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

MARTA ISABEL MUELAS TUNUBALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E INGENIERIAS
INGENIERIA DE SISTEMA
POPAYÁN
JULIO 2020

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

MARTA ISABEL MUELAS TUNUBALA

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN)

TUTOR:
GUSTAVO ADOLFO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E INGENIERIAS
INGENIERIA DE SISTEMAS
POPAYÁN

julio de 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

Este documento está plasmado el desarrollo de las pruebas de habilidades CCNA 2020 en el cual aplicaremos la teoría adquirida durante el periodo académico del Diplomado de Profundización de CISCO CCNA, donde mostraremos las habilidades y aptitudes adquiridas en temas como configuración básica de dispositivos, direccionamiento IPv4 e IPv6, conexión de redes, protocolos, entre otros.

La metodología de trabajo propuesto incluye dos escenarios, en los cuales se desarrollará los aspectos relacionados con la seguridad y diseño de las redes, configuración inicial básica de dispositivos, procesos de routing de capa 3, combinación de protocolos de routing dinámica y estática para la transferencia de paquetes de una red a otra, actualizaciones RIP, protocolos de routing de estado de enlace IPv4. De acuerdo a este temario en este documento se expondrá paso a paso el proceso en cada escenario, mediante los comandos utilizados para la configuración y la manera de verificación del correcto funcionamiento de la configuración con los diversos comandos show, donde se evidencia este proceso con capturas de pantallas.

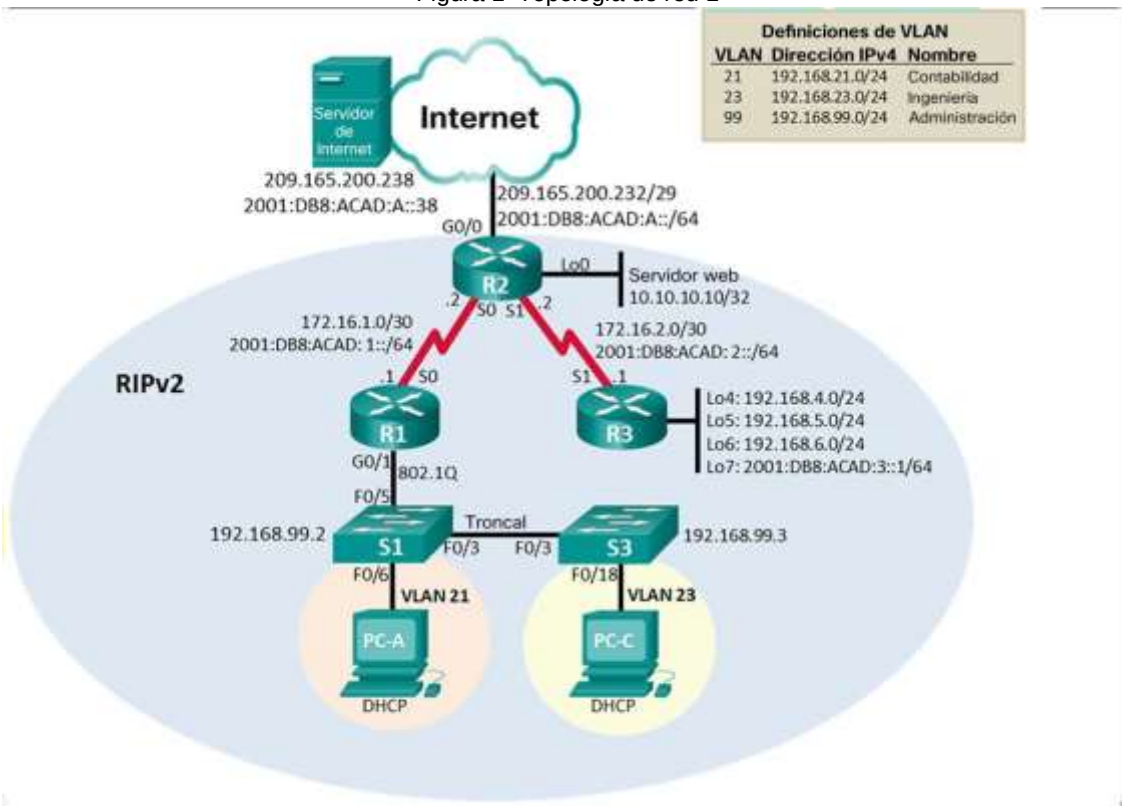
Cabe resaltar que el desarrollo de esta actividad se realiza en el programa Packer Tracer que es una gran herramienta de aprendizaje que nos permite desarrollar diversas simulaciones física y lógicas de redes, además nos permite comprender el funcionamiento de redes y como fluyen los datos, y de esta manera nos ayudara a mejorar nuestras habilidades y competencias.

Al final del documento se anexan las direcciones link de los proyectos de ambos escenarios desarrollados en Packer Tracer.

ESCENARIO 1:

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

Figura 1 Topología de red 1



Fuente: archivo prueba de habilidades.

1.1. PARTE1: INICIALIZAR DISPOSITIVOS

1.1.1. PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.
Como proceso inicial para la configuración de redes siempre es necesario realizar el proceso de inicialización y carga de los dispositivos, además es necesario

asegurarnos que los dispositivos en uso se hayan borrado y no tengan ninguna configuración de inicio. De lo contrario, los resultados podrán presentar fallas. para este proceso ingresara el comando erase startup-config que eliminará la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM). Cuando se haya finalizado la eliminación del archivo es necesario insertar el comando reload, este comando también cumple con la función de eliminar configuración antigua de la memoria; aparecerá el mensaje para continuar con la carga, se debe presionar Enter para confirmar. En caso de presionar otra tecla, se anulará la recarga.

En los switch debemos verificar que la base de datos de VLAN no esté en la memoria flash con el comando show flash, por tal razón es importante eliminar la base de datos Vlan presentes con el comando delete vlan.dat donde pide que se confirme el proceso. Con el comando show running-config en el modo EXEC privilegiado se puede verificar que un archivo de configuración este limpio.

Tabla 1 Inicialización y recarga de dispositivos

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router# erase startup-config
Volver a cargar todos los routers	Router# reload
Eliminar el archivo startup-config de todos los switches eliminar la base de datos de VLAN anterior	Switch# **erase startup-config** Switch# **delete vlan.dat** Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch# **reload** Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# **show flash**

Fuente: Comandos ingresados en Packer Tracer

1.2. PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

1.2.1. PASO 1: CONFIGURAR LA COMPUTADORA DE INTERNET

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

De acuerdo al escenario 1 con respecto a la computadora de Internet podemos identificar que están presentes dirección ipv4 de clase C y dirección IPv6

Tabla 2 Direccionamiento IPv4 - IPv6 de R2

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8: ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente propia

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.

1.2.2. PASO 2: CONFIGURAR R1

Para configurar el R1 se seguirán diferentes modos de configuración:

En el modo EXEC privilegiado se debe emitir el comando no ip domain-lookup que evitara las búsquedas de DNS no deseadas; es importante asignar un nombre a cada dispositivo para ello se usara el comando hostname y el nombre de la siguiente manera hostname R1; se continuara proporcionando un acceso seguro al modo

EXEC privilegiado con la asignación de una contraseña encriptada con el comando enable secret con el password class.

Además, se debe restringir el acceso al puerto de consola, ya que al no realizar esta restricción la configuración predeterminada no solicitará contraseña y permitirá todas las conexiones de consola y cualquier persona podrá fácilmente ingresar y generar peligro en la red. Esta contraseña será la primera que debemos ingresar para el modo EXEC del usuario.

También debemos configurar la VTY para que el router permita el acceso por Telnet. Si no se configura una contraseña de VTY, no se podrá acceder al router por medio de Telnet.

La Contraseña de acceso a la consola y acceso a VTY es cisco.
Luego pasaremos a encriptar todas estas contraseñas de texto no cifrado con el comando service password-encryption, encriptara todas las contraseñas anteriores y futuras, de esta manera se evitará que personas no autorizadas detecten las contraseñas.

Es importante configurar mensajes que cuando una persona inicia sesión en el router pueda ver el mensaje o también es útil cuando ingresan personas que no están autorizada y vean la advertencia de prohibición al acceso, son llamados mensajes del día o mensajes MODT con el comando banner motd seguido de comillas ira el mensaje que queremos que aparezca.

Se procederá a configurar las interfaces del router y a activarlos, en esta parte se configura la interface S0/0/0, se asignará la dirección Ipv4 e Ipv6, es necesario configurar una descripción de la interfaz donde indique a que dispositivo está conectada en este caso a R2. Se establecerá la frecuencia de reloj en 128000 debido a que el serial esta rotulado DCE, con el comando clock rate, finalmente se activará la interfaz con el comando no shutdown.

La configuración de rutas predeterminadas es importante debido a que especificaran el punto de salida que debe utilizar cuando la tabla de routing no presenta una ruta para la red de destino, en esta configuración se utilizó el comando de configuración global ip route 0.0.0.0 0.0.0.0 s0/0/0, con esta configuración se lograra una ruta predeterminada dirigida hacia los otros routers, un router enviara paquetes solamente a redes indicadas en la tabla de enrutamiento en caso de que la red no aparezca en la lista, el paquete se descartara. Debido a que esta red está configurada con direccionamiento IPv6 se configura una ruta IPv6 predeterminada de S0/0/0.

Después de realizar estas configuraciones es necesario guardar los archivos de configuración en la NVRAM con el comando copy running-conf startup-conf.
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configuración básica R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router (config)# no ip domain-lookup
Nombre del router	Router (config)# hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)# banner motd "¡Se Prohibe el acceso no autorizado" R1(config)# exit
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Establecer la frecuencia de reloj en 128000 Establecer la dirección IPv6 Activar la interfaz	R1(config)# interfaz S0/0/0 R1(config-if) # description link to R2 R1(config-if) # ip address 172.16.1.1 255.255.255.252 R1(config-if)# clock rate 128000 R1(config-if)# ip Ipv6 address 2001:DB8:ACAD:1::2/64 R1(config-if)# no shutdown
Rutas predeterminadas • Configurar una ruta IPv4 predeterminada de S0/0/0	R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0

• Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)# ipv6 route ::/0 S0/0/0

fuente Comandos ingresados en Packer Tracer

1.2.3. PASO 3: CONFIGURAR R2

En este paso se realizará la configuración inicial básica del router como la desactivación de la búsqueda DNS, asignación de nombre como R2, protección de acceso a la consola 0, consola vty con contraseña cisco, configuración de contraseña secreta de enable class, mensaje modt, encriptación de todas las contraseñas de texto no cifrado.

Solicita habilitar el servidor HTTP, pero el programa Packer Tracer no soporta por lo tanto se agrega un servidor web a la topología.

En el R2 se configura la interfaz S0/0/0 que va conectada con el R1 y la interfaz S0/0/1 conectada al R3, en esta interfaz se establece la frecuencia de reloj en 128000; la interfaz G0/0 va conectada a la Pc como servidor de internet. En la guía se solicita agregar Lo0 que es in interfaz virtual, pero debido a que Packer Tracer no soporta habilitar el servidor Http se optó por agregar un servidor que va conectada a la interfaz G0/1, se realizado la activación a todas las interfaces; se les asigno el direccionamiento Ipv4 e Ipv6.

