PRUEBA DE HABILIDADES BASICAS CCNA

MARIA LUISA SOLIS RACINES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGIAS
INGENIERIA EN SISTEMAS
2020

PRUEBA DE HABILIDADES BASICAS CCNA

MARIA LUISA SOLIS RACINES

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

TUTOR. GUSTAVO ADOLFO RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGIAS

INGENIERIA EN SISTEMAS

2020

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

INTRODUCCION

A través del presente documento se desarrollan dos situaciones escenarios de diseño de redes, las cuales han sido implementadas en la herramienta Pa Tracer.

Las soluciones implementar para los dos escenarios, comprenden procesos o especificaciones relacionadas con la configuración básica de dispositivos, direccionamiento IPV4 e IPV6, configuración de subredes, troncales, configuración de VLANs, puertos de acceso, configuración de interfaces 802.1Q, protocolos de routing dinámico, OSPF, entre otros aspectos necesarios para llevar a cabo el proceso de conexión entre dispositivos, acorde a los planteamientos iniciales.

Para la configuración del escenario 1 se llevará a cabo mediante IPV4 e IPV6, configuración de los dispositivos con parámetros de seguridad, se configurará el Routing Información Protocol, RIP v2, que es un protocolo de enrutamiento interno que envía señales de actualización a través de las direcciones multicast, este protocolo utiliza la cuenta de saltos para desarrollar su proceso de routing. El NTP o Network Time Protocolo, es una herramienta que permite la sincronización de los dispositivos de red, esta sincronización se hace en forma jerarquica, donde uno de los dispositivos funciona como servidor de sincronización y los demás que se encuentren configurados para el uso de este protocolo atienden al llamado de sincronización efectuado en dispositivo principal con NTP.

En el escenario 2, se usara el protocolo OSPF Open shortest path first, abrir el camino más corto primero, que al igual que el protocolo RIP, es de funcionamiento interno y realiza su proceso de enrutamiento a partir de reconocer los dispositivos conectados directamente, es decir el router MEdellin1, como es el caso de la topología que se enmarca en este trabajo para la escenario 2, conoce y reconoce los routers que están a su alrededor, específicamente, sus routers vecinos, sus direcciones y la distancia a la cual se encuentra cada uno de ellos, lo que le permite que al enviar información o paquetes de datos, este a través de este reconocimiento previo, realice este proceso a través de la ruta por la cual tenga que dar menos saltos.

En ambos escenarios, se configuraran NAT o Network Address Traslations, para que las redes usen un rango de direcciones especiales, que colabora en el ahorro de direcciones IP, por cuanto permite que cuando un dispositivo ubicado en una red configurada con NAT, se conecte a Internet, este y todos los dispositivos de esta red, hagan uso de una única dirección IPV4.

Estos son algunos aspectos de la configuración a desarrollar en el presente documento de estudio, que permitirá conocer mas a fondo la implementación o practica de los protocolos ya mencionados, entre otros.

OBJETIVOS

GENERAL

Identificar el grado de desarrollo de competencias adquiridas en la implementación de redes Cisco

ESPECIFICOS

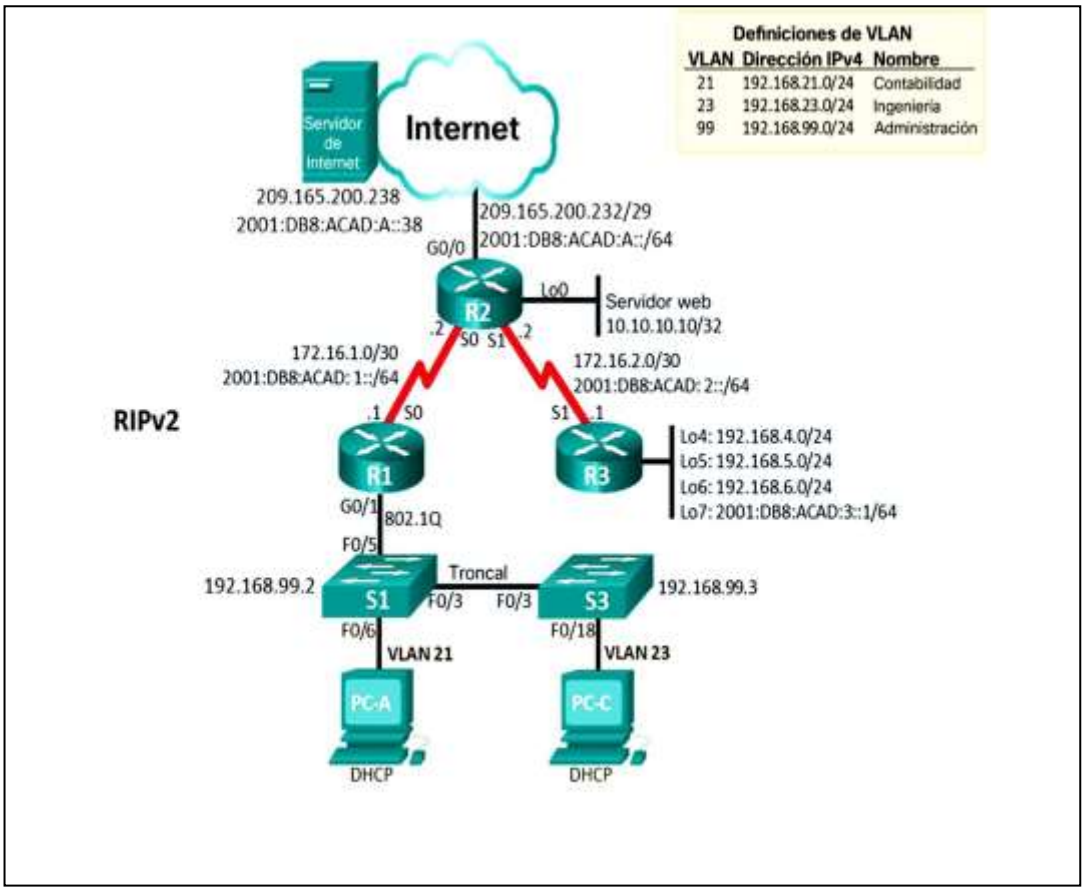
1. Reconocer las habilidades adquiridas para la implementación de diversos escenarios de conectividad.
2. Conocer y configurar diversos dispositivos que conforman una red
3. Poner uso protocolos y estándares para la conexión de redes
4. Usar comandos que permitan verificar la conectividad entre redes

1. PLANTEAMIENTO DEL ESCENARIO I

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.

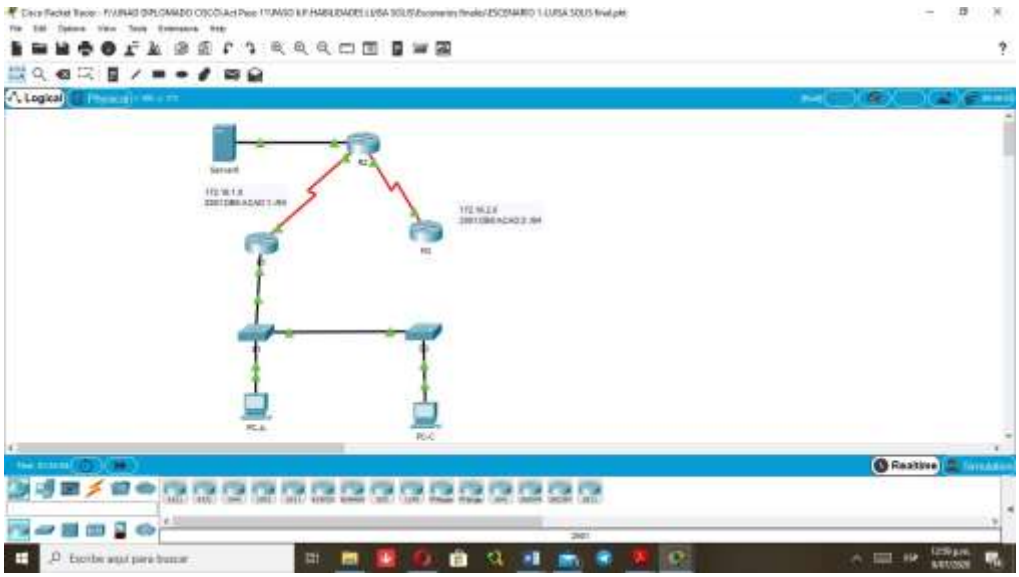
1.1. Topología a implementar

Figura. 1.Topología de red a implementar en el escenario 1



Fuente. PRUEBA DE HABILIDADES CCNA 2020 16-02. UNAD

Figura. 2. Implementación física de la topología de red



1.2. Direccionamiento IP

Tabla 1. Asignación de direccionamiento IP a dispositivos

		DIR IPV4	MASCARA	Puerta de Enlace Predeterminado (Default Gateway)	DIR IPV6	Puerta de Enlace IPv6 (IPv6 Gateway)
Servidor de Internet	G0/0	209.165.200.238	255.255.255.248	209.165.200.232/28	2001:DB8:ACAD:A::38	2001:DB8:ACAD:A:: /64
R1	Se0/0/0	172.16.1.1	255.255.255.252	172.16.1.0/30	2001:DB8:ACAD:1::1/64	2001:DB8:ACAD:1::/64
	G0/0-21	192.168.21.1	255.255.255.0	192.168.21.1/24		
	G0/0-23	192.168.23.1	255.255.255.0	192.168.23.1/24		
	G0/0-99	192.168.99.1	255.255.255.0	192.168.99.1/24		
R2	G0/0	209.165.200.232	255.255.255.240	209.165.200.225/28	2001:DB8:ACAD:A::32	2001:DB8:ACAD:A::/64
	Se0/0/0	172.16.1.2	255.255.255.252	172.16.1.0/30	2001:DB8:ACAD:1::2/64	2001:DB8:ACAD:1::/64
	Se0/0/1	172.16.2.2	255.255.255.252	172.16.2.0/30	2001:DB8:ACAD:2::2/64	2001:DB8:ACAD:2::/64
	Lo0	10.10.10.10	255.255.255.255	10.10.10.10/32		
R3	Se0/0/0	172.16.2.1	255.255.255.252	172.16.2.0/30	2001:DB8:ACAD:2::1/64	

	Lo4	192.168.4.1	255.255.255.255	192.168.4.0/32		
	Lo5	192.168.5.1	255.255.255.0	192.168.5.0/24		
	Lo6	192.168.6.1	255.255.255.0	192.168.6.0/24		
	Lo7	2001:db8:acad:3::1/64				
S1)	Vlan 21 a Vlan23 (99	192.168.99.3	255.255.255.0			
S2	Vlan 21 a Vlan23 (99	192.168.99.3	255.255.255.0			

Tabla 2. Identificación de conexiones entre dispositivos

CONEXION	DIRECCION IPV4	DIRECCION DE RED	DIRECCION IPV6	DIRECCION DE RED IPV6
R1 A R2 Se0/0/0	172.16.1.1	172.16.1.0/30	2001:DB8:ACAD:1::1/64 FE80::1 link-local	2001:DB8:ACAD:1::/64
R1 A S1 G0/1	192.168.99.1	192.168.99.0/24	2001:DB8:ACAD:B::1/64 FE80::1 link-local	2001:DB8:ACAD:B::
R2 A SERVIDOR INT G0/0	209.165.200.233	209.165.200.232/29	2001:DB8:ACAD:A::1 FE80::2 link-local	2001:DB8:ACAD:A::/64
R2 A R1 Se0/0/0	172.16.1.2	172.16.1.0/30	2001:DB8:ACAD:1::2/64 FE80::2 link-local	2001:DB8:ACAD:1::/64
R2 A R3 Se0/0/1	172.16.2.2	172.16.2.0/32	2001:DB8:ACAD:2::1/64 FE80::2 link-local	2001:DB8:ACAD:2::/64
SERVIDOR INT	209.165.200.238	209.165.200.225/29	2001:DB8:ACAD:A::38/64 FE80::2 link-local	2001:DB8:ACAD:A::/64
R3 A R2 Se0/0/1	172.16.2.3	172.16.2.0/32	2001:DB8:ACAD:2::2/64 FE80::3 link-local	2001:DB8:ACAD:2::/64
R2 Lo0	10.10.10.10	10.10.10.10/32		
R3 Lo4	192.168.4.1	192.168.4.1/24	::/0 G0/0	0.0.0.0.0.0.0.0
R3 Lo5	192.168.5.1	192.168.5.1/24	::/0 S0/0/1	0.0.0.0.0.0.0.0
R3 Lo6	192.168.6.1	192.168.6.1/24	::/0 S0/0/1	0.0.0.0.0.0.0.0
R3 Lo7	2001:db8:acad:3::144		2001:DB8:ACAD:3::2	2001:DB8:ACAD:3::1

1.3. Parte 1. INICIALIZAR DISPOSITIVOS

1.3.1. Inicializar y volver a cargar los routers y los switches

A través de este proceso se alistaran los dispositivos presentes en la implementación topológica, en aras de prepararlos para el proceso de configuración

Tabla 3. Inicialización 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 y eliminar la base de datos de VLAN anterior	Switch#erase startup-config
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 flash

1.3.2. Parte 2. Configurar los parámetros básicos de los dispositivos

Mediante el proceso que se describe a continuación, se configuran los parámetros o especificaciones básicas de los dispositivos, como los nombres, asignación de claves de acceso, entre otros.

1.3.3. Configurar la computadora de Internet

Tabla 4. Parámetros de configuración para el servidor de Internet

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIONES
DIRECCION IPV4	209.165.200.238
MASCARA DE SUBRED IPV4	255.255.255.248
GATEWAT PREDETERMINADO	209.165.200.232/28
DIRECCION IPV6	2001:DB8:ACAD:2::38/64
GATEWAY PREDETERMINADO IPV6	2001:DB8:ACAD:2::1/64

1.3.4. Descripción de la configuración básica de los routers

Para los routers y switch, presentes en la topología que se está implementando, se lleva a cabo el proceso de asignación de nombre, el cual se realiza mediante el comando host name “Nombre a asignar”, se configura la contraseña de acceso a exec privilegiado, que es la sección o plataforma del dispositivo donde se puede llevar a cabo el proceso de configuración, el comando usado para dicho fin se realiza mediante el comando enable secret y luego se asigna la contraseña, que en este caso es class, es decir el comando ejecutado en este caso es enable secret class.

Por otra parte se configura la contraseña para acceso a consola, para ello se utiliza el comando line console 0, que permite acceder al modo de configuración de consola, luego se configura la desconexión por inactividad con el comando exec-timeout, al cual se le asigna el valor de 0 y con el comando password se le asigna una contraseña, que en este caso es “cisco”, el comando login, configura

el dispositivo para que este solicite o requiera la contraseña al momento de iniciar, es decir para que requiera autenticación.

Para la configuración de Telnet se ingresa al modo de configuración del mismo con el comando line vty, luego se asigna la contraseña mediante el comando password “cisco” y el comando login para habilitar las contraseñas de seguridad.

El comando service password-encryption, permite cifrar las contraseñas permite cifrar las contraseñas configuradas y el comando ip domain-loockup permite deshabilitar la traducción de nombres, ya que si se ingresa con una contraseña errónea el dispositivo no ingresará el acceso al mismo, debido a que este comando lo que hace es que este no lo busque en sus bases de datos y lo reconozca.

banner motd & “mensaje a asignar” &, es una línea de comando que arroja un mensaje de error ante un intento fallido de ingreso.

En la configuración de las interfaces de los routers, se asigna una dirección IP asociada a una máscara de subred, operación que se realiza mediante el comando *ip address “dirección IP y mascara de subred”,* este comando se usa para el Protocolo de Internet Versión 4 (IPV4), de igual manera se asigna una dirección IP, con formato de Protocolo de Internet Versión 6 (IPV6), mediante el comando *ipv6 address “dirección IP en formato IPV6”.*

Una dirección IP, sigla que viene de Internet Protocol o Protocolo de Internet, traducido al español, es una dirección única e irrepetible, que se asigna a un dispositivo de red y que le permite la comunicación con otros dispositivos a través de Internet, dicha dirección es primordial para establecer comunicación entre dispositivos configurados en la red.

De igual manera, la máscara de subred junto con la dirección IP identifica un dispositivo, pero la máscara de subred es mucho más específica, atendiendo a que si por ejemplo dos dispositivos cuentan con una dirección IP cuyo tres primeros octetos son similares y solo varía el último, la máscara de subred particulariza la identificación del octeto diferente en las IP, haciendo único al dispositivo que la posee; es decir, que si el PC1 tiene una dirección IP compuesta por 192.168.1.2 y el PC2 tiene una dirección IP 192.168.1.3, las mascara de subred particulariza el ultimo octeto que especifica si es la PC1

o la PC2, coloquialmente, se puede decir que la dirección IP junto con la máscara de subred son la “cédula” o “Nit” del dispositivo cuando este se conecta a una red.

A continuación se encuentran los parámetros de configuración para routes

1.3.4.1. Configurar R1

Tabla 5. Parámetros de configuración básica R1

Elemento o tarea de configuración	Especificaciones
Desactivar la búsqueda DNS Nombre del router Contraseña de exec privilegiado cifrada Contraseña de acceso a la consola Contraseña de acceso Telnet Cifrar las contraseñas de texto no cifrado Mensaje MOTD	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R1 R1(config)#enable secret class R1(config)#line console 0 R1(config-line)#exec-timeout 0 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#logging synchronous R1(config-line)#line vty 0 4 R1(config-line)#exec-timeout 0 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#logging synchronous R1(config-line)#exit R1(config)#service password-encryption R1(config)#banner motd &se prohibe el acceso no autorizado& R1(config)#exit R1#copy run start
Interfaz S0/0/0	R1>enable Password: R1#configure terminal R1(config)#interface serial 0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#description R1 to r2 R1(config-if)#clock rate 128000 R1(config-if)#ipv6 add 2001:DB8:ACAD:1::/64 R1(config-if)#no shutdown R1(config-if)#end R1#

Rutas predeterminadas	R1#configure terminal R1(config)#ipv6 route 2001:DB8:ACAD:2::/64 serial0/0/1 R1(config)#ip route 172.16.2.0 255.255.255.252 172.16.2.2 R1(config)#ip route 172.16.2.0 255.255.255.252 serial 0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.0 R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#end
No configure aun G0/0	

1.3.4.2. Configuración de R2

Tabla 6. Configuración básica de R2

Elemento o tarea de configuración	Especificaciones
Desactivar la búsqueda DNS	Router>enable Router#config ter Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R2 R2(config)#no ip domain-lookup R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#exec-timeout 0 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#logging synchronous R2(config-line)#exit R2(config)#service password-encryption R2(config)#exit R2#
Nombre del router	
Contraseña de exec privilegiado cifrada	
Contraseña de acceso a la consola	
Contraseña de acceso Telnet	
Cifrar las contraseñas de texto no cifrado	
Mensaje motd	
Habilitar el servidor HTTP	R2(config)#ip http server Nota: al ejecutar este comando, da como resultado un mensaje de error, ya que este paso no es soportado por la plataforma
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description link R1 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)#end R2#
Interfaz S0/0/1	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#interface serial 0/0/1 R2(config-if)#description link R3

	R2(config-if)#ip add 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#end R2#wr
Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config-if)#description R2-Internet R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:db8:acad:a::32/64 R2(config-if)#no shutdown R2(config-if)#end
Interfaz loopback 0 (servidor web simulado)	R2#config ter Enter configuration commands, one per line. End with CNTL/Z. R2(config)#interface g0/0 R2(config-if)# R2(config-if)#description link R3 R2(config-if)#description link R2 R2(config-if)#end R2# R2#configure terminal R2(config)#interface loopback 0 R2(config-if)#ip add 10.10.10.10 255.255.255.255 R2(config-if)#end
Configurar rutas predeterminadas	Configurar ruta predeterminada ipv4: R2(config)#interface g0/0 R2(config)# ip route 0.0.0.0 255.255.255.248 209.165.200.238 Configurar ruta predeterminada ipv6: R2(config)#interface g0/0 R2(config-if)# ipv6 route ::/0 g0/0

1.3.4.3. Configuración de R3

Tabla 7. Configuración básica de R3

Elemento o tarea de configuración	Especificaciones
Desactivar la búsqueda DNS	Router>enable Router#config te Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R3
Nombre del router	
Contraseña de exec privilegiado cifrada	
Contraseña de acceso a la consola	

Contraseña de acceso Telnet Cifrar las contraseñas de texto no cifrado Mensaje motd	R3(config)#no ip domain-lookup R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#exec-timeout 0 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#logging synchronous R3(config-line)#exit R3(config)#service password-encryption R3(config)#exit R3# %SYS-5-CONFIG_I: Configured from console by console R3#copy run start Destination filename [startup-config]? Building configuration... [OK] R3#
Habilitar el servidor HTTP	R3(config)#ip http server Nota: al ejecutar este comando, se optiene como resultado un mensaje de error, o de entrada no valida, ya que éste no es soportado.
Interfaz S0/0/1	R3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#interface serial 0/0/1 R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#description link to r2 R3(config-if)#description link to r3 R3(config-if)#ipv6 add 2001:ddb8:acad:1::2/64 R3(config-if)#no shutdown R3(config-if)#end
Interfaz loopback 4 Interfaz loopback 5 Interfaz loopback 6	R3(config)#interface loopback 4 R3(config-if)#ip add 192.168.4.1 255.255.255.255 R3(config-if)# R3(config-if)#exit R3(config)#interface loopback 5 R3(config-if)#ip add 192.168.5.1 255.255.255.255 R3(config-if)#exit R3(config)#interface loopback 6 R3(config-if)#ip add 192.168.6.1 255.255.255.255 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 add 2001:db8:acad:3::1/64

	R3(config-if)# R3(config-if)#exit R3(config)#

En la configuración de los routers especificadas en los ítems anteriores, se visualiza que se establecen rutas predeterminadas, que es una ruta estática que le permite al router almacenar todas las rutas para todas las redes en su tabla de routing, entiéndase tabla de routing o de enrutamiento como el conjunto de reglas que le permite al router dirigir los paquetes o datos por el camino más pertinente; entonces las rutas predeterminadas especifican o se identifican con todas las rutas o caminos posibles de envío de un paquete desde un router y se usa cuando ninguna ruta coincide con la dirección IP con la del destino el paquete.

En los routers 2 y 3 se configuran interfaces de loopback, que es o son interfaces virtuales de red, que no se asigna a puertos físicos y pueden servir para administrar el dispositivo, asegurando que una interface siempre esté disponible.

