

PRUEBA DE HABILIDADES
DIPLOMADO DE PROFUNDIZACIÓN CISCO

JULIA ISABEL RODRIGUEZ VASQUEZ

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
2019

TABLA DE CONTENIDO

RESUMEN	4
ABSTRACT	5
INTRODUCCION	6
OBJETIVOS	7
Objetivo General	7
Objetivos Específicos.....	7
DESCRIPCIÓN DE LOS ESCENARIOS	8
Escenario 1	8
Imágenes	
Fig.1	8
Fig.2	9
Fig.3	9
Fig.4	10
Fig.5	10
Fig.6	11
Fig.7	11
Fig.8 y 9	12
Fig.10	13
Fig.11	13
Fig.12	14
Fig.13	14
Fig.14 y 15	15
Fig.16 y 17	16
Fig.18	17
Fig.19 y 20	18

Fig.21 y 22	19
Fig.23	20
Fig.24	20
Fig.25	21
Escenario 2	22
Fig.26	22
Fig.27 y 28	23
Fig.29 y 30	24
Fig.31 y 32	25
Fig.33 y 34	26
Fig.35 y 36	27
Fig.37	28
Fig.38 y 39	29
Fig.40 y 41	30
Fig.42 y 43	31
Fig.44 y 45	32
Fig.46	33
Fig.47 y 48	34
Fig.49 y 50	35
Fig.51 y 52	36
CONCLUSION	37
BIBLIOGRAFIA	38

RESUMEN

La carrera de Ingeniería de Sistemas ha permitido que yo logre conocer y más que todo descubrir habilidades que no sabía que existían o que yo podía desarrollar, sin embargo durante todo este tiempo, semestre tras semestre fui experimentando facetas nuevas que lograron perpetuarse en mí para poder ser la profesional que soy hoy en día. Gracias a la universidad y a todos los tutores que nos enseñaron cada día, año tras año, a todos los que han hecho posible que todos nosotros seamos capaces de formarnos como unos excelentes profesionales. Mediante este Diplomado hemos conocido también temas interesantísimos que son realmente necesarios e importantes durante el desarrollo de nuestra carrera profesional, temas de alta calidad, teniendo en cuenta que CISCO es una plataforma en redes LAN-WAN de todo el mundo, la cual es una parte fundamental e indispensable de las ingenierías, que va desde la manera más sencilla hasta la más compleja de construir una red LAN y que por supuesto, mediante todo el aprendizaje que hemos obtenido, logramos llegar siempre a la solución y desarrollo de cualquier situación que se nos presente.

ABSTRACT

The Systems Engineering career has allowed me to get to know and, above all, discover skills that I did not know existed or that I could develop, however during all this time, semester after semester I was experiencing new facets that managed to perpetuate me in order to be the professional that I am today. Thanks to the university and all the tutors who taught us every day, year after year, to all who have made it possible for all of us to be able to train as excellent professionals. Through this Diploma we have also known very interesting topics that are really necessary and important during the development of our professional career, high quality issues, taking into account that CISCO is a platform in LAN-WAN networks around the world, which is a part fundamental and indispensable engineering, which goes from the simplest to the most complex way to build a LAN network and that of course, through all the learning we have obtained, we always reach the solution and development of any situation that we are I presented.

INTRODUCCION

Mediante todo el desarrollo de los módulos CCNA I y II, hemos aprendido conceptos claros del funcionamiento de redes en torno a Cisco, haciendo uso de las herramientas tecnológicas que no provee Packet Tracer con las cuales, recibimos las bases para entornos reales en donde se requiera la administración de redes, conceptos como Routing, Switching, VLAN, OSPF, NAT, PAT, autenticación CHAP y PAP, configuraciones básicas de seguridad como la asignación de contraseñas, bloqueos de interfaces, mensajes de advertencia, encriptación de contraseñas, entre muchas funciones que nos ofrecen los dispositivos Cisco. Además, haciendo uso del modelo OSI como referencia lógica del funcionamiento de red y el protocolo TCP/IP como estándar global, nosotros como futuros ingenieros bien sea de telecomunicaciones o de sistemas podremos dar soluciones óptimas a todo tipo de situaciones que se pueden presentar a lo largo de nuestras carreras. En el siguiente trabajo haremos usos de las habilidades adquiridas durante el proceso de formación a lo largo del diplomado, planteando soluciones a escenarios propuestos, para así poner en práctica lo aprendido.

OBJETIVOS

GENERAL

- Desarrollar de manera concisa y muy puntual los escenarios 1 y 2

ESPECIFICOS

- Describir para cada escenarios el paso a paso de cada punto realizado
- Digitar el código de configuración aplicado para cada escenario
- Evidenciar por medio de imágenes los resultados de comandos ping, traceroute, show ip route, entre otros.

DESCRIPCION DE LOS ESCENARIOS

ESCENARIO 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

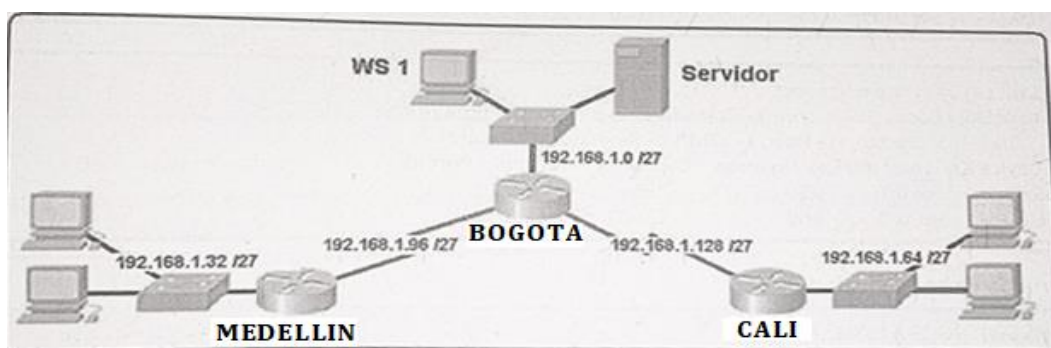
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.

Fig. 1



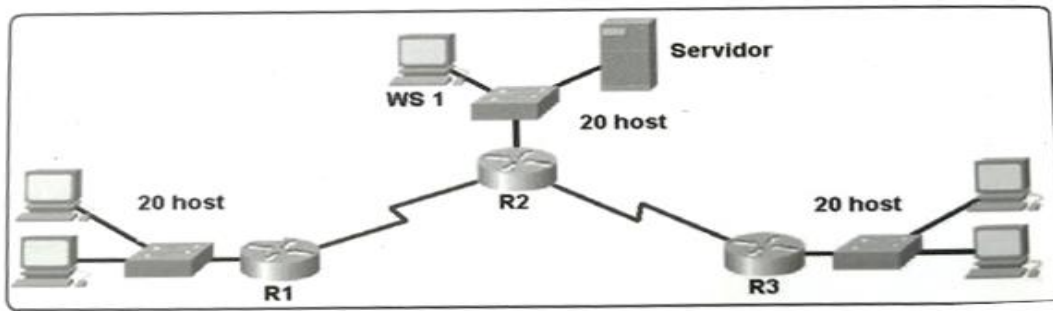


Fig. 2

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

Creamos los dispositivos de red en el escenario

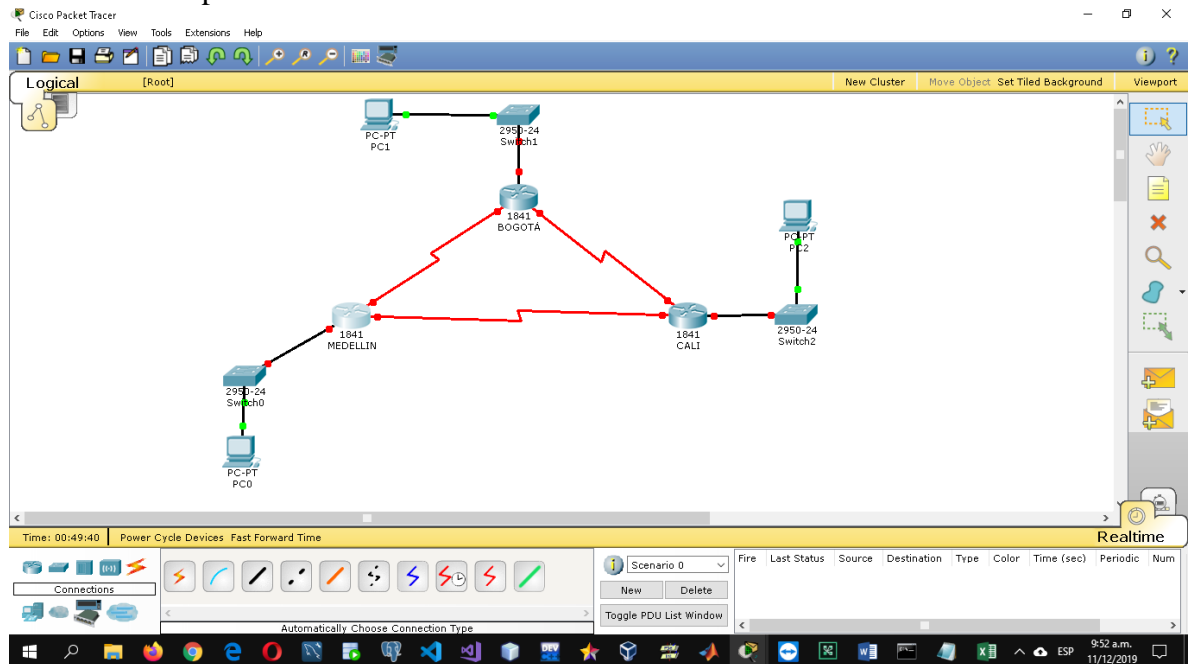


Fig. 3

Parte 1: Asignación de direcciones IP:

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

Se realiza el respectivo subneteo

Formula	subredes requeridas	bit necesarios	redes totales
2^n	8	2^3	8
	red	rango de host	broadcast
	192.168.1.0/27	192.168.1.1 -- 192.168.1.30	192.168.1.31
	192.168.1.32/27	192.168.1.33 -- 192.168.1.62	192.168.1.63
	192.168.1.64/27	192.168.1.65 -- 192.168.1.94	192.168.1.95
	192.168.1.96/27	192.168.1.97 -- 192.168.1.126	192.168.1.127
	192.168.1.128/27	192.168.1.129 -- 192.168.1.158	192.168.1.159
	192.168.1.160/27	192.168.1.161 -- 192.168.1.190	192.168.1.191
	192.168.1.192/27	192.168.1.193 -- 192.168.1.222	192.168.1.223
	192.168.1.224/27	192.168.1.225 -- 192.168.1.254	192.168.1.255

Fig. 4

b. Asignar una dirección IP a la red.

Se asignan las direcciones IP teniendo en cuenta el subneteo

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz Fa 0/0	192.168.1.33	192.168.1.11	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200

FastEthernet0/0 configuration details:

- Port Status: On
- Bandwidth: Auto
- Duplex: Half Duplex
- MAC Address: 00E0.A362.1501
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.224
- Tx Ring Limit: 10

Fig. 5

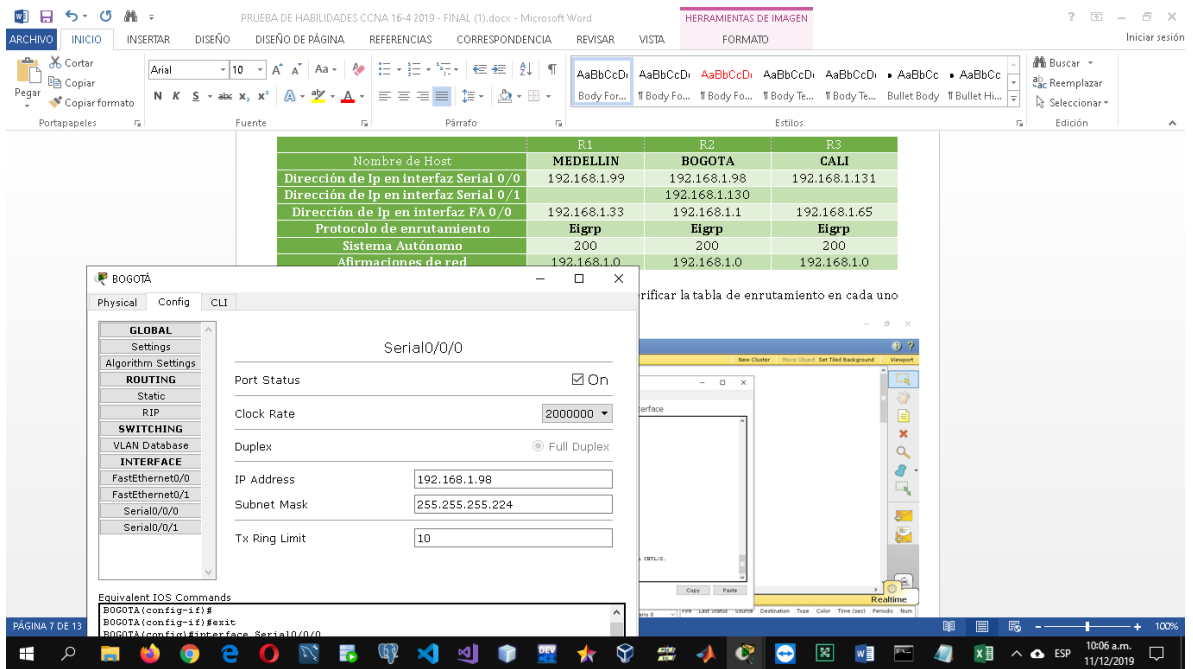
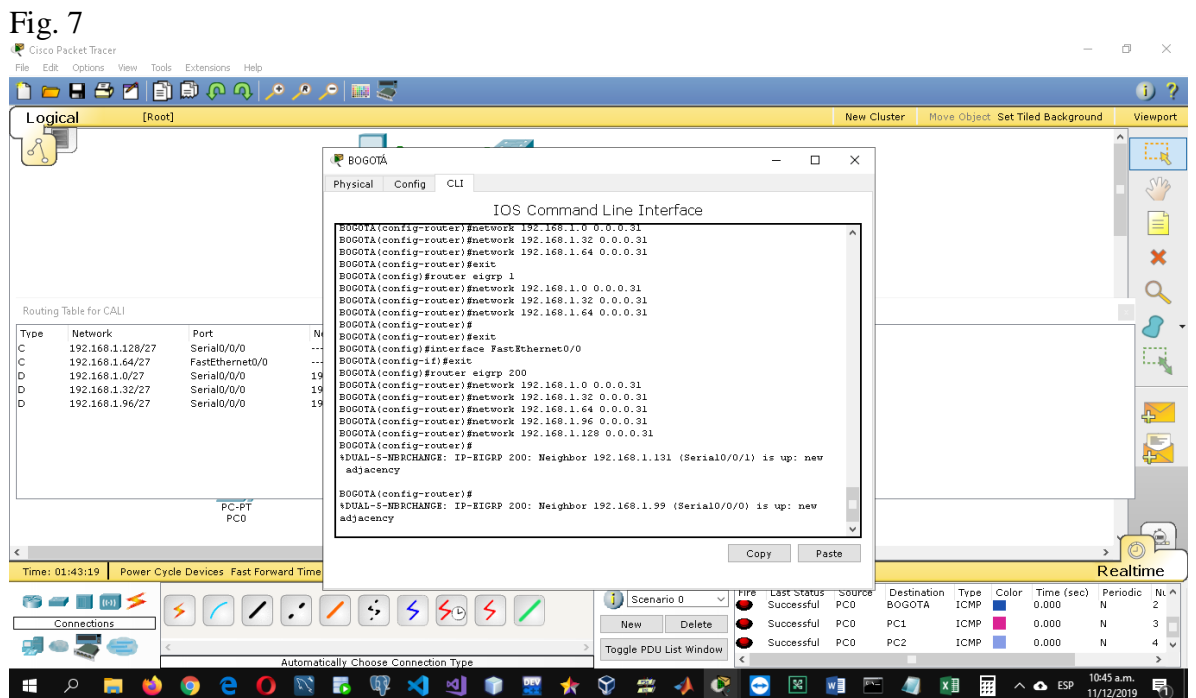