Se configura una ruta IPv4 predeterminada de G0/0 y una ruta IPv6 predeterminada de G0/1 que está conectada al servidor de internet.

La configuración del R2 incluye las siguientes tareas:

Tabla 4 Configuración básica R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router (config)# no ip domain-lookup
Nombre del router	Router (config)# hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	No soporta.
Mensaje MOTD	R2(config)# banner motd “!Se prohíbe el acceso no autorizado!”
• Interfaz S0/0/0 • Establezca la descripción • Establezca la dirección IPv4. • Establezca la dirección IPv6. • Activar la interfaz	R2(config)# interfaz S0/0/0 R2(config-if)# description link to R1 R2(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64 R2(config-if)# no shutdown
• Interfaz S0/0/1 • Establecer la descripción • Establezca la dirección IPv4. • Establezca la dirección IPv6. • Establecer la frecuencia de reloj en 128000. • Activar la interfaz	R2(config)# interfaz S0/0/1 R2(config-if)# description link to R3 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config-if)# ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)# clock rate 128000 R2(config-if)# no shutdown
• 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)# description connection to internet R2(config-if)# ip address 209.165.200.233 255.255.255.248

• Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. • Activar la interfaz	R2(config-if)# ipv6 address 2001:DB8:ACAD:A::33/64 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 G0/1 R2(config-if)# description connection to servidor-web. R2(config-if)# ip address 10.10.10.1 255.255.255.0
• Ruta predeterminada • Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)# ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)# ipv6 route ::/0 G0/0

Fuente: Comandos ingresados en Packer Tracer.

1.2.4. PASO 4: CONFIGURAR R3

En este paso se realizará la configuración inicial básica del router como la desactivación de la búsqueda DNS, asignación de nombre como R3, protección de acceso a la consola 0, consola vty con contraseña cisco, configuración de contraseña secreta de enable con class, mensaje modt, encriptación de todas las contraseñas de texto no cifrado.

La configuración de la interface la interface S0/0/0, se asignará la dirección Ipv4 e Ipv6, es necesario configurar una descripción de la interfaz donde indique a que dispositivo está conectado en este caso a R2.

La interfaz Loopback se define como una interfaz lógica interna, no se asignan a un puerto físico por esta razón nunca se podrá conectar a otro dispositivo, automáticamente se coloca en estado activo siempre y cuando el router esté funcionando; la función de este tipo de interfaz es para probar procesos de routing interno por medio de la simulación de redes, además se pueden habilitar varias interfaces loopback, cada interfaz loopback se le asignará una dirección ip que será única. La configuración es similar a los otros tipos de interfaz. En el R3 se habilitan 3 interfaces Loopback con direccionamiento IPv4 y una con direccionamiento IPv6.

La configuración de una ruta IPv4 predeterminada de S0/0/1 y las configuraciones una ruta IPv6 predeterminada de S0/0/1

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configuración básica R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router (config)# no ip domain-lookup
Nombre del router	Router (config)# hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)# banner motd "¡Se Prohibe el acceso no autorizado"
• Interfaz S0/0/1 • Establezca la descripción • Establezca la dirección IPv4. • Establezca la dirección IPv6. • Activar la interfaz	R3(config)# interfaz S0/0/1 R3(config-if)# Description connection to R3 R3(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)# no shutdown
• Interfaz loopback 4	R3(config)# interfaz Lo4 R3(config-if)# ip address 192.168.4.1 255.255.255.0

• Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	
• Interfaz loopback 5 • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)# interface Lo5 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)#interface Lo6 R3(config-if)# ip address192.168.6.1 255.255.255.0 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 Lo7 R3(config-if)# ipv6 address 200:DB8:ACDA:3::1/64 R3(config-if)# exit
Rutas predeterminadas • Configurar una ruta IPv4 predeterminada de S0/0/1 • Configurar una ruta IPv6 predeterminada de S0/0/1	R3(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)# ipv6 route ::/0 S0/0/1

Fuente: Comandos ingresados en Packer Tracer.

1.2.5. PASO 5: CONFIGURAR S1

La configuración inicial básica del dispositivo switch incluye la desactivación de la búsqueda DNS, asignación de nombre como S1, protección de acceso a la consola 0, consola vty con contraseña cisco para ambas consolas, configuración de contraseña secreta de enable con class, mensaje modt con aviso para advertir la prohibición a las personas que accedan, encriptación de todas las contraseñas de texto no cifrado anteriores y futuras.

La configuración del S1 incluye las siguientes tareas:

Tabla 6 Configuración básica S1

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

Fuente: Comandos ingresados en Packer Tracer.

1.2.6. PASO 6: CONFIGURAR EL S3

La configuración inicial básica del dispositivo switch incluye la desactivación de la búsqueda DNS, asignación de nombre como S3, protección de acceso a la consola 0, consola vty con contraseña cisco para ambas consolas, configuración de contraseña secreta de enable con class, mensaje modt con aviso para advertir la prohibición a las personas que accedan, encriptación de todas las contraseñas de texto no cifrado anteriores y futuras.

La configuración del S3 incluye las siguientes tareas:

Tabla 7 Configuración básica S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch (config)# no ip domain-lookup
Nombre del switch	Switch (config)# hostname S3
Contraseña de exec privilegiado cifrada	S3 (config)#enable secret class
Contraseña de acceso a la consola	S3 (config)#line console 0 S3 (config-line)#password cisco S3 (config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)# banner motd "¡Se Prohibe el acceso no autorizado" S3(config)# exit

Fuente: Comandos ingresados en Packer Tracer

1.2.7. PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.
Con el comando ping se verifico la conectividad de R1 hacia R2 con los dos tipos de dirección que se configuro y dio un resultado de ping 5/5 quiere decir que, si hay conectividad, podemos verificar que la configuración realizada anteriormente es correcta.

Las demás pruebas como R2 a R3 y Pc de Internet a Gateway con correctas.
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

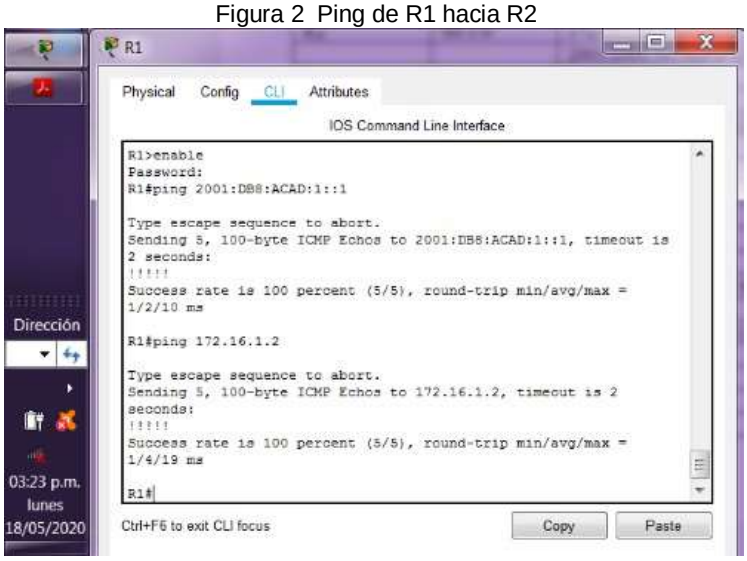
Tabla 8 Prueba de verificación

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::1	5/5
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	5/5
PC de Internet	Gateway predeterminado	209.165.200.233	4/4

Fuente: ping en los dispositivos

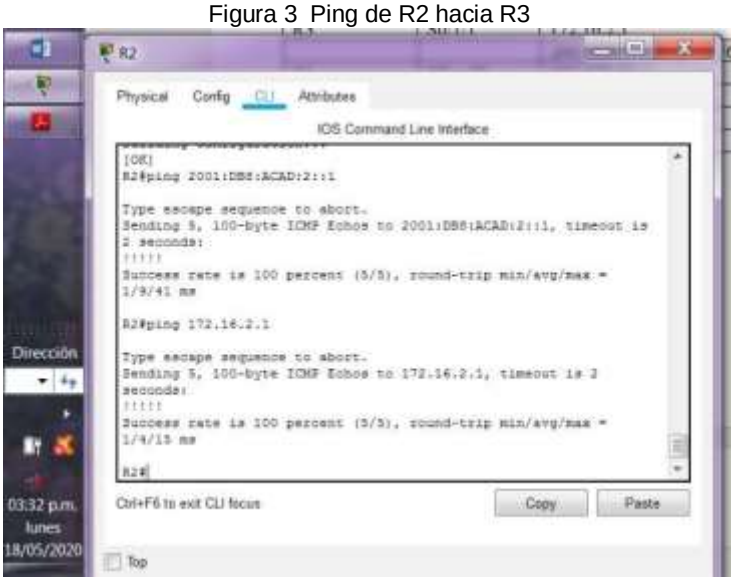
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente

Figura 2 Ping de R1 hacia R2



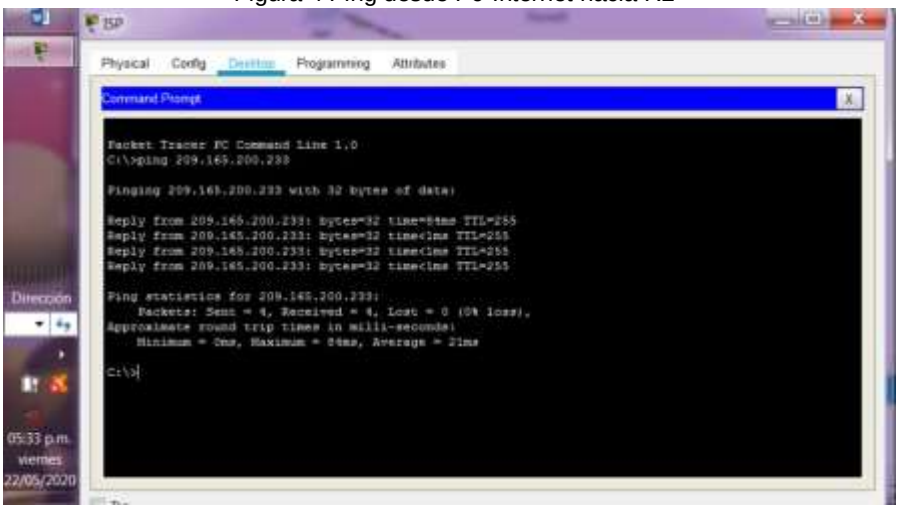
Fuente: propia

Figura 3 Ping de R2 hacia R3



Fuente: propia

Figura 4 Ping desde Pc-Internet hacia R2



Fuente: propia

1.3. PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

1.3.1. PASO 1: CONFIGURAR S1

VLAN: red de área local virtual, inicialmente las VLAN se utilizaban en redes LAN, actualmente se implementan en redes MAN y WAN; la VLAN se pueden agrupar dispositivos dentro de una red LAN, estos se comunican como si estuvieran

conectados al mismo cable, otra característica es que las VLAN se basan en conexiones lógicas en vez de conexiones físicas.

En esta red los dispositivos dentro de la VLAN van a funcionar como si estuvieran en su propia red. También se aplica la implementación del esquema de direccionamiento de red jerárquico es decir de manera ordenada se describe a continuación: vlan 21, 23 y 99; a cada VLAN se le debe asignar un nombre: contabilidad, ingeniería y administración respectivamente. Las dos primeras son VLAN de datos, estas están configuradas para transportar tráfico generado por los usuarios.

