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

JESÚS ALBERTO PULIDO SILVA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
JULIO 2020

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

JESÚS ALBERTO PULIDO SILVA

TUTOR
GUSTAVO ADOLFO RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
JULIO 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

El primer escenario del trabajo final nos evidenciara el desarrollo de diferentes ejercicios simulados en la herramienta Packet Tracer, donde nos permite establecer escenarios LAN/WAN.

Nos mostrara minuciosamente algunas actividades como, conexiones, Comandos, validaciones de los Equipos entre otros propuestos en la guía.

El desarrollo de las practicas nos lleva a utilizar cada uno de los conocimientos practicados en laboratorios anteriores por separados e implementarlos en un solo avance para aplicar las destrezas cosechas en el transcurso del aprendizaje, como los son la propagación OSPF con sus ventajas, la aplicación de DCHP, el control de seguridad PPP y las Comandos NAT, por supuesto no podemos dejar un lado las Comandos más básicas de enrutamiento y organización de la estructura de la topología propuesta en la guía.

Cabe destacar que el aprendizaje continuo y el material implementado en el consolidado de la practica final, es causa ferviente del trabajo duro para lograr implementar cada uno de los objetivos propuestos en la aplicación de cada uno de los escenarios propuestos y sus respectivos desafíos como lo son la implementación de la topología inicial, la configuración OSPF, la autenticación pap y chap y las Comandos NAT, destacando esta última como una de mayor valor en el concepto de aprendiza de distribución de las redes dentro de una compañía y su respectiva navegación por la red implementada y disponible para sus uso.

ABSTRACT

The first scenario of the final work will show us the development of different simulated exercises in the Packet Tracer tool, where it allows us to establish LAN / WAN scenarios.

It will show us in detail some activities such as, connections, Commands, Equipment validations among others proposed in the guide.

The development of the practices leads us to use each of the knowledge practiced in previous laboratories separately and implement them in a single advance to apply the skills learned in the course of learning, such as OSPF propagation with its advantages, the application of DCHP, PPP security control and NAT Commands, of course we cannot leave aside the most basic routing Commands and organization of the structure of the topology proposed in the guide.

It should be noted that continuous learning and the material implemented in the consolidation of the final practice, is a fervent cause of hard work to achieve the implementation of each of the proposed objectives in the application of each of the proposed scenarios and their respective challenges, such as the implementation of the initial topology, the OSPF configuration, the pap and chap authentication and the NAT Commands, highlighting the latter as one of greater value in the concept of learning how to distribute networks within a company and their respective web browsing implemented and available for use.

OBJETIVOS

Objetivo General:

Comprender los conceptos de redes LAN/WAN de acuerdo a los ejercicios propuestos en la guía que se evidenciarán y se simularán mediante la herramienta escogida en este caso Packet Tracer.

Objetivos específicos:

- Configurar los equipos en la herramienta de simulación.
- Validar conectividad y restricciones de los equipos.
- Evidenciar en cada ejercicio propuesto los resultados obtenidos en cada desarrollo.

DESARROLLO DE LA ACTIVIDAD

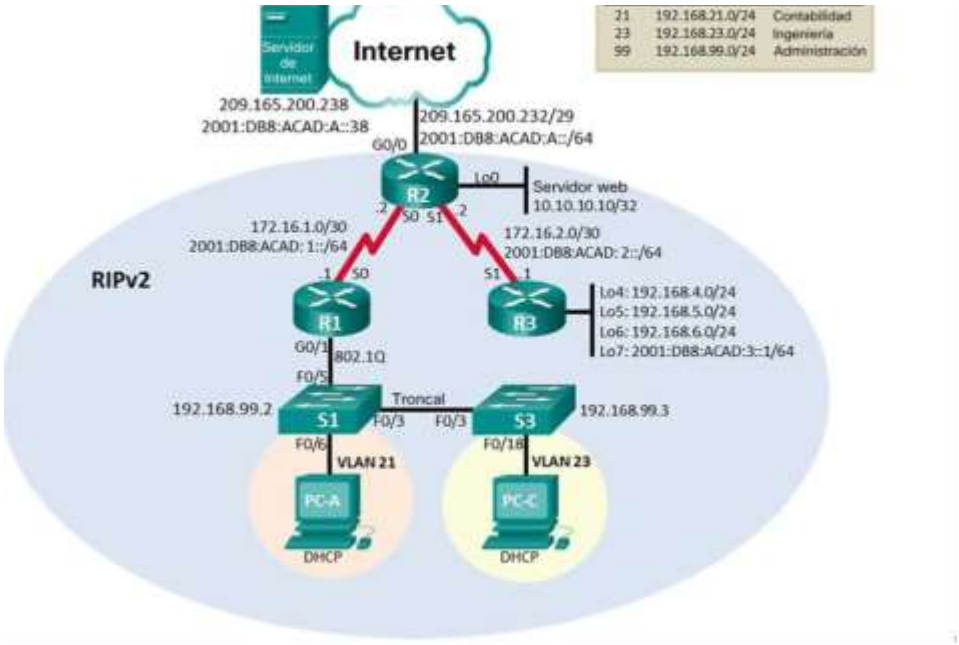
ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de

control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

Figura 1 Topología de red



Parte 1: Inicializar Equipos

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

Elimine las Comandos de inicio y vuelva a cargar los Equipos.
Se evidencia la eliminación de Comandos mediante el comando delete y reinicios de los equipos con el comando reload.

Tabla 1 Inicializar Equipos RyS

TAREA	COMANDO DE IOS
Eliminar el archivo startup-config de todos los routers	Router›ena Router# erase startup-config
Volver a cargar todos los routers	Router›ena Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch ›ena Switch# erase startup-config Switch# delete flash:vlan.dat
Volver a cargar ambos switches	Switch ›ena Switch# reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show vlan

Parte 2: Configurar los parámetros básicos de los Equipos

Paso 1: Configurar la computadora de Internet

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

Se evidencia la configuración del dispositivo servidor-internet para que simule el acceso a la nube.

Tabla 2 Configuración de parámetros básicos de los Equipos

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Se configura base del R1, con sus respectivos nombres, contraseña, mensaje de inicio motd, interfaz serial para conexión con R2 y se configuran rutas predeterminadas para que queden asociadas a la interfaz s0/0/0

Tabla 3 Configuración R1

TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Router›ena Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router›ena Router#conf t Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1›ena R1#conf t R1(config)#enable secret class
Contraseña de acceso a la consola	R1›ena R1#conf t R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1›ena R1#conf t R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1›ena R1#conf t R1(config)#service password-encryption
Mensaje MOTD	R1›ena R1#conf t R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1›ena R1#conf t R1(config)#interface s0/0/0 R1(config-if)#Description Conexion R1 y R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shu
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

En la anterior tabla se evidencia la configuración base del R2, se configura nombre, contraseña, mensaje motd, configuración de interfaz g0/0 y se configuran rutas predeterminadas para que queden asociadas a la interfaz g0/0

Tabla 4 Configuración R2

ELEMENTOO TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Router›ena Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router›ena Router#conf t Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2›ena R2#conf t R2(config)#enable secret class
Contraseña de acceso a la consola	R2›ena R2#conf t R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2›ena R2#conf t R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2›ena R2#conf t R2(config)#service password-encryption
Habilitar el servidor HTTP	R2›ena R2#conf t R2(config)#ip http server

Mensaje MOTD	R2›ena R2#conf t R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2›ena R2#conf t R2(config)#interface s0/0/0 R2(config-if)#description Conexion entre R2 y R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shu
Interfaz S0/0/1	R2›ena R2#conf t R2(config)#interface s0/0/1 R2(config-if)#description Conexion R2 y R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shu
Interfaz G0/0 (simulación de Internet)	R2›ena R2#conf t R2(config)#interface g0/0 R2(config-if)#description Conexion R2 a Internet R2(config-if)#ip address 209.165.200.232 255.255.255.248 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shu

Interfaz loopback 0 (servidor web simulado)	R2›ena R2#conf t R2(config)#interface loopback 0 R2(config-if)#description interface Loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit R2(config)#interface g0/1 R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shu
Ruta predeterminada	R2›ena R2#conf t R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2›ena R2#conf t R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Se evidencia la configuración base del R3, tales como nombre, contraseña, mensaje inicial motd, interfaces loopback, interfaz serial conexión con R2 y rutas predeterminadas para asociar a la int s0/0/1.y configuraciones de seguridad en texto planos con mensaje de restricción y encriptación junto con las interfaces virtuales según las topología propuesta.

Tabla 5 Configuración R3

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Router›ena Router#conf t Router(config)#no ip domain-lookup
Nombre del router	Router›ena Router#conf t Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3›ena R3#conf t 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 vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #se prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)# description conexion R2 y R3 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shu

Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.0 255.255.255.0 R3(config-if)#exit R3(config)#
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.0 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.0 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En la siguiente tabla se evidencia la configuración de router S1 tales como Nombre, contraseñas de incios de sesión, consola, vty, mensaje motd de autenticación fallida y cifrado de contraseñas

Tabla 6 Configuración S1

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del Switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado.#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:
En la siguiente tabla se evidencia la configuración de router S3 tales como Nombre, contraseñas de exec, consola, vty, mensaje motd y cifrado de contraseñas.

Tabla 7 Configuración S3

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado.#

Paso 7: Verificar la conectividad de la red

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:
En la siguiente tabla se evidencia las pruebas conectividad exitosas mediante ping desde R1 hacia R2, y de R2 a R3.

Tabla 8 Verificar conectividad de red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/13 ms
R2	R3, S0/0/1	172.16.2.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/13 ms
PC de Internet	Gateway predeterminado		

Figura 2 Ping desde R1

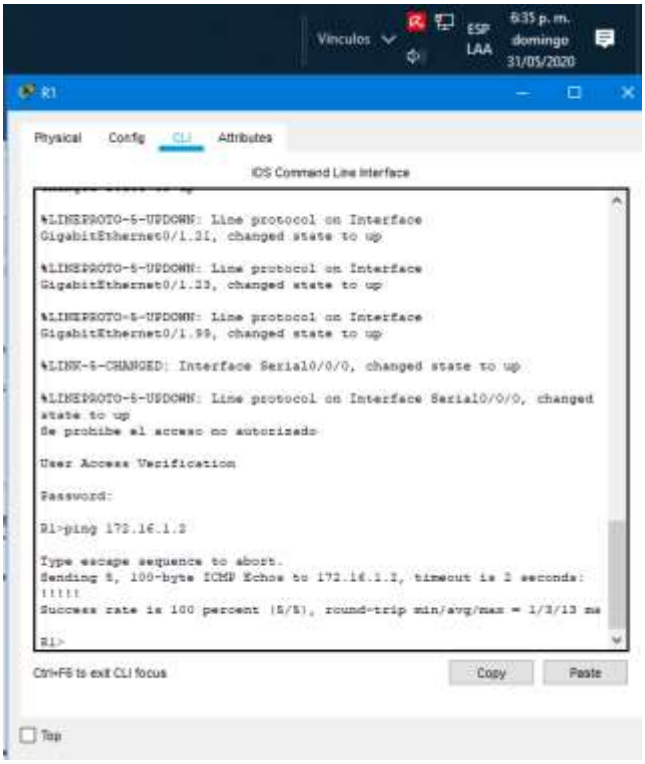
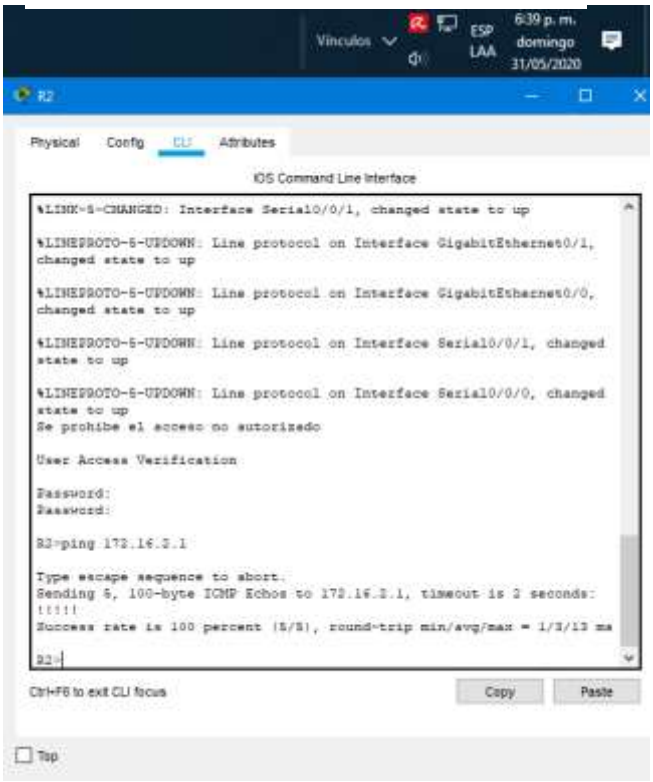


Figura 3 Ping desde R2



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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En la siguiente tabla se evidencia la creación de base de datos de VLAN 21-23- 99, y la configuración de los mismos con sus nombres, direccionamiento, Gateway predeterminado, la interfaz f0/5 puerto troncal y los demás en modo de acceso teniendo en cuenta la descripción de la tabla 9 en la columna elemento o tarea de configuración.

Tabla 9 Configuración Seguridad S1

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear la base de datos de VLAN	S1›ena S1#conf t S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1›ena S1#conf t S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shu

Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1›ena S1#conf t S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1›ena S1#conf t S1(config)#interface 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)#interface range f0/1, f0/2, f0/4, f0/7- 24, g0/1-2 S1(config-if-range)#switchport mode Access
Asignar F0/6 a la VLAN 21	S1›ena S1#conf t S1(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)#interface range f0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#interface f0/4 S1(config-if)#shutdown S1(config-if)#interface range f0/7-24 S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar Seguridad S3

La configuración del S3 incluye las siguientes tareas:
En la siguiente tabla se evidencia en el S3 la creación de la base de datos de las VLAN 21-23-99, y se configura nombres, direccionamiento de la vlan 99 y el puerto f0/3 como troncal, los demás puertos se dejan en modo de acceso y los que no están en uso se apagan.

Tabla 10 Configuración Seguridad S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23 (se modifica teniendo en cuenta que en grafico aparece vlan 23)	S3(config)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar Seguridad R1

Las tareas de configuración para R1 incluyen las siguientes:

En la siguiente tabla se evidencia la configuración de las sub-interfaces en la interfaz g0/1 para las redes 21- 23-99 mediante encapsulamiento dot1q.

Tabla 11 Configuración Seguridad R1

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN de Contabilidad 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)#interface g0/1.23 R1(config-subif)#description LAN de Ingenieria 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)#interface g0/1.99 R1(config-subif)#description LAN de Administracion 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)#interface g0/1 R1(config-if)#no shu

Paso 4: Verificar la conectividad de la red

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

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

Se realizan pruebas de conectividad mediante ping: Desde S1 hacia R1 vlan99, Desde S3 hacia R1 vlan99, Desde S1 hacia R1 vlan21, Desde S3 hacia R1 vlan23, Desde S3 hacia R1 vlan23. Y todas fueron satisfactorias.