1.3.5. Configuración de Switchs

Para la configuración básica de Switch se usan los mismos comandos que para los routers, tano para la asignación de nombres como para el establecimiento de parámetros de acceso

1.3.5.1. Configuración básica S1

Tabla 8. Configuración básica S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup S1(config)#exit
Nombre del switch	Switch>enable Switch#configure termina Switch(config)#hostname S1 S1(config)#enable pass cisco S1(config)#enable secret class S1(config)#line console 0 S1(config-line)#pass cisco S1(config-line)#login S1(config-line)#exit S1(config)#line vty 0 15 S1(config-line)#pass cisco S1(config-line)#login S1(config-line)#exit S1(config)#service password-encryption
Contraseña de exec privilegiado cifrada	
Contraseña de acceso a consola	
Contraseña de acceso a telnet	
Cifrar las contraseñas de texto no cifrado	
Mensaje motd	

	S1(config)#banner motd &se prohibe el acceso no autorizado& S1(config)#end S1#

1.3.5.2. Configuración básica S3

Tabla 9. Configuración básica de S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch#configure ter Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S3 S3(config)#enable pass cisco S3(config)#enable secret class S3(config)#line console 0 S3(config-line)#pass cisco S3(config-line)#login S3(config-line)#exit S3(config)#line vty 0 15 S3(config-line)#pass cisco S3(config-line)#login S3(config-line)#exit S3(config)#service password-encryption S3(config)#end

1.3.6. Verificación de conectividad

Tabla 10. Parámetros para la verificación de conectividad

Desde	A	Dirección IP	Resultado de ping
R1	R2, s0/0/0	172.16.1.2	Correcto
R2	R3 s0/0/1	172.16.2.1	Correcto
Pc internet	Gateway predeterminado	209.165.200.232	Correcto

Figura. 3. Ping de R1 a R2

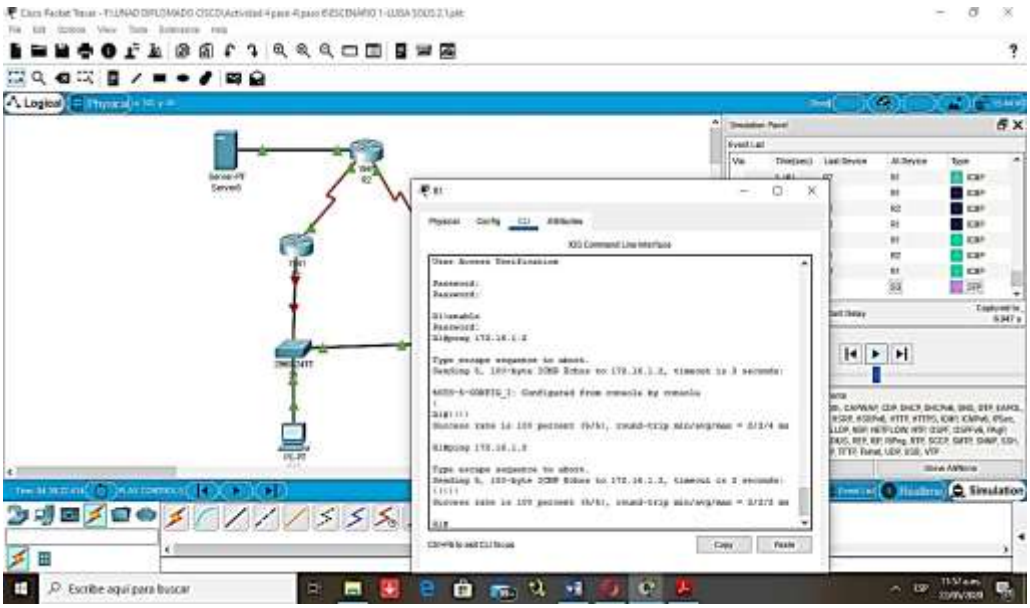
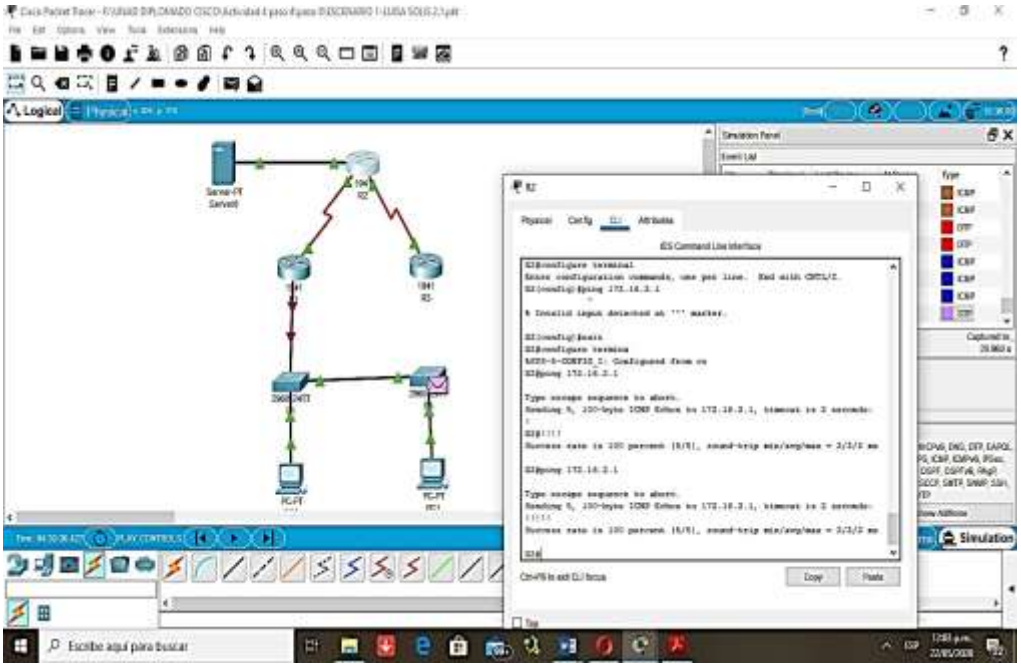
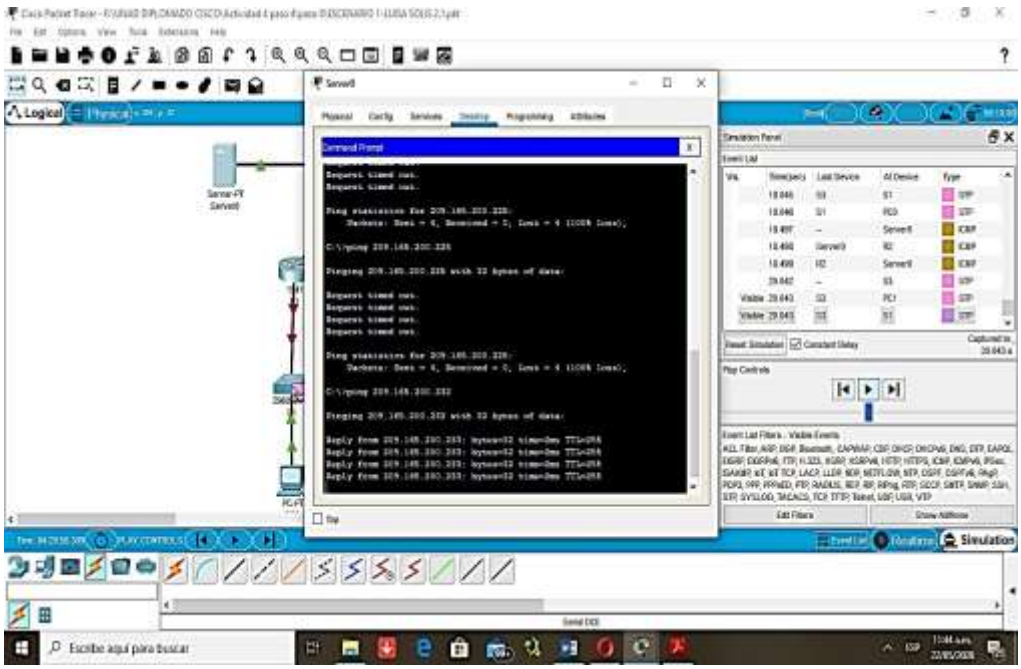


Figura. 4.Ping de R2 a R3



Fuente propia.

Figura. 5.Ping de Server0 a Gateway



Fuente propia

1.4. Parte 3. Configurar la seguridad en los Switch, VLAN y el routing entre VLAN

Tabla 11. Especificaciones de seguridad en switch, valn y routing entre vlan

VLAN	DIRECCION IPV4	NOMBRE
21	192.168.21.0/24	CONTABILIDAD
23	192.168.23.0/24	INGENIERIA
99	192.168.99.0/24	ADMINISTRACION

Una VLAN o red de área local virtual permite creer redes lógicas independientes en una misma red física y permiten administrar una red, es decir, en una única red física se puede contener varias redes pero en forma virtual.

Para configurar las VLAN en los switchs S1 y S3, se procede a especificar o crear una base de datos de las VLAN que estos contendrán, esto se lleva a cabo mediante el comando vlan “numero”, es decir primero se especifica una red virtual con un número, luego a través del comando name, se les especifica un nombre que la identifique.

Después se le asigna una dirección IP con su correspondiente mascara de subred y una dirección de Gateway predeterminado, que corresponde a la interface del router conectado directamente al switch, que en el caso de esta topología, corresponde a R1 conectado con S1 y R3 conectado con S3, precisando así el mejor camino para el envío de paquetes; la configuración del Gateway se realiza mediante el comando ip default-gateway

También se realiza el proceso de forzar enlace troncal mediante la ejecución del comando switchport mode trunk, permitiendo extender la VLAN por la red. Posteriormente se ejecuta el comando switchport trunk native vlan 1, que especifica si una VLAN será de administración o nativa, en este caso la Vlan 1 es nativa, se asigna a un puerto troncal (802.1Q) que coloca el tráfico no especificado en esta VLAN.

Finalmente se configuran los demás puertos como puertos de acceso y se asigna una interfaz a la VLAN administrada y se apagan las interfaces o puertos sin usar, mediante el comando interface range, para definir el rango de puertos a apagar y luego se ejecuta el comando shutdown.

1.4.1. Configurar parámetros en S1

Tabla 12. Configuración de parámetros en S1

Elemento o tarea de configuración	Especificaciones
Crear la base de datos de VLAN	S1>enable Password: S1#conf te S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit S1(config)#
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# S1(config-if)#ip add 192.168.99.3 255.255.255.0 S1(config-if)#exit S1(config)#
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1 S1(config)#exit S1#
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#interface f0/5 S1(config-if)# S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#interface f0/5

	S1(config-if)# S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown S1(config-if)#exit
Asignar F0/6 a la VLAN 21	**S**1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range fa0/1-4, fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

1.4.2. Configurar parámetros en S3

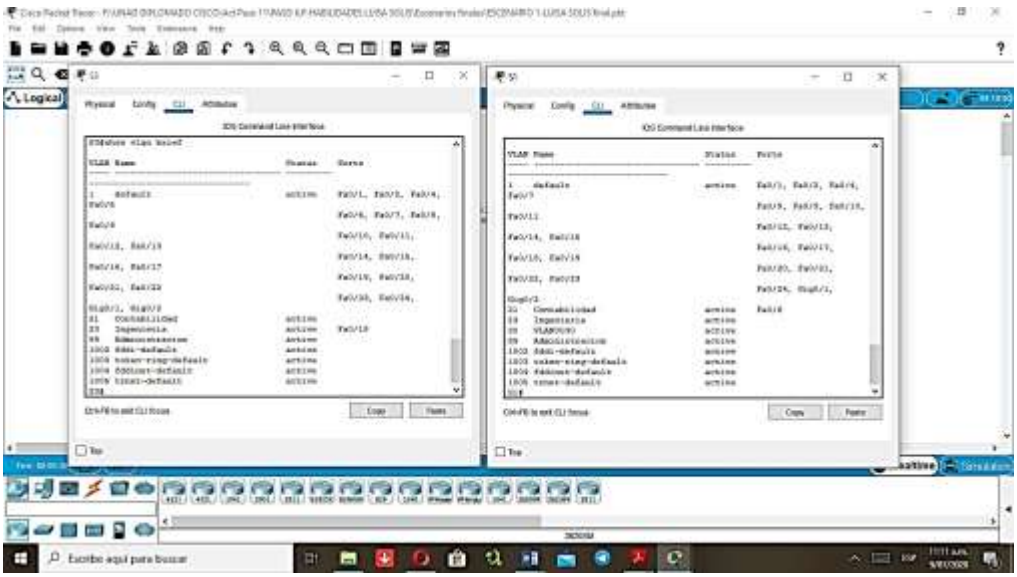
Tabla 13. Configuración de parámetros en S3

Elemento o tarea de configuración	Especificaciones
Crear la base de datos de VLAN	S3>enable Password: S3#config ter 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)#end
Asignar la dirección IP de administración.	S3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S3(config)#interface vlan 99 ip add 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1 S3(config)#exit
Forzar el enlace troncal en la interfaz F0/3	S3#conf ter Enter configuration commands, one per line. End with CNTL/Z. S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#

Configurar el resto de los puertos como puertos de acceso	S3#conf ter Enter configuration commands, one per line. End with CNTL/Z. S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit S3(config)#
Asignar F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)#switchport mode acces S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/2, fa0/4, fa0/6-17, fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

El comando show vlan brief, permite mostrar las interfaces VLAN configuradas en los switchs

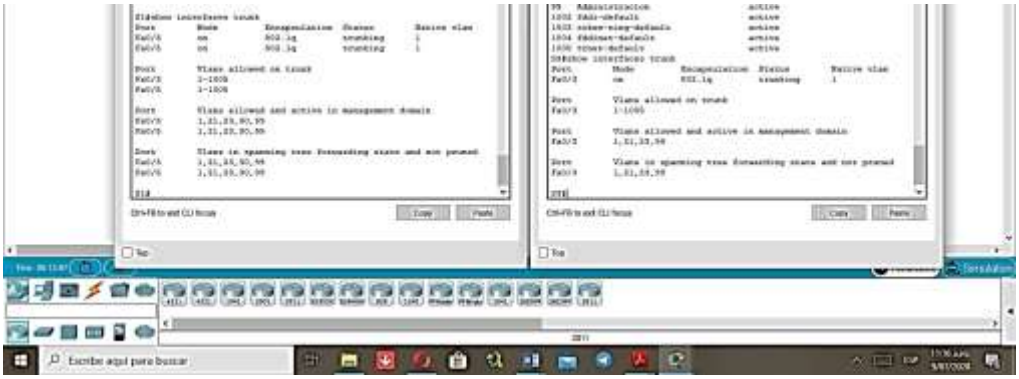
Figura. 6.Ejecución del comando show vlan brief en los switch



Fuente propia

El comando show interface trunk permite verificar las interfaces o puertos troncales del switch

Figura. 7Ejecución comando show interface trunk en los switchs



Fuente propia

1.4.3. Configurar subinterfaces 802.1Q en R1

Este proceso es el que permite la configuración de ruteo o routing entre VLAN.

En la sección anterior, se configuraban puertos troncales, de acceso y se configuraba VLAN nativa y se especificaba que la VLAN nativa se asignaba al puerto 802.1Q, entonces, al configurar las subinterfaces 802.1Q en R1, se establecen los procedimientos para que el R1 tenga una interfaz lógica en cada VLAN.

Para la configuración de subinterfaces 802.q, para cada interfaz conectada desde el router directamente al switch, que en este caso es R1 conectado por la interfaz Gigabitethernet 0/1 al S1, se debe configurar una subinterface por cada VLAN activa en el switch; para dicha configuración se procede como se especifica en la tabla a continuación.

Tabla 14. Configurar subinterfaces 802.1Q en R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure ter R1(config)#interface g0/1 R1(config-if)#no ip address R1(config-if)#interface g0/1.21 R1(config-if)#description acouting lan Administracion R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit R1(config)#end R1#
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface g0/1 R1(config-if)#no ip address R1(config-if)#interface g0/1.23 R1(config-subif)#description accouting lan Ingenieria

	R1(config-subif)#encapsulation dot1q 23 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)#interface g0/1 R1(config-if)#interface g0/1.99 R1(config-subif)#description acocouting lan Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar interfaz G0/1	no shutdown

1.4.4. Verificar conectividad

Tabla 15. Especificaciones para la verificación de conectividad

Desde	A	Dirección IP	Resultado ping
S1	R1, dirección VLAN 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto
S3	R1, dirección VLAN 23	192.168.23.1	Correcto

Figura. 8Ping de S1 a R1

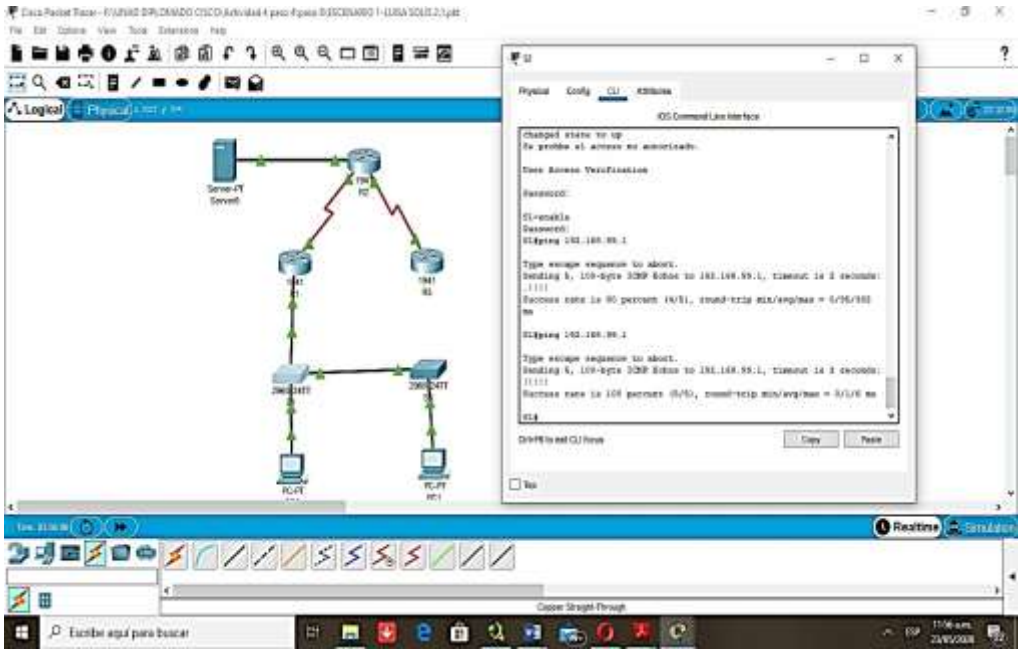
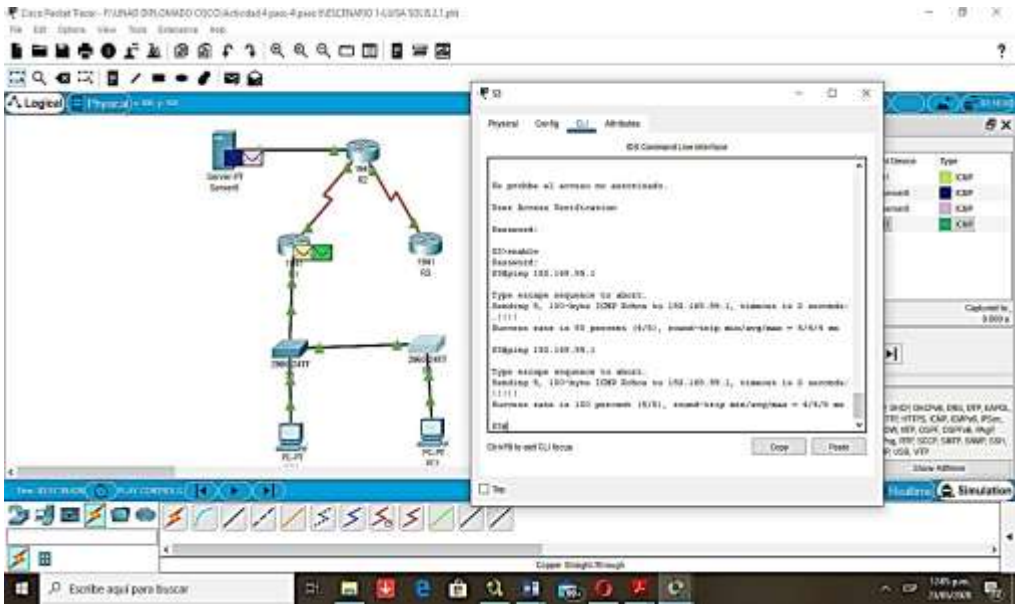
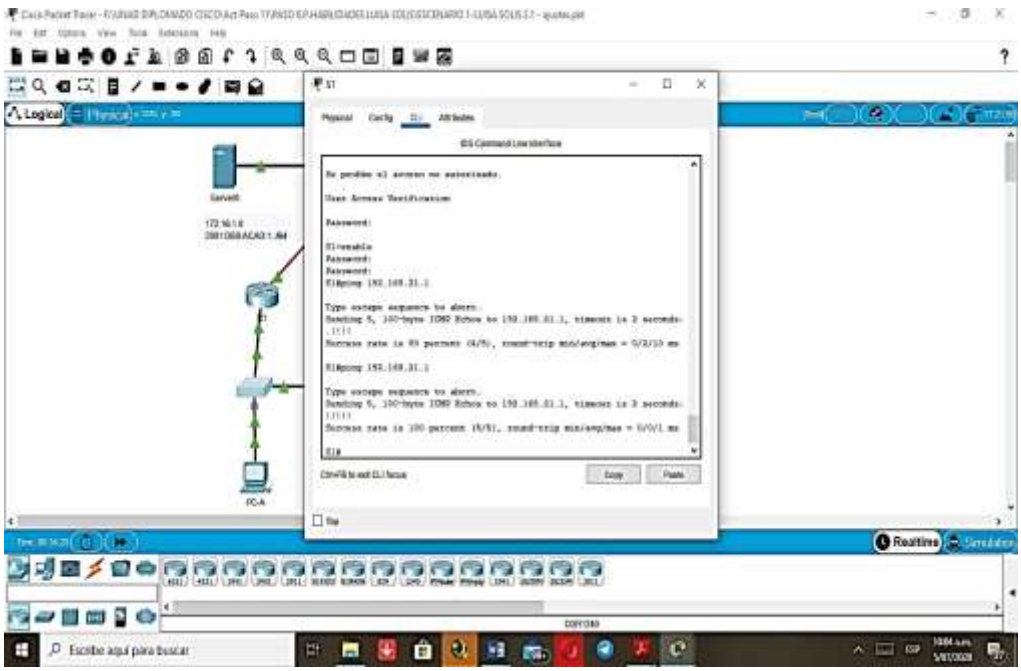


Figura. 9Ping de S3 a R1 VLAN 99



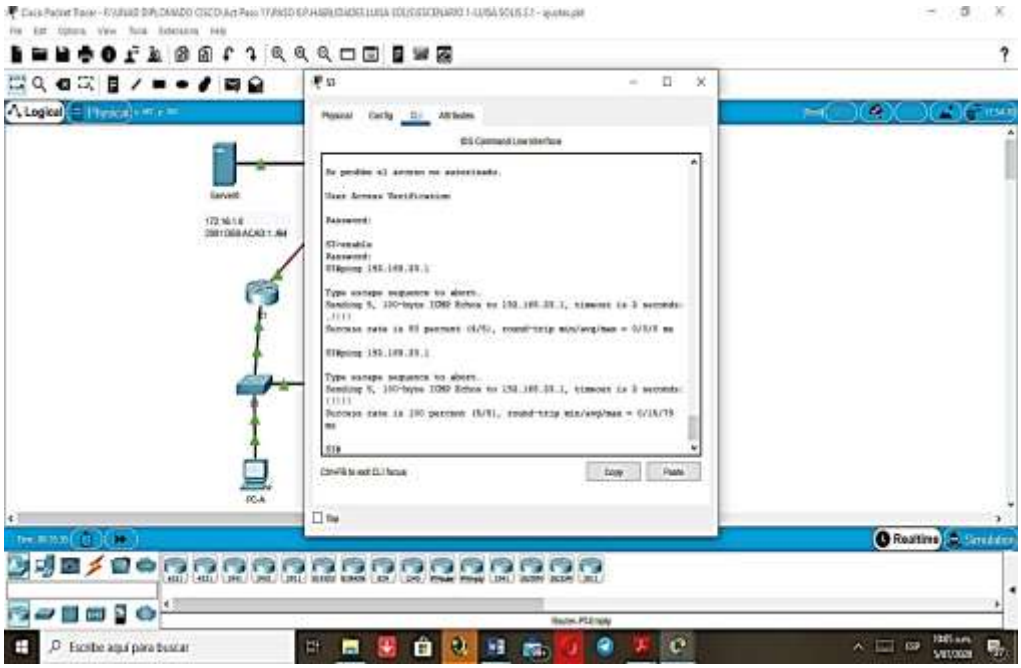
Fuente propia

Figura. 10Ping S1 a R1 VLAN 21



Fuente propia

Figura. 11Ping S3 a R1 VLAN 23



Fuente propia

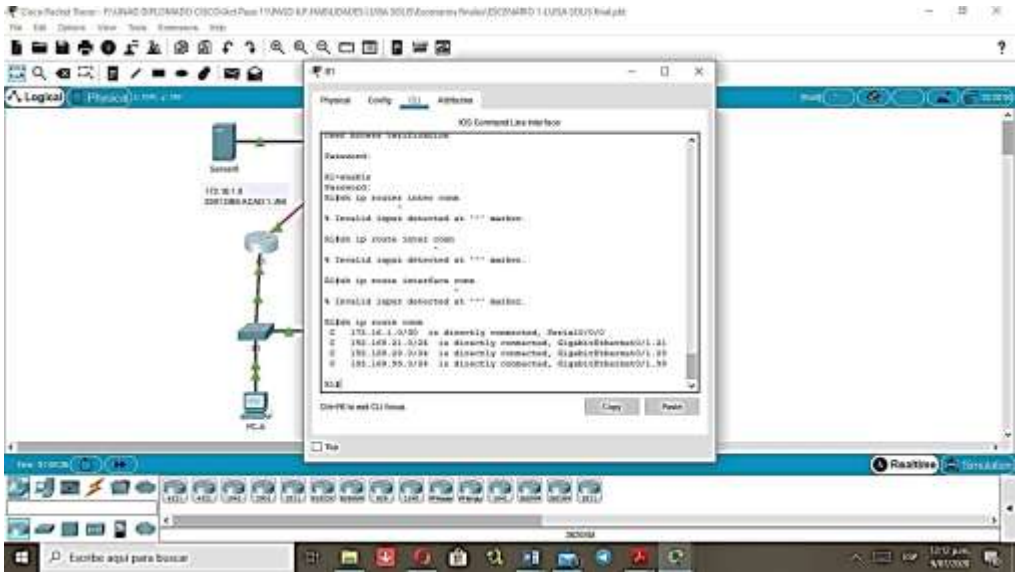
1.5. Parte 4. Configurar el protocolo de routing dinámico RIPv2

El enrutamiento dinámico versión 2 o RIPv2, le permite al router conocer y tener acceso a las demás redes, publicando las redes conectadas directamente, este ruteo permite que se tome la mejor distancia para la emisión de los paquetes de datos, a través del reconocimiento de los “siguientes saltos” o pasos que debe dar para llegar al destino.

Para configurar este protocolo, se cita o se llama mediante el comando router rip, luego se especifica la versión, con el comando versión 2, luego se llaman o citan las redes conectadas directamente al router con el comando network y la dirección de la red conectada.