Fig. 6
Parte 2: Configuración Básica.

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

Se asignan todas las direcciones ip y se agrega el protocolo de enrutamiento para permitir la conexión



	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Fig. 8

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas. Se comprueba el direccionamiento ip mediante la tabla de enrutamiento de los routers

Fig. 9

The screenshot shows the Cisco Packet Tracer interface. The network diagram displays a central router labeled '1841 BOGOTA' connected to a switch '2950-24 Switch1'. The switch is connected to PC-PT PC1. Another PC-PT PC2 is shown nearby. The routing table for the MEDELLIN router is displayed below the diagram.

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.32/27	FastEthernet0/0	---	0/0
C	192.168.1.96/27	Serial0/0/0	---	0/0
D	192.168.1.0/27	Serial0/0/0	192.168.1.98	90/2172416
D	192.168.1.128/27	Serial0/0/0	192.168.1.98	90/2681856
D	192.168.1.64/27	Serial0/0/0	192.168.1.98	90/2684416

The interface also shows a 'Connections' window with a table of active connections:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	N
●	Successful	PC0	BOGOTA	ICMP	Blue	0.000	N	2
●	Successful	PC0	PC1	ICMP	Pink	0.000	N	3
●	Successful	PC0	PC2	ICMP	Blue	0.000	N	4

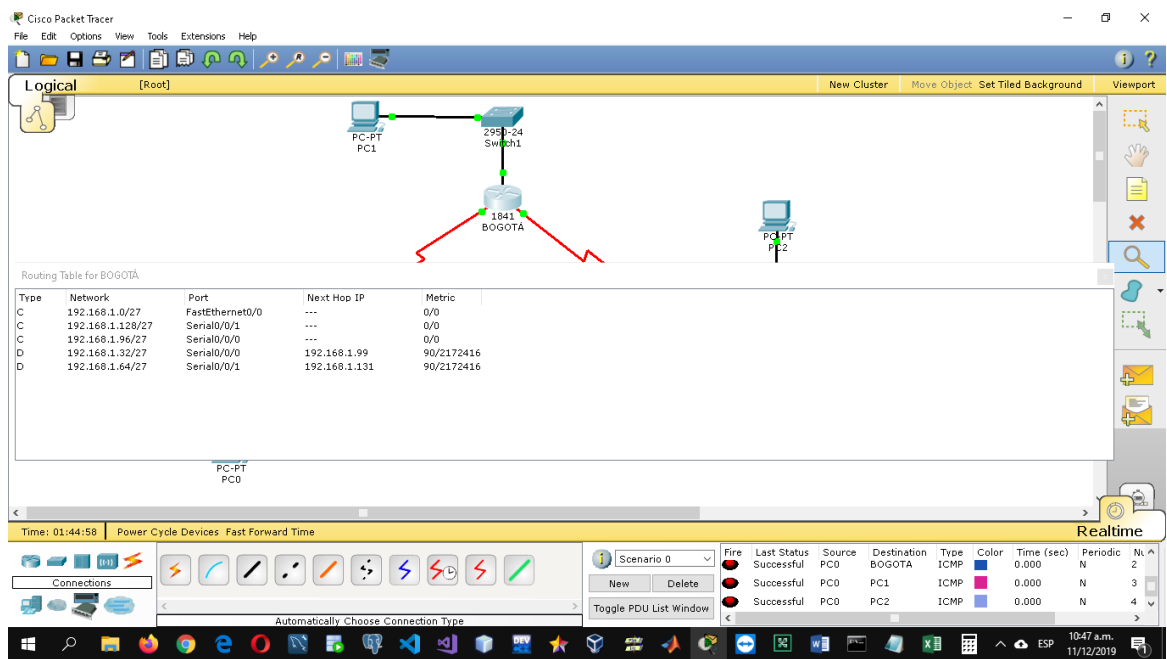
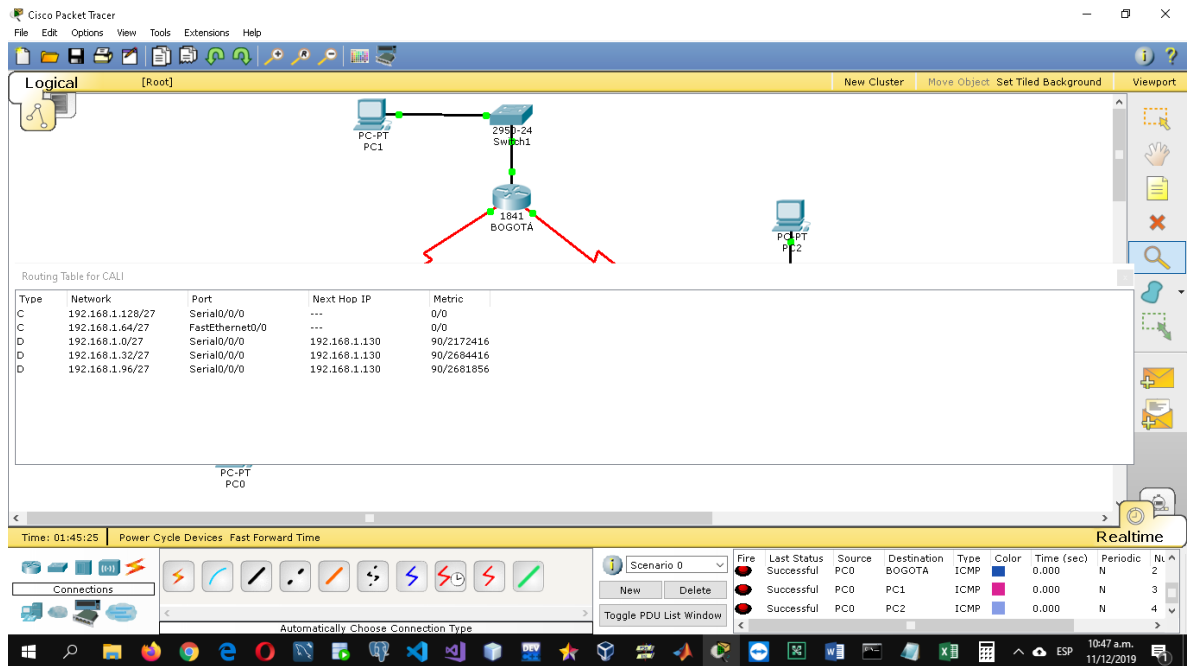


Fig. 10

Fig. 11



- c. Verificar el balanceo de carga que presentan los routers.
Se verifica el balanceo de carga mediante el comando show ip route –address

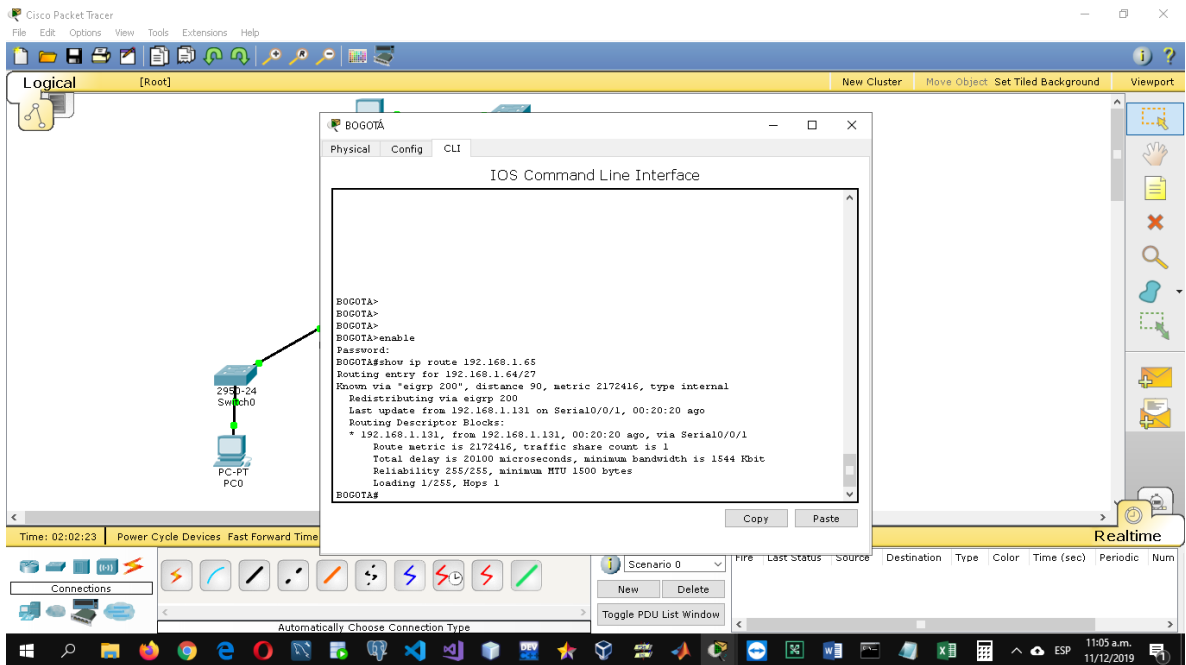
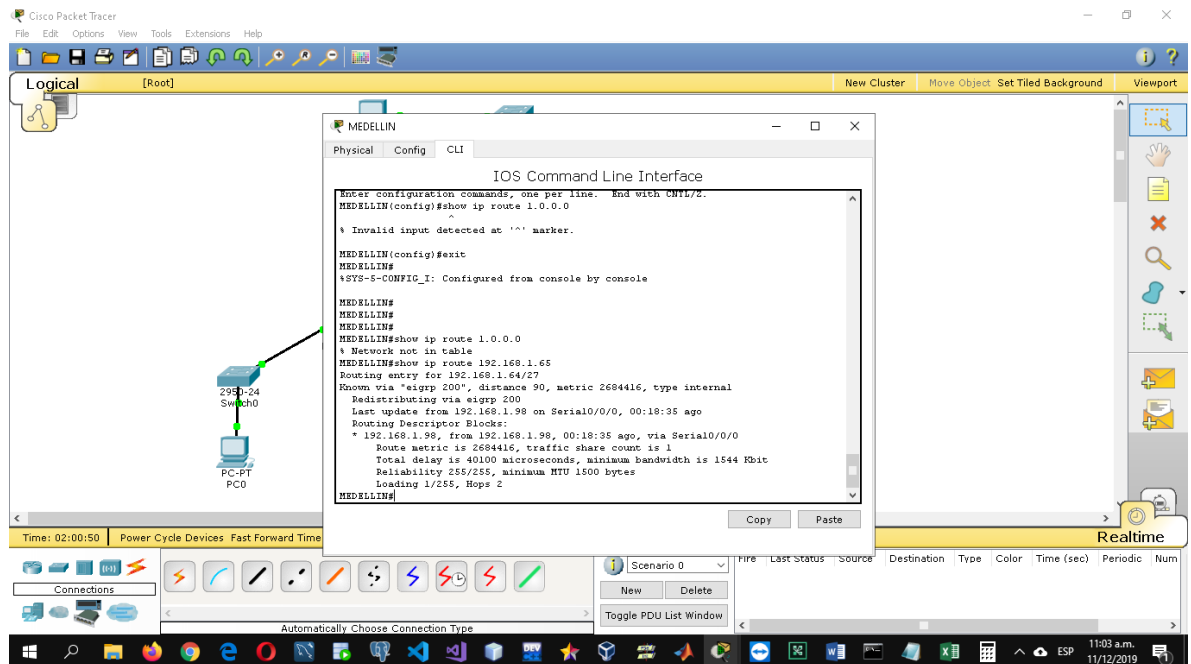