La VLAN 99 se configuro como una VLAN de administración, lo cual permitirá acceder a las capacidades de administración del switch; se le asignó una dirección IP con mascará de subred a la interfaz virtual de switch.

Es necesario asignar la primera dirección IPv4 de la subred como el Gateway predeterminado que identificara la conexión del router R1.
Para el correcto funcionamiento de esta red se debe habilitar el enlace troncal de VLAN, que se define como “un enlace de capa 2 en el modelo OSI entre dos switch que transporta el tráfico para todas las VLAN” Contador. (2019. pág., 98) Se puede restringir la lista de VLAN permitidas de forma manual o dinámica.

Para configurar la interfaz F0/3 y F0/5 que son extremos del enlace troncal se utilizara el comando switchport mode trunk que cambiara al modo de enlace troncal permanente, además se especificara la VLAN nativa 1 para el enlace troncal 802.1Q.

El resto de puertos se configura como puertos de acceso, utilizando el comando interface range y switchport mode Access.

Asignar F0/6 a la VLAN 21, con el comando switchport mode Access el cual cumple con la función de “colocar la interfaz en modo de enlace no troncal permanente y negocia para convertir el enlace en uno no troncal” Contador (2019. pág., 103); aunque la interfaz vecina sea una interfaz troncal.

Finalmente, por seguridad se deben apagar los puertos sin usar con el comando shutdown

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Enlace troncal S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name ingeniería S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name administración 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	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)#ip default-Gateway 192.168.99.1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/3. Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switch mode trunk S1(config-if)#Switch trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5. Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switch mode trunk S1(config-if)#Switch trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#int range fa0/1-2, fa0/4, fa0/7-24, G0/1-2 S1(config-if-range)#switch mode access

Utilizar el comando interface rango	
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switch mode access S1(config-if)#switch Access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range fa0/1-2, fa0/4, fa0/7-24, G0/1-2 S1(config-if)#shutdown S1(config-if)#exit

Fuente: Comandos ingresados en Packer Tracer

1.3.2. PASO 2: CONFIGURAR EL S3

En el Switch 3 se habilitaron las siguientes VLAN 21, 23 y 99; a cada VLAN se nombraron a cada una como: contabilidad, ingeniería y administración respectivamente. Las dos primeras son VLAN de datos, estas están configuradas para transportar tráfico generado por los usuarios.
En la VLAN 99 se configuro como VLAN de administración, lo cual permitirá acceder a las capacidades de administración del switch; se le asignó una dirección IP con mascará de subred a la interfaz virtual de switch.
También se asigna la primera dirección IPv4 de la subred como el Gateway predeterminado que identificara la conexión del router R1.
La interfaz F0/3 de S3 es el otro extremo del enlace troncal por lo tanto se realiza la configuración para que cambie al modo de enlace troncal permanente utilizando el comando switchport mode trunk, se especifica la VLAN nativa 1 para el enlace troncal 802.1Q.
El resto de puertos se configura como puertos de acceso, utilizando el comando interface range y switchport mode Access.
Asignar F0/18 a la VLAN 23, con el comando switchport mode Access, finalmente se deben apagar los puertos sin uso.

La configuración del S3 incluye las siguientes tareas:

Tabla 10 Enlace troncal S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name ingeniería S3(config-vlan)#exit

se indican Dé nombre a cada VLAN.	S3(config)#vlan 99 S3(config-vlan)#name administración S3(config-vlan)#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)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(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 S3(config)#exit
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config)#int range fa0/1-2, fa0/4-17, fa0/19-24, G0/1-2 S3(config-if-range)#switch mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23	S3(config)#int f0/18 S3(config-if)#switch mode access S3(config-if)#switch Access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#int range fa0/1-2, fa0/4-17, fa0/19-24, G0/1-2 S3(config-if)#shutdown S3(config-if)#exit

Fuente: Comandos ingresados en Packer Tracer

1.3.3. PASO 3: CONFIGURAR R1

En la configuración de la subinterfaz 802.1Q.21, la subinterfaz se crea con el comando interfaz seguida de la id_interfaz física luego la id_subinterfaz, luego se debe configurar la subinterfaz de modo que funciones en una VLAN especifica con el comando encapsulation dot1q VLAN_id, luego se le debe asignar una dirección

Ip a la subinterfaz, finalmente se debe activar la interfaz física con el comando no shutdown.
En R1 se configura la subinterfaz 802.1Q .21 en G0/1 con descripción: LAN de Contabilidad y se asigna a la VLAN 21, la subinterfaz 802.1Q .23 en G0/1 con descripción: LAN de Ingeniería y se asigna la VLAN 23, se debe configurar la subinterfaz 802.1Q .99 en G0/1, en estas tres se debe asignar la primera dirección disponible a cada interfaz; finalmente activar la interfaz G0/1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuración subinterfaz 802.1Q

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int G0/1.21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#description link to contabilidad R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#int G0/1.23 R1(config-subif)#encapsulation dot1q 23 description link to ingenieria R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int G0/1.99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#description link to Administracion R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int G0/1 R1(config-if)#no shutdown R1(config-if)#exit

Fuente: Comandos ingresados en Packer Tracer

1.3.4. PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

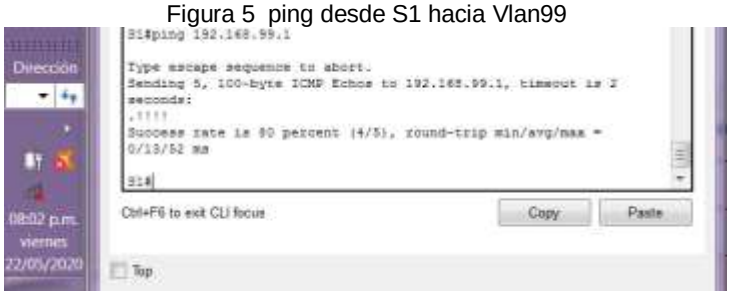
Al realizar el proceso de verificación de la conectividad de la tres mediante el comando ping podemos notar que los resultados son exitosos.

Tabla 12 Verificación de la conectividad de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	4/5
S3	R1, dirección VLAN 99	192.168.99.1	4/5
S1	R1, dirección VLAN 21	192.168.21.1	5/5
S3	R1, dirección VLAN 23	192.168.23.1	5/5

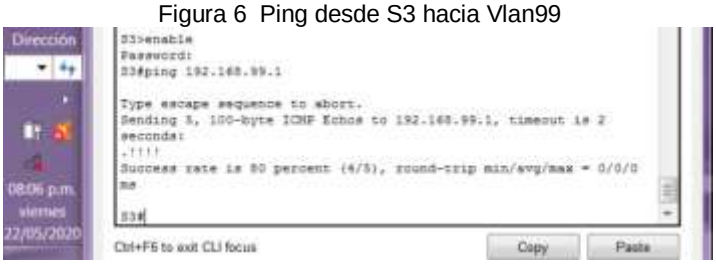
Fuente: Ping en los dispositivos

Figura 5 ping desde S1 hacia Vlan99



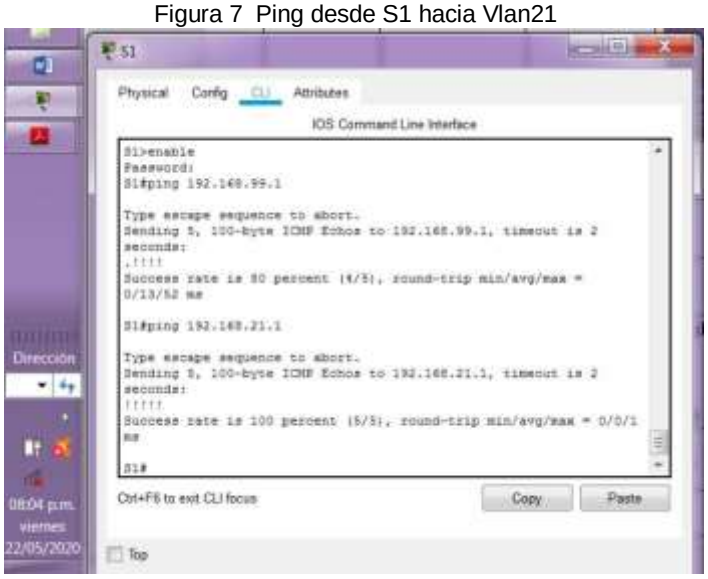
Fuente: propia

Figura 6 Ping desde S3 hacia Vlan99



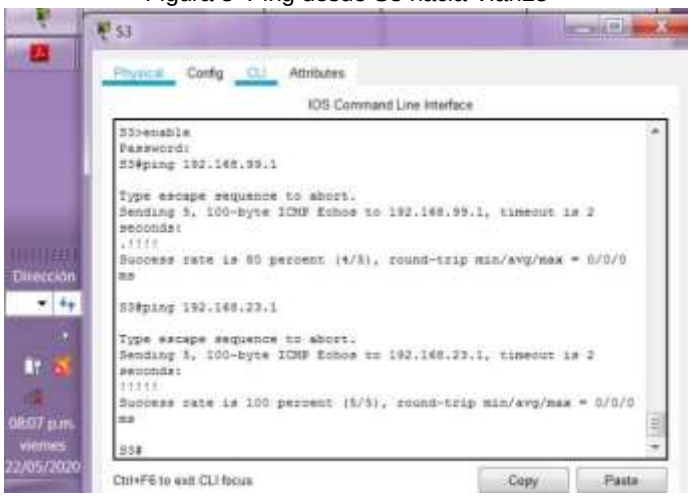
Fuente: propia

Figura 7 Ping desde S1 hacia Vlan21



Fuente: propia

Figura 8 Ping desde S3 hacia Vlan23



Fuente: propia

1.4. PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

1.4.1. PASO 1: CONFIGURAR RIPV2 EN EL R1

El protocolo de routing dinámico RIPv2: hace parte de los protocolos de routing vector distancia, se caracteriza porque comparten actualizaciones entre vecinos, los

cuales son routers que comparten un enlace, su configuración es para usar el mismo protocolo de enrutamiento. El protocolo RIPv2 utiliza direcciones de multidifusión de esta manera reciben actualizaciones solamente los vecinos que la requieran. Se diferencia de los otros protocolos porque es un protocolo de routing sin clase, presenta mayor eficiencia, entradas de routing reducidas, protección de las actualizaciones.

Usa el conteo de saltos como métrica, la desventaja es que la cantidad máxima es de 15 saltos. La distancia administrativa es de 120.
Para la configuración de este protocolo se debe iniciar habilitando RIP con el comando router rip, permitiendo el acceso al modo de configuración del router, luego se debe habilitar el routing RIP para una red, pero es necesario emitir el comando versión 2 para habilitar RIPv2, esta es importante ya que hará que sea un protocolo de routing sin clase.

Con el comando network dirección_red, para introducir todas las direcciones de red que están conectadas al router directamente, de esta manera se habilita el RIP en todas las interfaces que pertenecen a la red, ahora las interfaces asociadas ya pueden enviar y recibir actualizaciones RIP.

El comando passive-interface es útil para evitar que las actualizaciones de routing se comuniquen por medio de una interfaz del router, aun así, esa red se seguirá anunciando a los otros routers.
Para desactivar la sumarización automática en el modo de configuración del router utilizar el comando no auto-summary, esto permite que RIPv2 ya no resume las redes en su dirección con clase en los routers fronterizos, ya que incluye todas las subredes y sus máscaras en sus actualizaciones.