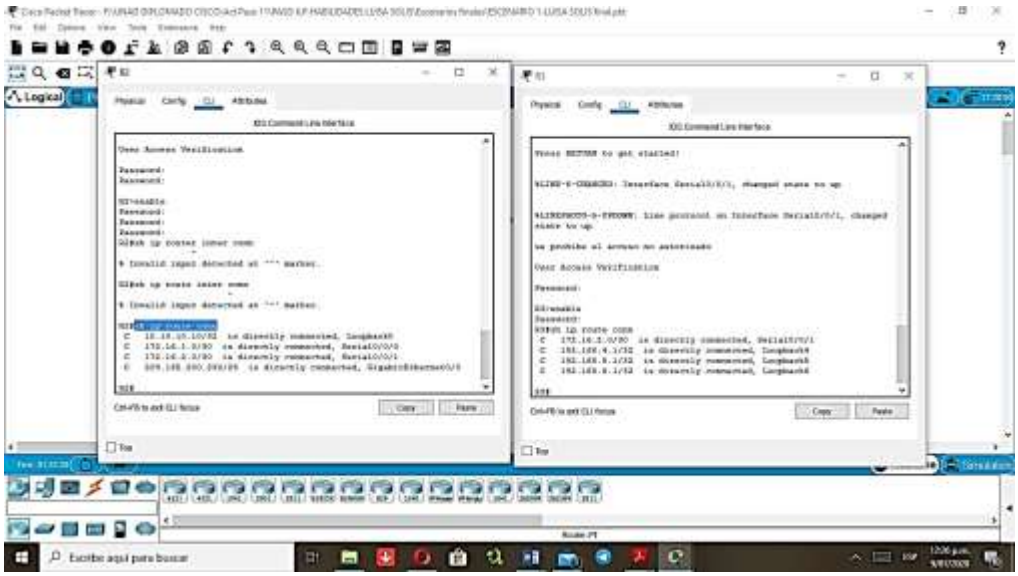
Para saber cuales son las redes que se deben citar o invocar con el comando network, se puede aplicar antes el comando *show ip route connec, como se muestra a continuación*

Figura. 12Comando show ip route connec en R1



Fuente propia

Figura. 13Ejecución del comando show ip route conne en R2 y R3



Fuente propia

Luego de citar o anunciar las redes conectadas, se establecen las interfaces LAN como pasivas, para suprimir el tráfico de información necesario, es decir para que las redes LAN no emitan información de enrutamiento que no es necesaria; esto se hace ejecutando directamente en la interfaz LAN, el comando passive-interface.

1.5.1. Configuración de RIPv2 en R1

Tabla 16. Configuración de RIPV2 en R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2 R1(config-router)#
Anunciar las redes conectadas directamente	R1(config-router)#network 192.168.1.0 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	no auto-summary

1.5.2. Configuración de RIPv2 en R2

Tabla 17. Configuración de RIPv2 en R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2 R2(config-router)#
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.0 R2(config-router)#network 209.165.200.0
Establecer todas las interfaces LAN como pasivas	R2(config-router)#passive-interface g0/1 R2(config-router)#passive-interface lo0 R2(config-router)#exit
Desactive la sumarización automática	no auto-summary

1.5.3. Configuración de RIPv2 en R3

Tabla 18. Configuración RIPv2 en R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#route rip R3(config-router)#version 2
Anunciar las redes conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 172.16.4.0 R3(config-router)#network 172.16.5.0 R3(config-router)#network 172.16.6.0
Establecer todas las interfaces LAN como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#exit
Desactive la sumarización automática	no auto-summary

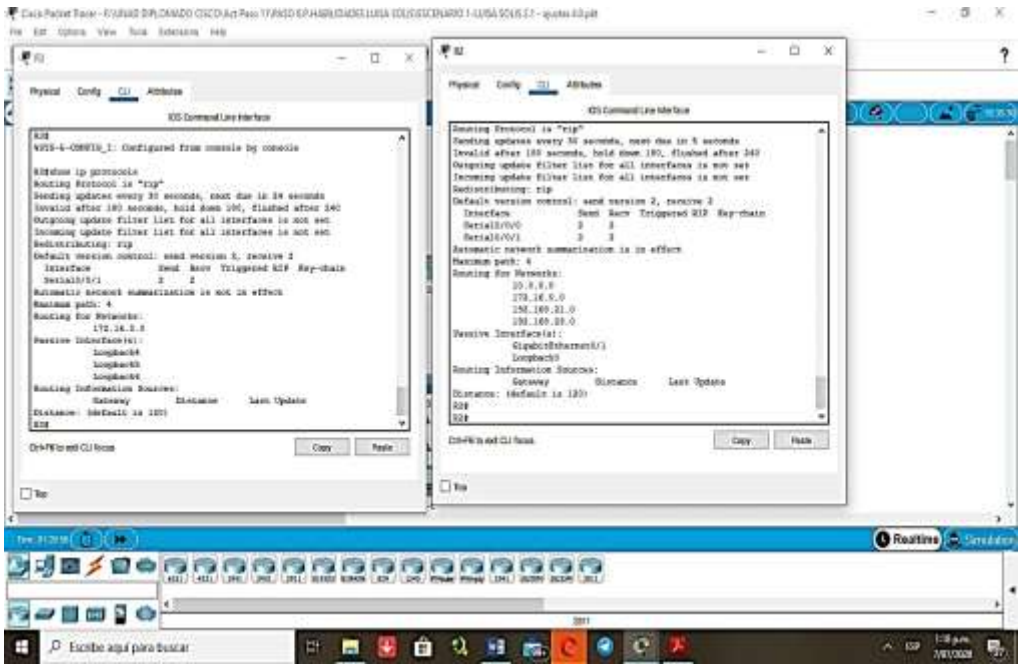
El comando no auto-summary permite que no se sumaricen las rutas que tiene.

1.5.4. Verificación de la información RIP

Tabla 19. Verificar la información de RIP

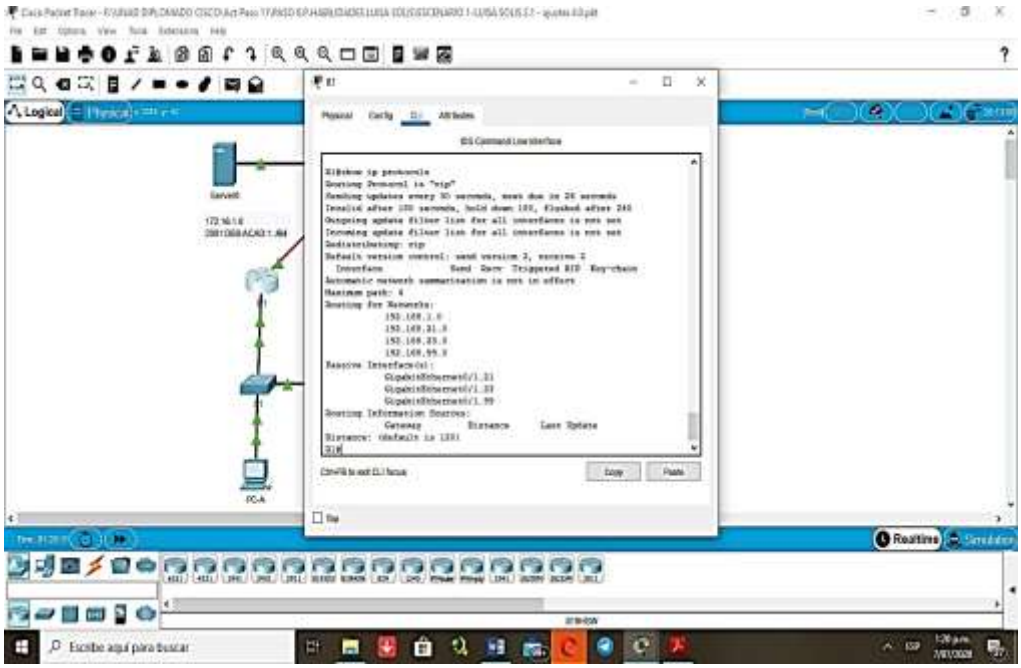
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route
¿Qué comando muestra la sección de RIP de la configuración en ejecución?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

Figura. 14Comando show ip protocols en R3 y R2



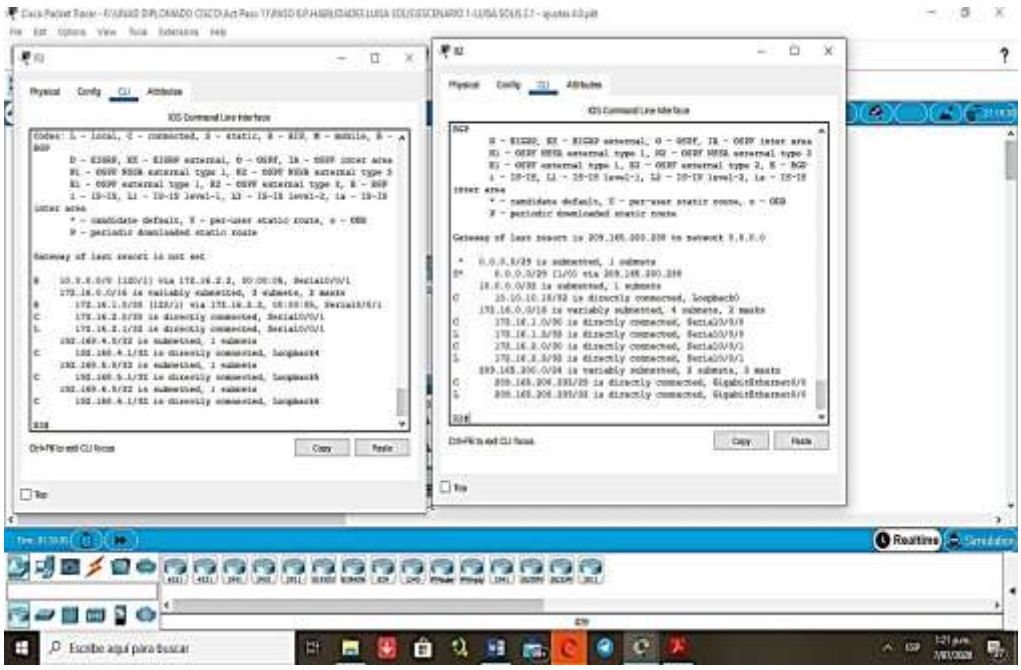
Fuente propia

Figura. 15 Comando show ip protocols en R1



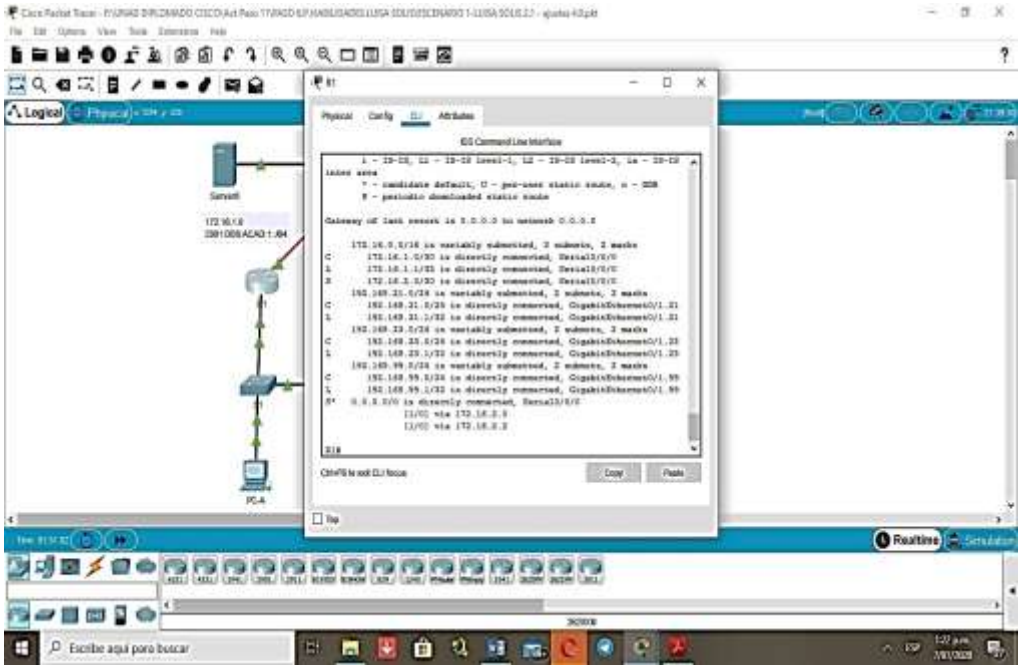
Fuente propia

Figura. 16 Comando show ip route en R2 y R3



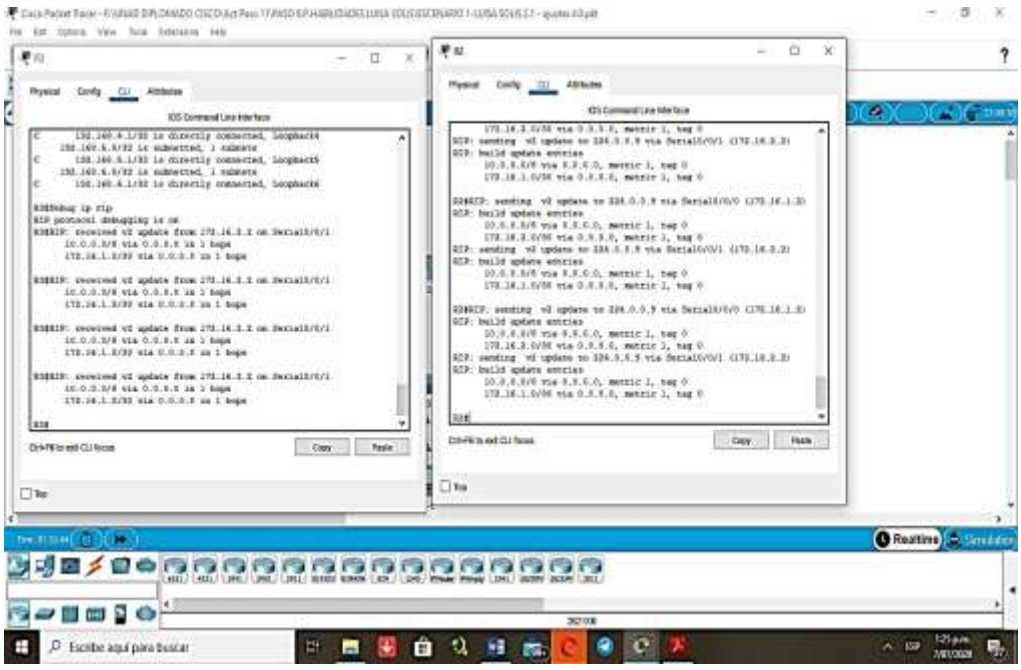
Fuente propia

Figura. 17 Comando show ip route en R1



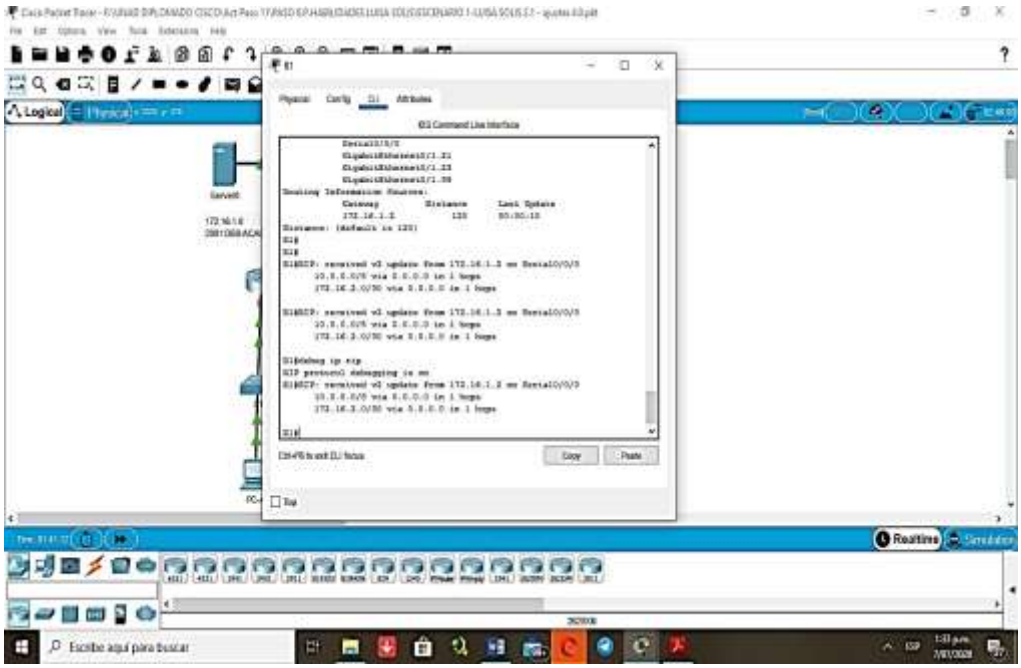
Fuente propia

Figura. 18 Ejecución comando debug ip rip en R2 y R3



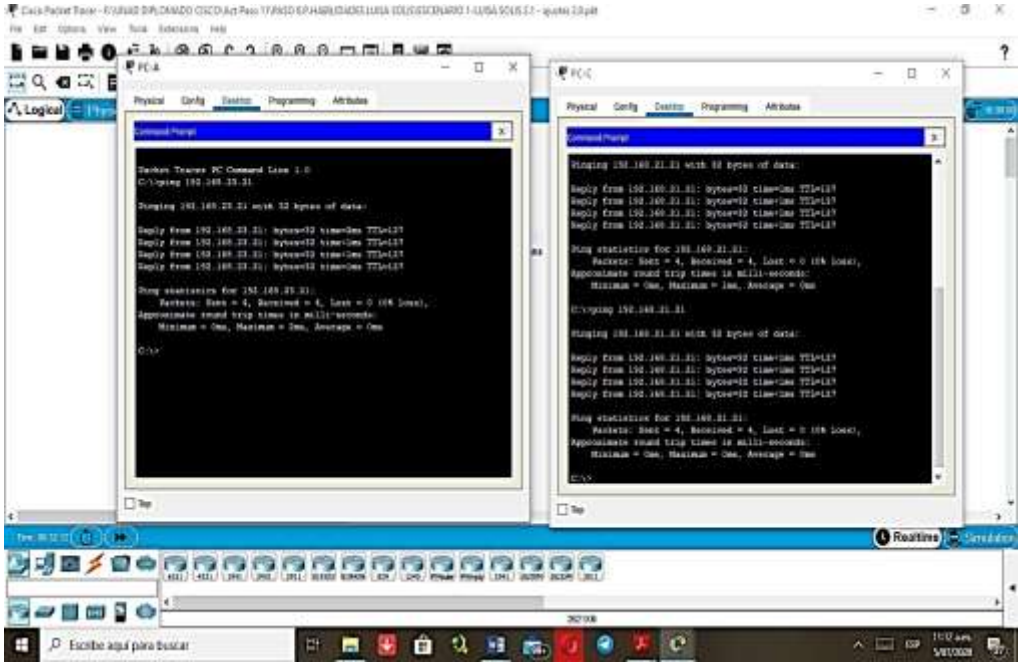
Fuente propia

Figura. 19 Ejecución comando debug ip rip en R1



Fuente propia

Figura. 20 Verificación de ping entre PC's



Fuente propia

1.6. Parte 5. Implementar DHCP y NAT para IPv4

El Protocolo De Configuración De Host Dinámico o DHCP, permite que los host conectados a una red se configuren en forma automática, es decir que se asigne en forma automática IP, mascara de subred y la identificación del Gateway

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

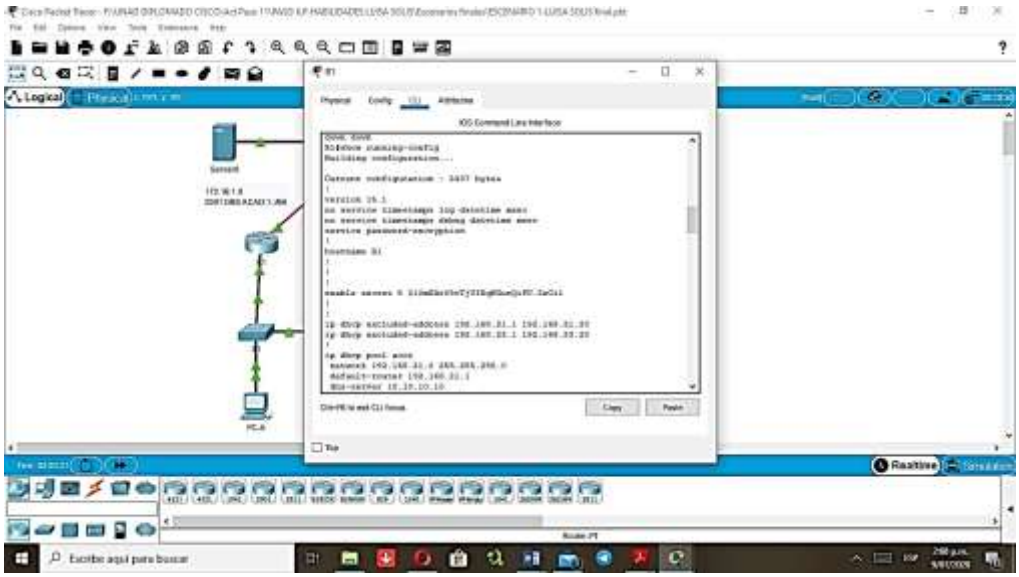
Tabla 20. Especificaciones para configurar DHCP

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)#domain-name ccna-sa.com R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#end R1#
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#exit

Al aplicar el comando ip dhcp excluded-address, se le indica al router que se excluya el rango de IP que se envían junto con este comando, para que no se asignen como direcciones de host o clientes finales.

Para ver la aplicación correcta de este comando usamos show running-config

Figura. 21 Comando show running-config para mostrar direcciones excluidas

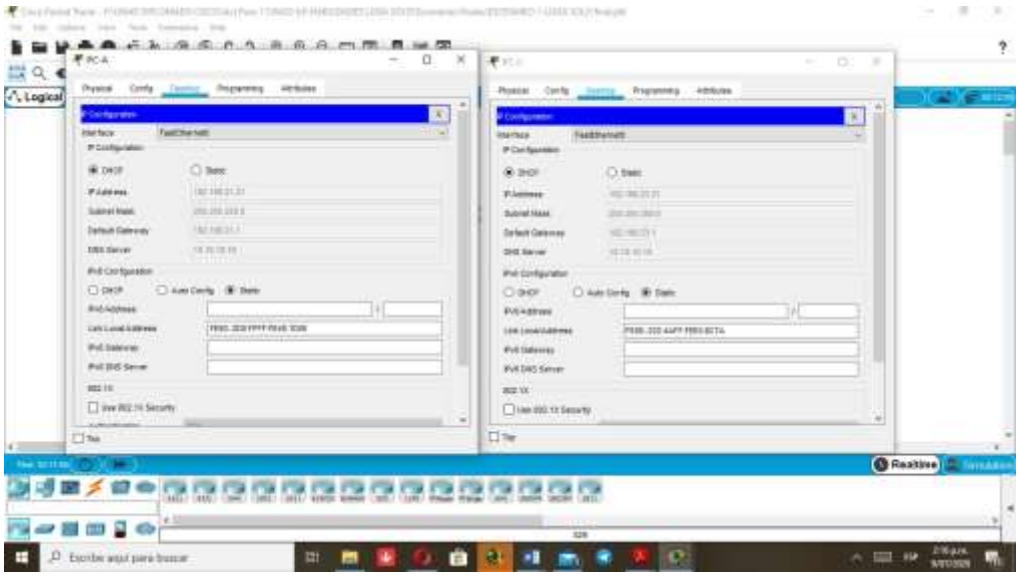


Fuente propia

Las direcciones 1992.168.21.1 y 192.168.23.1, corresponden a las subinterfaces g0/1.21 y g0/1.23.

También se puede observar que como el rango de direcciones excluidas van desde las citadas como subinterfaces, hasta las direcciones 192.168.21.20 y 192.168.23.20, los host asumen direcciones IP en sus respectivas redes, a partir de la dirección 192.168.21.21 y 192.168.23.21, respectivamente, esto lo podemos comprobar en la configuración de los PC a cada extremo.

Figura. 22 Verificación de la configuración de los host a través de DHCP



Fuente propia

El comando dchp pool “nombre”, asigna un nombre al pool o grupo de direcciones IP, luego network “IP + mascara de subred”, configura una direccion IP y una mascara para el pool identificado con el nombre acct, indicando el rango de redes disponibles para asignación.

Domain-name define el nombre del dominio y el comando dns-server configura el nombre de DNS o servicio de traduccion de nombres o hostname a direcciones IP

Default-router es la gateway predeterminada del router que se puede observar en la ilustracion 22, como se asgina automaticamente a los host en el espacio establecido para esta dirección por defecto.

