

SOLUCIONES INTEGRADAS LAN / WAN  
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JAIR HERNÁNDEZ BARRIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
FACULTAD DE INGENIERIA DE SISTEMAS  
BOGOTA 2020

SOLUCIONES INTEGRADAS LAN / WAN  
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Trabajo de grado para optar al título en Ingeniería de sistemas

JAIR HERNÁNDEZ BARRIOS

GUSTAVO RODRÍGUEZ  
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
FACULTAD DE INGENIERIA DE SISTEMAS  
BOGOTA 2020

Nota aceptación

---

---

---

Presidente de jurado

---

---

Jurado

---

---

Jurado

---

---

Bogotá julio 21 de 2020

### Dedicatoria

El presente trabajo es dedicado a todas aquellas personas que se esforzaron solas en el trasegar de la vida y a los que desean ser.

## AGRADECIMIENTOS

El presente tiene como objeto un profundo agradecimiento a mis padres, a mi familia, amigos y todas aquellas personas que con su grano de arena permitieron llegar hasta este punto, a los docentes, directores, compañeros que de alguna u otra manera permitieron adquirir nuevos conocimientos y abren las puertas de nuevas posibilidades hacia futuro, gracias.

## Tabla de contenido

Glosario .....	10
Resumen .....	11
Introducción .....	12
Objetivo General.....	13
Objetivos Específicos .....	13
Planteamiento del problema .....	14
Justificación .....	14
Escenario 1.....	15
Paso 1: Inicializar y volver a cargar los routers y los switches.....	15
Parte 1: Configurar la computadora de Internet.....	16
Parte 2: Configurar los parámetros básicos de los dispositivos .....	16
Paso 2: Configurar R1.....	17
Paso 3: Configurar R2.....	18
Paso 4: Configurar R3.....	20
Paso 5: Configurar S1 .....	21
Paso 6: Configurar el S3 .....	21
Paso 7: Verificar la conectividad de la red.....	22
Paso 8: Configurar S1 .....	23
Paso 9: Configurar R1.....	25
Paso 10: Verificar la conectividad de la red.....	25
Paso 11: Configurar RIPv2 en el R1.....	26
Parte 3: Configurar el protocolo de routing dinámico RIPv2 .....	26
Paso 12: Configurar RIPv2 en el R2.....	27
Paso 13: Configurar RIPv3 en el R2.....	28
Paso 14: Verificar la información de RIP .....	28
Paso 15: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	30
Parte 4: Implementar DHCP y NAT para IPv4 .....	30
Paso 16: Configurar la NAT estática y dinámica en el R2.....	31
Paso 17: Verificar el protocolo DHCP y la NAT estática .....	31
Parte 5: Configurar NTP.....	33

Parte 6: Configurar y verificar las listas de control de acceso (ACL).....	33
Paso 18: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.....	34
Escenario 2:.....	37
Cuadro de direccionamiento IP .....	41
Configuración del enrutamiento.....	46
Configuración de PAT. ....	54
Enlaces a escenarios virtuales realizados en Packet Tracer.....	57
Escenario 1:.....	57
Escenario 2: .....	57
Conclusiones .....	58
Bibliografía.....	59

## LISTA DE FIGURAS

Figura 1 Topología inicial escenario 1, fuente: propia .....	15
Figura 2 Configuración dispositivos de internet.....	17
Figura 3 Verificación conectividad de red entre R1 y R2 e internet .....	22
Figura 4 Verificación configuración RIP2 en R1 .....	27
Figura 5 Verificación configuración RIP2 en R2 .....	27
Figura 6 Verificación configuración RIP2 en R3 .....	28
Figura 7 Verificación show ip protocols .....	29
Figura 8 Verificación protocolo ip route rip .....	30
Figura 9 Verificación ip dinámica en PC-A y PC-C.....	32
Figura 10 Verificación entre los equipos y acceso web .....	32
Figura 11 Verificación de ACL en R1 .....	34
Figura 12 Mostrar mediante show ip nat translations .....	35
Figura 13 Verificación conectividad al servidor .....	36
Figura 14 Topología Final Escenario 1.....	36
Figura 15 Topología inicial escenario 2.....	37
Figura 16 lista conexión interfaces ISP y Medellín1 .....	46
Figura 17 Conexión interfaces seriales Medellín2 y Medellín3 .....	46
Figura 19 Configuración PC'S LAN .....	48
Figura 20 Configuración rutas distribuidas OSPF Routers Medellín1 y Bogotá1 .....	49
Figura 21 Verificación conexiones OSPF .....	49
Figura 22 Lista conexión protocolo OSPF .....	50
Figura 23 Configuración rutas estáticas Routers Medellín y Bogotá.....	50
Figura 24 Conexiones OSPF en Bogotá y Medellín 1 .....	51
Figura 25 Verificación DHCP LANS Medellín .....	54
Figura 26 Verificación DHCP LANS Bogotá.....	54
Figura 27 Verificación conectividad de la NAT Bogotá desde LAN2.....	56
Figura 28 Verificación conectividad de la NAT Bogotá desde LAN1 .....	56
Figura 29 Verificación traducción NAT desde LAN 2.....	56
Figura 30 Verificación NAT desde LAN 1 .....	57
Figura 31 Topología final conectada .....	57



## LISTA DE TABLAS

Tabla 1 Inicialización de switches .....	16
Tabla 2 Configuración servidor internet.....	17
Tabla 3 Configuración de Router 1 .....	17
Tabla 4 Configuración Router 2 .....	18
Tabla 5 Configuración Router 3 .....	20
Tabla 6 Configuración Switch 1.....	21
Tabla 7 Configuración Switch 3.....	21
Tabla 8 Verificación conectividad de red.....	22
Tabla 9 Configuración vlans en switches .....	23
Tabla 10 Configuración vlans en switch 3.....	24
Tabla 11 Configuración protocolo 802.1q en Router 1 .....	25
Tabla 12 Conectividad entre switches y R1.....	25
Tabla 13 Resultados conectividad entre R1 y R2.....	26
Tabla 14 Configuración enrutamiento en R1 .....	26
Tabla 15 Configuración enrutamiento en R3.....	28
Tabla 16 Configuración DHCP y NAT para IPV4 en R1 .....	30
Tabla 17 Verificación DHCP y NAT estática .....	31
Tabla 18 Configuración NTP .....	33
Tabla 19 Mostrar asociaciones NTP en R1 .....	33
Tabla 20 Configuración controles acceso ACL.....	33
Tabla 21 Lista de host permitidos en NAT.....	35
Tabla 22 Configuraciones básicas routers Medellín y Bogotá .....	38
Tabla 23 Configuración direccionamiento IP Medellín y Bogotá.....	42
Tabla 24 Enrutamiento OSPF en Routers Medellín y Bogotá.....	46
Tabla 25 Rutas estáticas de ISP direcciones públicas .....	50
Tabla 26 Deshabilitación protocolo OSPF Routers Medellín 1 y 2, Bogotá 1 y 2.....	51
Tabla 27 Configuración autenticación CHAT y PAP.....	52
Tabla 28 Configuración Configuración DHCP en routers Medellín 2y3, Bogotá 3y2.....	53
Tabla 29 Configurar NAT en routers Medellín1 y Bogotá1 .....	55

## GLOSARIO

**ACL:** Listas de control de acceso, es la designación de un conjunto de redes y direcciones permitidas con un protocolo de seguridad el cual permite ingresar o salir de una determinada red.

**ENRUTAMIENTO:** Es la acción de buscar el camino entre todos los posibles para llegar a un host mediante configuraciones especiales de conectividad en routers con el fin de transmitir a usuarios finales en paquetes.

**IPV6:** protocolo de red de capa 2 el cual usa sistema de numeración hexadecimal usados para la conmutación o envío de paquetes de un destino a otro.

**GATEWAY:** Es la primera dirección después de la configuración de dirección de red usada como referente para identificar el punto de acceso a otra red.

**NAT:** Network Acces Traslation es usada para la traducción de direcciones IP privadas a públicas en una red con el fin de usar menos direcciones IP y mejorar los niveles de seguridad de la organización.

**RIP:** Es el protocolo de información de enrutamiento usado entre los router para determinar las rutas autorizadas para flujo de información que transportan las direcciones de host.

**VLAN:** Es una red virtual local configurada en switches para identificar subredes o subconjuntos específicos de usuarios en una determinada organización.

## RESUMEN

A través del presente trabajo se busca obtener aprendizaje significativo respecto de la configuración de dispositivos de red que funcionan en las locaciones habitaciones y organizaciones como protocolo de comunicación en el envío de información, estas prácticas son llevadas a cabo mediante una capacitación inicial enfocado al entorno laboral como insumo de formación que permite adquirir competencias ante la sociedad.

De igual manera la creciente demanda de dispositivos eléctricos y electrónicos requieren de esta disciplina para permitir la comunicación mediante la configuración de redes mediante instrucciones o protocolos.

Palabras Clave: Protocolos, enrutamiento, red, host, IP, NAT, simulación, conectividad.

## INTRODUCCIÓN

El presente trabajo está orientado a evidenciar los conocimientos adquiridos en los diferentes dispositivos de CISCO a través de la herramienta packet – tracer, teniendo como referente los contenidos de la academia web CISCO Netacad, las consultas a través de las referencias bibliográficas y libres en la web.

Adicionalmente esta práctica de habilidades se complementa de las tutorías realizadas a través de web conferencias, con el cual estaré en la capacidad de realizar configuraciones en un entorno empresarial, administrar la red y monitorear su comportamiento en una determinada organización.

Dentro de las temáticas abordadas, se destacan la configuración de vlan corporativas, configuración de medidas de seguridad, enrutamiento, redireccionamiento IP y configuraciones básicas de seguridad.

Cabe resaltar que el presente trabajo tiene sugerencias de configuraciones sobre temáticas recientes, razón por la cual se complementa con las actividades prácticas y encuentros realizados a través de las tutorías virtuales organizadas por la directora de curso y tutor en cada unidad además de prácticas finales.

