config)#router ospf 1 Medellin2(config-router)#router-id 2.2.2.2 Medellin2(config-router)#network 172.29.6.0 0.0.0.3 area 0 Medellin2(config-router)#network 172.29.6.4 0.0.0.3 area 0 Medellin2(config-router)#network 172.29.4.0 0.0.0.127 area 0 Medellin2(config-router)#default-information originate Medellin2(config-router)#passive-interface g0/0 Medellin2(config-router)#end
Bogotá	Bogota(config)#router ospf 1 Bogota(config-router)#router-id 11.11.11.11

	Bogota(config-router)#network 172.29.3.0 0.0.0.3 area 0 Bogota(config-router)#network 172.29.3.4 0.0.0.3 area 0 Bogota(config-router)#network 172.29.3.8 0.0.0.3 area 0 Bogota(config-router)#end Bogota#wr
Bogota1	Bogota_1(config)#router ospf 1 Bogota_1(config-router)#router-id 22.22.22.22 Bogota_1(config-router)#network 172.29.3.12 0.0.0.3 area 0 Bogota_1(config-router)#network 172.29.3.8 0.0.0.3 area 0 Bogota_1(config-router)#network 172.29.1.0 0.0.0.255 area 0 Bogota_1(config-router)#default-information originate Bogota_1(config-router)#passive-interface g0/0 Bogota_1(config-router)#end Bogota_1#
Bogota2	Bogota_2(config)#router ospf 1 Bogota_2(config-router)#router-id 33.33.33.33 Bogota_2(config-router)#network 172.29.3.0 0.0.0.3 area 0 Bogota_2(config-router)#network 172.29.3.4 0.0.0.3 area 0 Bogota_2(config-router)#network 172.29.3.12 0.0.0.3 area 0 Bogota_2(config-router)#network 172.29.0.0 0.0.0.255 area 0 Bogota_2(config-router)#default-information originate Bogota_2(config-router)#passive-interface g0/0 Bogota_2(config-router)#end Bogota_2#

b. Los routers Bogotá 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.

Configuración rutas distribuidas en OSPF en Medellín Y Bogotá

Tabla 25 Rutas distribuidas en Medellín y Bogotá en OSPF

Dispositivos	Configuración rutas Distribuidas en OSPF
Medellín	Medellin(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medellin(config)#router ospf 1 Medellin(config-router)#default-information originate
Bogota	Bogota(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota(config)#router ospf 1 Bogota(config-router)#default-information originate

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

.Configuración en Bogotá y Medellín para sumarizacion de las subredes

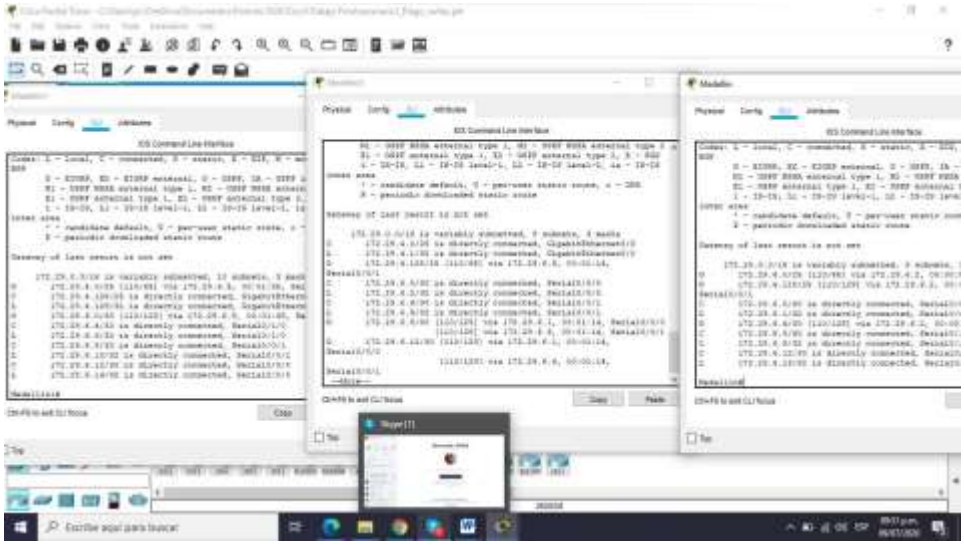
Tabla 26 Sumarizacion de subredes en Bogotá y Medellín

Dispositivo	Configuración Rutas estáticas Sumarizadas a sedes
Medellín	ISP(config)#ip route 172.29.0.0 255.255.252.0 S0/0/0
Bogota	ISP(config)#ip route 172.29.0.0 255.255.252.0 S0/0/0

Tabla de Enrutamiento.