1.6.2. Configurar la NAT estática y dinámica en el R2

Tabla 21. Especificaciones para configurar NAT

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
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Este comando no se puede ejecutar correctamente, no es soportado
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#ip nat inside R2(config-if)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255

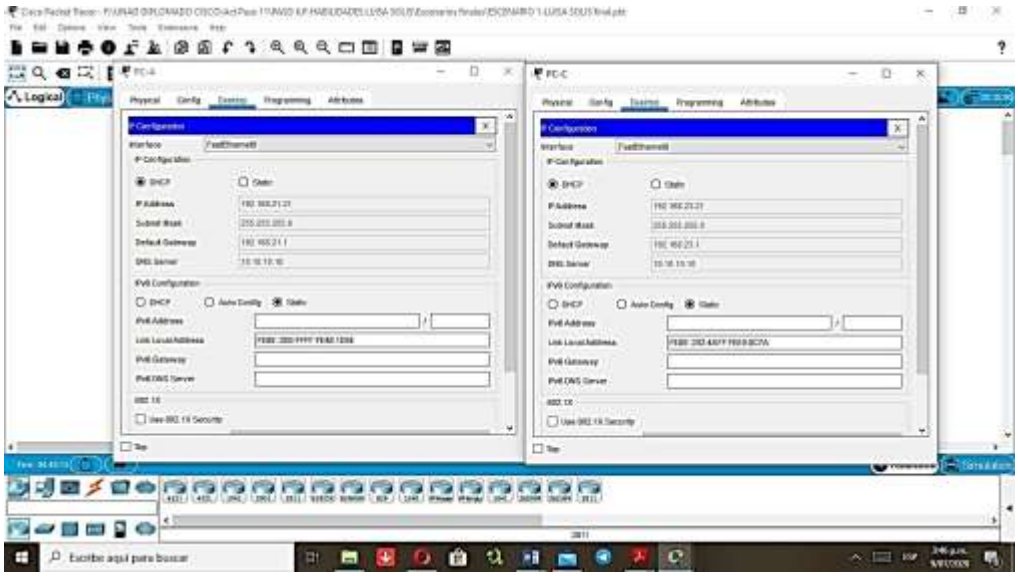
	R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** R2(config)#ip nat pool Internet 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET

NAT o Network Address Traslations, permite la utilización de rango de redes especiales, permitiendo el ahorro de direcciones IPV4 al conectar múltiples máquinas de una red a Internet, usando una dirección IP pública única, además de que los dispositivos contenidos en la red configurada con NAT no son visibles, disminuyendo así los ataques.

1.6.3. Verificar el protocolo DHCP y NAT estática

1.6.3.1. Verificar la asignación de direcciones IP en los PC usando DHCP o asignación automática

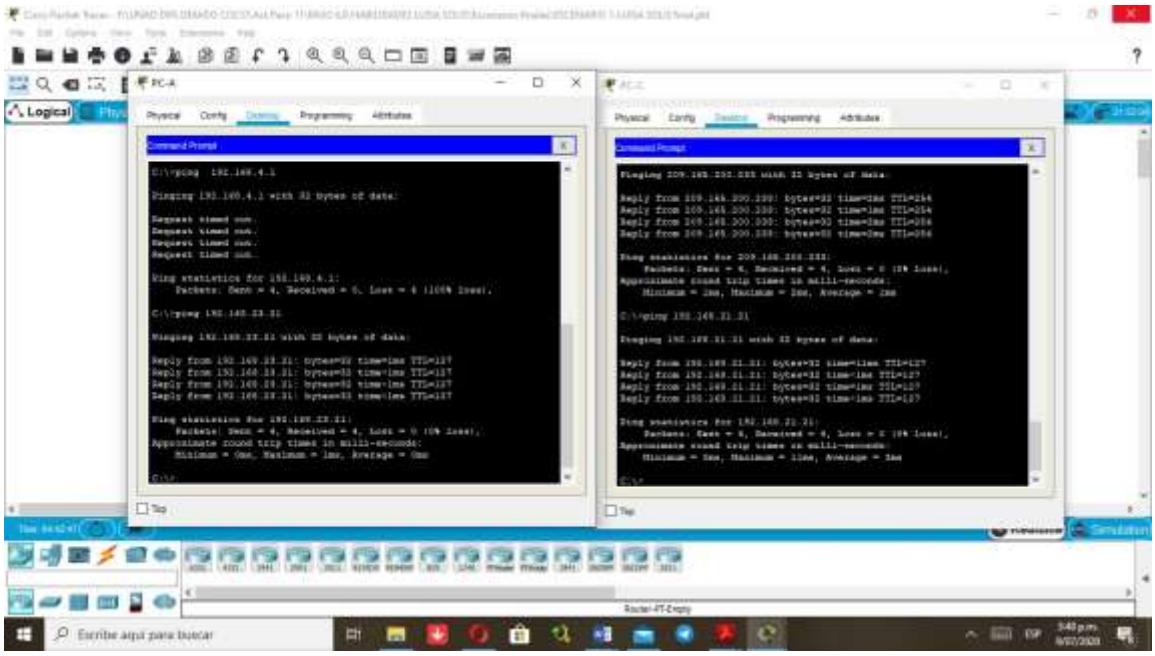
Figura. 23 Verificar de asignación de direcciones IP a los PC mediante DHCP



Fuente propia

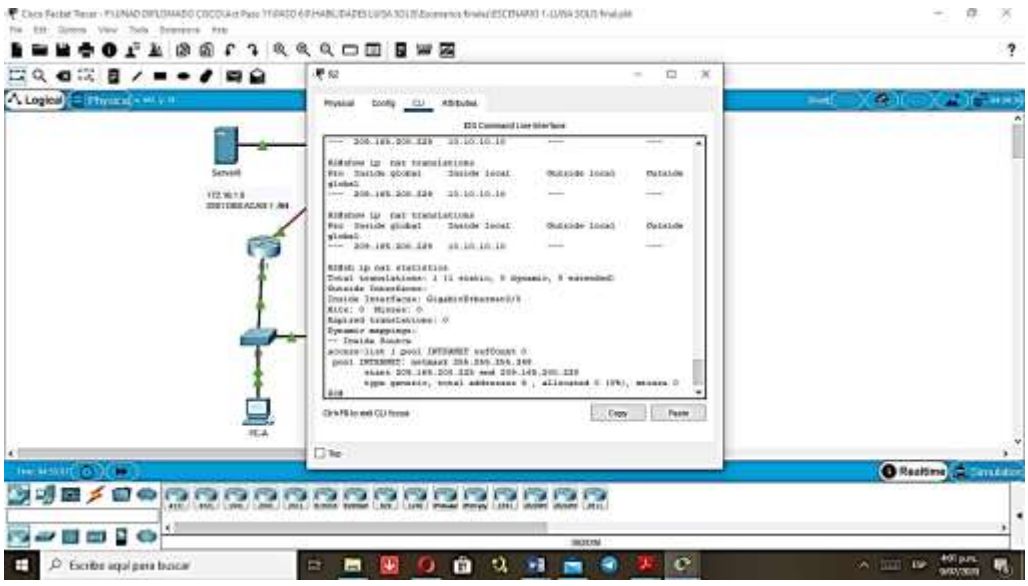
1.6.3.2. Verificación de comunicación o ping entre los host de la topología

Figura. 24 Verificar que se pueda realizar ping entre PC-A y PC-C



Fuente propia

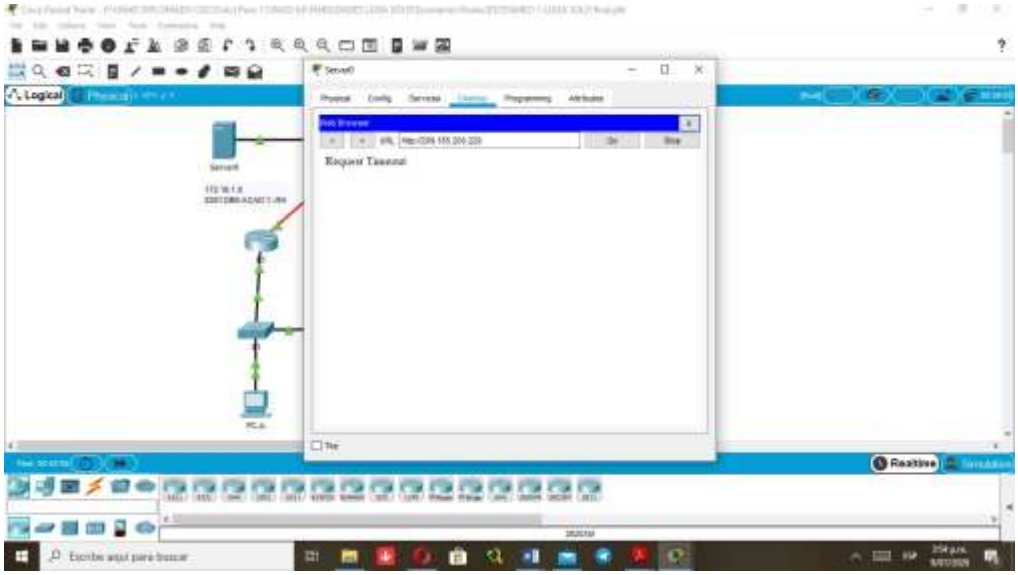
Figura. 25 Verificación de configuración de NAT en R2



Fuente propia

1.6.3.3. 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

Figura. 26 Comprobación de conexión a la direccion 209.165.200.229



Fuente propia

Debido a que no soporta los comandos de configuración de HTTP, no se puede llevar a cabo esta conexión

1.7. Parte 6. Configurar NTP

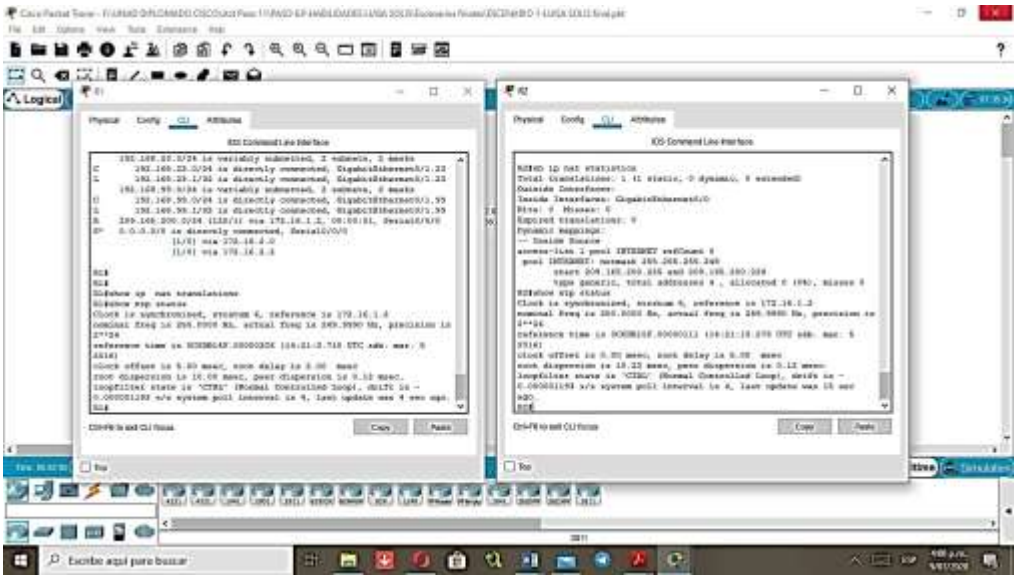
NTP son las siglas de Network Time Protocol, y permite sincronizar los dispositivos de una red

1.7.1. Configuración de NTP

Tabla 22. Elementos para la configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 march 5 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#show ntp status

Figura. 27 Verificar la configuración de NTP en R1 y R2



Fuente propia

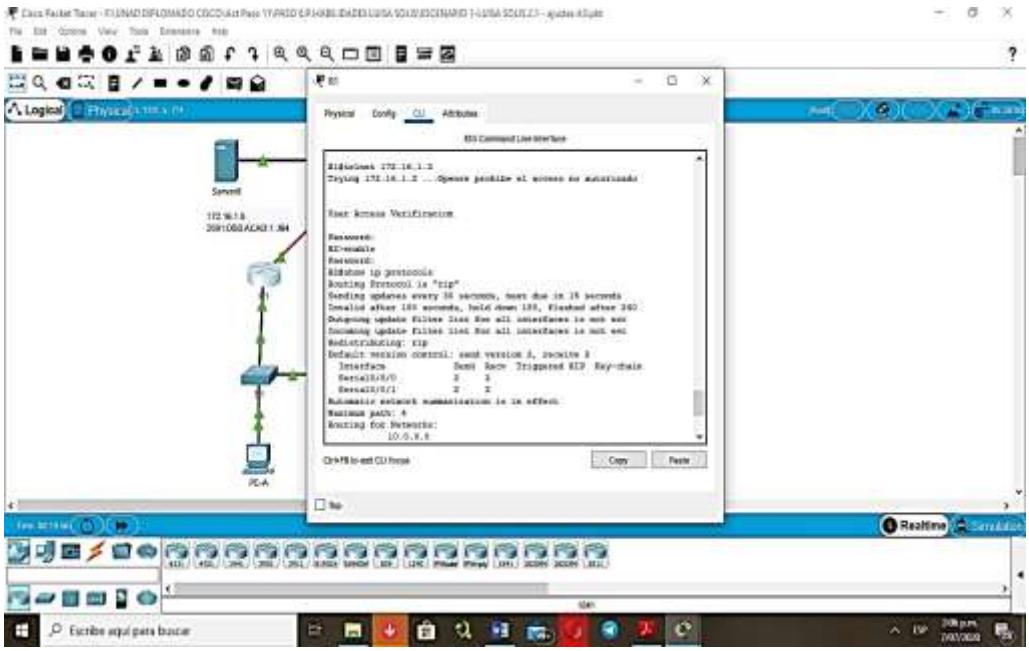
1.8. Configurar y verificar las listas de control de acceso (ACL)

Tabla 23. Elementos para la configuración de ACL

Elemento o tarea de configuración	
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 R2(config-std-nacl)# permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

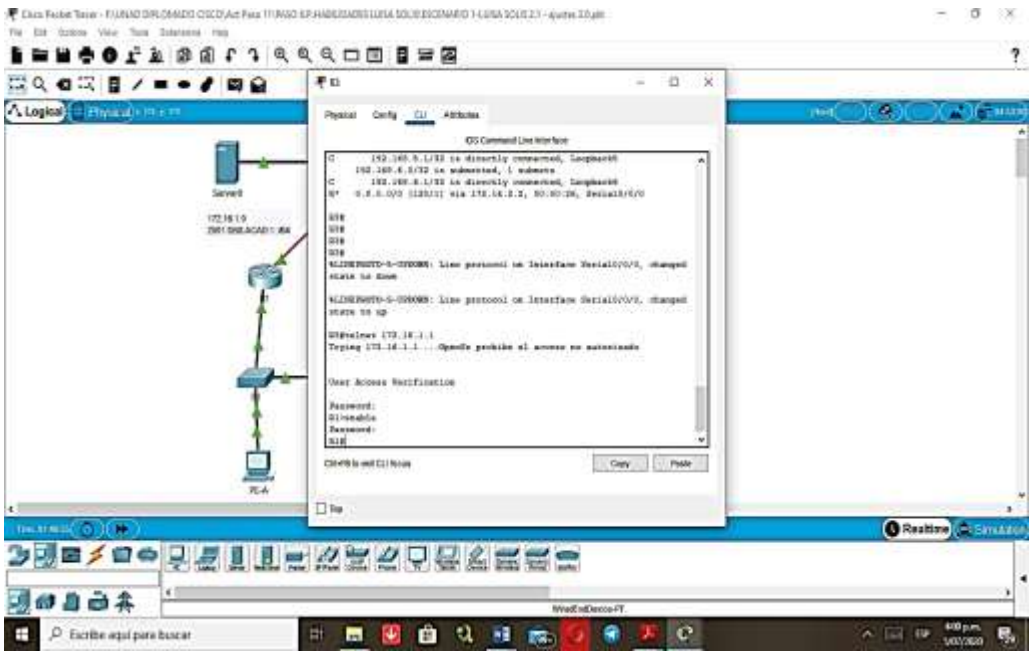
Si realizamos telnet desde el R1 a R2, a continuación, podremos ver la imagen que verifica que se obtenga acceso en forma correcta.

Figura. 28 Telnet de R1 a R2



Fuente propia

Figura. 29 Telnet dese R3 a 172.16.1.1, R1



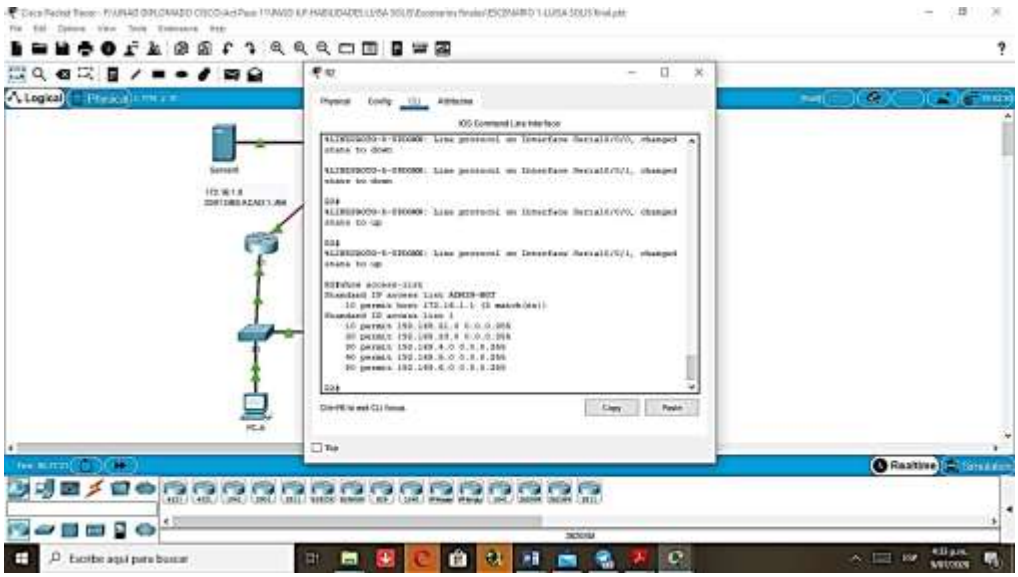
Fuente propia

1.8.1. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 24. Estudio de comando CLI

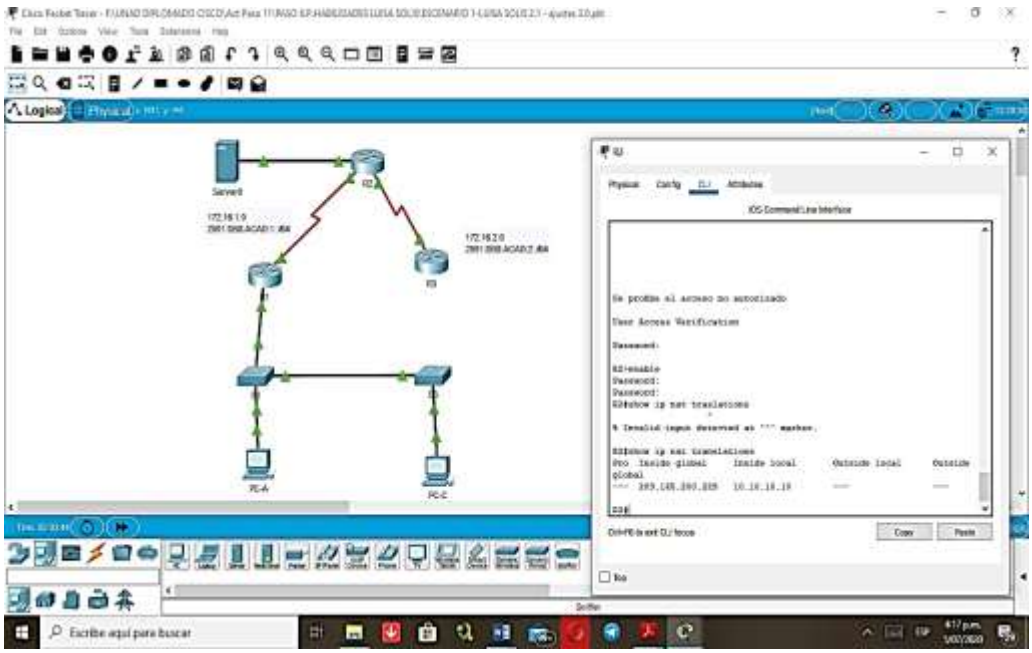
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface g0/1 Router(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat

Figura. 30 Comando show access-list en R2



Fuente propia

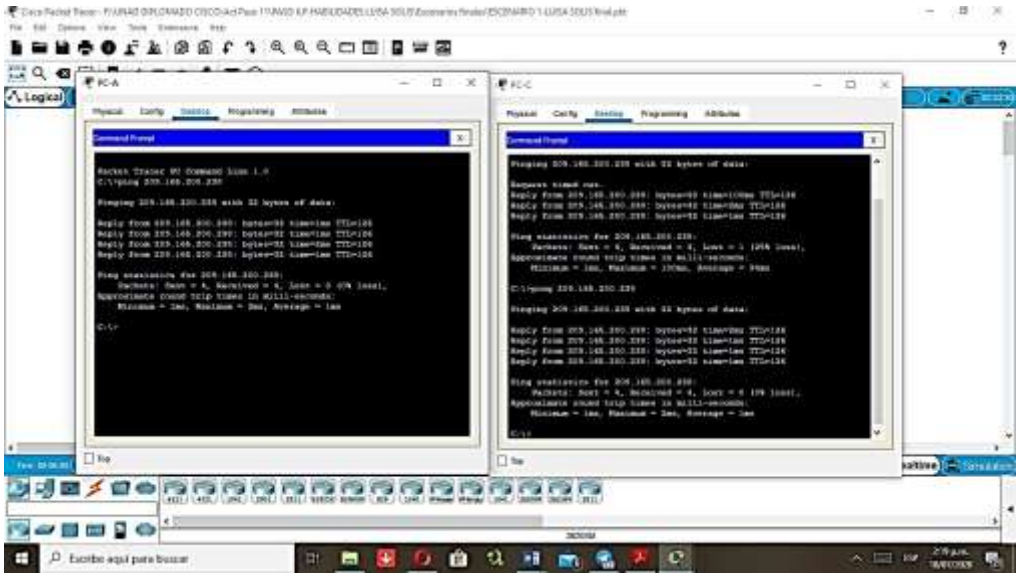
Figura. 31 Comando show ip nat translations en R2



Fuente propia

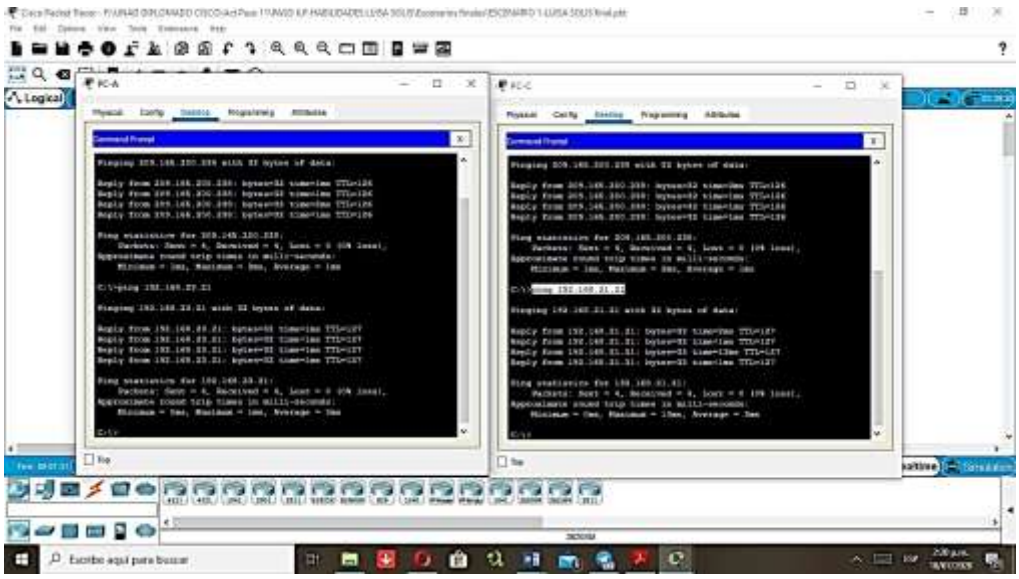
1.9. Comprobación de ping

Figura. 32.ping desde los PC al servidor de Internet



Fuente propia

Figura. 33. Ping de PC-A a PC-C



Fuente propia

2. PLANTEAMIENTO 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.

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

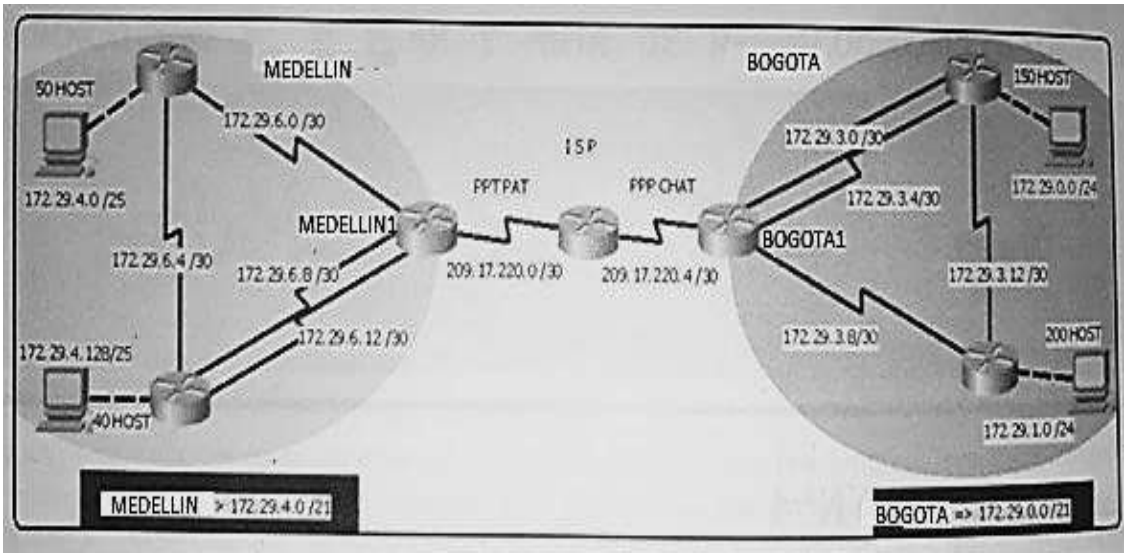
Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

