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

**OMAR DARIO PEDRAZA VALLE**

**GIOVANNI ALBERTO BRACHO**
**GRUPO_203092_21**
**Ingeniero de sistemas**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**PROGRAMA DE INGENIERÍA DE SISTEMAS**
**VALLEDUPAR, CESAR**
**2019**

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

**GIOVANNI ALBERTO BRACHO**
**GRUPO_203092_21**
**Ingeniero de sistemas**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**PROGRAMA DE INGENIERÍA DE SISTEMAS**
**VALLEDUPAR, CESAR**
**2019**

## TABLA DE CONTENIDO

## RESUMEN

La temática desarrollada en el transcurso de la carrera de ingeniería de sistemas , el diplomado de profundización en CISCO y la solución a los escenarios propuestos en la guía de actividades , me ayudo a fortalecerme al momento de realizar una instalación de dispositivos, configuración de una red local o empresarial , administrar las distintas redes que en el futuro se puedan presentar y aún más significativo la manera de atesorar cada uno de los problemas en redes pequeñas y empresariales como por ejemplo LAN y WAN, durante el desarrollo del trabajo en conjunto apoyado firmemente por profesionales y especialistas del área, con el fin de optimizar cada una de las destrezas adquiridas y de trabajar modo autónomo en el esquema de redes. Esta actividad logro afianzar mis conocimientos sobre protocolos de enrutamiento avanzados como IGRP, RIP, OSPF, se utilizó tanto el direccionamiento IPV4 e IPV6, con ellos se enfatizó en la seguridad. Una temática que es suma importancia la cual día a día es importante a momento del diseño de una red. El presente trabajo validad estas habilidades y nos da una visión más clara de lo que nos enfrentaremos, conjuntamente es la manera de evaluar nuestros conocimientos obtenidos durante el desarrollo de las unidades que forman el curso, así como la formación autónoma que el diplomado tiene como requerimiento.

## ABSTRACT

The theme developed in the course of the systems engineering career, the diploma of deepening in CISCO and the solution to the scenarios proposed in the activity guide, helped me to strengthen myself when performing a device installation, configuration of a network local or business, manage the different networks that may arise in the future and even more significant how to treasure each of the problems in small and business networks such as LAN and WAN, during the development of joint work strongly supported by professionals and specialists in the area, in order to optimize each of the acquired skills and work independently in the network scheme. This activity was able to strengthen my knowledge about advanced routing protocols such as IGRP, RIP, OSPF, IPV4 and IPV6 addressing was used, with them security was emphasized. A theme that is very important which day by day is important when designing a network. The present work validates these skills and gives us a clearer vision of what we will face, together it is the way to evaluate our knowledge obtained during the development of the units that form the course, as well as the autonomous training that the diploma has as a requirement .

## INTRODUCCIÓN

En el período de estudio y desarrollo de esta prueba de habilidades final se aplicara todo lo trabajado en el semestre del Diplomado, por lo que se empleará enrutamiento, cada uno de los parámetros de seguridad y diferentes accesos de dispositivos en la red, implementación DHCP, NAT, Asignación del protocolo de enrutamiento EIGRP. etc.

Desarrollando esta actividad lograremos determinar la capacidad de cumplir con un informe demostrando paso a paso de como brindar una solución a cada uno de los escenarios que veremos. son totalmente distintos y que estos están basados en problemas habituales en nuestro ámbito laboral ,los cuales tienen mucha relación con las redes y telecomunicaciones.

# OBJETIVOS

## OBJETIVO GENERAL

Se Efectúan destrezas alcanzadas en las prácticas que se vieron anteriormente, y se estudian cada una de las teorías para identificar y aplicar una solución a unos escenarios donde se estudian casos de Networking basados en nuestro diario vivir.

## OBJETIVOS ESPECÍFICOS

- Configurar dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en los Router y demás políticas necesarias
- Identificar que dispositivos utilizar para la construcción de una topología de red

## Descripción de escenarios propuestos para la prueba de habilidades

### 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.

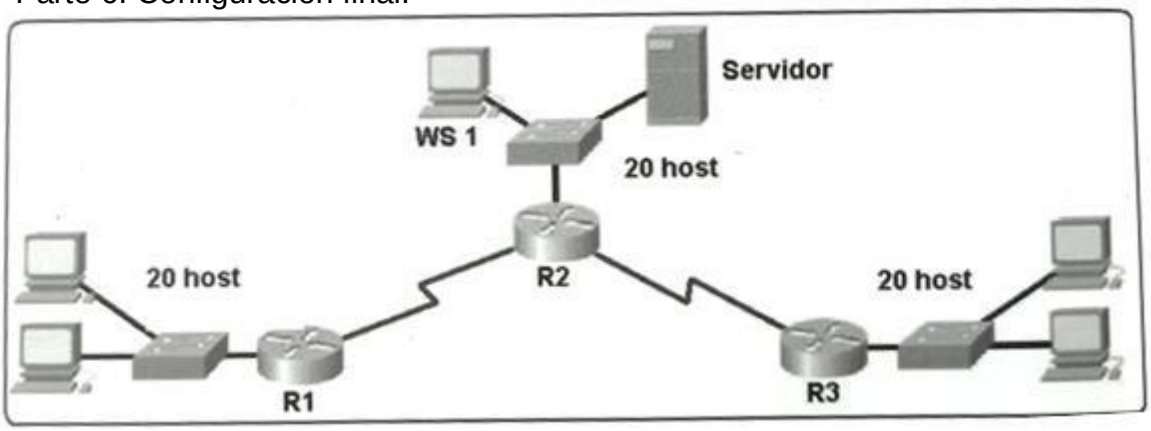
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

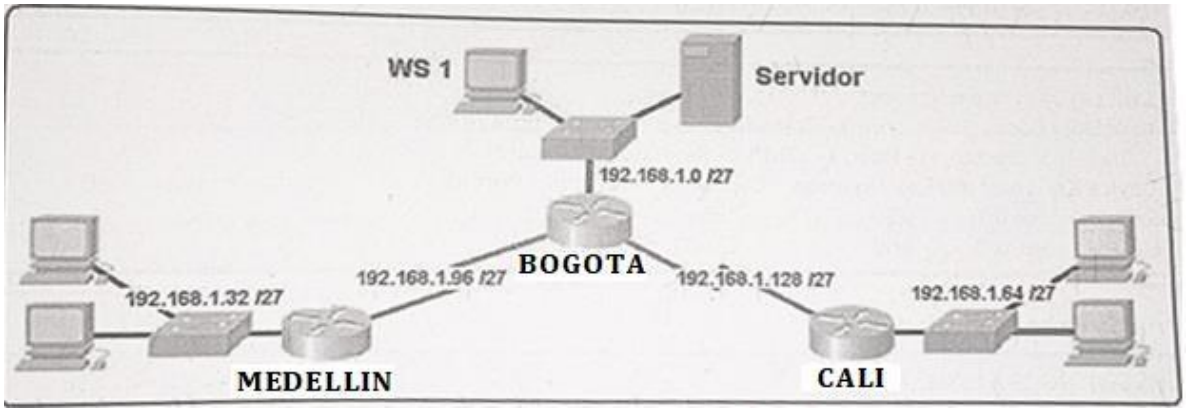
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.






**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 fisica de los equipos con base en la topología de red

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

**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.
b. Asignar una dirección IP a la red.

**Parte 2: Configuración Básica.**

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

| | 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 |

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.
c. Verificar el balanceo de carga que presentan los routers.
d. Realizar un diagnóstico de vecinos uando el comando cdp.
e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

**Parte 3: Configuración de Enrutamiento.**

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
b. Verificar si existe vecindad con los routers configurados con EIGRP.
c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.
d. 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.

**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:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.
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.
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.

**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.

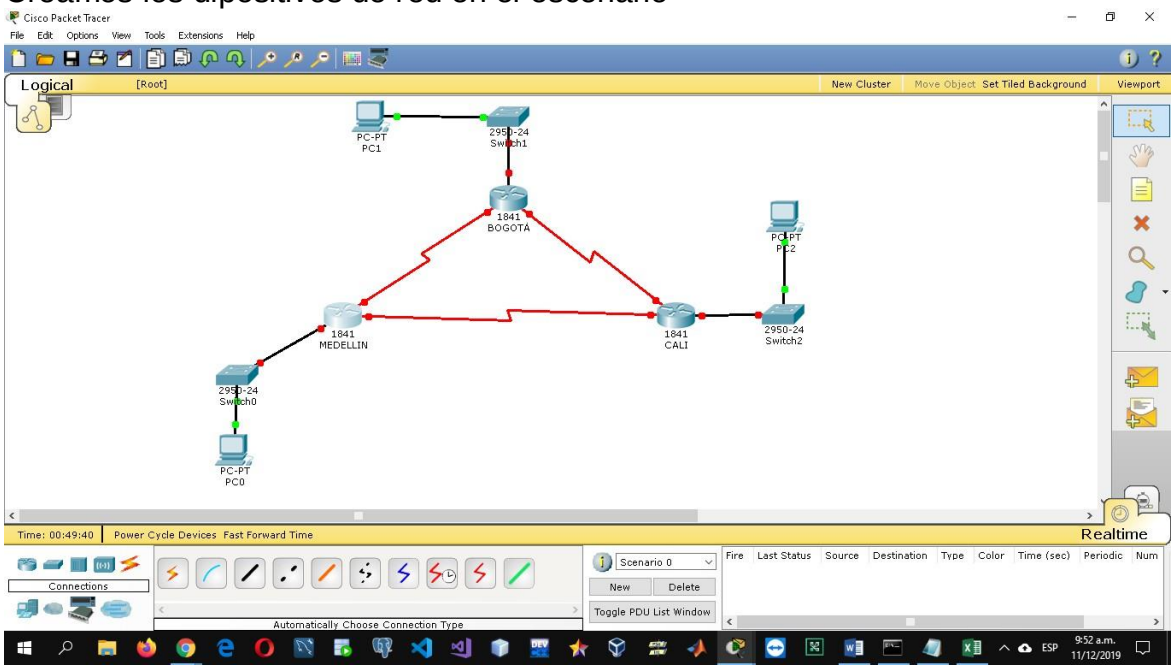
| | ORIGEN | DESTINO | RESULTADO |
|---|---|---|---|
| TELNET | Router MEDELLIN | Router CALI | |
| | WS_1 | Router BOGOTA | |
| | Servidor | Router CALI | |
| | Servidor | Router MEDELLIN | |
| | LAN del Router MEDELLIN | Router CALI | |
| TELNET | LAN del Router CALI | Router CALI | |
| | LAN del Router MEDELLIN | Router MEDELLIN | |
| | LAN del Router CALI | Router MEDELLIN | |
| | LAN del Router CALI | WS_1 | |
| PING | LAN del Router MEDELLIN | WS_1 | |
| | LAN del Router MEDELLIN | LAN del Router CALI | |
| | LAN del Router CALI | Servidor | |
| | LAN del Router MEDELLIN | Servidor | |
| PING | Servidor | LAN del Router MEDELLIN | |
| | Servidor | LAN del Router CALI | |
| | Router CALI | LAN del Router MEDELLIN | |
| | Router MEDELLIN | LAN del Router CALI | |

## 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).OK!
- Realizar la conexión fisica de los equipos con base en la topología de red.OK!

Configurar la topología de red, de acuerdo con las siguientes especificaciones.
Creamos los dipositivos de red en el escenario



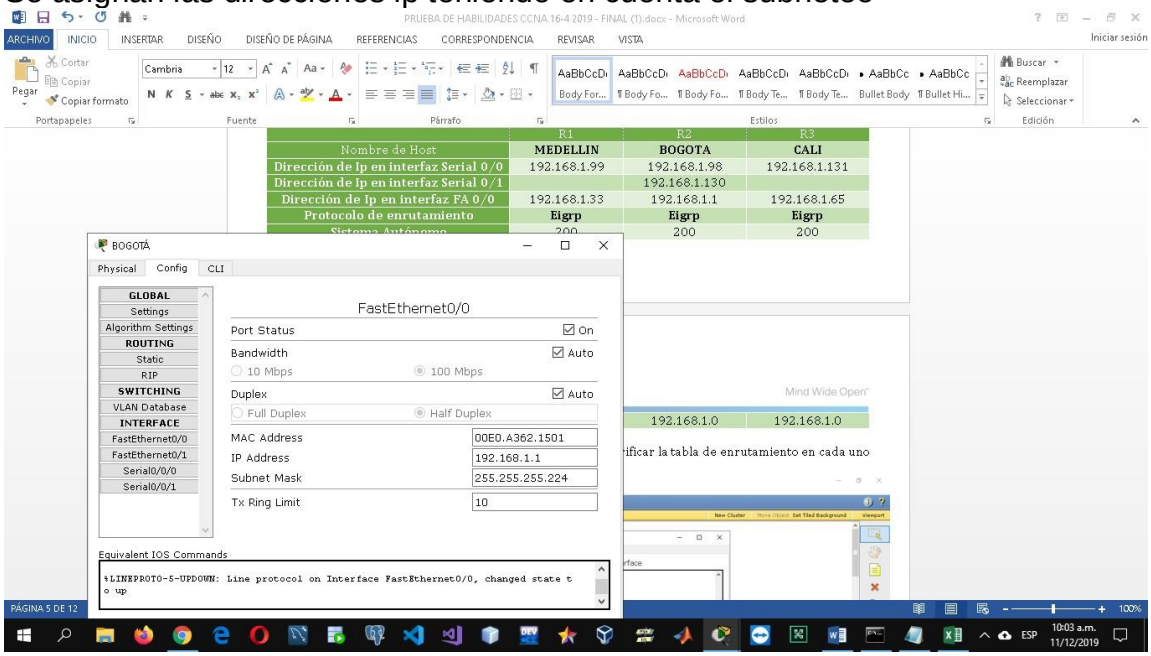

### Parte 1: Asignación de direcciones IP:

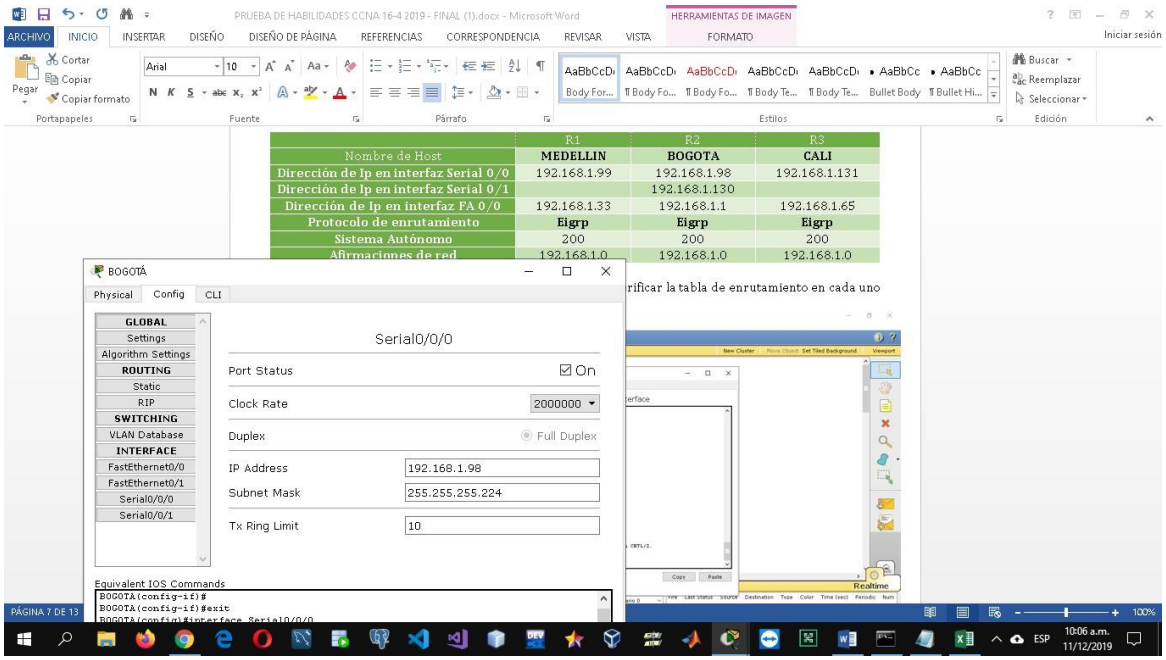
c. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.

