

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

YULEIDY ALEXANDRA BARRETO PAEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ECBTI, INGENIERIA DE SISTEMAS

IBAGUE

2019

CONTENIDO

RESUMEN	5
ABSTRACT	5
INTRODUCCION	6
OBJETIVOS	7
Objetivo General	7
Objetivos Específicos	7
DESARROLLO ESCENARIO 1	8
DESARROLLO ESCENARIO 2	28
CONCLUSIONES	50
BIBLIOGRAFIA	53

RESUMEN

En el presente trabajo se desarrollará La evaluación denominada “Prueba de habilidades prácticas”, la cual forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, cuyo objetivo es identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se disponen de dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show IP, route, entre otros.

Palabras claves

CISCO, CCNA, PROTOCOLOS, CONFIGURACION, SEGURIDAD, ACL, IP, ROUTER, TRACEROUTE, PING, EIGRP, VLMS

ABSTRACT

In the present work, the evaluation developed “Test of practical skills” will be developed, the qualification is part of the evaluation activities of the CCNA Deepening Diploma, whose objective is to identify the degree of development of skills and abilities that were acquired throughout the diploma . The essential thing is to test the levels of understanding and solution of problems related to various aspects of Networking.

There are two (2) proposed scenarios, accompanied by the documentation processes of the solution, corresponding to the registration of the configuration of each of the devices, the specific description of the step by step of each of the stages performed during its development , the registration of connectivity verification processes through the use of ping, traceroute, show ip route commands, among others.

Keywords

CISCO, CCNA, PROTOCOLS, CONFIGURATION, SECURITY, ACL, IP, ROUTER, TRACEROUTE, PING, EIGRP, VLMS

INTRODUCCION

Con la presente actividad se pretende resolver los casos de estudio para el curso CCNA nivel 1 denominado aspectos básicos del Networking y para el curso CCNA nivel 2 denominado conceptos y protocolos de enrutamiento. Es por esto que se desarrollan cada uno de los puntos planteados, de esta manera se logra fortalecer los conocimientos adquiridos durante el curso.

La actividad se desarrolla en el simulador de Cisco "Packet Tracer" esta herramienta permite evaluar los procedimientos realizados y hallar los errores al momento de crear una topología de red, al mismo tiempo de configurar un dispositivo, simular redes, insertar paquetes entre otras.

En el presente informe se encontrará la metodología usada, el desafío consiste en configurar cada uno de los requerimientos de enrutamiento y conmutación, por otra parte, se refuerzan los conocimientos en redes locales virtuales Vlan.

OBJETIVOS

Objetivo General

- Realizar las configuraciones necesarias para las topologías de red propuestas.

Objetivos Específicos

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Subnetear la red indicada para la implementación y solución de la red planteada en el ejercicio
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en Switch, elaboración de Vlans e inter Vlan Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.

DESARROLLO ESCENARIO 1

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.

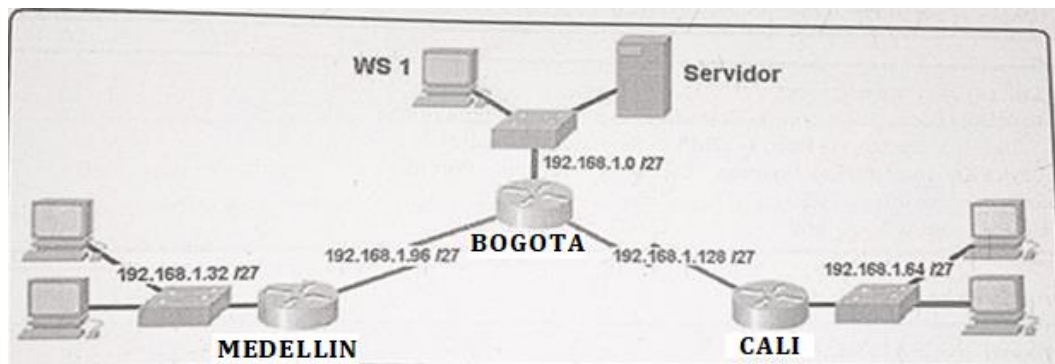
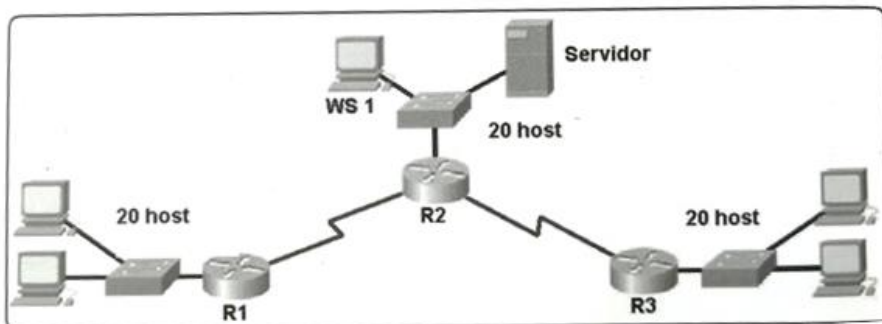
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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.

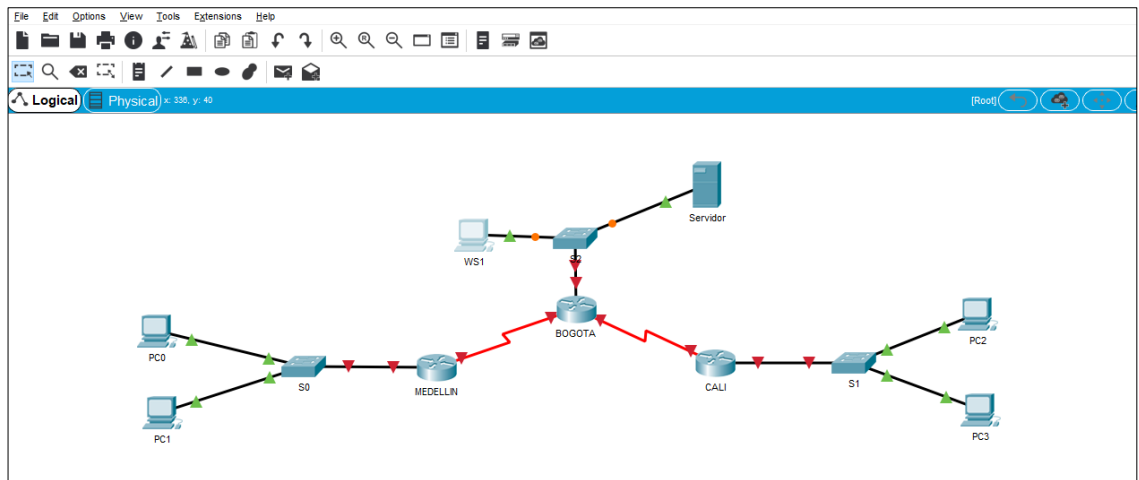
Parte 6: Configuración final



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 física de los equipos con base en la topología de red



```
Switch>
Switch>enable
Switch#
Switch#config t
Switch(config)#
Switch(config)#hostname S1
S1(config)#
S1(config)#enable password admin
S1(config)#exit
S1#
S1#exit
^SYS-5-CONFIG_I: Configured from console by console

Switch>
Switch>enable
Switch#
Switch#config t
Switch(config)#
Switch(config)#hostname S2
S2(config)#
S2(config)#enable password admin
S2(config)#

Switch>enable
Switch#
Switch#
Switch#config t
Switch(config)#
Switch(config)#hostname S3
S3(config)#
S3(config)#enable password admin
S3(config)#
S3(config)#exit
S3#
^SYS-5-CONFIG_I: Configured from console by console
```

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#enable password admin
BOGOTA(config)#
BOGOTA(config)#
BOGOTA(config)#exit
```

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#enable password admin
CALI(config)#
CALI(config)#
CALI(config)#exit
```

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable password admin
MEDELLIN (config)#
MEDELLIN (config)#
MEDELLIN (config)#exit
```



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname S1
S1(config)#
S1(config)#enable password admin
S1(config)#
S1(config)#exit
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname S2
S2(config)#
S2(config)#enable password admin
S2(config)#
S2(config)#exit
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname S3
S3(config)#
S3(config)#enable password admin
S3(config)#
S3(config)#exit
```

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.

No. Red	ID DE RED	RANGO DE DIRECCIONES		BROADCAST
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255
MASK	255.255.255.224			

b. Asignar una dirección IP a la red.

IP de red	192.168.1.1
------------------	--------------------

Parte 2: Configuración Básica.

```
BOGOTA > enable
BOGOTA # configure terminal
BOGOTA (config)# int se0/0/0
BOGOTA (config-if)# ip address 192.168.1.98 255.255.255.224
```

```
BOGOTA (config-if)# exit
BOGOTA (config)#
BOGOTA (config)# int se0/1/0
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA (config-if)# exit
BOGOTA (config)#
BOGOTA(config)#int fa0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
BOGOTA (config-if)# exit
```

```
MEDELLIN > enable
MEDELLIN # configure terminal
MEDELLIN (config)# int se0/0/0
MEDELLIN (config-if)# ip address 192.168.1.99 255.255.255.224
MEDELLIN (config-if)# exit
MEDELLIN (config)#
MEDELLIN (config)#int fa0/0
MEDELLIN (config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN (config-if)#no shutdown
MEDELLIN (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
MEDELLIN (config-if)# exit
```

```

CALI > enable
CALI # configure terminal
CALI (config)# int se0/1/0
CALI (config-if)# ip address 192.168.1.131 255.255.255.224
CALI (config-if)# exit
CALI (config)#
CALI (config)#int fa0/0
CALI (config-if)#ip address 192.168.1.65 255.255.255.224
CALI (config-if)#no shutdown
CALI (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
CALI (config-if)# exit

```

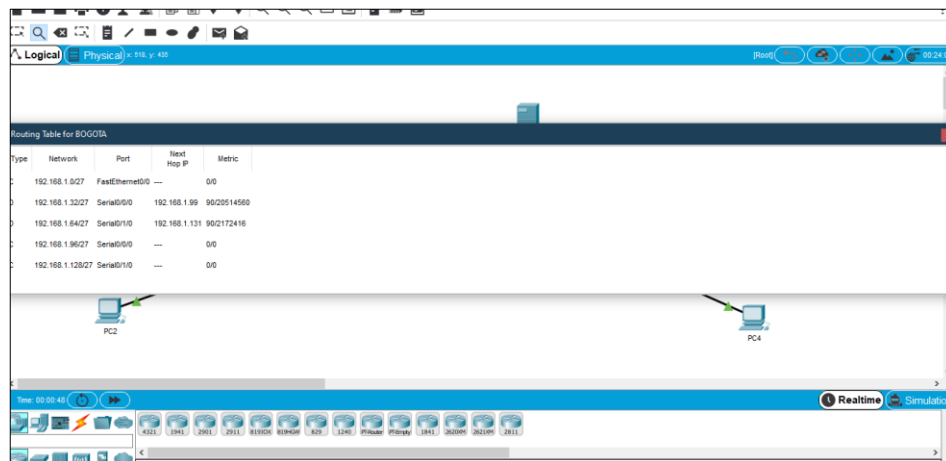
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	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
Nombre de Host	PC 1	WS1	PC 3
Direccionamiento IP en interfaz	FA 0/4	FA 0/5	FA 0/4
Dirección IP	192.168.1.34	192.168.1.2	192.168.1.66