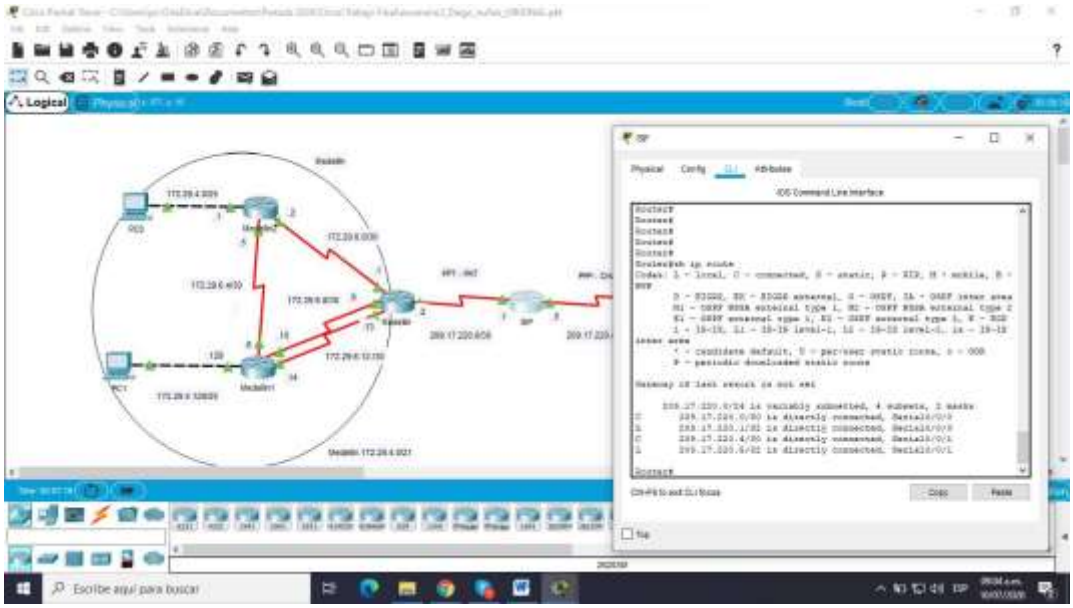
a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
b. Verificar el balanceo de carga que presentan los routers.

Figura 13 Tablas de enrutamiento 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 14 Rutas estáticas Router ISP



Deshabilitar la propagación del protocolo OSPF.

• 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.

Se configura tabla para las interfaces que no están en uso.

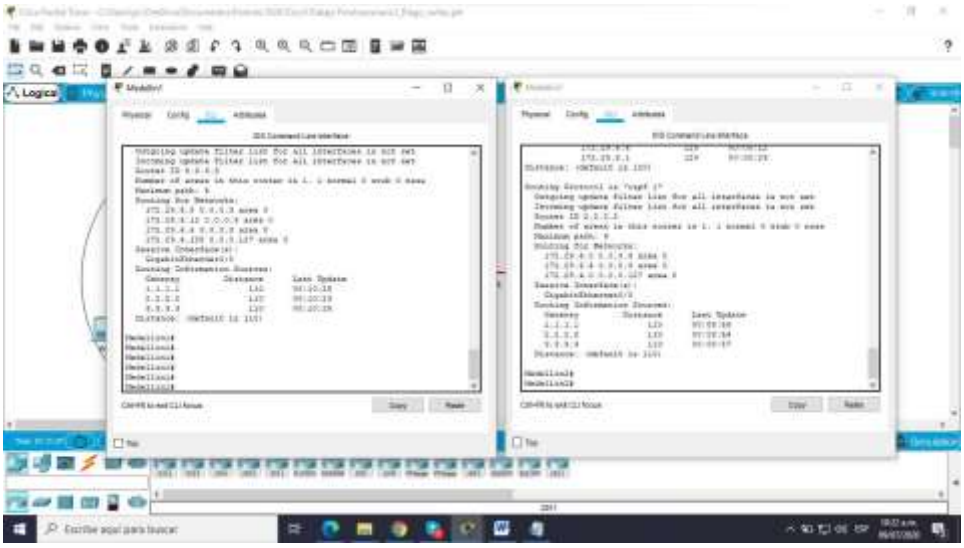
Tabla 27 Se deshabilita la propagación OSPF