Se realiza el respectivo subneteo

| Formula | | bit necesarios | redes totales |
|---|---|---|---|
| 2^n | subredes requeridas 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 |

d. Asignar una dirección IP a la red.
Se asignan las direcciones ip teniendo en cuenta el subneteo

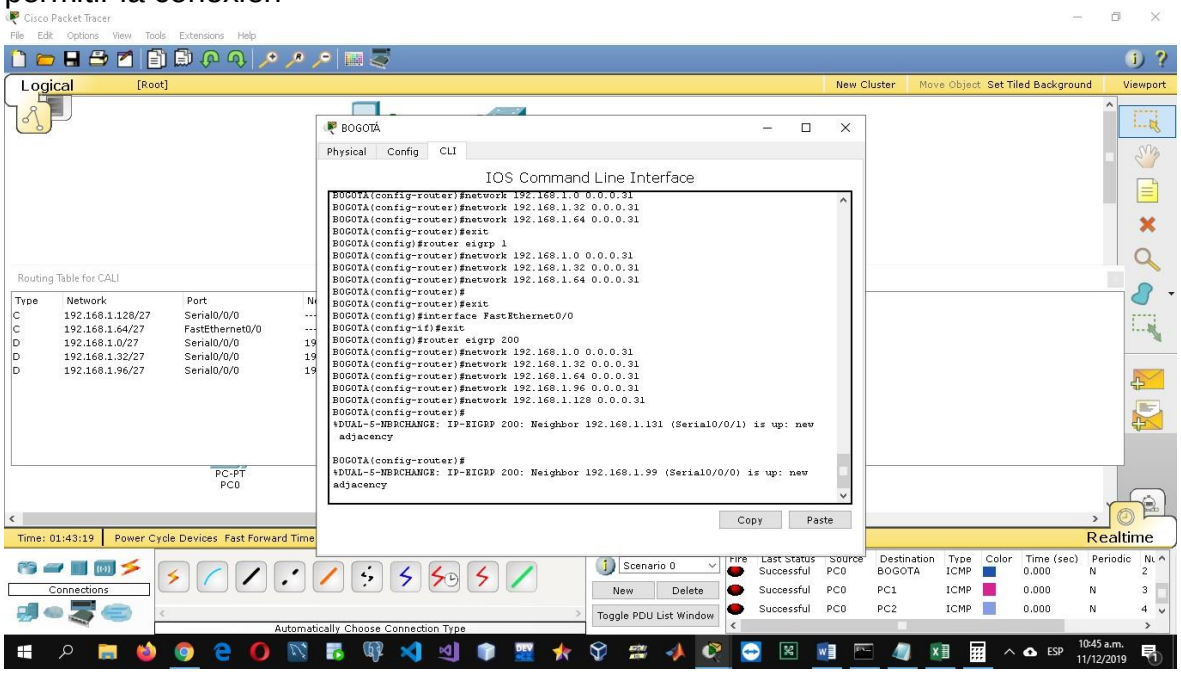





## Parte 2: Configuración Básica.

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

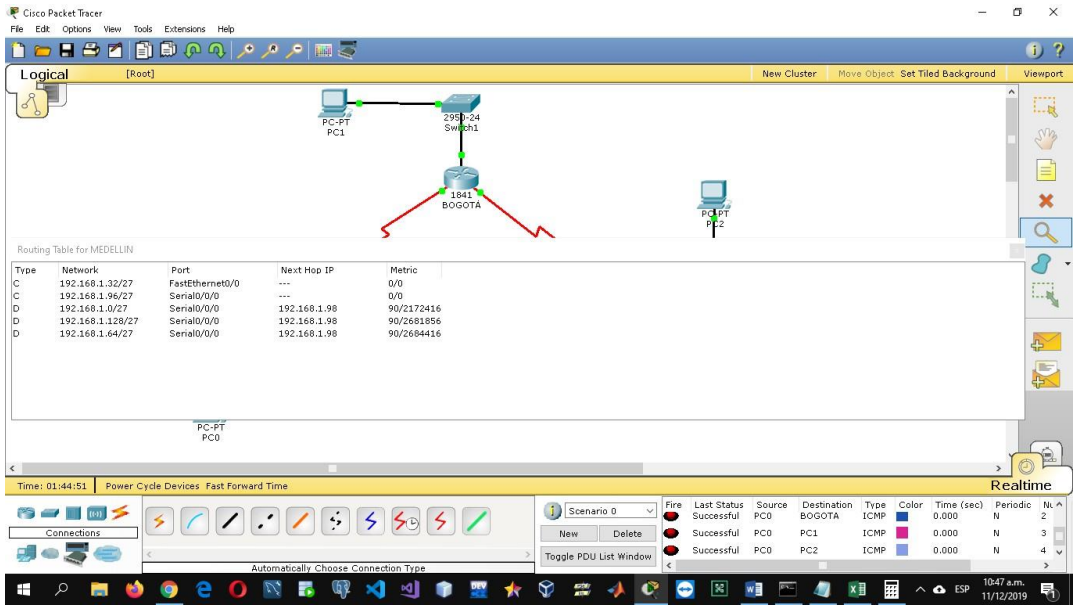
Se asignan todas las direcciones ip y se agrega el protocolo de enrutamiento para permitir la conexion

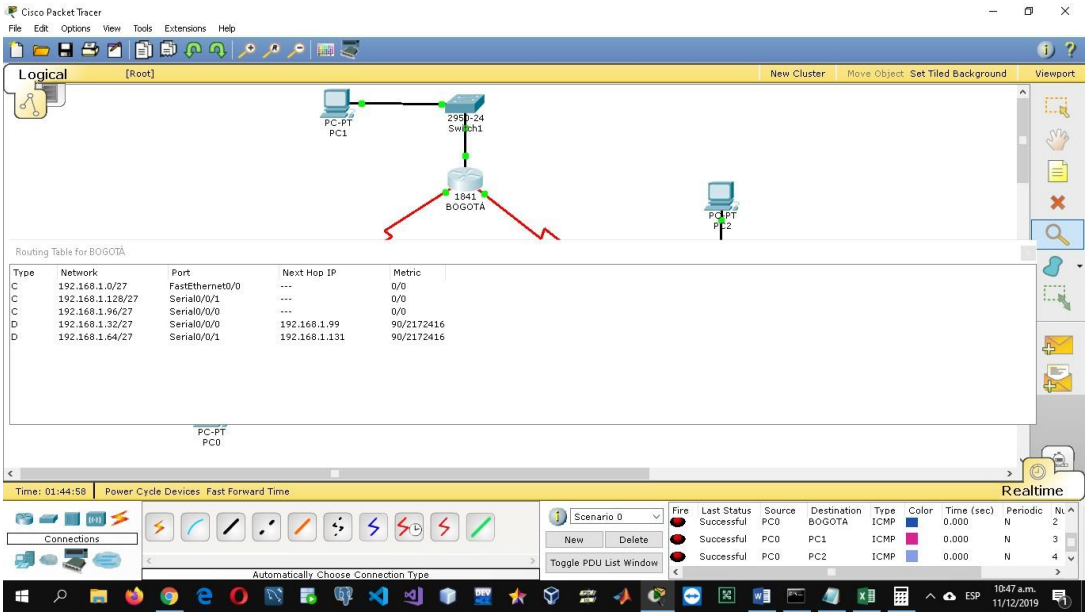


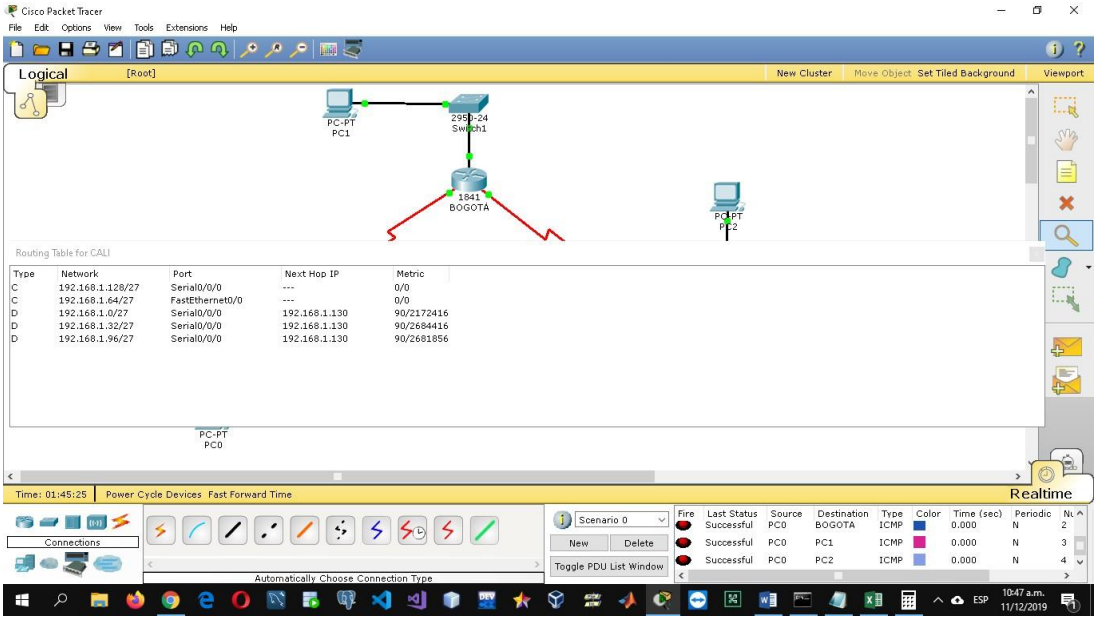
| | R1 | R2 | R3 |
|---|---|---|---|
| Nombre de Host | **MEDELLIN** | **BOGOTA** | **CALI** |
| **Dirección de Ip en interfaz Serial 0/0** | 192.168.1.99 | 192.168.1.98 | 192.168.1.131 |
| **Dirección de Ip en interfaz Serial 0/1** | | 192.168.1.130 | |
| **Dirección de Ip en interfaz FA 0/0** | 192.168.1.33 | 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 |

g. 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

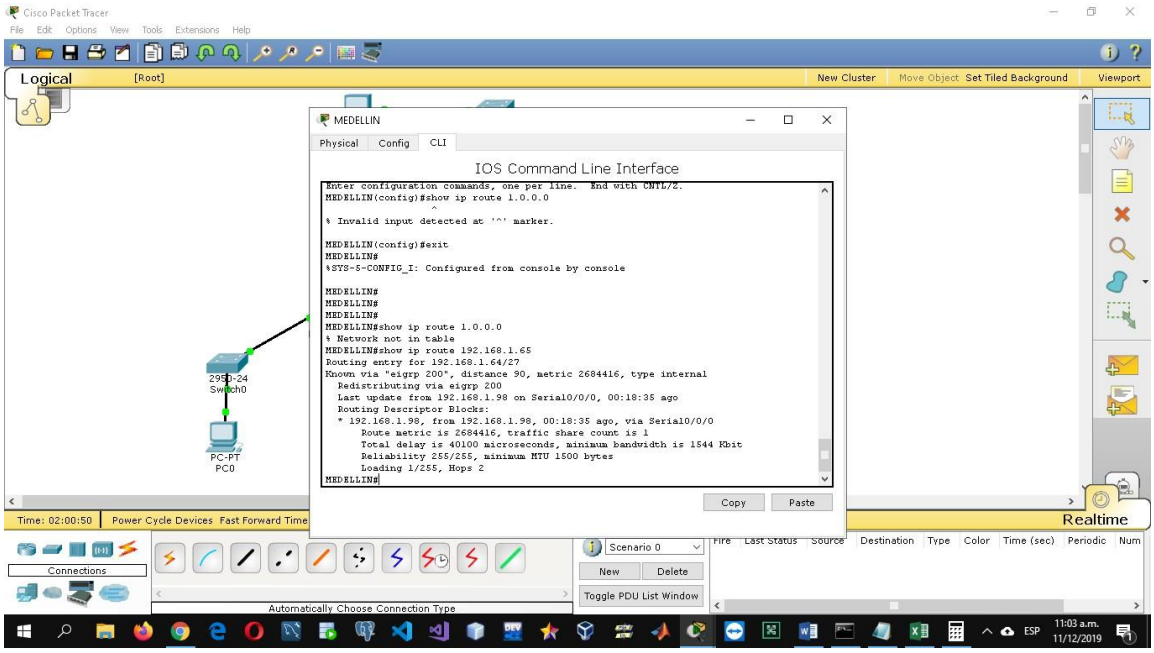


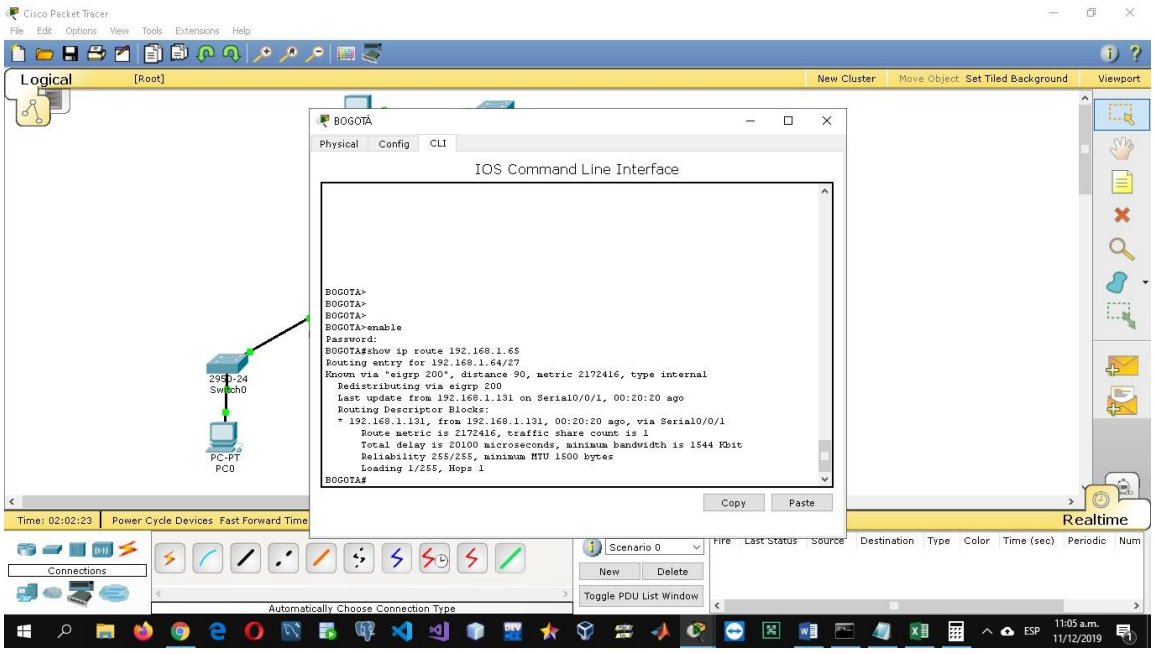


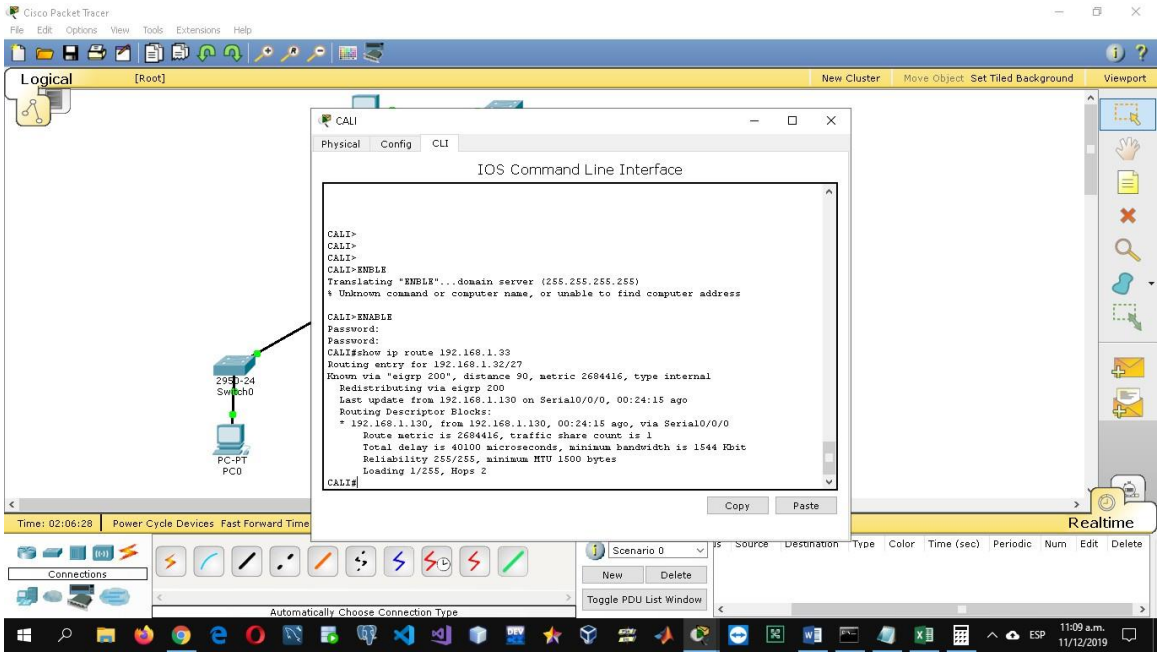




h. Verificar el balanceo de carga que presentan los routers.