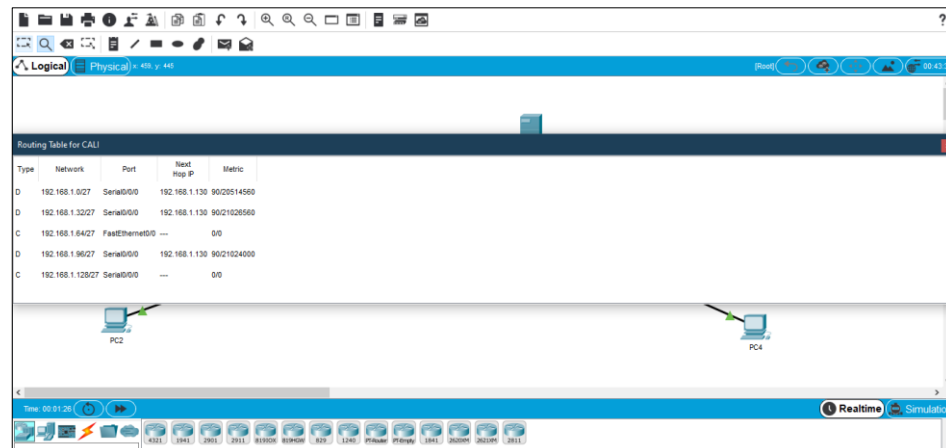
Mask	255.255.255.224	255.255.255.224	255.255.255.224
Default Gateway	192.168.1.33	192.168.1.1	192.168.1.65
Nombre de Host	PC 2	SERVIDOR	PC 4
Direccionamiento IP en interfaz	FA 0/5	FA 0/6	FA 0/5
Dirección IP	192.168.1.35	192.168.1.3	192.168.1.67
Mask	255.255.255.224	255.255.255.224	255.255.255.224
Default Gateway	192.168.1.33	192.168.1.1	192.168.1.65

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.

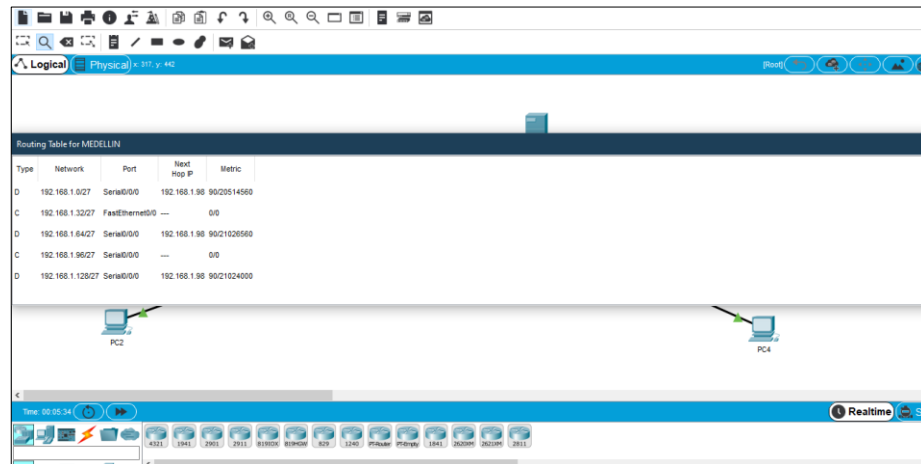
ROUTER BOGOTA



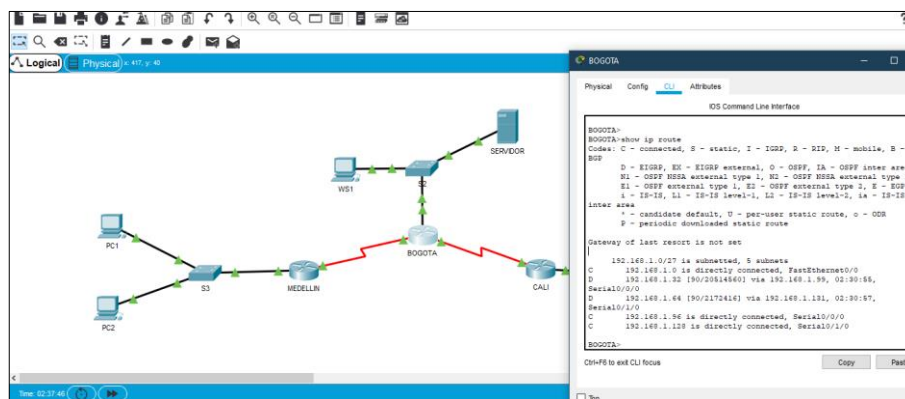
ROUTER CALI



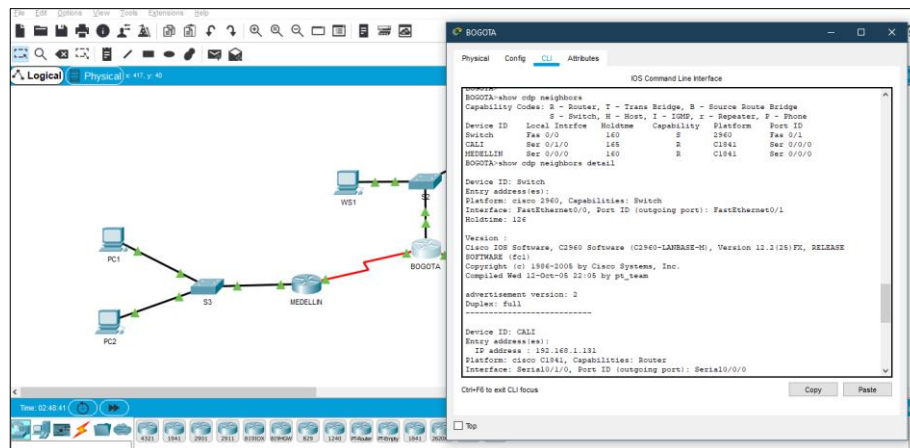
ROUTER MEDELLIN

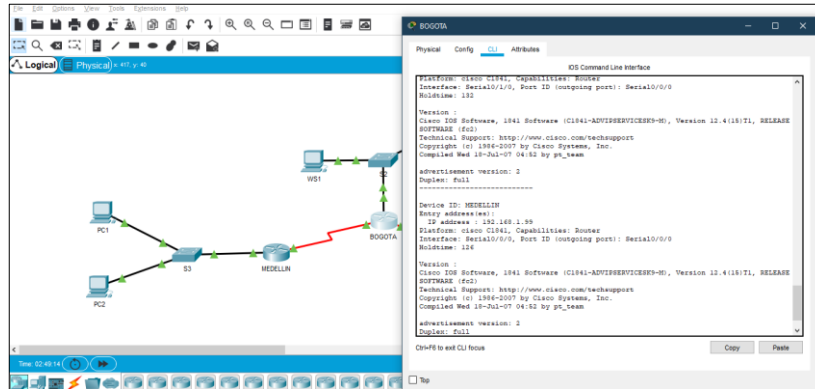


c. Verificar el balanceo de carga que presentan los routers.



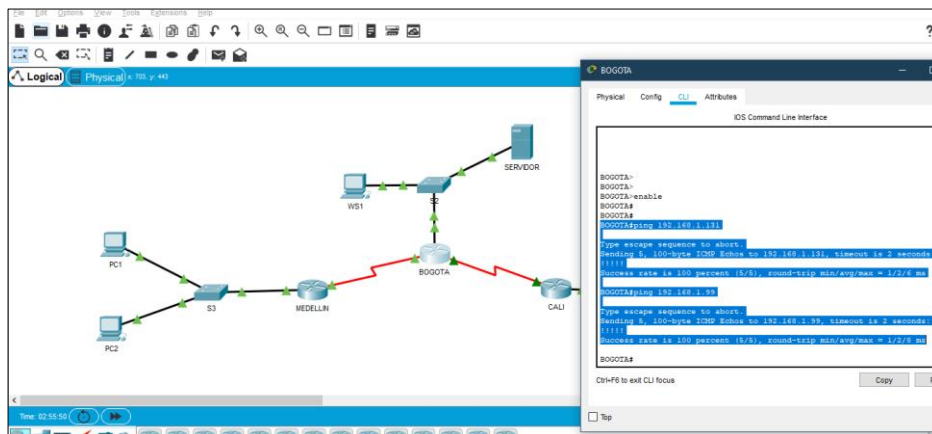
d. Realizar un diagnóstico de vecinos usando el comando cdp.