Fig. 12

Fig. 13



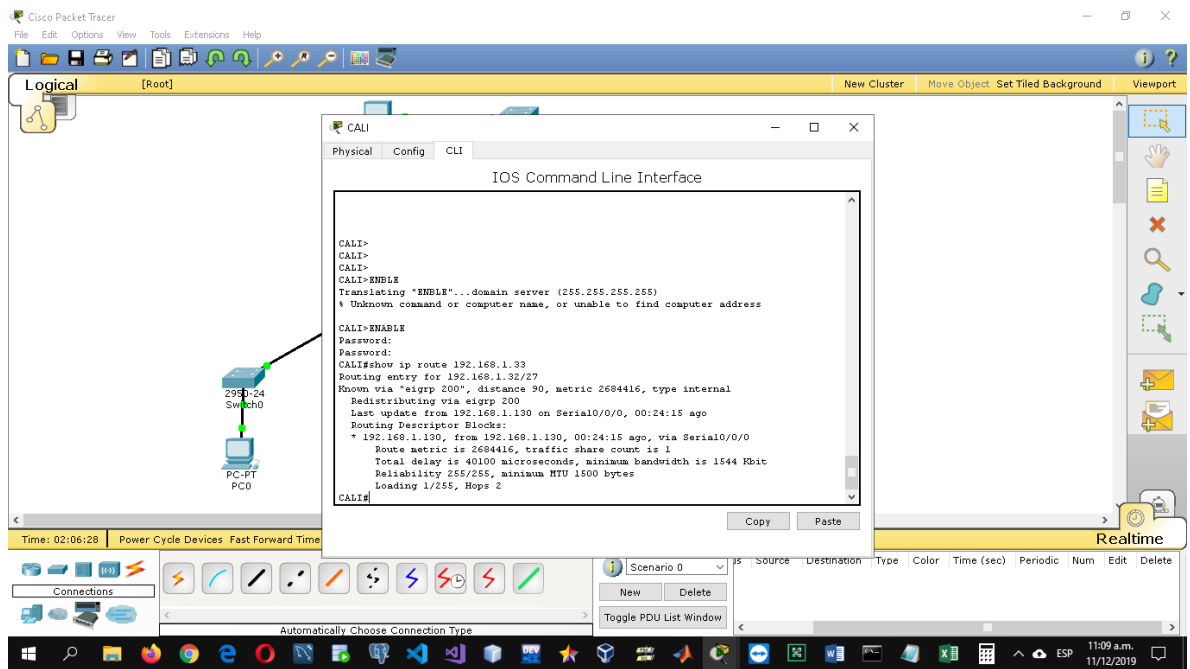


Fig. 14

d. Realizar un diagnóstico de vecinos usando el comando cdp. Mediante el comando cdp se realiza el diagnostico detallado y genera

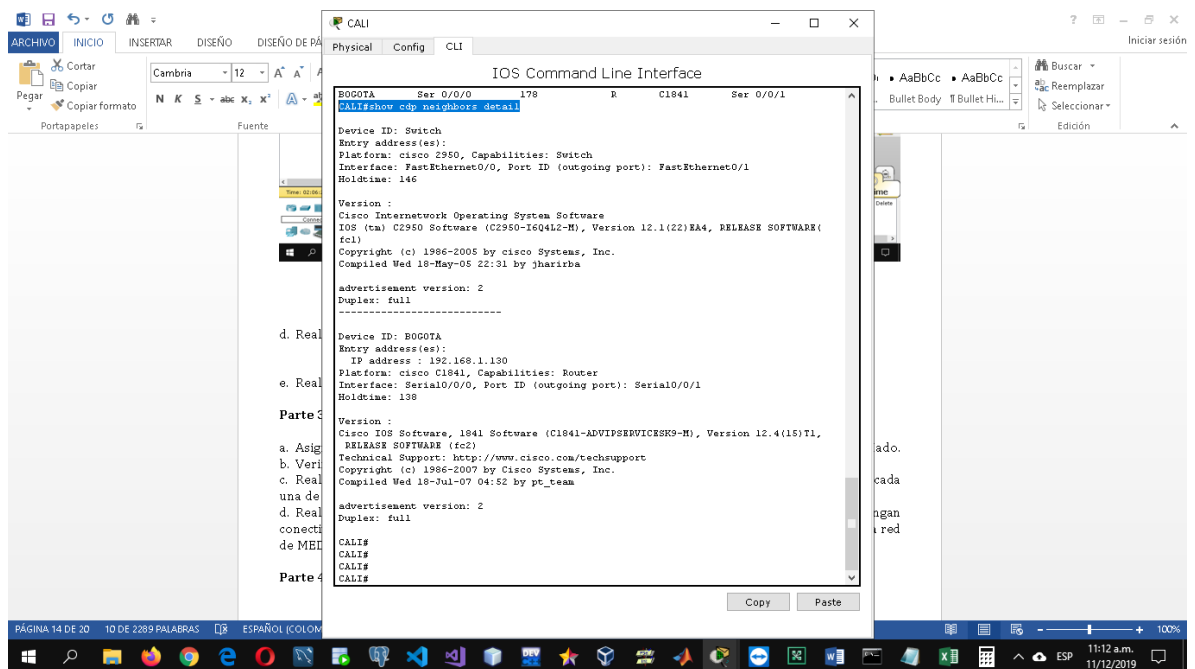


Fig. 15

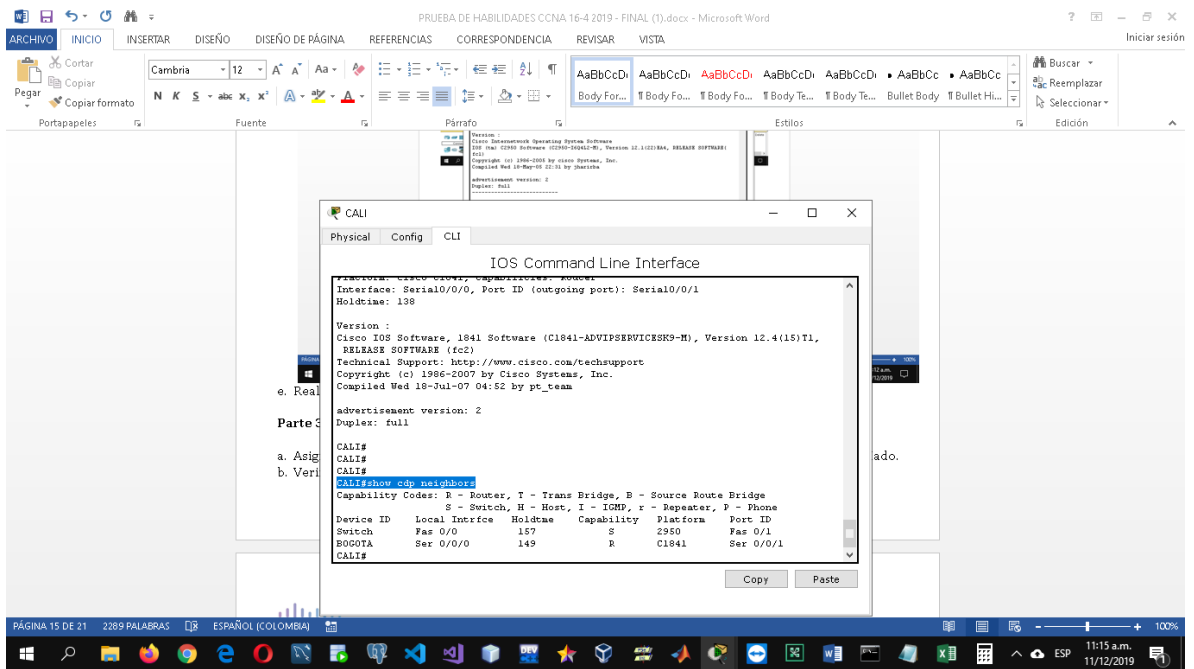
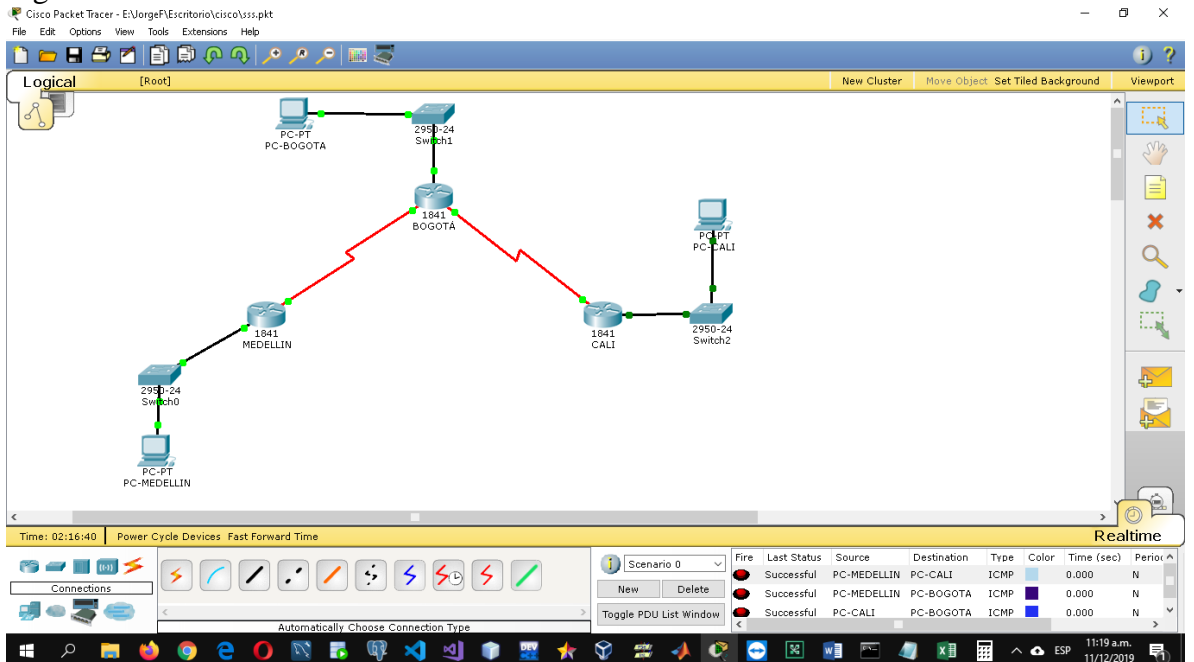


Fig. 16

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping. Se envían los respectivos mensajes para verificar la conexión

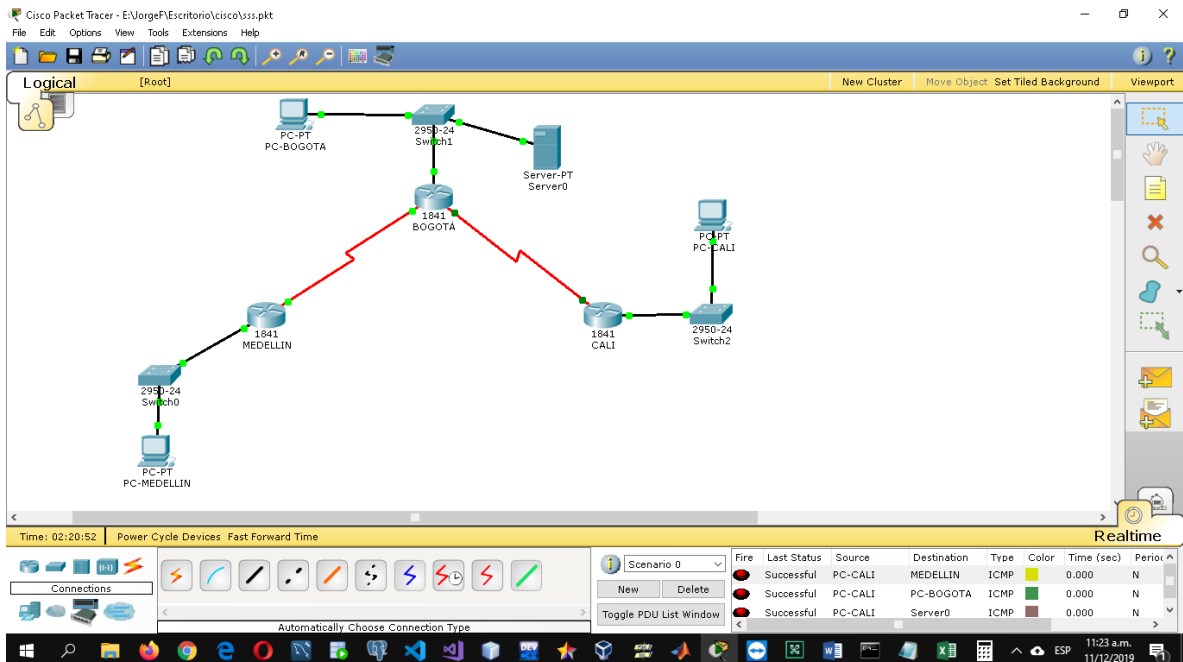
Fig. 17



Parte 3: Configuración de Enrutamiento.

- Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
- Verificar si existe vecindad con los routers configurados con EIGRP.
- Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.
- Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

La parte tres se desarrolló completamente en la parte anterior como se puede comprobar en las imágenes de esa sección y la siguiente imagen Fig. 18



Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
 Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión según lo requerido

Fig. 21

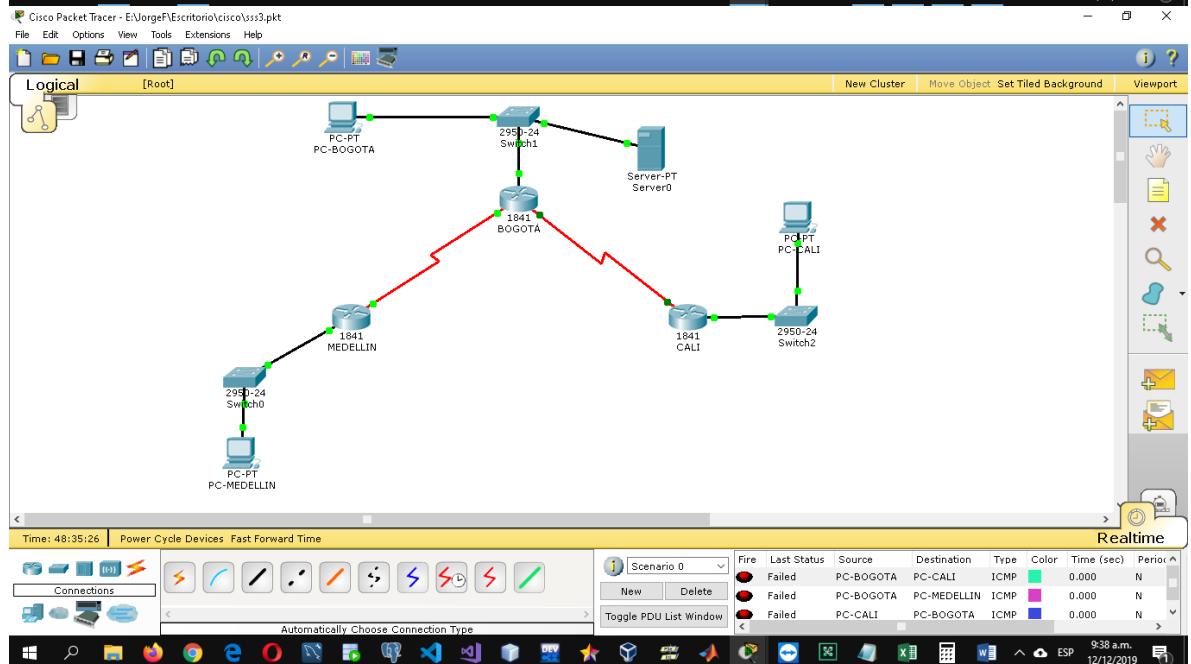
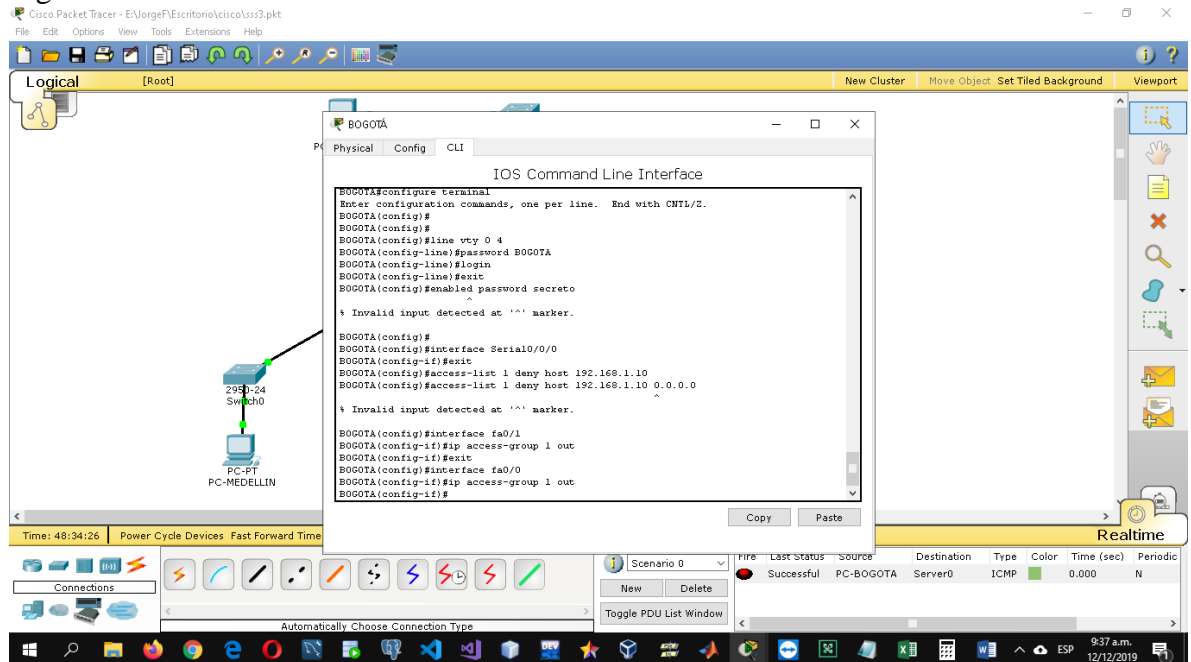


Fig. 22

c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor. Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión según lo requerido

Fig. 23

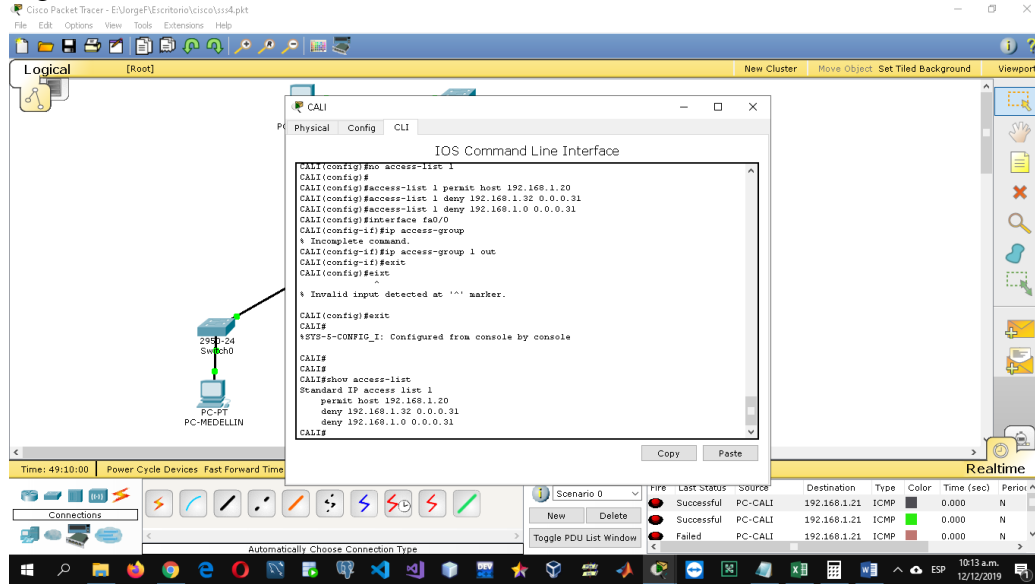
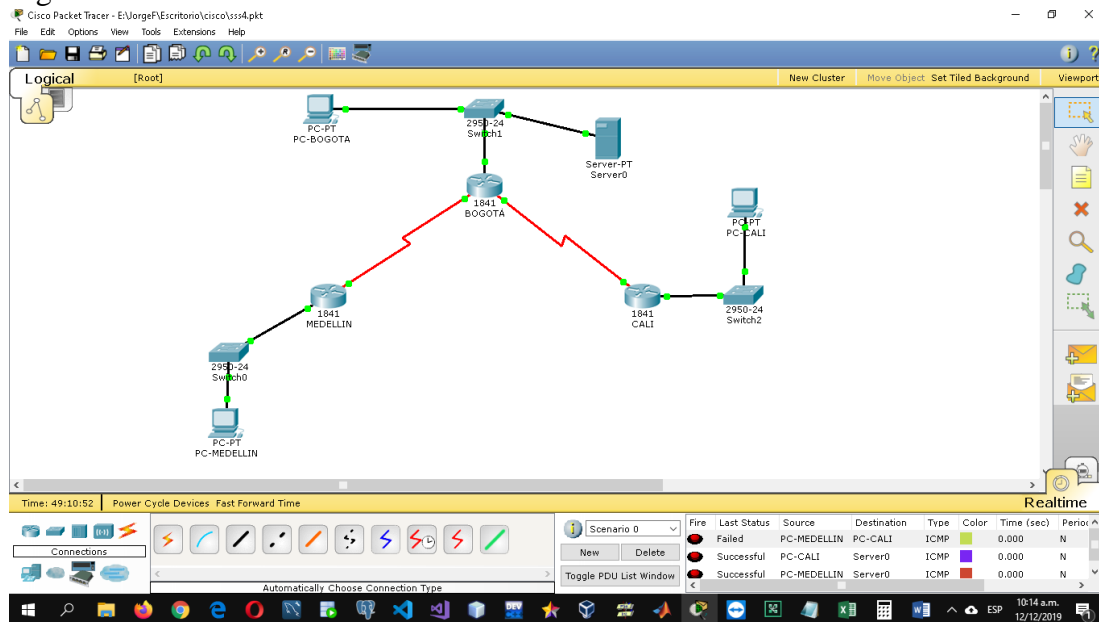


Fig. 24



Parte 5: Comprobación de la red instalada.

- a. Se debe probar que la configuración de las listas de acceso fue exitosa.
- b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	SUCCESSFULL
	WS_1	Router BOGOTA	SUCCESSFULL
TELNET	Servidor	Router CALI	SUCCESSFULL
	Servidor	Router MEDELLIN	SUCCESSFULL
	LAN del Router MEDELLIN	Router CALI	Connection timed out; remote host not responding
	LAN del Router CALI	Router CALI	SUCCESSFULL
TELNET	LAN del Router MEDELLIN	Router MEDELLIN	SUCCESSFULL
	LAN del Router CALI	Router MEDELLIN	Connection timed out; remote host not responding
PING	LAN del Router CALI	WS_1	FAILED
	LAN del Router MEDELLIN	WS_1	FAILED
	LAN del Router MEDELLIN	LAN del Router CALI	FAILED
	LAN del Router CALI	Servidor	SUCCESSFULL
	LAN del Router MEDELLIN	Servidor	SUCCESSFULL
PING	Servidor	LAN del Router MEDELLIN	SUCCESSFULL
	Servidor	LAN del Router CALI	SUCCESSFULL
	Router CALI	LAN del Router MEDELLIN	FAILED
	Router MEDELLIN	LAN del Router CALI	FAILED

Fig. 25

ESCENARIO 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

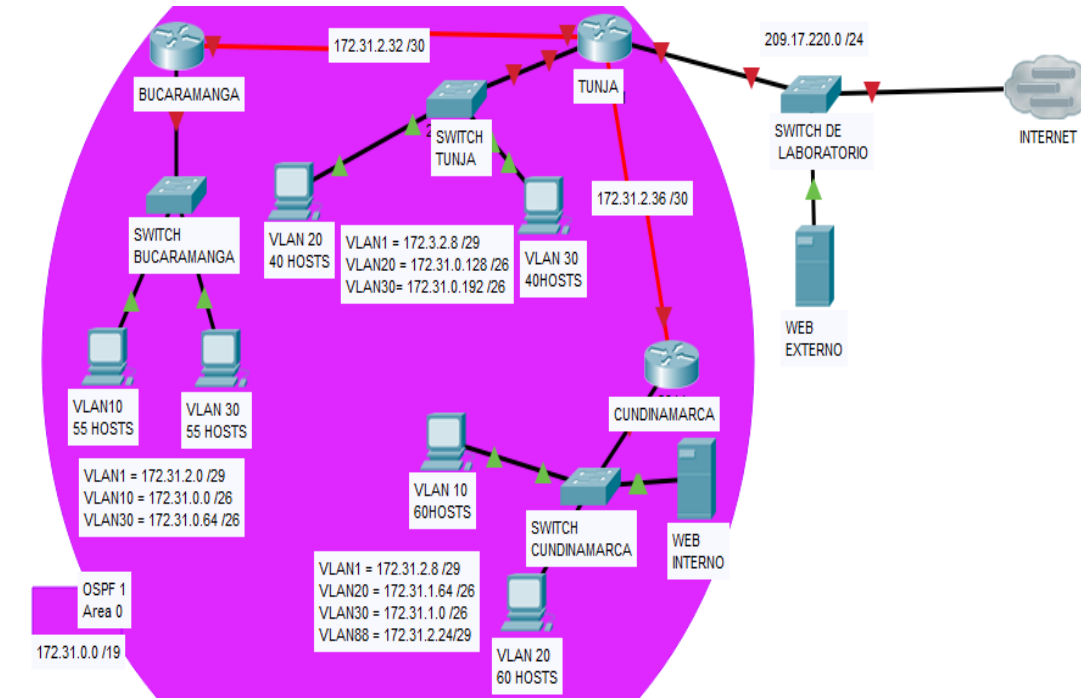


Fig. 26

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
 - Configuración básica.
 - Autenticación local con AAA.
 - Cifrado de contraseñas.
 - Un máximo de internos para acceder al router.
 - Máximo tiempo de acceso al detectar ataques.
 - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

Se realiza la configuración básica en donde se cambia el nombre de los router se configura la contraseña, las direcciones ip y el enrutamiento