Tabla 12 Verificación de conectividad en la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S3	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S1	R1, dirección VLAN 21	192.168.21.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S3	R1, dirección VLAN 23	192.168.23.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

Figura 4 Ping S1 a R1 vlan99

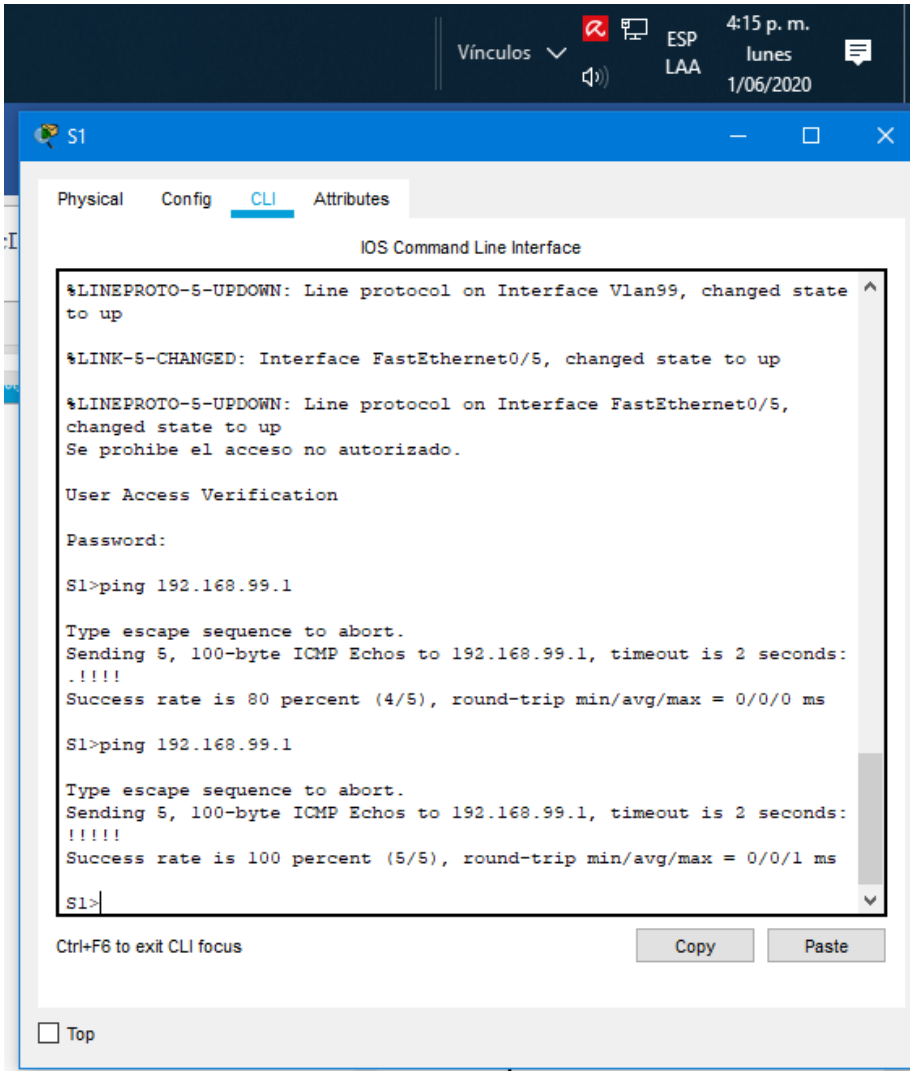


Figura 5 Ping S3 a R1 vlan99

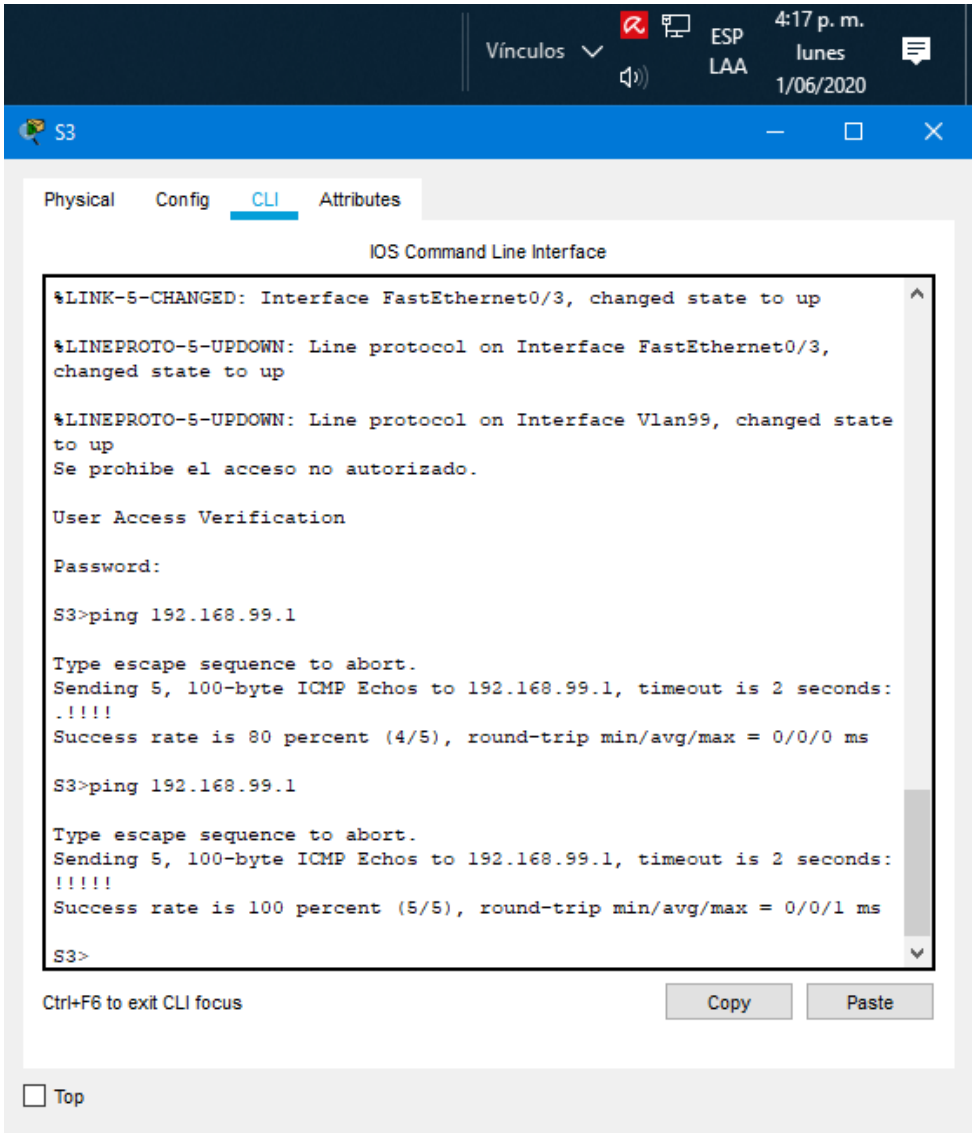


Figura 6 Ping S1 a R1 vlan21

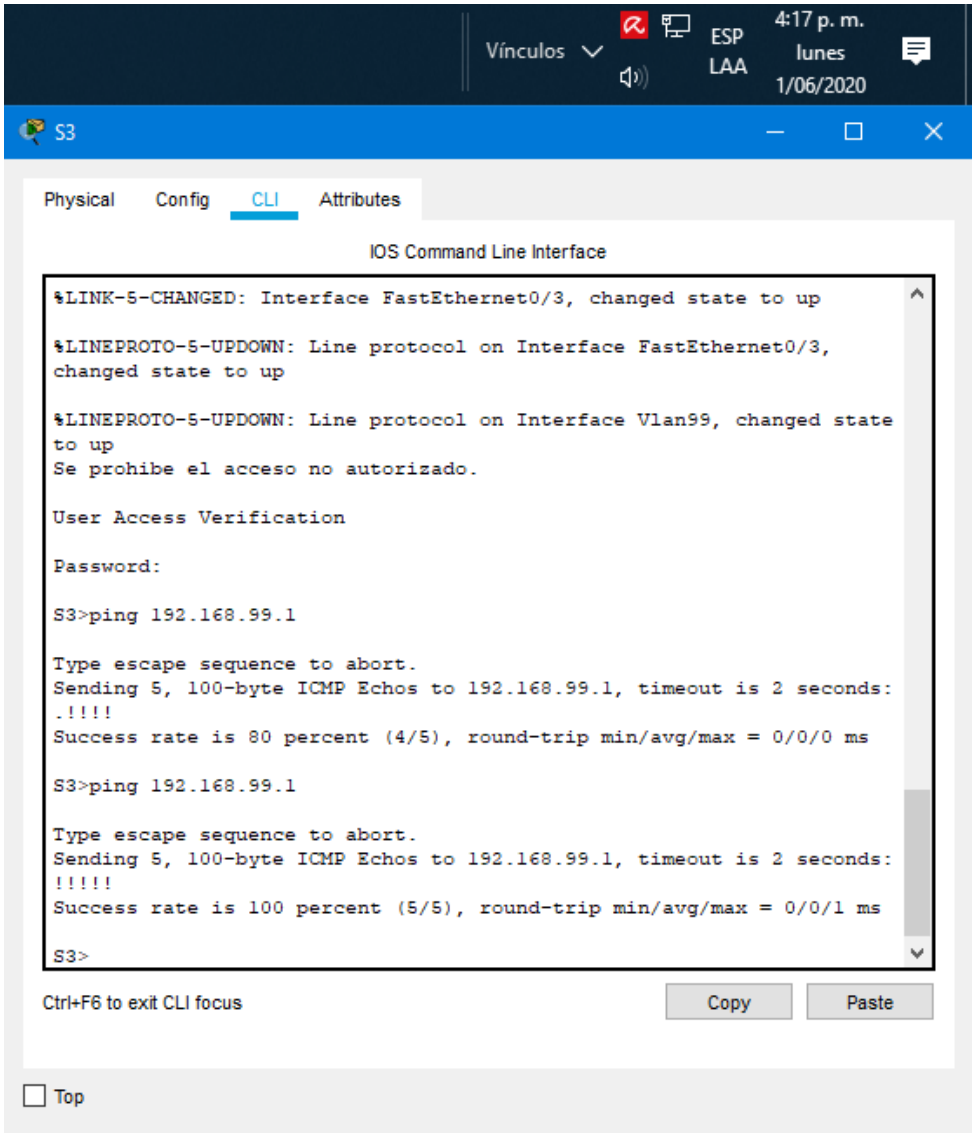
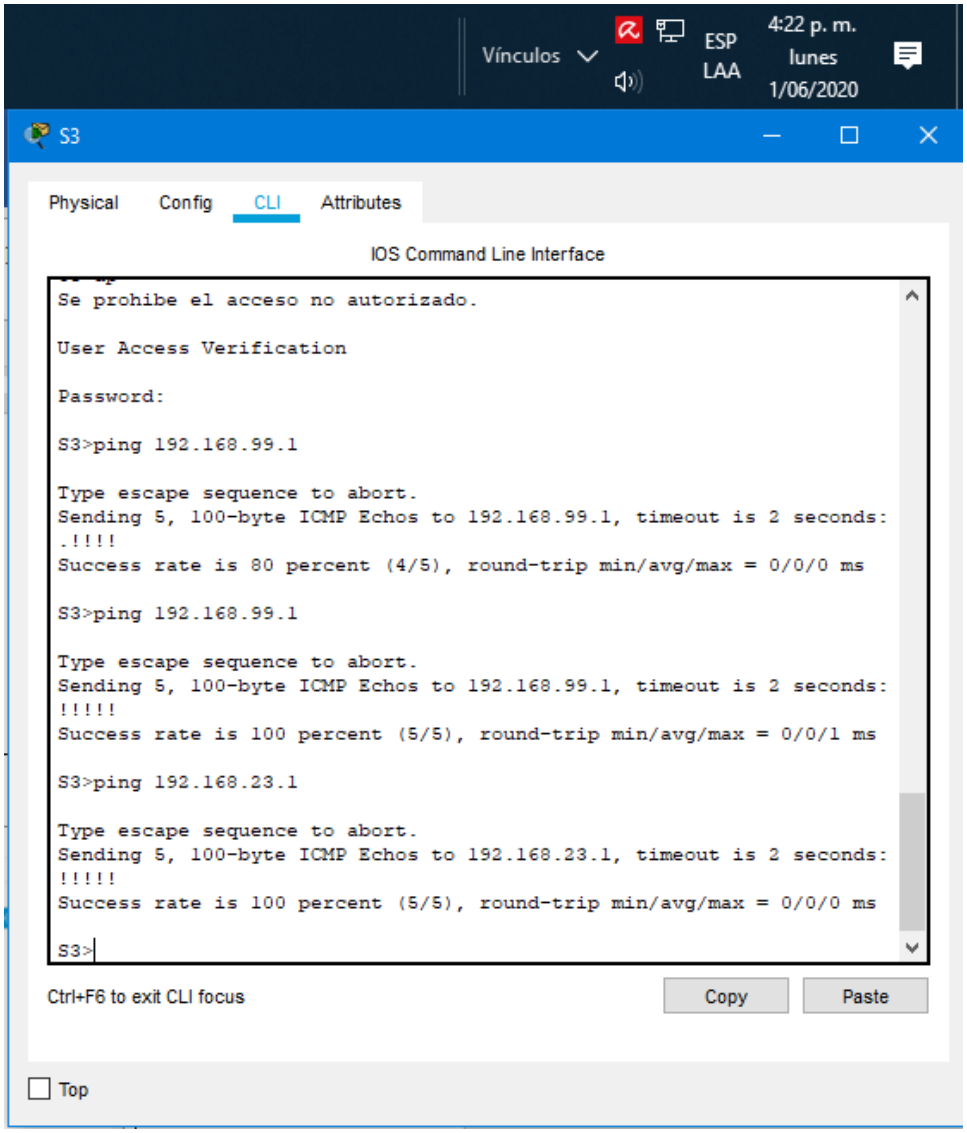


Figura 7 Ping S3 A R1 vlan23



Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:
En la siguiente tabla se evidencia la configuración de RIP en R1, y se ingresan las redes 21,23,99 y 172.16.1.0. y al final se desactiva la sumarización automática.

Tabla 13 Configurar RIPv2 en el R1

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar RIP versión 2	R1›ena R1#conf t R1(config)#router rip R1(config-router)#ver 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network192.168.21.0 R1(config-router)#network192.168.23.0 R1(config-router)#network192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface s0/0/0 R1(config-router)#passive-interface gig0/1
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:
En la siguiente tabla se evidencia la configuración de RIP versión 2 para el R2, y se agregan las redes 172.16.1.0, 172.16.2.0 y la 10.10.10.0

Tabla 14 Configurar RIPv2 en el R2

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar RIP versión 2	R2›ena R2#conf t R2(config)#router rip R2(config-router)#version 2
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
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#no passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

En la siguiente tabla se evidencia la configuración RIP ver 2 en el R3 y se anuncian las redes IPv4, se establecen las loockback como pasivas y se desactiva la sumarización automática.

Tabla 15 Configurar RIPv3 en el R2

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar RIP versión 2	R3›ena R3#conf t R3(config)#router rip R3(config-router)#ver 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 loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:
En la siguiente tabla se evidencia la verificación de los enrutamientos mediante RIP configuración en el equipo R1.