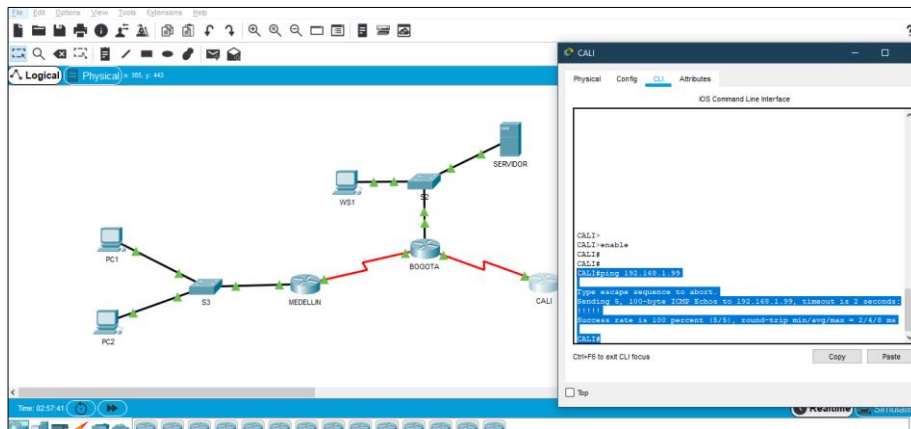


e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

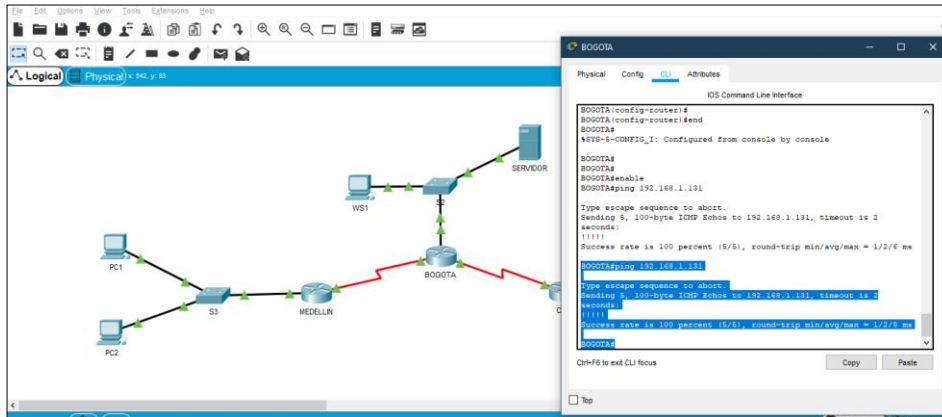
ROUTER BOGOTA a CALI y MEDELLIN



ROUTER CALI a MEDELLIN



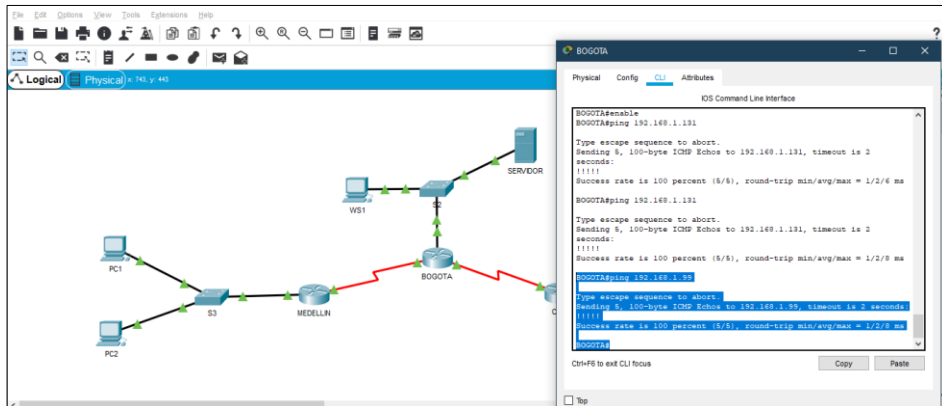
ROUTER BOGOTA a CALI



The screenshot shows the Packet Tracer interface with a network diagram and the CLI of Router Bogota. The network diagram includes PC1, PC2, S3, MEDELLIN, BOGOTA, WS1, and SERVIDOR. The CLI window shows the following commands and output:

```
BOGOTA(config-router)#  
BOGOTA(config-router)#end  
BOGOTA#  
BOGOTA#show ip interface brief  
BOGOTA#enable  
BOGOTA#ping 192.168.1.131  
Type escape sequence to abort:  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
!!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms  
BOGOTA#ping 192.168.1.131  
Type escape sequence to abort:  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
!!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms  
BOGOTA#
```

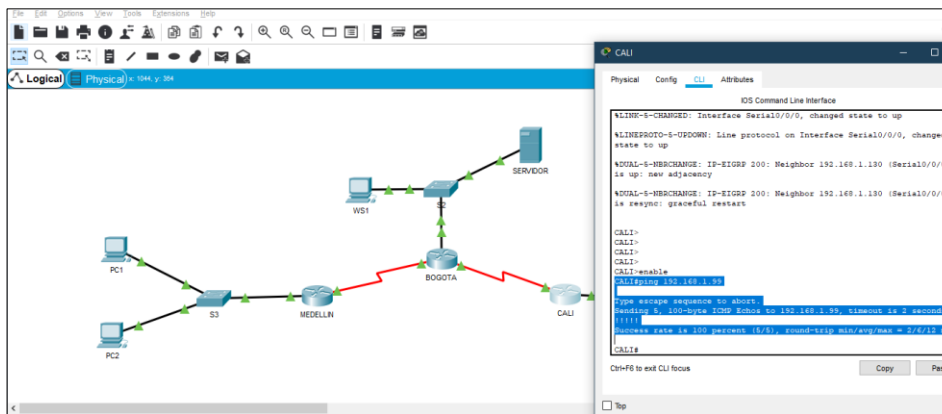
ROUTER BOGOTA a MEDELLIN



The screenshot shows the Packet Tracer interface with a network diagram and the CLI of Router Bogota. The network diagram includes PC1, PC2, S3, MEDELLIN, BOGOTA, WS1, and SERVIDOR. The CLI window shows the following commands and output:

```
BOGOTA#enable  
BOGOTA#ping 192.168.1.131  
Type escape sequence to abort:  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
!!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms  
BOGOTA#ping 192.168.1.131  
Type escape sequence to abort:  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
!!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms  
BOGOTA#
```

ROUTER CALI a MEDELLIN



The screenshot shows the Packet Tracer interface with a network diagram and the CLI of Router Cali. The network diagram includes PC1, PC2, S3, MEDELLIN, BOGOTA, WS1, and SERVIDOR. The CLI window shows the following commands and output:

```
!LINEAR-CHANGED: Interface Serial0/0/0, changed state to up  
!LINEPROTO-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up  
NDAL-5-NEIGHBORCHANGE: IP-IGMP 200: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency  
NDAL-5-NEIGHBORCHANGE: IP-IGMP 200: Neighbor 192.168.1.130 (Serial0/0/0) is reorg: graceful restart  
CALI#  
CALI#  
CALI#  
CALI#enable  
CALI#ping 192.168.1.131  
Type escape sequence to abort:  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
!!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/13 ms  
CALI#
```

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

ROUTER CALI

Routing Table for CALI

Type	Network	Port	Next Hop IP	Metric
D	192.168.1.0/27	Serial0/0/0	192.168.1.130 90/20514560	
D	192.168.1.32/27	Serial0/0/0	192.168.1.130 90/21026560	
C	192.168.1.64/27	FastEthernet0/0	---	0/0
D	192.168.1.96/27	Serial0/0/0	192.168.1.130 90/21024000	
C	192.168.1.128/27	Serial0/0/0	---	0/0

PC2 PC4

ROUTER BOGOTA

Routing Table for BOGOTA

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/27	FastEthernet0/0	---	0/0
D	192.168.1.32/27	Serial0/0/0	192.168.1.99 90/20514560	
D	192.168.1.64/27	Serial0/1/0	192.168.1.131 90/2172416	
C	192.168.1.96/27	Serial0/0/0	---	0/0
C	192.168.1.128/27	Serial0/1/0	---	0/0

PC2 PC4

ROUTER MEDELLIN

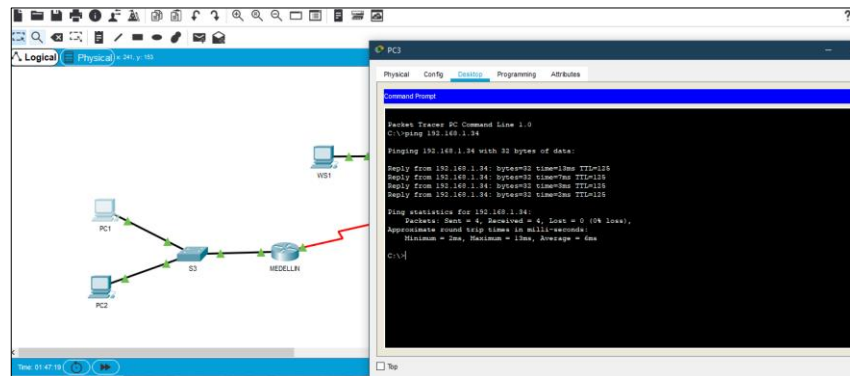
Routing Table for MEDELLIN

Type	Network	Port	Next Hop IP	Metric
D	192.168.1.0/27	Serial0/0/0	192.168.1.98 90/20514560	
C	192.168.1.32/27	FastEthernet0/0	---	0/0
D	192.168.1.64/27	Serial0/0/0	192.168.1.98 90/21026560	
C	192.168.1.96/27	Serial0/0/0	---	0/0
D	192.168.1.128/27	Serial0/0/0	192.168.1.98 90/21024000	

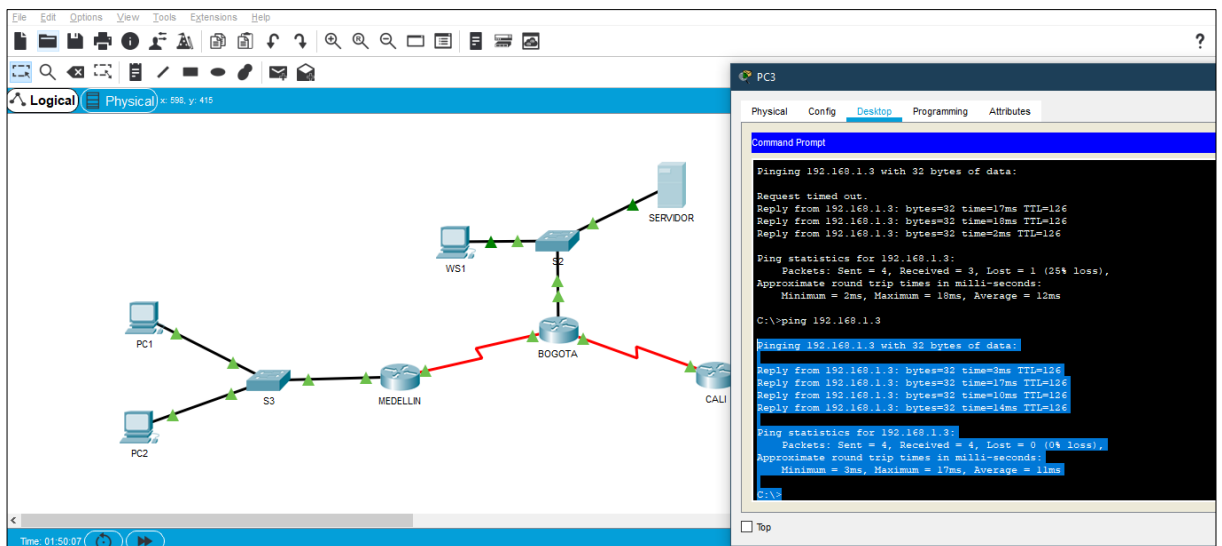
PC2 PC4

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.