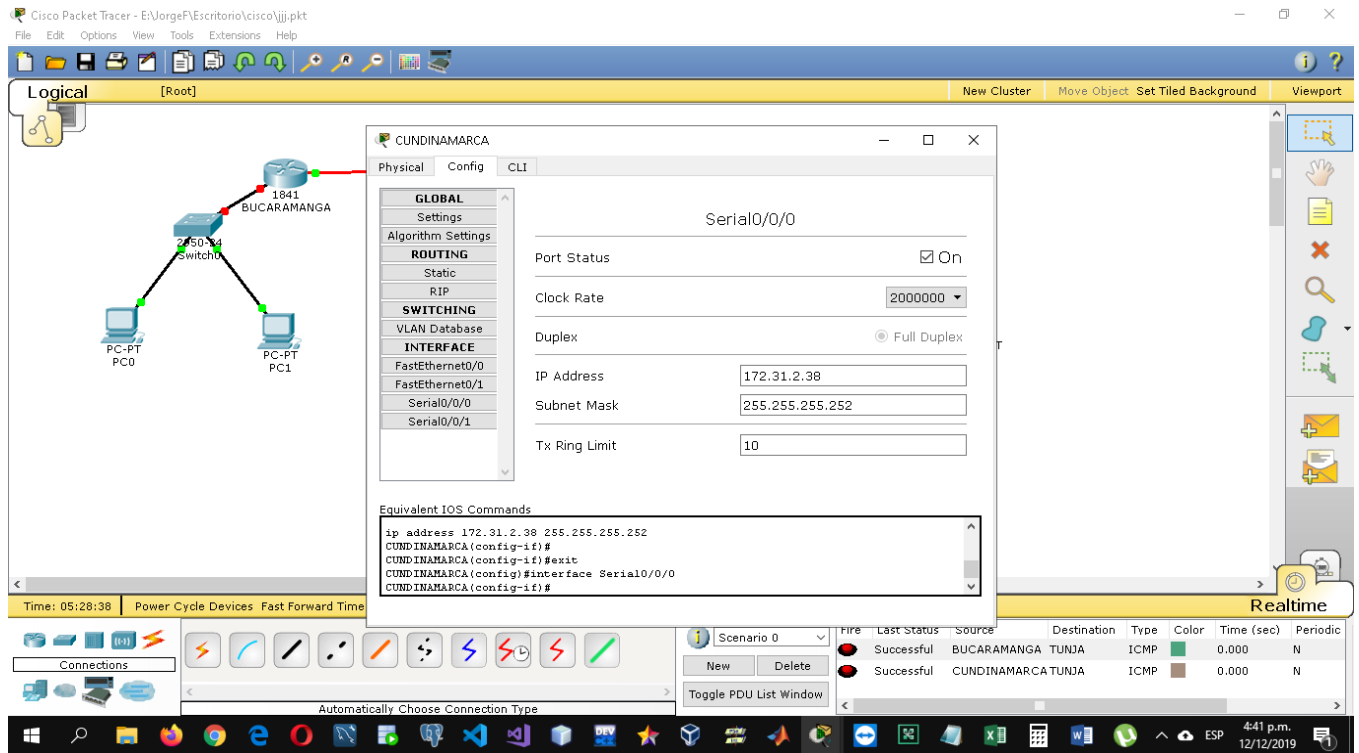


Fig. 27

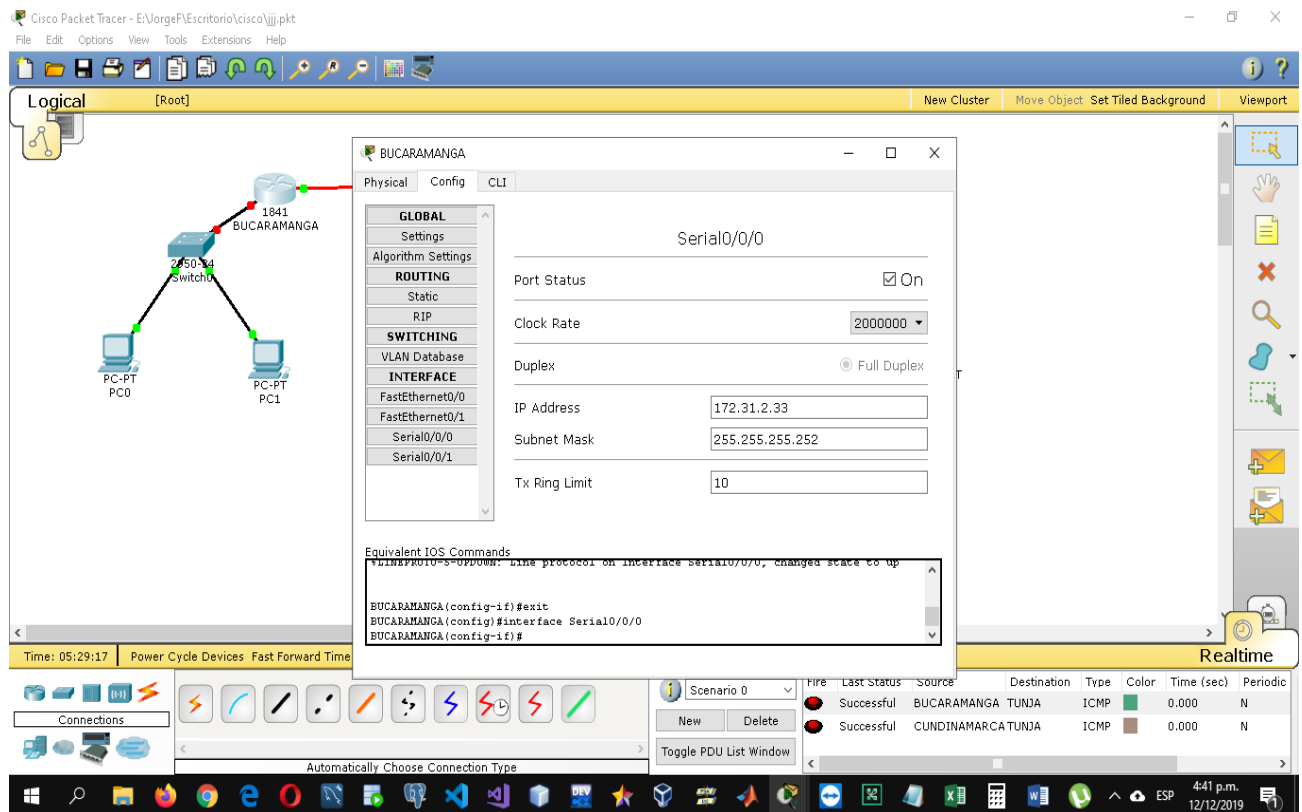
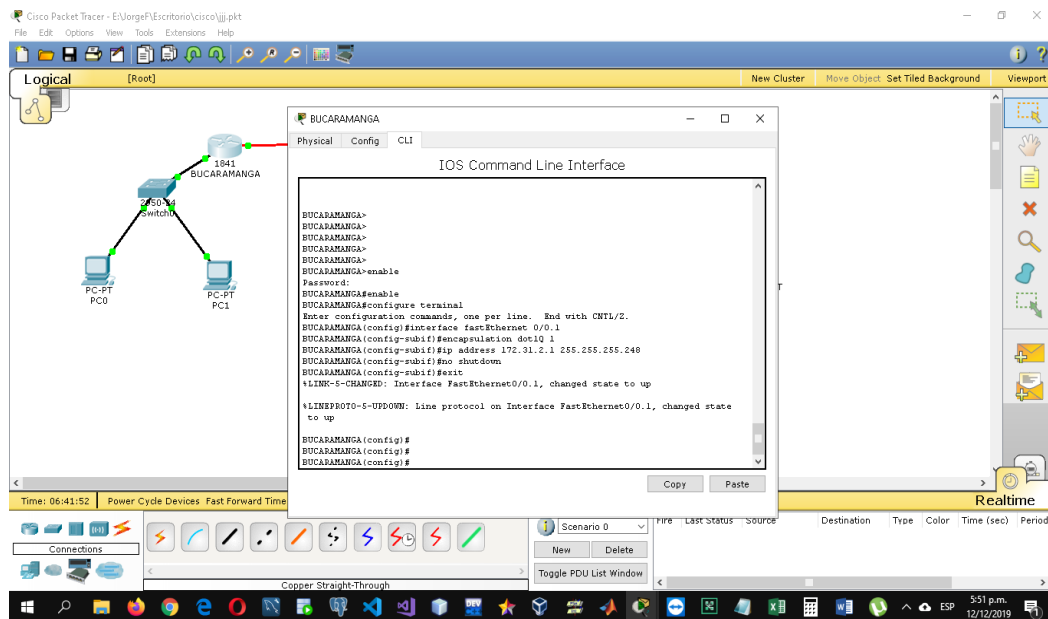
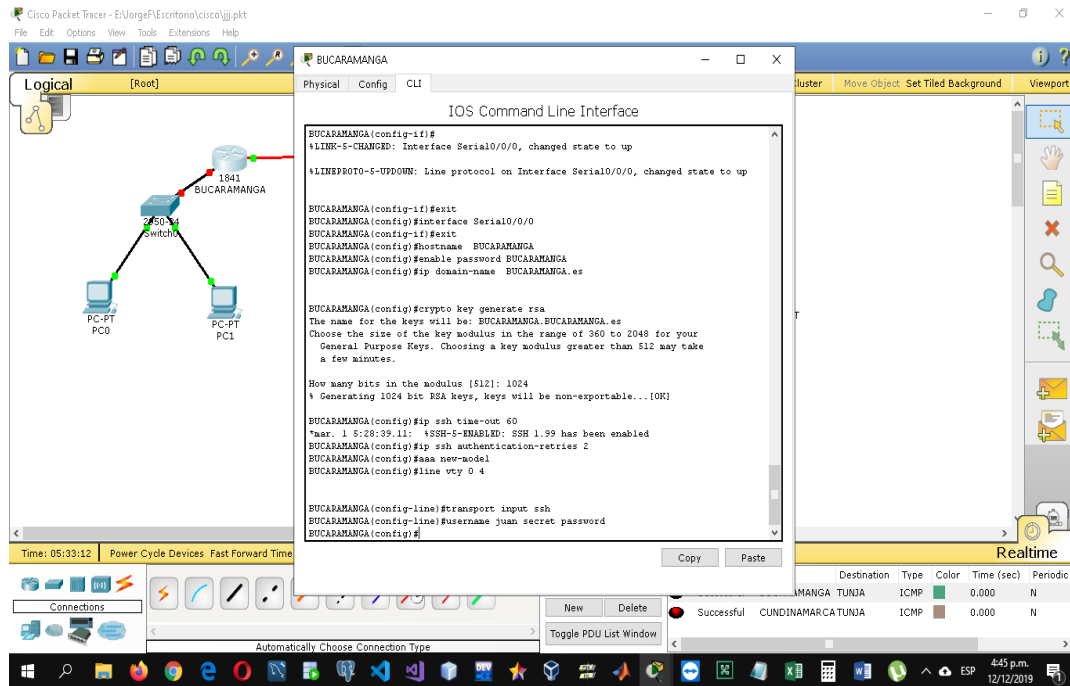


Fig. 28

Se hace la autenticación local con aaa se hace el cifrado de contraseña mediante rsa de 1024 bytes se establece un máximo de intentos de 2 y máximo de tiempo de 60 Fig. 29 y 30



Se copia la información de los routers en el servidor tftp

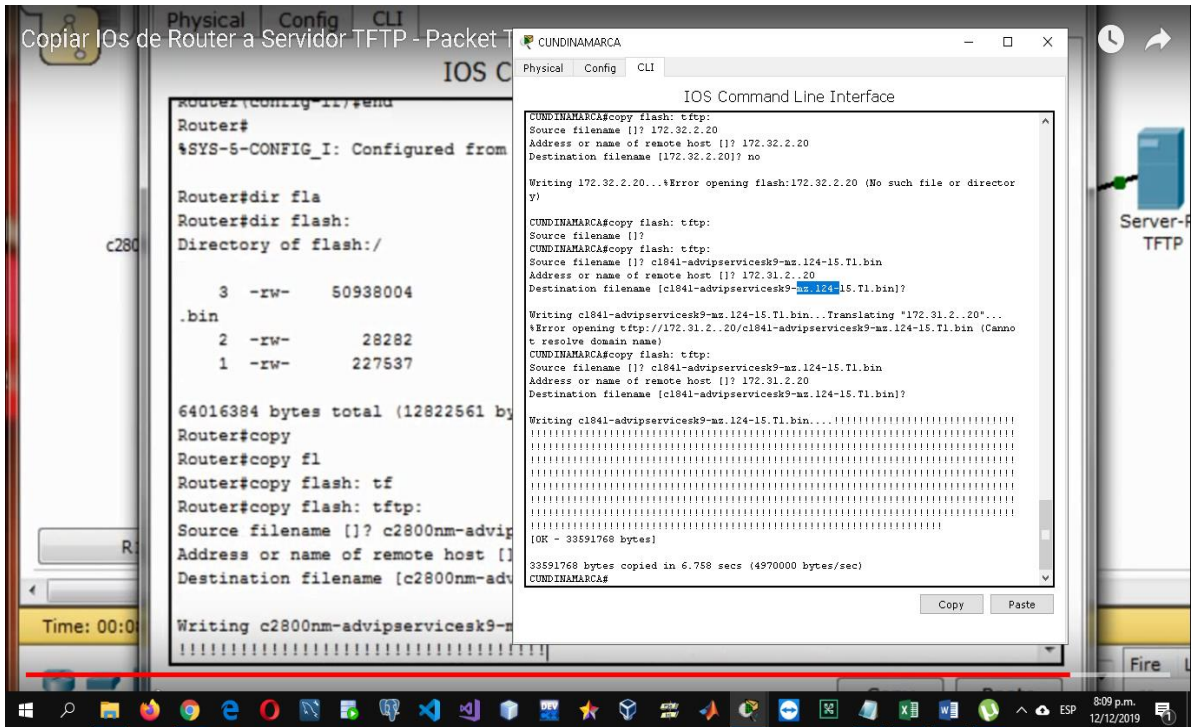
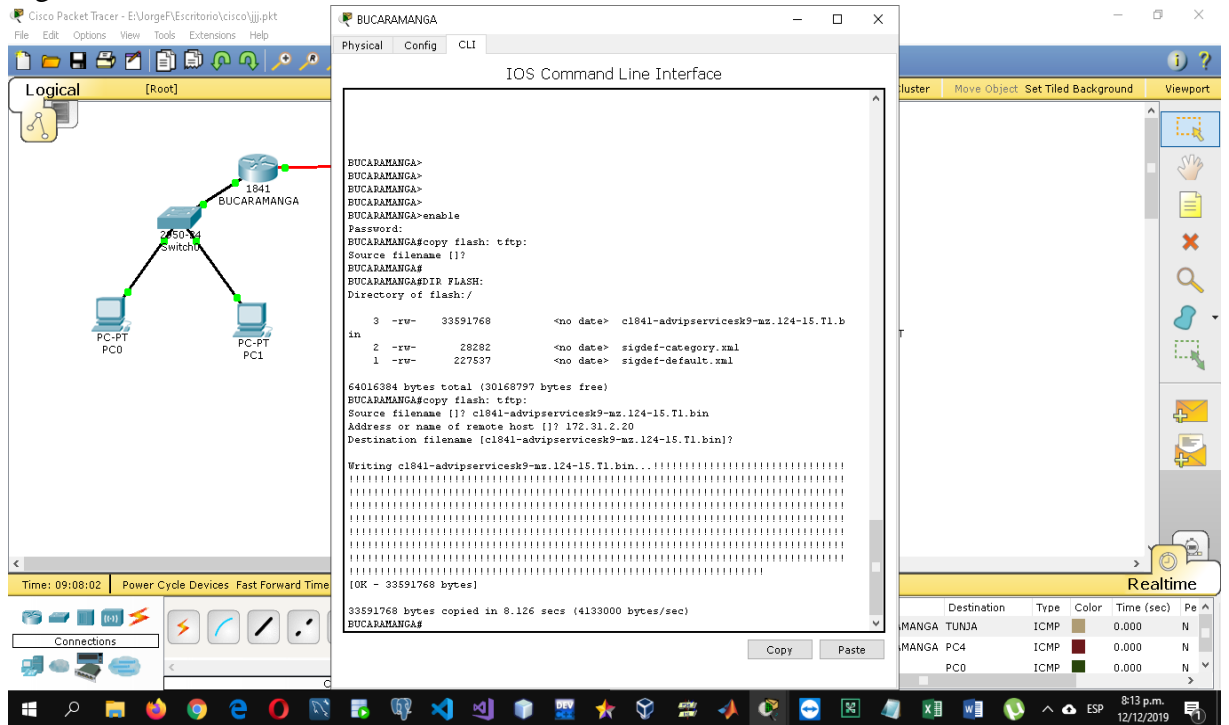