En el R1 se configura RIP versión 2, se anuncian todas las redes conectadas directamente a este router, en este caso son 4, se establecen solamente las interfaces LAN como pasivas y se desactiva la sumarización automática.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configuración RIP en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#versión 2
Anunciar las redes conectadas directamente	R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0 R1(config-router)#network 172.16.1.0

Asigne todas las redes conectadas directamente.	
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface G0/1.21 R1(config-router)#passive-interface G0/1.23 R1(config-router)#passive-interface G0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Fuente: Comandos ingresados en Packer Tracer

1.4.2. PASO 2: CONFIGURAR RIPV2 EN EL R2

En el R2 se configura RIP versión 2, se anuncian todas las redes conectadas directamente a este router, en este caso son 3 y se omite la red perteneciente G0/0 debido a que dicha red es externa, se solicita establecer la interfaz LAN (loopback) como pasiva, pero en nuestro caso se aplicó a la red G0/1 (Packer Tracer no soporta servidor http) y se desactiva la sumarización automática.

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configuración RIP en R2

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#versión 2
Anunciar las redes conectadas directamente. **Nota:** Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface G0/1
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Fuente: Comandos ingresados en Packer Tracer

1.4.3. PASO 3: CONFIGURAR RIPV2 EN EL R3

En el R3 se configura RIP versión 2, se anuncian todas las redes conectadas directamente a este router con direccionamiento IPv4, en este caso son 4, una que va dirigida hacia el router R2 y las tres otras son las redes loopback (se omite la loopback con direccionamiento IPv6); igualmente estas 3 redes LAN se establecen como pasiva, finalmente se desactiva la sumarización automática.

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configuración RIP en R3

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#versión 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0 R3(config-router)#network 172.16.2.0
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

Fuente: Comandos ingresados en Packer Tracer

1.4.4. PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

El comando show ip protocols, presenta diversas funciones entre las cuales se pueden verificar la configuración RIP y la versión que se habilito, aquí podemos apreciar que la versión de RIP configurada es RIPv2; se puede apreciar los diversos valores de los temporizadores, la sumarización de red automática no está operativa porque se deshabilito la sumarización automática, podemos ver que R1 envía la siguiente actualización de routing en 4 segundos. También se puede apreciar las redes con clase que anuncia R1 y las que incluye en sus actualizaciones. Se identifican las interfaces pasivas configuradas en R1.

Finalmente observamos la dirección IP del siguiente salto, la distancia administrativa que es de 120 y el momento en que el R2 recibió la última actualización.

El comando show ip route rip muestra las rutas instaladas en la tabla de routing, como se muestra en la figura (). solo se indican las redes RIP.
Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 16 Comandos de verificación.

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?	R1#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R1# show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Se pueden usar los siguientes comandos debug ip rip, show ip protocols y show run

Fuente: propia

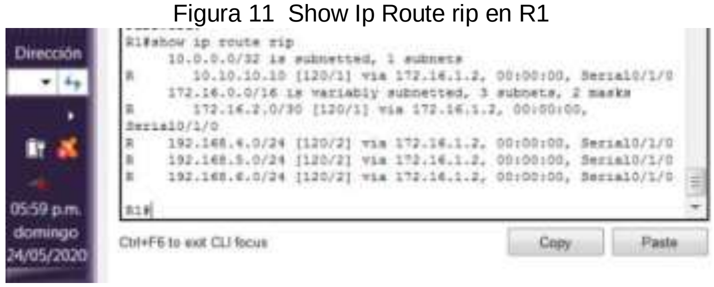
Figura 9 Show Ip Protocols enR1

Fuente: propia

Figura 10 Debug in rip en R1

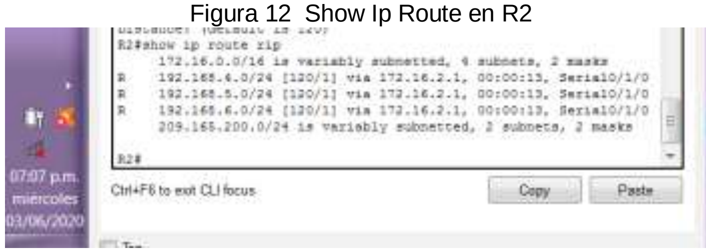
Fuente: propia

Figura 11 Show Ip Route rip en R1



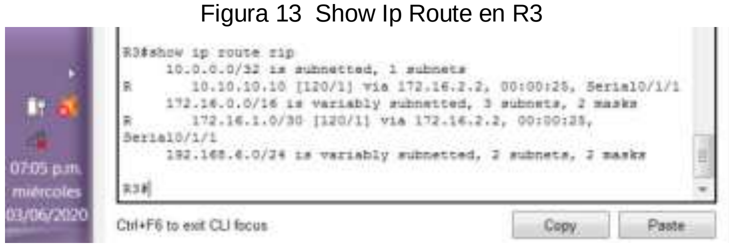
Fuente: propia

Figura 12 Show Ip Route en R2



Fuente: propia

Figura 13 Show Ip Route en R3



Fuente: propia

1.5. PARTE 5: TRANSACCIÓN IMPLEMENTAR DHCP Y NAT PARA IPV4

1.5.1. PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

El protocolo de configuración dinámica de host (DHCP), en una red que simplifica el tema de la asignación de direccionamiento IP en diversos dispositivos PC, otra ventaja de uso de servidor de DHCP centralizado proporciona la administración de todas las asignaciones de dirección IP, desde un servidor único.

El protocolo DHCP está disponible para direccionamiento IPv4 e IPv6.

Para iniciar la configuración del protocolo DHCP en el router es necesario activar el servicio DHCP con el comando service DHCP; en algunas redes tienen configuradas en algunos dispositivos direcciones ip estáticas, las cuales no pueden ser asignadas en otros dispositivos, por lo tanto, estas deben se excluidas por medio del comando ip dhcp excluded-address.

En toda configuración DHCP es necesario definir un conjunto de direcciones que se deben asignar, para ello utilizamos el comando ip dhcp pool ACCT, en esta parte se crea un pool con un nombre y el router pasa al modo de configuración dhcp-config.

En este modo se puede definir el rango de direcciones disponibles en la red con el comando network seguida de la dirección de red y la máscara de subred.

También es importante definir el Gateway predeterminado, que por lo general es la interfaz LAN del router que se encuentra más cerca a los dispositivos, con el comando default-router.

El comando dns-server seguida de la dirección ip del servidor DNS disponible, además se puede definir el nombre del dominio con el comando domain-name y asignar el nombre.

En el R1 se reservaron las primeras 20 direcciones IP en la VLAN 21 y las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas.

Se crea un pool de DHCP para la VLAN 21 con nombre: ACCT y la VLAN 23 se crear un pool de DHCP con el nombre: ENGNR, se emite el servidor DNS con la dirección ip 10.10.10.10 del servidor, también se genera nombre de dominio: ccna-sa.com, para la VLAN 21 se establece el Gateway predeterminado 192.168.21.1 y para la VLAN 23 el Gateway predeterminado 192.168.23.1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configuración DHCP en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#service DHCP 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)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 • Nombre: ENGNR • Servidor DNS: 10.10.10.10 • Nombre de dominio: ccna-sa.com • Establecer el Gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

Fuente: Comandos ingresados en Packer Tracer

1.5.2. PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

Hoy en día todas las empresas cuentan con diversos dispositivos y cada uno de ellos contiene direcciones Ip los cuales se consideran direcciones privadas que permiten la comunicación local, pero estas direcciones privadas no se pueden enrutar a través de Internet; para lograr que un dispositivo con este tipo de dirección

permita acceder a recursos o dispositivos de redes externas primero es necesario ejecutar la traducción de direcciones de red (NAT), es decir traducir la dirección privada a una dirección pública.

Una única dirección IPv4 publica se puede compartir con miles de dispositivos y cada uno configurado con una dirección privada.
La función principal de la NAT es conservar las direcciones IPv4 públicas, se consigue al permitir que las redes utilicen direcciones privadas internas, cuando se realiza la traducción a una dirección pública solamente en casos necesarios, la NAT también permite un alto grado de privacidad y seguridad a la red porque oculta las direcciones internas de las redes externas.

La NAT presenta tres tipos de traducciones:

NAT estática: permite la asignación de direcciones uno a uno entre una dirección local y una dirección global; la NAT estática en los servidores web debe tener una dirección constante y esta debe ser accesible desde internet y el servidor web de la empresa.

La NAT dinámica: permite la asignación de varias direcciones varias direcciones entre locales y globales. Utiliza un conjunto de direcciones públicas, se asigna según el orden de llegada; en el momento que un dispositivo interno busca acceso a una red externa la NAT dinámica asigna una dirección pública del conjunto que esté disponible.

La traducción de la dirección del puerto (PAT): permite la asignación de varias direcciones a una dirección entre locales y globales.
Para la configuración de la NAT estática inicialmente se debe establecer la traducción estática entre una dirección local interna y una dirección global interna con el comando ip nat inside source static seguida de la ip-local y la ip global.
Se debe especificar la interfaz interna con el correspondiente comando, es necesario marcar la interfaz como conectada al interior ip nat inside, luego salir del modo de configuración de la interfaz con el comando exit.
Pasamos a marcar la interfaz como conectada al exterior con ip nat outside.

Para la configuración de la NAT dinámica, primero se debe definir el conjunto de direcciones esta se utilizará para la traducción, el conjunto de las direcciones públicas se define señalando la primera y la última dirección IP. Con el comando ip nat pool seguido del nombre y el conjunto de direcciones con netmask.
Se define la traducción dinámica NAT para configurar la ACL al conjunto para ello se emite el comando ip nat inside source list numero-lista-acceso pool nombre-conjunto.

Posteriormente se pasa a identificar la interfaz que se conecten a la red interna y también la interfaz que se conecte con la red externa.

En la configuración del R2 inicialmente se crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser, Contraseña: cisco12345, Nivel de privilegio: 15.