Router	Interfaz
Medellin1	Medellin1(config-router)#passive-interface g0/0 Medellin1(config-router)#end
Medellin2	Medellin2(config-router)#passive-interface g0/0 Medellin2(config-router)#end
Bogota_1	Bogota_1(config-router)#passive-interface g0/0 Medellin2(config-router)#end
Bogota_2	Bogota_2(config-router)#passive-interface g0/0 Bogota_2(config-router)#end

Verificación del protocolo OSPF.

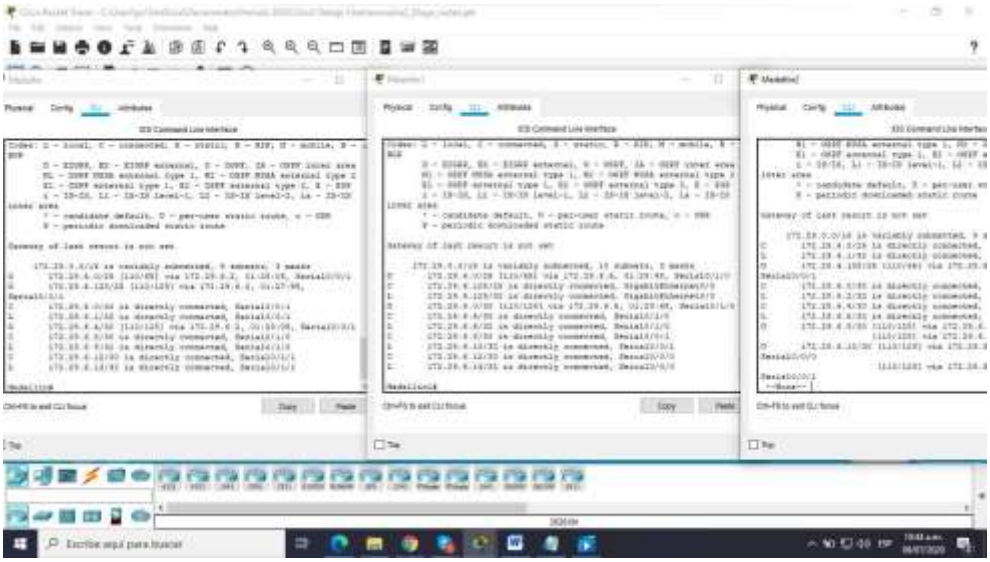
a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura 15 Verificación del protocolo OSPF en Medellin1 y Medellin2



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.

Figura 16 Verificación la base datos OSPF



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 CHAP.

Configuración de Router Medellín, Bogotá, y ISP

Esta configuración PPP se utiliza para seguridad de los enlaces WAN.

Tabla 28 Encapsulamiento y autenticación PPP en Bogotá y ISP

Dispositivo	Encapsulación y autenticación PPP
Medellín PAT	ISP(config)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#end ISP#
Bogota	Bogota(config)#username ISP password cisco Bogota(config)#int s0/0/0 Bogota(config-if)#encapsulation ppp Bogota(config-if)#ppp authentication chap
ISP	ISP(config)#username Bogota password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap ISP(config-if)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#end ISP#wr ISP(config)#username Bogota password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap ISP(config-if)#end

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.
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.