Fig. 31

Fig. 32



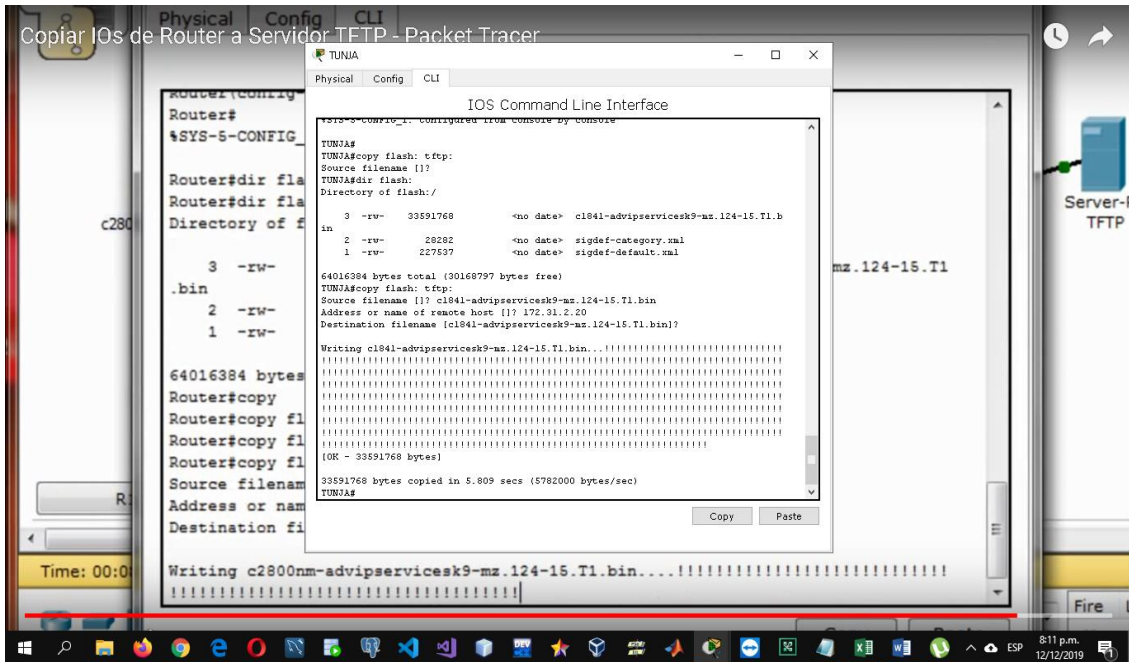
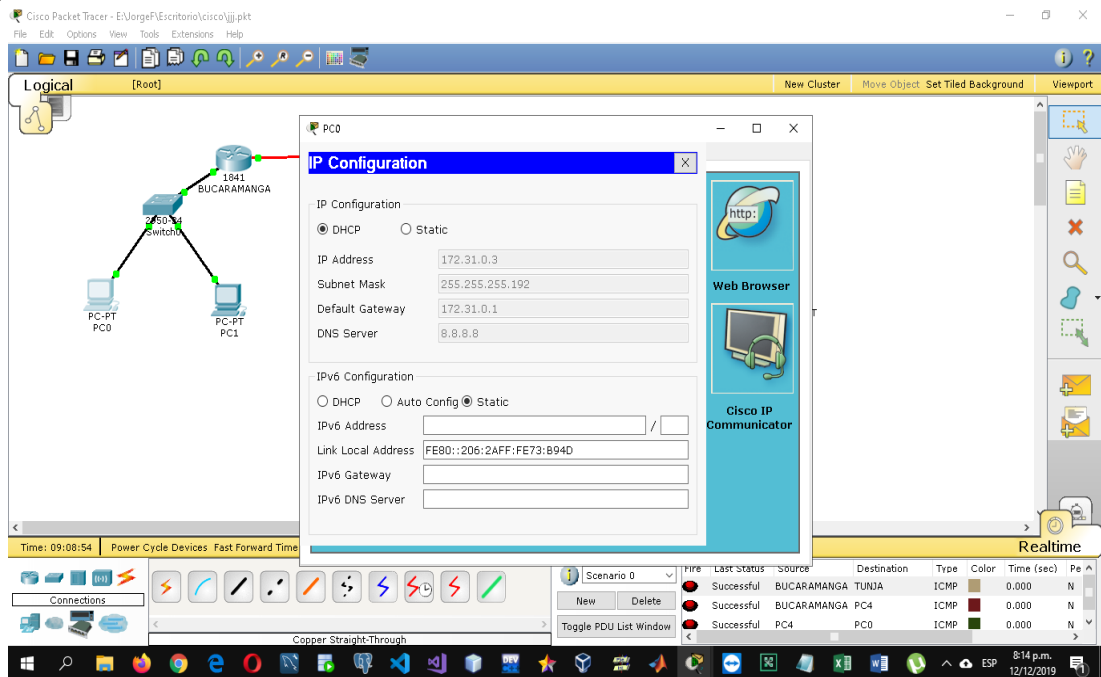


Fig. 33

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

Mediante el comando dhcp pool se crean los diferentes rangos de direcciones que se van a asignar mediante dhcp a las diferentes subinterfaces

Fig. 34



Se hace la verificación de que se haya realizado la traducción con éxito. Como podemos observar la ip se 172.31.1.67 fue traducida a la 209.17.220.1.26

Luego realizamos la configuración de la nat con sobrecarga (PAT) para ello creamos una access-list donde agregamos las direcciones que deseamos que sean traducidas, y luego la usamos en la configuración de la nat mas la interfaz de salida a internet y el comando overload. En las imágenes podemos ver la ip del pc y su respectiva traducción.

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram shows a router (TUNIA) connected to a switch (2450-14) and a cloud (Cloud-PT INTERNET). The router is also connected to two PCs (PC-PT BUCARAMANGA and PC-PT PC1). The main window displays the CLI of the TUNIA router with the following configuration and output:

```
TUNIA(config)#interface fa 0/1
TUNIA(config-if)#ip nat outside
TUNIA(config-if)#interface se 0/0/1
TUNIA(config-if)#ip nat inside
TUNIA(config-if)#exit
TUNIA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
TUNIA(config)#interface fa 0/1
TUNIA(config-if)#ip nat outside
TUNIA(config-if)#interface se 0/0/1
TUNIA(config-if)#ip nat inside
TUNIA(config-if)#exit
TUNIA(config)#show ip nat translations

+ Invalid input detected at '^' marker.

TUNIA(config)#exit
TUNIA#
+SYS-5-CONFIG_I: Configured from console by console

TUNIA#
TUNIA#show ip nat translations
Pro Inside global   Inside local   Outside local  Outside global
icmp 209.17.220.1:26 172.31.1.67:26 209.17.220.2:26 209.17.220.2:26
--- 209.17.220.1   172.31.1.67   ---            ---
TUNIA#
```

Fig. 37

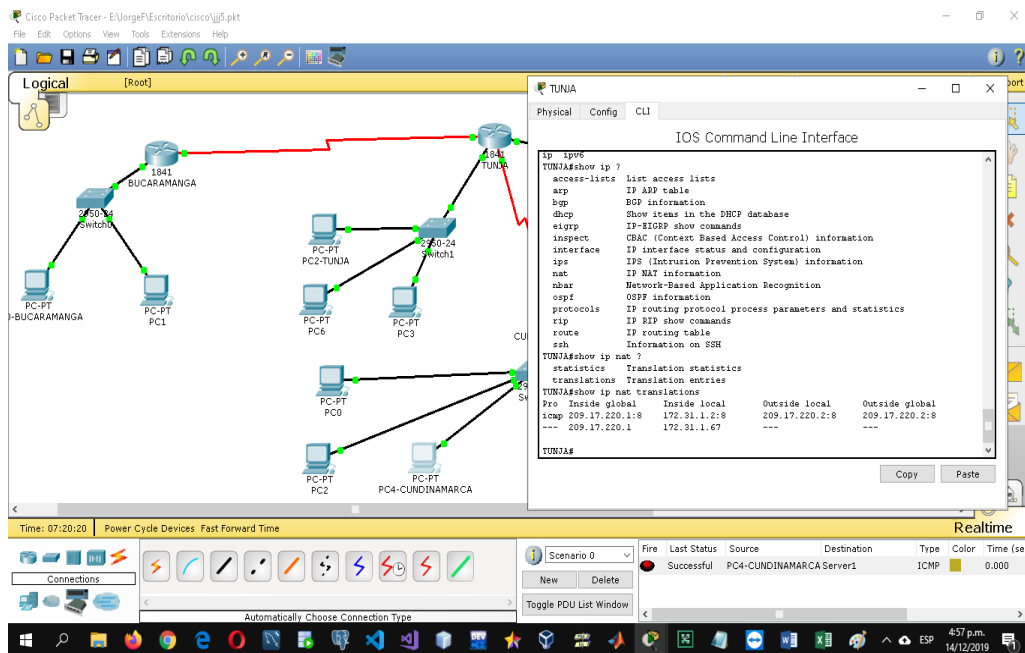


Fig. 38

4. El enrutamiento deberá tener autenticación.

Se agrega el enrutamiento con su respectiva autenticación mediante el algoritmo md5 con la contraseña CISCO