Tabla 16 Verificación del 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?	R1›sh ip protocols
¿Qué comando muestra solo las rutas RIP?	R1#sh ip route R
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#debug ip rip R1#no debug ip rip

Figura 8 sh ip protocols en R1

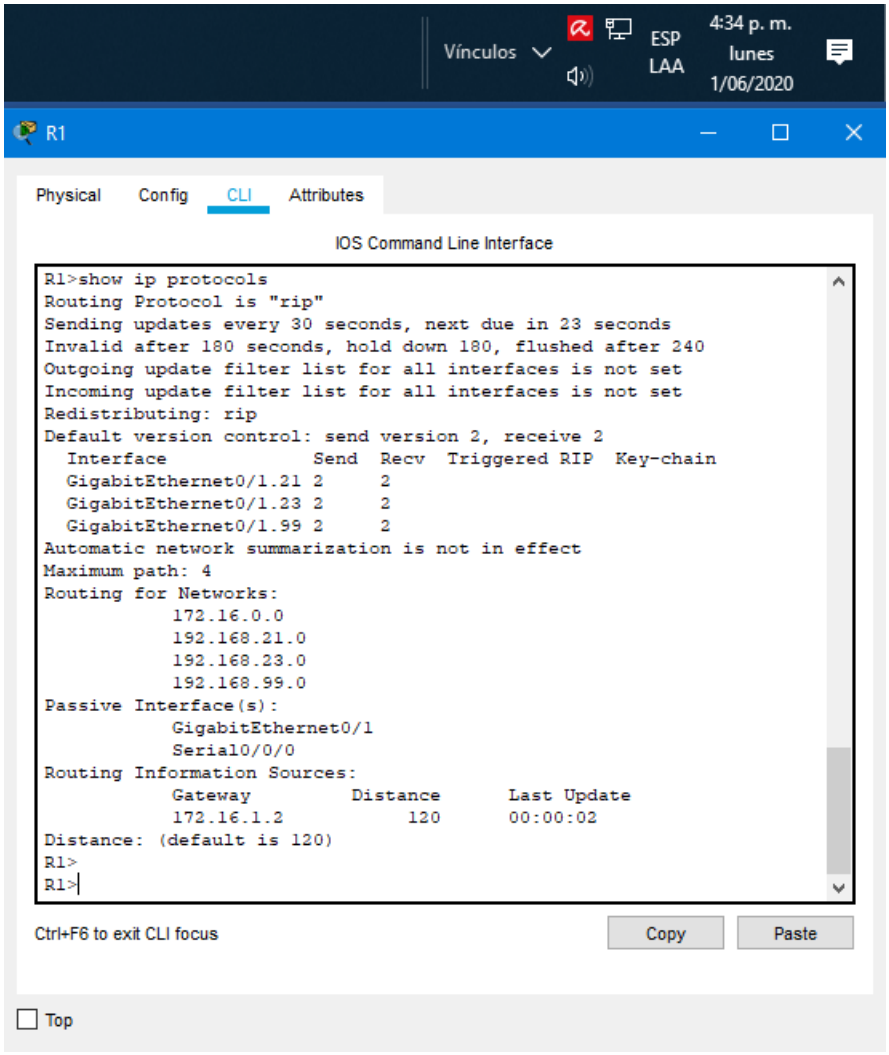


Figura 9 sh ip route R en R1

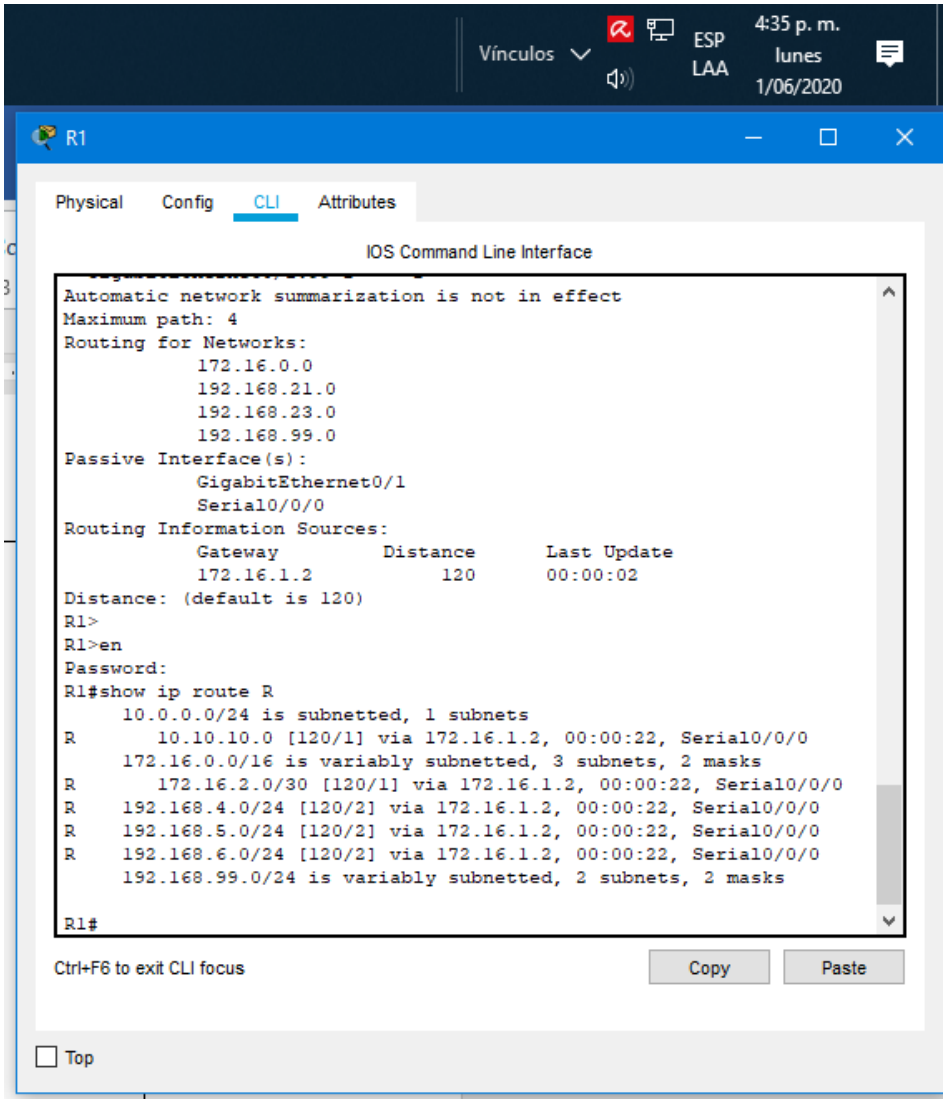
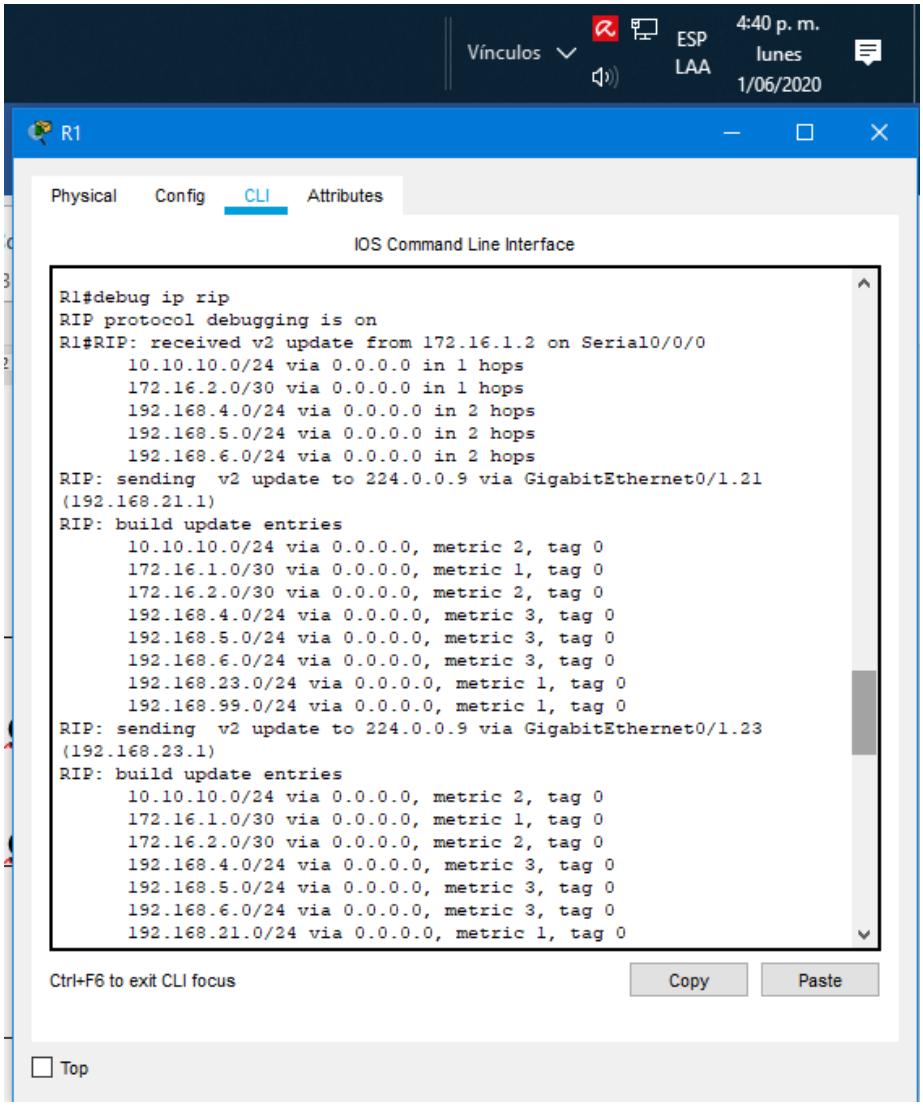


Figura 10 debug ip rip



Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:
En la siguiente tabla se evidencia la configuración en R1 el servicio DHCP para que delegue direccionamiento a las redes 21-23 y se configura reserva DHCP de las primeras 20 IPs para cada red.

Tabla 17 Configuración R1 como servidor de DHCP

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Reservar las primeras 20 direcciones IP en la VLAN 21 para Comandos estáticas	R1›ena R1#conf t 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 Comandos estáticas	R1›ena R1#conf t 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)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

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

La configuración del R2 incluye las siguientes tareas:
En la siguiente tabla se evidencia la configuración de NAT estática para que desde internet el servidor 10.10.10.10 sea visible con la IP 209.165.200.238.

Tabla 18 Configuración de la NAT en R2

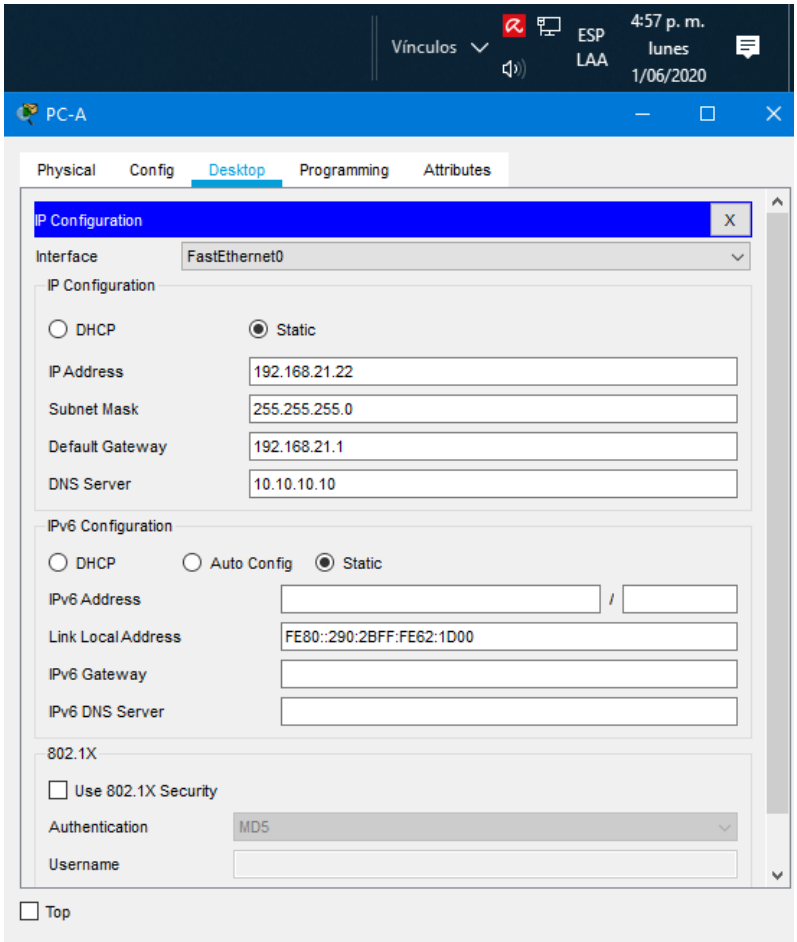
ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Crear una base de datos local con una cuenta de usuario	R2›ena R2#conf t R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No se puede configurar este comando en el simulador packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No se puede configurar este comando en el simulador packet tracer
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238 R2(config)#interface g0/0 R2(config-if)#ip nat out R2(config-if)#ip nat outside R2(config-if)#interface g0/1 R2(config-if)#ip nat inside
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 R3(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R3(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R3(config)#access-list 1 permit 192.168.6.1 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las Comandos 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.

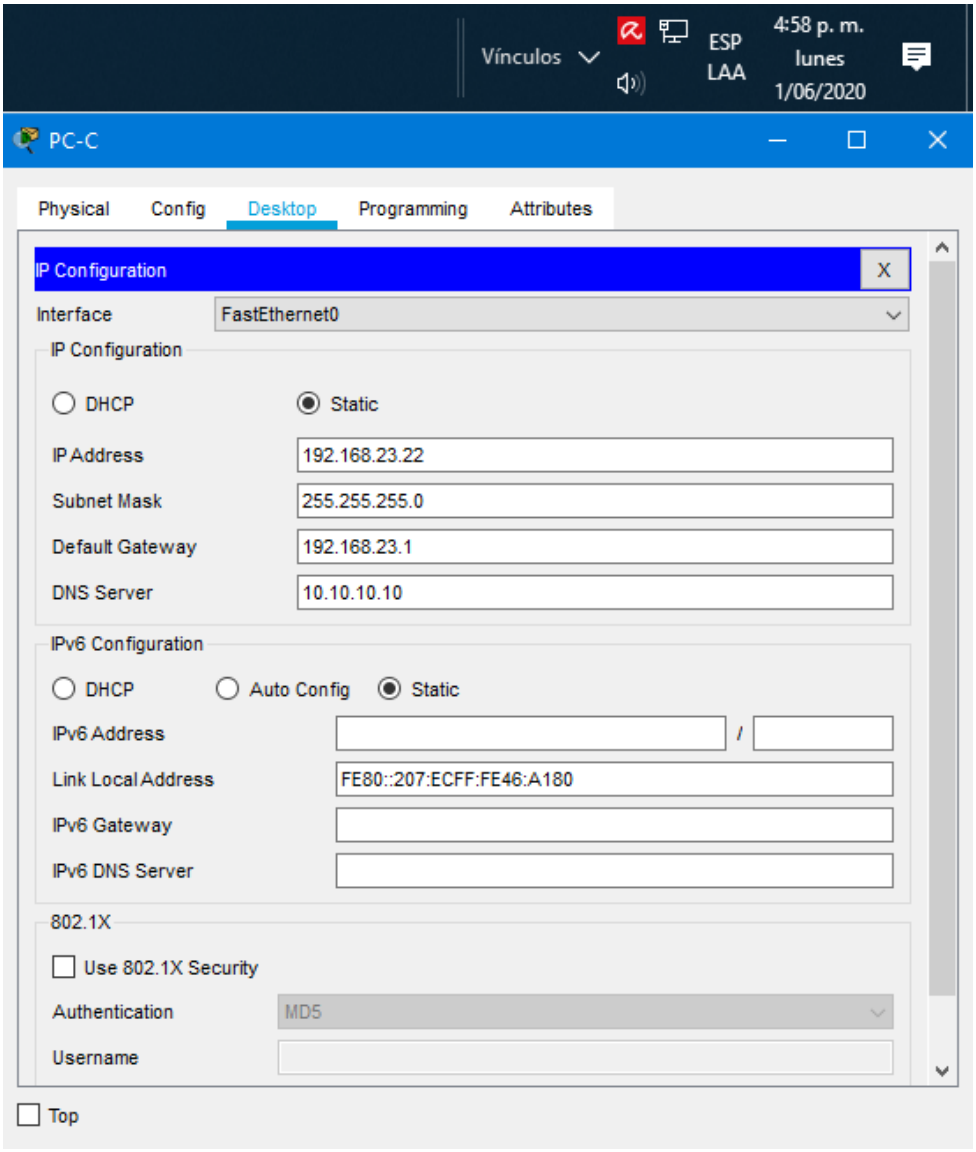
- Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 11 Configuración PC-A