Configuramos la NAT en cada equipo route de Medellín y Bogotá

Configuramos los dispositivos Bogota y Medellín con el protocolo NAT que es para intercambiar paquetes entre dos redes con direccionamiento incompatible.

Tabla 29 Configuración de PAT en Medellín y Bogotá

Dispositivo	Configuración PAT
Medellin	Medellin(config)#ip access-list standard Lan-Medellin Medellin(config-std-nacl)#permit 172.29.0.0 0.0.255.255 Medellin(config-std-nacl)#exit Medellin(config)#ip nat inside source list Lan-Medellin interface s0/0/0 overload Medellin(config)#int s0/0/0 Medellin(config-if)#ip nat outside Medellin(config-if)#exit Medellin(config)#int s0/0/1 Medellin(config-if)#ip nat inside Medellin(config-if)#exit Medellin(config)#int s0/1/0 Medellin(config-if)#ip nat inside Medellin(config-if)#exit Medellin(config)#int s0/1/1 Medellin(config-if)#ip nat inside Medellin(config-if)#exit Medellin(config)#exit

Bogota	Bogota(config)#ip access-list standard Lan-Bogota Bogota(config-std-nacl)#permit 172.29.0.0 0.0.255.255 Bogota(config-std-nacl)#exit Bogota(config)#ip nat inside source list Lan-Bogota interface s0/0/0 overload Bogota(config)#int s0/0/0 Bogota(config-if)#ip nat outside Bogota(config-if)#exit Bogota(config)#int s0/0/1 Bogota(config-if)#ip nat inside Bogota(config-if)#exit Bogota(config)#int s0/1/0 Bogota(config-if)#ip nat inside Bogota(config-if)#exit Bogota(config)#int s0/1/1 Bogota(config-if)#ip nat inside Bogota(config-if)#exit Bogota(config)#exit

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 Medellín2 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín1.

c. Configurar la red Bogotá2 y Bogotá1 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.

Tabla 30 Configuración DHCP en Medellin2 y Bogota_2

Dispositivo	Configuración DHCP
Medellin2	Medellin2(config)#ip dhcp excluded-address 172.129.4.129 172.29.4.131 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)#exit Medellin2(config)#ip dhcp pool Medellin1 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 2.2.2.2 Medellin2(dhcp-config)#exit
Medellin1	Medellin1(config)#int g0/0 Medellin1(config-if)#ip helper-address 172.29.6.5

	Medellin1(config-if)#exit
Bogota_2	Bogota_2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 Bogota_2(config)#ip dhcp pool bogota_2 Bogota_2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota_2(dhcp-config)#default-router 172.29.1.1 Bogota_2(dhcp-config)#exit Bogota_2(config)#ip dhcp pool Bogota_1 Bogota_2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota_2(dhcp-config)#default-route 172.29.0.1 Bogota_2(dhcp-config)#end
Bogota_1	Medellin1(config)#int g0/0 Medellin1(config-if)#ip helper-address 172.29.3.13 Medellin1(config-if)#exit