PC3 RED CALI a PC1 RED MEDELLIN



PC3 RED CALI a 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:


```
BOGOTA> enable
BOGOTA# configure terminal
BOGOTA(config)# line vty 0 4
BOGOTA(config-line)# password BOGOTA
BOGOTA(config-line)# login
BOGOTA(config-line)# exit
```

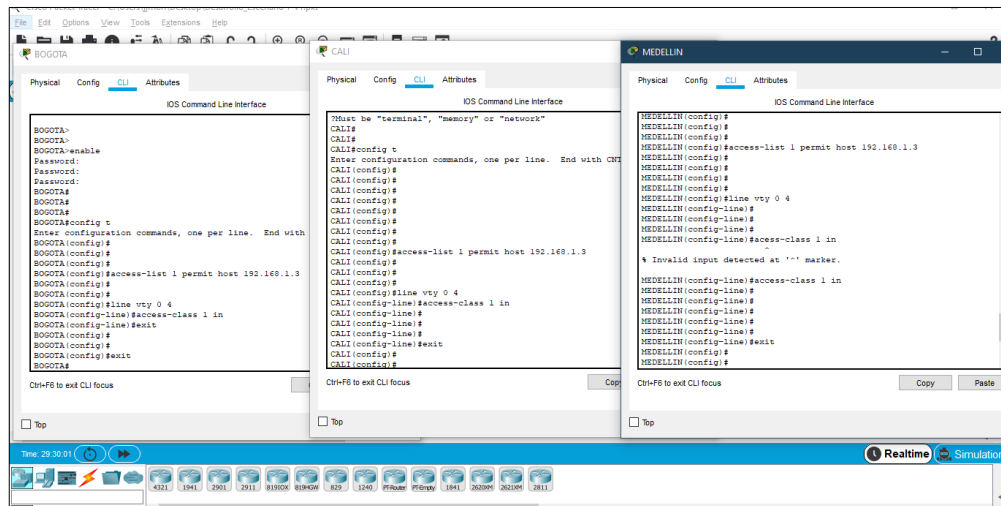
ROUTER MEDELLIN

The screenshot shows a network simulator interface with a network topology on the left and a CLI window for the MEDELLIN router on the right. The topology includes a central router labeled 'MEDELLIN' connected to other routers: 'S3', 'BOGOTA', and 'CALI'. 'S3' is connected to 'PC1' and 'PC2'. 'BOGOTA' is connected to 'WS1' and 'SERVER'. The CLI window shows the following configuration commands:

```
MEDELLIN> enable
MEDELLIN# configure terminal
MEDELLIN#
MEDELLIN#
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#
MEDELLIN(config)#
MEDELLIN(config)#
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password MEDELLIN
MEDELLIN(config-line)#login
MEDELLIN(config-line)#
MEDELLIN(config-line)#
MEDELLIN(config-line)#exit
MEDELLIN(config)#
MEDELLIN(config)#
MEDELLIN(config)#
MEDELLIN(config)#
```

```
MEDELLIN> enable
MEDELLIN# configure terminal
MEDELLIN(config)# line vty 0 4
MEDELLIN(config-line)# password MEDELLIN
MEDELLIN(config-line)# login
MEDELLIN(config-line)# exit
```

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.



```

BOGOTA>enable
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)# acces-list 1 permit host 192.168.1.3
BOGOTA (config)# line vty 0 4
BOGOTA (config-line)# access-class 1 in
BOGOTA (config-line)# exit

```

```

CALI>enable
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)# acces-list 1 permit host 192.168.1.3
CALI (config)# line vty 0 4
CALI (config-line)# access-class 1 in
CALI (config-line)# exit

```

```

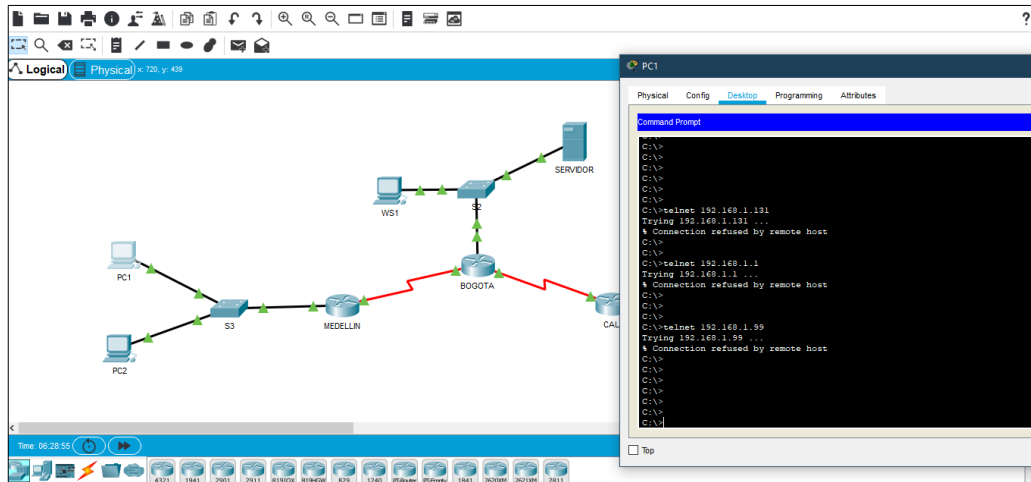
MEDELLIN> enable
MEDELLIN# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN (config)# acces-list 1 permit host 192.168.1.3
MEDELLIN (config)# line vty 0 4
MEDELLIN (config-line)# access-class 1 in
MEDELLIN (config-line)# exit

```

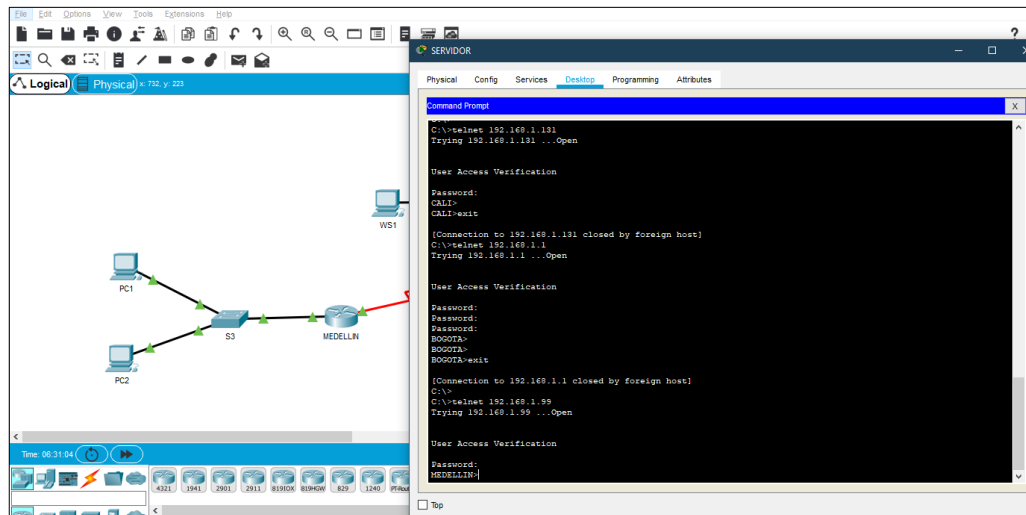
Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.

ACEESO DENEGADO DESDE OTRO HOST



ACEESO PERMITIDO DESDE EL SERVIDOR



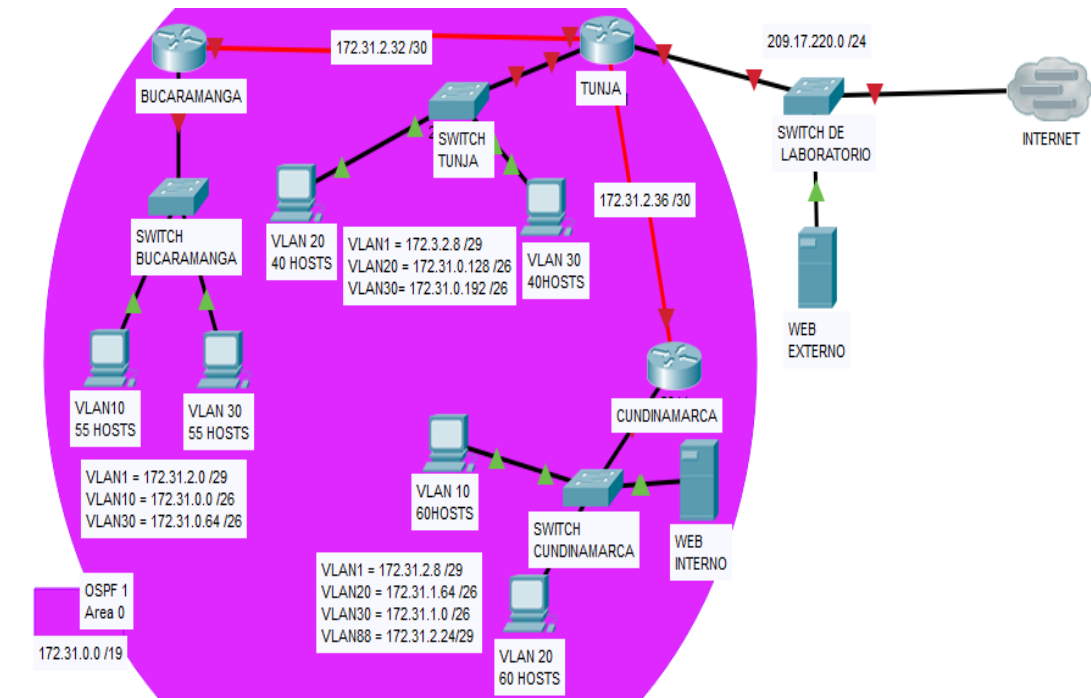
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	DENY
	WS_1	Router BOGOTA	DENY
	Servidor	Router CALI	PERMIT
	Servidor	Router MEDELLIN	PERMIT
TELNET	LAN del Router MEDELLIN	Router CALI	DENY
	LAN del Router CALI	Router CALI	DENY
	LAN del Router MEDELLIN	Router MEDELLIN	DENY
	LAN del Router CALI	Router MEDELLIN	DENY
PING	LAN del Router CALI	WS_1	PERMIT
	LAN del Router MEDELLIN	WS_1	PERMIT
	LAN del Router MEDELLIN	LAN del Router CALI	PERMIT
PING	LAN del Router CALI	Servidor	PERMIT
	LAN del Router MEDELLIN	Servidor	PERMIT
	Servidor	LAN del Router MEDELLIN	PERMIT
	Servidor	LAN del Router CALI	PERMIT
	Router CALI	LAN del Router MEDELLIN	PERMIT
	Router MEDELLIN	LAN del Router CALI	PERMIT

DESARROLLO ESCENARIO 2

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.



Desarrollo

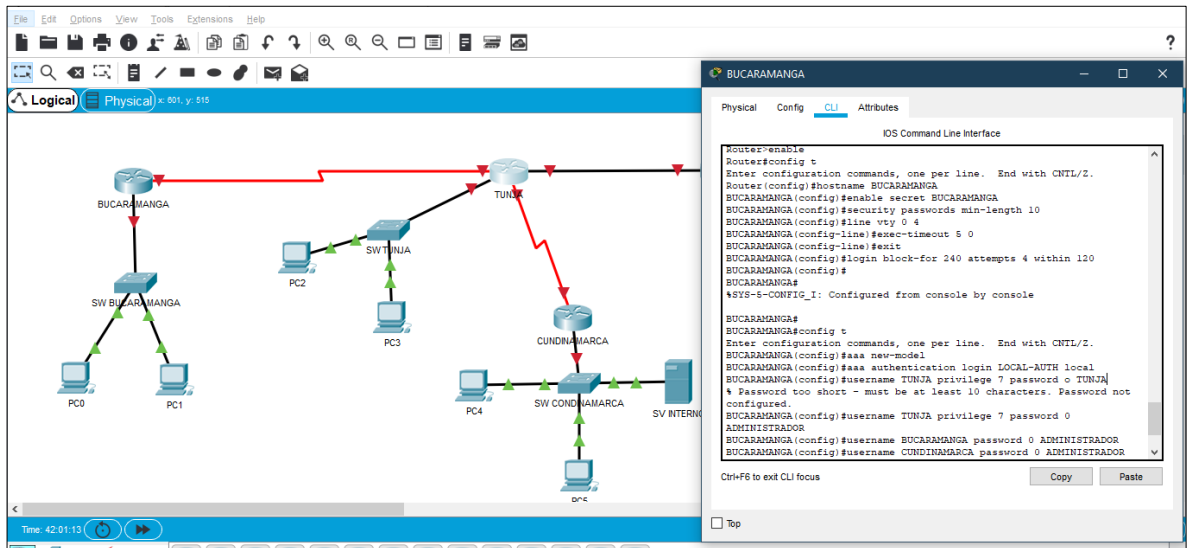
Los siguientes son los requerimientos necesarios:

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.