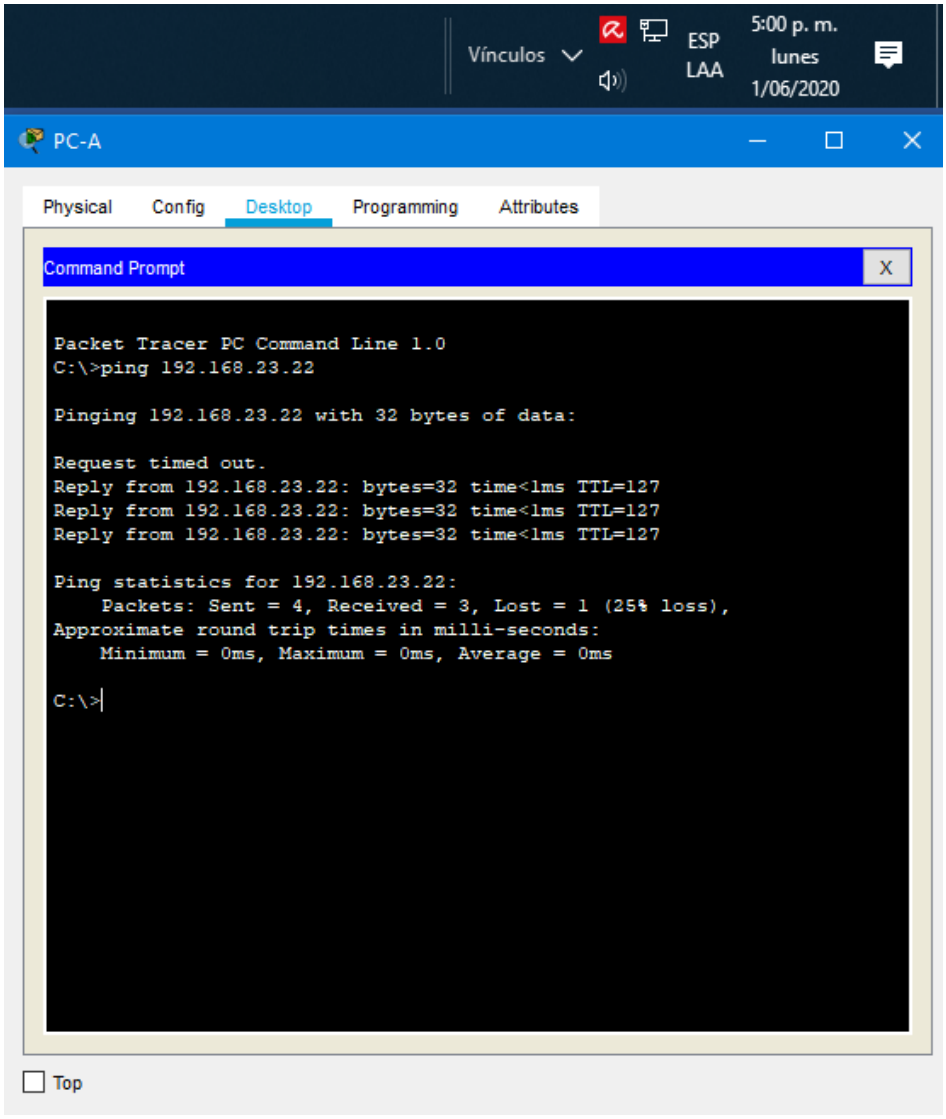
- Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Figura 12 Configuración PC-C



- Verificar que la PC-A pueda hacer ping a la PC- C
  Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 13 Ping PC-A y PC-C



- Utilizar un navegadorweb en la computadora de Internet para acceder al servidor web (c) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 14 Servidor Web 209.165.200.238

Parte 6: Configurar NTP

En la siguiente tabla se evidencia la configuración de NTP en R1 Y R2. Entre ellas el ajuste de la fecha y hora,R2 como maestro NTP. R1 como cliente NTP, se actualizan los calendarios periódicamente con hora NTP, y por ultimo verificamos los comandos con show ntp associations.

Tabla 19 Configuración NTP

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 mar 2016 R2#show clock
Configure R2 como un maestro NTP.	R2(config)# ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1# show ntp associations

Parte 7: Configurar y verificar las listas de control de acceso (ACL) Restringir el acceso a las líneas VTY en el R2

Paso 1: Restringir el acceso a las líneas VTY en el R2

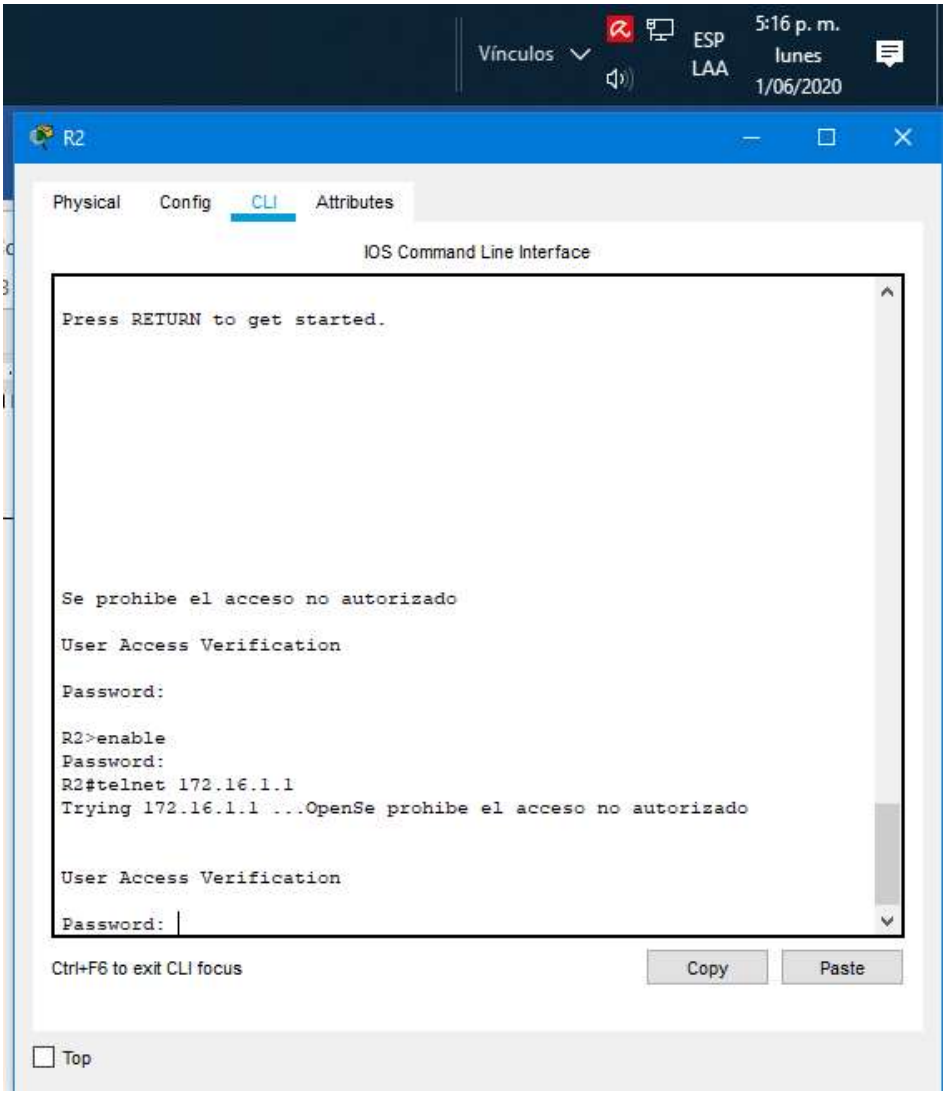
En la siguiente tabla se evidencia la configuración de lista de acceso ACL con nombre a las líneas vty, permitir acceso por telnet a vty y verificación ACL en R2 que las Comandos terminen exitosas.

Tabla 20 Configuración 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(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 15
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R2#telnet 172.16.1.1

- Verificar que la ACL funcione como se espera

Figura 15 Verificación ACL



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

En la siguiente tabla se evidencia el manejo del comando CLI en los Equipos para verificar coincidencias recibidas, reestablecer contadores, mostrar ACL, mostrar y eliminar traducciones NAT.

Tabla 21 Access list.

DESCRIPCIÓN DEL COMANDO	ENTRADA DEL ESTUDIANTE (COMANDO)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2(config)#interface s0/0/0 R2(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	R2#sh ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Figura 16 Show access-Lists

Figura 17 Clear Acces

Figura 18 sh ip nat translations

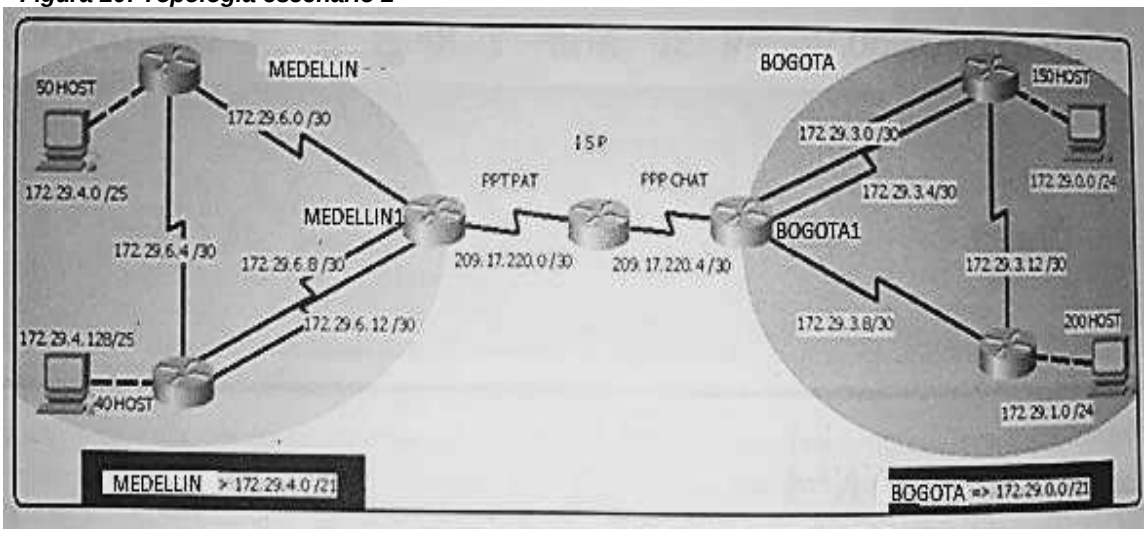
Figura 19 clear ip nat translation

DESARROLLO 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 Equipos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología de red

Figura 20: Topología 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. Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

A continuación, configuraremos los parámetros básicos en los equipos como la asignación de nombres, desactivar DNS para desactivar la traducción de nombres a dirección del dispositivo y la configuración de seguridad por inicio de sesión, asignamos contraseñas en texto plano con el comando password para no utilizar encriptación, esta configuración la utilizamos para todos los equipos de la tabla 22.

Tabla 22 Configuración inicial Router

Equipos	Comandos
ISP	Router(config)#hostname ISP ISP(config)#no ip domain-lookup 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)#exit ISP(config)#service password-encryption ISP(config)#banner motd #Prohibido el acceso no autorizado#

BOGOTA1	Router(config)#hostname BOGOTA1 BOGOTA1(config)#no ip domain-lookup 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)#linevty 0 15 BOGOTA1(config-line)#password cisco BOGOTA1(config-line)#login BOGOTA1(config-line)#exit BOGOTA1(config)#service password-encryption BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado#
BOGOTA2	Router(config)#hostname BOGOTA2 BOGOTA2(config)#no ip domain-lookup 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)#exit BOGOTA2(config)#service password-encryption BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado#
BOGOTA3	Router(config)#hostname BOGOTA3 BOGOTA3(config)#no ip domain-lookup 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)#exit BOGOTA3(config)#service password-encryption

	BOGOTA3(config)#banner motd #prohibido el acceso no autorizado#
MEDELLIN1	Router(config)#hostname MEDELLIN1 MEDELLIN1(config)#no ip domain-lookup 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)#exit MEDELLIN1(config)#service password-encryption MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado#
MEDELLIN2	Router(config)#hostname MEDELLIN2 MEDELLIN2(config)#no ip domain-lookup 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)#exit MEDELLIN2(config)#service password-encryption MEDELLIN2(config)#banner motd #prohibido el acceso no autorizado#
MEDELLIN3	Router(config)#hostname MEDELLIN3 MEDELLIN3(config)#no ip domain-lookup 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)#exit MEDELLIN3(config)#service password-encryption MEDELLIN3(config)#banner motd #prohibido el acceso no autorizado.#

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

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

Se realiza configuración de todas las interfaces para establecer conexión entre todos los routers mediante el direccionamiento ip y clock rate permitiendo la sincronización de la comunicación de los routers entre si.

Tabla 23 Comandos físicas

Equipos	Comandos
Router ISP	ISP(config)#interface s0/0/0 ISP(config-if)#ip address 209.17.220.1 255.255.255.252 ISP(config-if)#description Conexion ISP a MEDELLIN1 ISP(config-if)#clock rate 128000 ISP(config-if)#no shu ISP(config-if)#interface s0/0/1 ISP(config-if)#ip address 209.17.220.5 255.255.255.252 ISP(config-if)#description Conexion ISP a BOGOTA1 ISP(config-if)#clock rate 128000 ISP(config-if)#no shu

BOGOTA1	BOGOTA1(config)#interface s0/0/0 BOGOTA1(config-if)#description BOGOTA1 a ISP BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252 BOGOTA1(config-if)#no shu BOGOTA1(config-if)#interface s0/1/1 BOGOTA1(config-if)#description conexion BOGOTA1 a BOGOTA3 BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shu BOGOTA1(config-if)#interface s0/0/1 BOGOTA1(config-if)#description conexion Bogota1.0 a Bogota2.0 BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shu BOGOTA1(config-if)#interface s0/1/0 BOGOTA1(config-if)#description conexion Bogota1.1 a Bogota2.1 BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252 BOGOTA1(config-if)#clock rate 128000 BOGOTA1(config-if)#no shu
BOGOTA2	BOGOTA2(config)#interface s0/0/0 BOGOTA2(config-if)#description conexion Bogota2.0 a Bogota1.0 BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252 BOGOTA2(config-if)#no shu BOGOTA2(config-if)#interface s0/1/1 BOGOTA2(config-if)#description conexion Bogota2.1 a Bogota 1.1 BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252 BOGOTA2(config-if)#no shu BOGOTA2(config-if)#interface s0/0/1 BOGOTA2(config-if)#description conexion Bogota2 a Bogota3 BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252 BOGOTA2(config-if)#clock rate 128000 BOGOTA2(config-if)#no shu BOGOTA2(config-if)#interface g0/0 BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0 BOGOTA2(config-if)#no shu

BOGOTA3	BOGOTA3(config)#interface s0/0/0 BOGOTA3(config-if)#description conexion Bogota3 A Bogota1 BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252 BOGOTA3(config-if)#no shu BOGOTA3(config-if)#interface s0/0/1 BOGOTA3(config-if)#description conexion Bogota3 a Bogota2 BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252 BOGOTA3(config-if)#no shu BOGOTA3(config-if)#interface g0/0 BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0 BOGOTA3(config-if)#no shu
MEDELLIN1	MEDELLIN1(config)#interface s0/0/0 MEDELLIN1(config-if)#description MEDLLIN1 a ISP MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252 MEDELLIN1(config-if)#no shu MEDELLIN1(config-if)#interface s0/1/0 MEDELLIN1(config-if)#description MEDELLIN1 a MEDELLIN2 MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shu MEDELLIN1(config-if)#interface s0/1/1 MEDELLIN1(config-if)#description MEDELLIN1.1 a MEDELLIN3.1 MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shu MEDELLIN1(config-if)#interface s0/0/1 MEDELLIN1(config-if)#description MEDELLIN1.2 a MEDELLIN3.2 MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252 MEDELLIN1(config-if)#clock rate 128000 MEDELLIN1(config-if)#no shu

MEDELLIN 2	MEDELLIN2(config)#interface s0/0/0 MEDELLIN2(config-if)#description MEDELLIN2 a MEDELLIN1 MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252 MEDELLIN2(config-if)#no shu MEDELLIN2(config-if)#interface s0/0/1 MEDELLIN2(config-if)#description MEDELLIN2 a MEDELLIN3 MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252 MEDELLIN2(config-if)#clock rate 128000 MEDELLIN2(config-if)#no shu MEDELLIN2(config-if)#interface g0/0 MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128 MEDELLIN2(config-if)#no shu
MEDELLIN3	MEDELLIN3(config)#interface s0/0/0 MEDELLIN3(config-if)#description MEDELLIN3.1 a MEDELLIN1.1 MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252 MEDELLIN3(config-if)#no shu MEDELLIN3(config-if)#interface s0/0/1 MEDELLIN3(config-if)#description MEDELLIN3 A MEDELIN2 MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252 MEDELLIN3(config-if)#no shu MEDELLIN3(config-if)#interface s0/1/1 MEDELLIN3(config-if)#description MEDELLIN3.2 a MEDELLIN1.2 MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252 MEDELLIN3(config-if)#no shu MEDELLIN3(config-if)#interface g0/0 MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128 MEDELLIN3(config-if)#no shu

Parte 1: Configuración del enrutamiento

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

Se configuran los Equipos BOGOTA1, BOGOTA2, BOGOTA3, MEDELLIN1, MEDELLIN2, MEDELLIN3 utilizando el protocolo de direccionamiento OSPF V2, se declara red principal en cada uno y se desactiva la sintetización de múltiples rutas IP contiguas en una única ruta o sumarización.