## OBJETIVOS

### OBJETIVO GENERAL:

Adquirir los conocimientos necesarios en el diseño y comunicación de redes de telecomunicaciones aplicando los protocolos, conceptos de conmutación, canales de comunicación e interpretación de información de forma organizada, permitiendo a las grandes organizaciones y personas enviar y recibir información en tiempo real como satisfacción de suministro de información.

### OBJETIVOS ESPECÍFICOS:

- Brindar conectividad entre dispositivos de comunicación a través de instrucciones y comandos preexistentes, bajo esquemas de conmutación a través de protocolos de internet.
- Solucionar necesidades de comunicación en las organizaciones y personas mediante la configuración, mantenimiento y sostenimiento de los equipos de comunicación.

## PLANTEAMIENTO DEL PROBLEMA

Se proponen necesidades del entorno actual empresarial cuyo fin primordial es la comunicación y flujo de información a través de dispositivos de conmutación de paquetes, estas necesidades se derivan por la ausencia de canales de comunicación entre las dependencias y sucursales del cliente.

Se escala la necesidad a los especialistas o conocedores de la configuración de dispositivos para emitir una adecuada solución que permita el flujo de información de forma acertada teniendo en cuenta las disposiciones legales actuales vigentes en cuanto a comunicaciones se refiere.

## JUSTIFICACIÓN

Las organizaciones y personas recurren a las tecnologías de telecomunicaciones con el fin de brindar soluciones de expansión a sus razones sociales, es por ello que existen empresas dedicadas a la configuración y prestación de servicios de las comunicaciones en el entorno social, buscando brindar el flujo de información de forma rápida y efectiva desde diferentes lugares del mundo transmitiendo información en tiempo real, solución que genera avances, nuevos conocimientos, mayor productividad y evolución a nivel mundial.

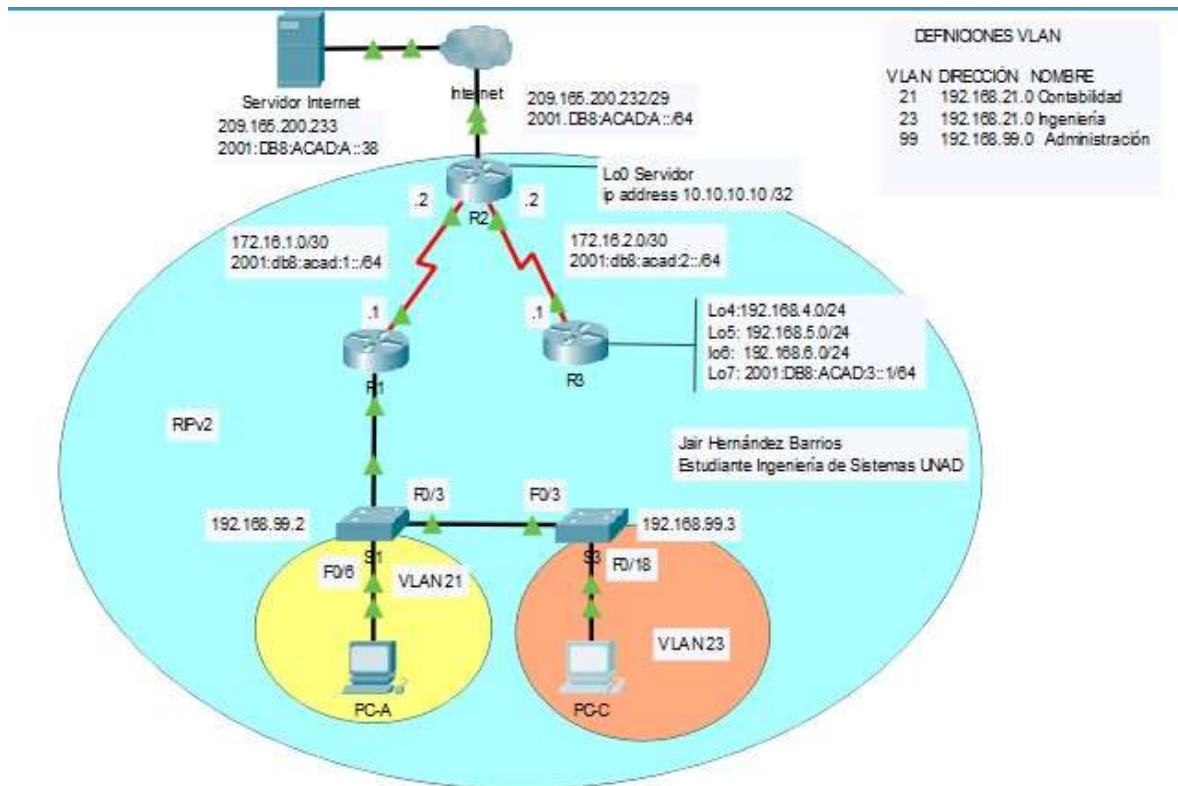
Con el trascurrir del tiempo y las experiencias o lecciones aprendidas las organizaciones y empresas de telecomunicaciones se han adquiridos destrezas que han permitido técnicamente mejorar acorde a las necesidades del cliente mediante protocolos específicos de enrutamiento, creación de redes privadas, traducción de redes, bases de datos, programaciones nuevas, diversificación de los protocolos de comunicación generando una evolución a gran escala de comunicación mediante canales de información.

Hoy en día las telecomunicaciones son la evolución inminente a gran escala del progreso de las organizaciones y personas.

## ESCENARIO 1

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

Figura 1 Topología inicial escenario 1, fuente: propia



Fuente: propio

Paso 1: Inicializar y volver a cargar los routers y los switches

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

Para este paso de inicialización como administradores de red y ante la necesidad de realizar una configuración nueva y limpia se eliminan posibles configuraciones anteriores para asegurar que las nuevas instrucciones sean adecuadas.

Estas configuraciones se realizan mediante el comando:

```
Router#erase startup-config
```

Una vez confirmado se realiza el reinicio mediante el comando:

```
Router#reload
```

Este paso se aplicará para Inicializar los routers 1, 2 y 3:

Inicializando switches

Se aplican los mismos pasos de borrado que los router adicionando el comando:

```
Switch#Delete vlan.dat
```

Posteriormente se reinicia el switch mediante el comando:

```
Switch#reload
```

Si se desea verificar las configuraciones realizadas se debe digitar el comando:

```
Switch#show flash
```

```
Switch#Show vlan brief
```

*Tabla 1 Inicialización de switches*

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

Parte 1: Configurar la computadora de Internet

Se realizan las respectivas asignaciones IP acorde a la siguiente topología.

Parte 2: Configurar los parámetros básicos de los dispositivos.



Las tareas de configuración del servidor de internet incluyen el siguiente direccionamiento IP:

*Tabla 2 Configuración servidor internet*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Dirección IPv4	209.165.200.233
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:db8:acad:2::1

Se realizan las respectivas asignaciones IP a los dispositivos router y switch con los datos de configuración relacionados evidenciados en la figura 3.

*Figura 2 Configuración dispositivos de internet*

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

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes instrucciones:

Establezca la descripción

Se establece la dirección IPv4 acorde al diagrama de topología para conocer la información de direcciones, posteriormente se establece la dirección IPv6 acorde a la topología para conocer la información de direcciones

*Tabla 3 Configuración de Router 1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
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 15 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 #Acceso no autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.2 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 g0/0

**Nota:** Todavía no se configura G0/1.

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes instrucciones similares a las de router 1, tales como nombrar el router configurar los accesos a consola, mensajes de seguridad, luego configuraciones posteriores de redireccionamiento:

*Tabla 4 Configuración Router 2*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	R2(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
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 15 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	R2(config)#ip http server

	% Invalid input detected at '^' marker. No funciona en packet tracer
Mensaje MOTD	R2(config)#banner motd #Acceso no autorizado#
Interfaz S0/0/0 Gateway fe80::1	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description connection 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 This command applies only to DCE interfaces R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description connection to internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Se establece la dirección IPv4 para servidor simulado: R2(config)# lo0 R2(config-if)# ip address 10.10.10.10 /32
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R2(config)#ipv6 route ::/0 g0/0

#### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes instrucciones:

*Tabla 5 Configuración Router 3*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
Nombre del router	R3(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
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 15 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 #Acceso no autorizado#
Interfaz S0/0/1	R3(config-if)#int s0/0/1 R3(config-if)#description connection to R2 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)#clock rate 128000 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int lo 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#int lo 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#int lo 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#int lo 7 R3(config-if)#ipv6 address 2001:DB8.ACAD:3::1/64

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1
-----------------------	---

### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes instrucciones para proteger la seguridad de acceso:

*Tabla 6 Configuración Switch 1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S1(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 15 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 #Acceso No Autorizado#

### Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes instrucciones para proteger su acceso a configuraciones:

*Tabla 7 Configuración Switch 3*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S3(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 15 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 #Acceso No Autorizado#

Paso 7: Verificar la conectividad de la red

Se utiliza el comando **ping** para probar la conectividad entre los dispositivos de red R1 y R2.