Figura 17 Ping a las rutas sumarizadas

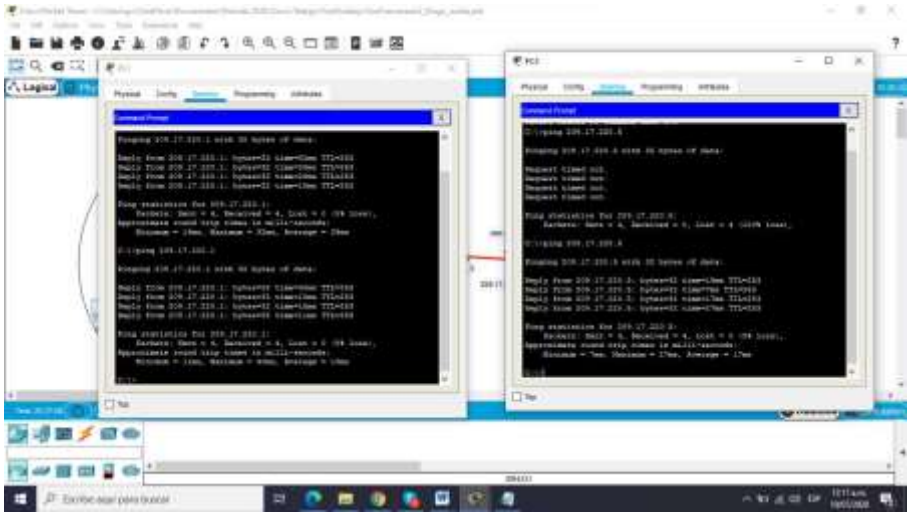


Figura 18 Verificación en los pc0 y pc2 la configuración DHCP

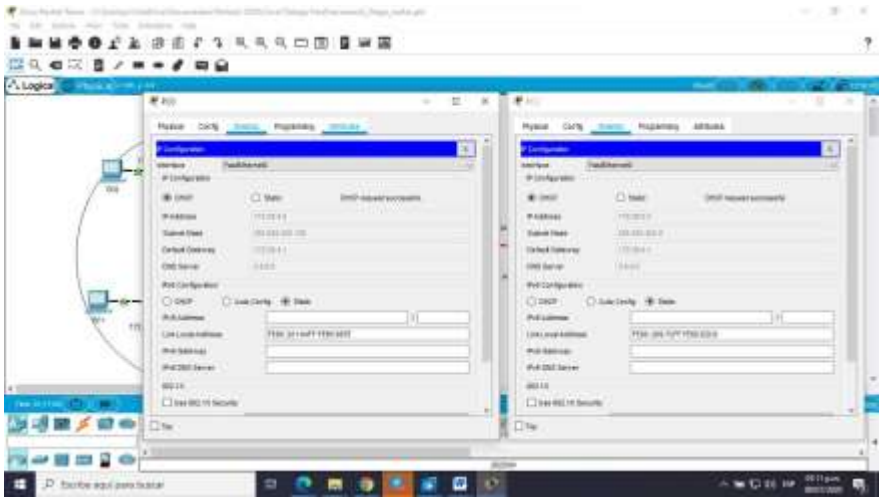


Figura 19 Escenario final 2.