Se verifica el balanceo de carga mediante el comando show ip route -address-

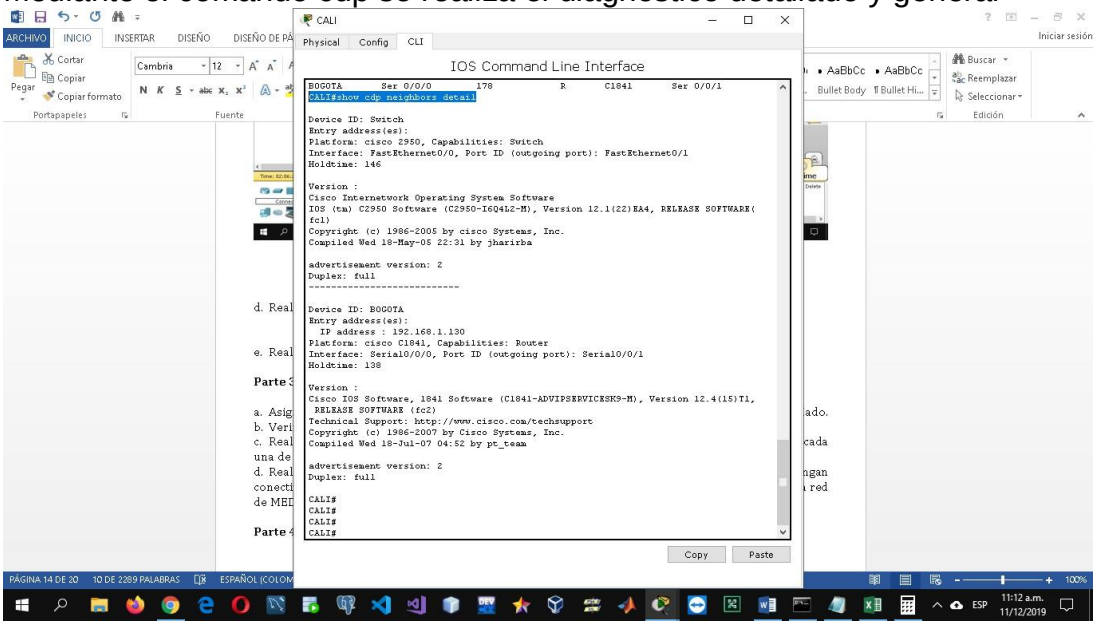

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
MEDELLIN
Physical
Config
CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#show ip route 1.0.0.0
^
% Invalid input detected at '^' marker.
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#show ip route 1.0.0.0
% Network not in table
MEDELLIN#show ip route 192.168.1.65
Routing entry for 192.168.1.64/27
Known via "eigrp 200", distance 90, metric 2684416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.98 on Serial0/0/0, 00:18:35 ago
Routing Descriptor Blocks:
* 192.168.1.98, from 192.168.1.98, 00:18:35 ago, via Serial0/0/0
Route metric is 2684416, traffic share count is 1
Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 2
MEDELLIN#
Copy
Paste
2950-24
Switch0
PC-PT
PC0
Time: 02:00:50
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
ESP
11:03 a.m.
11/12/2019

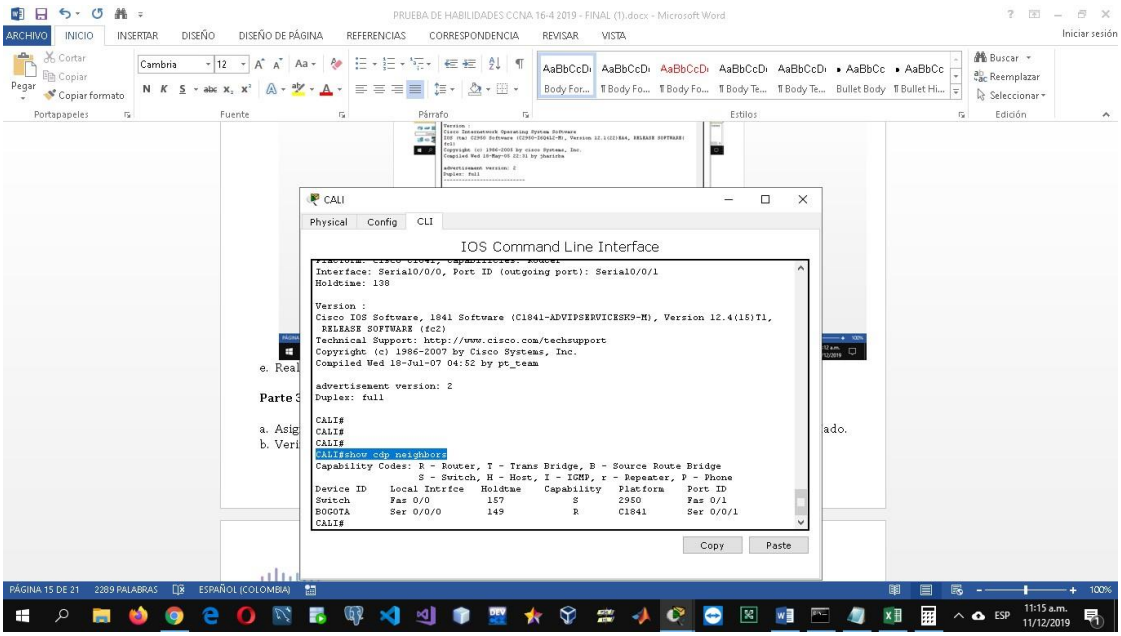

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
BOGOTA
Physical
Config
CLI
IOS Command Line Interface
BOGOTA>
BOGOTA>
BOGOTA>
BOGOTA>enable
Password:
BOGOTA#show ip route 192.168.1.65
Routing entry for 192.168.1.64/27
Known via "eigrp 200", distance 90, metric 2172416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.131 on Serial0/0/1, 00:20:20 ago
Routing Descriptor Blocks:
* 192.168.1.131, from 192.168.1.131, 00:20:20 ago, via Serial0/0/1
Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1
BOGOTA#
Copy
Paste
2950-24
Switch0
PC-PT
PC0
Time: 02:02:23
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
ESP
11:05 a.m.
11/12/2019




i. Realizar un diagnóstico de vecinos uando el comando cdp.

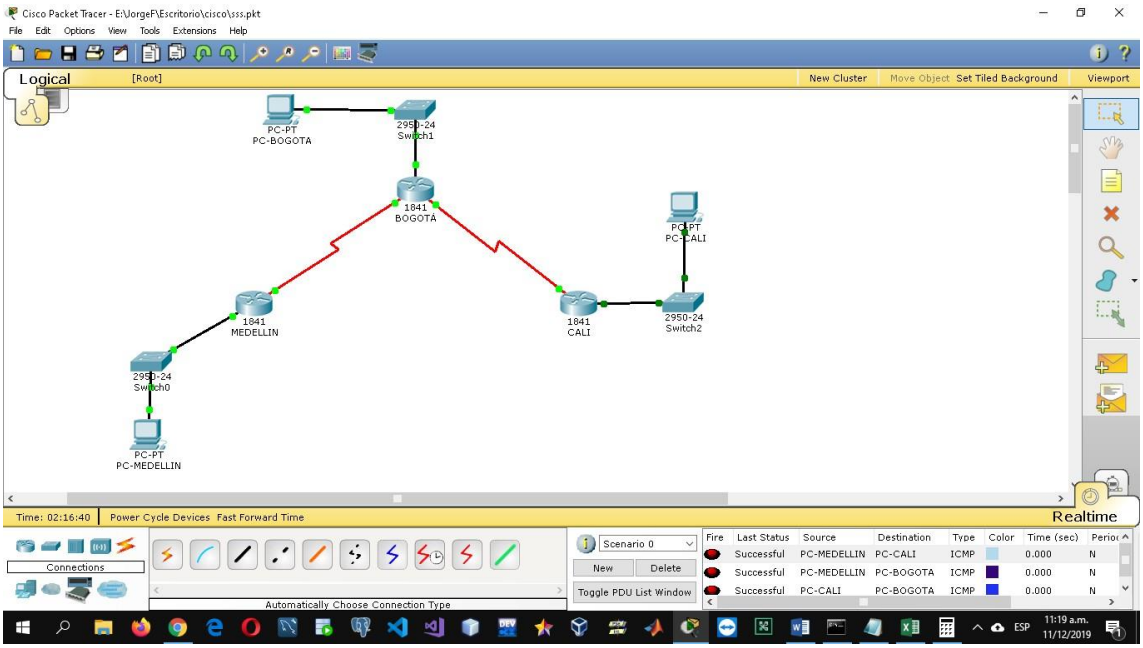
Mediante el comando cdp se realiza el diagnostico detallado y general





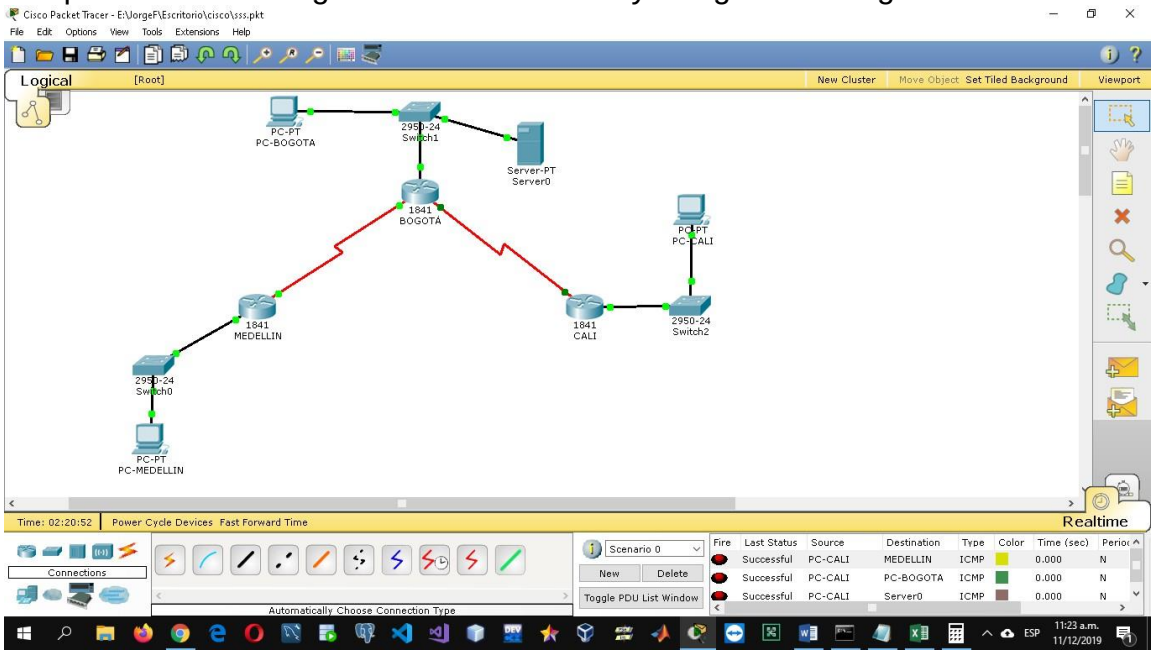

j. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Se envian los respectivos mensajes para verificar la conexión



**Parte 3: Configuración de Enrutamiento.**

e. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
f. Verificar si existe vecindad con los routers configurados con EIGRP.
g. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.
h. 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

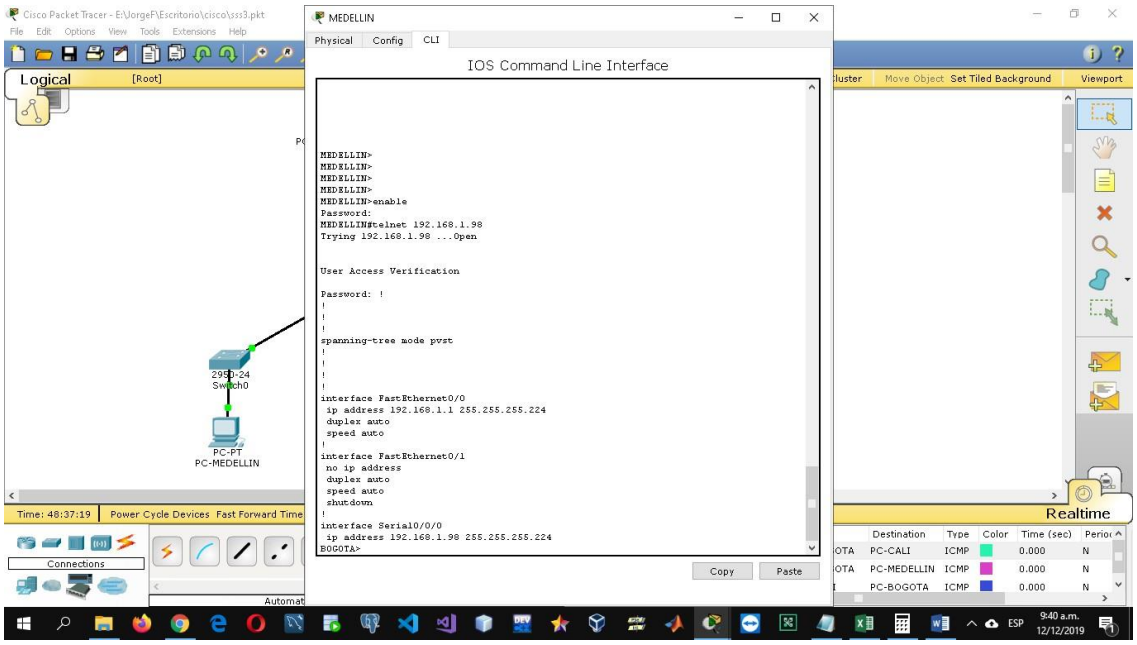


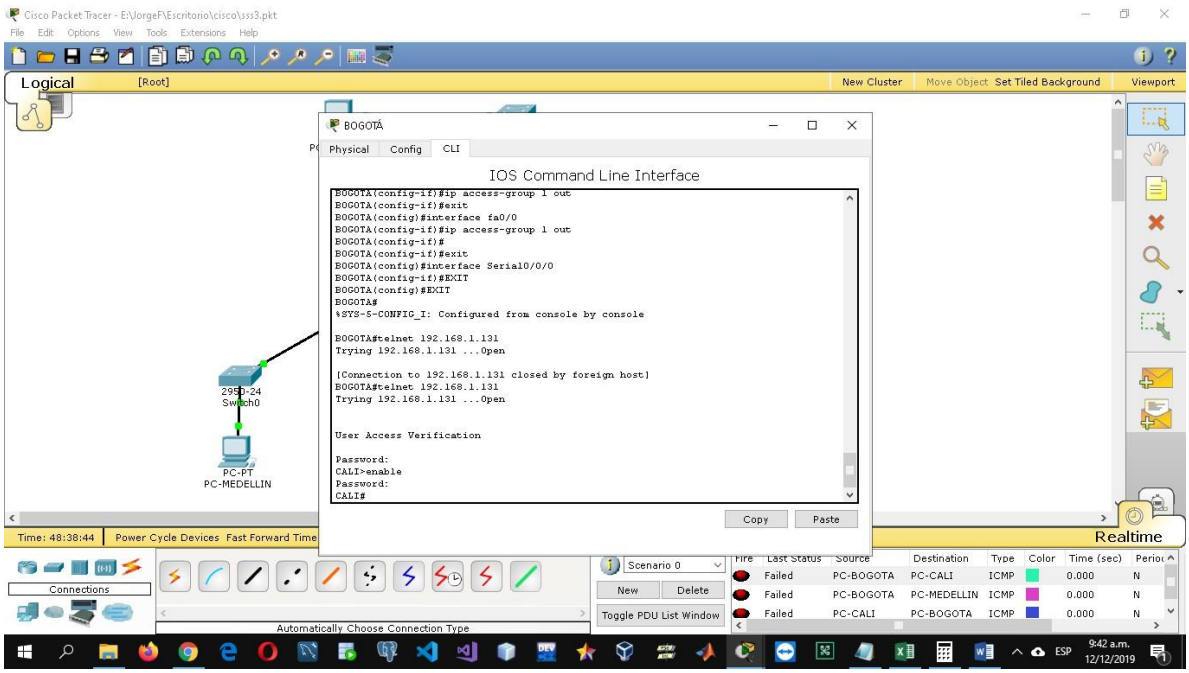

**Parte 4: Configuración de las listas de Control de Acceso.**

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.