Fig. 39

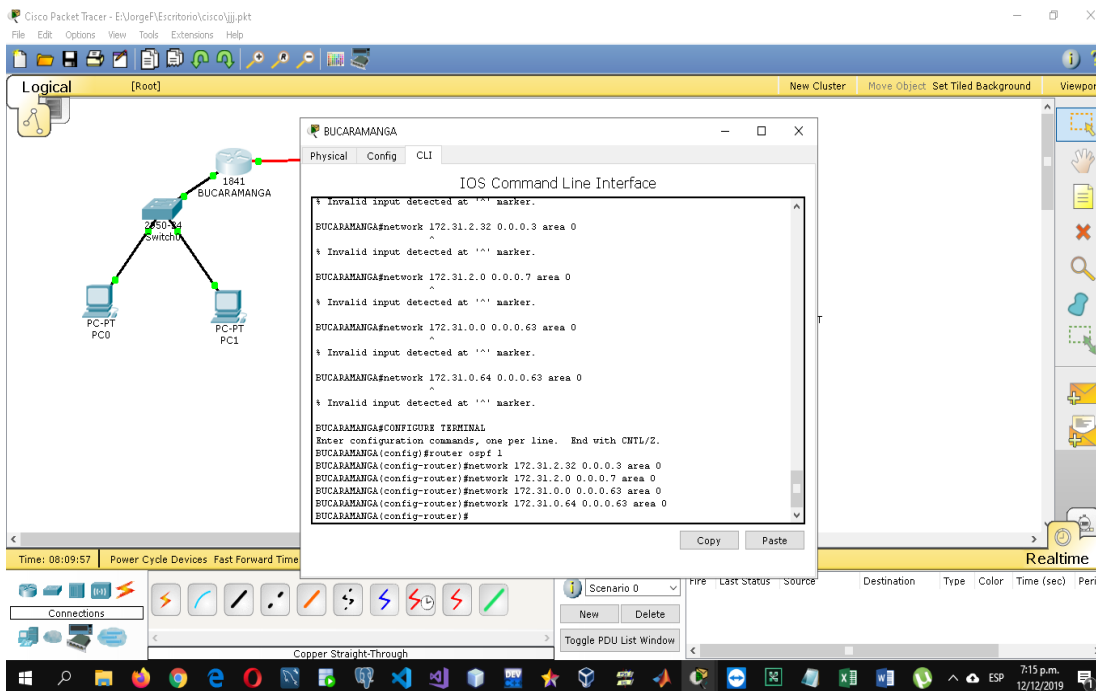


Fig. 40

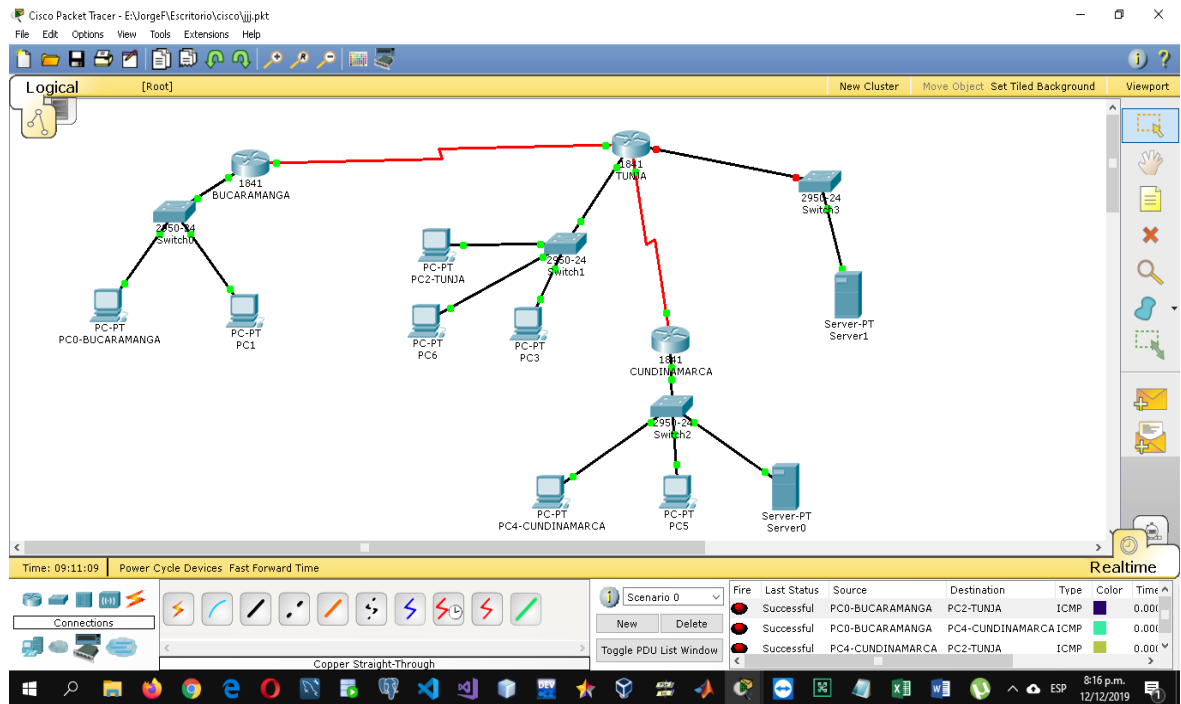
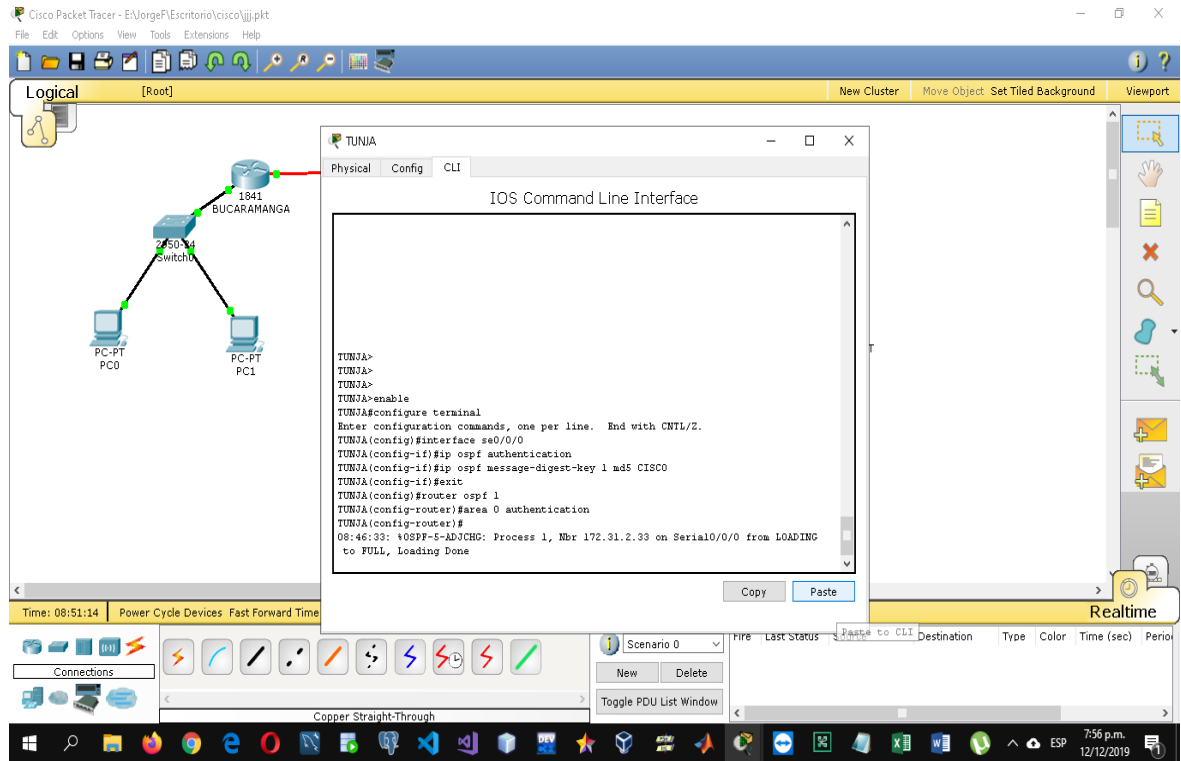


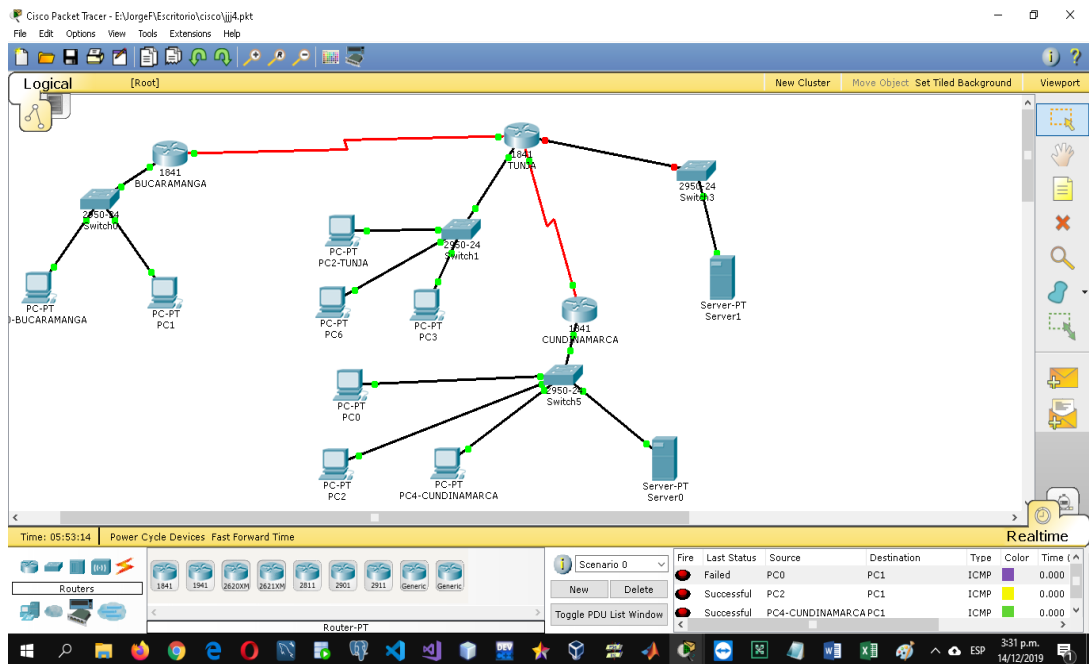
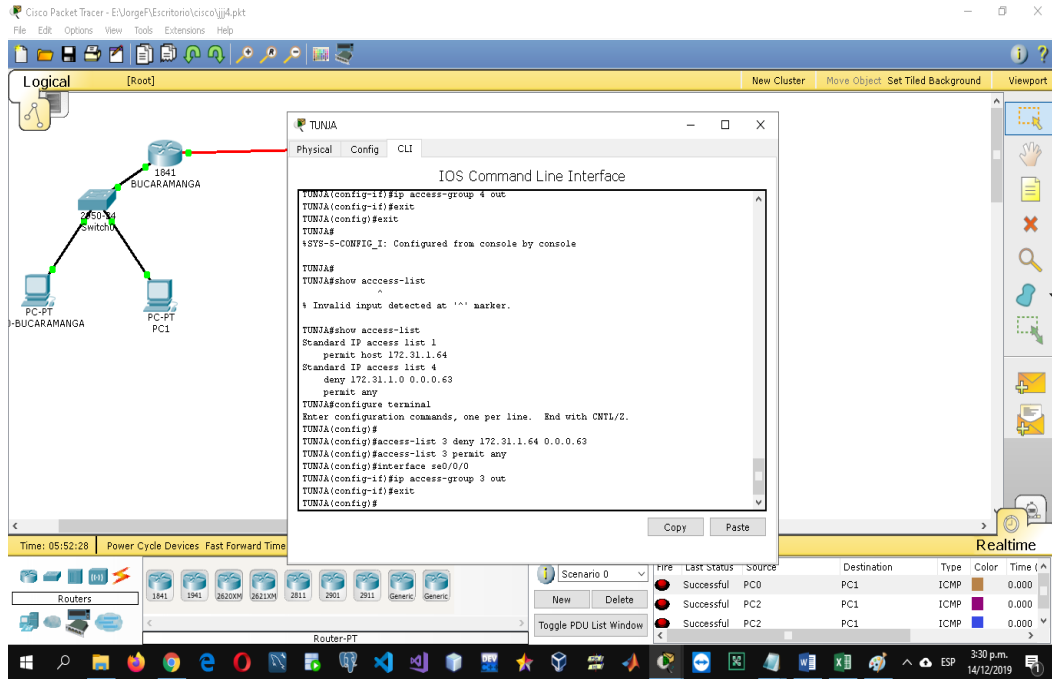
Fig. 41

4- Listas de control de acceso:

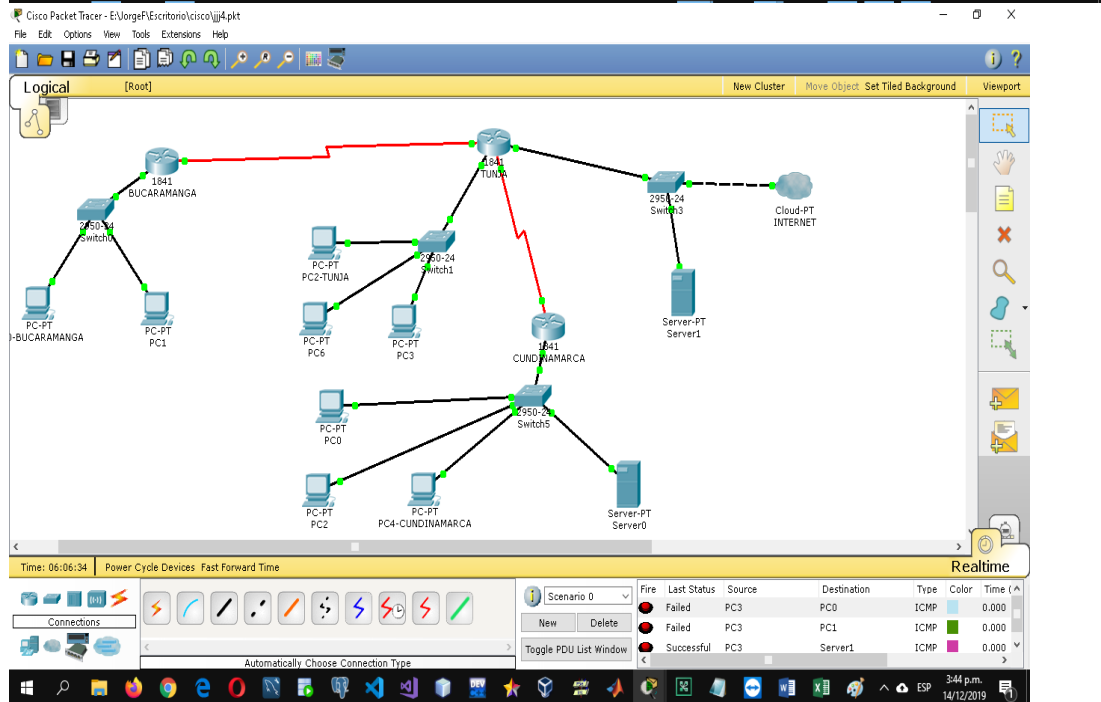
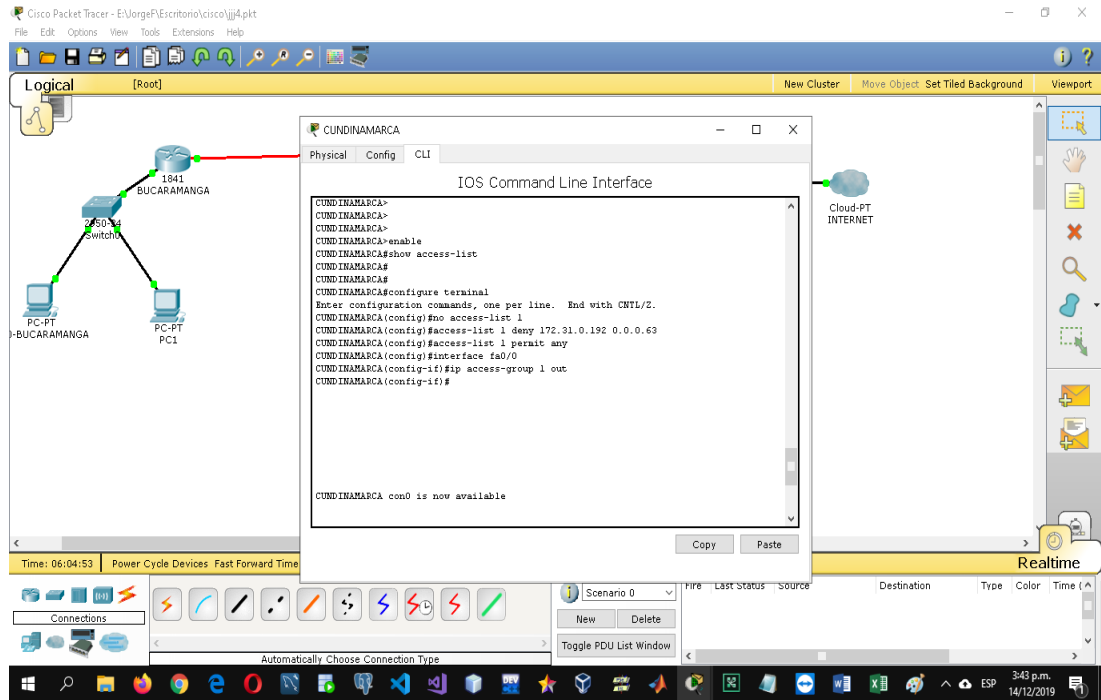
- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

Se crean las listas de control de acceso

Fig. 42 y 43



- Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
 - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
- Fig. 44 y 45



5- VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.
Se realiza la tabla de enrutamiento VLSM teniendo en cuenta la dirección dada

no	host	host encontrados	direccion de red	mascara	mascara decimal punteada
1	55	62	172.31.0.0	26	255.255.255.192
2	55	62	172.31.0.64	26	255.255.255.192
3	40	62	172.31.0.128	26	255.255.255.192
4	40	62	172.31.0.192	26	255.255.255.192
5	60	62	172.31.1.0	26	255.255.255.192
6	60	62	172.31.1.64	26	255.255.255.192
7			172.31.1.128		
8			172.31.1.192		
9	6	6	172.31.2.0	29	255.255.255.248
10	6	6	172.31.2.8	29	255.255.255.248
11	6	6	172.31.2.16	29	255.255.255.248
12			172.31.2.24		
13	2	2	172.31.2.32	30	255.255.255.252
14	2	2	172.31.2.36	30	255.255.255.252