Tabla 24 Configuración de enrutamiento

Equipos	Comandos
BOGOTA1	BOGOTA1(config)#router ospf 1 BOGOTA1(config-router)#router-id 4.4.4.4 BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0 BOGOTA1(config-router)#end
BOGOTA2	BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#router 5.5.5.5 BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 0 BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 0 BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0 BOGOTA2(config-router)#end
BOGOTA3	BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#router-id 6.6.6.6 BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0 BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0 BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0 BOGOTA3(config-router)#end
MEDELLIN1	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 MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0 MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0 MEDELLIN1(config-router)#end
MEDELLIN2	MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#router-id 2.2.2.2 MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 0 MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0 MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN2(config-router)#end
MEDELLIN3	MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#router-id 3.3.3.3 MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.255 area 0 MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0 MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0 MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0 MEDELLIN3(config-router)#end

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

Tabla 25 Publicaciones de OSPF

Equipos	Comandos OSPF
MEDELLIN1	MEDELLIN1#configure t MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1 MEDELLIN1(config)#router ospf 1 MEDELLIN1(config-router)#default-information originate MEDELLIN1(config-router)#end
BOGOTA1	BOGOTA1#configure t 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 BOGOTA1(config-router)#end

a. 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 26 Configuración ruta estática ISP

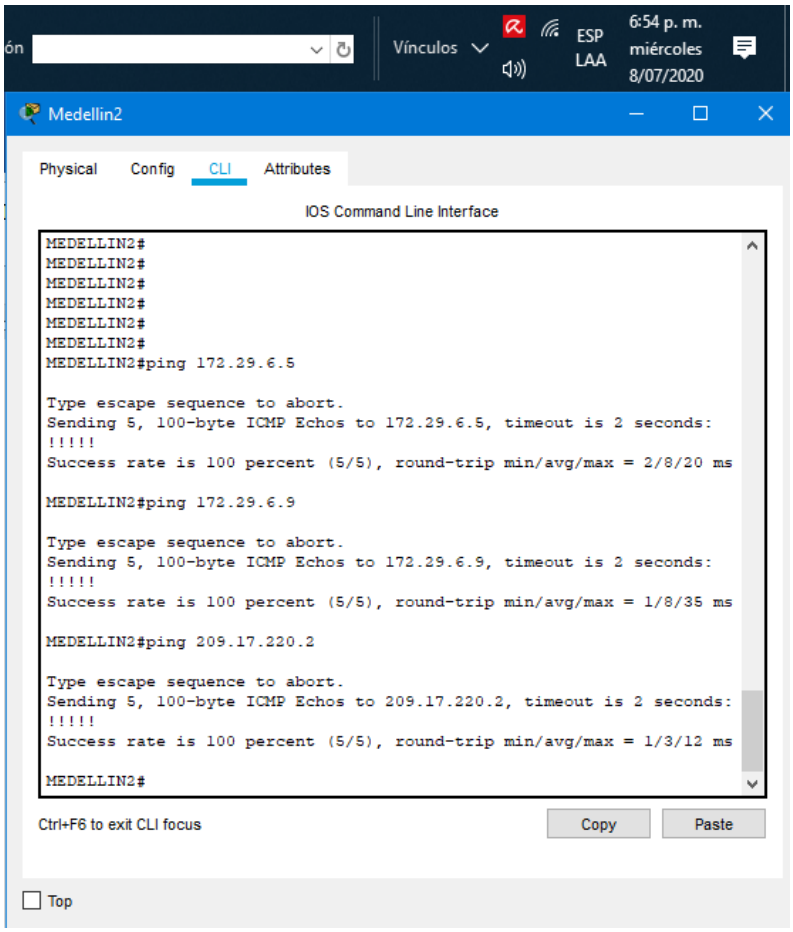
Equipos	Comandos
ISP	ISP#configure t ISP(config)#ip route 172.29.4.0255.255.255.0 ISP(config)#ip route 172.29.0.0255.255.255.0

Parte 2: Tabla de Enrutamiento.

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

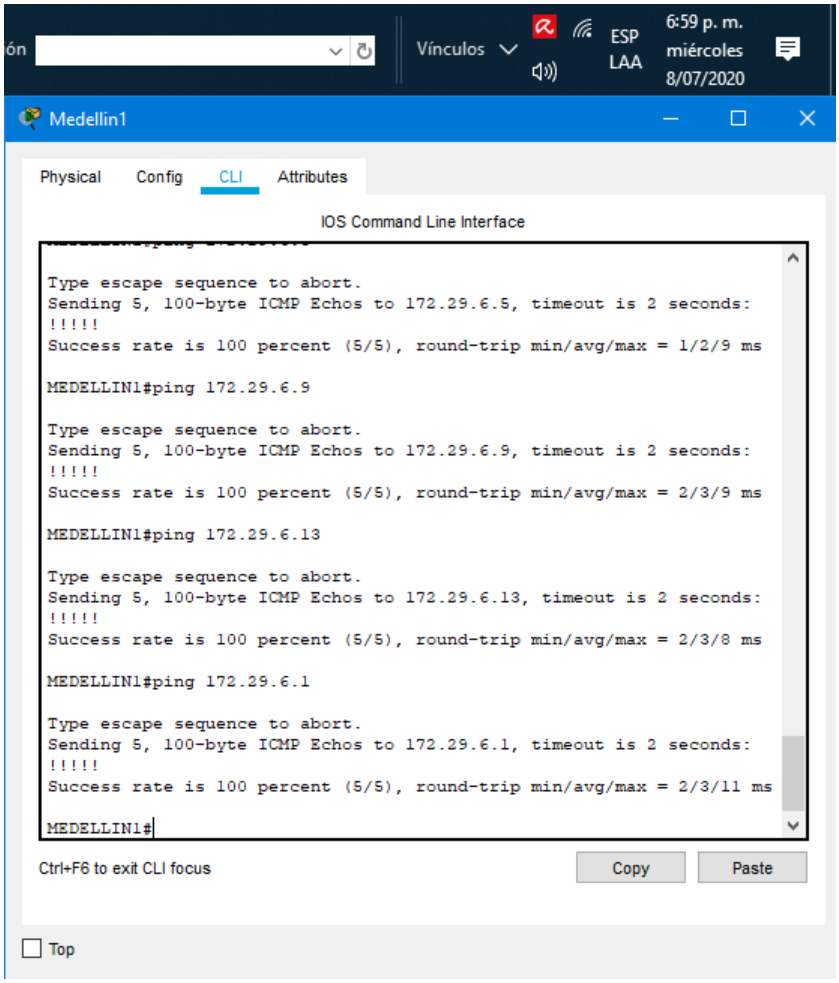
Realizamos pings exitosos desde Medellin2 a MEDELLIN1, MEDELLIN3, IPS con esto confirmamos las conexiones exitosas también podemos utilizar el comando show ip route para ver las directamente conectadas.

Figura 20 Verificación de Enrutamiento MEDELLIN2



- Realizamos pings exitosos de MEDELLIN1 a MEDELLIN2, MEDELLIN3.

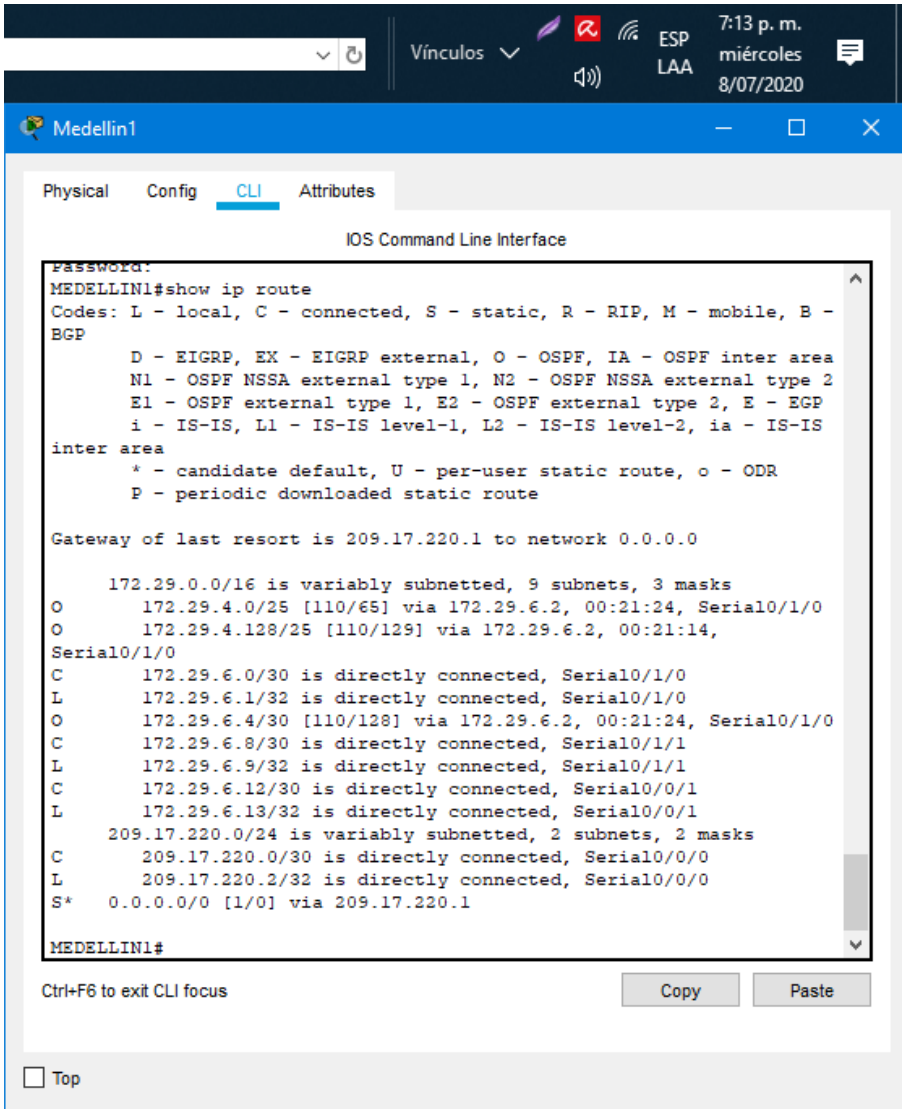
Figura 21 Verificación de Enrutamiento MEDELLIN2



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

Presentan trayectorias al mismo costo y la misma distancia administrativa del destino por lo tanto hay balanceo de carga, el objetivo es verificar que un router utilice varias trayectorias a un destino al reenviar paquetes.

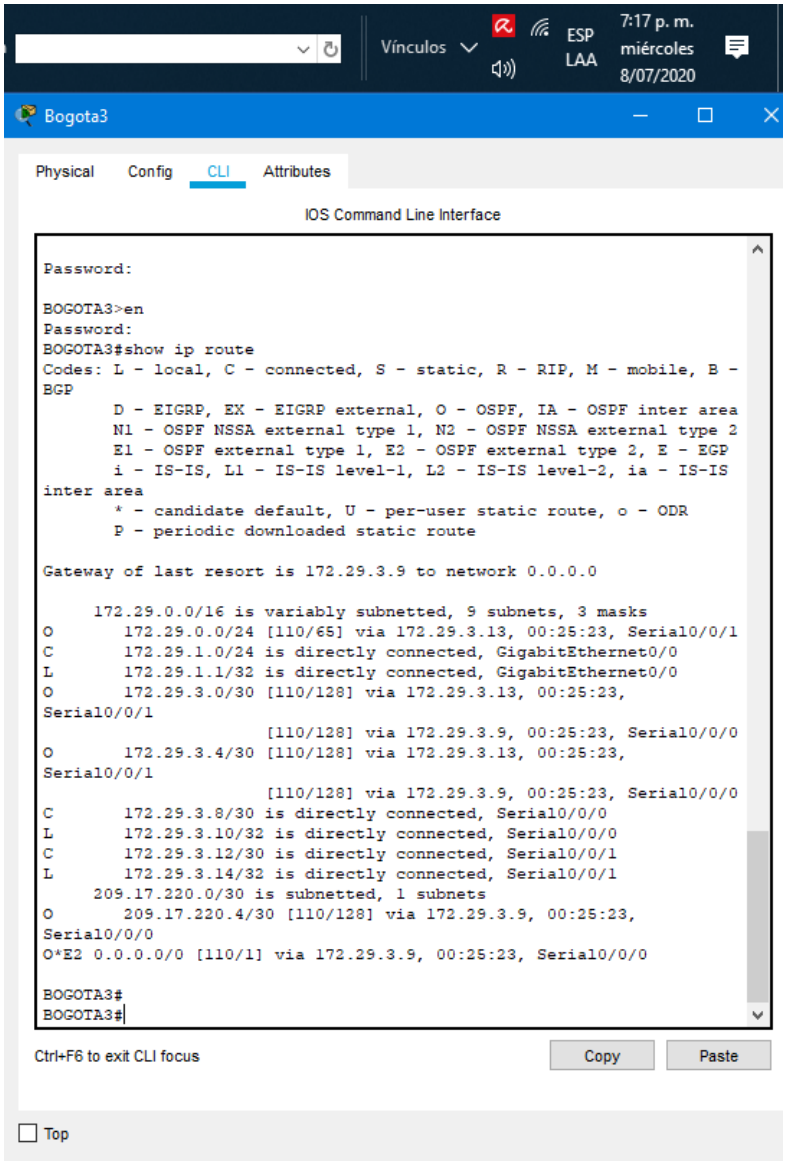
Figura 22 Verificación Balanceo MEDELLIN1



Balanceo Bogota3

Presentan trayectorias al mismo costo y la misma distancia administrativa del destino por lo tanto hay balanceo de carga.