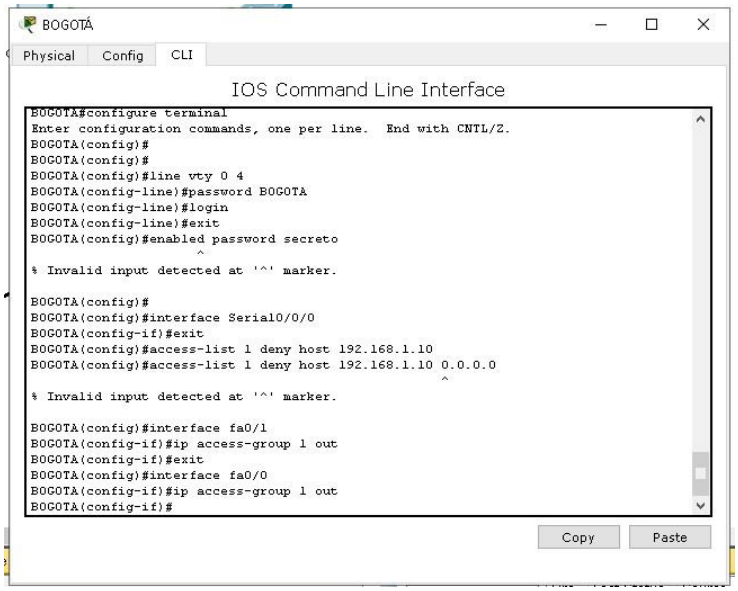
Las condiciones para crear las ACL son las siguientes:

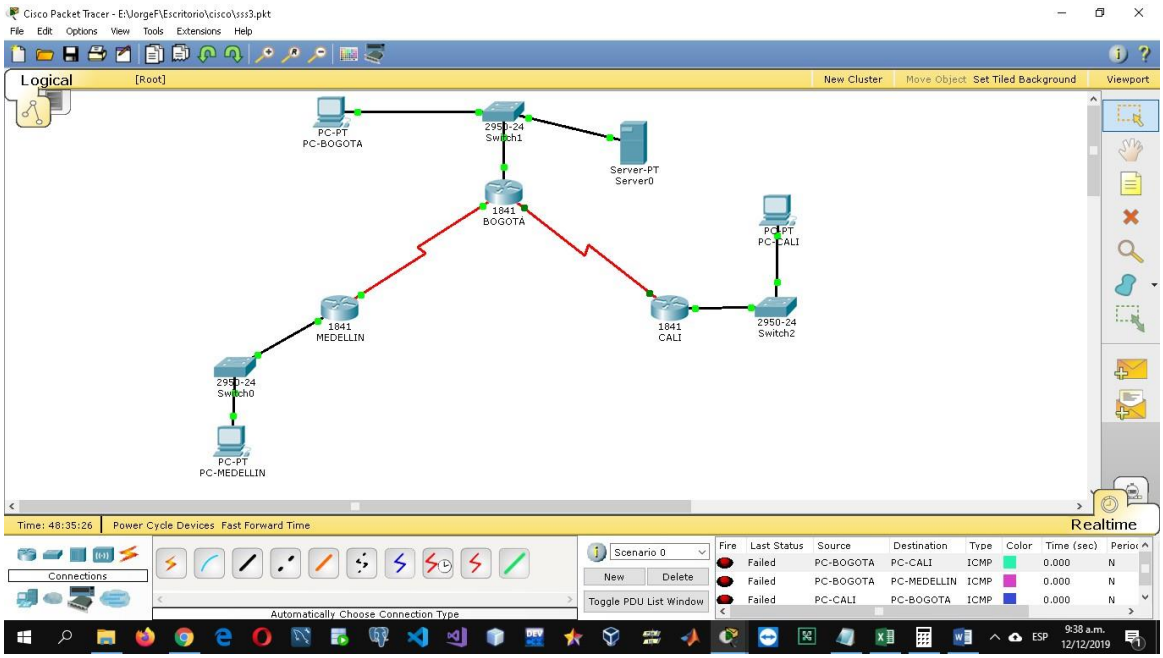
d. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.
Se habilitan las conexiones telnet mediante la consola vty y activando el password


MEDELLIN
Physical
Config
CLI
IOS Command Line Interface
MEDELLIN>
MEDELLIN>
MEDELLIN>
MEDELLIN>
MEDELLIN>enable
Password:
MEDELLIN#telnet 192.168.1.98
Trying 192.168.1.98 ...Open
User Access Verification
Password: !
!
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 192.168.1.98 255.255.255.224
BOGOTA>
Copy
Paste
Logical
[Root]
2950-24
Switch0
PC-PT
PC-MEDELLIN
Realtime
Destination
Type
Color
Time (sec)
PC-CALI
PC-MEDELLIN
PC-BOGOTA
ICMP
0.000


BOGOTA
Physical
Config
CLI
IOS Command Line Interface
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#interface fa0/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#
BOGOTA(config-if)#exit
BOGOTA(config)#interface Serial0/0/0
BOGOTA(config-if)#EXIT
BOGOTA(config)#EXIT
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#telnet 192.168.1.131
Trying 192.168.1.131 ...Open
[Connection to 192.168.1.131 closed by foreign host]
BOGOTA#telnet 192.168.1.131
Trying 192.168.1.131 ...Open
User Access Verification
Password:
CALI>enable
Password:
CALI#
Copy
Paste
Logical
[Root]
2950-24
Switch0
PC-PT
PC-MEDELLIN
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Failed
PC-BOGOTA
PC-CALI
PC-MEDELLIN
ICMP
0.000

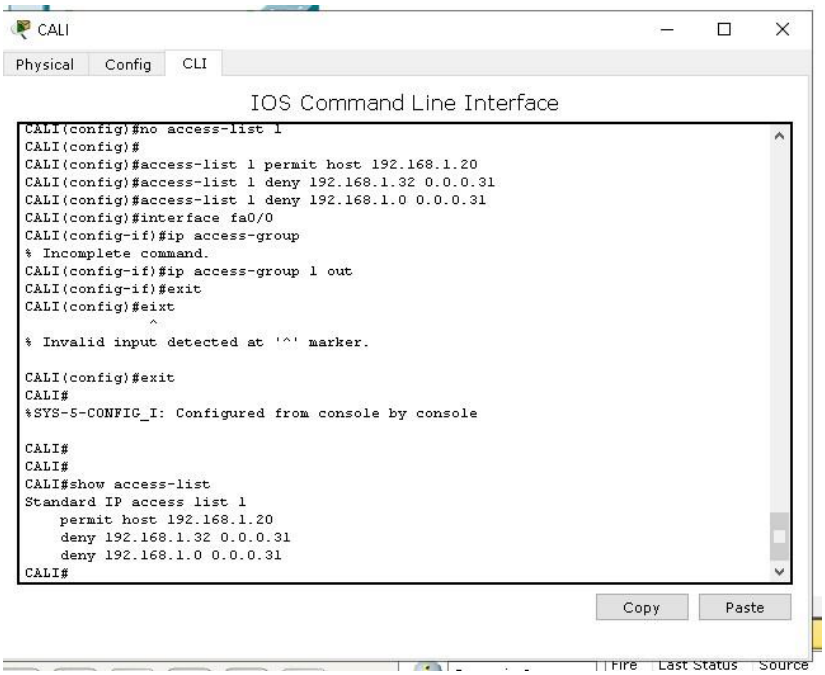
e. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión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

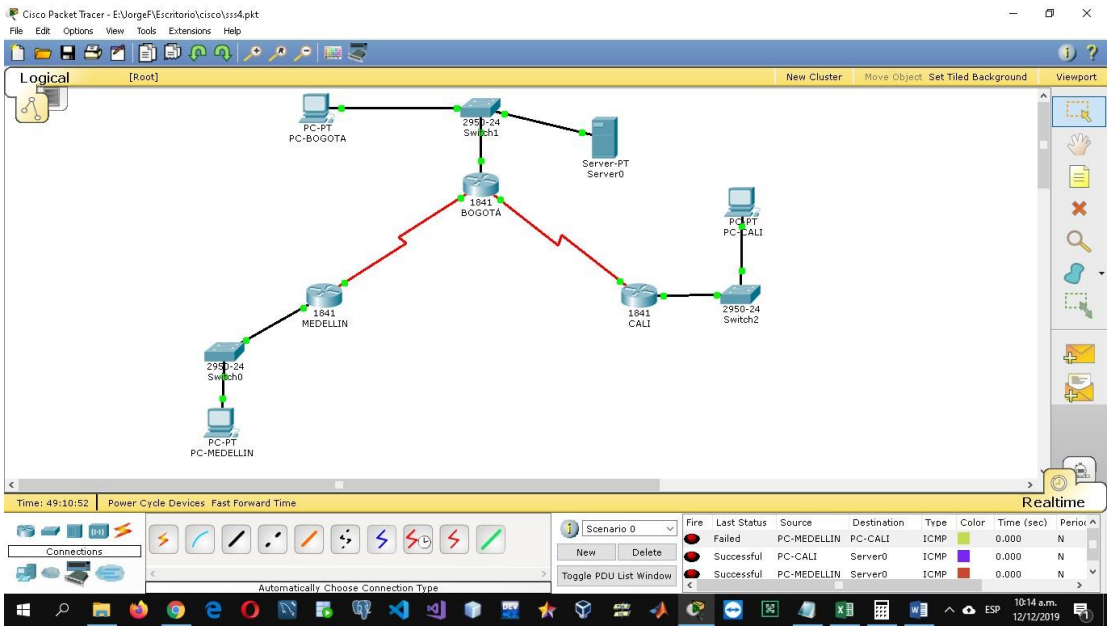



f. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión según lo requerido




**Parte 5: Comprobación de la red instalada.**

c. Se debe probar que la configuración de las listas de acceso fue exitosa.
d. 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 |
| | Servidor | Router CALI | SUCCESSFULL |
| | Servidor | Router MEDELLIN | SUCCESSFULL |
| | LAN del Router MEDELLIN | Router CALI | Connection timed out; remote host not responding |
| TELNET | LAN del Router CALI | Router CALI | SUCCESSFULL |
| | 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 |

**Código de configuración escenario 1**

```
enable
configure terminal
hostname CALI
enable password CALI
exit
```

**router eigrp 200**
**network network-number**
**bandwidth kilobits**
**eigrp log-neighbor-changes**

**router eigrp 200**
**network 192.168.1.0 0.0.0.31**
**network 192.168.1.32 0.0.0.31**
**network 192.168.1.64 0.0.0.31**
**network 192.168.1.96 0.0.0.31**
**network 192.168.1.128 0.0.0.31**
**bandwidth kilobits**
**eigrp log-neighbor-changes**

**hostname remoto**
**line vty 0 4**
**password MEDELLIN**
**login**
**exit**
**enabled password secreto**

**line vty 0 4**
**password BOGOTA**
**login**
**exit**
**enabled password secreto**

**line vty 0 4**
**password CALI**
**login**
**exit**
**enabled password secreto**

**access-list 1 deny host 192.168.1.10**

**access-list 1 permit host 192.168.1.20**
**access-list 1 deny 192.168.1.64 0.0.0.31**
**access-list 1 deny 192.168.1.0 0.0.0.31**

**access-list 1 permit host 192.168.1.20**
**access-list 1 deny 192.168.1.32 0.0.0.31**
**access-list 1 deny 192.168.1.0 0.0.0.31**

**access-list 102 permit host any any eq telnet**

**access-list 101 permit tcp any any eq telnet**

**VLAN 1**
**NAME VLAN--1**
**EXIT**

**VLAN 10**
**NAME VLAN--10**
**EXIT**

**VLAN 30**
**NAME VLAN--30**
**EXIT**

**interface range f0/21-22**
**switchport mode access**
**switchport access vlan 1**

**exit**

**interface range f0/2-10**
**switchport mode access**
**switchport access vlan 10**
**exit**

**interface range f0/11-20**
**switchport mode access**
**switchport access vlan 30**
**exit**

**enable**
**configure terminal**
**interface fastEthernet 0/0.1**
**encapsulation dot1Q 1**
**ip address 172.31.2.1 255.255.255.248**
**no shutdown**
**exit**

**enable**
**configure terminal**
**interface fastEthernet 0/0.10**
**encapsulation dot1Q 10**
**ip address 172.31.0.1 255.255.255.192**
**no shutdown**
**exit**

**interface fastEthernet 0/0.30**
**encapsulation dot1Q 30**
**ip address 172.31.0.65 255.255.255.192**
**no shutdown**
**exit**

**ip dhcp pool vlan-1**

**network 172.31.2.0 255.255.255.248**
**default-router 172.31.2.1**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool vlan-10**
**network 172.31.0.0 255.255.255.192**
**default-router 172.31.0.1**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool vlan-30**
**network 172.31.0.64 255.255.255.192**
**default-router 172.31.0.65**
**dns-server 8.8.8.8**
**exit**

***************************************
**ROUTER BUCARAMANGA**
***************************************
**router ospf 1**
**network 172.31.2.32 0.0.0.3 area 0**
**network 172.31.2.0 0.0.0.7 area 0**
**network 172.31.0.0 0.0.0.63 area 0**
**network 172.31.0.64 0.0.0.63 area 0**

**interface se0/0/0**
**ip ospf authentication**
**ip ospf message-digest-key 1 md5 CISCO**
**exit**
**router ospf 1**
**area 0 authentication**

**copy flash: tftp:**

```
access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.192 0.0.0.63
access-list 101 deny any
int vlan 2
ip access-group 101 out

access-list 102 deny ip 192.168.2.0 0.0.0.63 192.168.2.128 0.0.0.63
access-list 102 permit ip any any
!
access-list 103 deny ip 192.168.2.64 0.0.0.63 192.168.2.0 0.0.0.63
access-list 103 perit ip any any
!
access-list 104 deny ip 192.168.2.128 0.0.0.63 192.168.2.0 0.0.0.63
access-list 104 permit ip any any
!

!
int vlan 3
  ip access-group 102 in
!
int vlan 4
  ip access-group 103 in
!


access-list 1 permit ip 192.168.2.128 0.0.0.63 192.168.2.0 0.0.0.63

interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in



access-list 1 permit 172.31.0.128
access-list 1 permit 172.31.0.192
access-list 1 deny any
interface Ethernet0/0.20
ip access-group 1 in
```

**ip dhcp pool tunja-vlan-30**
**network 172.31.0.192 255.255.255.192**
**default-router 172.31.0.193**
**dns-server 8.8.8.8**
**exit**

**show ip dhcp pools tunja-vlan-30**

****************************************
**SWITCH TUNJA**
****************************************

**VLAN 1**
**NAME VLAN--1**
**EXIT**

**VLAN 20**
**NAME VLAN--10**
**EXIT**

**VLAN 30**
**NAME VLAN--30**
**EXIT**

**interface range f0/2-10**
**switchport mode access**
**switchport access vlan 20**
**exit**

**interface range f0/11-20**
**switchport mode access**
**switchport access vlan 30**
**exit**

****************************************
**ROUTER TUNJA**

**********

**router ospf 1**
**network 172.31.2.36 0.0.0.3 area 0**
**network 172.31.2.32 0.0.0.3 area 0**
**network 172.31.2.8 0.0.0.7 area 0**
**network 172.31.0.128 0.0.0.63 area 0**
**network 172.31.0.192 0.0.0.63 area 0**

**enable**
**configure terminal**
**interface fastEthernet 0/0.1**
**encapsulation dot1Q 1**
**ip address 172.31.2.9 255.255.255.248**
**no shutdown**
**exit**

**interface fastEthernet 0/0.20**
**encapsulation dot1Q 20**
**ip address 172.31.0.129 255.255.255.192**
**no shutdown**
**exit**

**interface fastEthernet 0/0.30**
**encapsulation dot1Q 30**
**ip address 172.31.0.193 255.255.255.192**
**no shutdown**
**exit**

**ip dhcp pool 20**
**network 172.31.0.128 255.255.255.192**
**default-router 172.31.0.129**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool 30**
**network 172.31.0.192 255.255.255.192**
**default-router 172.31.0.193**
**dns-server 8.8.8.8**

**exit**

**ip helper-address 172.31.2.33**

****************************************
**SWITCH CUNDINAMARCA**
****************************************

**VLAN 1**
**NAME VLAN--1**
**EXIT**

**VLAN 20**
**NAME VLAN--20**
**EXIT**

**VLAN 30**
**NAME VLAN--30**
**EXIT**

**VLAN 88**
**NAME VLAN--88**
**EXIT**

**VLAN 90**
**NAME VLAN--90**
**EXIT**

**interface range f0/20-24**
**switchport mode access**
**switchport access vlan 1**
**exit**

**interface range f0/2-8**
**switchport mode access**
**switchport access vlan 20**
**exit**

**interface range f0/9-15**
**switchport mode access**
**switchport access vlan 30**
**exit**

**interface range f0/16-20**
**switchport mode access**
**switchport access vlan 88**
**exit**

**int f0/1**
**switchport mode trunk**
**switchport nonegotiate**
**switchport native vlan 90**

****************************************
**ROUTER CUNDINAMARCA**
****************************************
**router ospf 1**
**network 172.31.2.36 0.0.0.3 area 0**
**network 172.31.2.16 0.0.0.7 area 0**
**network 172.31.1.64 0.0.0.63 area 0**
**network 172.31.1.0 0.0.0.63 area 0**
**network 172.31.1.24 0.0.0.7 area 0**

**enable**
**configure terminal**
**interface fastEthernet 0/0.1**
**encapsulation dot1Q 1**
**ip address 172.31.2.17 255.255.255.248**
**no shutdown**
**exit**

**interface fastEthernet 0/0.20**
**encapsulation dot1Q 20**
**ip address 172.31.1.65 255.255.255.192**
**no shutdown**
**exit**

**interface fastEthernet 0/0.30**
**encapsulation dot1Q 30**
**ip address 172.31.1.1 255.255.255.192**
**no shutdown**
**exit**

**interface fastEthernet 0/0.88**
**encapsulation dot1Q 88**
**ip address 172.31.2.25 255.255.255.248**
**no shutdown**
**exit**

**ip dhcp pool vlan-1**
**network 172.31.2.16 255.255.255.248**
**default-router 172.31.2.17**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool vlan-20**
**network 172.31.1.64 255.255.255.192**
**default-router 172.31.1.65**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool cvlan-30**
**network 172.31.1.0 255.255.255.192**
**default-router 172.31.1.1**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool vlan-88**
**network 172.31.2.24 255.255.255.248**
**default-router 172.31.2.25**
**dns-server 8.8.8.8**
**exit**