Para este paso se aplican los siguientes comandos:

R1#ping 172.16.1.2

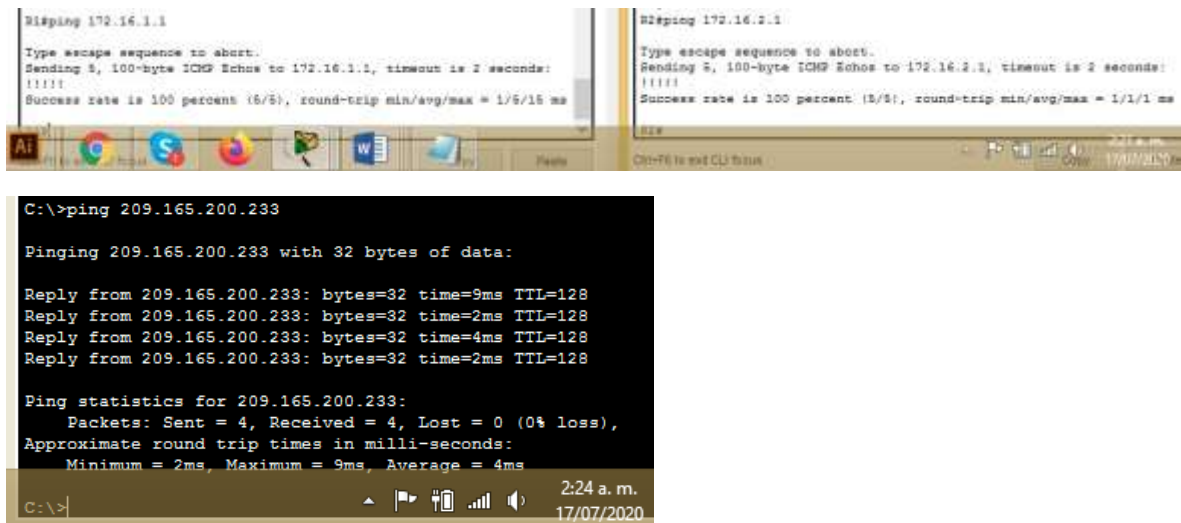
R2#ping 172.16.2.2

*Tabla 8 Verificación conectividad de red*

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	100 %
R2	R3, S0/0/1	172.16.2.1	100 %
PC de Internet	Gateway predeterminado	200.165.200.233	100%

Los resultados deberán presentar una conectividad del 100 por ciento acorde a figura 4.

*Figura 3 Verificación conectividad de red entre R1 y R2 e internet*



Fuente: propio

En ambos routers se evidencia la conectividad al 100 por ciento al igual que la conectividad en el servidor de internet.

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

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

Paso 8: Configurar S1

La configuración del S1 incluye las siguientes instrucciones:

*Tabla 9 Configuración vlans en switches*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	Se asigna la dirección IPv4 a la VLAN de administración. Se utiliza la dirección IP asignada al S1 en el diagrama de topología: S1(config-if)#ip address 192.168.99.1 255.255.255.0
Asignar el gateway predeterminado	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk
Forzar el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown
-----------------------------------	---

Descripción grafica de las configuraciones previamente mencionadas.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes instrucciones:

*Tabla 10 Configuración vlans en switch 3*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración.	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown



## Paso 9: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 11 Configuración protocolo 802.1q en Router 1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Cabe resaltar que el protocolo 802.1Q .21 se usa para comunicar los switches entre si con la finalidad de que los usuarios se puedan conectar entre vlans o redes.

## Paso 10: Verificar la conectividad de la red

Se utiliza el comando **ping** para probar la conectividad entre los switches y el R1. y así verificar metódicamente la conectividad con cada dispositivo de red. Se toman acciones de mejora o ajuste para establecer la conectividad si alguna de las pruebas falla:

*Tabla 12 Conectividad entre switches y R1*

<b>Desde</b>	<b>A</b>	<b>Dirección IP</b>	<b>Resultados de ping</b>
S1	dirección VLAN 99 en R1	192.168.99.1	100 %
S3	dirección VLAN 99 en R1	192.168.99.1	100 %

S1	dirección VLAN 21 en R1	192.168.21.1	100 %
S3	dirección VLAN 23 en R1	192.168.23.1	100 %

Se evidencia la adecuada conectividad entre los routers 1 y 2.

*Tabla 13 Resultados conectividad entre R1 y R2*

```

R1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R2#
Password:
R2#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

R2#ping 192.168.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

```

Fuente: propio

### Paso 11: Configurar RIPv2 en el R1

#### Parte 3: Configurar el protocolo de routing dinámico RIPv2

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 14 Configuración enrutamiento en R1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99

Desactive la sumarización automática R1(config-router)#no auto-summary

Figura 4 Verificación configuración RIP2 en R1

```
R1(config-router)#do show ip route Connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#
```

Ctrl+F6 to exit CLI focus 3:11 a.m. 17/07/2020

Fuente: propio

Paso 12: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2#configure terminal R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

La comunicación RIP versión 2 se aplica para la comunicación entre routers, busca que los paquetes enviados por parte de los usuarios desde diferentes redes lleguen a su destino en organizaciones diferentes.

Figura 5 Verificación configuración RIP2 en R2

```
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#
```

Ctrl+F6 to exit CLI focus 3:18 a.m. 17/07/2020

Fuente: propio

### Paso 13: Configurar RIPv3 en el R2

Se realizan configuraciones a través de RIP 2 la cual soporta subredes y características de autenticación.

La configuración del R3 incluye las siguientes tareas:

*Tabla 15 Configuración enrutamiento en R3*

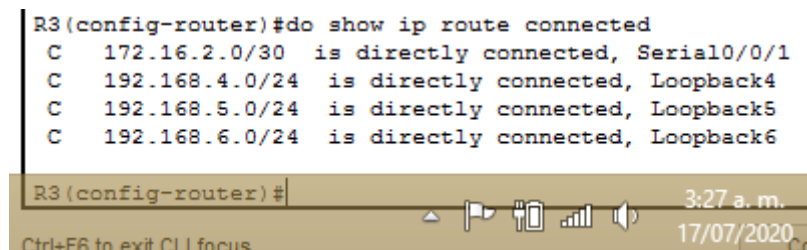
Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

### Paso 14: Verificar la información de RIP

*Figura 6 Verificación configuración RIP2 en R3*

```
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6

R3 (config-router) #
```



Fuente: propio

A continuación se verifica router 1 se visualizan las redes loopback y demás redes directamente conectadas a través de las interfaces sugeridas.

Se verifica el enrutamiento de paquetes entre las tres redes configuradas.

A continuación se responde a las preguntas sobre códigos de certificación de RIP configurados anteriormente:

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?	R2#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R2#show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R2#show run   section router rip

Figura 7 Verificación show ip protocols

```

R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 20 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0         2    2
  Serial0/0/1         2    2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.16.0.0
Passive Interface(s):
  Loopback0
Routing Information Sources:
  Gateway         Distance      Last Update
  172.16.2.1      120          00:00:10
  172.16.1.1      120          00:00:22
Distance: (default is 120)
R2#

```

trl+F6 to exit CLI focus

Copy Paste

3:31 a. m.  
17/07/2020

Fuente: propio

Figura 8 Verificación protocolo ip route rip

```

R2#show ip route rip
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R       192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:24, Serial0/0/1
R       192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:24, Serial0/0/1
R       192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:24, Serial0/0/1
R       192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:05, Serial0/0/0
R       192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:05, Serial0/0/0
R       192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:05, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
  
```

Fuente: propio

Paso 15: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Parte 4: Implementar DHCP y NAT para IPv4

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configuración DHCP y NAT para IPV4 en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
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.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Paso 16: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2#configure terminal R2(config)#username webuser privilege 15 secret cisco12345
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 17: 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 17 Verificación DHCP y NAT estática*

Elemento o tarea de configuración	Especificación
Se verifica que la PC-A haya adquirido información de IP del servidor de DHCP	Verificado y funcional
Se verifica que la PC-C haya adquirido información de IP del servidor de DHCP	Verificado y funcional

<p>Se verifica que la PC-A pueda hacer ping a la PC-C  <b>Nota:</b> Quizá sea necesario deshabilitar el firewall de la PC.</p>	<p>Verificado y funcional</p>
--	-------------------------------

Figura 9 Verificación ip dinámica en PC-A y PC-C

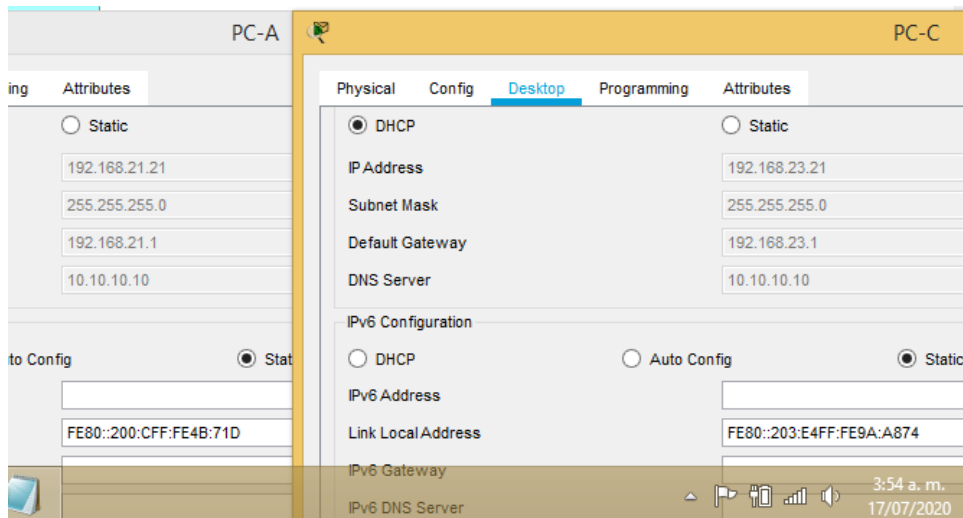
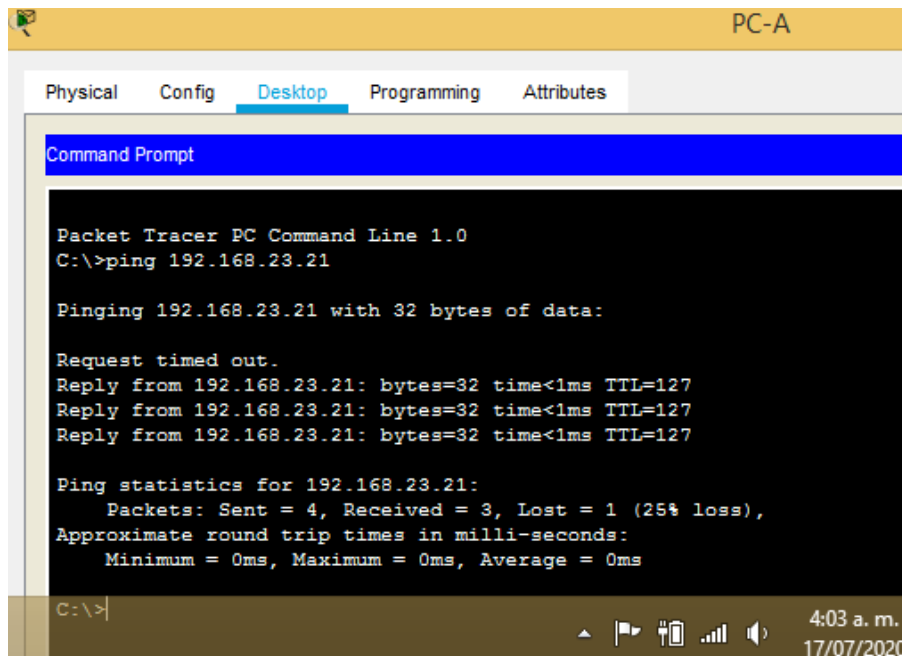