Se crea una NAT estática al servidor web. Con dirección global interna: 209.165.200.229, se asigna la interfaz interna y externa para la NAT estática; como interfaz interna se establece G0/1 y la interfaz externa G0/0.
Se configura la NAT dinámica dentro de una ACL privada, con lista de acceso: 1, se permite la traducción de las redes de Contabilidad y de Ingeniería en el R1 y se permitir la traducción de un resumen de las redes LAN (loopback) en el R3.
Se define el pool de direcciones IP públicas utilizables con el nombre del conjunto: INTERNET y el conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228

Finalmente se define la traducción de NAT dinámica

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configuración NAT en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	R2(config)# User webuser privilege 15 secret cisco12345 R2(config)# exit
Habilitar el servicio del servidor HTTP	Ip http server (no soportado en PKT)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.229**	R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)# exit
Asignar la interfaz interna y externa para la NAT estática	R2(config)# interface G0/1 R2(config-if)# ip nat inside R2(config-if)# interface G0/0

	R2(config-if)# ip nat outside 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 192.168.0.0 0.0.0.255 R2(config)# exit
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**	R2(config)# ip nat pool INTERNET 209.165.200.225 – 209.165.200.228 netmask 255.255.255.248 R2(config)# exit
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET R2(config)#interface G0/1 R2(config)#ip nat inside R2(config)#interface s0/0/0 R2(config)#ip nat outside

Fuente: Comandos ingresados en Packer Tracer

1.5.3. PASO 3: VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

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

Tabla 19 Verificación de protocolos DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ip address 192.168.21.21 Mascara de subred 255.255.255.0 Default gateway 192.168.21.1 DNS-server 10.10.10.10

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ip address 192.168.23.21 Mascara de subred 255.255.255.0 Default gateway 192.168.23.1 DNS-server 10.10.10.10
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	exitoso
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**	Exitoso

Fuente: propia

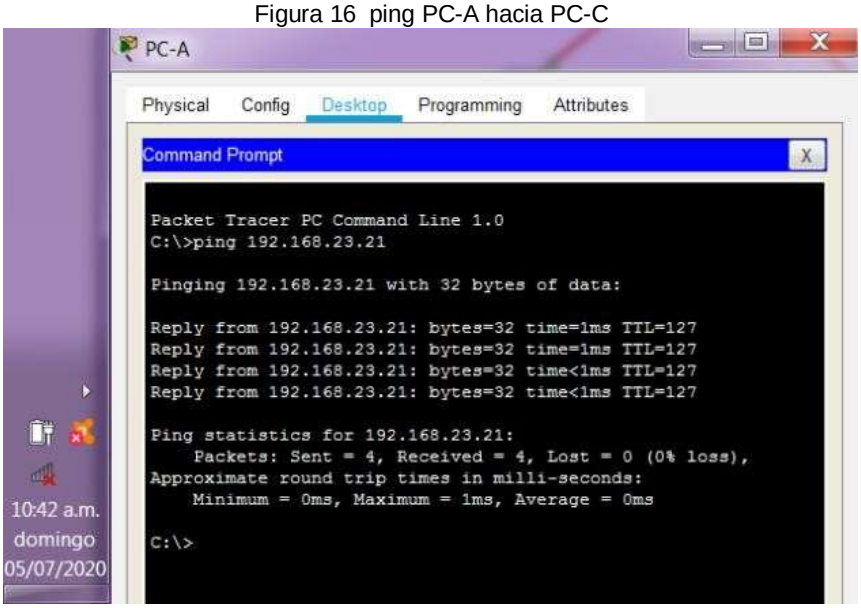
Figura 14 Direccionamiento PC-A

Fuente: propia

Figura 15 Direccionamiento PC-C

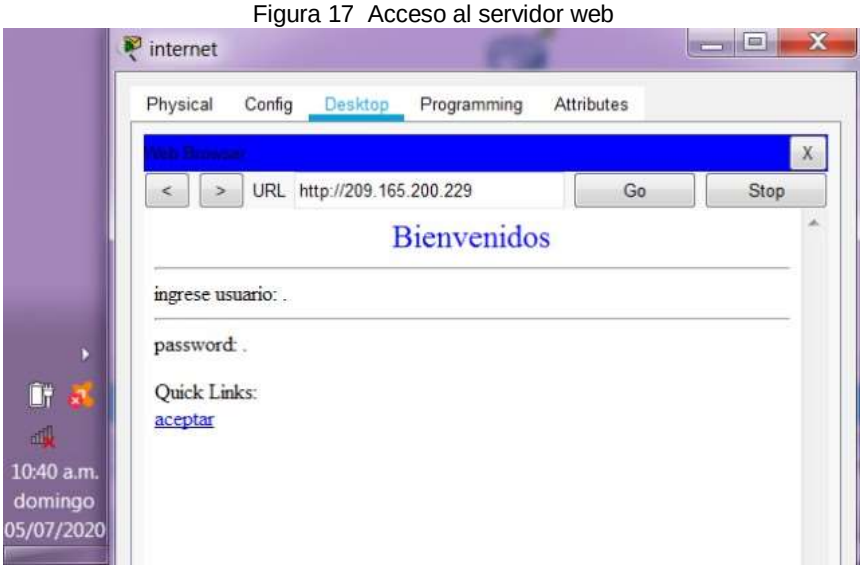
Fuente: propia

Figura 16 ping PC-A hacia PC-C



Fuente: propia

Figura 17 Acceso al servidor web



Fuente: propia

1.6. PARTE 6: CONFIGURAR NTP

El protocolo de tiempo de red (NTP) es un protocolo que permita que los dispositivos de red sincronicen la configuración de la hora con un servidor NTP. Los dispositivos de la red pueden configurar como servidor NTP o cliente NTP.

Para que un servidor horario NTP permita la sincronización del reloj de software se debe usar el comando ntp server dirección-IP en el cliente NTP, también se debe

configurar un dispositivo con un reloj maestro NTP para que los peers puedan sincronizar con el comando ntp master capa; el valor de la capa va de 1 a 15.
Para iniciar con la configuración NTP es necesario ajustar la fecha y hora en R2 con la fecha 5 de marzo de 2016, 9 a.m.

Se configura R2 como un maestro NTP con capa o nivel de estrato: 5. Al R1 se configura como un cliente NTP y se asigna la dirección Gateway de R2 como servidor.

En R1 se configura para actualizaciones de calendario periódicas con hora NTP. Finalmente, con el comando do show ntp status se verifica la configuración de NTP en R1.

Tabla 20 Configuración NTP en R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	R2#clock set 9:00:00 05 Mar 2016
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(config)#do show ntp status

Fuente: Comandos ingresados en Packer Tracer

1.7. PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

1.7.1. PASO 1: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Las listas de control de acceso (ACL), “es una lista secuencial de instrucciones que permit (permitir) o deny (denegar) que se aplican a los protocolos de capa superior o a las direcciones”, Contador (2019. pág., 495); es muy útil para controlar el tráfico hacia y desde la red, también se puede configurar ACL para los protocolos de red enrutada, es importante configurar ACL porque proporciona seguridad en la red.

La lista de acceso se debe configurar con un nombre para permitir que el R1 establezca una conexión Telnet con R2, en este caso se nombra la ACL como ADMIN-MGT.

Las ACE pueden permitir o denegar un solo host o un rango de direcciones host, esta configuración se aplica la ACL con nombre a las líneas VTY, permitiendo al host 172.16.1.1 el acceso por Telnet a las líneas de VTY.

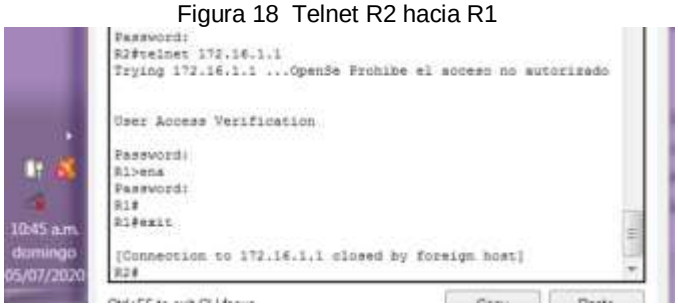
Para verificar que la ACL funciones correctamente podemos probar en R2 emitiendo telnet 172.16.1.1, vemos que hace la prueba y luego ingresa a R1 solicita el password y entramos a R1

Tabla 21 Configuración ACL en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: **ADMIN-MGT**	R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Verificar que la ACL funcione como se espera	Si funciona

Fuente: Comandos ingresados en Packer Tracer

Figura 18 Telnet R2 hacia R1



Fuente: propia

1.7.2. PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

Con el comando show Access-lists nos muestra una lista de acceso permitidas como las VLAN 21 y 23, y el resumen de la red loopback del R3, adicional a estos se agregó el acceso por Telnet a las líneas de VTY desde R2 hacia R1.

Tabla 22 Comandos de verificación NAT.

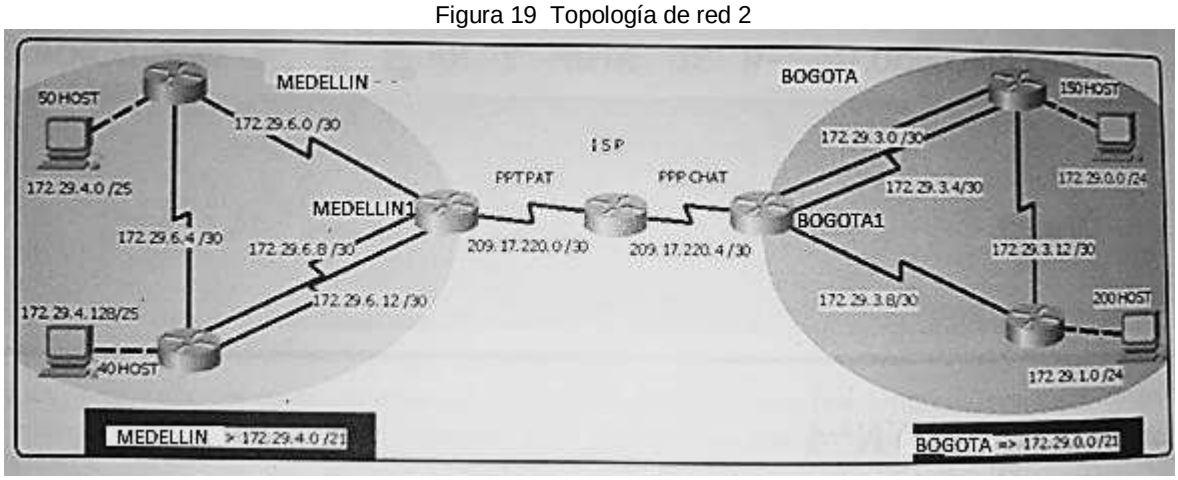
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show Access-lists
Restablecer los contadores de una lista de acceso	R2#clear access list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Interface G0/0 ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	show ip nat 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?	Clear ip nat translations

Fuente: propia

ESCENARIO 2

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

Figura 19 Topología de red 2



Fuente archivo prueba de habilidades

2.1. DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

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

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

NOTA: en esta parte inicial se siguieron los siguientes parámetros básico de configuración para todos los routers.

En esta actividad se inicializo con la eliminación de la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM) con el comando erase startup-config. Cuando se haya finalizado la eliminación del archivo es necesario insertar el comando reload para la recarga del dispositivo.

En el siguiente paso se realizará la configuración inicial básica de los routers como la desactivación de la búsqueda DNS aplicando el comando router(config)#no ip

domain-lookup, asignación de nombre con el comando router(config)#hostname seguida del nombre en el modo de configuración global.

Los nombres asignados a los routers son los siguientes: ISP, Medellin1, Medellin2, Medellin3, Bogota1, Bogota2, y Bogota3.

Para la protección del modo de acceso al modo privilegiado se estableció como contraseña class:

Se realizó la protección de acceso seguro a la línea de consola se accedió al modo config-line y se asignó la contraseña de consola cisco.

Para poder acceder al dispositivo mediante Telnet se debe configurar la VTY una contraseña “cisco”.

Se configuro un mensaje modt para que las personas vayan a iniciar sesión puedan ver el mensaje de advertencia "¡Se Prohibe el acceso no autorizado"

Se realizó la configuración de la encriptación de todas las contraseñas de texto no cifrado anteriores y futuras.

Se debe guardar el archivo de configuración en el modo EXEC privilegiado.