**ip dhcp pool tunja-vlan-20**

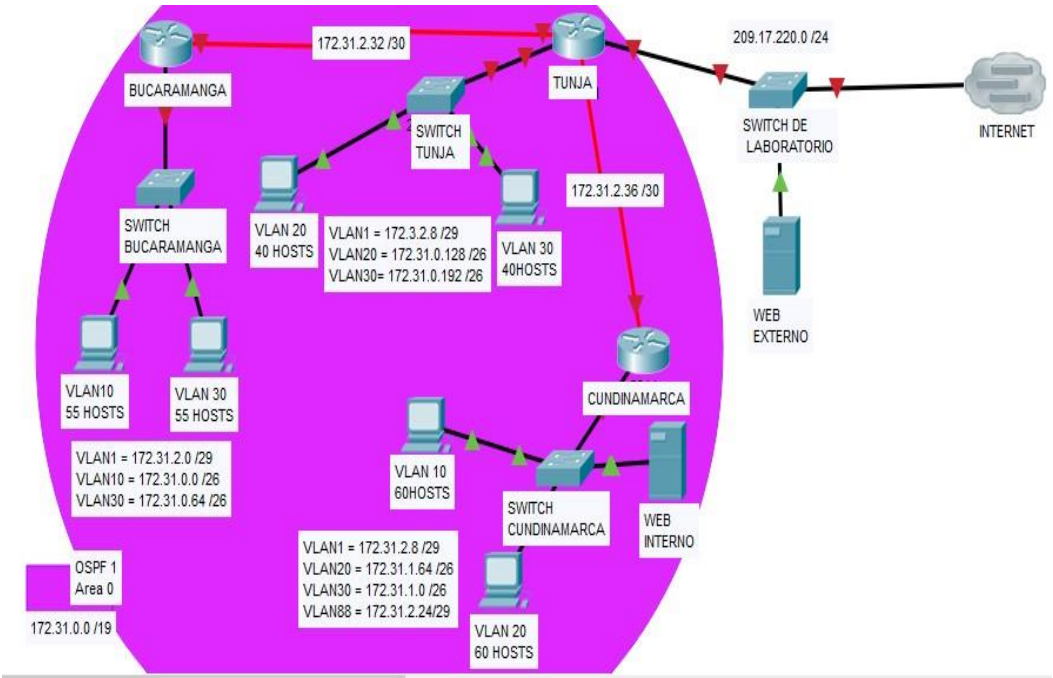
**network 172.31.0.128 255.255.255.192**
**default-router 172.31.0.129**
**dns-server 8.8.8.8**
**exit**

**access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.192 0.0.0.63**
**access-list 101 deny ip any any**
**int vlan 20**
**ip access-group 101 out**

**access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.192 0.0.0.63**
**access-list 101 deny ip any any**
**int vlan 20**
**ip access-group 101 out**

## Desarrollo Escenario 2

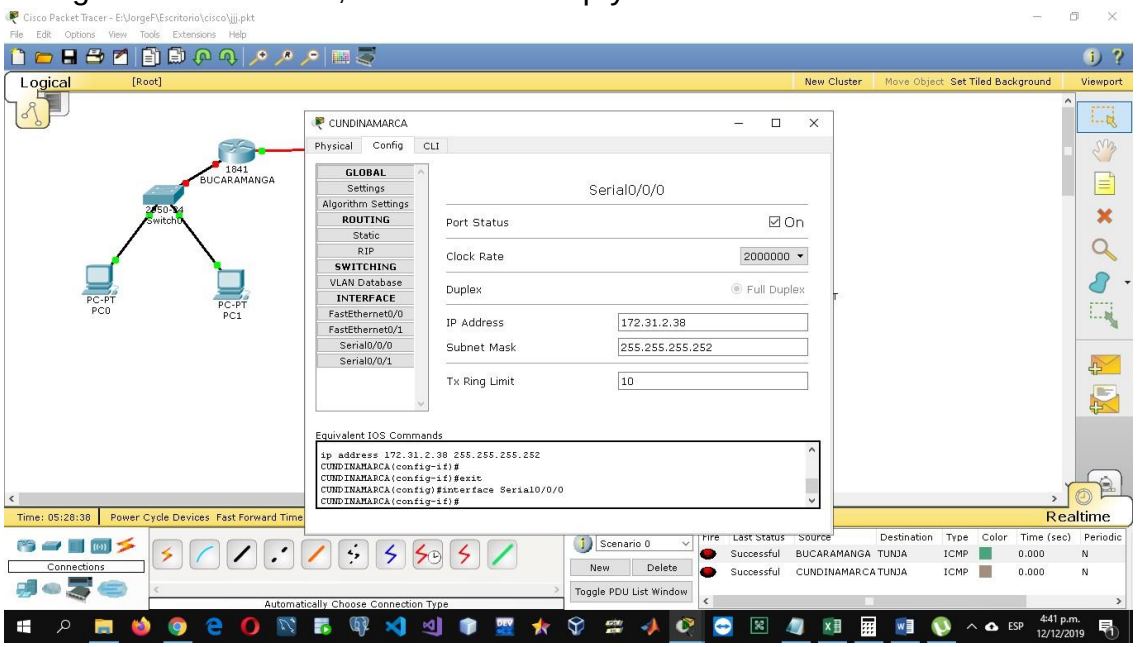
Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

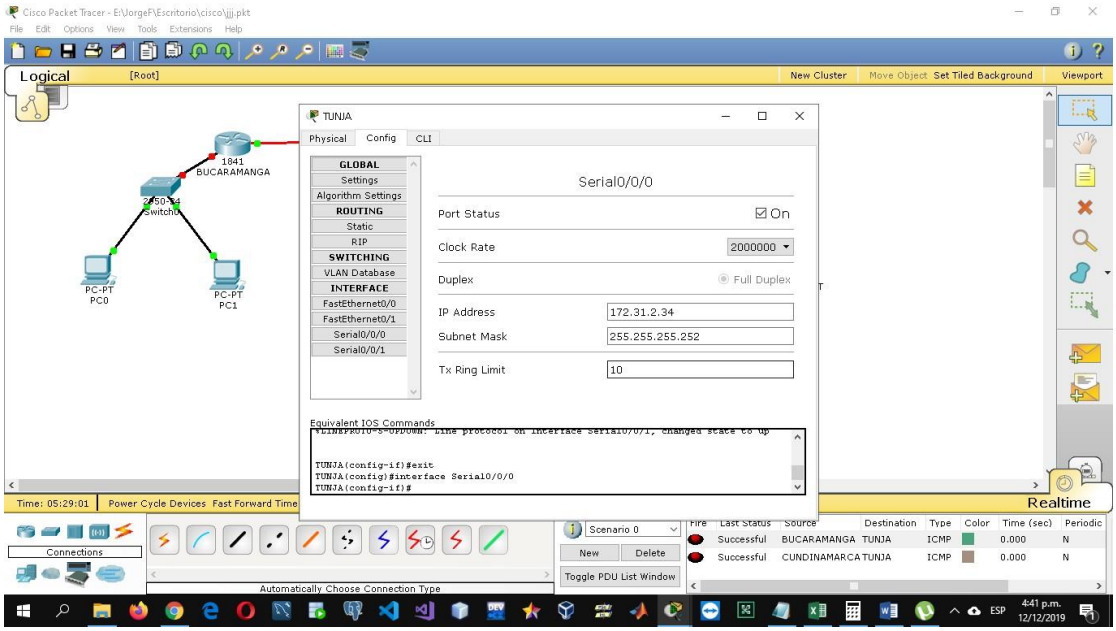


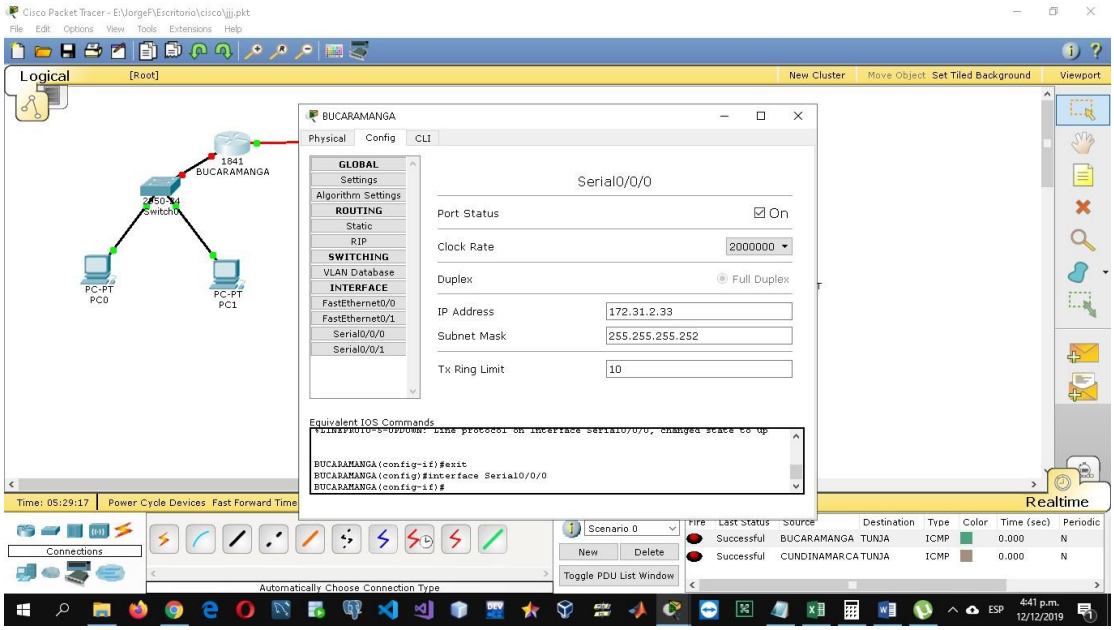
Los siguientes son los requerimientos necesarios:

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.

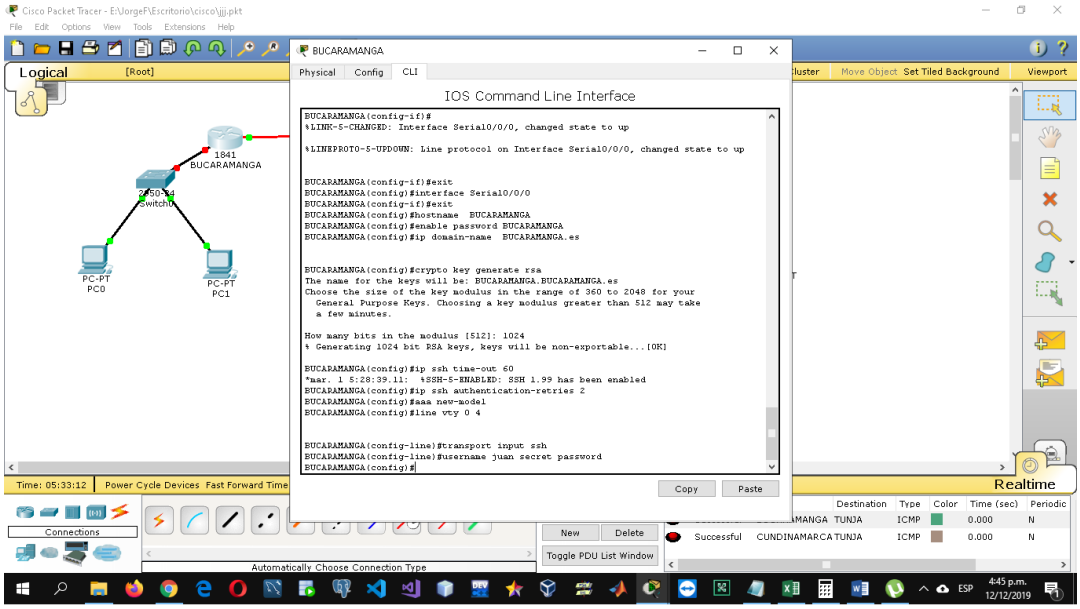
Se realiza la configuración básica en donde se cambia el nombre de los router se configura la contraseña, las direcciones ip y el enrutamiento

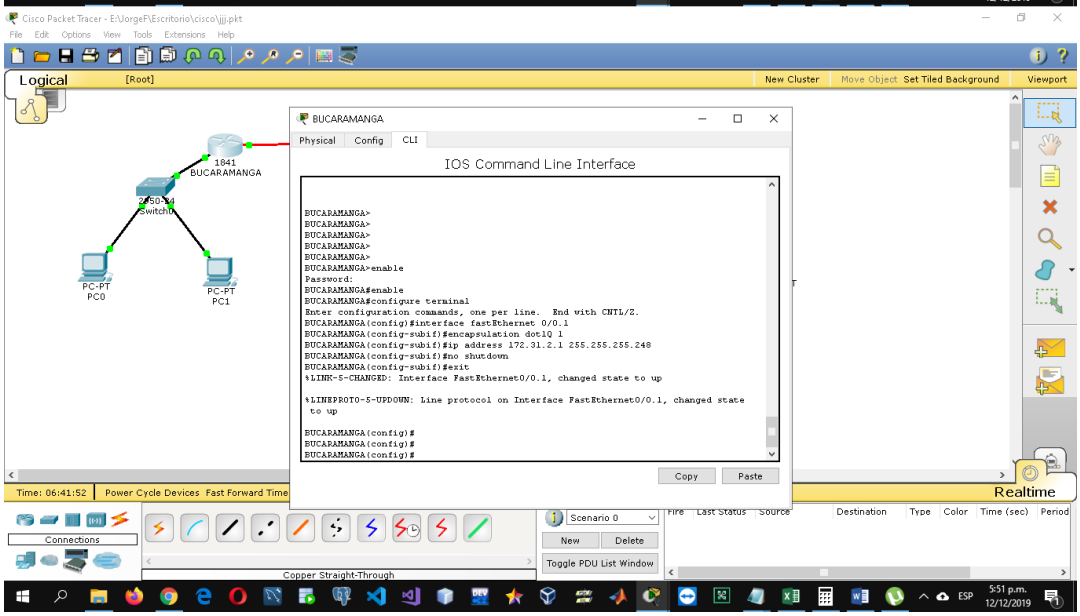




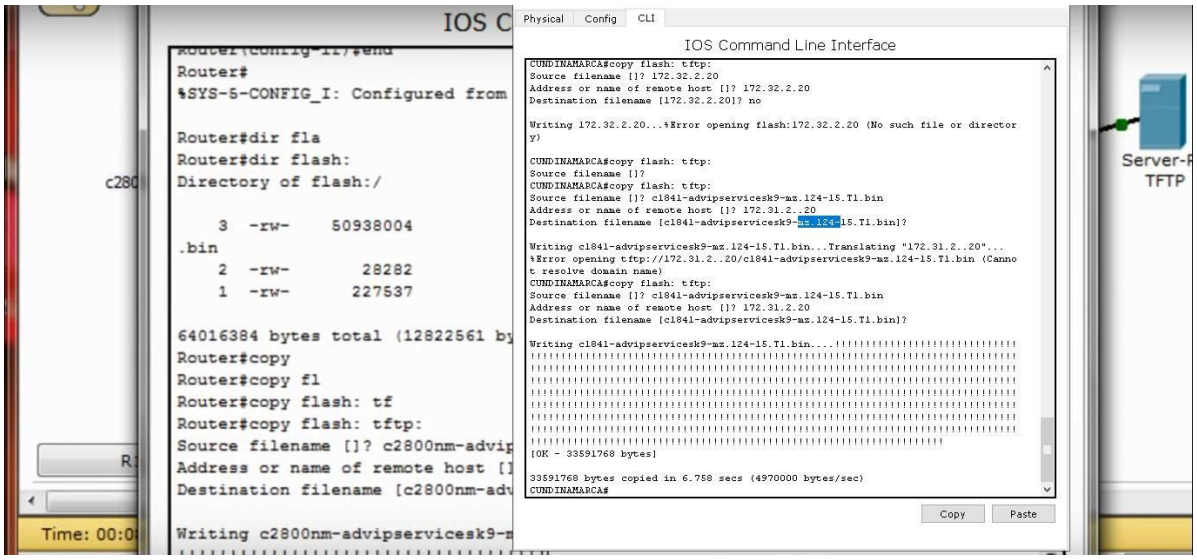



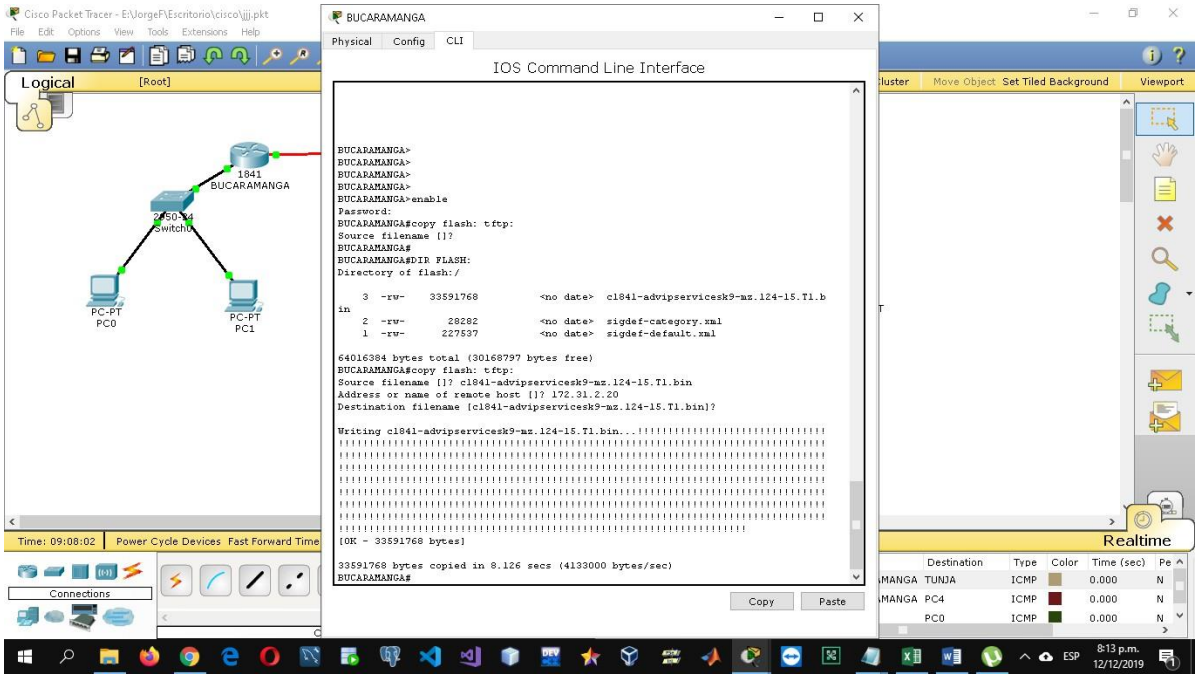

Se hace la auntenticacion local con aaa se hace el cifrado de contraseña mediante rsa de 1024 bytes se establece un máximo de intentos de 2 y máximo de tiempo de 60