Figura 10 Verificación entre los equipos y acceso web



Fuente: propio



## Parte 5: Configurar NTP


Se realizan las respectivas validaciones y configuraciones de horario en los router 1 y 2 con el fin de que todas sus asociaciones y servidores tengan la hora correcta

*Tabla 18 Configuración NTP*

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp server 209.165.200.229
Verifique la configuración de NTP en R1.	R1#show ntp associations

*Tabla 19 Mostrar asociaciones NTP en R1*

```
R1#show ntp associations
address      ref clock      st  when  poll  reach  delay      offset      disp
~209.165.200.229.INIT.  16  -    64    0    0.00    0.00    0.48
~172.16.1.2    127.127.1.1   5   10   16    37    2.00    726123150188.00  0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```



Fuente: propio

## Parte 6: Configurar y verificar las listas de control de acceso (ACL)

*Tabla 20 Configuración controles acceso ACL*

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2#configure terminal R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#transport input telnet
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)#
Verificar que ACL funcione acorde a lo esperado	Verificado y funcional

Figura 11 Verificación de ACL en R1

```

R1>ena
R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenAcceso no autorizado

User Access Verification

Password: |

```

Fuente: propio

Paso 18: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Elemento o tarea de configuración	Especificación
<p>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</p>	<pre> R2#show access-list Standard IP access list 1   10 permit 192.168.21.0 0.0.0.255   20 permit 192.168.23.0 0.0.0.255 (90 match(es))   30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT   10 permit host 172.16.1.1 (2 match(es))  R2#show ip access-list Standard IP access list 1   10 permit 192.168.21.0 0.0.0.255   20 permit 192.168.23.0 0.0.0.255 (90 match(es))   30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT   10 permit host 172.16.1.1 (2 match(es)) </pre>
<p>Restablecer los contadores de una lista de acceso</p>	<pre> R2#clear access-list counters R2#clear ip ? </pre>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<pre> R2#show ip interface </pre>

¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations

Tabla 21 Lista de host permitidos en NAT

```

R2#
R2#show access-lists
Standard IP access list 99
 10 permit host 172.16.1.1
R2#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top 11:22 p. m. 07/06/2020

Fuente. propio

Figura 12 Mostrar mediante show ip nat translations

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

R2#
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 ---
tcp 209.165.200.233:1025192.168.23.21:1025 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1026192.168.23.21:1026 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1027192.168.23.21:1027 200.165.200.237:443200.165.200.237:443
tcp 209.165.200.233:1028192.168.23.21:1028 200.165.200.237:443200.165.200.237:443
tcp 209.165.200.233:1029192.168.23.21:1029 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1030192.168.23.21:1030 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1031192.168.23.21:1031 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1032192.168.23.21:1032 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1033192.168.23.21:1033 200.165.200.237:80 200.165.200.237:80
tcp 209.165.200.233:1034192.168.23.21:1034 209.165.200.236:80 209.165.200.236:80
tcp 209.165.200.233:1035192.168.23.21:1035 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1036192.168.23.21:1036 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1038192.168.23.21:1038 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1039192.168.23.21:1039 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1040192.168.23.21:1040 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1041192.168.23.21:1041 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1042192.168.23.21:1042 200.165.200.238:80 200.165.200.238:80
tcp 209.165.200.233:1043192.168.23.21:1043 200.165.200.233:80 200.165.200.233:80
tcp 209.165.200.233:1044192.168.23.21:1044 200.165.200.233:80 200.165.200.233:80
tcp 209.165.200.233:1045192.168.23.21:1045 200.165.200.233:80 200.165.200.233:80
tcp 209.165.200.233:1046192.168.23.21:1046 200.165.200.233:80 200.165.200.233:80