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

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1

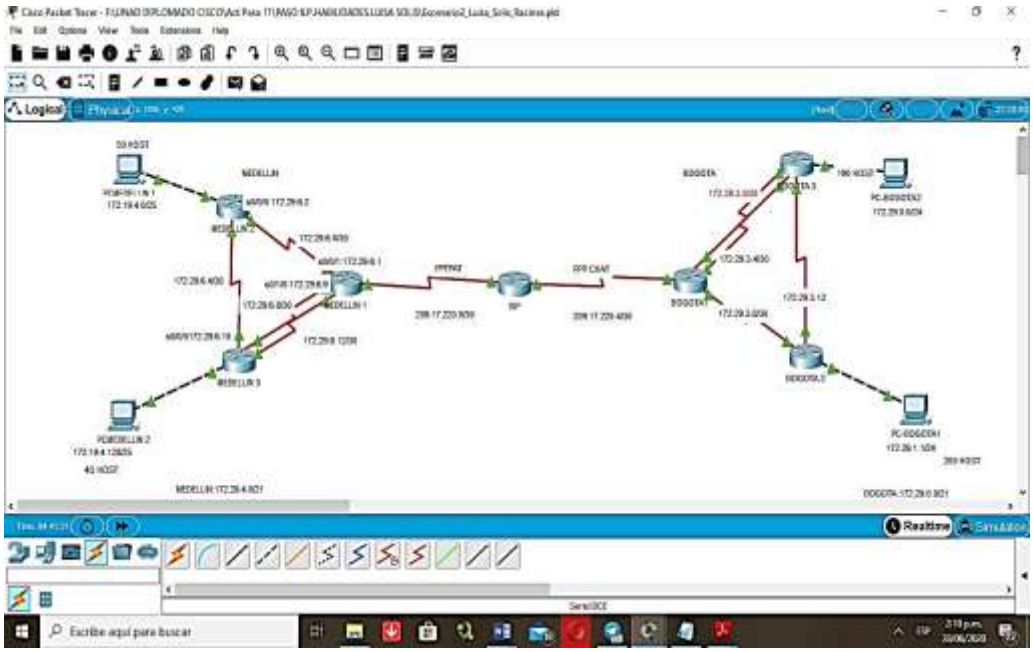
2.1. Topología a implementar en el escenario 2

Figura. 34 Diagrama de la topología a implementar



Fuente. Prueba de habilidades CCNA 2020

Figura. 35 Implementación física de la topología de red



Fuente propia

2.2. Direccionamiento IP

DISPOSITIVO	INTERFACE	DIRECCION IP	MASCARA DE SUBRED	GATEWAY
ISP	Se 0/0/0	209.17.220.1	255.255.255.252	
	Se 0/0/1	209.17.220.5	255.255.255.252	
MEDELLIN 1	Se 0/0/0	209.17.220.2	255.255.255.252	
	Se 0/0/1	**172.29.6.1**	**255.255.255.252**	
	Se 0/1/0	**172.29.6.9**	**255.255.255.252**	
	Se 0/1/1	172.29.6.13		
MEDELLIN 2	**Se 0/0/0**	**172.29.6.2**	255.255.255.252	
	Se 0/0/1	172.29.6.5	255.255.255.252	
	G0/0	172.29.4.1	255.255.255.128	
MEDELLIN 3	**Se 0/0/0**	**172.29.6.10**	**255.255.255.252**	
	Se 0/0/1	172.29.6.14	255.255.255.252	
	Se 0/1/0	172.29.6.6	255.255.255.252	
	G0/0	172.29.4.129	255.255.255.128	
BOGOTA 1	Se 0/0/0	209.17.220.6	255.255.255.252	
	Se 0/0/1	172.29.3.9	255.255.255.252	
	Se 0/1/0	172.29.3.1	255.255.255.252	
	Se 0/1/1	172.29.3.5	255.255.255.252	
BOGOTA 2	Se 0/0/0	172.29.3.10	255.255.255.252	
	Se 0/0/1	172.29.3.13	255.255.255.252	
	Se 0/1/0	172.29.3.18	255.255.255.252	
	G0/0	172.29.1.1	255.255.255.0	
BOGOTA3	Se 0/0/0	172.29.3.2	255.255.255.252	
	Se 0/0/1	172.29.3.6	255.255.255.252	
	Se 0/1/0	172.29.3.14	255.255.255.252	

	G0/0	172.29.0.1	255.255.255.128	
PC-BTA 1		172.29.1.2	255.255.255.0	172.29.1.1
PC-BTA 2		172.29.0.2	255.255.255.0	172.29.0.1
PC.ME -1		172.19.4.2	255.255.255.128	172.29.4.1
PC-ME – s0/0/2		172.19.4.130	255.255.255.128	172.29.4.129

2.3. Configuración básica de dispositivos

A continuación se llevará a cabo la configuración básica de los routers presentes en la tipología, en este proceso se asignaran los nombres a los dispositivos, configuración de contraseñas de exec privilegiado, Telnet, entre otros aspectos básicos de seguridad, cuyo proceso se especifica a continuación.

Tabla 25. Configuración básica de los routers

Dispositivo	Configuración Básica
ISP	Router1#no ip domain-lookup Router1#hostname Bogota1 ISP(config)#hostname ISP ISP(config)#enable secret class ISP(config)#line console 0 ISP(config)#exec-timeout 0 0 ISP(config)#pass cisco ISP(config)#login ISP(config)#logging synchronous ISP(config)#line vty 0 4 ISP(config)#pass cisco ISP(config)#exec-timeout 0 0 ISP(config)#pass cisco ISP(config)#login ISP(config)#logging synchronous ISP(config)#service password-encryption ISP(config)#banner motd &acceso no autorizado& ISP(config)#exit ISP#copy running-config startup-config
Medellin1	Router2#config ter Router2config)#no ip domain-lookup Medellin1(config)#hostname Medellin1 Medellin1(config)#enable secret class Medellin1(config)#line console 0 Medellin1(config)#exec-timeout 0 0 Medellin1(config)#pass cisco Medellin1(config)#login Medellin1(config)#logging synchronous Medellin1(config)#line vty 0 4 Medellin1(config)#pass cisco Medellin1(config)#exec-timeout 0 0 Medellin1(config)#pass cisco Medellin1(config)#login Medellin1(config)#logging synchronous service password-encryption banner motd &acceso no autorizado& Medellin1(config)#exit copy running-config startup-config
Medellin2	Router3#no ip domain-lookup Router3#hostname Bogota1 Medellin2(config)#hostname Medellin2 Medellin2(config)#enable secret class Medellin2(config)#line console 0 Medellin2(config)#exec-timeout 0 0 Medellin2(config)#pass cisco Medellin2(config)#login

	Medellin2(config)#logging synchronous Medellin2(config)#line vty 0 4 Medellin2(config)#pass cisco Medellin2(config)#exec-timeout 0 0 Medellin2(config)#pass cisco Medellin2(config)#login Medellin2(config)#logging synchronous service password-encryption Medellin2(config)#banner motd &acceso no autorizado& Medellin2(config)#exit Medellin2#copy running-config startup-config
Medellin3	Router3#no ip domain-lookup Router3#hostname Bogota1 Medellin3(config)#hostname Medellin2 Medellin3(config)#enable secret class Medellin3(config)#line console 0 Medellin3(config)#exec-timeout 0 0 Medellin3(config)#pass cisco Medellin3(config)#login Medellin3(config)#logging synchronous Medellin3(config)#line vty 0 4 Medellin3(config)#pass cisco Medellin3(config)#exec-timeout 0 0 Medellin3(config)#pass cisco Medellin3(config)#login Medellin3(config)#logging synchronous Medellin3(config)#logging service password-encryption Medellin1(config)#banner motd &acceso no autorizado& Medellin3(config)#exit Medellin3#copy running-config startup-config
Bogota1	Router4#no ip domain-lookup Router4#hostname Bogota1 Router4(config)#hostname Bogota1 Bogota1(config)#enable secret class Bogota1(config)#line console 0 Bogota1(config)#exec-timeout 0 0 Bogota1(config)#pass cisco Bogota1(config)#login Bogota1(config)#logging synchronous Bogota1(config)#line vty 0 4 Bogota1(config)#pass cisco Bogota1(config)#exec-timeout 0 0 Bogota1(config)#pass cisco Bogota1(config)#login Bogota1(config)#logging synchronous Bogota1(config)#service password-encryption Bogota1(config)#banner motd &acceso no autorizado& Bogota1(config)#exit Bogota1#copy running-config startup-config
Bogota2	Router5#no ip domain-lookup Router5#hostname Bogota2 Router5(config)#hostname Bogota2 Bogota2(config)#enable secret class Bogota2(config)#line console 0 Bogota2(config)#exec-timeout 0 0 Bogota2(config)#pass cisco Bogota2(config)#login Bogota2(config)#logging synchronous Bogota2(config)#line vty 0 4 Bogota2(config)#pass cisco Bogota2(config)#exec-timeout 0 0 Bogota2(config)#pass cisco Bogota2(config)#login Bogota2(config)#logging synchronous Bogota2(config)#service password-encryption Bogota2(config)#banner motd &acceso no autorizado& Bogota2(config)#exit

	Bogota2#copy running-config startup-config
Bogota3	Router6#no ip domain-lookup Router6#hostname Bogota2 Router6(config)#hostname Bogota3 Bogota3(config)#enable secret class Bogota3(config)#line console 0 Bogota3(config)#exec-timeout 0 0 Bogota3(config)#pass cisco Bogota3(config)#login Bogota3(config)#logging synchronous Bogota3(config)#line vty 0 4 Bogota3(config)#pass cisco Bogota3(config)#exec-timeout 0 0 Bogota3(config)#pass cisco Bogota3(config)#login Bogota3(config)#logging synchronous Bogota3(config)#service password-encryption Bogota3(config)#banner motd &acceso no autorizado& Bogota1(config)#exit Bogota1#copy running-config startup-config

2.3.1. Configuración de las interfaces de los routers

Tabla 26. Configuración de las interfaces de los routes

Dispositivo	Configuración de la interface
ISP	ISP(config-if)#interface serial 0/0/0 ISP(config-if)#ip add 209.17.220.1 255.255.255.252 ISP(config-if)#no shut ISP(config-if)#interface s0/0/1 ISP(config-if)#ip add 209.17.220.5 255.255.255.252 ISP(config-if)#no shutdown
Medellin1	Medellin1(config)#interface s0/0/0 Medellin1(config-if)#ip add 209.17.220.2 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)# Medellin1(config-if)#interface serial 0/0/1 Medellin1(config-if)#ip add 172.29.6.1 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config)#interface serial0/1/0 Medellin1(config-if)#ip add 172.29.6.9 255.255.255.252 Medellin1(config-if)#no shutdown Medellin1(config-if)#exit Medellin1(config)#inter serial 0/1/1 Medellin1(config-if)#ip add 172.29.6.13 255.255.255.252 Medellin1(config-if)#no shutdown
Medellin2	Medellin2(config)#inter s0/0/0 Medellin2(config-if)#ip add 172.29.6.2 255.255.255.252 Medellin2(config-if)#no shut Medellin2(config-if)#inter s0/0/1 Medellin2(config-if)#ip add 172.29.6.5 255.255.255.252 Medellin2(config-if)#no shut Medellin2(config-if)#exit Medellin2(config-if)#exit Medellin2(config)#interface g0/0 Medellin2(config-if)#ip add 172.29.4.1 255.255.255.128 Medellin2(config-if)#no shutdown
Medellin3	Medellin3(config)#interf serial 0/0/0 Medellin3(config-if)#ip add 172.29.6.10 255.255.255.252 Medellin3(config-if)#no shutdown

	Medellin3#conf ter Medellin3(config)#interface ser0/0/1 Medellin3(config-if)#ip add 172.29.6.14 255.255.255.252 Medellin3(config)#interf s0/1/0 Medellin3(config-if)#ip add 172.29.6.6 255.255.255.252 Medellin3(config-if)#no shutdown Medellin3(config)#interface g0/0 Medellin3(config-if)#ip add 172.29.4.129 255.255.255.128 Medellin3(config-if)#no shutdown
Bogota1	Bogota1(config)#inter serial 0/0/0 Bogota1(config-if)#ip add 209.17.220.6 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config)#inter se 0/0/1 Bogota1(config-if)#ip add 172.29.3.9 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config)#inter se 0/1/0 Bogota1(config-if)#ip add 172.29.3.1 255.255.255.252 Bogota1(config-if)#no shutdown Bogota1(config)#inter se 0/1/1 Bogota1(config-if)#ip add 172.29.3.5 255.255.255.252 Bogota1(config-if)#no shutdown
Bogota2	Bogota2(config)#inter serial 0/0/0 Bogota2(config-if)#ip add 172.29.3.10 255.255.255.252 Bogota2(config-if)#no shutdown Bogota2(config)#inter serial 0/0/1 Bogota2(config-if)#ip add 172.29.3.13 255.255.255.252 Bogota2(config-if)#no shutdown Bogota2(config-if)#exit Bogota2(config)#inter g0/0 Bogota2(config-if)#ip add 172.29.1.1 255.255.255.0 Bogota2(config-if)#no shutdown
Bogota3	Bogota3(config)#interface serial 0/0/0 Bogota3(config-if)#ip add 172.29.3.2 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config)#inter serial 0/0/1 Bogota3(config-if)#ip add 172.29.3.6 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#inter serial 0/1/0 Bogota3(config-if)#ip add 172.29.3.14 255.255.255.252 Bogota3(config-if)#no shutdown Bogota3(config-if)#exit Bogota3(config)#inter g0/0 Bogota3(config-if)#ip add 172.29.0.1 255.255.255.128 Bogota3(config-if)#no shutdown

Parte 1. Configuración del enrutamiento

Para configurar el enrutamiento en la red, se implementará el protocolo OSPF (Open Shortest Path First), que se define como un protocolo de enrutamiento jerárquico y que calcula la ruta más corta, a través de que cada router conozca o identifique los routers cercanos junto con sus direcciones y la distancia a la cual se

encuentra ubicado, lo que le permite conocer en forma anticipada, cual es la ruta más corta para enviar un paquete de datos a determinado destino.

2.3.2. Parámetros para la configuración de OSPF

Tabla 27. Parámetros de configuración OSPF

Configuration Item or Task	Specification
Router ID ISP	No configurar
Router ID MEdellin1	2.2.2.2
Router ID Bogota1	3.3.3.3
Router ID Bogota2	4.4.4.4
Router ID Bogota3	5.5.5.5
Router ID Medellin2	6.6.6.6
Router ID MEdellin3	7.7.7.7
Configurar todas las interfaces LAN como pasivas	
Establecer ancho de banda de referencia en los routers	auto-cost reference-bandwidth 100

Tabla 28. Configuración de OSPF

Dispositivo	Configuración	Redes conectadas
Medellin1	Medellin1(config)#router ospf 1 Medellin1(config-router)#router-id 2.2.2.2 Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0 Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0 Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0	172.29.6.0/30 Serial0/0/1 172.29.6.8/30 Serial0/1/0 172.29.6.12/30
Bogota1	Bogota1(config)#router ospf 1 Bogota1(config-router)#router-id 3.3.3.3 Bogota1(config-router)#network 172.29.3.0 0.0.0.3 area 0 Bogota1(config-router)#network 172.29.3.4 0.0.0.3 area 0 Bogota1(config-router)#network 172.29.3.8 0.0.0.3 area 0	172.29.3.0/30 Serial0/1/0 172.29.3.4/30 Serial0/1/1 172.29.3.8/30
Medellin2	Medellin2(conf)#router ospf 1 Medellin2(conf-router)#router-id 4.4.4.4 Medellin2(conf-router)#network 172.29.6.0 0.0.0.3 area 0 Medellin2(conf-router)#network 172.29.6.4 0.0.0.3 area 0 Medellin2(conf-router)#network 172.29.4.0 0.0.0.3 area 0	172.29.4.0/25, Gig0/0 172.29.6.0/30 Serial0/0/0 172.29.6.4/30 Serial0/0/1
Medellin3	Medellin3(conf)#router ospf 1 Medellin3(conf-router)#router-id 5.5.5.5 Medellin3(conf-router)#network 172.29.6.4 0.0.0.3 area 0 Medellin3(conf-router)#network 172.29.6.8 0.0.0.3 area 0 Medellin3(conf-router)#network 172.29.6.12 0.0.0.3 area 0 Medellin3(conf-router)#network 172.29.4.128 0.0.0.3 area 0	172.29.4.128/25 Gi0/0 172.29.6.4/30 Serial0/1/0 172.29.6.8/30 Serial0/0/0 172.29.6.12/30 Serial0/0/1
Bogotá2	Bogota2(config)#router ospf 1	172.29.1.0/24 Gi0/0

	Bogota2(config-router)#router-id 6.6.6.6 Bogota2(config-router)#network 172.29.3.8 0.0.0.3 area 0 Bogota2(config-router)#network 172.29.3.12 0.0.0.3 area 0 Bogota2(config-router)#network 172.29.1.0 0.0.0.3 area 0	172.29.3.8/30 Serial0/0/0 172.29.3.12/Serial0/0/1
Bogota3	Bogota3(config)#router ospf 1 router-id 7.7.7.7 Bogota3(config-router)#network 172.29.3.0 0.0.0.3 area 0 Bogota3(config-router)#network 172.29.3.4 0.0.0.3 area 0 Bogota3(config-router)#network 172.29.3.12 0.0.0.3 area 0 Bogota3(config-router)#network 172.29.0.0 0.0.0.3 area 0	172.29.0.0/25, Gig0/0 172.29.3.0/30 Serial0/0/0 172.29.3.4/30 Serial0/0/1 172.29.3.12/30 Serial0/1/0

Para la configuración del protocolo OSPF, se configura una identificación de router, mediante el comando router-id, esta identificación debe ser única, ya que es como la cédula del dispositivos en la red.

Luego se realiza un proceso de anuncio de las redes conectadas directamente al dispositivo o router, mediante el comando network, el área 0, es el área principal de la red, esta debe existir obligatoriamente y todas las deben estar conectadas a ella; para ver las redes conectadas directamente, se usa el comando show ip route connected; por último se establecen las interfaces LAN como pasivas, a través del comando passive-interface, esto para que no emitan ninguna información extra de routing.

Figura. 36 Ejecución del comando show ip route connented

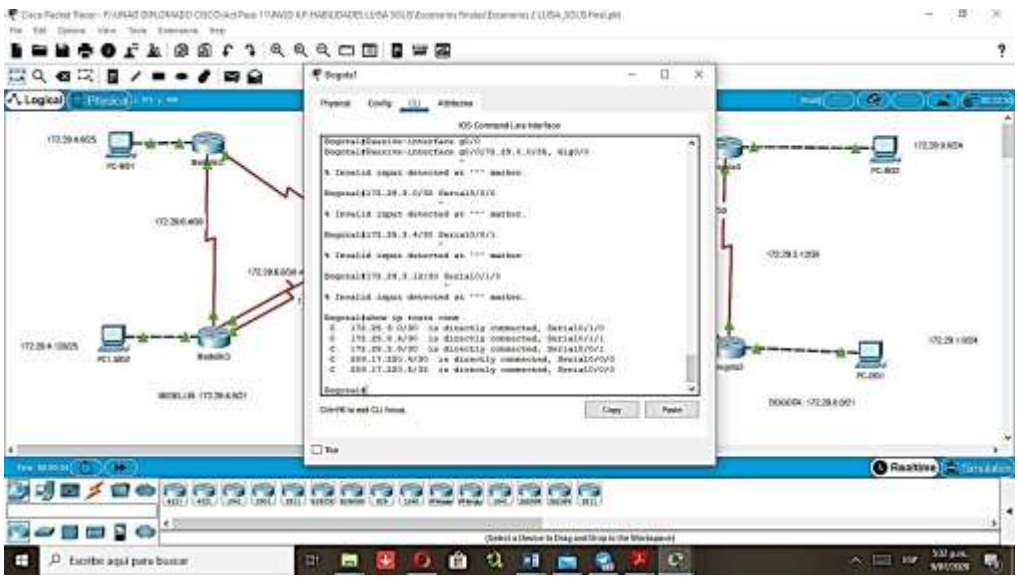
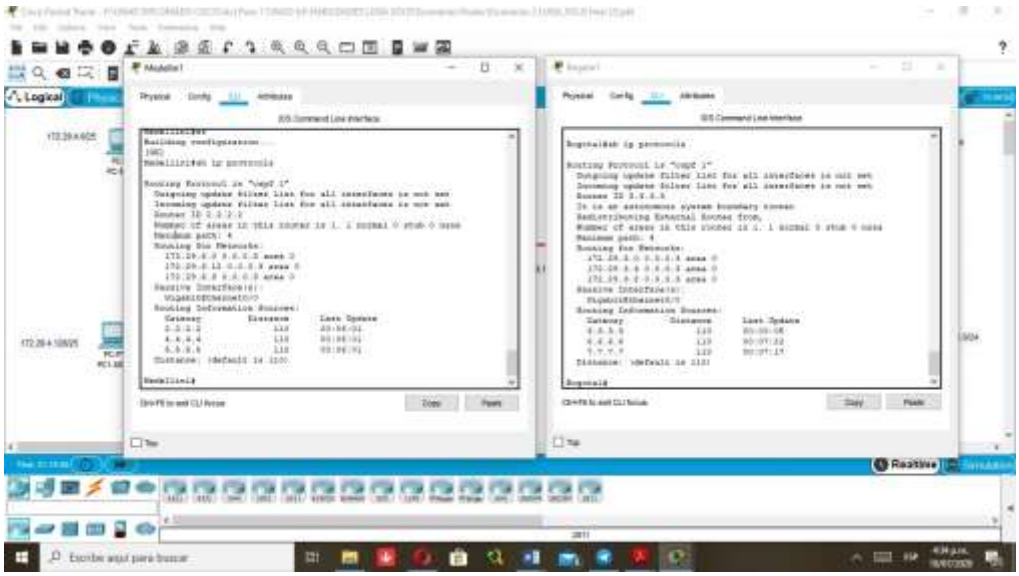


Figura. 37 Implementación del comando show ip protocols en Medellin1 y Bogota1



Fuente propia

2.3.3. Configuración de rutas por defecto en Bogota1 y Medellin1

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

Tabla 29. Configuración de rutas por defecto desde Bogota1 y Medellin1 hacia ISP

Dispositivo	Configuración
Bogota1	Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.4 Bogota1(config)#router ospf 1 Bogota1(config-router)#default-information originate Bogota1(config-router)#end Passive-interface g0/0
Medellin1	Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.0 Medellin1(config)#router ospf 1 Medellin1(config-router)#default-information originate Medellin1(config-router)#Passive-interface g0/0

El comando ip route 0.0.0.0 0.0.0.0 id-red y luego el comando router ospf 1, permite configurar el Gateway de ultimo recurso o ruta por defecto y a través del comando default-infortmation originate, se le ordena al dispositivo que la ruta creada por defecto se comparta con todos los routers conectados a la red.

Esta ruta se usa para enrutar o redirigir los paquetes que van hacia redes que no están especificadas o enumeradas en la tabla de enrutamiento.

2.3.4. 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.