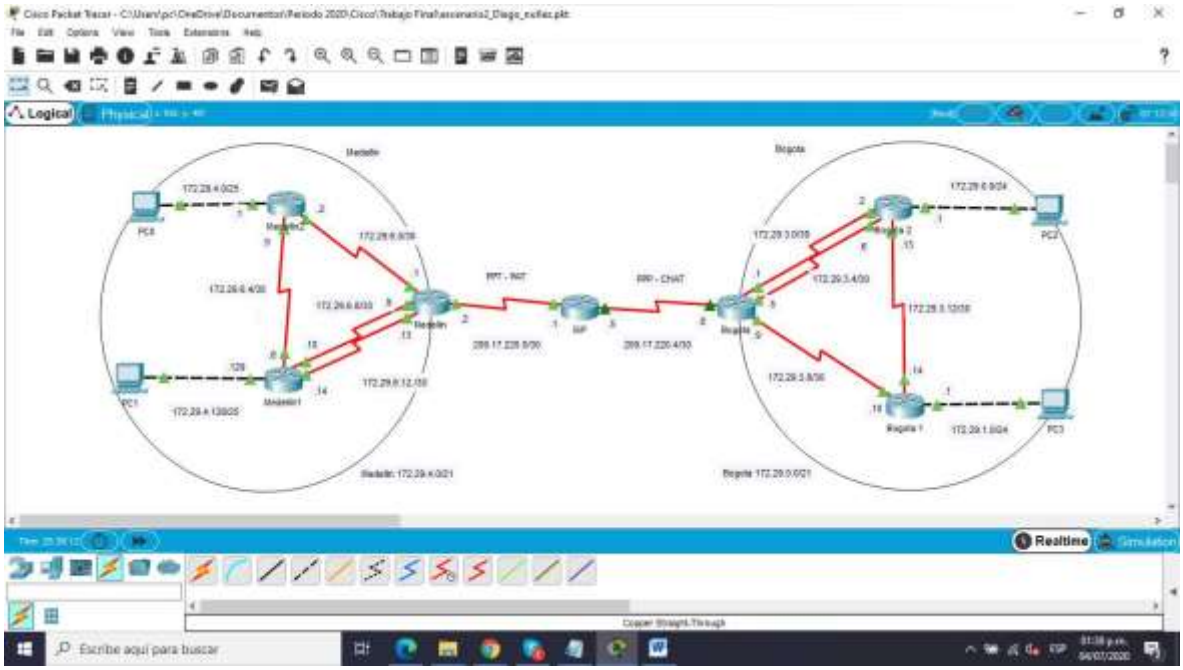
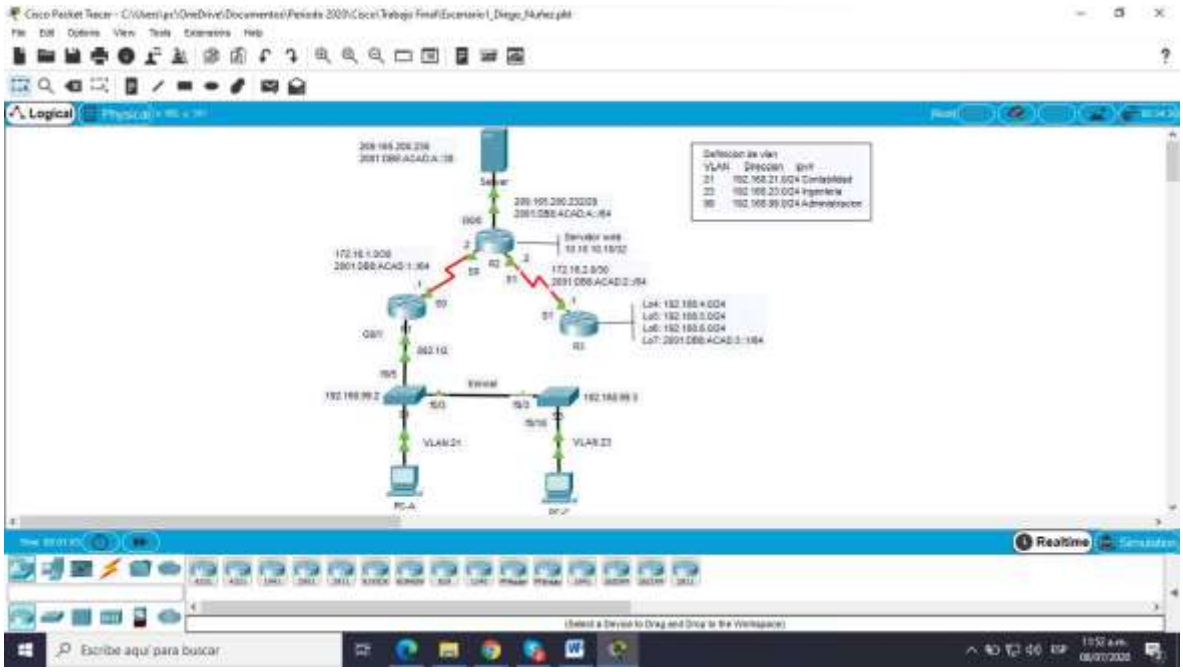


Figura 20 Escenario final 1



CONCLUSIONES

- Al desarrollar esta práctica se puedo concluir que existen protocolos fáciles de implementar, los cuales ayudan a establecer comunicación entre dispositivos que conforman una red, haciendo énfasis en router y switch y las cuales se pueden aplicar en redes ipv4 y ipv6

- La exigencia por parte de la Universidad Nacional Abierta y a Distancia UNAD permitió el crecimiento académico y de conocimientos para el manejo de la herramienta de Packet Tracer y GNS-3

- Los dos escenarios de estudio presentados en este trabajo son con el fin de dar a los estudiantes conocimientos a solución a un planteamiento en el mundo real, en el cual se basan las redes y las telecomunicaciones.

BIBLIOGRAFÍA

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). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

ISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

ANEXO

Link de los dos Escenarios propuestos de CCNA

https://drive.google.com/drive/folders/1qBUkkmpggQP1ewZtrJ_0g1cMQhtaG8e7?usp=sharing