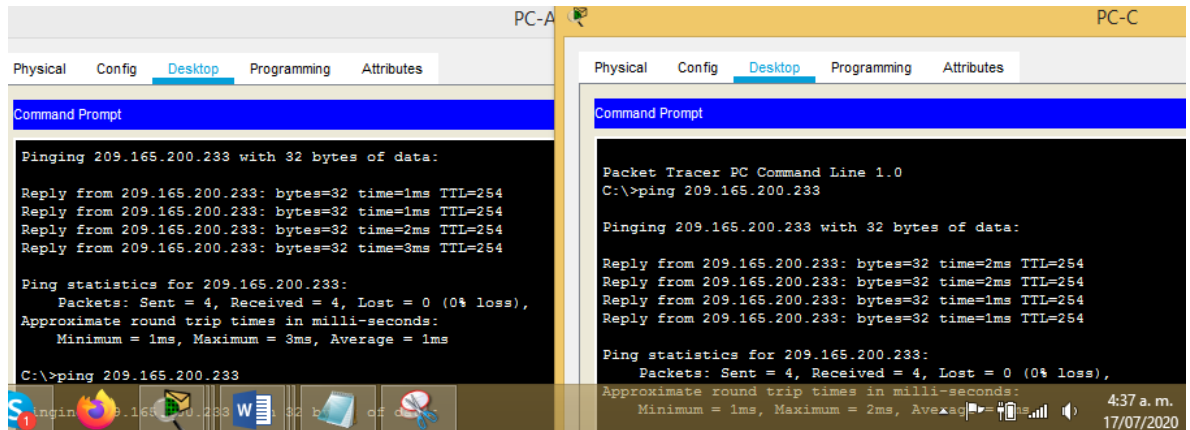
```

Ctrl+F6 to exit CLI focus

4:32 a. m. 17/07/2020

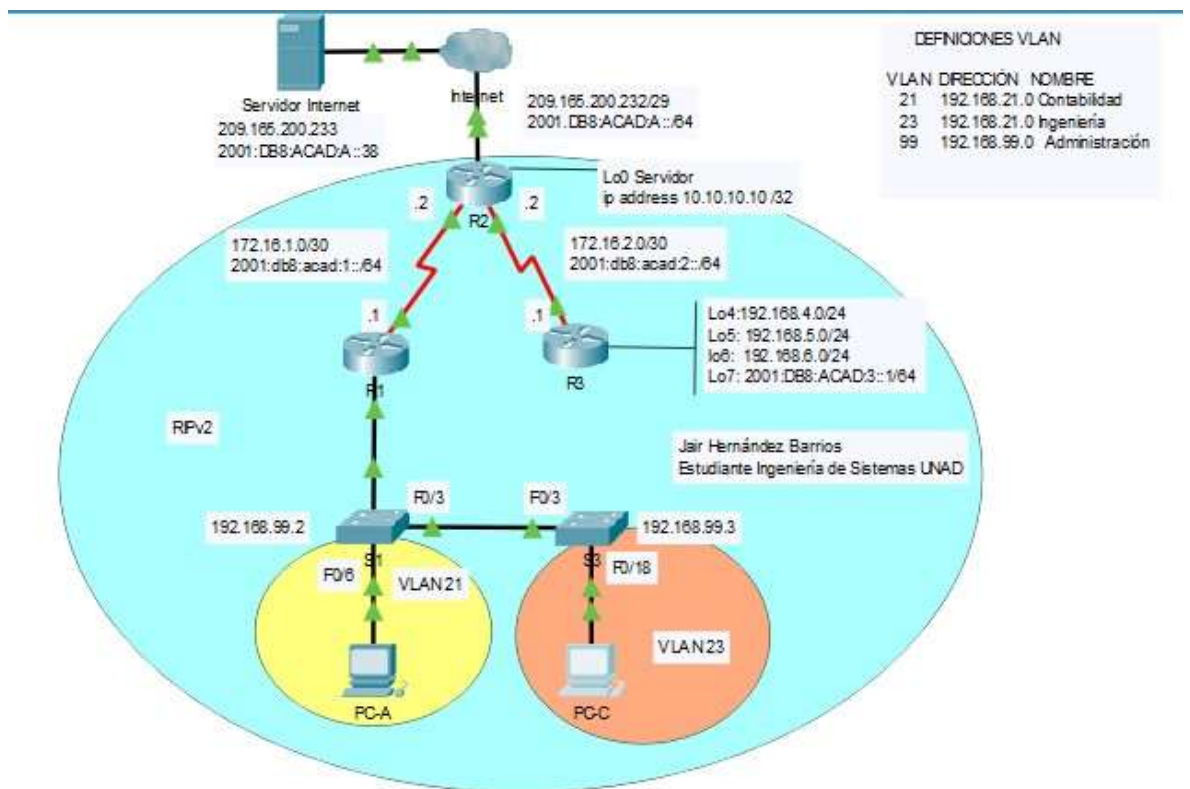
Fuente: propio

Figura 13 Verificación conectividad al servidor



Fuente: propio

Figura 14 Topología Final Escenario 1



Fuente: propio

## ESCENARIO 2:

### Actividad Práctica Temario Escenario 2

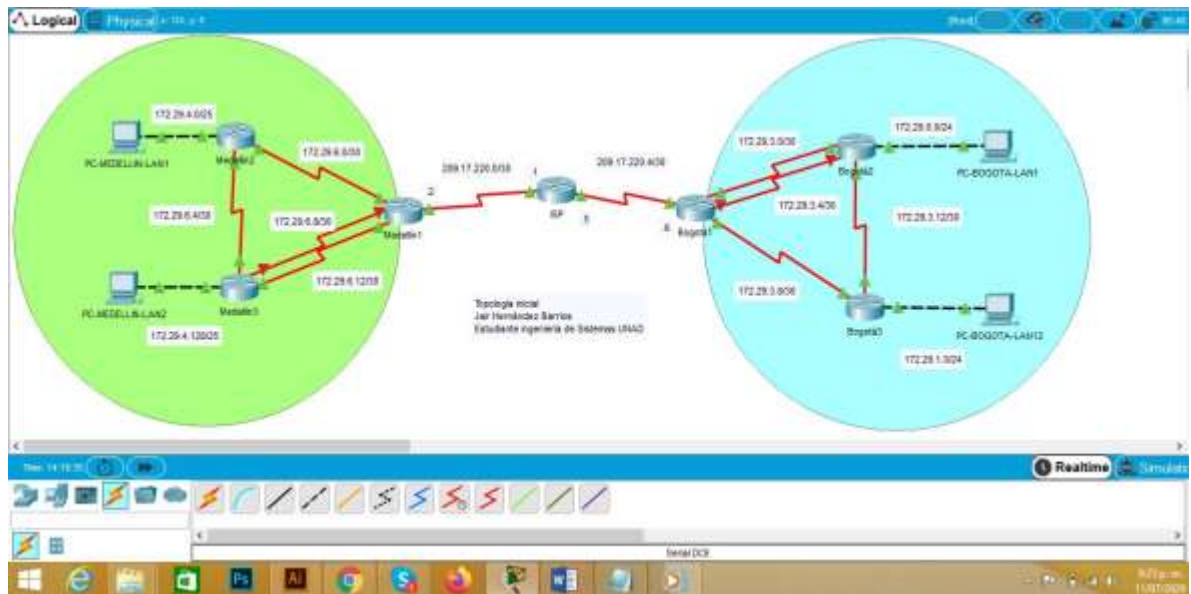
Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Se habilitará NAT de sobrecarga en los routers Bogota1 y medellin1.

Figura 15 Topología inicial escenario 2



Fuente: propio

Se realizan las rutinas de diagnóstico y se dejan los equipos listos para su configuración (se asignan nombres de equipos, claves de seguridad, etc), de igual manera se asignan las redes acorde al planteamiento inicial, se configuran las interfaces en los routers, así como en los PC LAN 1 y 2 para ambos casos Medellín y Bogotá.

Para el presente caso se cuenta con un total de cuatro vlan, dos por cada red las cuales tendrán direccionamiento dinámico o DHCP.

Tabla 22 Configuraciones básicas routers Medellín y Bogotá

A continuación se realizan las respectivas inicializaciones en los routers, switches, se configuran los parámetros de acceso a consola y telnet, se configura banner modo mensaje, esto con el fin de proteger las configuraciones, seguridad y la estabilidad de las redes.

Dispositivo	Configuración Básica
<b>Medellín1</b>	<pre> Router&gt;enable Router#configure terminal 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)# exit Medellin1(config)#line vty 0 15 Medellin1(config-line)# password cisco Medellin1(config-line)# login Medellin1(config-line)#service password-encryption Medellin1(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." Medellin1(config)#end Medellin1#wr                     </pre>
<b>Medellín2</b>	<pre> Router&gt;enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. 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)# exit Medellin2(config)#line vty 0 15 Medellin2(config-line)# password cisco Medellin2(config-line)# login Medellin2(config-line)#service password-encryption Medellin2(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." Medellin2(config)#end Medellin2#wr                     </pre>
<b>Medellin3</b>	<pre> Router&gt;enable Router#configure terminal Router(config)#hostname Medellin3                     </pre>

	<pre> Medellin3(config)#enable secret class Medellin3(config)#line console 0 Medellin3(config-line)# password cisco Medellin3(config-line)# login Medellin3(config-line)# exit Medellin3(config)#line vty 0 15 Medellin3(config-line)# password cisco Medellin3(config-line)# login Medellin3(config-line)#service password-encryption Medellin3(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." Medellin3(config)#end Medellin3#wr </pre>
<b>Bogota1</b>	<pre> Router&gt;enable Router#configure terminal 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)# exit Bogota1(config)#line vty 0 15 Bogota1(config-line)# password cisco Bogota1(config-line)# login Bogota1(config-line)#service password-encryption Bogota1(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." Bogota1(config)#end Bogota1#wr </pre>
<b>Bogota2</b>	<pre> Router&gt;enable Router#configure terminal 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)# exit Bogota2(config)#line vty 0 15 Bogota2(config-line)# password cisco Bogota2(config-line)# login Bogota2(config-line)#service password-encryption Bogota2(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." </pre>

	<pre>Bogota2(config)#end Bogota2#wr</pre>
<b>Bogota3</b>	<pre>Router&gt;enable Router#configure terminal 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)# exit Bogota3(config)#line vty 0 15 Bogota3(config-line)# password cisco Bogota3(config-line)# login Bogota3(config-line)#service password-encryption Bogota3(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." Bogota3(config)#end Bogota3#wr</pre>
<b>ISP</b>	<pre>Router&gt;enable Router#configure terminal 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)# exit ISP(config)#line vty 0 15 ISP(config-line)# password cisco ISP(config-line)# login ISP(config-line)#service password-encryption ISP(config)#banner motd "prohibido el acceso no autorizado por Jair Hernandez." ISP(config)#end ISP#wr</pre>

Acorde a las configuraciones inicialmente planteadas, se elabora el cuadro de direccionamiento IP la cual nos permite identificar las direcciones IP especificas en cada interfaz con su respectiva mascara de red, así como las puertas de enlace predeterminada, para el caso de las LAN 1 y 2 en las dos redes Bogotá y Medellín.



### Cuadro de direccionamiento IP

Se establece el cuadro de direccionamiento IP acorde con las interfaces sugeridas y las redes asignadas.

Dispositivo	Interfaz	Conexión	Dirección IP	Máscara de Subred	Gateway Predeterminado
Medellín1	S0/0/0	Medellín3	172.29.6.9	255.255.255.252	
	S0/1/0	ISP	209.17.220.2	255.255.255.252	N.A
	S0/0/1	Medellín2	172.29.6.1	255.255.255.252	N.A
	S0/1/1	Medellín3-1	172.29.6.13	255.255.255.252	N.A
Medellín2	S0/0/0	Medellín1	172.29.6.2	255.255.255.252	N.A
	S0/0/1	Medellín3	172.29.6.5	255.255.255.252	N.A
	G0/0	Medellín-LAN1	172.29.4.1	255.255.255.128	N.A
Medellín3	S0/0/0	Medellín1	172.29.6.10	255.255.255.252	N.A
	S0/0/1	Medellín1	172.29.6.14	255.255.255.252	N.A
	S0/1/0	Medellín2	172.29.6.6	255.255.255.252	N.A
	G0/0	Medellín-LAN2	172.29.4.129	255.255.255.128	N.A
Bogotá1	S0/0/0	ISP	209.17.220.6	255.255.255.252	
	S0/0/1	Bogotá3	172.29.3.1	255.255.255.252	N.A
	S0/1/0	Bogotá3	172.29.3.5	255.255.255.252	N.A
	S0/1/1	Bogotá2	172.29.3.9	255.255.255.252	N.A
Bogotá2	S0/0/0	Bogotá1	172.29.3.10	255.255.255.252	N.A
	S0/0/1	Bogotá3	172.29.3.13	255.255.255.252	N.A
	G0/0	Bogotá-LAN1	172.29.0.1	255.255.255.0	N.A
Bogotá3	S0/0/0	Bogotá1	172.29.3.6	255.255.255.252	N.A
	S0/0/1	Bogotá1	172.29.3.2	255.255.255.252	N.A
	S0/1/0	Bogotá2	172.29.3.14	255.255.255.252	
	G0/0	Bogotá-LAN2	172.29.1.1	255.255.255.0	N.A
ISP	S0/0/0	Medellín1	209.17.220.1	255.255.255.252	N.A
	S0/0/1	Bogotá1	209.17.220.5	255.255.255.252	N.A
PC-Medellín-LAN1	Fa0	Medellín 2	DHCP	255.255.255.0	172.29.4.1
PC-Medellín-LAN2	Fa0	Medellín 3	DHCP	255.255.255.0	172.29.4.129
PC-Bogotá-LAN1	Fa0	Bogotá 2	DHCP	255.255.255.0	172.29.0.1
PC-Bogotá-LAN2	Fa0	Bogotá 3	DHCP	255.255.255.0	172.29.1.1

Tener un cuadro de direccionamiento IP permite identificar y clarificar las interfaces para conectar, así como las configuraciones posteriores.

Se realizan las configuraciones de asignación de direccionamiento IP, puertos de enlace, velocidad de comunicación, descripciones, una vez se han configurado se procede a encender los dispositivos.

Tabla 23 Configuración direccionamiento IP Medellín y Bogotá

Dispositivo	Configuración Direccionamiento IP
<b>Medellin1</b>	<pre> Medelln1#Configure terminal Medelln1(config)#int s0/1/0 Medelln1(config-if)# description Conexion a ISP Medelln1(config-if)# ip address 209.17.220.2 255.255.255.252 Medelln1(config-if)# clock rate 128000 Medelln1(config-if)# no shutdown  Medelln1#Configure terminal Medelln1(config)#int s0/0/1 Medelln1(config-if)# description Conexion a <b>Medellin2</b> Medelln1(config-if)# ip address 172.29.6.1 255.255.255.252 Medelln1(config-if)# no shutdown Medelln1(config-if)# end Medelln1#wr  Medellin1#Configure terminal Medelln1(config)#int s0/0/0 Medelln1(config-if)# description Conexion a Medellin3 Medelln1(config-if)# ip address 172.29.6.9 255.255.255.252 Medelln1(config-if)# clock rate 128000 Medelln1(config-if)# no shutdown Medelln1(config-if)# end Medelln1#wr  Medelln1#Configure terminal Medelln1(config)#int s0/1/1 Medelln1(config-if)# description Conexion a Medellin3 Medelln1(config-if)# ip address 172.29.6.13 255.255.255.252 Medelln1(config-if)# no shutdown Medelln1(config-if)# end Medelln1#wr </pre>
<b>Medellin2</b>	<pre> Medelln2#Configure terminal Medelln2(config)#int s0/0/0 Medelln2(config-if)# description Conexion a Medellin1 Medelln2(config-if)# ip address 172.29.6.9 255.255.255.252 Medelln2(config-if)# clock rate 128000 Medelln2(config-if)# no shutdown </pre>

	<pre> Medelln2(config-if)# end Medelln2#wr  Medelln2#Configure terminal Medelln2(config)#int s0/0/1 Medelln2(config-if)# description Conexion a Medellin3 Medelln2(config-if)# ip address 172.29.6.5 255.255.255.252 Medelln2(config-if)# clock rate 128000 Medelln2(config-if)# no shutdown Medelln2(config-if)# end Medelln2#wr </pre>
<b>Medellin3</b>	<pre> Medelln3#Configure terminal Medelln3(config)#int s0/0/0 Medelln3(config-if)# description Conexion a Medellin1 Medelln3(config-if)# ip address 172.29.6.10 255.255.255.252 Medelln3(config-if)# no shutdown Medelln3(config-if)# end Medelln3#wr  Medelln3#Configure terminal Medelln3(config)#int s0/0/1 Medelln3(config-if)# description Conexion a Medellin1 Medelln3(config-if)# ip address 172.29.6.14 255.255.255.252 Medelln3(config-if)# clock rate 128000 Medelln3(config-if)# no shutdown Medelln3(config-if)# end Medelln3#wr  Medelln3#Configure terminal Medelln3(config)#int s0/1/0 Medelln3(config-if)# description Conexion a Medellin2 Medelln3(config-if)# ip address 172.29.6.6 255.255.255.252 Medelln3(config-if)# no shutdown Medelln3(config-if)# end Medelln3#wr </pre>