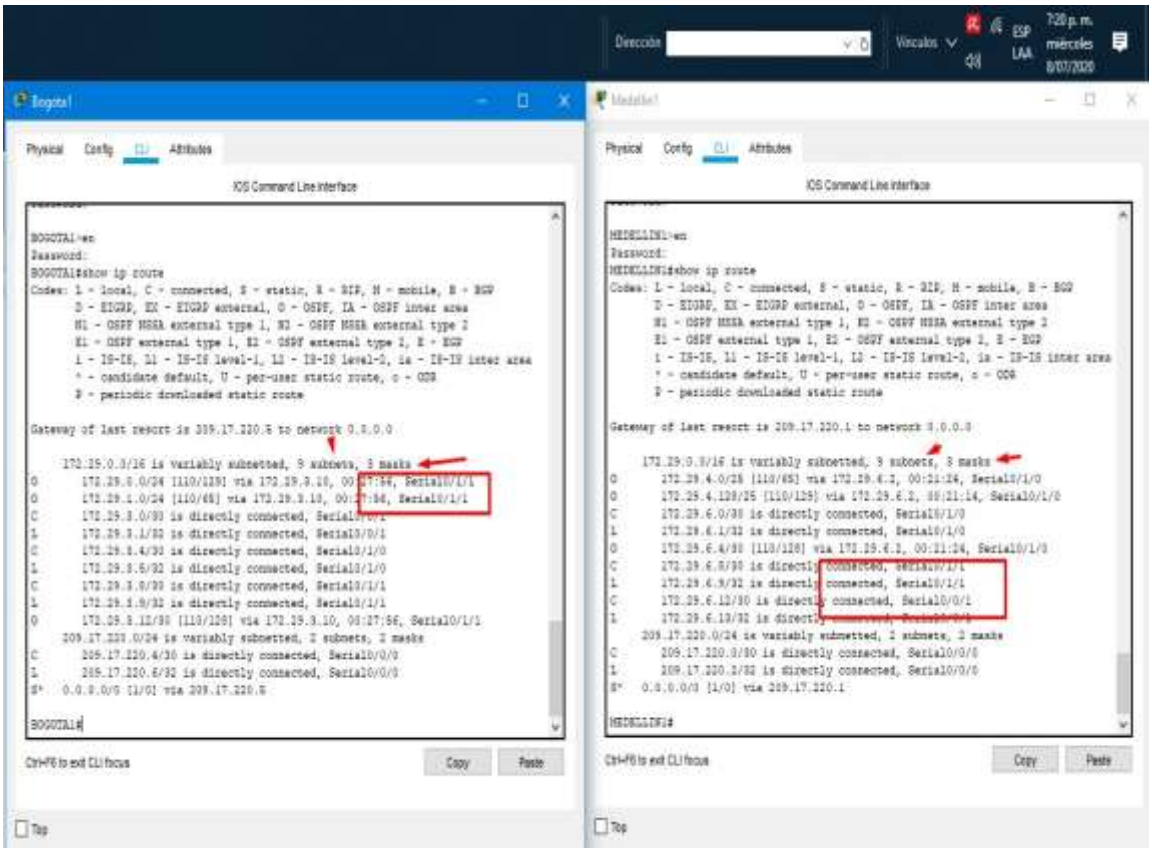
Figura 23 Verificación Balanceo Bogota3



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

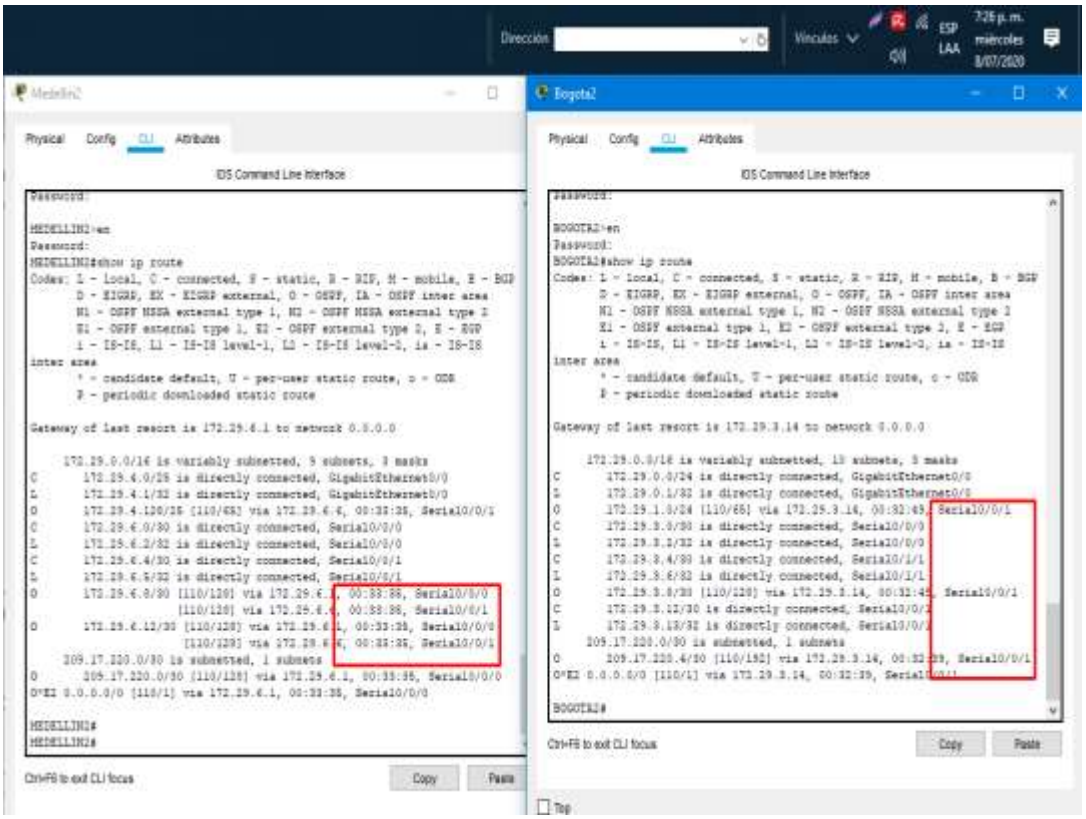
BOGOTA1 Y MEDELLIN1 comprenden cierta similitud por sus rutas de redes.

Figura 24 Similitud Routers BOGOTA1MEDELLIN1



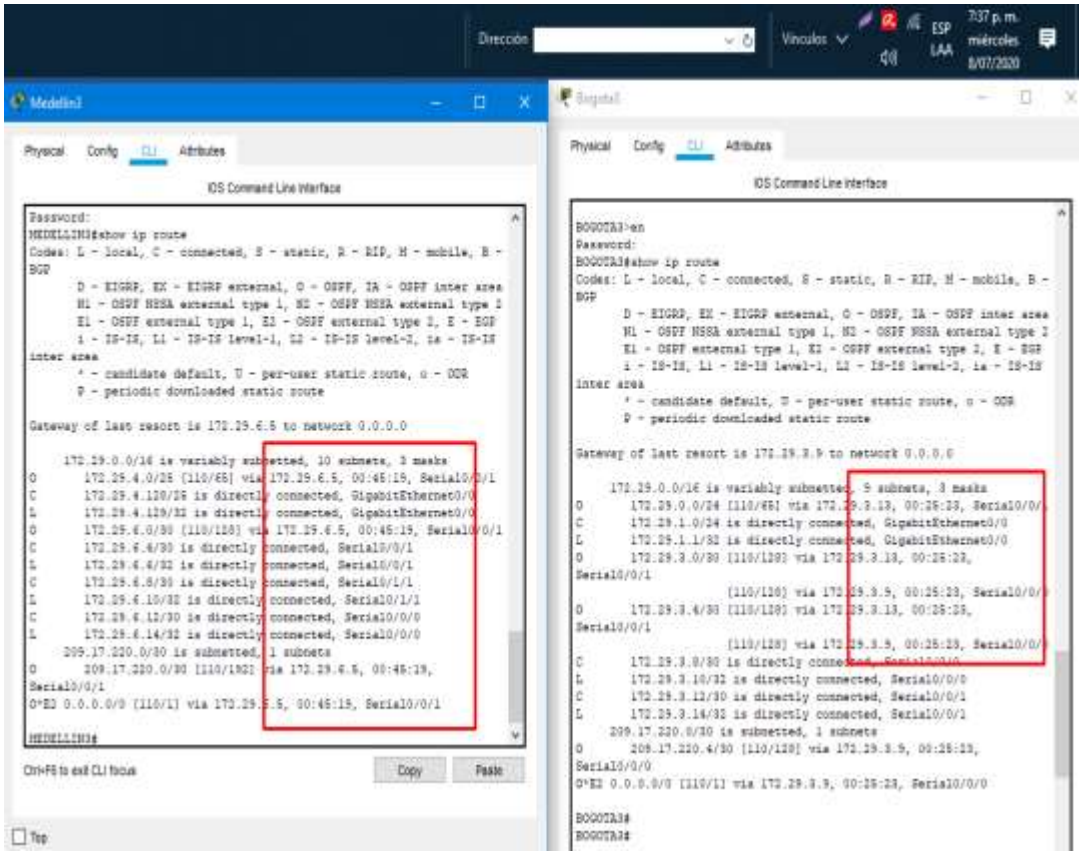
d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

Figura 25 Sh ip route Medellin2 y Bogota2



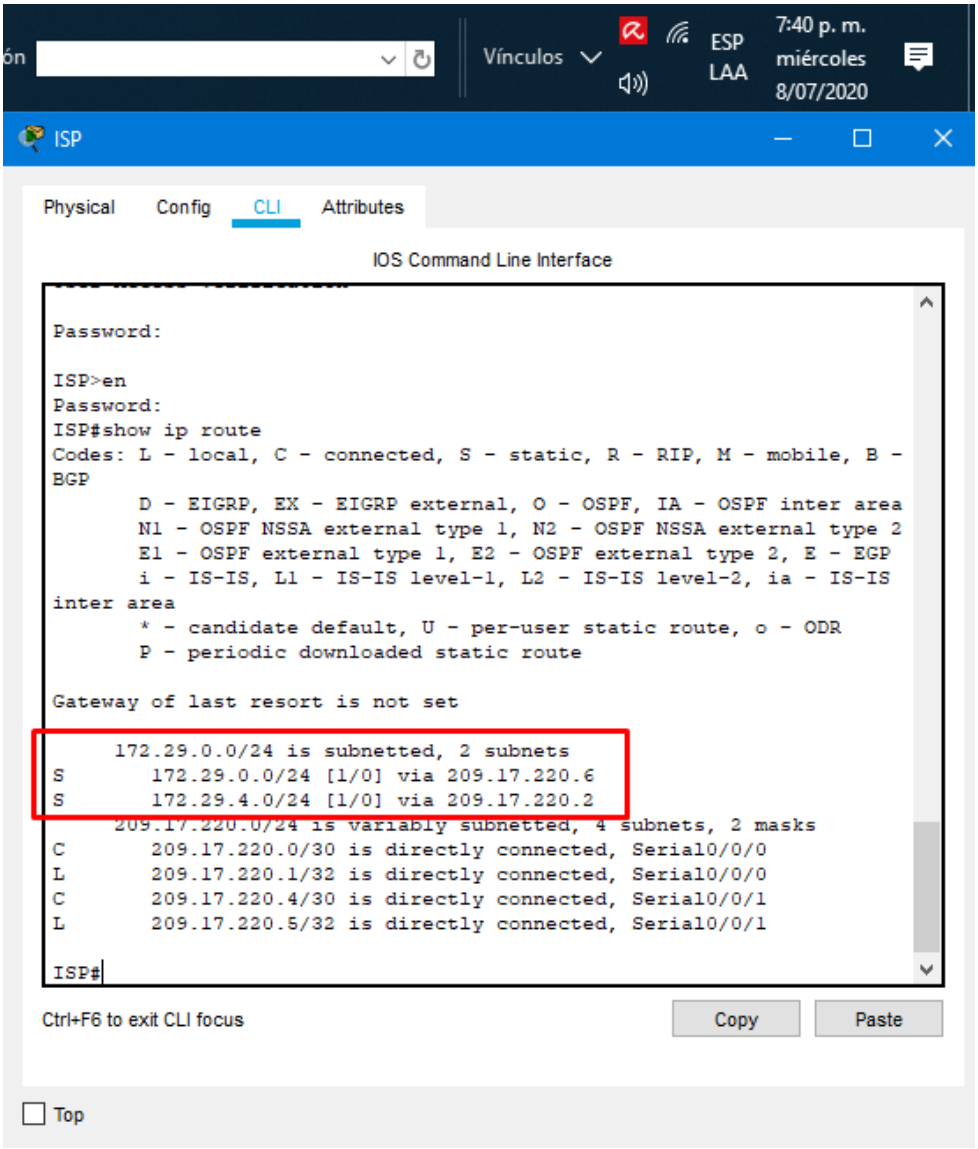
e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Figura 26 Show rutas redundantes



f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas. Se observa la ip de destino y la ip donde tiene que ser enviado.

Figura 27 Sh ISP



Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Se realizan Comandos OSPF que ayuda a que la propagación del protocolo, en los router BOGOTA2, BOGOTA3, MEDELLIN2, MEDELLIN3, se deshabiliten

Tabla 27 Propagación de OSPF

EQUIPOS	COMANDOS
BOGOTA1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
BOGOTA2	BOGOTA2#conf t BOGOTA2(config)#router ospf 1 BOGOTA2(config-router)#passive-interface g0/0 BOGOTA2(config-router)#end BOGOTA2#wr
BOGOTA3	BOGOTA3#conf t BOGOTA3(config)#router ospf 1 BOGOTA3(config-router)#passive-interface g0/0 BOGOTA3(config-router)#end BOGOTA3#wr
MEDELLÍN1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
MEDELLÍN2	MEDELLIN2#conf t MEDELLIN2(config)#router ospf 1 MEDELLIN2(config-router)#passive-interface g0/0 MEDELLIN2(config-router)#end MEDELLIN2#wr
MEDELLÍN3	MEDELLIN3#conf t MEDELLIN3(config)#router ospf 1 MEDELLIN3(config-router)#passive-interface g0/0 MEDELLIN3(config-router)#end MEDELLIN3#wr
ISP	No lo requiere

Parte 4: Verificación del protocolo OSPF.

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

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

Verificamos los puntos a y b con el comando sh ip protocols también podemos verificar con el comando sh ip route ospf para información de las rutas de OSPF, se comprueba en todos los equipos routers.