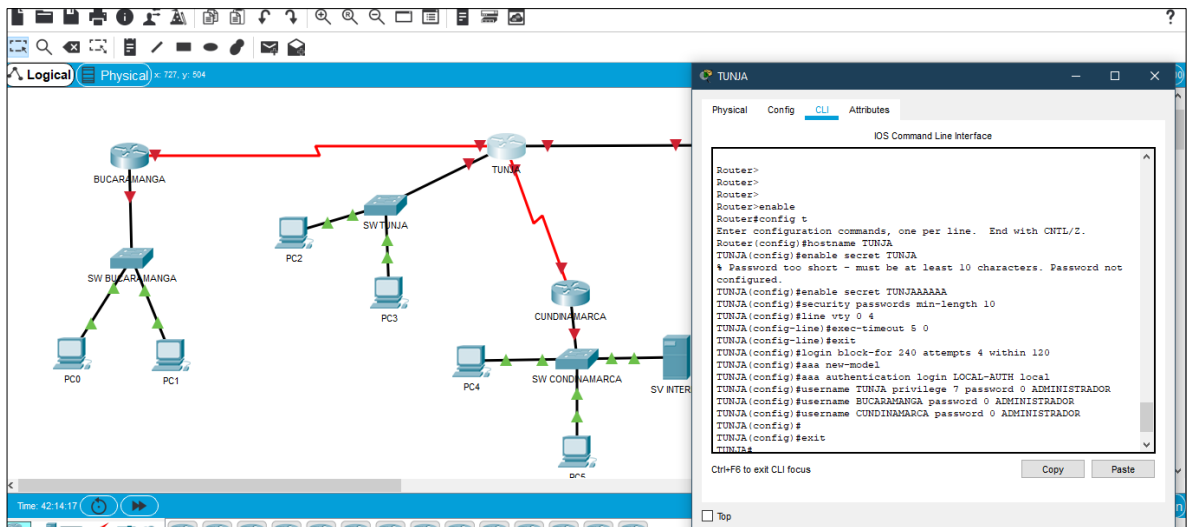
ROUTER BUCARAMANGA

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable secret BUCARAMANGA
BUCARAMANGA(config)#security passwords min-length 10
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#exec-timeout 5 0
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#login block-for 240 attempts 4 within 120
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login LOCAL-AUTH local
BUCARAMANGA(config)#username TUNJA privilege 7 password 0
ADMINISTRADOR
BUCARAMANGA(config)#username BUCARAMANGA password 0
ADMINISTRADOR
BUCARAMANGA(config)#username CUNDINAMARCA password 0
ADMINISTRADOR
BUCARAMANGA(config)#exit
```



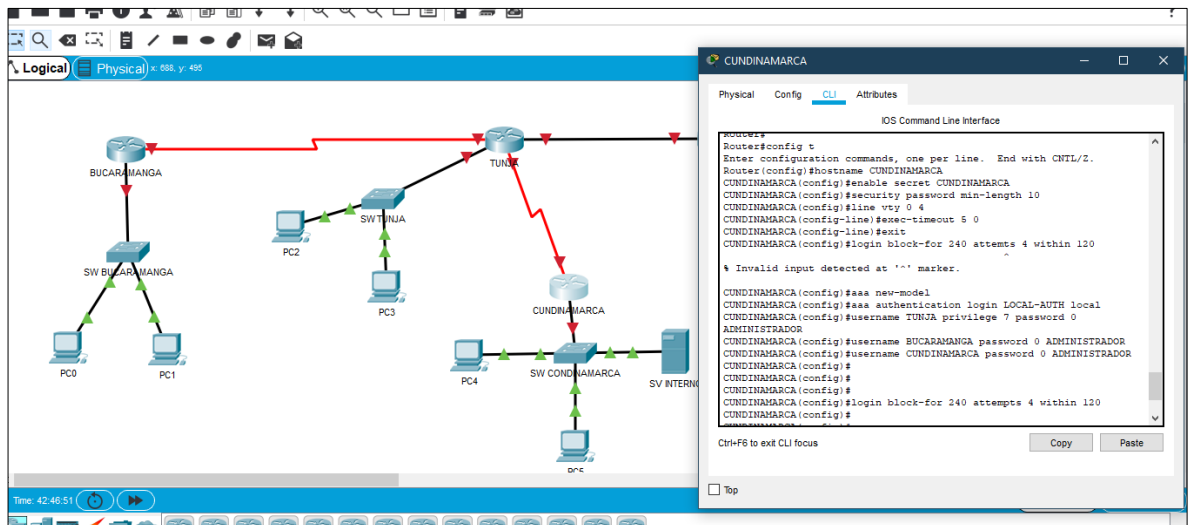
ROUTER TUNJA

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#enable secret TUNJAAAAAA
TUNJA(config)#security passwords min-length 10
TUNJA(config)#line vty 0 4
TUNJA(config-line)#exec-timeout 5 0
TUNJA(config-line)#exit
TUNJA(config)#login block-for 240 attempts 4 within 120
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login LOCAL-AUTH local
TUNJA(config)#username TUNJA privilege 7 password 0 ADMINISTRADOR
TUNJA(config)#username BUCARAMANGA password 0 ADMINISTRADOR
TUNJA(config)#username CUNDINAMARCA password 0 ADMINISTRADOR
TUNJA(config)#exit
```



ROUTER CUNDINAMARCA

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable secret CUNDINAMARCA
CUNDINAMARCA(config)#security passwords min-length 10
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#exec-timeout 5 0
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#login block-for 240 attempts 4 within 120
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login LOCAL-AUTH local
CUNDINAMARCA(config)#username TUNJA privilege 7 password 0
ADMINISTRADOR
CUNDINAMARCA(config)#username BUCARAMANGA password 0
ADMINISTRADOR
CUNDINAMARCA(config)#username CUNDINAMARCA password 0
ADMINISTRADOR
CUNDINAMARCA(config)#exit
```



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

ROUTER ISP

```
ISP#
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#
ISP(config)# area 0 authentication message-digest
ISP(config)# Network 172.31.0.128 0.0.0.63 area 0
ISP(config)# Network 172.31.0.19X 0.0.0.63 area 0
ISP(config)# Network 172.31.2.8 0.0.0.7 area 0
ISP(config)# Network 172.31.2.32 0.0.0.7 area 0
ISP(config)# Defaul-information originate
ISP(config)#exit

ISP(config)# Ip dhcp pool bucaramanga-30
ISP(config)# Network 172.31.0.64 255.255.255.192
ISP(config)# Defaul_router 172.31.0.65
ISP(config)# Ip dhcp Pool t-10
ISP(config)# Network 172.31.1.0 255.255.255.192
ISP(config)# Defaul_router 172.31.1.1
ISP(config)# Ip dhcp Pool t-20
ISP(config)# Network 172.31.1.64 255.255.255.192
ISP(config)# Defaul_router 172.31.1.65
ISP(config)# Ip dhcp Pool bucaramanga-10
ISP(config)# Network 172.31.0.0 255.255.255.192
ISP(config)# Defaul_router 172.31.0.1
ISP(config)#exit

ISP(config)# Ip dhcp excluded-address 172.31.1.65 172.31.1.70
ISP(config)# Ip dhcp excluded-address 192.31.1.1 172.31.1.5
ISP(config)# Ip dhcp excluded-address 172.31.0.1 172.31.0.5
ISP(config)# Ip dhcp excluded-address 172.31.065 172.31.0.70

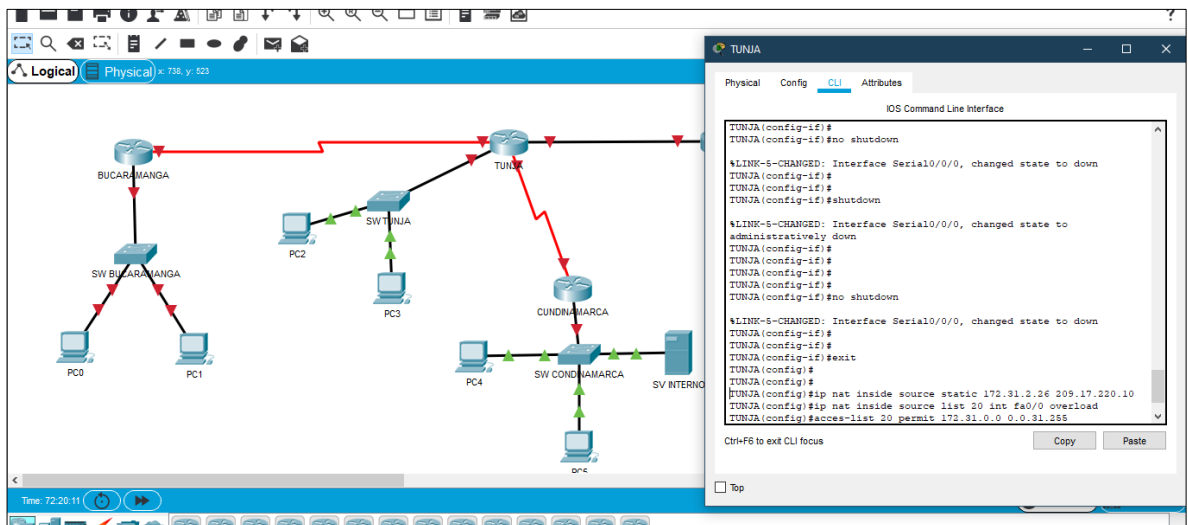
ISP(config)# Ip dhcp pool bucaramanga-30
ISP(config)# Network 172.31.0.64 255.255.255.192
ISP(config)# Defaul_router 172.31.0.65
ISP(config)# Ip dhcp Pool t-10
ISP(config)# Network 172.31.1.0 255.255.255.192
ISP(config)# Defaul_router 172.31.1.1
ISP(config)# Ip dhcp Pool t-20
```

```
ISP(config)# Network 172.31.1.64 255.255.255.192
ISP(config)# Defaul_router 172.31.1.65
ISP(config)# Ip dhcp Pool bucaramanga-10
ISP(config)# Network 172.31.0.0 255.255.255.192
ISP(config)# Defaul_router 172.31.0.1
ISP(config)#end
```

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

ROUTER TUNJA

```
TUNJA>
TUNJA>enable
Password:
TUNJA#config t
TUNJA(config)#ip nat inside source static 172.31.2.26 209.17.220.10
TUNJA(config)#ip nat inside source list 20 int fa0/0 overload
TUNJA(config)#access-list 20 permit 172.31.0.0 0.0.31.255
TUNJA(config)#exit
```



4. El enrutamiento deberá tener autenticación.

ROUTER CUNDINAMARCA