<b>Bogota1</b>	<pre> Bogota1#Configure terminal Bogota1(config)#int s0/0/1 Bogota1(config-if)# description Conexion a ISP Bogota1(config-if)# ip address 209.17.220.6 255.255.255.252 Bogota1(config-if)# no shutdown  Bogota1#Configure terminal Bogota1(config)#int s0/0/1 </pre>

	<pre> Bogota1(config-if)# description Conexion a 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#Configure terminal Bogota1(config)#int s0/1/0 Bogota1(config-if)# description Conexion a 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  Bogota1#Configure terminal Bogota1(config)#int s0/1/1 Bogota1(config-if)# description Conexion a 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)# end Bogota1#wr </pre>
<b>Bogota2</b>	<pre> Configure terminal int s0/0/0 description Conexion a Bogota1 ip address 172.29.3.10 255.255.255.252 clock rate 128000 no shutdown end wr  Bogota2#Configure terminal Bogota2(config)#int s0/0/1 Bogota2(config-if)# description Conexion a Bogota3 Bogota2(config-if)# ip address 172.29.3.13 255.255.255.252 Bogota2(config-if)# no shutdown Bogota2(config-if)# end Bogota2#wr </pre>
<b>Bogota3</b>	<pre> Bogota3#Configure terminal Bogota3(config)#int s0/0/1 Bogota3(config-if)# description Conexion a Bogota1 Bogota3(config-if)# ip address 172.29.3.2 255.255.255.252 Bogota3(config-if)# no shutdown </pre>

	<pre> Bogota3(config-if)# end Bogota3#wr  Bogota3#Configure terminal Bogota3(config)#int s0/0/0 Bogota3(config-if)# description Conexion a Bogota1 Bogota3(config-if)# ip address 172.29.3.6 255.255.255.252 Bogota3(config-if)# no shutdown Bogota3(config-if)# end Bogota3#wr  Bogota3#Configure terminal Bogota3(config)#int s0/1/0 Bogota3(config-if)# description Conexion a Bogota2 Bogota3(config-if)# ip address 172.29.3.14 255.255.255.252 Bogota3(config-if)# clock rate 128000 Bogota3(config-if)# no shutdown Bogota3(config-if)# end Bogota3#wr </pre>
<b>ISP</b>	<pre> ISP#Configure terminal ISP(config)#int s0/0/0 ISP(config-if)# description Conexion a Medellin1 ISP(config-if)# ip address 209.17.220.1 255.255.255.252 ISP(config-if)# clock rate 128000 ISP(config-if)# no shutdown ISP(config-if)# end ISP#wr  ISP#Configure terminal ISP(config)#int s0/0/1 ISP(config-if)# description Conexion a 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 ISP(config-if)# end ISP#wr </pre>

Se puede evidenciar, que una vez ejecutada la instrucción show ip interface brief se muestran las interfaces con el direccionamiento IP asignado de forma manual, de igual manera se verifica el estado de encendido o “arriba” de cada uno de ellos.

Figura 16 lista conexión interfaces ISP y Medellín1



Fuente: propio

Figura 17 Conexión interfaces seriales Medellín2 y Medellín3



Fuente: propio

### Configuración del enrutamiento

Se realizan las configuraciones de enrutamiento en la red usando el protocolo OSPF versión 2, se declara la red principal, y se desactiva la sumarización automática.

Se utiliza el enrutamiento OSPF, con el fin pueda haber comunicación simultanea entre los routers y habilitarse de forma segura en tanto alguno pueda llegar a fallar, este permite un routing o enrutamiento dinámico similar al enrutamiento que se realiza con RIP.

En estas configuraciones también se ejecuta la instrucción ip route, que se define para toda IP conocida y cualquier mascara de red salga por la dirección asignada al proveedor de servicios de internet en este caso en particular.

Tabla 24 Enrutamiento OSPF en Routers Medellín y Bogotá

Dispositivo	Configuración OSPF en los Routers
<b>Medellin1</b>	<pre> Medellin1#configure terminal Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medellin1(config)#router ospf 1 Medellin1(config-router)#router-id 1.1.1.1 Medellin1(config-router)# network 172.29.6.0 0.0.0.3 area 0           </pre>

	<pre> Medelln1(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medelln1(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medelln1(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medelln1(config-router)# default-information originate Medelln1(config-router)# end Medelln1#wr </pre>
<b>Medellin2</b>	<pre> Medelln2#configure terminal Medelln2(config)#router ospf 1 Medelln2(config-router)#router-id 2.2.2.2 Medelln2(config-router)# network 172.29.6.0 0.0.0.3 area 0 Medelln2(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medelln2(config-router)# network 172.29.4.0 0.0.0.127 area 0 Medelln2(config-router)# default-information originate Medelln2(config-router)#passive-interface g0/0 Medelln2(config-router)# end Medelln2#wr </pre>
<b>Medellin3</b>	<pre> Medelln3#configure terminal Medelln3(config)#router ospf 1 Medelln3(config-router)#router-id 3.3.3.3 Medelln3(config-router)# network 172.29.6.4 0.0.0.3 area 0 Medelln3(config-router)# network 172.29.6.8 0.0.0.3 area 0 Medelln3(config-router)# network 172.29.6.12 0.0.0.3 area 0 Medelln3(config-router)# network 172.29.4.0 0.0.0.127 area 0 Medelln3(config-router)# default-information originate Medelln3(config-router)#passive-interface g0/0 Medelln3(config-router)# end Medelln3#wr </pre>
<b>Bogota1</b>	<pre> Bogota1#configure terminal Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota1(config)#router ospf 1 Bogota1(config-router)#router-id 4.4.4.4 Bogota1(config-router)# network 172.29.3.4 0.0.0.3 area 0 Bogota1(config-router)# network 172.29.3.0 0.0.0.3 area 0 Bogota1(config-router)# network 172.29.3.8 0.0.0.3 area 0 Bogota1(config-router)# network 172.29.3.12 0.0.0.3 area 0 Bogota1(config-router)# default-information originate Bogota1(config-router)# end Bogota1#wr </pre>
<b>Bogota2</b>	<pre> Bogota2#configure terminal Bogota2(config)#router ospf 1 Bogota2(config-router)# router-id 5.5.5.5 Bogota2(config-router)# network 172.29.3.8 0.0.0.3 area 0 </pre>

	<pre> Bogota2(config-router)# network 172.29.3.12 0.0.0.3 area 0 Bogota2(config-router)# network 172.29.1.0 0.0.0.255 area 0 Bogota2(config-router)# default-information originate Bogota2(config-router)# passive-interface g0/0 Bogota2(config-router)# end Bogota2#wr </pre>
<b>Bogota3</b>	<pre> Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)# router-id 6.6.6.6 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 Bogota3(config-router)# network 172.29.3.12 0.0.0.3 area 0 Bogota3(config-router)# network 172.29.0.0 0.0.0.255 area 0 Bogota3(config-router)# default-information originate Bogota3(config-router)# passive-interface g0/0 Bogota3(config-router)# end Bogota3#wr </pre>

Configuración equipos PC LAN 1 y 2 para Medellín y Bogotá.

Se realizan las respectivas configuraciones de asignación IP a las interfaces Gigabit Ethernet las cuales comunicas a los equipos LAN.

*Figura 18 Configuración PC'S LAN*

PC LAN 1 MEDELLIN	<pre> Medelln2#configure terminal Medelln2(config)#interface gi0/0 Medelln2(config-if)#ip address 172.29.4.1 255.255.255.128 Medelln2(config-if)#no shutdown Medelln2(config-if)#end Medelln2#wr </pre>
PC LAN 2 MEDELLIN	<pre> Medelln3#configure terminal Medelln3(config)#interface gi0/0 Medelln3(config-if)#ip address 172.29.4.129 255.255.255.128 Medelln3(config-if)#no shutdown Medelln3(config-if)#end Medelln3#wr </pre>
PC LAN 1 BOGOTA	<pre> Bogota3#configure terminal Bogota3(config)#interface gi0/0 Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0 Bogota3(config-if)#no shutdown Bogota3(config-if)#end </pre>



	Bogota3#wr
PC BOGOTÁ LAN 2	Bogota2#configure terminal Bogota2(config)#interface gi0/0 Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0 Bogota2(config-if)#no shutdown Bogota2(config-if)#end Bogota2#wr

Los Routers Medellin1 y Bogota1 añaden a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Se realiza el enrutamiento a través del comando IP route de toda la red privada hacia el direccionamiento público de las interfaces correspondientes al router de nombre ISP, para toda ip conocida direccionar hacia la salida a la red.

Figura 19 Configuración rutas distribuidas OSPF Routers Medellín1 y Bogotá1

Dispositivo	Configuración Ruta Distribuida en OSPF
<b>Medellin1</b>	Medelln1#configure terminal Medelln1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 Medelln1(config)#router ospf 1 Medelln1(config-router)# default-information originate
<b>Bogota1</b>	Bogota1#configure terminal Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5 Bogota1(config)#router ospf 1 Bogota1(config-router)# default-information originate

Mediante el comando show ip route ospf se identifica las direcciones IP y su trazabilidad a través de las interfaces de los router configurados.

Figura 20 Verificación conexiones OSPF