Figura 28 sh OSPF Medellin1

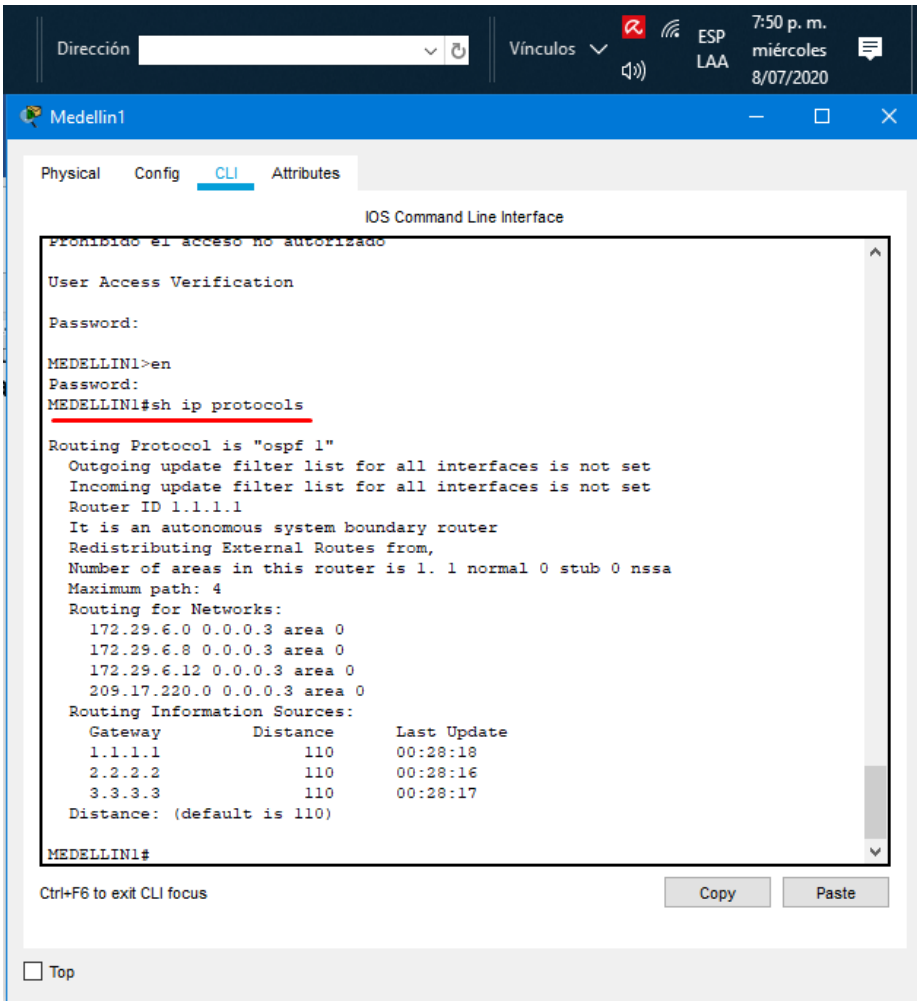


Figura 29 sh OSPF Medellin2

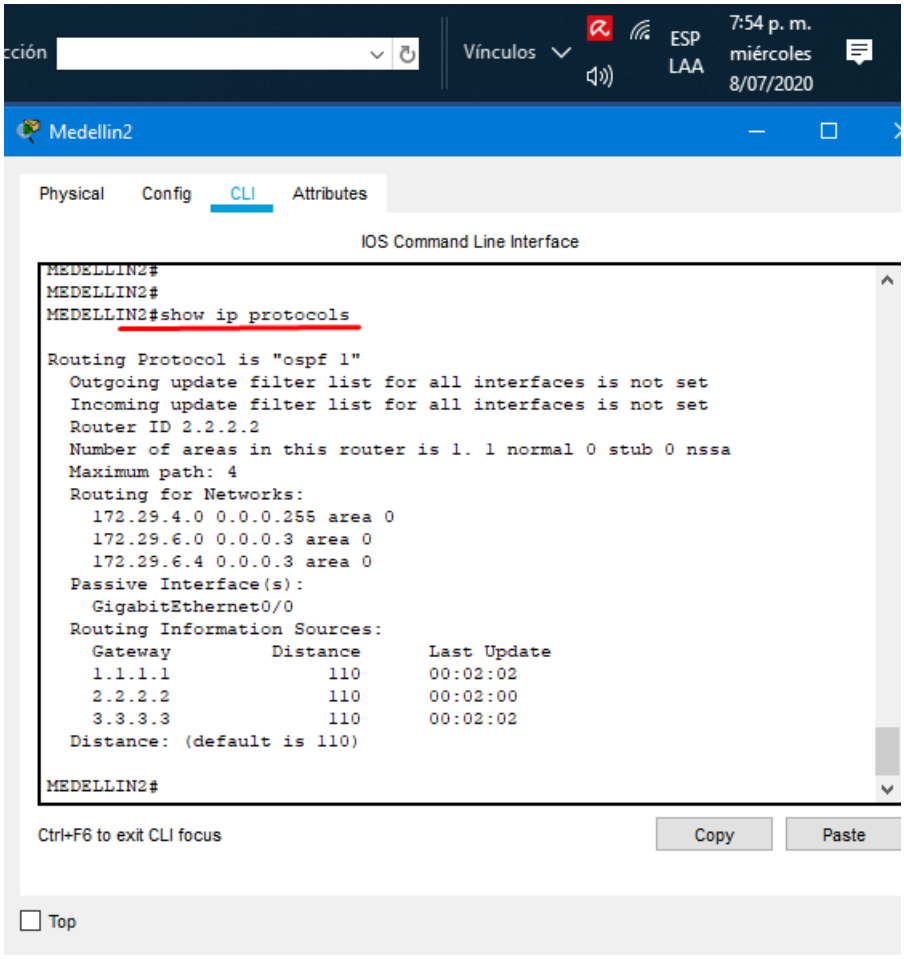


Figura 30 sh OSPF Medellin3

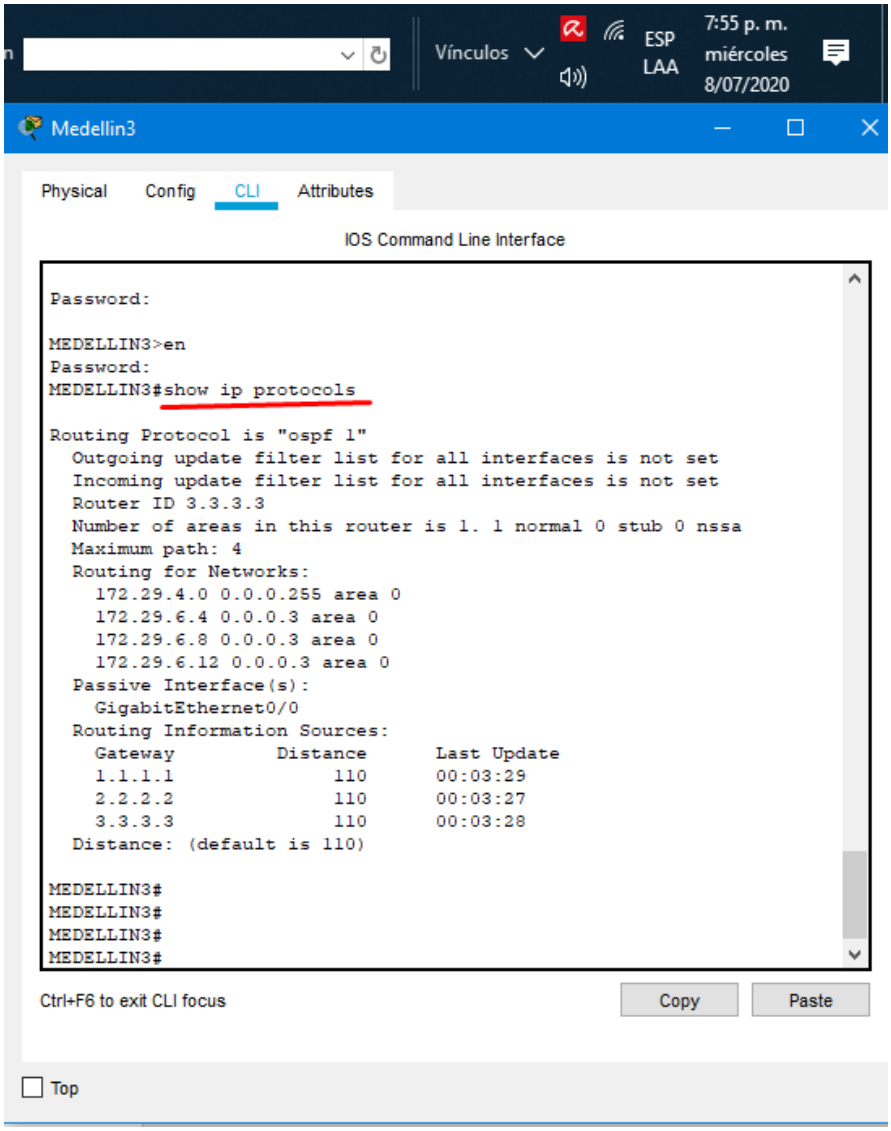


Figura 31 sh OSPF Bogota1

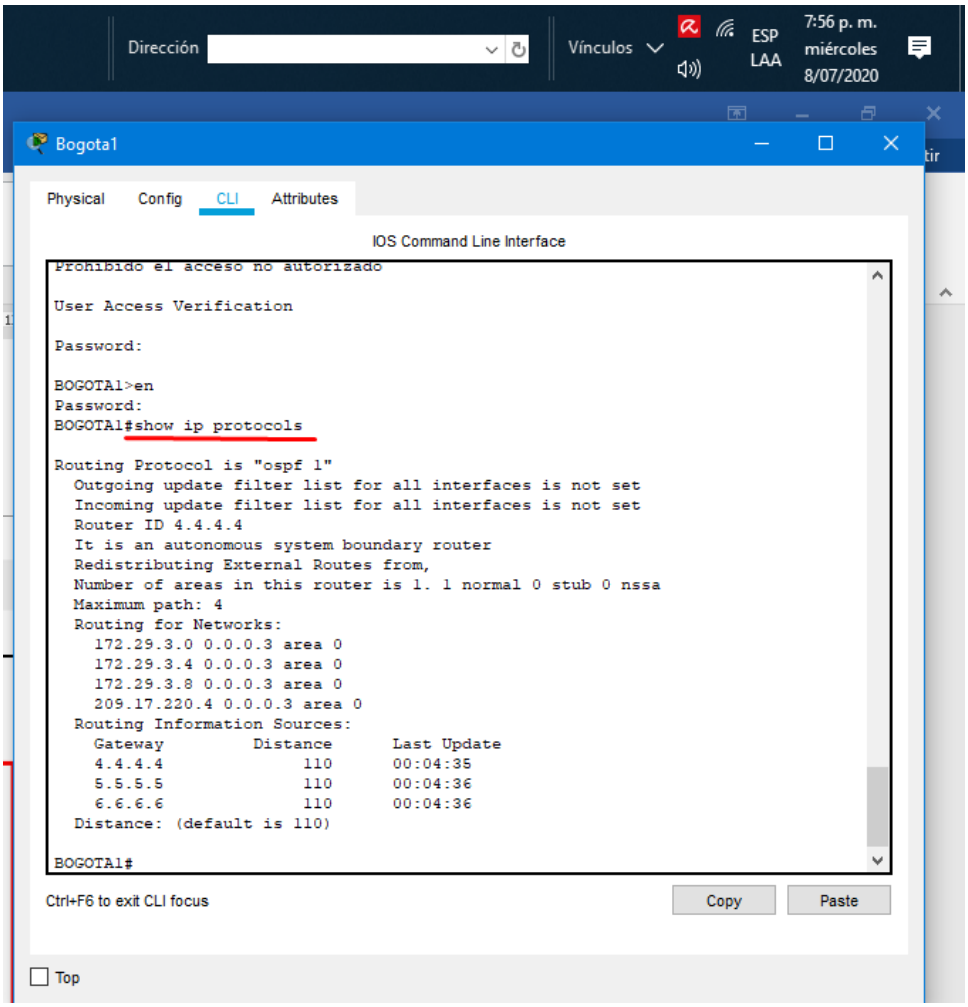


Figura 32 sh OSPF Bogota2

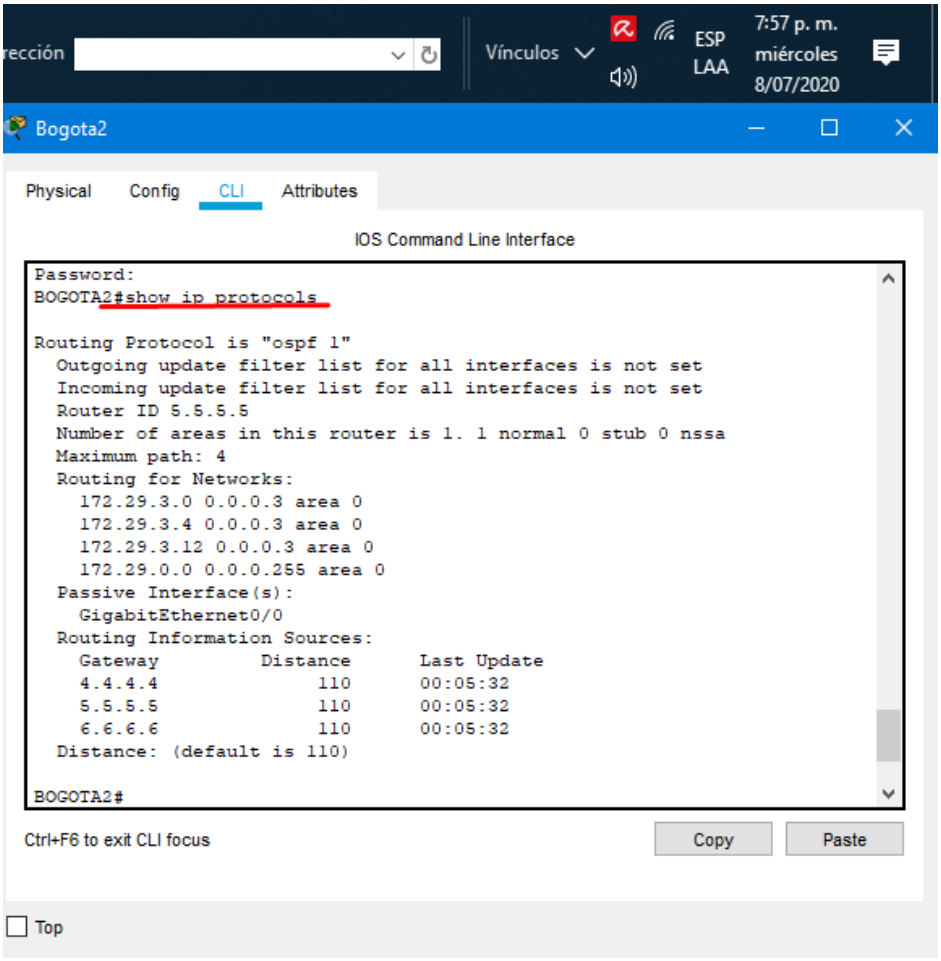
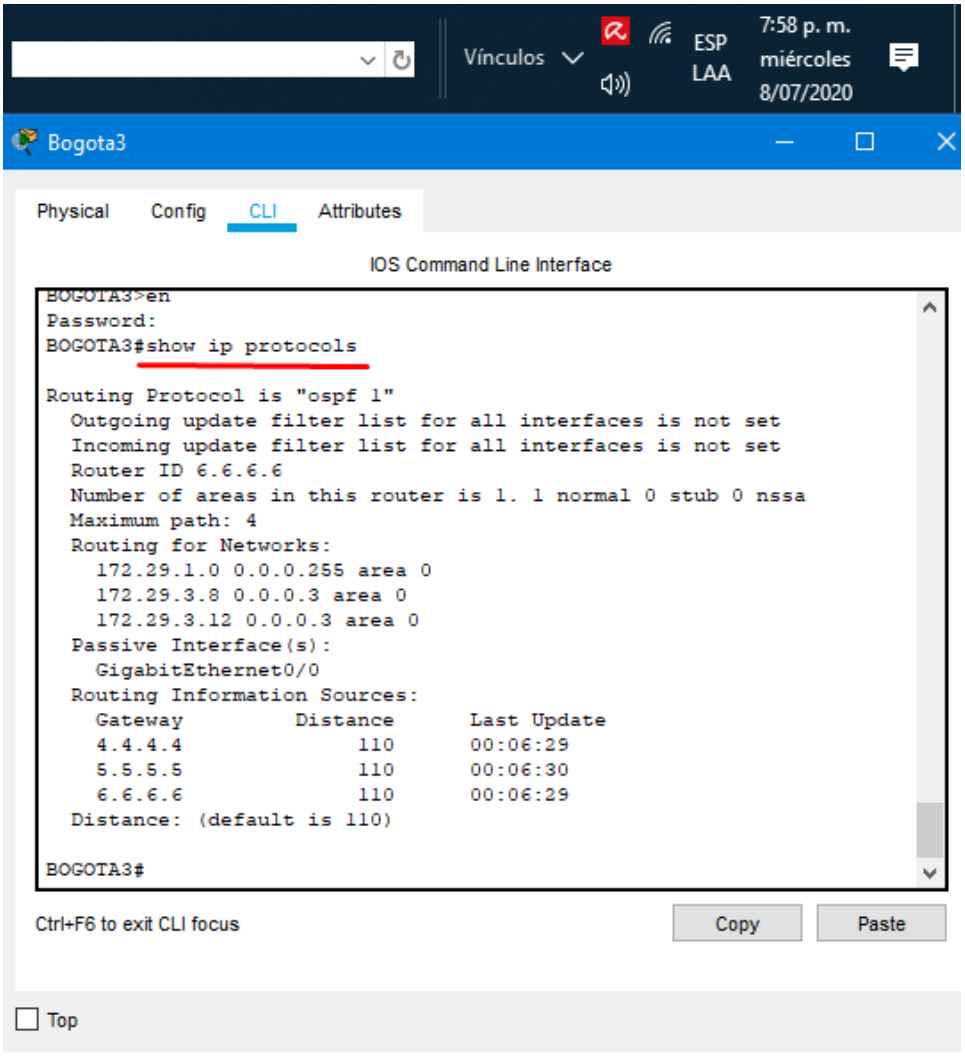


Figura 33 sh OSPF Bogota3



Parte 5: Configurar encapsulamiento y autenticación PPP.

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

   Configuramos la autenticación local del peer PPP remoto con el protocolo especificado para los dispositivos en las interfaces de los routers ISP y MEDELLIN1 también demos tener en cuenta la autenticación PPP que permite la negociación de los protocolos antes de que la capa de red transmitan por enlaces

Tabla 28 Authentication PAT

DISPOSITIVO	COMANDOS
ISP	ISP#conf t ISP(config)#username MEDELLIN1 password cisco ISP(config)#interface s0/0/0 ISP(config-if)#encapsulation PPP ISP(config-if)# ISP(config-if)#PPP authentication PAP ISP(config-if)#PPP PAP sent-username ISP password cisco ISP(config-if)#exit
MEDELLIN1	MEDELLIN1#conf t MEDELLIN1(config)#username ISP password cisco MEDELLIN1(config)#interface s0/0/0 MEDELLIN1(config-if)#encapsulation PPP MEDELLIN1(config-if)#PPP authentication PAP MEDELLIN1(config-if)#PPP PAP sent-username MEDELLIN1 password cisco MEDELLIN1(config-if)#exit

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

Se realizan Comandos en las interfaces de los router ISP y BOGOTA1 con autenticación chap.