```
CUNDINAMARCA>
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int se0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.37 255.255.255.252
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 7
ADMINISTRADOR
CUNDINAMARCA(config-if)# Area 0 authentication messag-digest
```

ROUTER TUNJA

```
TUNJA>
TUNJA>enable
Password:
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int se0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 64000
TUNJA(config-if)#exit
TUNJA(config)#int se0/0/1
TUNJA(config-if)#ip address 172.31.2.38 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#Area 0 authentication messag-digest
```


ROUTER BUCARAMANGA

```
BUCARAMANGA>
BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
BUCARAMANGA(config)#int se0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#ip ospf message-digest-key md5 7 ADMINISTRADOR
BUCARAMANGA (config-if)#Area 0 authentication messag-digest
```

5. Listas de control de acceso:

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
- Los hosts de VLAN 10 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.
- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

SWITCH BUCARAMANGA

```
SWBU>
SWBU>enable
SWBU#config t
SWBU#Log-adjacency-changes
SWBU#Área 0 authentication message-digest
SWBU# Access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255
eq bootps
```

```
SWBU# Access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
SWBU# Access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
SWBU# Access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255
eq bootps
SWBU# Access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.255.255
SWBU# Access-list 101 permit ip 172.31.1.64 0.0.0.63 any
SWBU# exit
```

SWITCH TUNJA

```
SWTU>
SWTU>enable
SWTU#config t
SWTU#Log-adjacency-changes
SWTU#Area 0 authentication message-digest
SWTU# Access-list 20 permit 172.31.0.0 0.0.31.255
SWTU# Access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
SWTU# Access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
SWTU# Access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www
SWTU# Access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
SWTU#exit
```

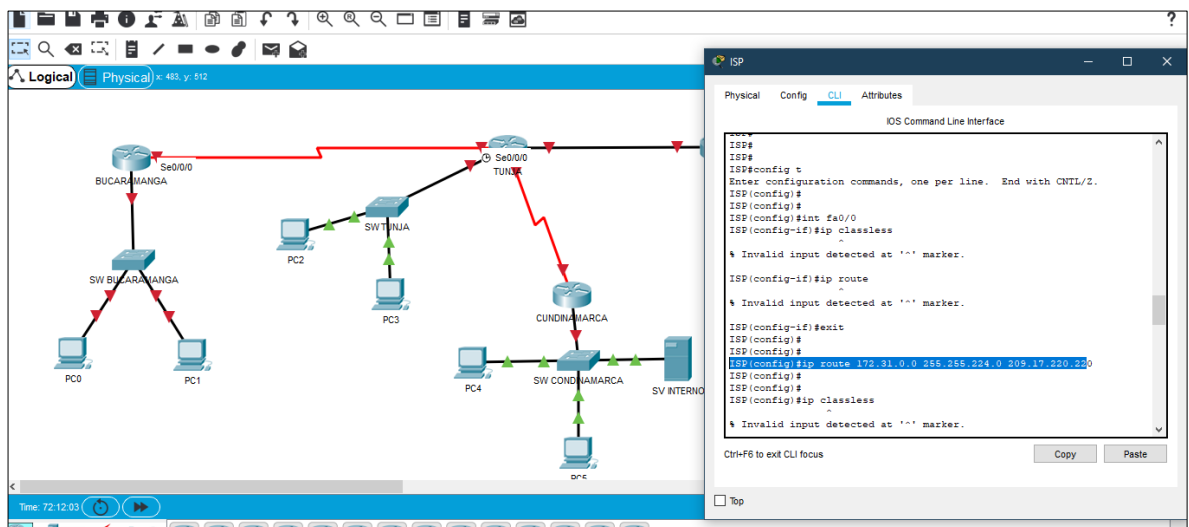
SWITCH CUNDINAMARCA

```
SWCU>
SWCU>enable
SWCU#config t
SWCU#Log-adjacency-changes
SWCU#Area 0 authentication message-digest
SWCU# Access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255
eq bootps
SWCU# Access-list 101 permit ip 172.31.X 0.0.0.63 172.31.0.128 0.0.0.63
SWCU#
SWCU# Access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255
eq bootps
SWCU# Access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.255.255
SWCU# Access-list 103 permit ip 172.31.0.64 0.0.0.63 any
SWCU#exit
```

6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

ROUTER ISP

```
ISP#  
ISP#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
ISP(config)#  
ISP(config)#ip route 172.31.0.0 255.255.224.0 209.17.220.220  
ISP(config)#exit
```



Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.

SWITCH BUCARAMANGA

```
Switch>  
Switch>enable  
Switch#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname SWBU  
SWBU(config)#enable password admin  
SWBU(config-line)#int vlan1
```

```

SWBU(config-if)#ip address 172.31.2.2 255.255.255.248
SWBU(config-if)#ip default-gateway 172.31.2.1
SWBU(config)#
SWBU(config)#int range fa0/12-24
SWBU(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
SWBU(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13,
changed state to down

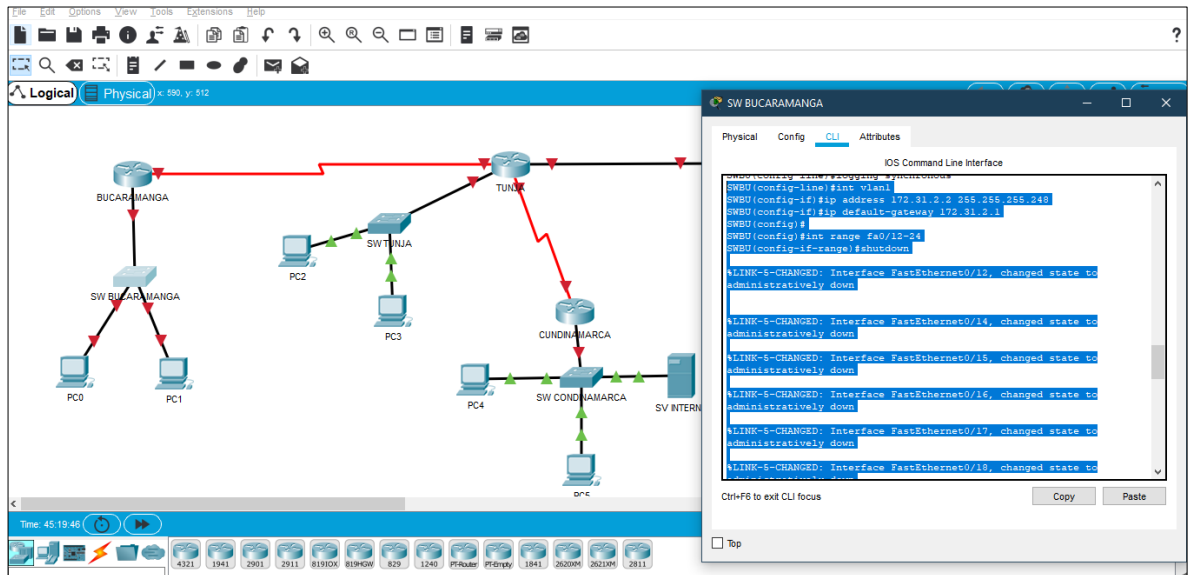
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,
changed state to down

SWBU(config-if-range)#exit
SWBU(config)#int vlan1
SWBU(config-if)#no shutdown

```

```
SWBU(config-if)#  
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```



SWITCH CUNDINAMARCA

```
Switch>
```

```
Switch>enable
```

```
Switch#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#hostname SWCU
```

```
SWCU(config)#no ip domain-lookup
```

```
SWCU(config)#enable password admin
```

```
SWCU(config-line)#int vlan1SWCU(config-if)#ip address 172.31.2.2 255.255.255.248
```

```
SWCU(config-if)#ip default-gateway 172.31.2.1
```

```
SWCU(config)#int range fa0/4-24
```

```
SWCU(config-if-range)#shutdown
```

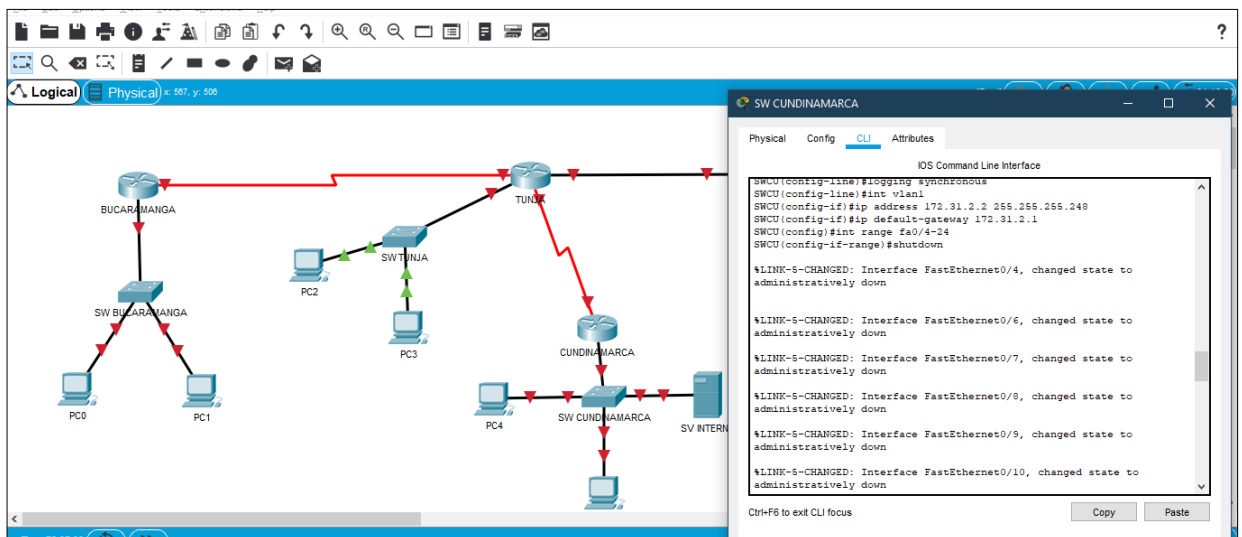
```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively  
down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively
down
SWCU(config-if-range)#
```

```

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed
state to down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
state to down
SWCU(config-if-range)#int vlan1
SWCU(config-if)#no shutdown
SWCU(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

```



SWITCH TUNJA

```

Switch>
Switch>enable

```

```
Switch#
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWTU
SWTU(config)#enable password admin
SWTU(config-line)#int vlan1
SWTU(config-if)#ip address 172.31.2.2 255.255.255.248
SWTU(config-if)#ip default-gateway 172.31.2.1
WTU(config)#int range fa0/12-23
SWTU(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
SWTU(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13,
changed state to down
```



```
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
```

```
SWTU(config-if-range)#exit
```