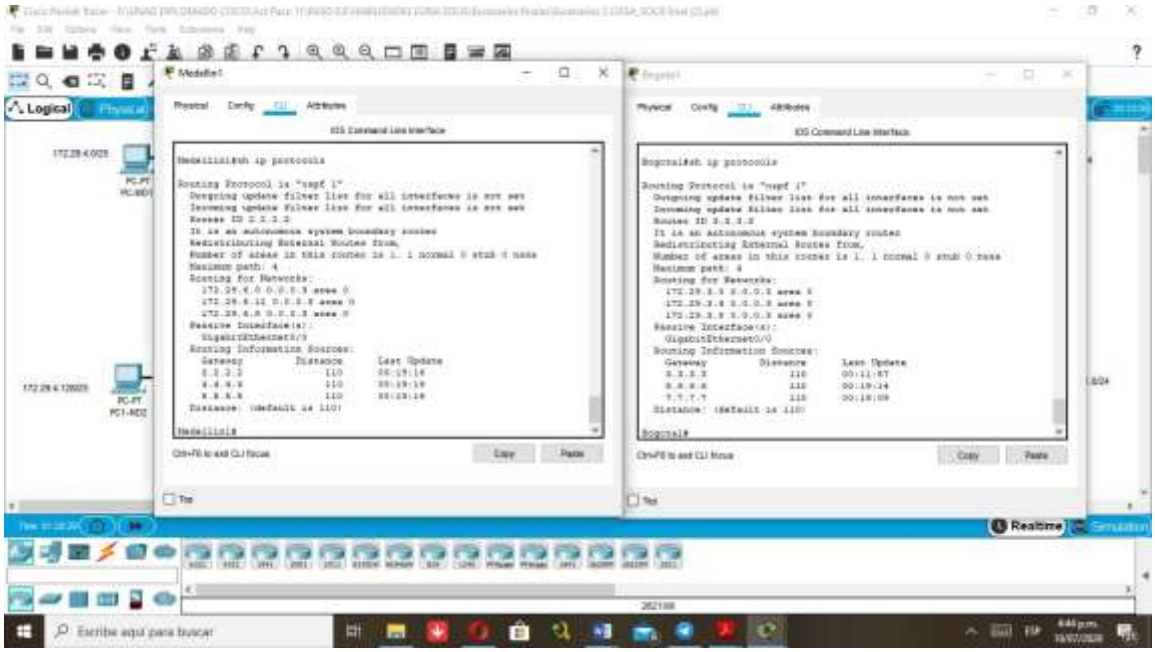
Tabla 30. Configuracion de rutas estáticas dirigidas en ISP

Dispositivo	Configuración
ISP	ISP(config)#ip route 172.29.4.0 255.255.255.0 209.17.220.0 ISP(config)#ip route 172.29.0.0 255.255.255.0 209.17.220.4

2.4. Parte 2. Tablas de enrutamiento

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

Figura. 38 Ejecutar comando show ip protocols en Medellin1 y Bogota1



Fuente propia

Figura. 39 Ejecución del comando show ip protocols en Bogota 2 y Medellin2

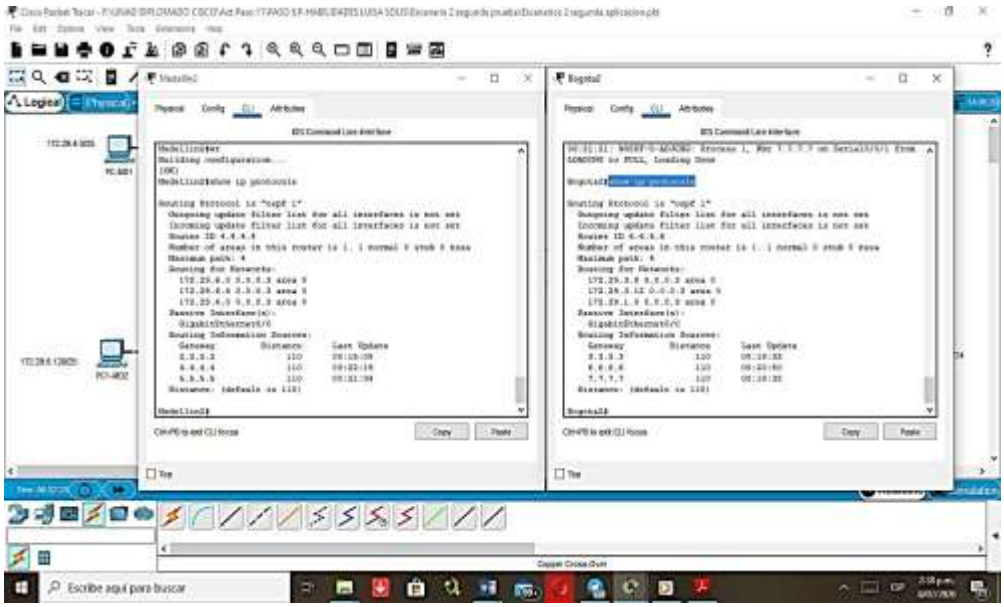
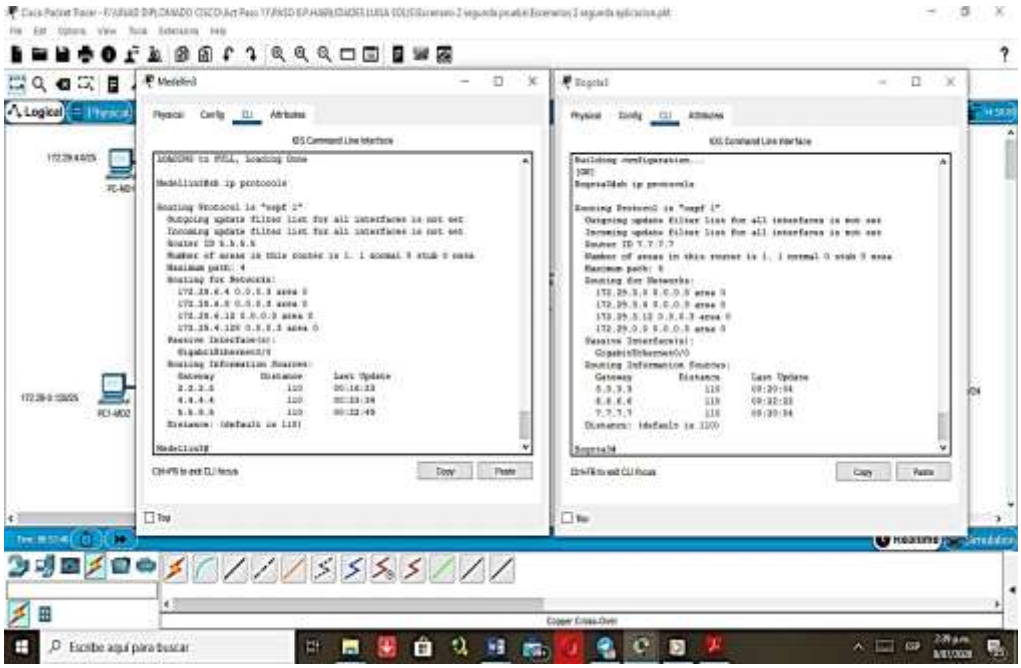


Figura. 40 Ejecución del comando show ip protocols en MEdellin3 y Bogota3



Fuente propia

2.4.2. Verificar el balanceo de carga que presentan los routes

A continuación mediante el comando show ip route, se mostrara el balanceo de carga que presentan los routers, se puede identificar la red con la mínima ruta o el salto mas corto, a través porque esta tiene un asterisco (*).

Este pasa cuando un router identifica varias o muchas rutas a través del proceso de ruteo y debe elegir aquella con el menor coste o con costo mas bajo.

Figura. 41 Identificación del balanceo de carga en Medellin1 y Bogota1

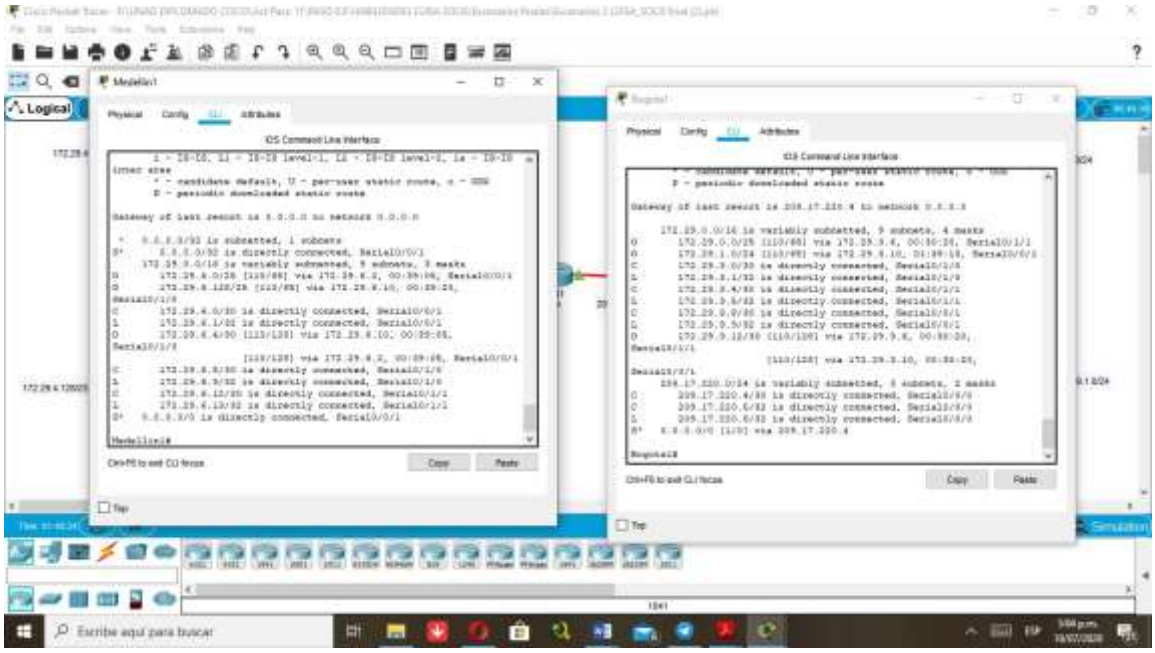
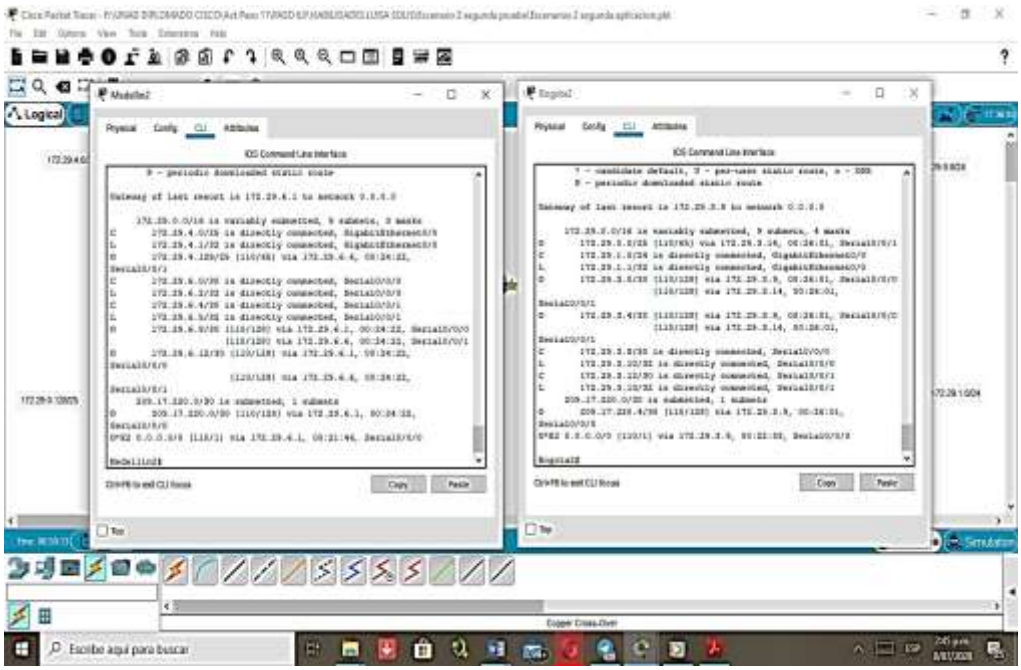
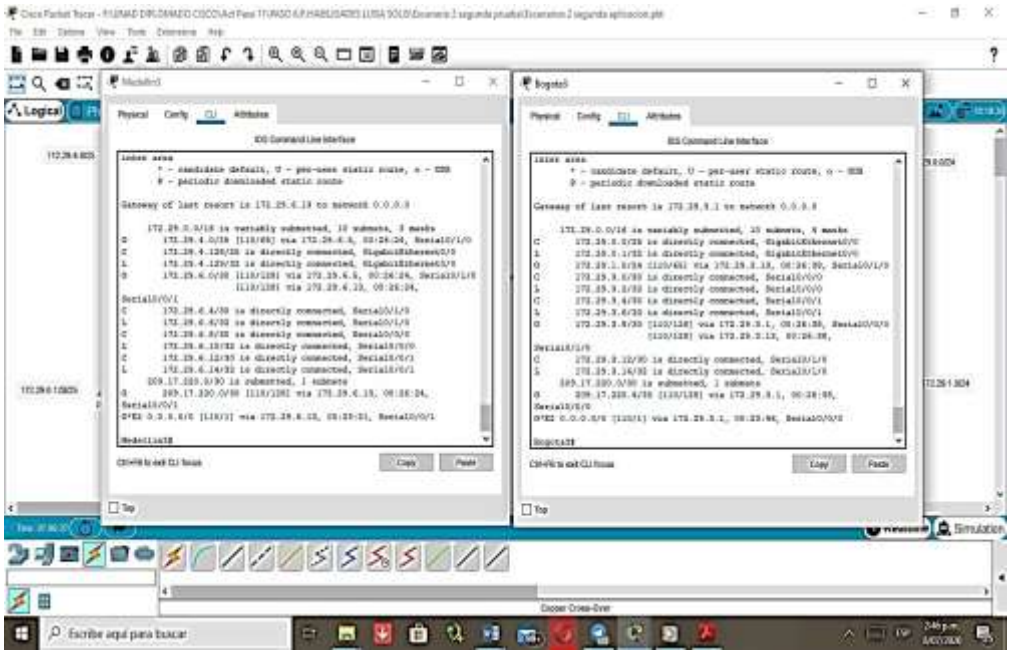


Figura. 42 Identificación de balanceo de carga en Medellin2 y Bogota2



Fuente propia

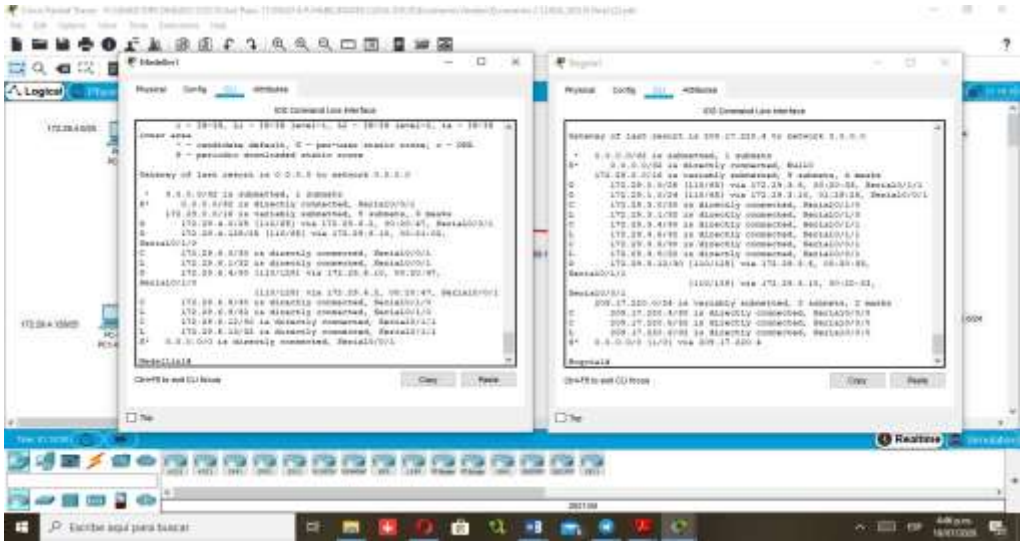
Figura. 43 Verificación de balanceo de carga en Medellin3 y Bogota3



Fuente propia

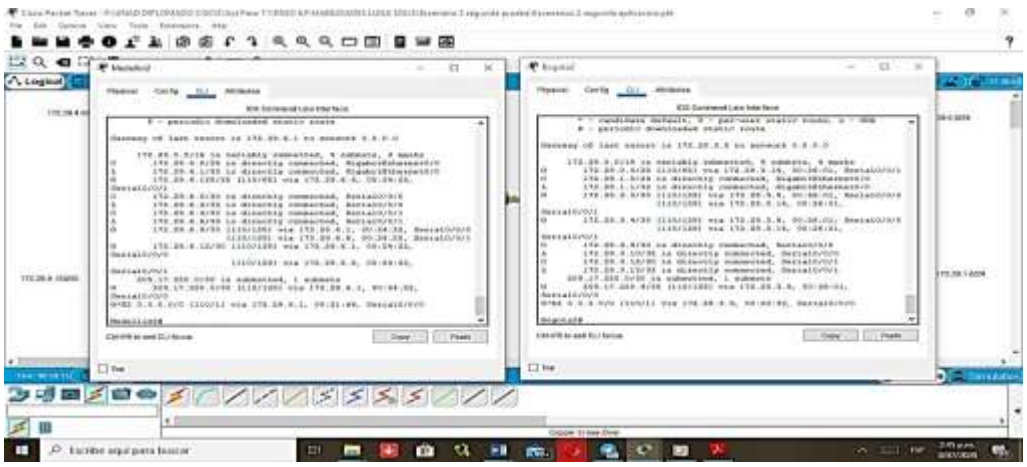
2.4.3. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Figura. 44 Similitudes entre los routes Bogota1 y Medellin1



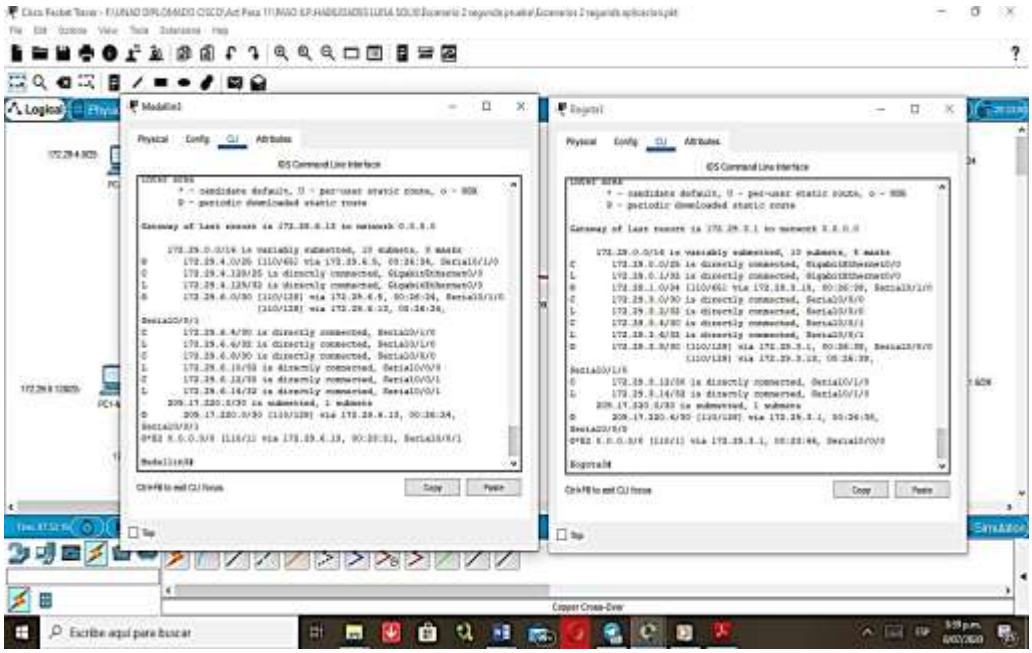
2.4.4. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

Figura. 45 Verificar el OSPF en los routers Medellin2 y Bogota2



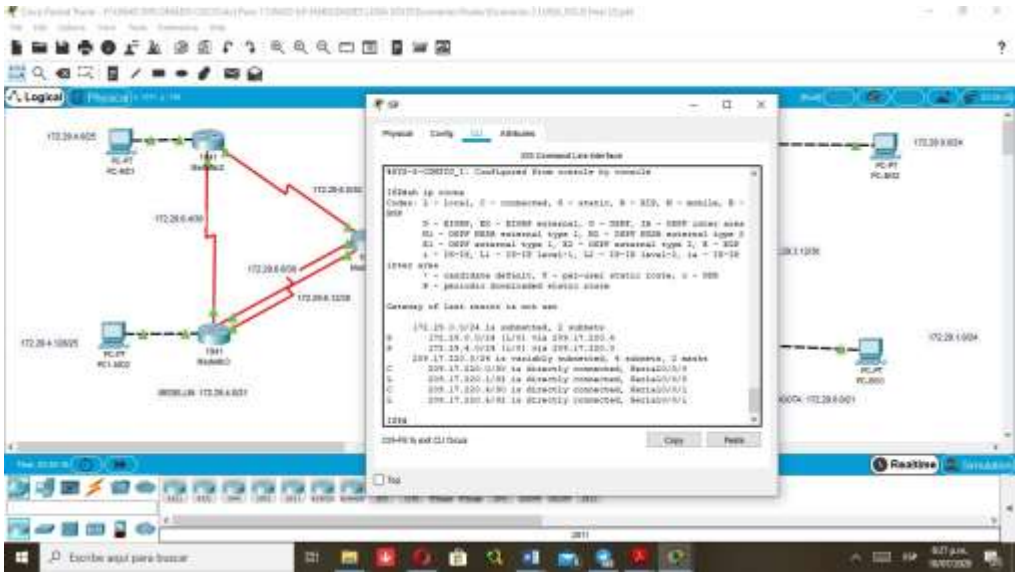
2.5.4. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Figura. 46 Visualización de OSPF en Bogota3 y Medellin3



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

Tabla 31. Rutas estáticas en ISP



2.6. Parte 3. Deshabilitar la propagación de OSPF

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

Tabla 32. Interfaces en las cuales no se debe deshabilitar la propagación de 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

Tabla 33. Configuración de LAN como pasivas

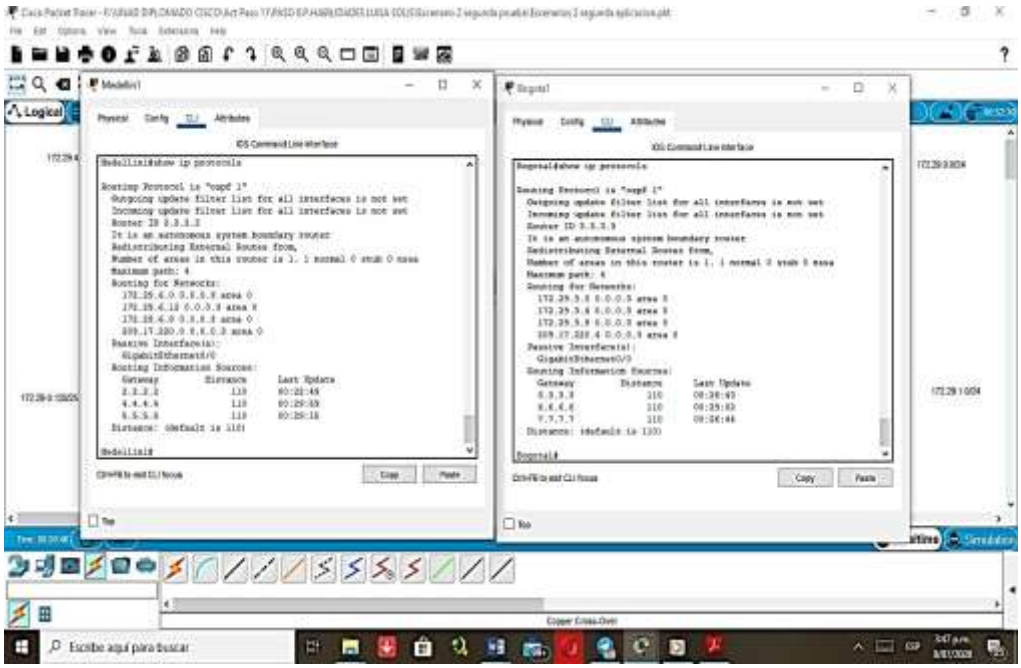
Dispositivo	Configuración
Medellin2	Medellin2(config)#router ospf 1 Medellin2(config-router)#passive-interface g0/0 Medellin2(config-router)#end
Medellin3	Medellin3(config)#router ospf 1 Medellin3(config-router)#passive-interface g0/0 Medellin3(config-router)#en
Bogota2	Bogota2(config)#router ospf 1 Bogota2(config-router)#Passive-interface g0/0 Bogota2(config-router)#end
Bogota3	Bogota3(config)#router ospf 1 Bogota3(config-router)#Passive-interface g0/0 Bogota3(config-router)#end

La configuración anterior solo se realiza en aquellos routers que tienen configurados redes LAN, como es el caso de los routers Bogota 1 y 2 y Medellín 1 y 2

2.7. Parte 4. Verificación de OSPF.

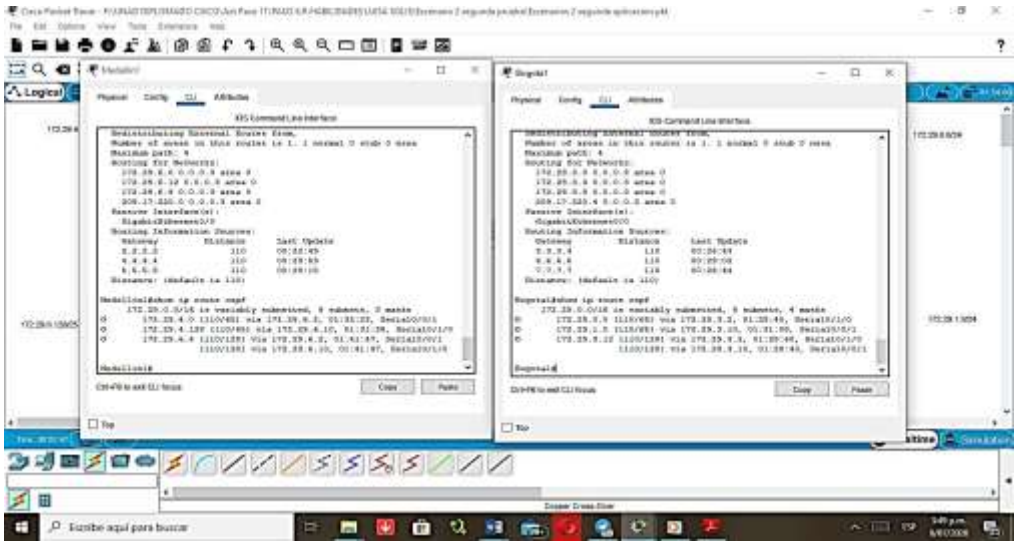
2.7.1. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

Figura. 47 Comando show ip protocols en Medellin1 y Bogota1.