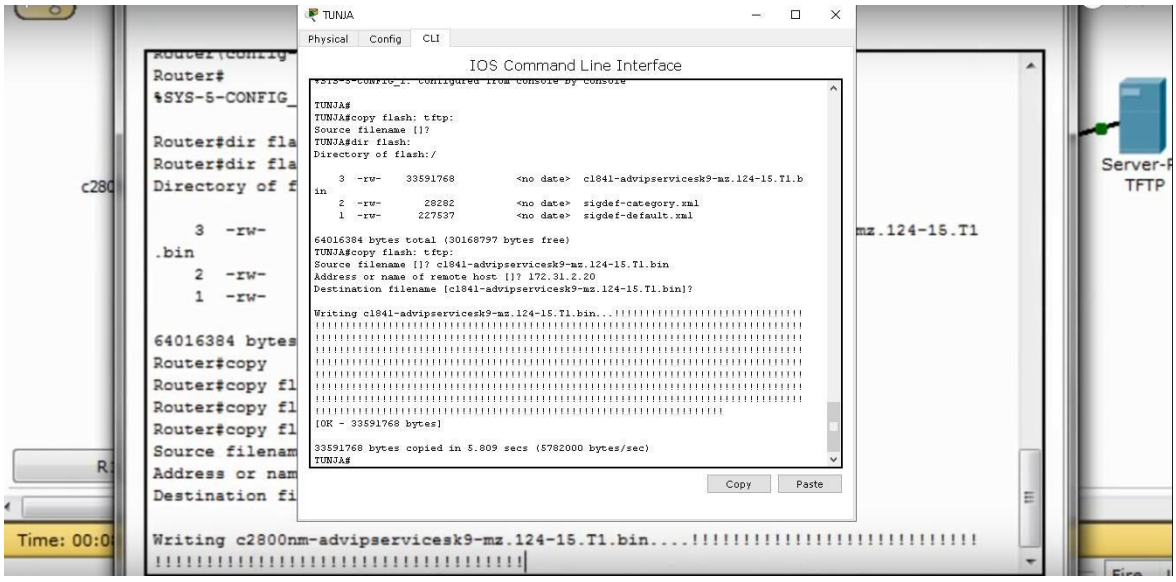



Se copia la información de los routers en el servidor tftp

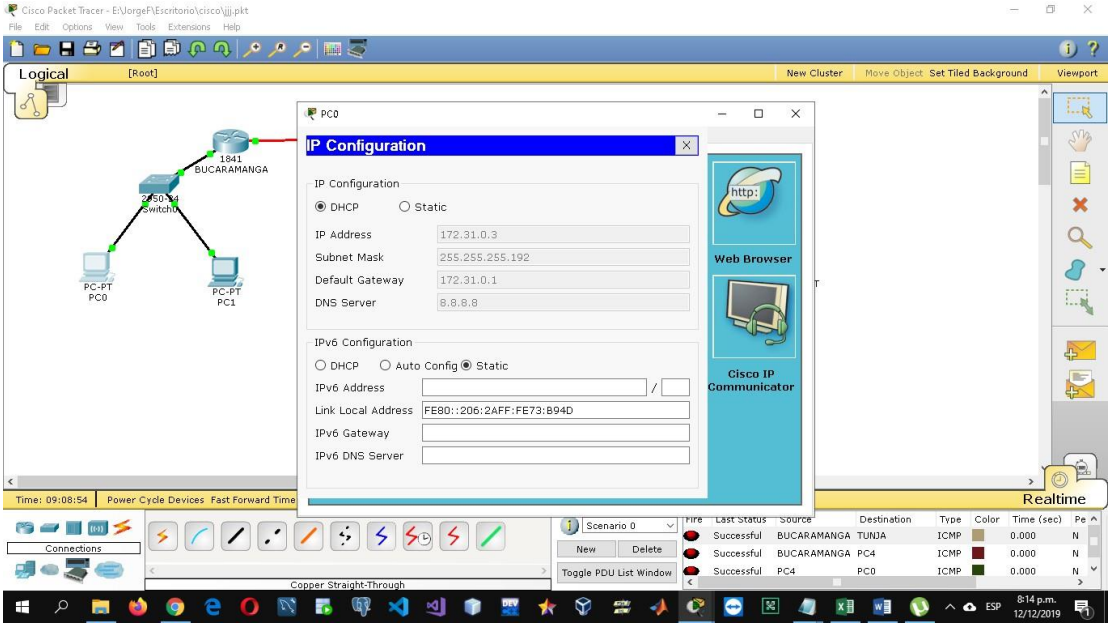

IOS C
Router#
%SYS-5-CONFIG_I: Configured from
Router#dir fla
Router#dir flash:
Directory of flash:/
3 -rw- 50938004
.bin
2 -rw- 28282
1 -rw- 227537
64016384 bytes total (12822561 by
Router#copy
Router#copy fl
Router#copy flash: tf
Router#copy flash: tftp:
Source filename []? c2800nm-advip
Address or name of remote host []
Destination filename [c2800nm-adv
Writing c2800nm-advipservicesk9-m
Time: 00:0
Physical
Config
CLI
IOS Command Line Interface
CUNDINAMARCA#copy flash: tftp:
Source filename []? 172.32.2.20
Address or name of remote host []? 172.32.2.20
Destination filename [172.32.2.20]? no
Writing 172.32.2.20...%Error opening flash:172.32.2.20 (No such file or director
y)
CUNDINAMARCA#copy flash: tftp:
Source filename []?
CUNDINAMARCA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2..20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing c1841-advipservicesk9-mz.124-15.T1.bin...Translating "172.31.2..20"...
%Error opening tftp://172.31.2..20/c1841-advipservicesk9-mz.124-15.T1.bin (Canno
t resolve domain name)
CUNDINAMARCA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing c1841-advipservicesk9-mz.124-15.T1.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]
33591768 bytes copied in 6.758 secs (4970000 bytes/sec)
CUNDINAMARCA#
Copy
Paste
Server-
TFTP

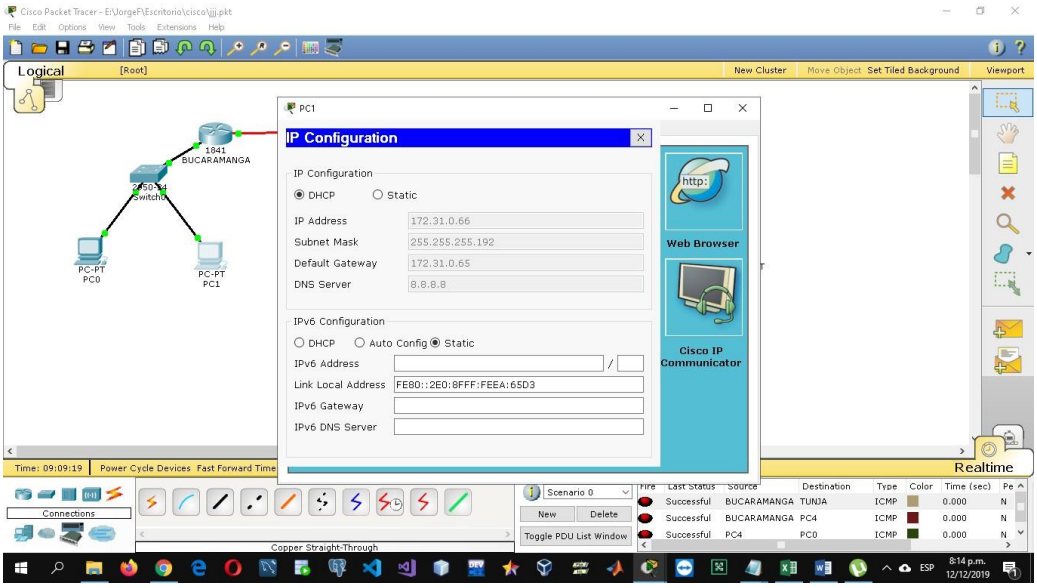

Cisco Packet Tracer - E:\JorgeF\Escritorio\cisco\jjj.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
1841
BUCARAMANGA
2950-24
Switch0
PC-PT
PC0
PC-PT
PC1
BUCARAMANGA
Physical
Config
CLI
IOS Command Line Interface
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>enable
Password:
BUCARAMANGA#copy flash: tftp:
Source filename []?
BUCARAMANGA#
BUCARAMANGA#DIR FLASH:
Directory of flash:/
3 -rw- 33591768 <no date> c1841-advipservicesk9-mz.124-15.T1.b
in
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml
64016384 bytes total (30168797 bytes free)
BUCARAMANGA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing c1841-advipservicesk9-mz.124-15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]
33591768 bytes copied in 8.126 secs (4133000 bytes/sec)
BUCARAMANGA#
Copy
Paste
Time: 09:08:02
Power Cycle Devices Fast Forward Time
Connections
Realtime
Destination
Type
Color
Time (sec)
MANGA TUNJA ICMP 0.000 N
MANGA PC4 ICMP 0.000 N
PC0 ICMP 0.000 N
ESP
8:13 p.m.
12/12/2019




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

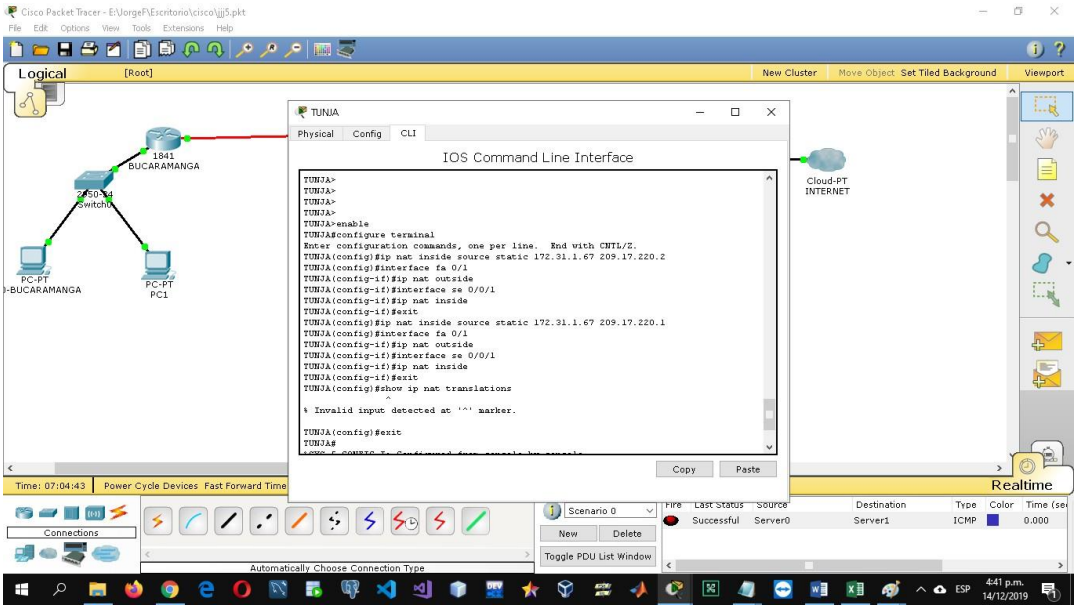
-Mediante el comando dchp pool se crean los diferentes rangos de direcciones que se van a asignar mediante dchp a las diferentes subinterfaces





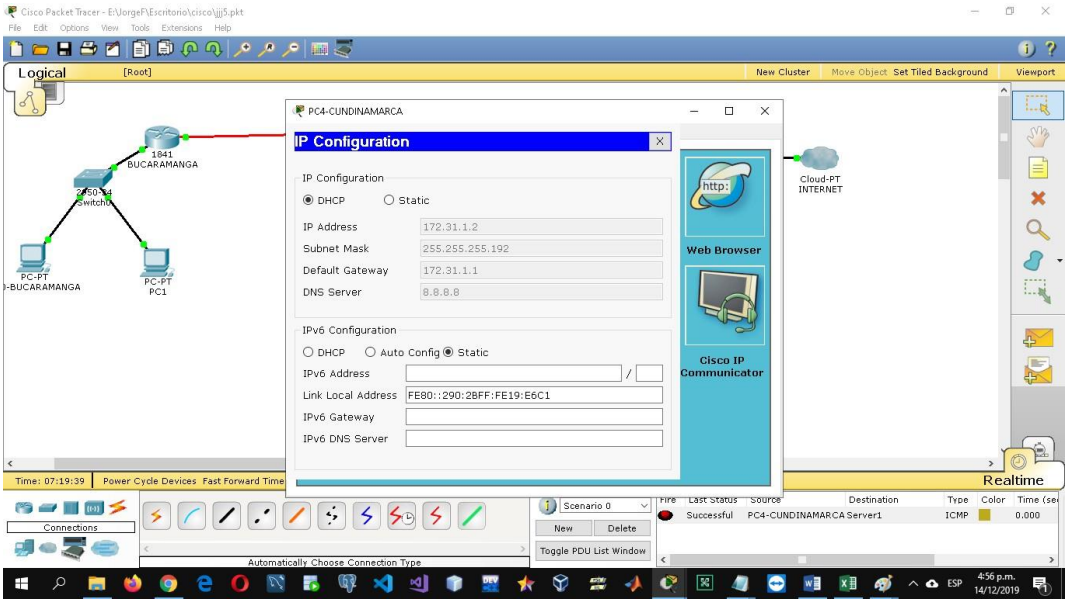

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

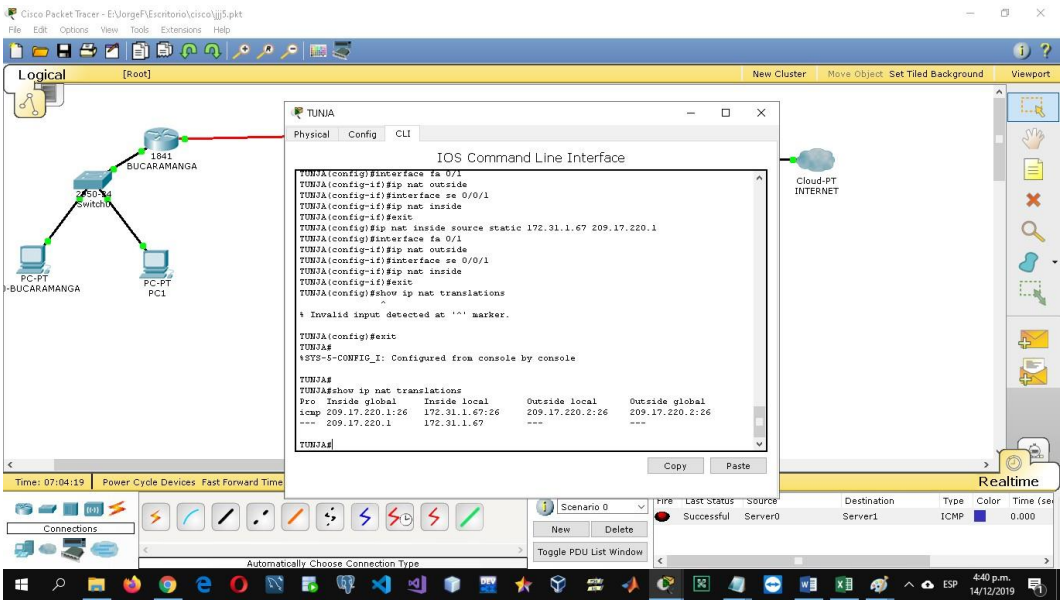
Se configura la nat estática




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

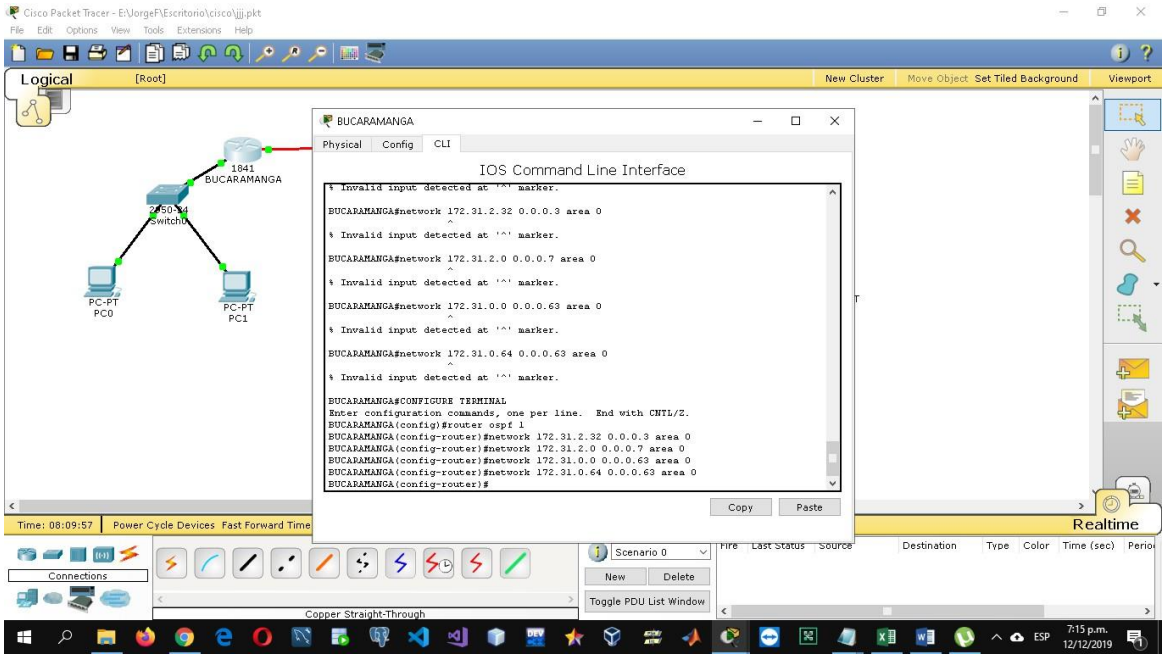
Luego realizamos la configuración de la nat con sobrecarga (PAT) para ello creamos una access-list donde agregamos las direcciones que deseamos que sean traducidas, y luego la usamos en la configuración de la nat mas la interfaz de salida a internet y el comando overload. En las imágenes podemos ver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