```

Medellin1#show ip route ospf
Medellin1#show ip route ospf
Medellin1#show ip route ospf
172.29.0.0/16 is variably subnetted, 10 subnets, 8 masks
O   172.29.4.0 [110/48] via 172.29.4.2, 00:00:36, Serial0/0/1
O   172.29.4.128 [110/48] via 172.29.4.14, 00:00:36, Serial0/1/1
O   172.29.6.4 [110/128] via 172.29.6.14, 00:00:36, Serial0/1/1
    [110/128] via 172.29.6.2, 00:00:36, Serial0/0/1

Bogota1#show ip route ospf
Bogota1#show ip route ospf
Bogota1#show ip route ospf
172.29.0.0/16 is variably subnetted, 5 subnets, 3 masks
O   172.29.1.0 [110/24] via 172.29.3.6, 00:01:03, Serial0/1/0
O   172.29.3.12 [110/24] via 172.29.3.10, 00:01:03, Serial0/1/1
O   172.29.3.12 [110/128] via 172.29.3.6, 00:01:03, Serial0/1/0
    [110/128] via 172.29.3.10, 00:01:03, Serial0/1/1
  
```

Fuente: propio

El Router ISP tiene una ruta estática dirigida hacia cada red interna de Medellín y Bogotá, en este sentido ISP se configura comunicación con las interfaces públicas de los routers Bogotá1 y Medellín1,

Tabla 25 Rutas estáticas de ISP direcciones públicas

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

Parte 2: Tabla de Enrutamiento.

- Se verifica la tabla de enrutamiento en cada uno de los Routers para comprobar las redes y sus rutas, las cuales se han identificado en sus puertas de enlace de forma numérica.

Figura 21 Lista conexión protocolo OSPF



Fuente: propio

- Se verifica el balanceo de carga que presentan los Routers.
- Se verifican las interfaces directamente conectadas de Bogotá y Medellín

Figura 22 Configuración rutas estáticas Routers Medellín y Bogotá



Fuente: propio

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

Figura 23 Conexiones OSPF en Bogotá y Medellín 1



Fuente: propio

- d. Las tablas de los Routers restantes permiten visualizar rutas redundantes para el caso de la ruta por defecto.
- e. El Router ISP solo indica sus rutas estáticas adicionales a las directamente conectadas.

**Parte 3: Deshabilitar la propagación del protocolo OSPF.**

- a. Se deshabilita la propagación del protocolo OSPF en los Router que tengan conexiones hacia las LAN.

Tabla 26 Deshabilitación protocolo OSPF Routers Medellín 1 y 2, Bogotá 1 y 2.

Dispositivo	Deshabilitación propagación del protocolo OSPF
<b>Medellin2</b>	Medellin2#configure terminal Medellin2(config)#router ospf 1 Medellin2(config-router)#passive-interface g0/0
<b>Medellin3</b>	Medellin3#configure terminal Medellin3(config)#router ospf 1 Medellin3(config-router)#passive-interface g0/0
<b>Bogota2</b>	Bogota2#configure terminal Bogota2(config)#router ospf 1 Bogota2(config-router)# passive-interface g0/0
<b>Bogota3</b>	Bogota3#configure terminal Bogota3(config)#router ospf 1 Bogota3(config-router)# passive-interface g0/0

Parte 5: Configurar encapsulamiento y autenticación PPP.

- a. Según la topología el enlace Bogota1 con ISP es configurado con autenticación PAT.
- b. El enlace Medellin1 con ISP es configurado con autenticación CHAT.

*Tabla 27 Configuración autenticación CHAT y PAP*

Dispositivo	Encapsulación y Autenticación PPP
<b>Bogota1</b>	<pre>Bogota1#configure terminal Bogota1(config)#username ISP password cisco Bogota1(config)#int s0/0/0 Bogota1(config-if)#encapsulation ppp Bogota1(config-if)#ppp authentication chap</pre>
<b>Medellin1</b>	<pre>Medelln1#configure terminal Medelln1(config)#int s0/1/0 Medelln1(config-if)#encapsulation ppp Medelln1(config-if)#ppp authentication pap Medelln1(config-if)#ppp pap sent-username Medellin1 password cisco Medelln1(config-if)#end Medelln1#wr</pre>
<b>ISP</b>	<pre>ISP#configure terminal ISP(config)#username Bogota1 password cisco ISP(config)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap  ISP#configure terminal ISP(config)#int s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP password cisco</pre>

Parte 6: Configuración del servicio DHCP.

- a. Se configuran las redes Bogota2 y Bogota3 donde el Router Bogota 2 es el servidor DHCP para ambas redes LAN.
- b. El Router Bogota3 habilita el paso de los mensajes broadcast hacia la IP del Router Bogota2.
- c. Se configura la red Medellin2 y Medellin3 donde el Router Bogota2 es el servidor DHCP para ambas redes LAN.
- d. El Router Medellin3 habilita el paso de los mensajes Broadcast hacia la IP del Router Medellin2.

Se realizan las configuraciones correspondientes para enrutamiento dinámico, inicialmente se excluyen el rango de direcciones 172.29.4.129 a 172.29.4.132.

*Tabla 28 Configuración Configuración DHCP en routers Medellín 2y3, Bogotá 3y2*

Dispositivo	Configuración DHCP
<b>Medellin2</b>	<pre> Medelln2#configure t Medelln2#configure terminal Medelln2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132 Medelln2(config)#ip dhcp pool MEDELLIN-LAN1 Medelln2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medelln2(dhcp-config)#default-server 172.29.4.2 Medelln2(dhcp-config)#default-router 172.29.4.1 Medelln2(dhcp-config)#dns-server 172.29.4.1  Medelln2(config)#ip dhcp pool MEDELLIN-LAN2 Medelln2(dhcp-config)#network 172.29.4.128 255.255.255.128 Medelln2(dhcp-config)#default-router 172.29.4.129 Medelln2(dhcp-config)#dns-server 172.29.4.1 Medelln2(dhcp-config)#exit </pre>
<b>Medellin3</b>	<pre> Medelln3#configure terminal Medelln3(config)#int g0/0 Medelln3(config-if)#ip helper-address 172.29.6.5 </pre>
<b>Bogota3</b>	<pre> Bogota3#configure terminal Bogota3(config)#ip dhcp excluded-address 172.29.0.0 172.29.0.4 Bogota3(config)#ip dhcp pool BOGOTA-LAN1 Bogota3(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota3(dhcp-config)#default-router 172.29.0.1 Bogota3(dhcp-config)#dns-server 172.29.0.1 Bogota3(dhcp-config)#exit  Bogota3(dhcp-config)#default-router 172.29.0.1 Bogota3(dhcp-config)#dns-server 172.29.0.1 Bogota3(dhcp-config)#exit Bogota3(config)#ip dhcp pool BOGOTA-LAN2 Bogota3(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota3(dhcp-config)#default-router 172.29.1.1 Bogota3(dhcp-config)#dns-server 172.29.0.1 Bogota3(dhcp-config)#exit </pre>
<b>Bogota2</b>	<pre> Bogota2#configure terminal Bogota2(config)#int g0/0 Bogota2(config-if)#ip helper-address 172.29.3.14 </pre>

Se evidencia que los PC de la red Medellín detectan la configuración IP dinámica en forma automática.

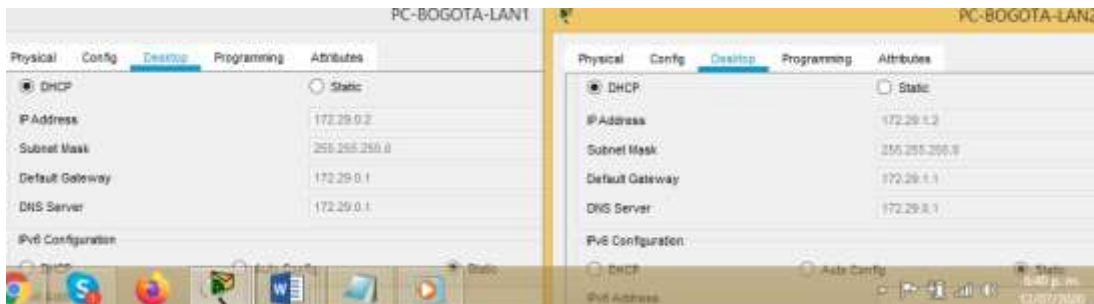
*Figura 24 Verificación DHCP LANS Medellín*



Fuente: propio

Se evidencia que los PC de la red Bogotá detectan la configuración IP dinámica en forma automática.

*Figura 25 Verificación DHCP LANS Bogotá*



Fuente: propio

Configuración de PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Medellin1 y Bogota1), los Routers internos de una ciudad no podrán llegar hasta los Routers internos en el otro extremo, sólo existirá comunicación hasta los Routers Medellin1, ISP y Bogota1.
- b. Después de verificar lo indicado en el paso anterior se procede a configurar el NAT en el Router Bogota1. Se comprueba que la traducción de direcciones indican las interfaces de entrada y de salida. Se verifica que al realizar una prueba de ping, la dirección privada se traduce automáticamente a la dirección de la interfaz serial externa del Router Bogota1 con una ip pública.

- c. Se procede a configurar el NAT en el Router Medellin1, se comprueba que la traducción de direcciones indica las interfaces de entrada y de salida. Se realizan pruebas de ping, la dirección privada es traducida automáticamente a la dirección de la interfaz externa con ip pública del Router Medellin1, cómo diferente puerto.

*Tabla 29 Configurar NAT en routers Medellín1 y Bogotá 1*

Dispositivo	Configuración PAT
<b>Medellin1</b>	<pre> Medelln1#configure terminal Medelln1(config)#ip access-list standard LAN-MEDELLIN Medelln1(config-std-nacl)# permit 172.29.0.0 255.255.0.0 Medelln1(config-std-nacl)# exit Medelln1(config)#ip nat inside source list LAN-MEDELLIN interface s0/1/0 overload Medelln1(config)#int s0/1/0 Medelln1(config-if)# ip nat outside Medelln1(config-if)#exit Medelln1(config)#int s0/1/1 Medelln1(config-if)# ip nat inside Medelln1(config-if)# exit Medelln1(config)#int s0/0/0 Medelln1(config-if)# ip nat inside Medelln1(config-if)#int s0/0/1 Medelln1(config-if)# ip nat inside Medelln1(config-if)# exit Medelln1(config)#end Medelln1#wr </pre>
<b>Bogota1</b>	<pre> Bogota1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Bogota1(config)#ip access-list standard LAN-BOGOTA Bogota1(config-std-nacl)# permit 172.29.0.0 0.0.255.255 Bogota1(config-std-nacl)# exit Bogota1(config)#ip nat inside source list LAN-BOGOTA interface s0/0/0 overload Bogota1(config)#int s0/0/0 Bogota1(config-if)# ip nat outside Bogota1(config-if)#exit Bogota1(config)#int s0/1/0 Bogota1(config-if)# ip nat inside Bogota1(config-if)# exit Bogota1(config)#int s0/0/1 Bogota1(config-if)# ip nat inside </pre>