Fuente propia

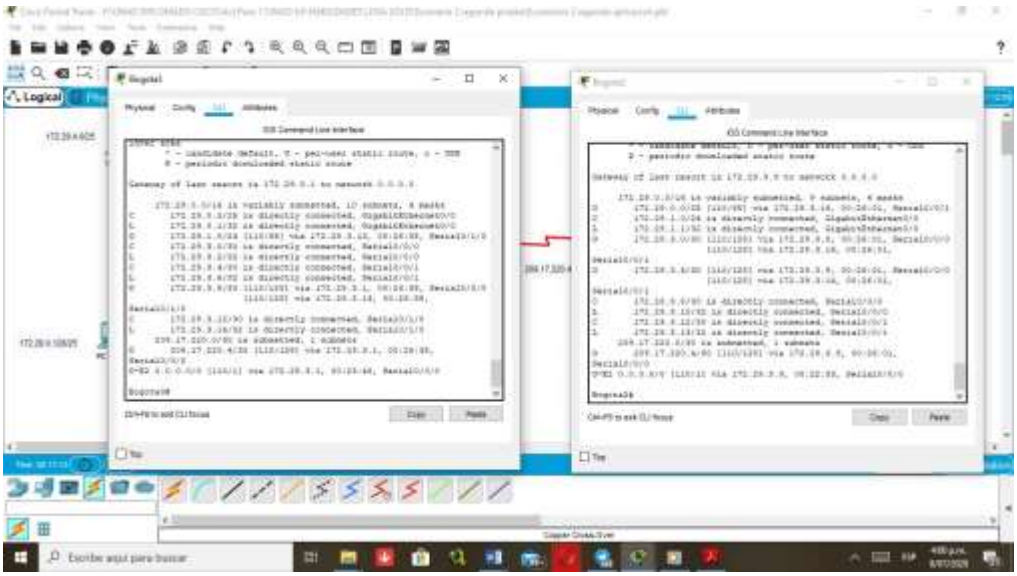
Figura. 48 Comando show ip route ospf en Medellin1 y Bogota1



Fuente propia

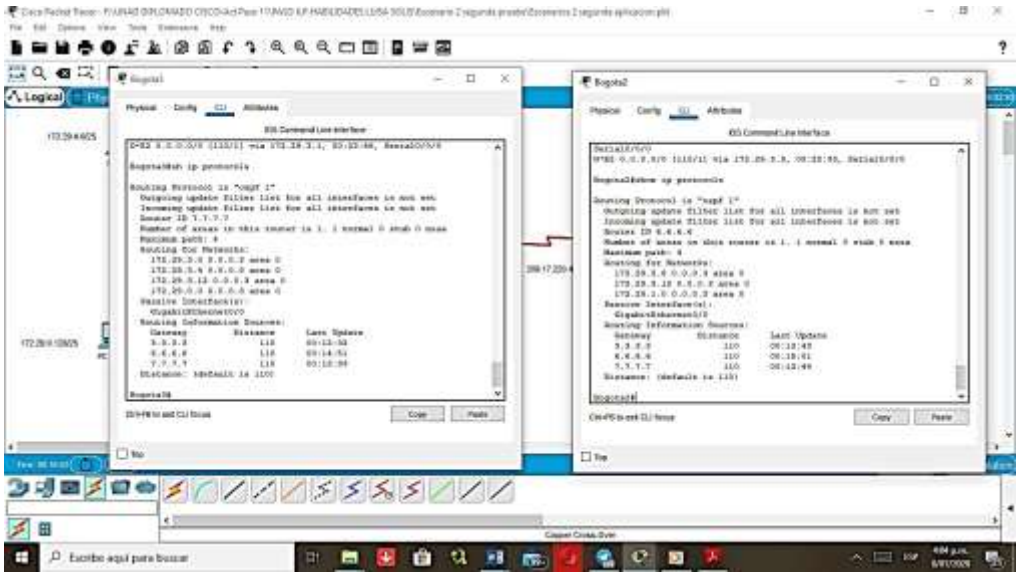
2.7.2. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Figura. 49 Uso del route en Bogota2 y Bogota3. Fuente propia comando show ip



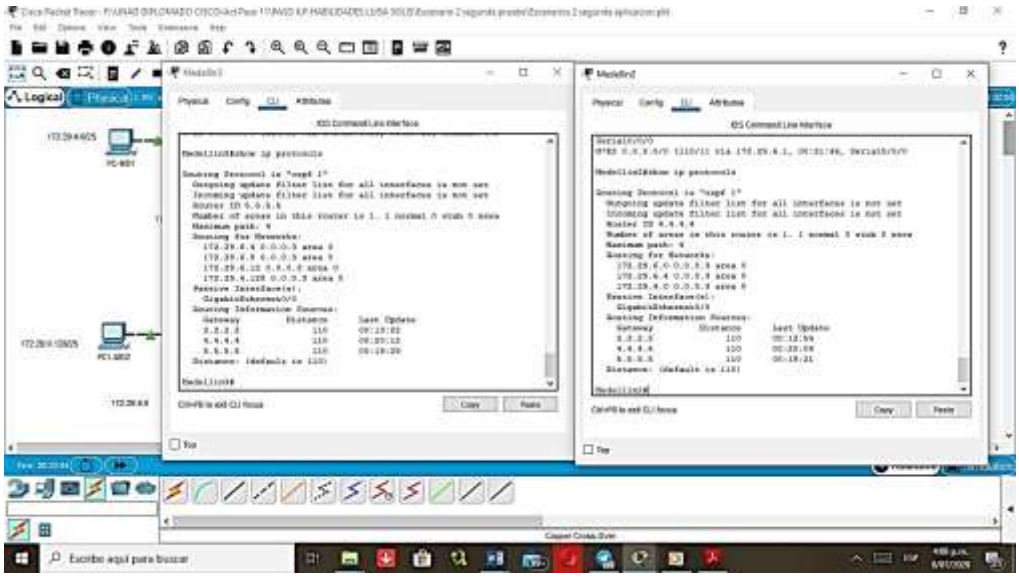
Fuente propia

Figura. 50 Uso del comando y show ip protocols en Bogota2 y Bogota3. Fuente propia



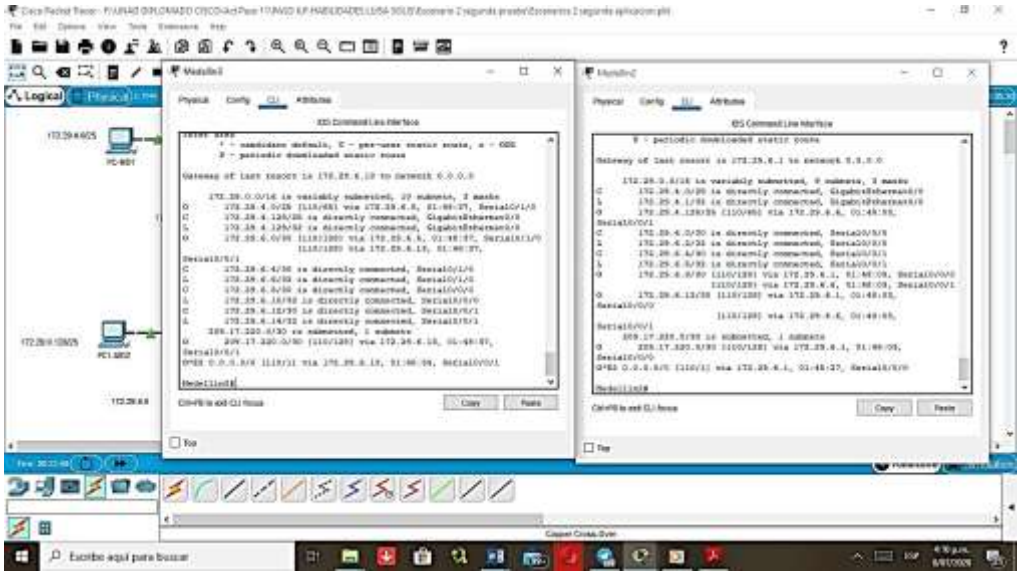
Fuente propia

Figura. 51 Comando show ip protocols en Medellin2 y Medellin3



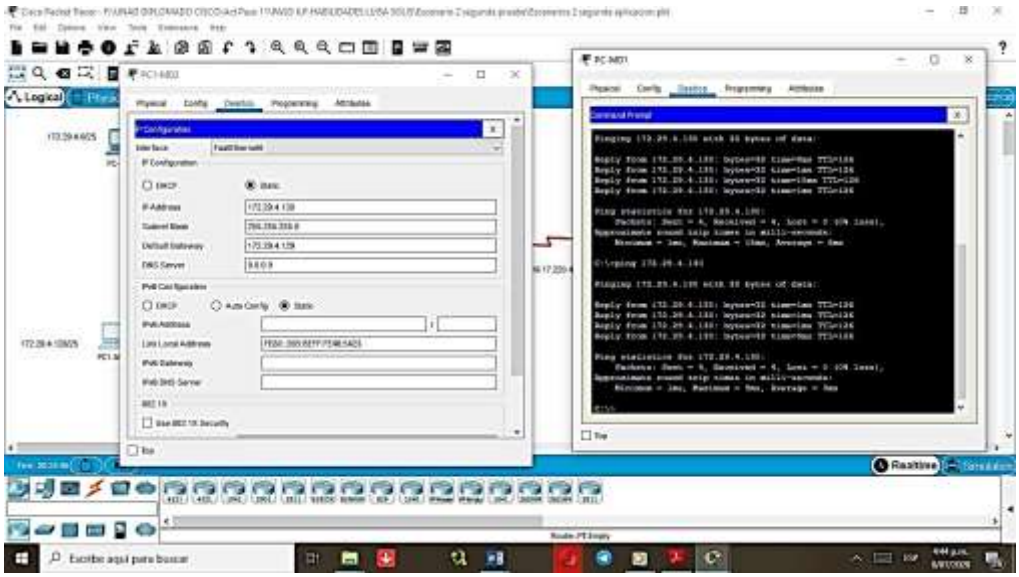
Fuente propia

Figura. 52 Comando show ip route en Medellin2 y Medellin3



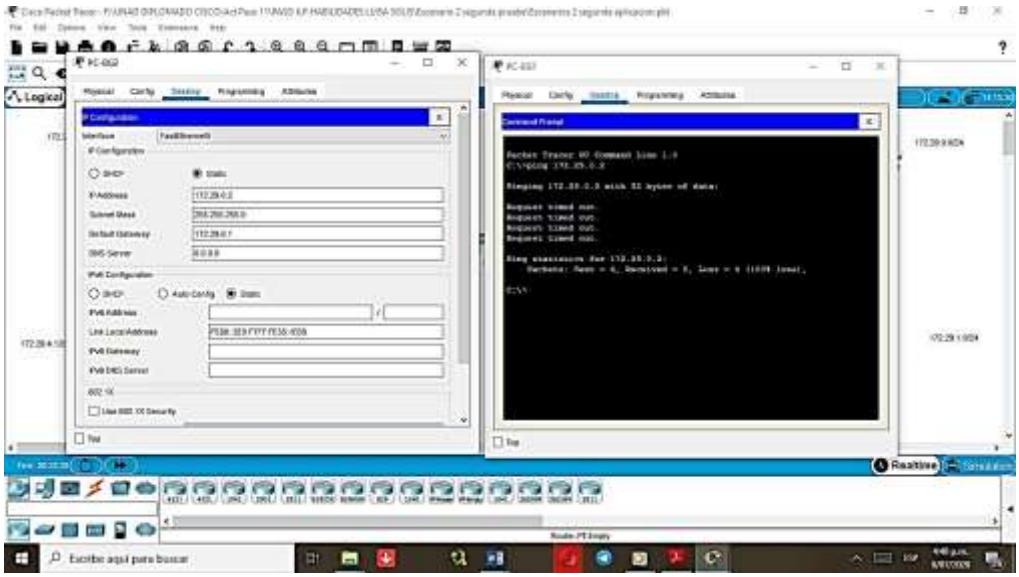
Fuente propia

Figura. 53 Verificación de conectividad entre host de la misma red, red Medellin1



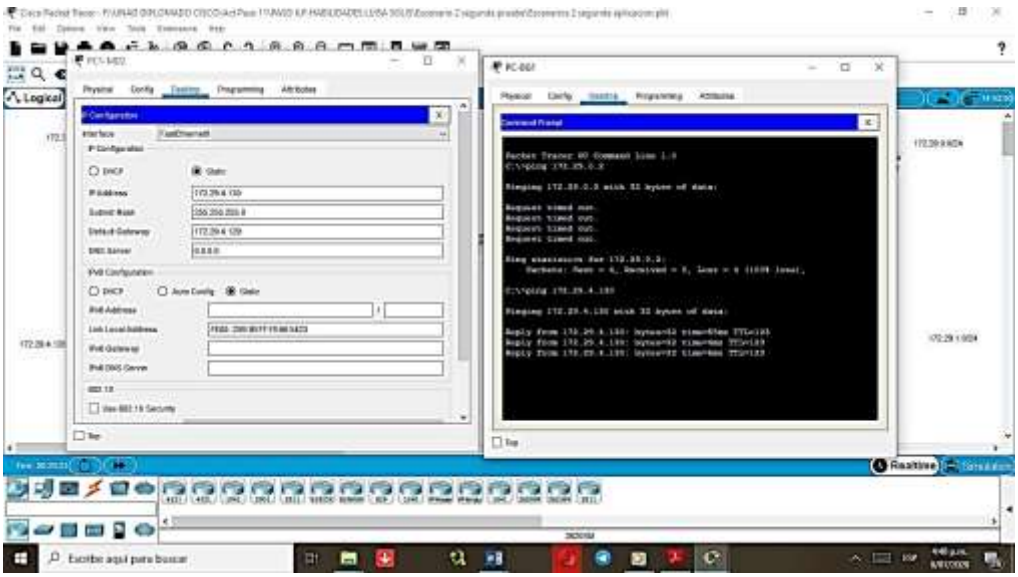
Fuente propia

Figura. 54 Verificación de conectividad entre host de la misma red. Bogota1



Fuente propia

Figura. 55 Verificación de conectividad entre host ubicados en distintas redes



Fuente propia

2.8. Parte 5: Configurar encapsulamiento y autenticación PPP.

PPP protocolo de punto a punto, permite establecer conexión entre dos nodo de una misma red.

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

Tabla 34. Configuración de encapculamiento y autenticación PPP

Dispositivo	Configuración
ISP	ISP(config)#username Medellin1 password cisco ISP(config)#interface s0/0/0 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication pap ISP(config-if)#ppp pap sent-username ISP pass cisco
Medellin1	Medellin1(config)#username ISP pass cisco Medellin1(config)#inter s0/0/0 Medellin1(config-if)#encapsulation ppp Medellin1(config-if)#ppp authentication pap Medellin1(config-if)#ppp pap sent-username Medellin1 pass cisco Medellin1(config-if)#exit

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

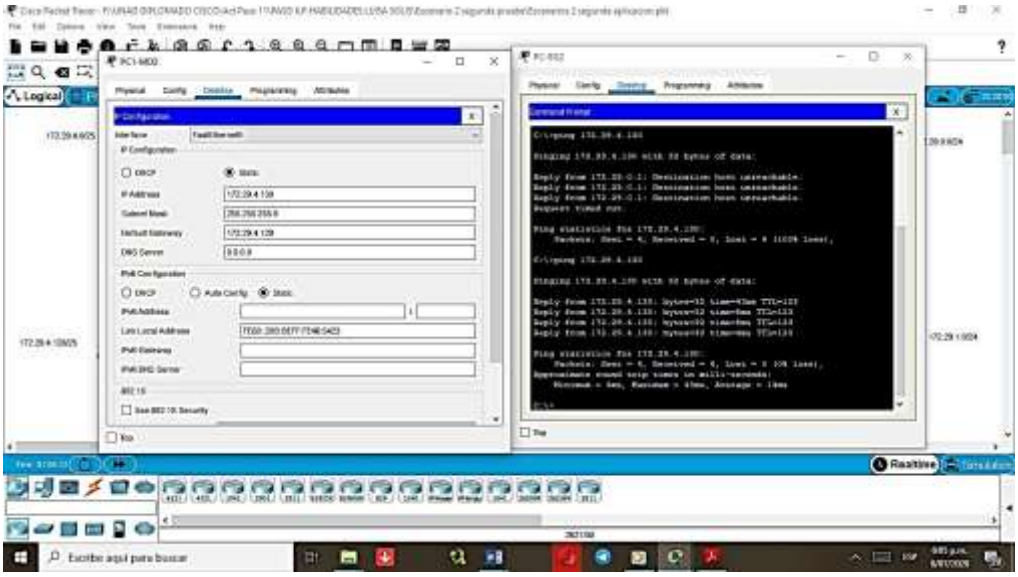
Tabla 35. Configuración de CHAT en Bogota

ISP	ISP(config)#username Bogota1 password cisco ISP(config-if)#int s0/0/1 ISP(config-if)#encapsulation ppp ISP(config-if)#ppp authentication chap
Bogota 1	Bogota1(config)#username ISP password cisco Bogota1(config)#int s0/0/0 Bogota1(config-if)#encapsulation ppp Bogota1(config-if)#ppp authentication chap Bogota1(config-if)#exit

2.9. Parte 6: Configuración de PAT.

2.9.1. 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.

Figura. 56 Probar conectividad entre host de distintas redes



Fuente propia

2.9.2. 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.

Tabla 36. Configuración de NAT

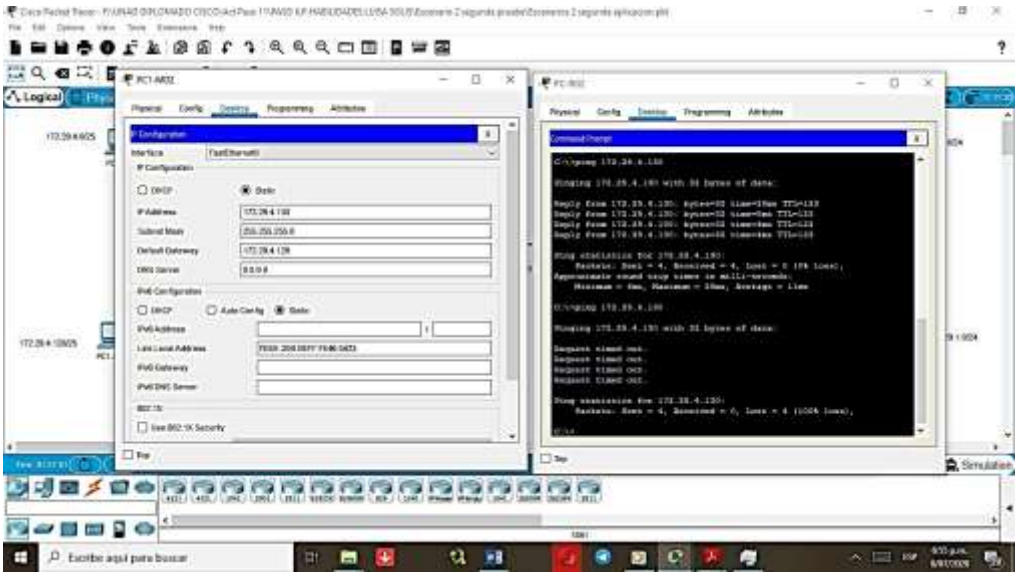
Dispositivos	Configuración
Medellin1	Medellin1(config)#ip access-lis standard LAN-Medellin1 Medellin1(config-std-nacl)#permit 172.29.4.0 0.0.255.255 Medellin1(config-std-nacl)#exit Medellin1(config)#ip nat inside source list Lan-Medellin1 interface s0/0/0 overload Medellin1(config)#int s0/0/0 Medellin1(config-if)#ip nat outside Medellin1(config-if)#exit Medellin1(config)#int s0/1/0 Medellin1(config-if)#ip nat inside Medellin1(config-if)#exit Medellin1(config)#int s0/1/1 Medellin1(config-if)#ip nat inside Medellin1(config)#int s0/0/1 Medellin1(config-if)#ip nat inside Medellin1(config-if)#exit Medellin1(config)#exit

2.9.3. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Tabla 37. Configuración de NAT en Bogota1

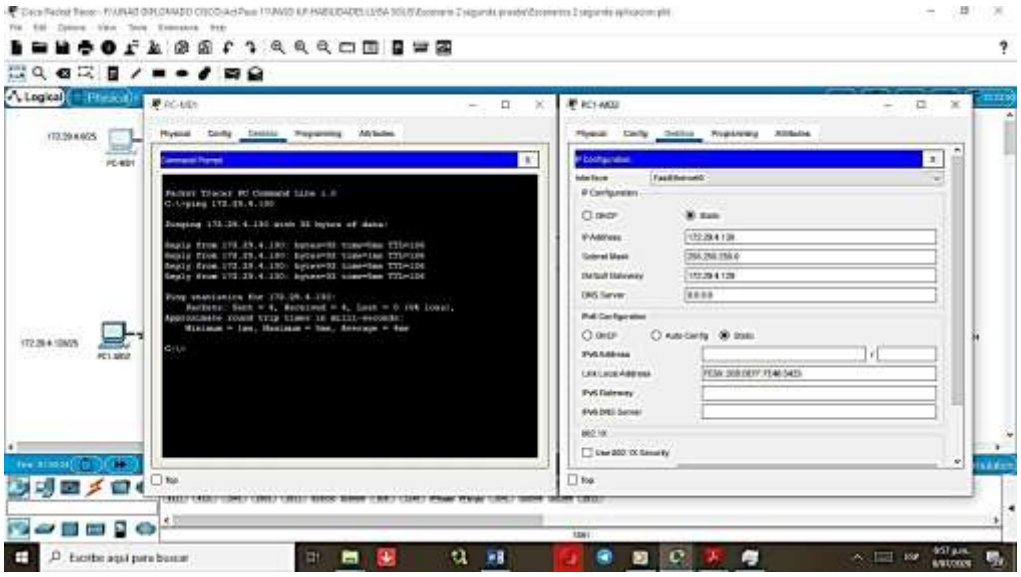
Dispositivos	Configuración
Bogota1	Bogota1(config)#ip access-lis standard LAN-Bogota1 Bogota1(config-std-nacl)#permit 172.29.0.0 0.0.255.255 Bogota1(config-std-nacl)#exit Bogota1(config)#ip nat inside source list LAN-Bogota1 interface s0/0/0 overload Bogota1(config)#int s0/0/0 Bogota1(config-if)#ip nat outside Bogota1(config-if)#exit Bogota1(config)#int s0/0/1 Bogota1(config-if)#ip nat inside Bogota1(config-if)#exit Bogota1(config)#int s0/1/1 Bogota1(config-if)#ip nat inside Bogota1(config-if)#exit Bogota1(config)#int s0/1/0 Bogota1(config-if)#ip nat inside Bogota1(config-if)#exit