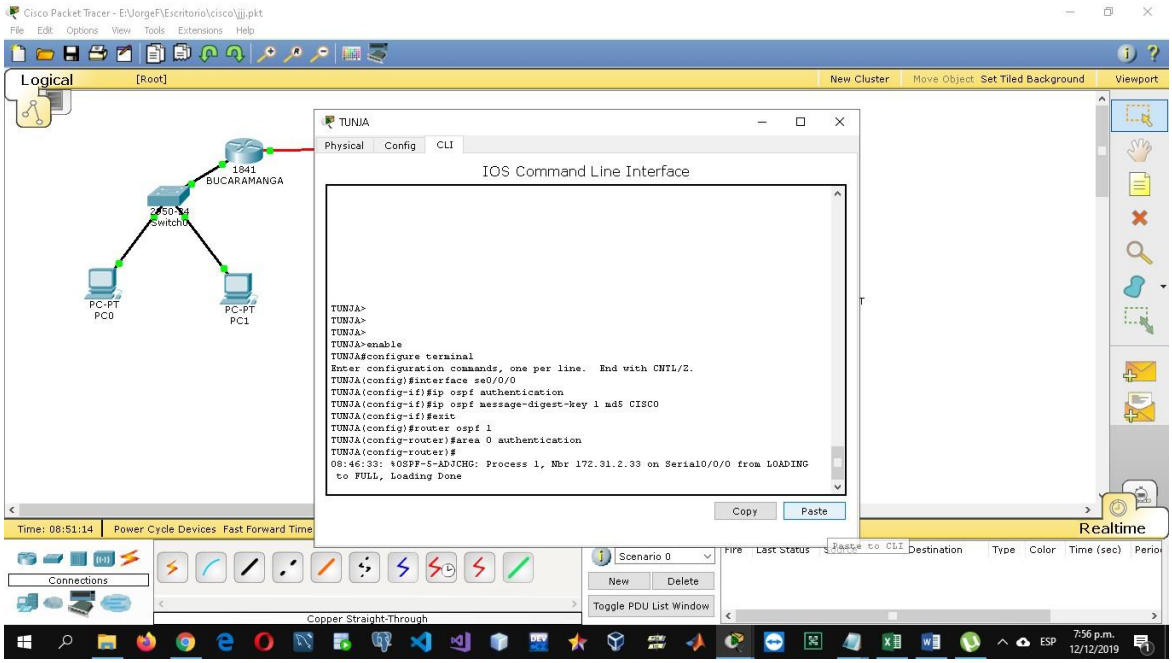


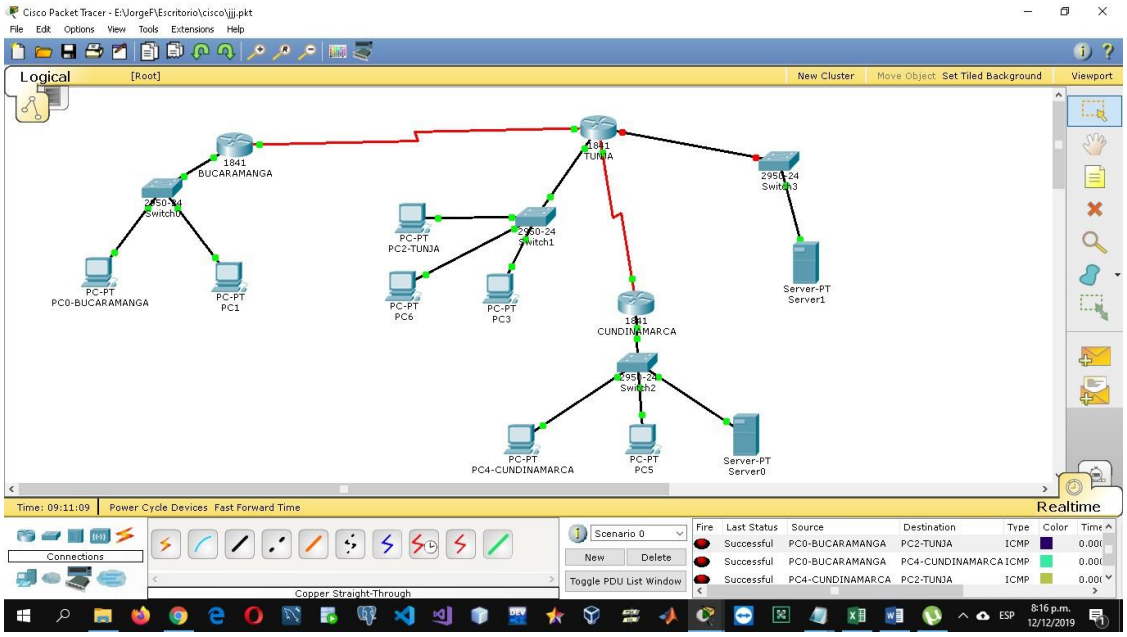




4. El enrutamiento deberá tener autenticación.

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

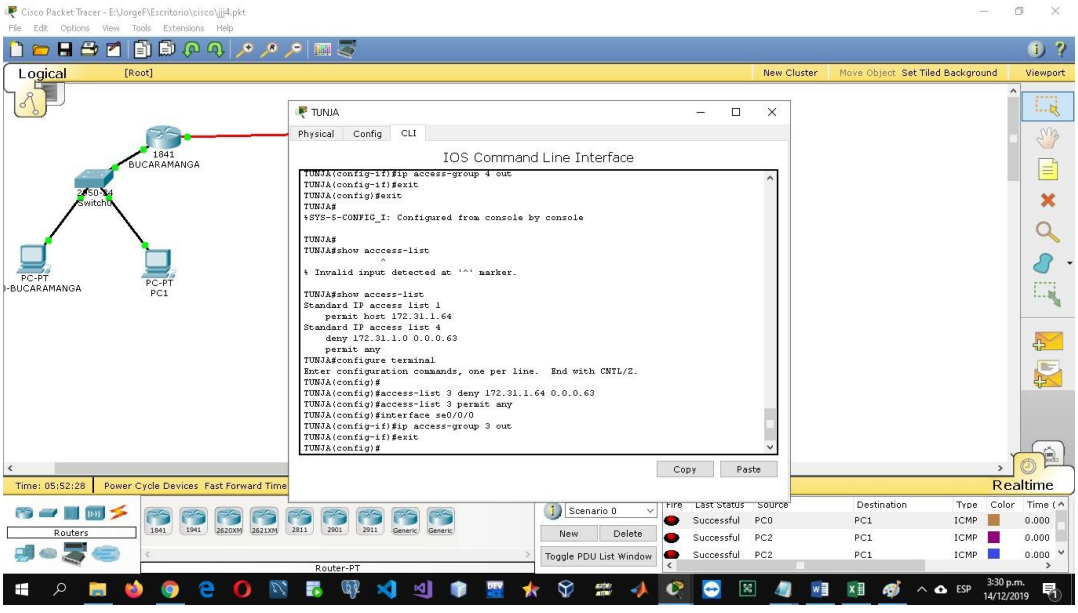

Cisco Packet Tracer - E:\JorgeF\Escritorio\cisco\jjj.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
BUCARAMANGA
Physical
Config
CLI
IOS Command Line Interface
% Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.2.32 0.0.0.3 area 0
% Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.2.0 0.0.0.7 area 0
% Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.0.0 0.0.0.63 area 0
% Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.0.64 0.0.0.63 area 0
% Invalid input detected at '^' marker.
BUCARAMANGA#CONFIGURE TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#
Copy
Paste
1841
BUCARAMANGA
2950-24
Switch0
PC-PT
PC0
PC-PT
PC1
Time: 08:09:57
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
ESP
7:15 p.m.
12/12/2019

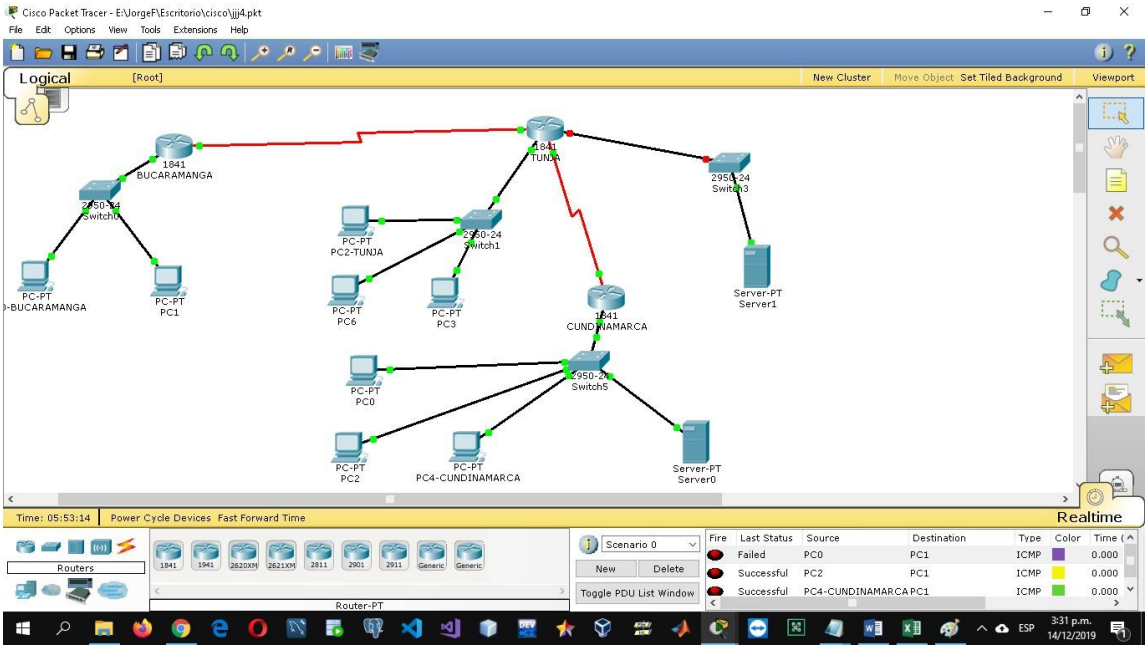

Cisco Packet Tracer - E:\JorgeF\Escritorio\cisco\jjj.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
TUNJA
Physical
Config
CLI
IOS Command Line Interface
TUNJA>
TUNJA>
TUNJA>
TUNJA>enable
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface se0/0/0
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
TUNJA(config)#router ospf 1
TUNJA(config-router)#area 0 authentication
TUNJA(config-router)#
08:46:33: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.33 on Serial0/0/0 from LOADING
to FULL, Loading Done
Copy
Paste
1841
BUCARAMANGA
2950-24
Switch0
PC-PT
PC0
PC-PT
PC1
Time: 08:51:14
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Paste to CLI
Destination
Type
Color
Time (sec)
ESP
7:56 p.m.
12/12/2019



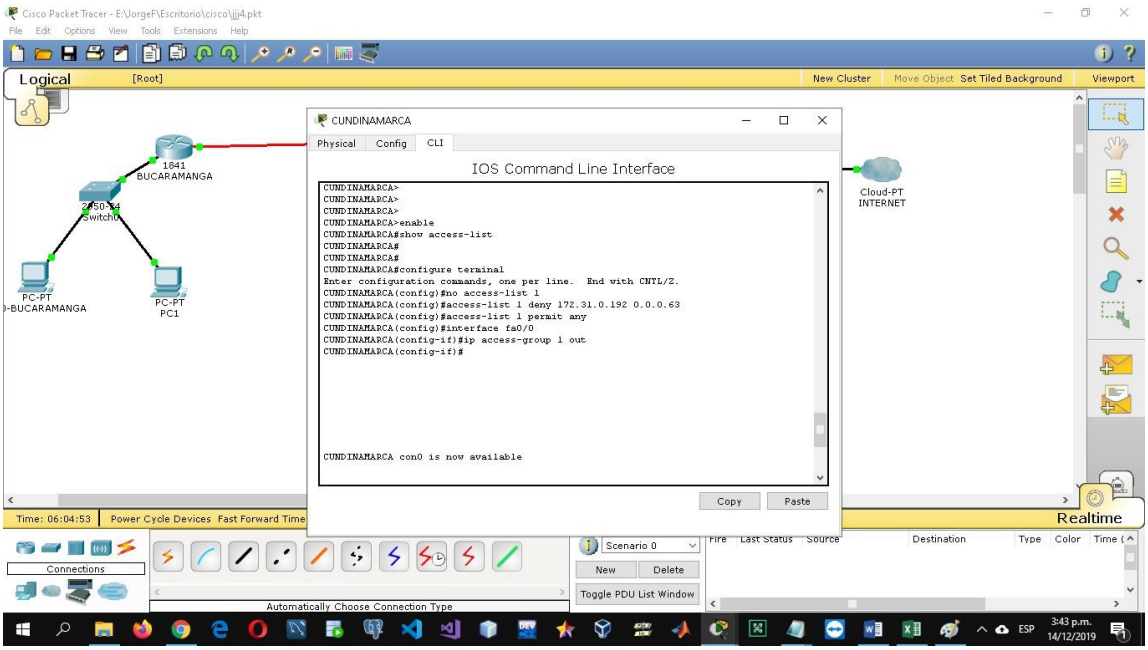

5. Listas de control de acceso:
   - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

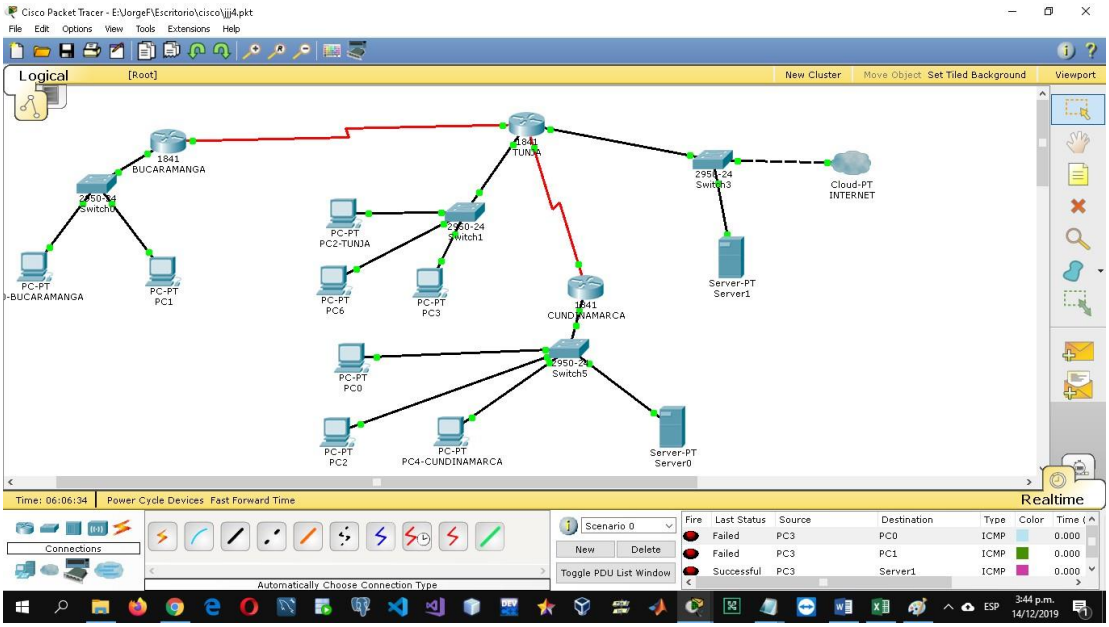
     Se crean las listas de control de acceso






- 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.