Tabla 23 Configuración básica de los dispositivos

Dispositivo	**Configuración básica**
ISP	Router(config)#no ip domain-lookup Router(config)#hostname ISP ISP(config)#enable secret class 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 ISP(config-line)#service password-encryption ISP(config)#banner motd "Se Prohibe el acceso no autorizado" ISP(config)#exit ISP(config)# copy running-conf startup-conf
Medellin1	Router(config)#no ip domain-lookup Router(config)#hostname Medellin1 Medellin1(config)#enable secret class 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 Medellin1(config-line)#service password-encryption Medellin1(config)#banner motd "Se Prohibe el acceso no autorizado" Medellin1(config)#exit Medellin1# copy running-conf startup-conf
Medellin2	Router(config)#no ip domain-lookup Router(config)#hostname Medellin2 Medellin2(config)#enable secret class 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 Medellin2(config-line)#service password-encryption Medellin2(config)#banner motd "Se Prohibe el acceso no autorizado" Medellin2(config)#exit Medellin2# copy running-conf startup-conf
Medellin3	Router(config)#no ip domain-lookup Router(config)#hostname Medellin3 Medellin3(config)#enable secret class 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 Medellin3(config-line)#service password-encryption Medellin3(config)#banner motd "Se Prohibe el acceso no autorizado" Medellin3(config)#exit Medellin3# copy running-conf startup-conf
Bogota1	Router(config)#no ip domain-lookup Router(config)#hostname Bogota1 Bogota1(config)#enable secret class 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 Bogota1(config-line)#service password-encryption Bogota1(config)#banner motd "Se Prohibe el acceso no autorizado"

	Bogota1(config)# Bogota1(config)#exit Bogota1# copy running-conf startup-conf
Bogota2	Router(config)#no ip domain-lookup Router(config)#hostname Bogota2 Bogota2(config)#enable secret class 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 Bogota2(config-line)#service password-encryption Bogota2(config)#banner motd "Se Prohibe el acceso no autorizado" Bogota2(config)# Bogota2(config)#exit Bogota2# copy running-conf startup-conf
Bogota3	Router(config)#no ip domain-lookup Router(config)#hostname Bogota3 Bogota3(config)#enable secret class 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 Bogota3(config-line)#service password-encryption Bogota3(config)#banner motd "Se Prohibe el acceso no autorizado" Bogota3(config)#exit Bogota3#copy running-conf startup-conf

Fuente: Comandos ingresados en Packer Tracer

Realizar la conexión física de los equipos con base en la topología de red

De acuerdo a la topología propuesta se asignó la dirección ip a cada una de las interfaces, ingresando al modo de configuración global se debe emitir comandos de direccionar y activar las interfaces; para toda la red se establece la dirección IPv4; también de configuro una descripción en cada interfaz que indica a que dispositivo está conectada.

Nota: se establece la frecuencia de reloj en 128000 en las interfaces seriales con DSL.

Tabla 24 direccionamiento IPv4

Isp	S0/0/0	Bogota1	209.17.220.5	255.255.255.252	209.17.220.4/30
Isp	S0/1/0	Medellin1	209.17.220.1	255.255.255.252	209.17.220.0/30
Medellin1	S0/1/0	ISP	209.17.220.2	255.255.255.252	209.17.220.0/30
Medellin1	S0/0/0	Medellin2	172.26.6.1	255.255.255.252	172.26.6.0/30
Medellin1	S0/0/1	Medellin3	172.29.6.9	255.255.255.252	172.29.6.8/30
Medellin1	S0/1/1	Medellin3	172.29.6.13	255.255.255.252	172.29.6.12/30
Medellin2	S0/0/0	Medellin1	172.26.6.2	255.255.255.252	172.26.6.0/30
Medellin2	S0/0/1	Medellin3	172.29.6.5	255.255.255.252	172.29.6.4/30
Medellin2	G0/0	PC-A	172.29.4.1	255.255.255.128	172.29.4.0/25
Medellin3	S0/0/1	Medellin2	172.29.6.6	255.255.255.252	172.29.6.4/30
Medellin3	S0/1/0	Medellin1	172.29.6.14	255.255.255.252	172.29.6.12/30
Medellin3	S0/0/0	Medellin1	172.29.6.10	255.255.255.252	172.29.6.8/30
Medellin3	G0/0	PC-B	172.29.4.129	255.255.255.128	172.29.4.128/25
Bogota1	S0/0/0	ISP	209.17.220.6	255.255.255.252	209.17.220.4/30
Bogota1	S0/0/1	Bogota3	172.29.3.1	255.255.255.252	172.29.3.0/30
Bogota1	S0/1/0	Bogota2	172.29.3.9	255.255.255.252	172.29.3.8/30
Bogota1	S0/1/1	Bogota3	172.29.3.5	255.255.255.252	172.29.3.4/30
Bogota2	S0/0/1	Bogota1	172.29.3.10	255.255.255.252	172.29.3.8/30
Bogota2	S0/0/0	Bogota3	172.29.3.13	255.255.255.252	172.29.3.12/30
Bogota2	G0/0	PC-D	172.29.1.1	255.255.255.0	172.29.1.0/24
Bogota3	S0/0/0	Bogota2	172.29.3.14	255.255.255.252	172.29.3.12/30

Bogota3	S0/1/0	Bogota1	172.29.3.6	255.255.255.252	172.29.3.4/30
Bogota3	S0/0/1	Bogota1	172.29.3.2	255.255.255.252	172.29.3.0/30
Bogota3	G0/0	PC-C	172.29.0.1	255.255.255.0	172.29.0.0/24

Fuente: propia

Tabla 25 Configuración de conexiones

DISPOSITIVO	CONFIGURACION DE CONEXION
ISP	ISP(config)#interface s0/0/0 ISP(config-if)#description link to BOGOTA1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown Serial0/0/0, changed state to down ISP(config-if)#interface s0/1/0 ISP(config-if)#description link to MEDELLIN1 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#clock rate 128000 ISP(config-if)#no shutdown
Medellin1	Medellin1(config)#interface s0/1/0 Medellin1(config-if)#description link to ISP Medellin1(config-if)#ip address 209.17.220.2 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#interface s0/0/0 Medellin1(config-if)#description link to MEDELLIN2 Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#interface s0/0/1 Medellin1(config-if)#description link to MEDELLIN3 Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config-if)#interface s0/1/1 Medellin1(config-if)#description link to MEDELLIN3 Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252 Medellin1(config-if)#clock rate 128000 Medellin1(config-if)#no shutdown Medellin1(config)#

Medellin2	Medellin2(config)#interface s0/0/0 Medellin2(config-if)#description link to MEDELLIN1 Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252 Medellin2(config-if)#no shutdown Medellin2(config-if)#interface s0/0/1 Medellin2(config-if)#description link to MEDELLIN3 Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252 Medellin2(config-if)#clock rate 128000 Medellin2(config-if)#no shutdown Medellin2(config-if)#interface G0/0 Medellin2(config-if)#description link to PC-Medellin2-Lan2 Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128 Medellin2(config-if)#no shutdown Medellin2(config-if)#exit
Medellin3	Medellin3(config)#interface s0/0/1 Medellin3(config-if)#description link to MEDELLIN2 Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config-if)#interface s0/1/0 Medellin3(config-if)#description link to MEDELLIN1 Medellin3(config-if)#ip address 172.29.6.14 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config-if)#interface s0/0/0 Medellin3(config-if)#description link to MEDELLIN1 Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config-if)#interface G0/0 Medellin3(config-if)#description link to PC-PC-Medellin3-Lan3 Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128 Medellin3(config-if)#no shutdown Medellin3(config-if)#exit
Bogota1	Bogota1(config)#interface s0/0/0 Bogota1(config-if)#description link to ISP Bogota1(config-if)#ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config-if)#interface s0/0/1 Bogota1(config-if)#description link to BOGOTA3 Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#interface s0/1/0

	Bogota1(config-if)#description link to BOGOTA2 Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown Bogota1(config-if)#interface s0/1/1 Bogota1(config-if)#description link to BOGOTA3 Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252 Bogota1(config-if)#clock rate 128000 Bogota1(config-if)#no shutdown
Bogota2	Bogota2(config)#interface s0/0/1 Bogota2(config-if)#description link to BOGOTA1 Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252 Bogota2(config-if)#no shutdown Bogota2(config-if)#interface s0/0/0 Bogota2(config-if)#description link to BOGOTA3 Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252 Bogota2(config-if)#clock rate 128000 Bogota2(config-if)#no shutdown Bogota2(config-if)#interface G0/0 Bogota2(config-if)#description link to PC-Bogota2-Lan2 Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0 Bogota2(config-if)#no shutdown
Bogota3	Bogota3(config)#interface s0/0/0 Bogota3(config-if)#description link to BOGOTA2 Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#interface s0/1/0 Bogota3(config-if)#description link to BOGOTA1 Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#interface s0/0/1 Bogota3(config-if)#description link to BOGOTA1 Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#interface G0/0 Bogota3(config-if)#description link to PC-Bogota3-Lan3 Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota3(config-if)#no shutdown

Fuente: Comandos ingresados en Packer Tracer

2.2. PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

Configurar el enrutamiento en la red usando el protocolo OSPF versión 2.

Declare la red principal, desactive la sumarización automática.

El protocolo OSPF permitirá que el router pueda enseñar las redes a los demás routers. Usamos el comando router ospf en el modo de configuración global para habilitar OSPF, en el modo de configuración del router se configuro una ID de router, para que conocer los vecinos y el router se identifique ante los otros routers.
Para determinar las interfaces del router que participan en el proceso de routing OSPF versión 2, se configurara una como una red de OSPF de área única 0, con el comando network se anunciara las redes con las respectivas mascaras wilcard que identificara las interfaces en base a sus direcciones de red.

Tabla 26 Configuración OSPF

Dispositivo	Configuración OSPF en los Routers
Bogota1	Bogota1(config)#**router ospf 1** Bogota1(config-router)#**router-id 1.1.1.1** Bogota1(config-router)# **network 172.9.3.0 0.0.0.3 area 0** Bogota1(config-router)# **network 172.9.3.4 0.0.0.3 area 0** Bogota1(config-router)# **network 172.9.3.8 0.0.0.3 area 0** Bogota1(config-router)# **network 209.17.220.4 0.0.0.3 area 0**
Bogota2	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 172.29.3.12 0.0.0.3 area 0** Bogota2(config-router)# **network 172.29.3.8 0.0.0.3 area 0**
Bogota3	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 172.29.3.12 0.0.0.3 area 0 Bogota3(config-router)# network 172.29.3.4 0.0.0.3 area 0 Bogota3(config-router)# network 172.29.3.0 0.0.0.3 area 0
Medelli1	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 0 Medellin1(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medellin1(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin1(config-router)# network 209.17.220.0 0.0.0.3 area 0
Medellin2	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 0 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
Medellin3	Medellin3(config)#router ospf 1 Medellin3(config-router)#router-id 33.33.33.33 Medellin3(config-router)# network 172.29.4.128 0.0.0.127 area 0 Medellin3(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medellin3(config-router)# network 172.29.6.4 0.0.0.3 area 0

Fuente: Comandos ingresados en Packer Tracer

b. 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.

Todo paquete que vaya a la red sumarizada envíela a Bogota1 Se configurara con el comando ip route de modo de configuración global, dirección de red de destino, mascara de subred que se sumarizan a /22 y el interfaz de salida.