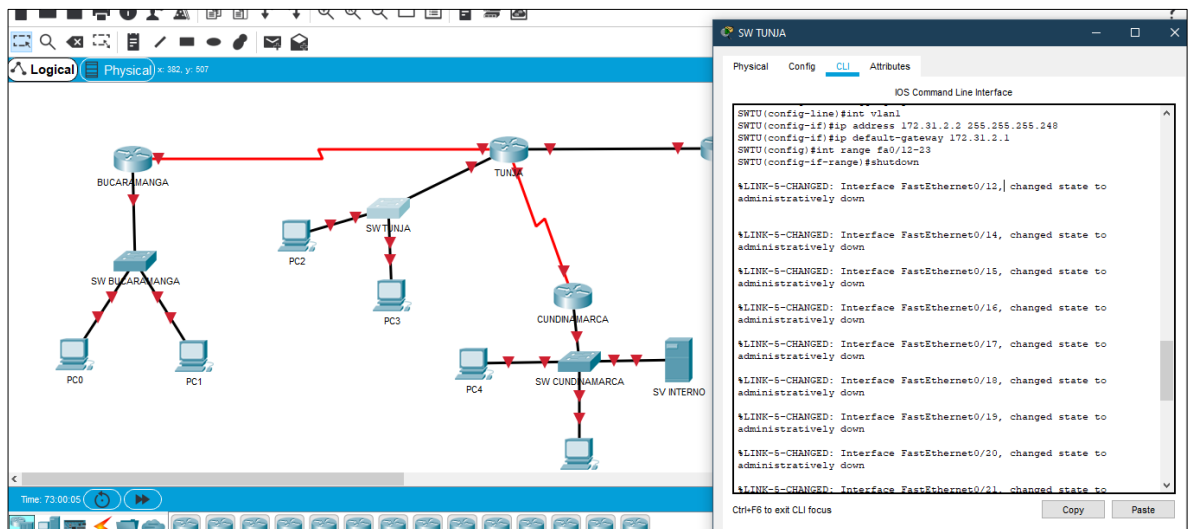
```
SWTU(config)#
```

```
SWTU(config)#int vlan1
```

```
SWTU(config-if)#no shutdown
```

```
SWTU(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```



- Enrutamiento OSPF con autenticación en cada router.

ROUTER BUCARAMANGA

```
BUCARAMANGA>
```

```
BUCARAMANGA>enable
```

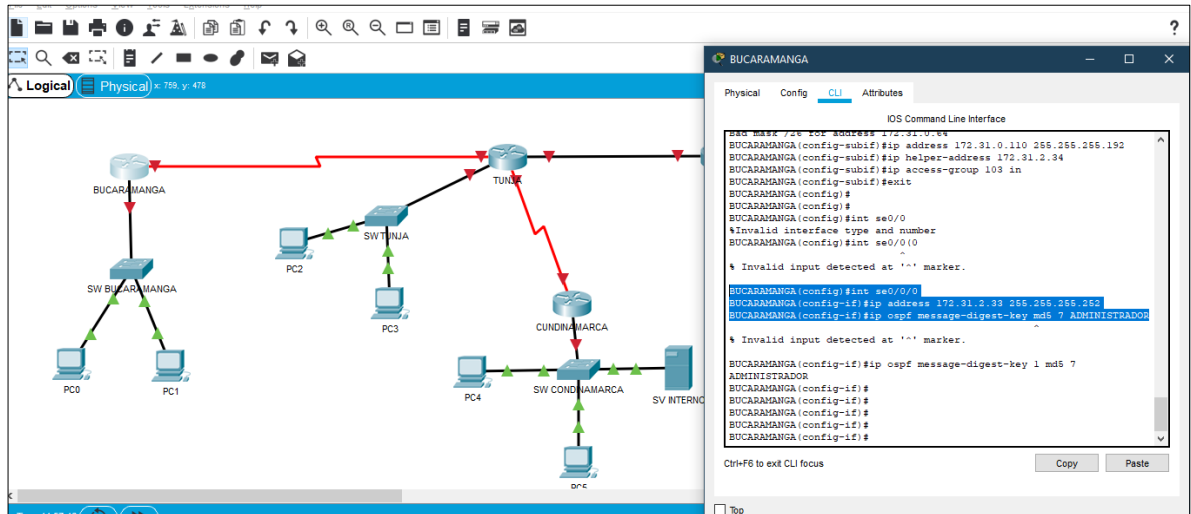
```
Password:
```

```
BUCARAMANGA#config t
```

```
BUCARAMANGA(config)#int se0/0/0
```

```
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
```

```
BUCARAMANGA(config-if)#ip ospf message-digest-key md5 7 ADMINISTRADOR
```



ROUTER TUNJA

```
TUNJA>
```

```
TUNJA>enable
```

```
Password:
```

```
TUNJA#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
TUNJA(config)#int se0/0/0
```

```
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
```

```
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
```

```
TUNJA(config-if)#ip nat inside
```

```
TUNJA(config-if)#clock rate 64000
```

```
TUNJA(config-if)#exit
```

```
TUNJA(config)#int se0/0/1
```

```
TUNJA(config-if)#ip address 172.31.2.38 255.255.255.252
```

```
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
```

```
TUNJA(config-if)#ip nat inside
```

TUNJA(config-if)#clock rate 64000

The screenshot shows a network diagram in Packet Tracer with a CLI window for the TUNJA router. The network includes routers BUCAR MANGA, TUNJA, and CUNDINAMARCA, along with switches SW BUCAR MANGA, SW TUNJA, and SW CONDINAMARCA, and PCs PC0 through PC4. The CLI window shows the following configuration:

```
IOS Command Line Interface
TUNJA(config-subif)#ip address 172.31.0.10 255.255.255.192
TUNJA(config-subif)#ip access-group 103 in
TUNJA(config-subif)#exit
TUNJA(config)#
TUNJA(config)#int se0/0/0
TUNJA(config-if)#ip address 172.31.0.34 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#clock rate 64000
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA(config)#int se0/0/1
TUNJA(config-if)#ip address 172.31.2.30 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 64000
TUNJA(config-if)#int vlan1
TUNJA(config-if)#no ip address
TUNJA(config-if)#shutdown
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Ctrl-F6 to exit CLI focus
```

ROUTER CUNDINAMARCA

```
CUNDINAMARCA>
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int se0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.37 255.255.255.252
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 7
ADMINISTRADOR
```

The screenshot shows the same network diagram as above, but with the CLI window for the CUNDINAMARCA router. The configuration is as follows:

```
IOS Command Line Interface
CUNDINAMARCA(config)#int fa0/1.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#ip access-group 102 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#int fa0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88 native
CUNDINAMARCA(config-subif)#ip address 172.31.2.26 255.255.255.248
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#int se0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.37 255.255.255.252
% Invalid input detected at '' marker.
CUNDINAMARCA(config-if)#ip address 172.31.2.37 255.255.255.252
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 7
ADMINISTRADOR
CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#area 0 authentication message-digest
% Invalid input detected at '' marker.
Ctrl-F6 to exit CLI focus
```

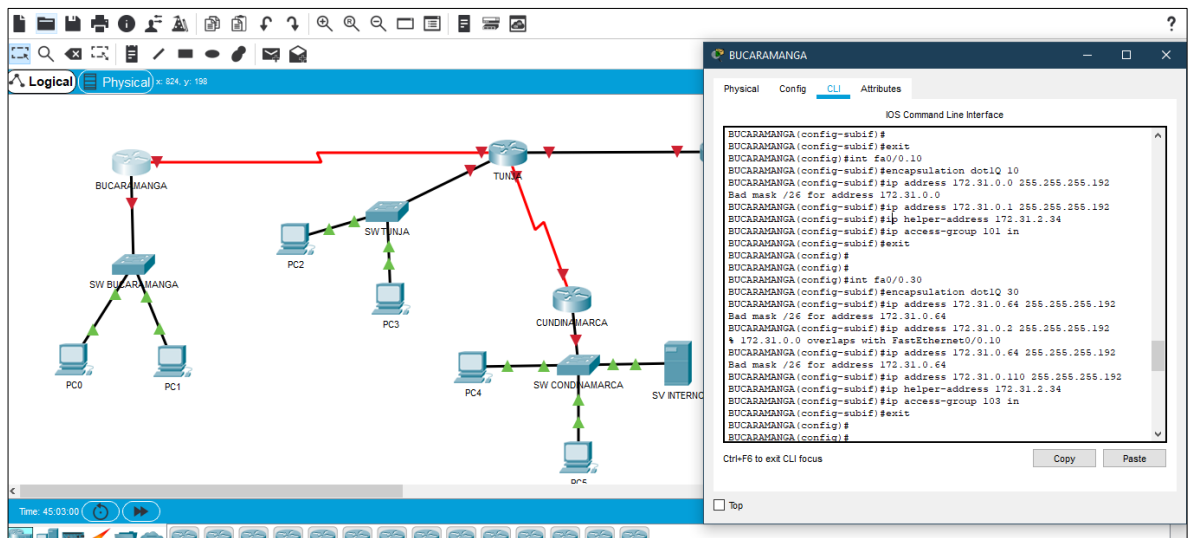
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

ROUTER BUCARAMANGA

```

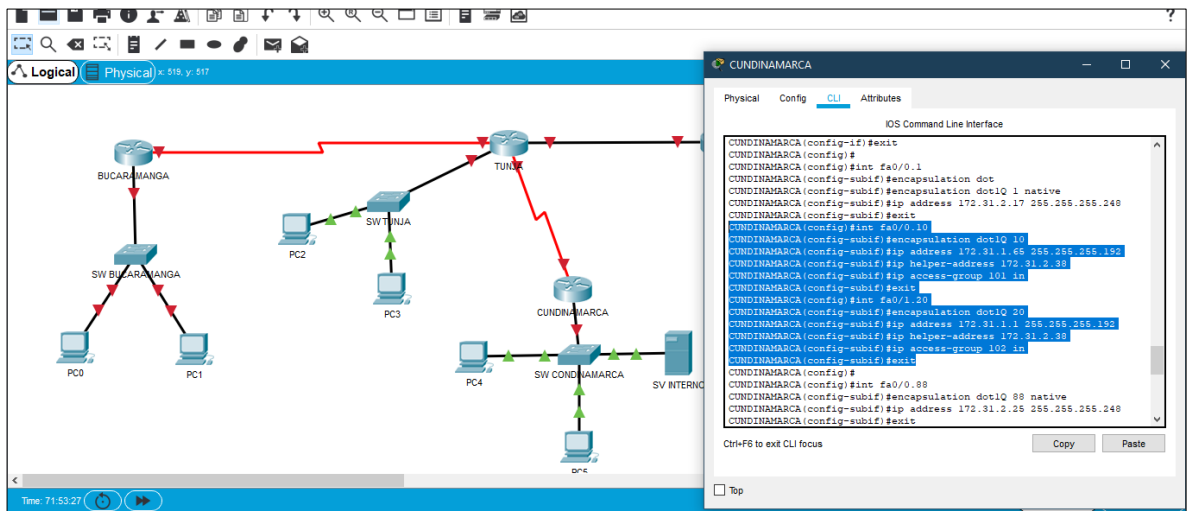
BUCARAMANGA>
BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
BUCARAMANGA(config)#int fa0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1Q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#ip access-group 101 in
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#int fa0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1Q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.110 255.255.255.192
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#ip access-group 103 in
BUCARAMANGA(config-subif)#exit

```



ROUTER CUNDINAMARCA