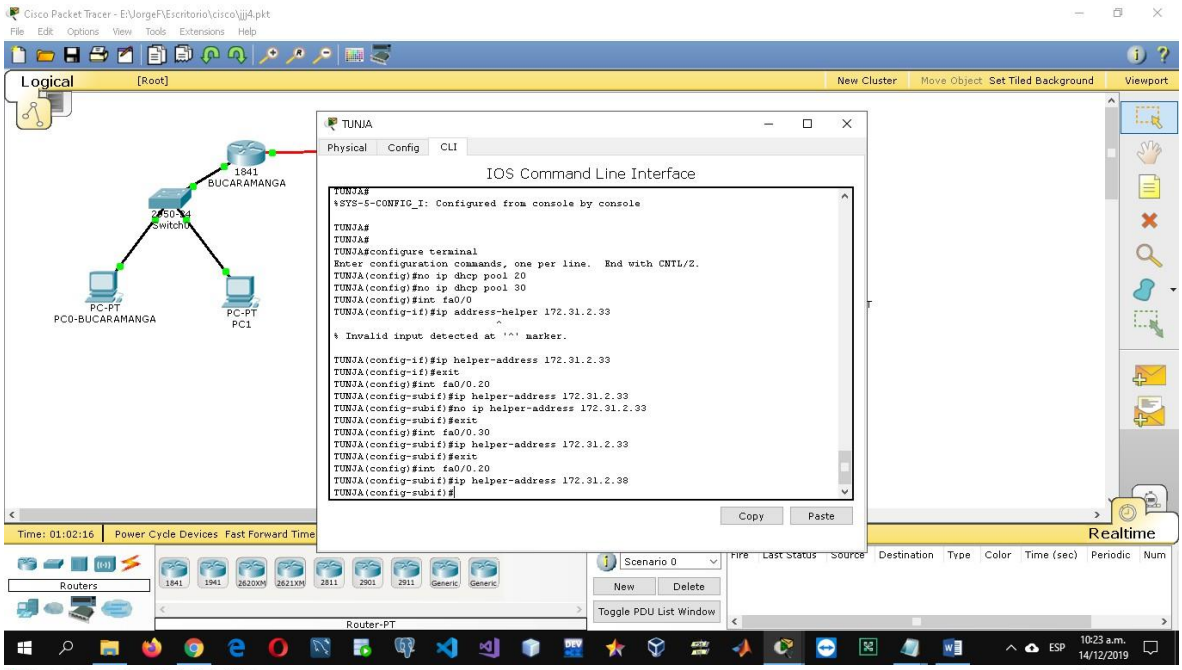

6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.
   Se realiza la tabla de enrutamiento VLSM teniendo en cuenta la dirección dada

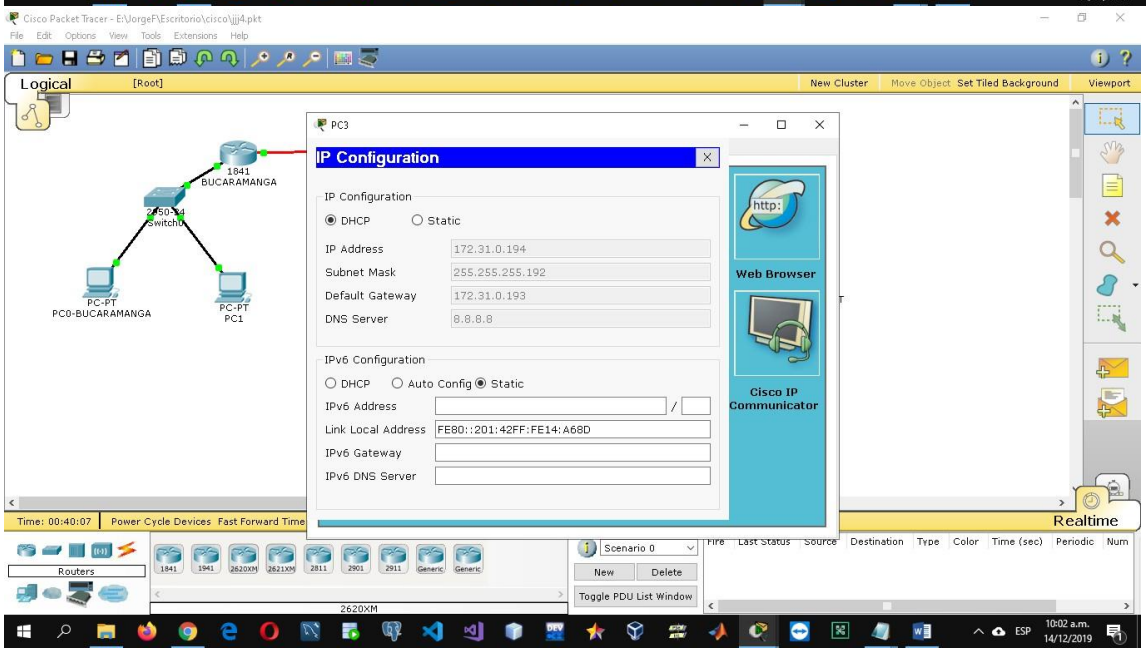
| no | host | host encontrados | direccion de red | mascara | mascara decimal punteada |
|---|---|---|---|---|---|
| 1 | 55 | 62 | 172.31.0.0 | 26 | 255.255.255.192 |
| 2 | 55 | 62 | 172.31.0.64 | 26 | 255.255.255.192 |
| 3 | 40 | 62 | 172.31.0.128 | 26 | 255.255.255.192 |
| 4 | 40 | 62 | 172.31.0.192 | 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 |

**Aspectos a tener en cuenta**

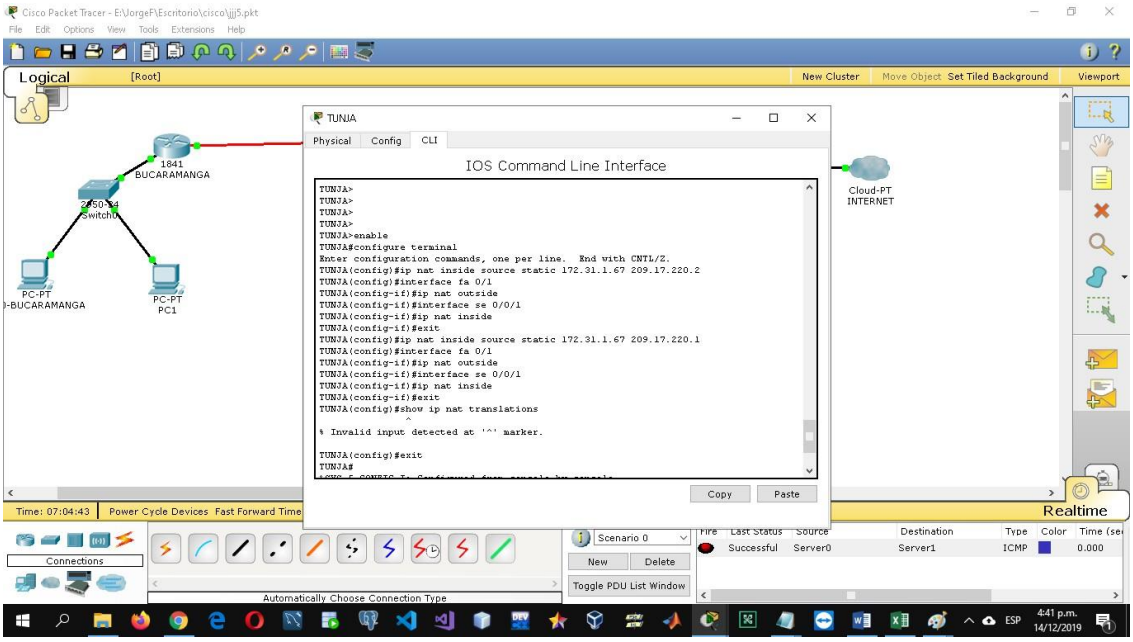
- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

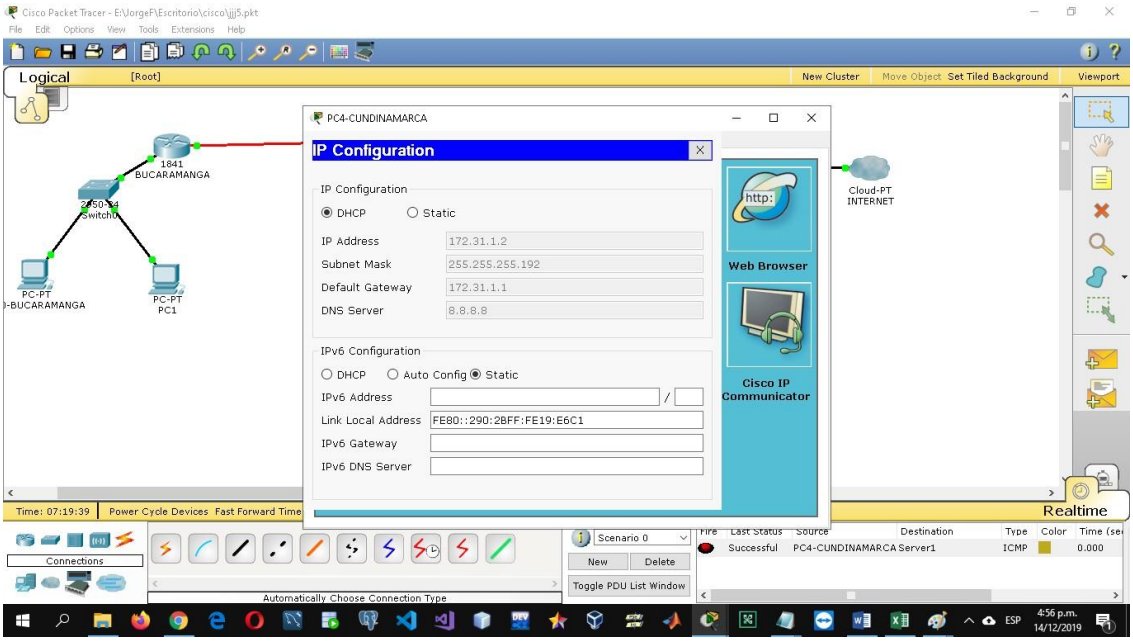
Luego de configurar los pools de direcciones en los router de Bucaramanga y Cundinamarca ingresamos en el modo de configuración del router Tunja, seguidamente entramos en la interfaz por donde vamos a permitir el paso del dchp que en este caso serían las interfaces y subinterfaces fa0/0, fa0/0.20 y fa0/0.30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

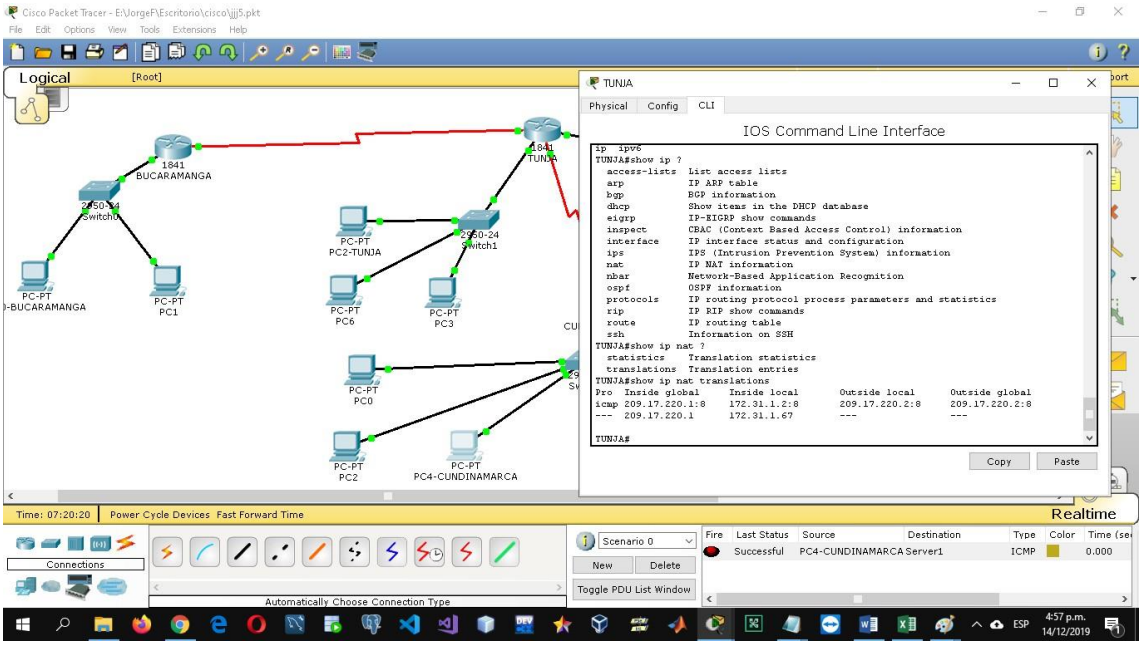


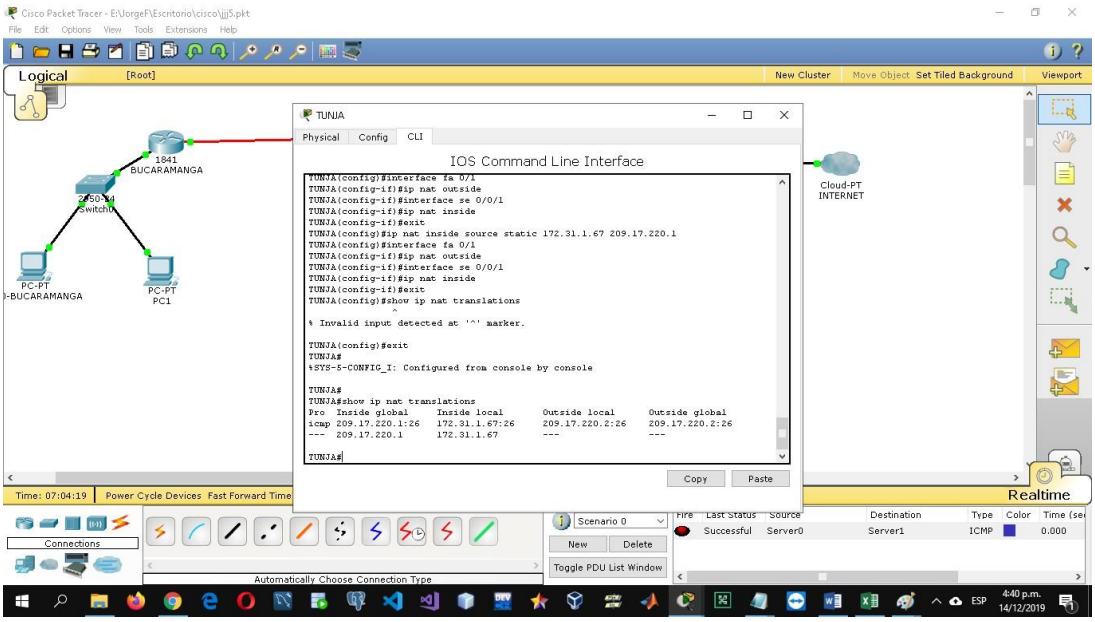



- Configuración de NAT estático y de sobrecarga.






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

## CONCLUSIONES

Durante el desarrollo de cada una de las actividades de CCNA de CISCO , obtuvimos resultados en los procedimientos al momento de configurar una red tanto elemental como complicada, donde identificamos y a su vez analizamos del como configurar dispositivos de red de acuerdo a las pautas necesarias requeridas por la rúbrica de actividades , en el transcurso del diplomado se logro comprender el grado de importancia que se debe tener en todo el equipo de red al momento de estipular las direcciones IP, también de implementar protocolos de seguridad en las diferentes capaz y otros dispositivos más permitiendo una red confidencial y fuerte.

En la etapa de adquisición de conocimiento como estudiante del Curso de CISCO obtuve con mucha disposición las enseñanzas establecidas, ya que me fue muy útil porque así me formo como una persona más competente en el ámbito laboral, y aprendí de forma autónoma.

## BIBLIOGRAFÍA


Temática: DHCP

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Temática: Traducción de direcciones IP para IPv4

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

- Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado 5 junio, 2019, de http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar- dhcp-en-cisco-router/

- Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

- Rosbarbosa, R. B. (2017, 25 septiembre). IP Helper y Relay Agent – Manteniendo un servidor DHCP en otra red.. Recuperado 5 junio, 2019, de https://www.seaccna.com/ip-helper-relay-agent/

Ángel Calvo, A. C. (2015, 11 mayo). RIP Cisco, aprende a configurar este protocolo facilmente.. Recuperado 5 junio, 2019, de https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-y- sencilla/

- Victor E. Martinez G, V. E. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route- router-cisco/

- Juansa, J. (2008, 5 octubre). Solucionando errores TCP/IP. 4 – Uno de los blogs de Juansa. Recuperado 5 junio, 2019, de https://geeks.ms/juansa/2008/10/05/solucionando-errores-tcpip-4/

- Leandro Di Tommaso, L. D. T. (2010, 28 febrero). Configuración de PPP y PAP en Cisco. Recuperado 5 junio, 2019, de https://www.mikroways.net/2010/02/28/configuracion-de-ppp-y-pap-en- cisco/

- Eugenio Duarte, E. D. (2016, 12 abril). Cisco CCNA – Cómo Configurar NAT Overload En Cisco Router. Recuperado 5 junio, 2019, de http://blog.capacityacademy.com/2014/06/18/cisco-ccna-como-configurar- nat-overload-en-cisco-router/