Tabla 27 Configuración de rutas sumarizadas

Dispositivo	Configuración Rutas Estáticas Sumarizada a Sedes
ISP	ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.200.2 ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.200.6

Fuente: Comandos ingresados en Packer Tracer

2.3. PARTE 2: 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.

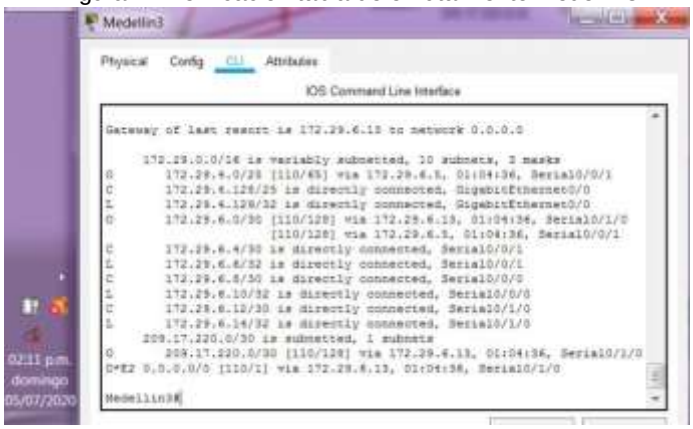
Para la verificación de la tabla de enrutamiento se emitirá el comando show ip route y si solamente queremos ver los del protocolo OSPF con el comando show ip route ospf en el modo EXEC privilegiado.

En Bogota3 verificamos que se ha configurado el protocolo OSPF, hay redes conectadas directamente conectas, como Gateway de último recurso 172.29.3.1 a través de la red 0.0.0.0 como ruta predeterminada y el interfaz de salida S0/0/1.
En Medellin3 verificamos que se ha configurado el protocolo OSPF, hay redes conectadas directamente conectas, como Gateway de último recurso 172.29.6.13 a través de la red 0.0.0.0 como ruta predeterminada y el interfaz de salida S0/1/0.

Figura 20 Verificación tabla de enrutamiento Bogota3

Fuente: propia

Figura 21 Verificación tabla de enrutamiento Medellin3

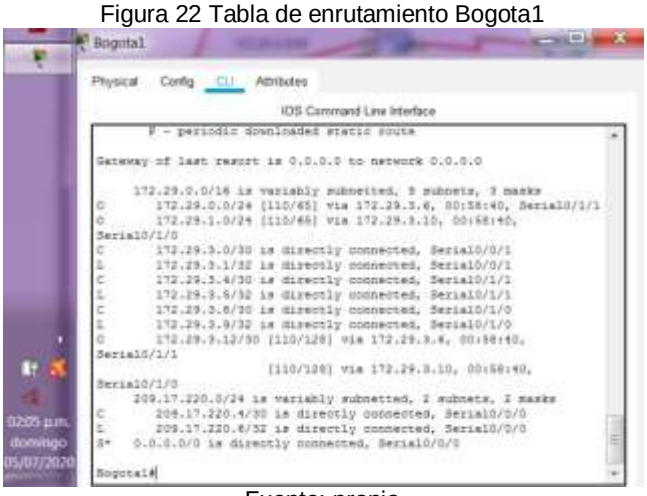


Fuente: propia

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.

En Bogota1 indica la ruta 0.0.0.0/0 por defecto conectada directamente con interfaz de salida S0/0/0 y tres rutas con protocolo OSPF.
En Medellin1 indica la ruta 0.0.0.0/0 por defecto conectada directamente con interfaz de salida S0/1/0 y tres rutas con protocolo OSPF.
Ambos routers tienen con Gateway de último recurso 0.0.0.0

Figura 22 Tabla de enrutamiento Bogota1



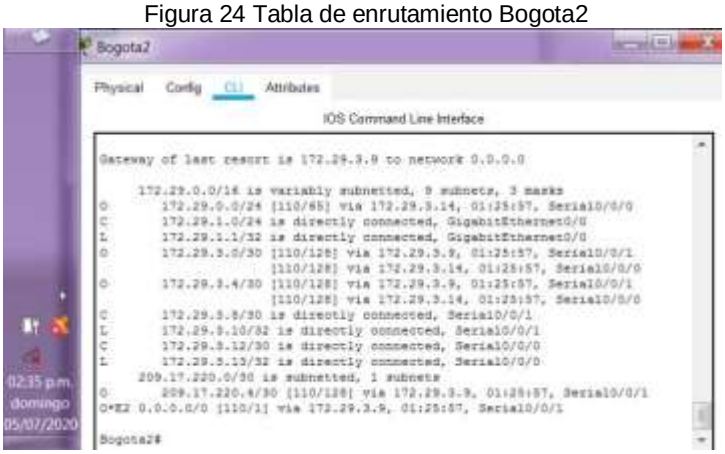
Fuente: propia

Figura 23 Tabla de enrutamiento Medellin1

Fuente: propia

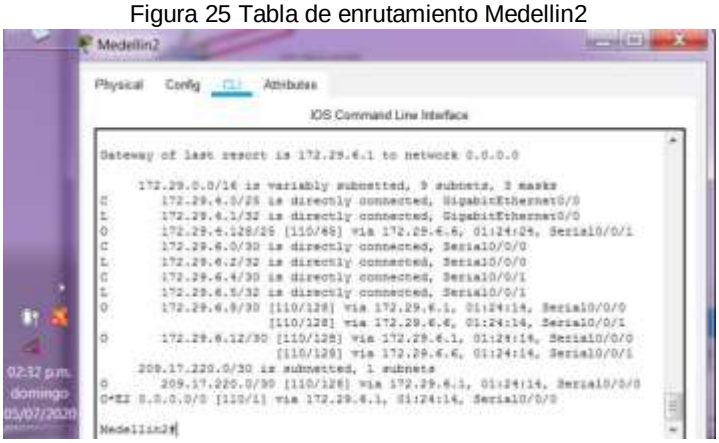
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.
e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Figura 24 Tabla de enrutamiento Bogota2



Fuente: propia

Figura 25 Tabla de enrutamiento Medellin2



Fuente: propia

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

Debido a que en el ISP no se aplicó la configuración del protocolo OSPF, aparecen en la tabla de routing dos rutas estáticas como la 172.29.0.0/22 y 172.29.4.0/22 y redes directamente conectadas,

Figura 26 Tabla de enrutamiento ISP

Fuente: propia

2.4. PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.

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

Tabla 28 Interfaces con protocolo OSPF

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

Fuente: archivo de Prueba de habilidades.

En los cuatro router internos se cambió la interfaz G0/0 a pasiva, esto con el fin de evitar la transmisión de mensajes routing por medio de una interfaz del router, de todos modos, sin dejar de permitir que se anuncie esa red a otros routers.

Tabla 29 deshabilitación de propagación OSPF

Dispositivo	Des habilitación propagación del protocolo OSPF
Bogota2	Bogota2(config-router)# **passive-interface G0/0**
Bogota3	Bogota3(config-router)# **passive-interface G0/0**
Medellin2	Medellin2(config-router)# **passive-interface G0/0**
Medellin3	Medellin 3(config-router)# **passive-interface G0/0**

Fuente: Comandos ingresados en Packer Tracer

2.5. PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos. 32

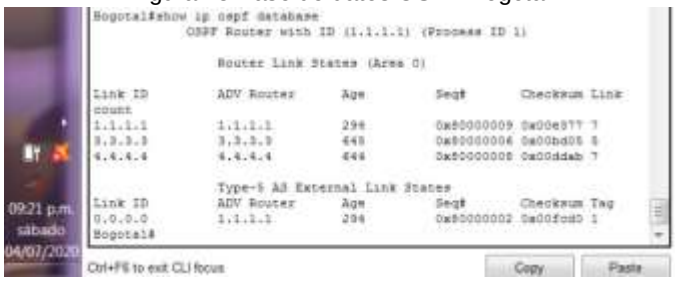
Figura 27 Verificación protocolo OSPF

Fuente: propia

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.

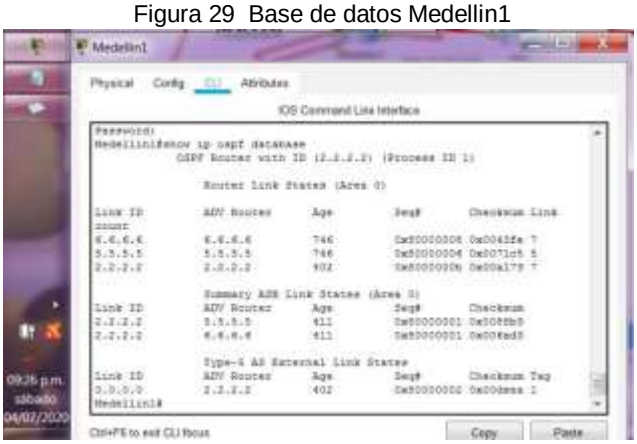
Con el comando show ip ospf basedate se puede verificar la información sobre todos los otros routers en la red, lo que significa que en esta base de datos está representada la topología de la red, además podemos verificar que todos los routers dentro de un área tienen la base de datos de estado de enlace iguales.

Figura 28 Base de datos OSPF Bogota1



Fuente: propia

Figura 29 Base de datos Medellin1



Fuente: propia

2.6. PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

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

Se configura la autenticación PAP de PPP entre ISP y Medellin1, para ello inicia con la autenticación por medio de clave acceso cisco
Se selecciona la interfaz para que utilice la encapsulación PPP con Medellin1
b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Se configura la autenticación CHAP de PPP entre ISP y Bogota1, para ello inicia con la autenticación por medio de clave acceso cisco
Se selecciona la interfaz para que utilice la encapsulación PPP con Medellin1

La contraseña enviada en cada puerto serial debe coincidir con la contraseña que espera el router externo

Tabla 30 Encapsulación y autenticación PPP

Dispositivo	Encapsulación y Autenticación PPP
Bogota1	Bogota1(config)#username ISP password cisco Bogota1(config)#int s0/0/0 Bogota1(config-if)#encapsulation ppp Bogota1(config-if)#ppp authentication chap
Medellin1	ISP(config-if)#username ISP secret cisco Medellin1(config)#int s0/1/0 Medellin1(config-if)#encapsulation PPP Medellin1(config-if)#PPP authentication PAP Medellin1(config-if)#PPP PAP sent-username Medellin1 password cisco
ISP	ISP(config)#username Bogota1 password cisco ISP(config)#int s0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)#ppp authentication chap ISP(config-if)#exit ISP(config-if)#username Medellin1 secret cisco ISP(config)#int s0/1/0 ISP(config-if)#encapsulation PPP ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco ISP(config-if)#exit

Fuente: Comandos ingresados en Packer Tracer

2.7. PARTE 6: CONFIGURACIÓN DE PAT.

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

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.

En Medellin1 iniciamos definiendo una lista de acceso estándar LAN-Bogotá que permita ver las direcciones que se deberán traducir, para ello se asignó la lista 1 y se permite la dirección estándar 172.29.4.0 con el wildcard de origen 0.0.0.255.

Pasamos a especificar las opciones de ACL, con la interfaz de salida que identificara la dirección IP que se utilizara en la traducción de direcciones internas, y sobrecarga con el fin de establecer la traducción dinámica de origen, emitiendo el comando ip nat inside source seguido del número de la lista de acceso, la interfaz más overload (sobrecargado) saldrá varias dirección por la misma ip publica, indicara al router que realice un seguimiento de los números de puerto con cada entrada de NAT.