Figura. 57 Ping en routers de distintas redes luego de configurar NAT



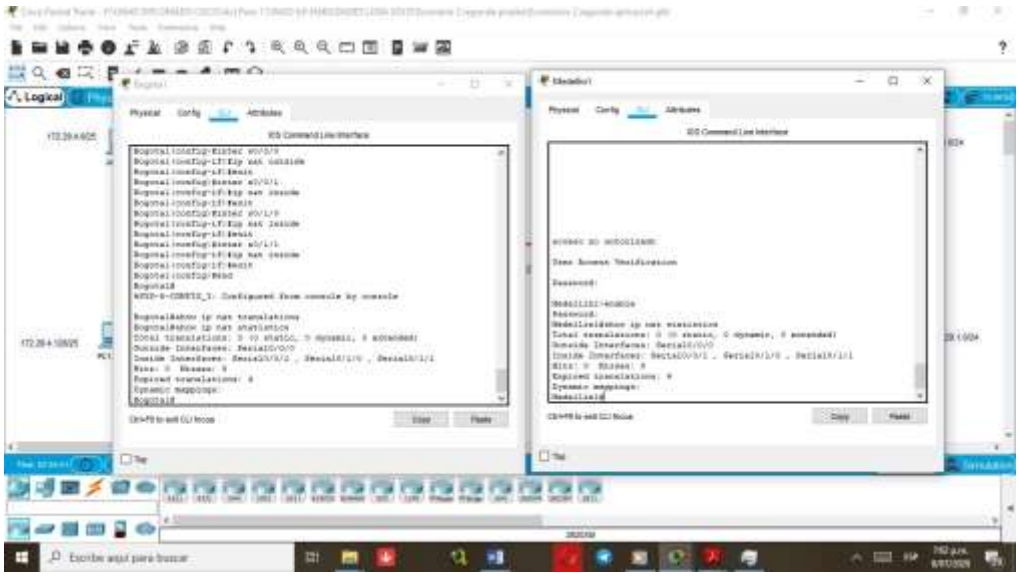
Fuente propia

Figura. 58 Ping entre host de una misma red luego de configurar NAT



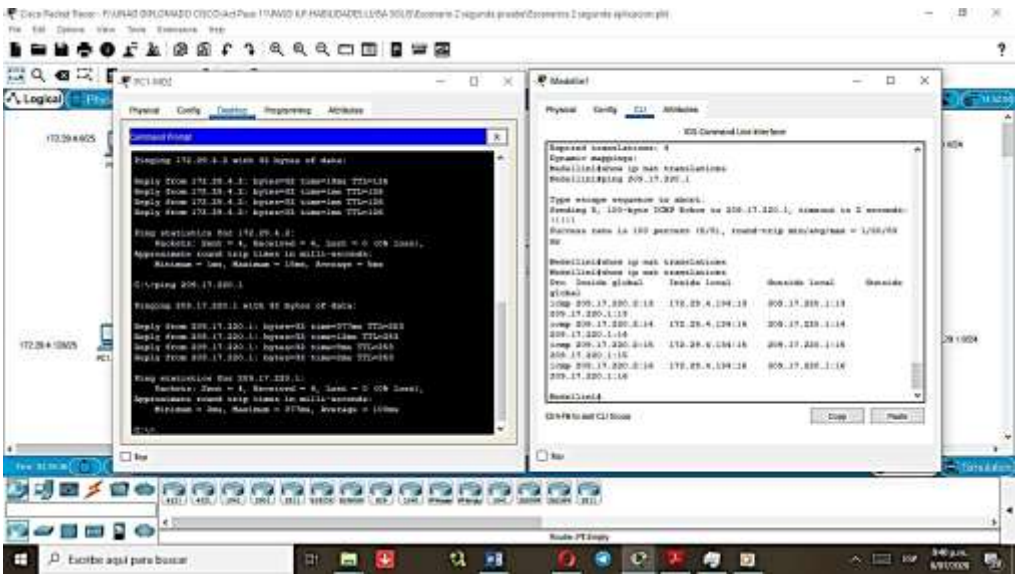
Fuente propia

Figura. 59 Comando show ip nat statistics



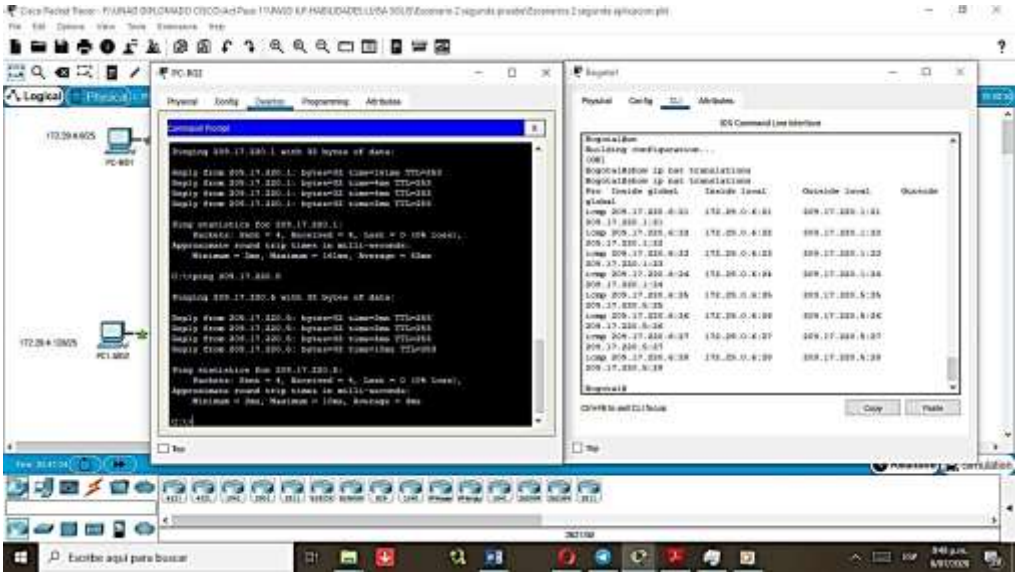
El comando show ip nat statistics permite ver la cantidad de traducciones activas, parámetros de configuración de NAT, cantidad de direcciones en el conjunto y la cantidad asignada.

Figura. 60 Verificar funcionamiento de NAT en Medellin



Fuente propia

Figura. 61 Verificar funcionamiento de NAT en Bogota



Fuente propia

2.10. Parte 7: Configuración del servicio DHCP.

2.10.1. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

Tabla 38. Configurar DHCP en Medellin

Dispositivos	Configuración
Medellin2	Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5 Medellin2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132 Medellin2(config)#ip dhcp pool Medellin2-LAN1 Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.1 Medellin2(dhcp-config)#domain-name lan1.cali.com Medellin2(dhcp-config)#exit Medellin2(dhcp-config)#ip dhcp pool Medellin3 Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128 Medellin2(dhcp-config)#default-router 172.29.4.129 Medellin2(dhcp-config)#dns-server 8.8.8.8 Medellin2(dhcp-config)#exit

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

Tabla 39. Habilitar el paso de broadcast en Medellin3

Dispositivos	Configuración
Medellin3	Medellin3(config)#inter g0/0 Medellin3(config-if)#ip helper-address 172.29.6.5 Medellin3(config-if)#exit

2.10.3. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes LAN

Tabla 40.Configuración de servidor DHCP de Bogota2

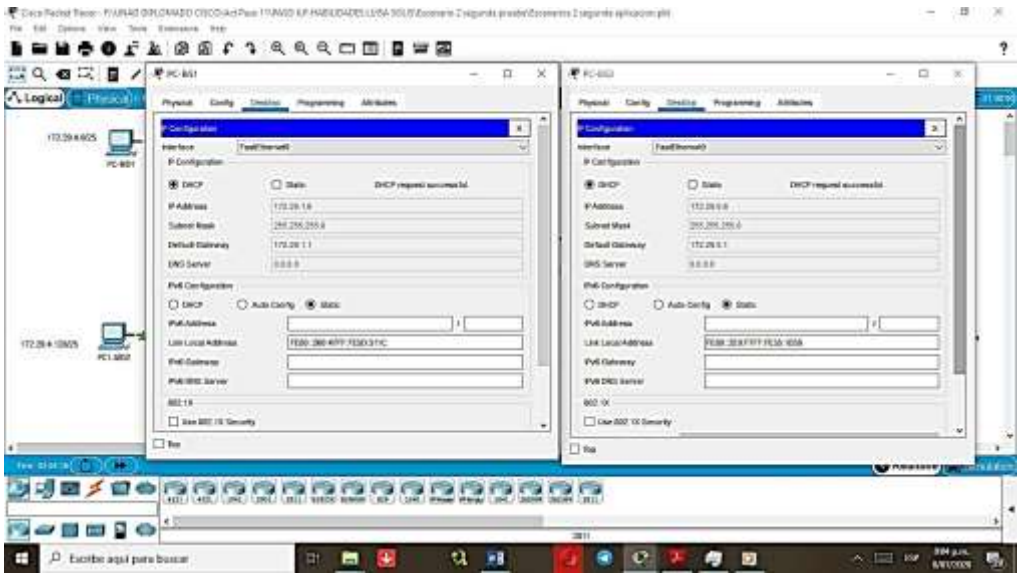
Dispositivos	Configuración
Bogota2	Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5 Bogota2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5 Bogota2(config)#ip dhcp pool Bogota2 Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.1.1 Bogota2(dhcp-config)#ip dhcp pool Bogota3 Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.0.1 Bogota2(config)# ip dhcp excluded-address 172.29.1.1 172.29.1.5 Bogota2(config)# ip dhcp excluded-address 172.29.0.1 172.29.0.5 Bogota2(config)#ip dhcp pool Bogota2 Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.1.1 Bogota2(dhcp-config)#ip dhcp pool Bogota3 Bogota2(dhcp-config)#network 172.29.0.0 255.255.255.0 Bogota2(dhcp-config)#default-router 172.29.0.1 Bogota2(dhcp-config)#exit

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

Tabla 41.Habilitar el paso de broadcast en Bogota3

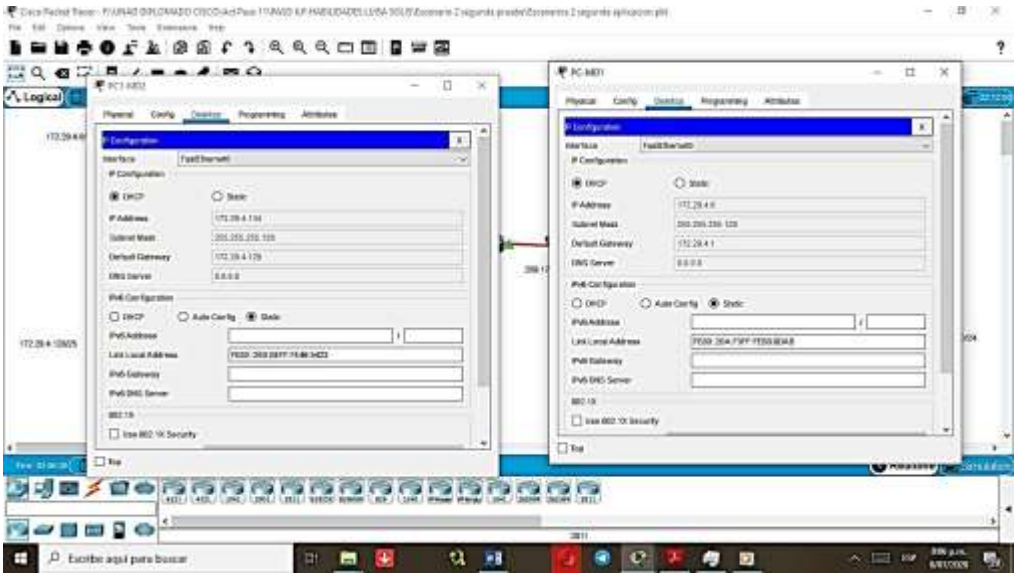
Dispositivos	Configuración
Bogota3	Bogota3(config)#inter g0/0 Bogota3(config-if)#ip helper-address 172.29.3.13 Bogota3(config-if)#

Figura. 62 Verificación de funcionamiento de DHCP en Bogota



Fuente propia

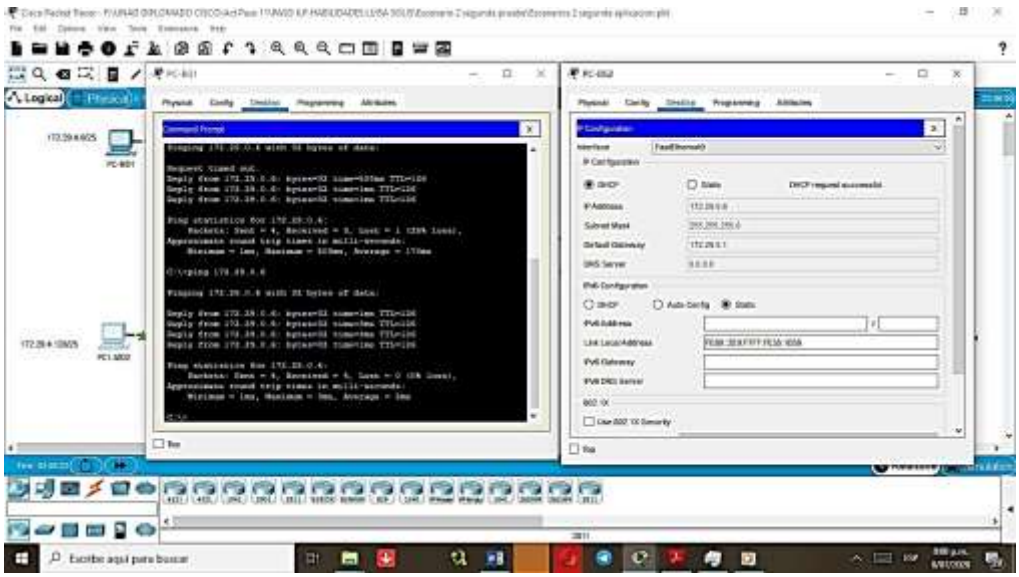
Figura. 63.Verificación de funcionamiento de DHCP en Medellín



Fuente propia

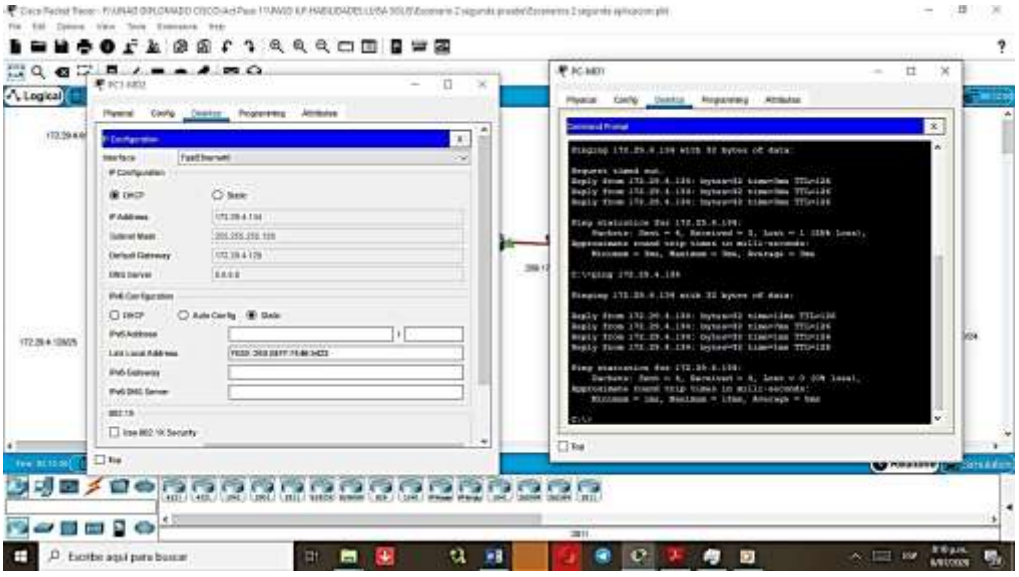
2.10.5. Comprobar ping entre los host de una misma red

Figura. 64 Ping entre host de una misma red- Bogota



Fuente propia

Figura. 65 Ping entre host de una misma red-Medellin



Fuente propia

2.10.6. Comprobación de conectividad

Figura. 66. Ping entre host de la red Medellin

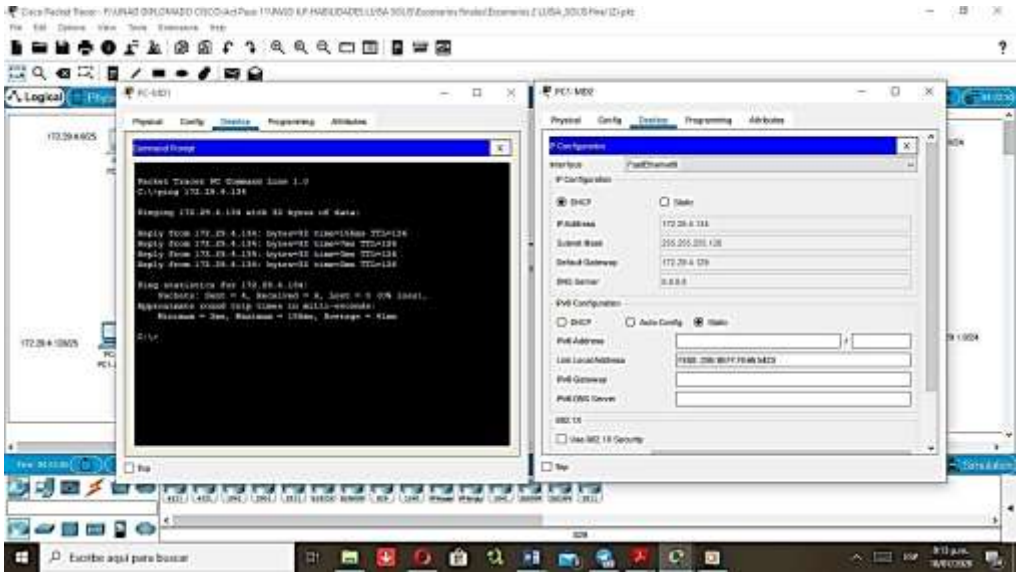
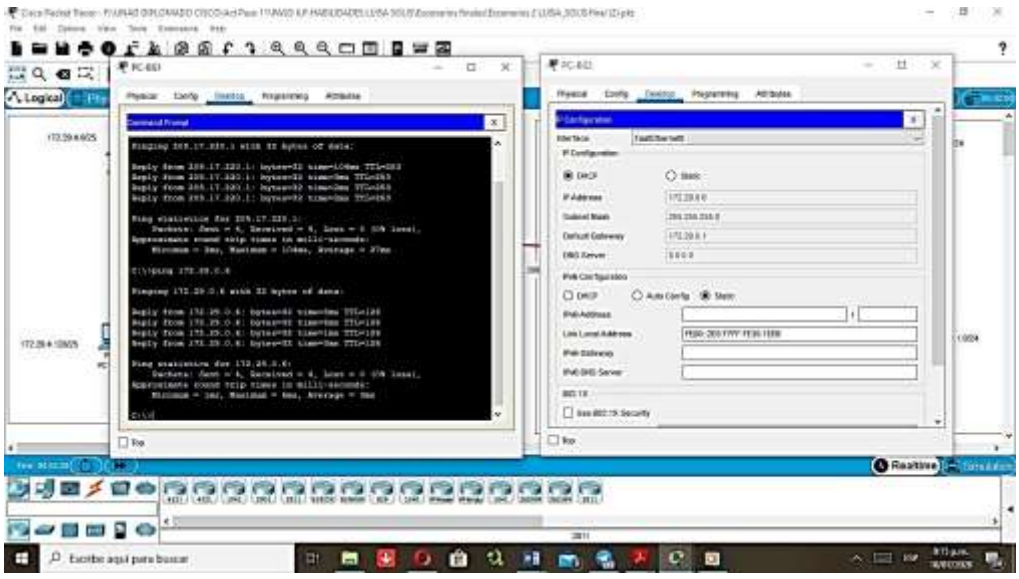
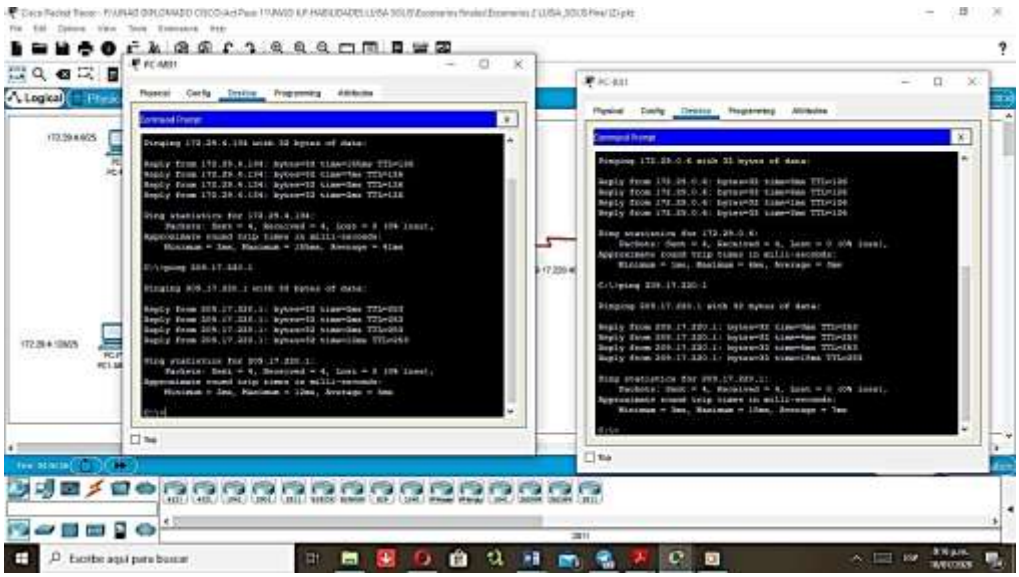


Figura. 67. Ping entre host de la red Bogota



Fuente propia

Figura. 68. Ping de PC-BG1 y PCMD-1 hacia ISP



Fuente propia

CONCLUSIONES

Para concluir con el desarrollo del presente documento se pueden resaltar que uno de los aspectos que fue posible identificar, es el hecho de que efectivamente una de las ventajas de los protocolos RIP y OSPF, es la sencillez de implementación, a través del llamado o anuncio de network conectadas o adyacentes a cada router, de igual manera RIP v2 soporta una creación de subredes permitiendo la administración virtual de espacios de trabajos configurados en las redes internas divididos en secciones, ambos protocolos soportan procesos de autenticación amplios, que permiten garantizar la seguridad de la red; ambos protocolos se basan en la definición de la mejor ruta para su proceso de routing, teniendo en cuenta el número de saltos o el menor recorrido para la transmisión de paquetes y ambos usan métricas para el cálculo de esta ruta; RIP hace uso de los saltos, como ya se decía y en OSPF esta métrica se denomina cost, aunque este último, configurado en el escenario 2, a diferencia del configurado en el escenario 1, tiene en cuenta variables como la congestión en los enlaces y el ancho de banda, difieren en este proceso, pues RIP únicamente se basa en el número de saltos, se podría decir que OSPF en este aspecto es un poco más avanzado, porque analizándolo bien, si solo se tienen en cuenta el número de saltos, como es el caso de RIP v2, pero no se tienen en cuenta métricas como el ancho de banda y la congestión en los enlaces, se puede incurrir en la demora al remitir los paquetes de datos, pues aunque una ruta se caracterice por ser el paso más corto, si hay cogestión y/o poco ancho de banda, puede verse afectado el funcionamiento óptimo de envío de información.

NAT proporciona el ahorro de direcciones IP4 en una red, proporciona una buena seguridad, ya que los dispositivos que se conecten a internet mediante NAT no son visibles en el exterior, su visibilidad mientras esté conectado el cliente, es casi nula o totalmente nula, pero tiene como desventaja que no todos los protocolos son compatibles con esta configuración

BIBLIOGRAFIA

WALTON, Alex “Configuración del Protocolo RIP”. {En línea}. {2020} disponible en: (https://ccnadesdecero.es/configuracion-del-protocolo-rip/)

ROSALES, Delfi “Seguridad y redes, Configuración de NTP con Autenticacion en un Router Cisco”. {En línea}. {30 de abril de 2015} disponible en: (https://delfirosales.blogspot.com/2015/10/configuracion-de-ntp-con-autenticacion_58.html)

Networking y tecnología en español ,“Networking y tecnología en español, NTP: Configurando tu router como servidor NTP”. {En línea}. {2 de abril de 2012} disponible en: (https://networkkings-es.blogspot.com/2012/06/ntp-configurando-tu-router-como.html)

Cisco, “Configure las configuraciones del Tiempo del sistema en un conmutador a través del comando line interface(cli)”. {En línea}. {14 de febrero de 2020} disponible en: (https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5584-configure-system-time-settings-on-a-switch-through-the-comma.html)

MACHADO MADRID, Richard Andrés “Data Networks, Enrutamiento dinámico RIP”. {En línea}. {2011} disponible en: (http://gestnetwork.blogspot.com/p/enrutamiento-dinamico-rip.html)

ANEXOS

Link para descargar archivos de pkt

https://drive.google.com/drive/folders/1WLeoH40oxEboFObeE4HEhSMiR3QSvrOh?usp=sharin g