Fig. 46

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

Luego de configurar los pools de direcciones en los router de Bucaramanga y Cundinamarca ingresamos en el modo de configuración del router Tunja, seguidamente entramos en la interfaz por donde vamos a permitir el paso del dhcp que en este caso serían las interfaces y subinterfaces fa0/0, fa0/0.20 y fa0/0.30 para ingresar el comando ip address-helper + la dirección del router que va a proveer el pool de direcciones dhcp

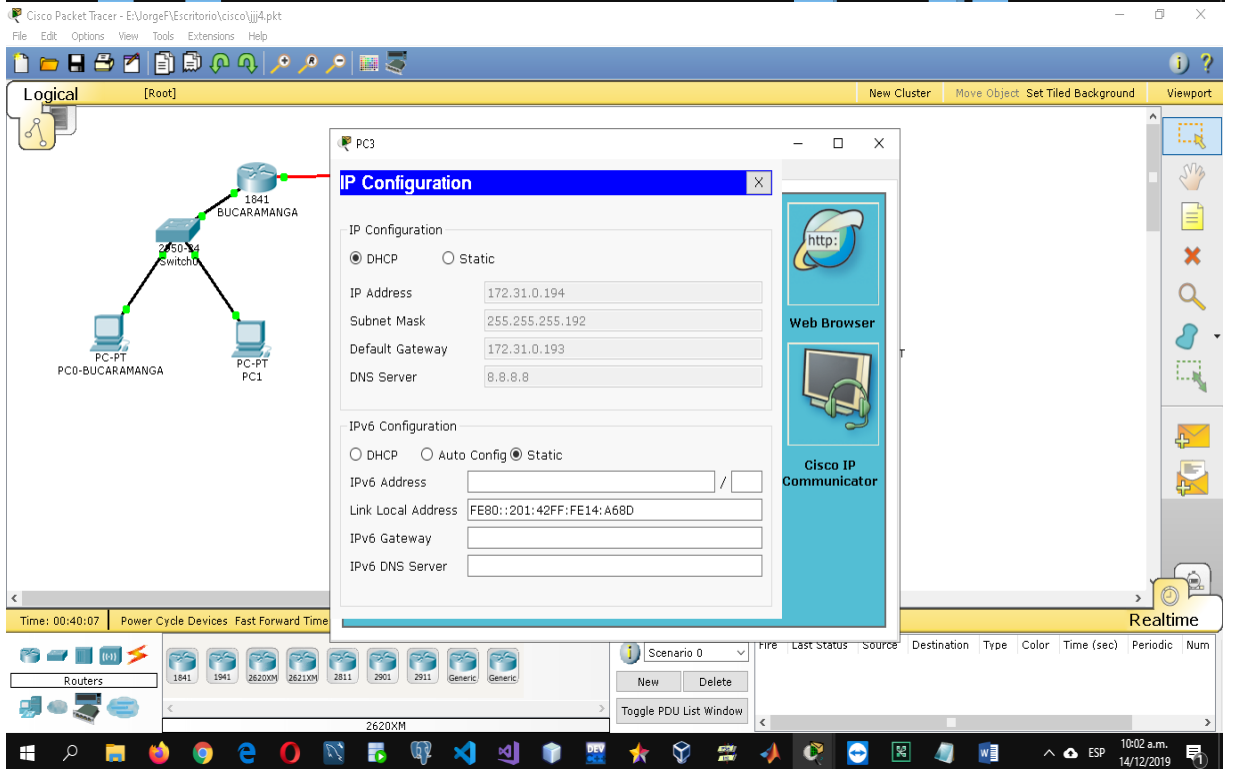
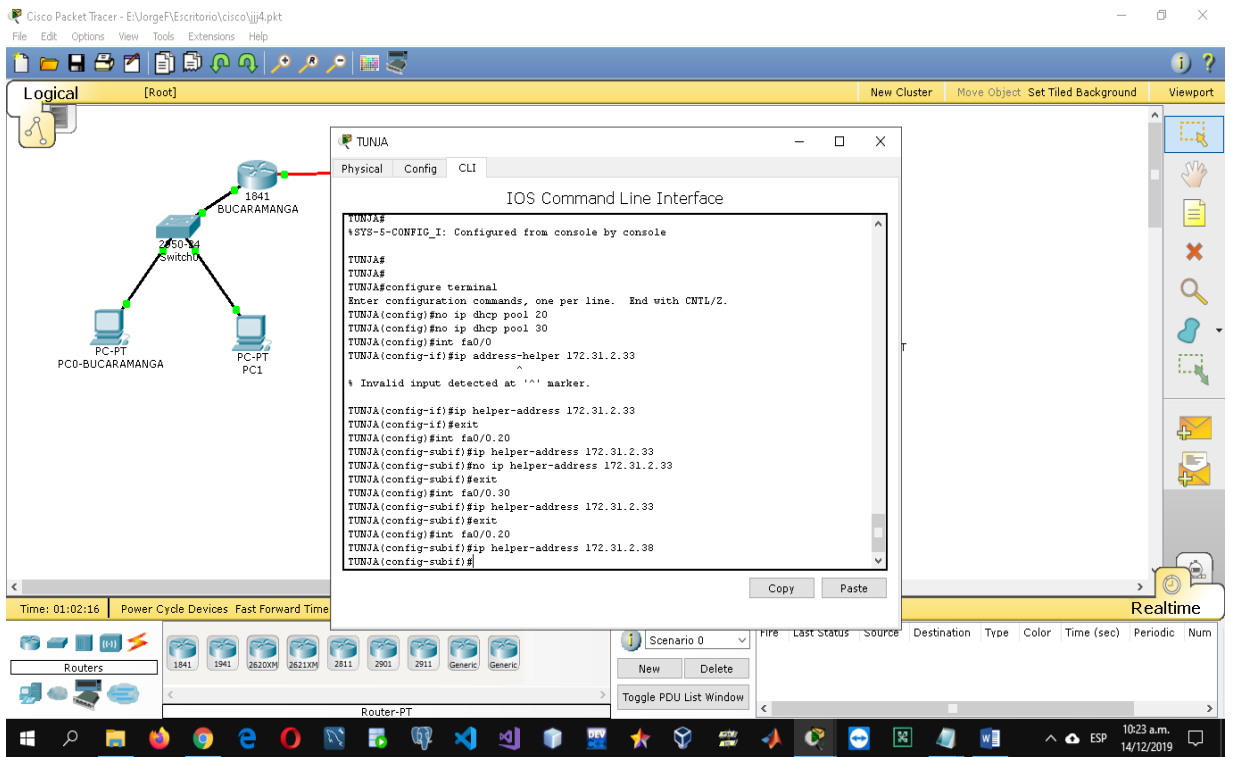


Fig. 47 y 48

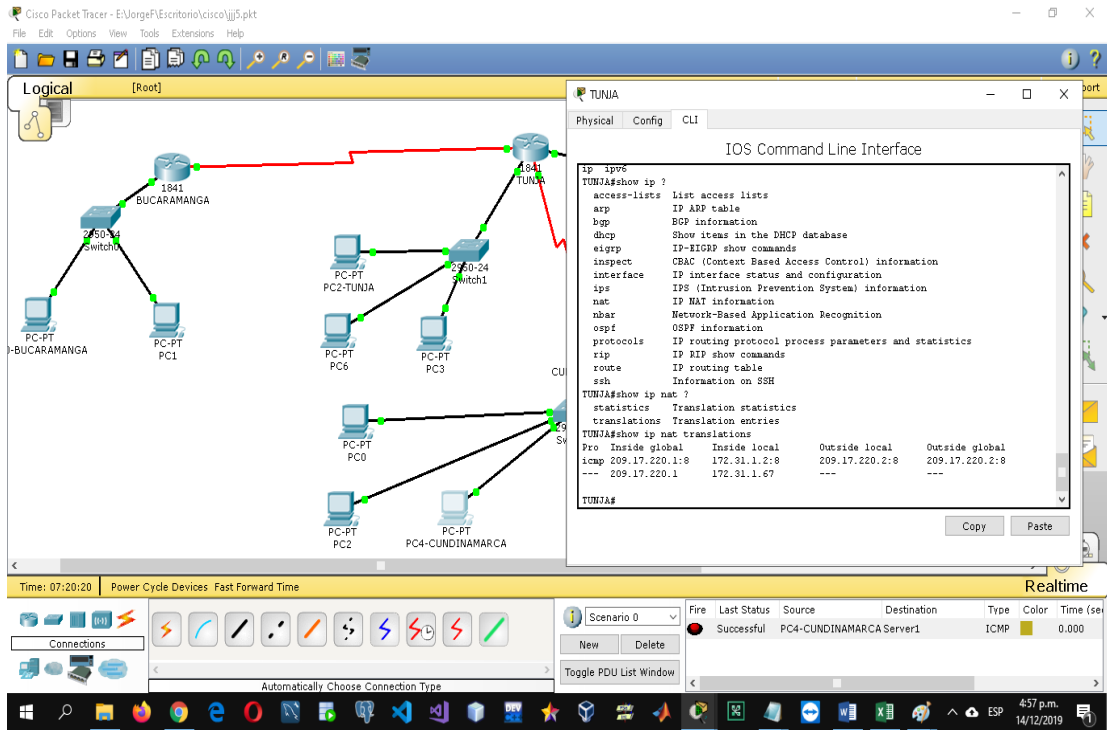
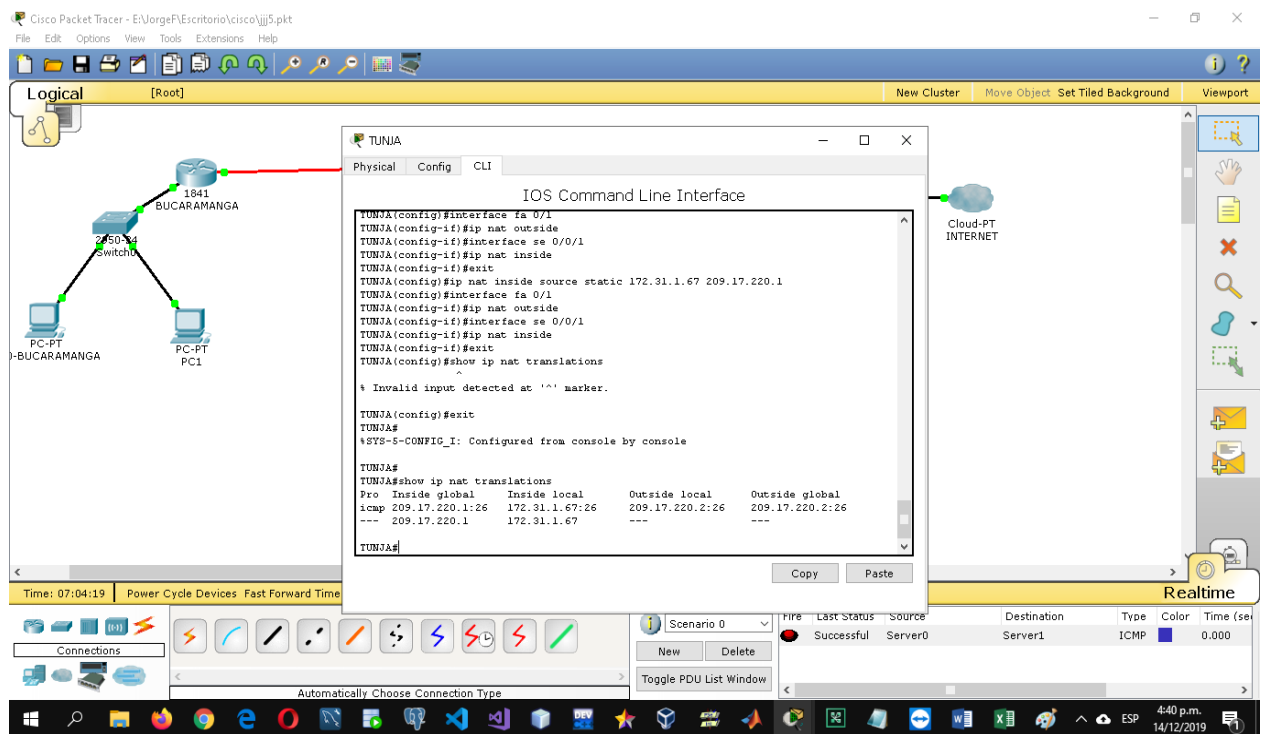


Fig. 51 y 52

- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual



CONCLUSION

Durante el desarrollo de las actividades se han aplicado los conocimientos adquiridos durante el diplomado de profundización CISCO, con la aplicación del modelo OSI y el análisis de dos escenarios que han sido planteados, nosotros como estudiantes identificamos la problemática y planteamos soluciones para buscar la configuración óptima a las situaciones planteadas utilizando SUBNETTING, NAT, protocolo de enrutamiento **EIGRP**, OSPF, VLAN, etc.

Como profesionales debemos tomar decisiones relacionadas a los planteamientos que se requieren en cada situación que se puede presentar y resulta muy importante conocer los diferentes mecanismos que se pueden implementar en una red para una óptima ejecución teniendo muy en cuenta los costos de implementación, la eficiencia, la escalabilidad y la seguridad.

BIBLIOGRAFIA

<https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ripv2-con-packet-tracer>

https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xen-3se/3850/dhcp-xe-3se-3850-book/config-dhcp-server.html

https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/200726-Configure-NAT-to-Enable-Communication-Between-Networks.html

<http://www.cerecon.frm.utn.edu.ar/archives/Libro-Dispositivos-y-protocolos-de-Redes-LAN-y-WAN.pdf>

<https://cdigital.uv.mx/bitstream/handle/123456789/41559/OrtizJuarezMiguel.pdf?sequence=1&isAllowed=y>

<http://repositorio.ug.edu.ec/bitstream/redug/41931/1/ESTUDIO%20Y%20ANALISIS%20DE%20FACTIBILIDAD%20DE%20UN%20NUEVO%20PROCOLO%20PARA%20LA%20EMPRESA%20AKROS%20GUAYAQUIL-FREDDY%20V.pdf>