```

Bogota1(config-if)# exit
Bogota1(config)#int s0/1/1
Bogota1(config-if)# ip nat inside
Bogota1(config-if)# exit
Bogota1(config)#end
Bogota1#wr

```

Se realiza un test de conectividad a través del comando ping, este evidencia la traducción ip privada a ip pública, con utilización de diferentes puertos lo que se conoce como Port Adress Traslation.

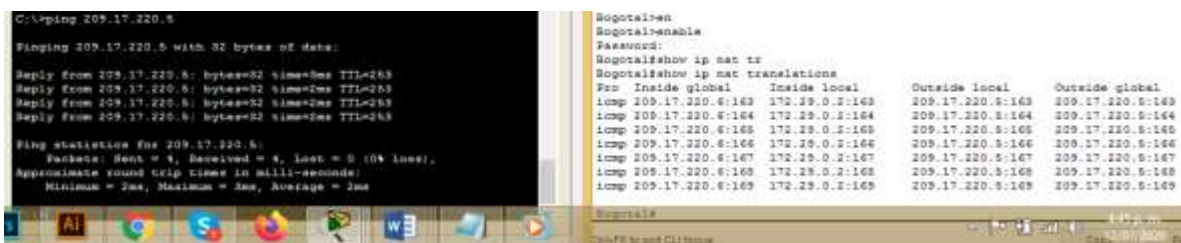
Figura 26 Verificación conectividad de la NAT Bogotá desde LAN2



Fuente: propio

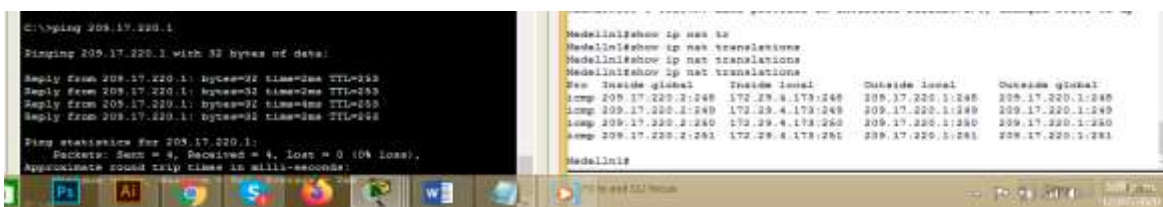
Se evidencia las direcciones locales entrantes y las IP públicas de salida con diferentes puertos.

Figura 27 Verificación conectividad de la NAT Bogotá desde LAN1



Fuente: propio

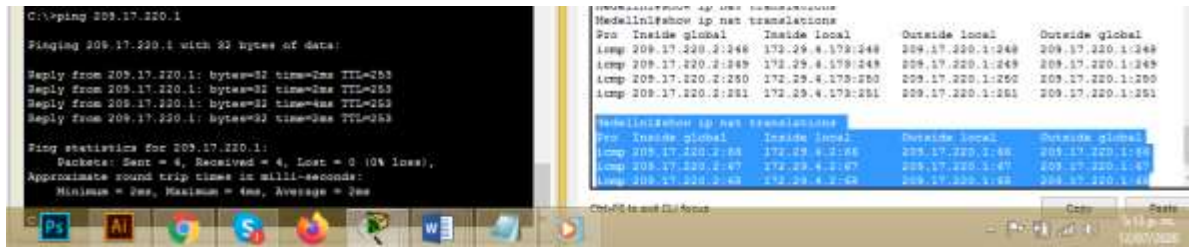
Figura 28 Verificación traducción NAT desde LAN 2



Fuente: propio



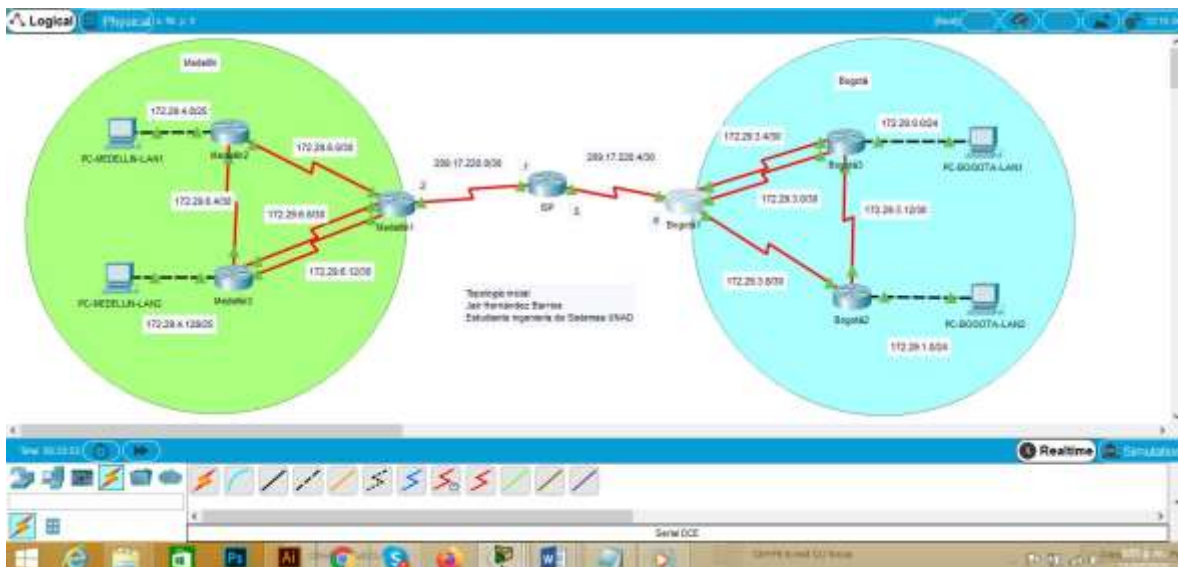
Figura 29 Verificación NAT desde LAN 1



Fuente: propio

Una vez verificada la conectividad se realizan pruebas, evidenciando el adecuado funcionamiento de comunicación de dos redes Bogotá y Medellín, con traducción de PAT y con servicio de DHCP en las redes LAN.

Figura 30 Topología final conectada



Enlaces a escenarios virtuales realizados en Packet Tracer

Escenario 1:

<https://drive.google.com/file/d/1k5cwnL44L9wZYbVuGIn2bPgasOwm0gTd/view?usp=sharing>

Escenario 2:

<https://drive.google.com/file/d/1A9SmcghZTruzUjsinK1KNENalo-f-SWQ/view?usp=sharing>

## CONCLUSIONES

Se adquieren conocimientos específicos para la comunicación entre dispositivos aplicando reglas o parámetros de comunicación como es el caso de vlans, con puertos específicos autorizados, listas de redes permitidas.

Es importante resaltar la traducción de direcciones IP privadas a IP comerciales o públicas autorizadas como medida de protección de la información como buena práctica de las organizaciones en telecomunicaciones o administradores de la red.

La formulación de estrategias para usar menos direcciones IPv4 ha permitido avanzar en métodos como la traducción de direcciones privadas a una IP con múltiples puertos de comunicación como es el caso de PAT.

El dominio en el acceso a los diferentes dispositivos de configuración de red es hoy en día clave en la protección de datos, para lo cual existen grupos y organizaciones dedicadas a establecer vulnerabilidades tales como red team, blue team, centros de incidentes de seguridad entre otros.

El aplicar adecuadamente los conceptos y protocolos en las redes permite reducir el riesgo de pérdida de información así como optimiza el flujo de información en las organizaciones.

La adecuada aplicación de las normas técnicas de redes y eléctricas permite el rendimiento adecuado de los centros de datos, configuraciones y equipos en la red.

## BIBLIOGRAFÍA

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

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

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

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

Temática: División de redes IP en subredes  
CISCO CCNA2. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de [https://1drv.ms/u/s!AmlJYei-NT1lhqCT9VCtl\\_pLtPD9](https://1drv.ms/u/s!AmlJYei-NT1lhqCT9VCtl_pLtPD9)

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de <http://hdl.handle.net/10596/24167>