Debemos activar las redes identificando cuales son las interfaces internas que se conectan con la red interna.

Finalmente se identifica la interfaz externa, debe ser la misma interfaz identificada en el segundo paso.

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 0/0/0 del router Bogotá1, cómo diferente puerto.

En Bogota1 iniciamos definiendo una lista de acceso estándar LAN-Bogotá que permita las direcciones que se deberán traducir, para ello se asignó la lista LAN-Bogotá se permite la dirección estándar 172.29.0.0 con el wildcard de origen 0.0.0.255.

Pasamos a especificar las opciones de ACL, con la interfaz de salida que identificara la dirección IP que se utilizara en la traducción de direcciones internas, y sobrecarga con el fin de establecer la traducción dinámica de origen, emitiendo el comando ip nat inside source seguido del número de la lista de acceso, la interfaz más overload que indicara al router que realice un seguimiento de los números de puerto con cada entrada de NAT.
Luego se identificarán cuáles son las interfaces internas que se conectan con la red interna.

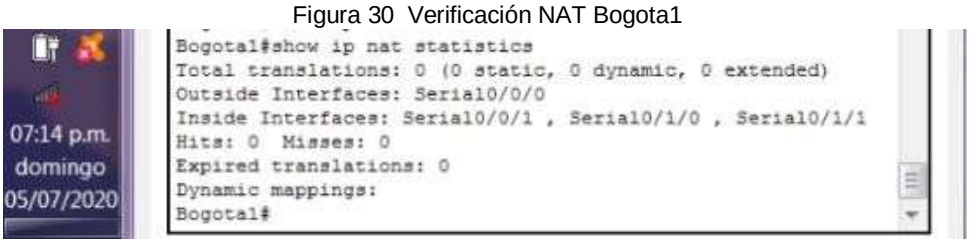
Finalmente se identifica la interfaz externa, debe ser la misma interfaz identificada en el segundo paso.

Tabla 31 Configuración PAT

Dispositivo	Configuración PAT
Bogota1	Bogota1(config)#ip access-list standard LAN-Bogota Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.0.255 Bogota1(config-std-nacl)#exit Bogota1(config)#ip nat inside source list LAN-Bogota int S0/0/0 overload Bogota1(config)#int S0/0/1 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int S0/1/0 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int S0/1/1 Bogota1(config-if)#ip nat inside Bogota1(config-if)#int S0/0/0 Bogota1(config-if)#ip nat outside Bogota1(config-if)#exit
Medellin1	Medellin1(config)#ip access-list standard LAN-Medellin Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.0.255 Medellin1(config-std-nacl)#exit Medellin1(config)#ip nat inside source list LAN-Medellin int S0/1/0 overload Medellin1(config)#int S0/1/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#int S0/0/0 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int S0/0/1 Medellin1(config-if)#ip nat inside Medellin1(config-if)#int S0/1/1 Medellin1(config-if)#ip nat inside Medellin1(config-if)#exit

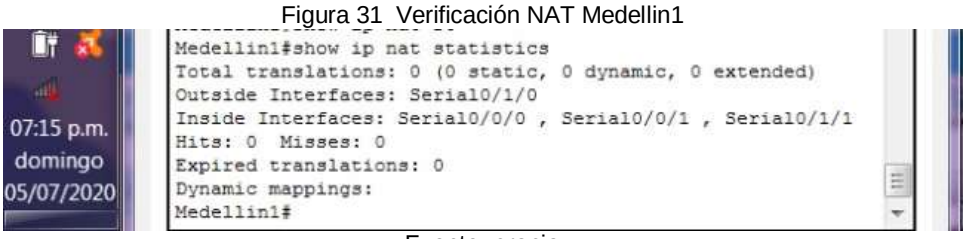
Fuente: Comandos ingresados en Packer Tracer

Figura 30 Verificación NAT Bogota1



Fuente: propia

Figura 31 Verificación NAT Medellin1

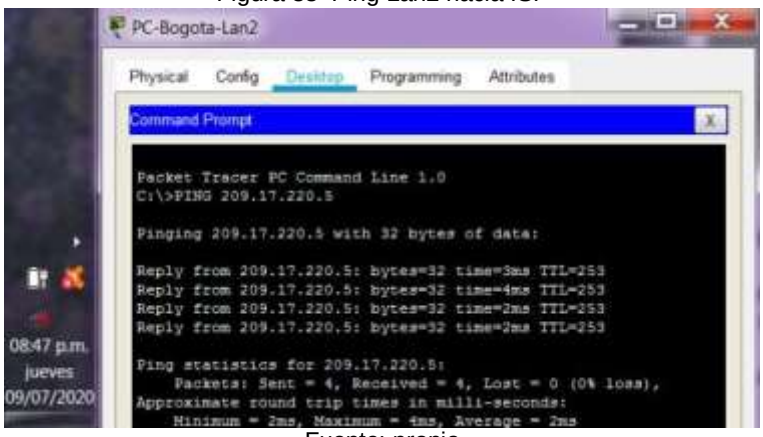


Fuente: propia

Figura 32 Ping Lan3 hacia ISP

Fuente: propia

Figura 33 Ping Lan2 hacia ISP



Fuente: propia

2.8. 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.

El servidor DHCP asigna automáticamente un conjunto de direcciones, la red de Medellin2 presentara el servicio DHCP para la red Medellin3, pero hay algunas direcciones que están asignadas estáticamente y no se pueden asignar a otros dispositivos por lo tanto se deben excluir estas direcciones con el comando excluded- address.

También debemos crear un pool con nombre especifico y pasara al modo de configuración DHCP, en el router Medellin1 creamos el pool Medellin-LAN3 y Medellin-LAN4.

Con el comando network se definirán el rango de direcciones que están disponibles, la network disponible es la direccion172.29.1.0 255.255.255.0 y la network 172.29.0.0 255.255.255.0.
Es importante definir el Gateway del router 172.29.4.1 y 172.29.4.129. Además, es necesario definir el nombre de dominio lan1.Bogota.com y lan2.Bogota.com

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
Debido a que Medellin3 no está configurado como servidor DHCP no podrá adquirir direcciones IPv4 y como el servidor DHCP está ubicado en otra red, para solucionar este problema se debe configurar una dirección de ayuda, esto permitir que el router reenvié difusiones de DHCP al servidor.
La interfaz G0/0 es la que recibe la difusión y con el comando ip helper-address seguida de la dirección Gateway del router Bogota1 que está conectada con Medellin3.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

El servidor DHCP asigna automáticamente un conjunto de direcciones, la red de Bogota2 presentara el servicio DHCP para la red Bogota3, pero hay algunas direcciones que están asignadas estáticamente y no se pueden asignar a otros dispositivos por lo tanto se deben excluir estas direcciones con el comando excluded- address.
También debemos crear un pool con nombre especifico y pasara al modo de configuración DHCP, en el router Bogota1 creamos el pool Bogota-LAN1 y Bogota-LAN2.

Con el comando network se definirán el rango de direcciones que están disponibles, la network disponible es la direccion172.29.1.0 255.255.255.0 y la network 172.29.0.0 255.255.255.0.
Es importante definir el Gateway del router 172.29.1.1 y 172.29.0.1. Además, es necesario definir el nombre de dominio lan1.Bogota.com y lan2.Bogota.com

d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Debido a que Bogota3 no está configurado como servidor DHCP no podrá adquirir direcciones IPv4 y como el servidor DHCP está ubicado en otra red, para solucionar este problema se debe configurar una dirección de ayuda, esto permitir que el router reenvié difusiones de DHCP al servidor.

La interfaz G0/0 es la que recibe la difusión y con el comando ip helper-address seguida de la dirección Gateway del router Bogota2 que está conectada con Bogota3.

Tabla 32 Configuración DHCP en Bogota2 y Medellin2

Dispositivo	Configuración DHCP
Bogota2	Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.9 Bogota2(config)#ip dhcp pool Bogota-LAN1 Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota2(dhcp-config)#default-route 172.29.1.1 Bogota2(dhcp-config)#domain-name lan1.Bogota.com Bogota2(dhcp-config)#exit Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.9 Bogota2(config)#ip dhcp pool Bogota-LAN2 Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)#default-route 172.29.0.1 Bogota2(dhcp-config)#domain-name lan2.Bogota.com
Bogota3	Bogota3(config)#interface G0/0 Bogota3(config-if)#ip helper-address 172.29.3.13
Medellin2	Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.9 Medellin2(config)#ip dhcp pool Medellin-LAN3 Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medellin2(dhcp-config)#default-route 172.29.4.1 Medellin2(dhcp-config)#domain-name lan3.Medellin.com Medellin2(dhcp-config)#exit Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.137 Medellin2(config)#ip dhcp pool Medellin-LAN4 Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128 Medellin2(dhcp-config)#default-route 172.29.4.129 Medellin2(dhcp-config)#domain-name lan3.Medellin.com Medellin2(dhcp-config)#exit
Medellin3	Medellin3(config)#interface G0/0 Medellin3(config-if)#ip helper-address 172.29.6.5

Fuente: Comandos ingresados en Packer Tracer

CONCLUSIONES

Se desarrollo los escenarios propuestos aplicando paso a paso las temáticas vistas durante el Diplomado de profundización CISCO CCNA como la configuración inicial básica de todo dispositivo, identificando las direcciones Ip y realizamos la conexión de red, en el escenario uno se configuro el protocolo de routing RIP y en el escenario dos se aplicó el protocolo de enlace de estado OSPF; además de configuraron protocolos NAT y NTP, se distribuyeron redes en las cuales se aplicó el protocolo DHCP.

En el escenario 1 se comprobó que con la configuración VLAN, donde enfatizan la importancia de la implementación de políticas de un acceso y seguridad que favorecerán en el crecimiento de una empresa.

En cuanto a la configuración del protocolo RIP, evidenciamos que a pesar de que este protocolo ya casi no se usa en redes modernas, pero es una base inicial útil para la comprensión de enrutamiento básico.

En el escenario 2 se aplicó el protocolo OSPF presenta ventajas tales como convergencia más rápida y se aplica en redes más grandes y podemos ver que hoy en día el uso del internet a crecido a grandes escalas por lo tanto esta práctica es una base y una oportunidad importante para aplicarlo laboralmente y lograr un buen desempeño profesional.

Se usó del programa Packer Tracer, esta herramienta nos permitió crear, experimentar los escenarios propuestos y se verifico el funcionamiento interno de las redes, la manera como fluyen los datos desde cuando se envía un mensaje y hace el recorrido paso a paso por toda la red hasta llegar a su destino.

BIBLIOGRAFÍA

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

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). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

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

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

CONTADOR. N. (2019). Fundamentos de Enrutamiento y Conmutación. (Routing and Switching Essentials) Cisco Networking Academy. Recuperado de https://www.lawebdelprogramador.com/pdf/15346-Fundamentos-de-enrutamiento-y-conmutacion-Routing-and-Switching-Essentials.html

Anexo 1 link de descarga del escenario 1

https://drive.google.com/file/d/1OCgkDUkWmu9H3Oq1q0HwydCyQkclmJi5/view?usp=sharing

Anexo 2 Link de descarga del escenario 2

https://drive.google.com/file/d/1SUr-LFufvaFH-0KCdRmV-XBSd3QjIA7O/view?usp=sharing