Tabla 29 Autenticación Chap

DISPOSITIVO	COMANDOS
ISP	ISP#conf t ISP(config)#username BOGOTA1 password cisco ISP(config)#interface s0/0/1 ISP(config-if)#encapsulation PPP ISP(config-if)#PPP authentication chap
BOGOTA1	BOGOTA1#conf t BOGOTA1(config)#username ISP password cisco BOGOTA1(config)#interface s0/0/0 BOGOTA1(config-if)#encapsulation PPP BOGOTA1(config-if)#PPP authentication chap

Parte 6: Configuración de PAT.

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

   A continuación, se evidencia en MEDELLIN1 y MEDELLIN2 la configuración para activar la traducción de direcciones de redes NAT, se ingresa desde cada interfaz las ip de direccionamiento para realizar respectiva configuración y conservar las direcciones IP permitiendo la salida a internet de las ip privadas que emplean direcciones no registradas y lo comprobamos con el comando sh ip nat translations

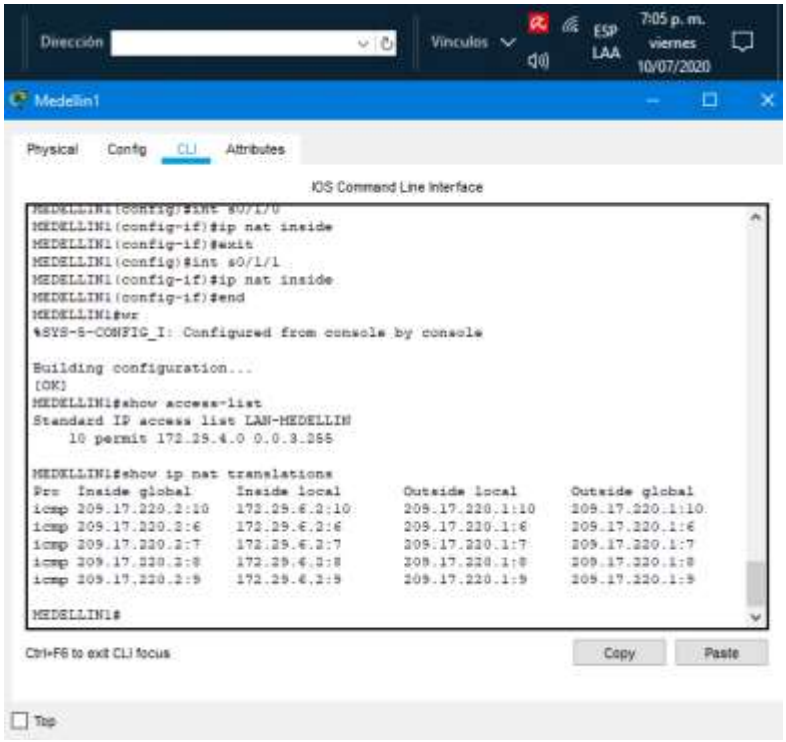
Tabla 30 Configuración de PAT

DISPOSITIVO	COMANDOS
MEDELLIN1	MEDELLIN1#conf t MEDELLIN1(config)#ip access-list standard LAN-MEDELLIN MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.3.255 MEDELLIN1(config-std-nacl)#exit MEDELLIN1(config)#ip nat inside source list LAN-MEDELLIN interface s0/0/0 overload MEDELLIN1(config)#interface s0/0/0 MEDELLIN1(config-if)#ip nat outside MEDELLIN1(config-if)#exit MEDELLIN1(config)#interface s0/0/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#exit MEDELLIN1(config)#interface s0/1/0 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#exit MEDELLIN1(config)#interface s0/1/1 MEDELLIN1(config-if)#ip nat inside MEDELLIN1(config-if)#end MEDELLIN1#wr
BOGOTA1	BOGOTA1#conf t BOGOTA1(config)#ip access-list standard LAN-BOGOTA BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.3.255 BOGOTA1(config-std-nacl)#exit

	BOGOTA1(config)#ip nat inside source list LAN-BOGOTA interface s0/0/0 overload BOGOTA1(config)#interface s0/0/0 BOGOTA1(config-if)#ip nat outside BOGOTA1(config-if)#exit BOGOTA1(config)#interface s0/0/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#exit BOGOTA1(config)#interface s0/1/0 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#exit BOGOTA1(config)#interface s0/1/1 BOGOTA1(config-if)#ip nat inside BOGOTA1(config-if)#end BOGOTA1#wr

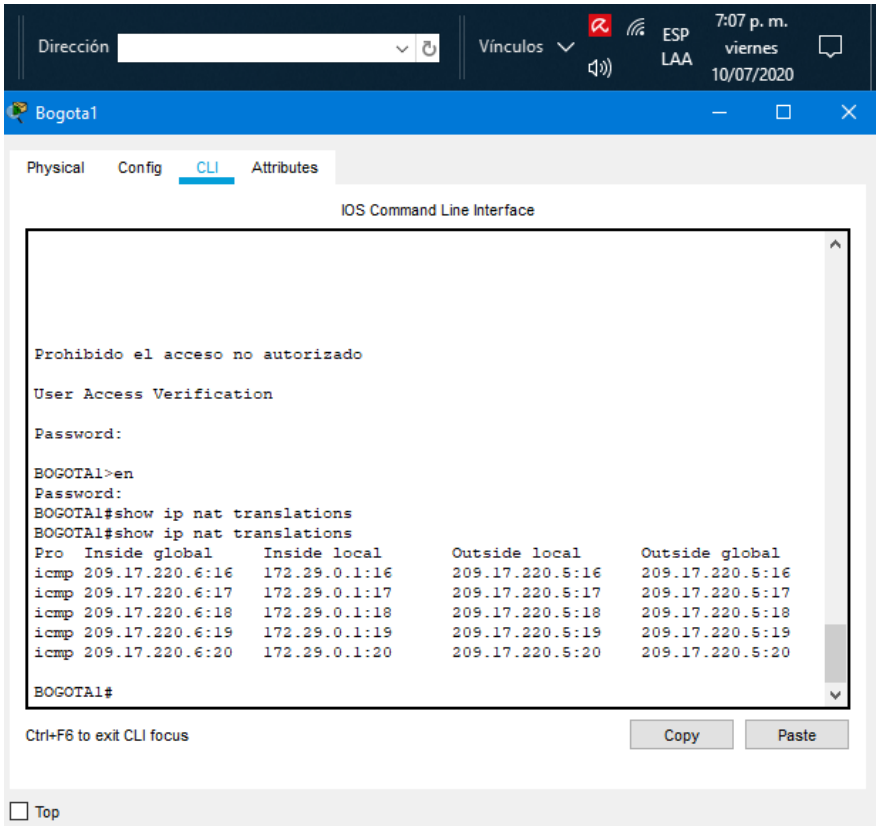
b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

Figura 34 NAT MEDELLIN1



c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar los ping, la dirección es traducida automáticamente a la dirección de la int s0/1/0 de Bogotá1, cómo puerto diferente.

Figura 35 NAT BOGOTA1



Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN permitiendo la conexión entre dispositivos para esa área igualmente configuramos DHCP en MEDELLIN2 para que sirva de servidor en juntas redes LAN.

Tabla 30 Configuración DHCP MEDELLIN2

DISPOSITIVO	COMANDOS
MEDELLIN2	MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.9 MEDELLIN2(config)#ip dhcp pool MEDELLIN-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.medellin.com MEDELLIN2(dhcp-config)#exit MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.136 MEDELLIN2(config)#ip dhcp pool MEDELLIN-LAN2 MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128 MEDELLIN2(dhcp-config)#default-router 172.29.4.129 MEDELLIN2(dhcp-config)#domain-name lan2.medellin.com MEDELLIN2(dhcp-config)#exit

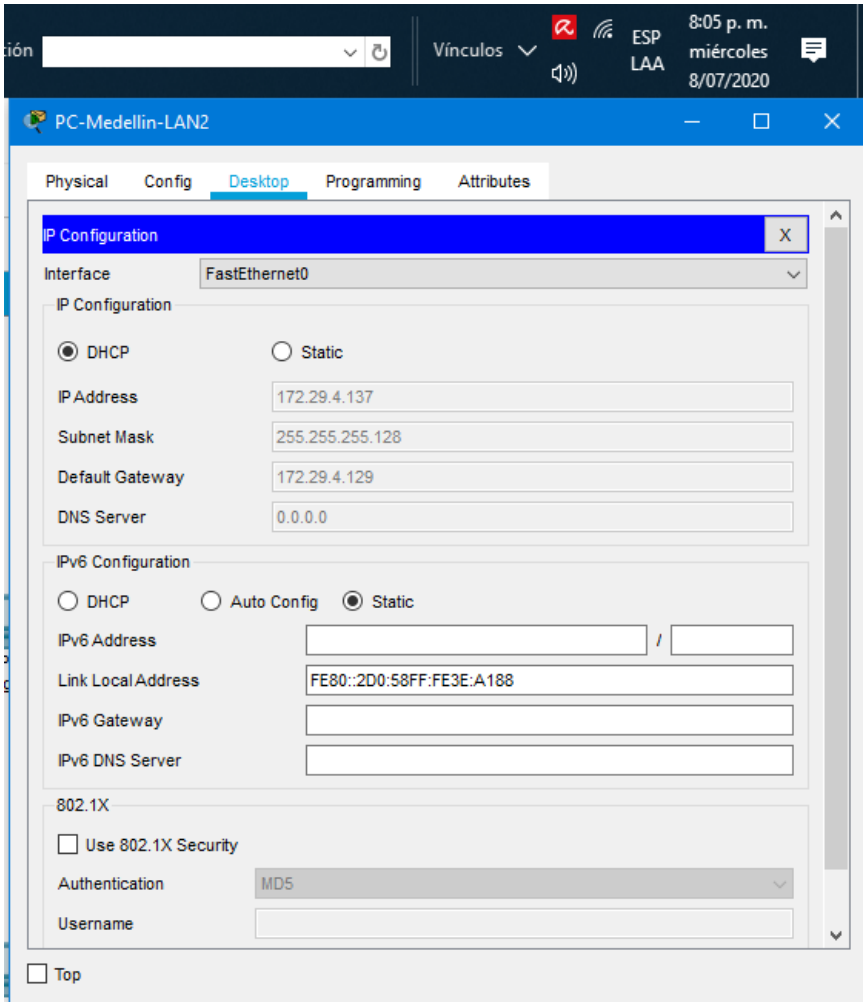
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

En MEDELLIN3 ejecutamos los comando para que se permita el paso de los mensajes broadcast

Tabla 31 HABILITAR PASO MEDELLIN3

DISPOSITIVO	COMANDOS
MEDELLIN3	MEDELLIN3(config)#interface g0/0 MEDELLIN3(config-if)#ip helper-address 172.29.6.5 MEDELLIN3(config-if)#exit MEDELLIN3(config)#

Figura 36 DHCP MEDELLIN



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

Se realizan comandos a BOGOTA2 con el fin de que habilite el paso para los mensajes broadcast.

Tabla 32 Servidor DHCP BOGOTA2

DISPOSITIVO	COMANDOS
BOGOTA2	BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4 BOGOTA2(config)#ip dhcp pool BOGOTA-LAN2 BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.1.1 BOGOTA2(dhcp-config)#exit BOGOTA2(config)#ip dhcp pool BOGOTA-LAN1 BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0 BOGOTA2(dhcp-config)#default-router 172.29.0.1

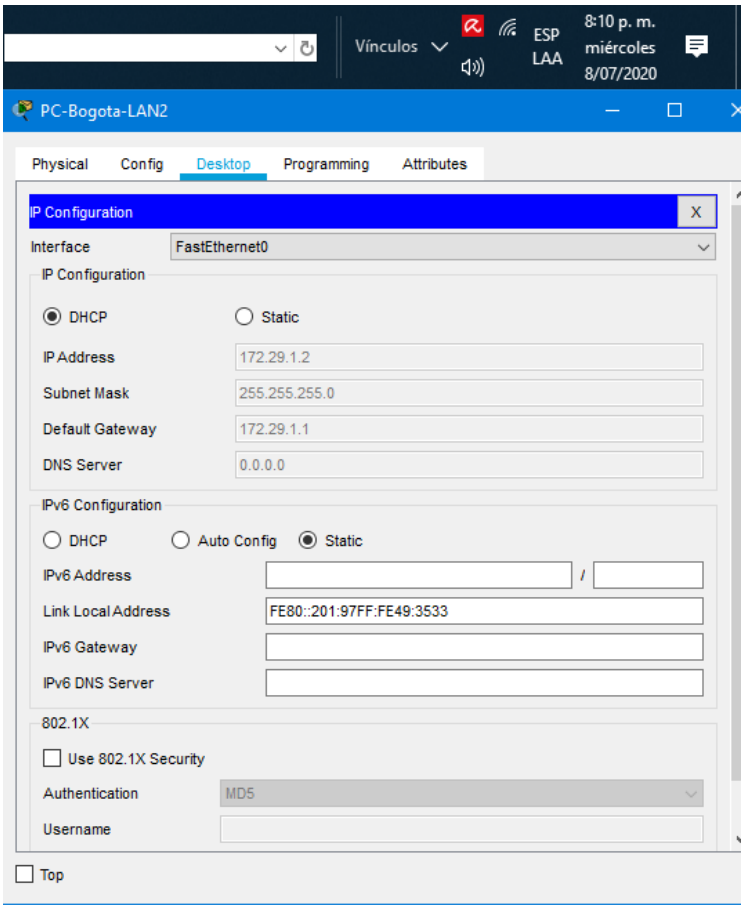
d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Se procede a realizar Comandos en BOGOTA3 para que habilite el paso de los mensajes broadcast.

Tabla 33 Habilitar paso BOGOTA3

DISPOSITIVO	COMANDOS
BOGOTA3	BOGOTA3(config)#interface g0/0 BOGOTA3(config-if)#ip helper-address 172.29.3.13 BOGOTA3(config-if)#exit

Tabla 34 DHCP BOGOTA



CONCLUSIÓN

La solución de los ejercicios propuestos en los escenarios nos permitió reconocer y comprender comandos de configuración cisco, desde cambiar un nombre a un dispositivo, brindarle seguridad, hasta verificar las conexiones realizadas, todo esto lo logramos de acuerdo al paso a paso realizado que nos proponen en la guía.

Se logró abarcar diversos ejercicios que son de la vida real dadas las características de localización de diferentes ciudades que logramos simular conexiones mediante comandos básicos a los router y switch, comandos de interfaces físicas y lógicas, VLANs, encapsulamientos, restricciones y parámetros que aumentan la seguridad en la red, OSPF, DHCP, NAT, todo esto lo logramos mediante la herramienta simuladora Packet Tracer.

BIBLIOGRAFIA

Configurar NAT Estático. {En línea}. Recuperado de: https://todopacketracer.com/2011/11/26/configurar-nat-estatico/)

Configure NTP on a Cisco router. Recuperado de: https://study-ccna.com/configure-ntp-on-a-cisco-router

Configuring NTP. {En linea}. Recuperado de: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8- 2glx/configuration/guide/ntp.html

Configure Commonly Used IP ACLs.Recuperado de: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

CCNA R&S: Introduction to Networks. Recuperado de: https://www.netacad.com/portal/learning

Dynamically Configuring DHCP Server Options. Recuperado de: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocationresolution/22920-dhcp-ser.html

UNAD.Configuración básica de Equipos. Recuperado de:

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2.2

UNAD.Configuración de Router Cisco. Recuperado de:

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6.4

UNAD. LAN Y WAN. Recuperado de:

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1.2

UNAD. Protocolos de comunicación de red. Recuperado de:

https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

ANEXO 1. ESCENARIO UNO Y ESCENARIO DOS

Link.

Archivos Packet Tracer escenario uno y escenario dos.