```
CUNDINAMARCA>
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int fa0/0.10
CUNDINAMARCA(config-subif)#encapsulation dot1Q 10
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#ip access-group 101 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#int fa0/1.20
CUNDINAMARCA(config-subif)#encapsulation dot1Q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#ip access-group 102 in
CUNDINAMARCA(config-subif)#exit
```



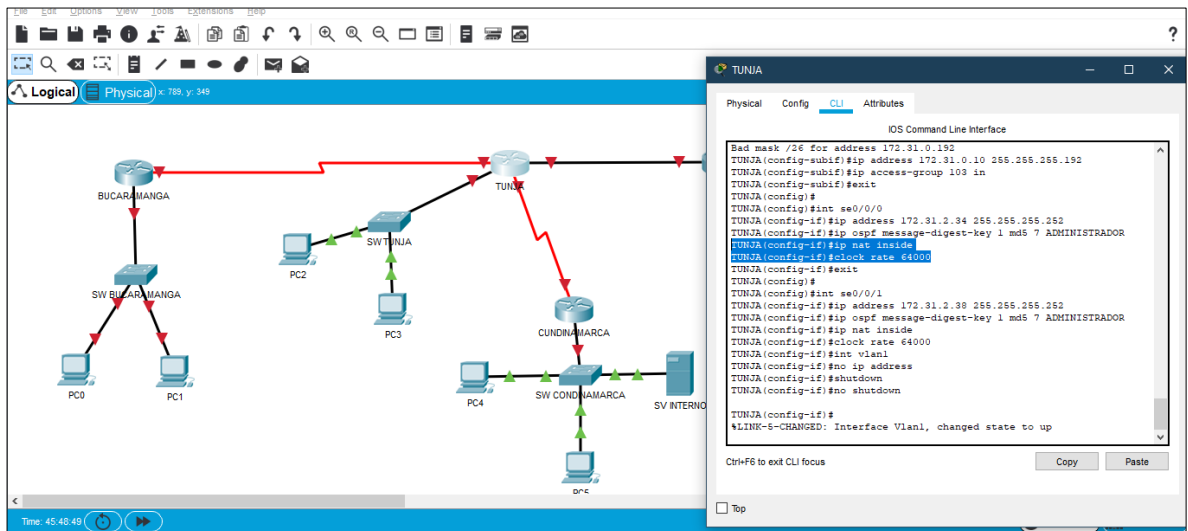
- Configuración de NAT estático y de sobrecarga.

ROUTER TUNJA

```

TUNJA>
TUNJA>enable
Password:
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int se0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 64000
TUNJA(config)#int se0/0/1
TUNJA(config-if)#ip address 172.31.2.38 255.255.255.252
TUNJA(config-if)#ip ospf message-digest-key 1 md5 7 ADMINISTRADOR
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#clock rate 6400

```



- Establecer una lista de control de acceso de acuerdo con los criterios señalados.

SWITCH BUCARAMANGA

```
SWBU>
SWBU>enable
SWBU#config t
SWBU#Log-adjacency-changes
SWBU#Área 0 authentication message-digest
SWBU# Network 172.31.1.0 0.0.0.63 area 0
SWBU# Network 172.31.1.64 0.0.0.63 area 0
SWBU# Network 172.31.2.16 0.0.0.7 area 0
SWBU# Network 172.31.2.36 0.0.0.3 area 0
SWBU# Network 172.31.2.24 0.0.0.7 area 0
SWBU# exit
```

SWITCH TUNJA

```
SWTU>
SWTU>enable
SWTU#config t
SWTU#Log-adjacency-changes
SWTU#Área 0 authentication message-digest
SWTU#Network 172.31.0.128 0.0.0.63 area 0
SWTU#Network 172.31.0.19X 0.0.0.63 area 0
SWTU#Network 172.31.2.8 0.0.0.7 area 0
SWTU#Network 172.31.2.32 0.0.0.7
SWTU#exit
```

SWITCH CUNDINAMARCA

```
SWCU>
SWCU>enable
SWCU#config t
SWCU#Log-adjacency-changes
SWCU#Área 0 authentication message-digest
SWCU#Network 172.31.0.X 0.0.0.63 area 0
SWCU#Network 172.31.0.X 0.0.0.63 area 0
SWCU#Network 172.31.2.X 0.0.0.7 area 0
SWCU#Network 172.31.2.X 0.0.0.7 area 0
SWCU#exit
```

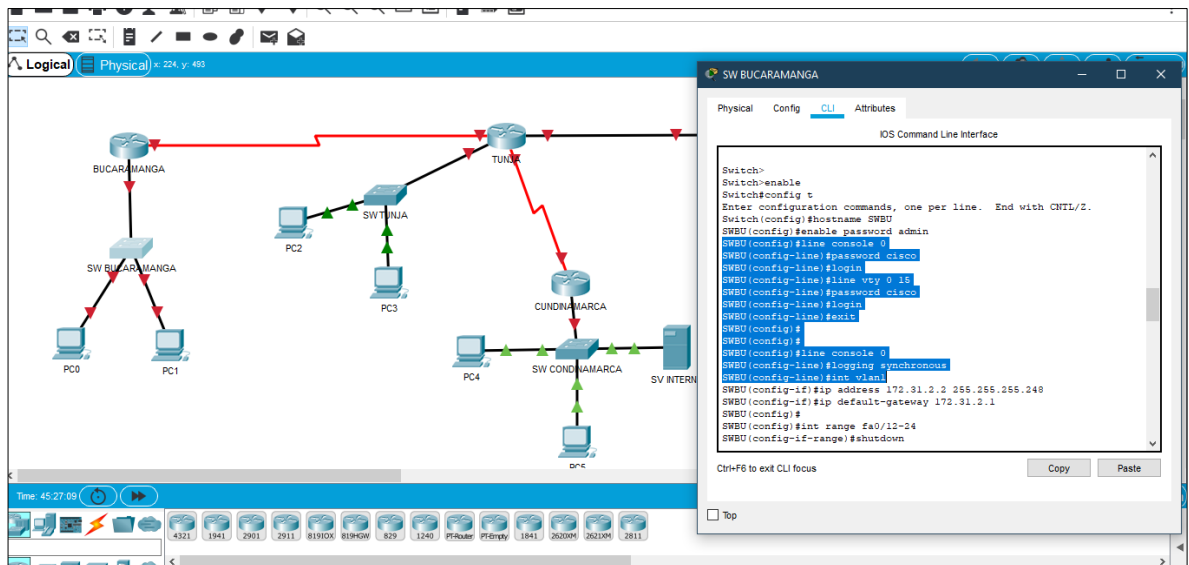
- Habilitar las opciones en puerto consola y terminal virtual

SWITCH BUCARAMANGA

```

SWBU>
SWBU>enable
SWBU#config t
SWBU(config-line)#password cisco
SWBU(config-line)#login
SWBU(config-line)#line vty 0 15
SWBU(config-line)#password cisco
SWBU(config-line)#login
SWBU(config)#line console 0
SWBU(config-line)#logging synchronous

```



SWITCH CUNDINAMARCA

```

SWCU>
SWCU>enable
SWCU#config t
SWCU(config-line)#password cisco
SWCU(config-line)#login
SWCU(config-line)#line vty 0 15
SWCU(config-line)#password cisco
SWCU(config-line)#login

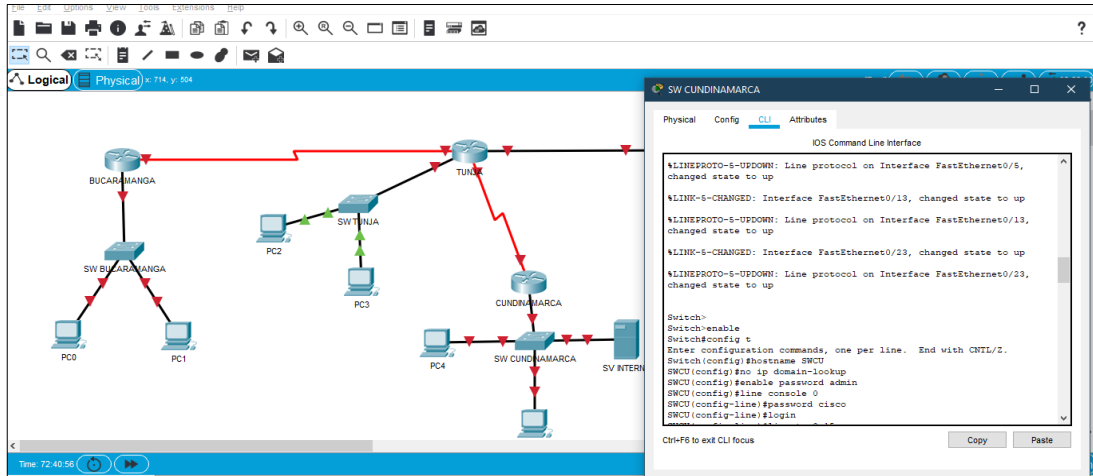
```



```

SWCU(config)#line console 0
SWCU(config-line)#logging synchronous

```

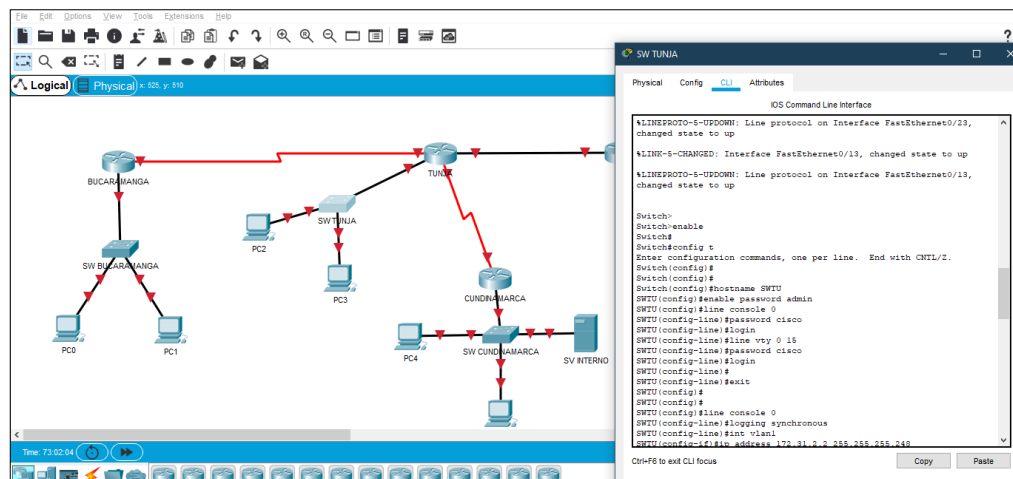


SWITCH TUNJA

```

SWTU>
SWTU>enable
SWTU#config t
SWTU(config-line)#password cisco
SWTU(config-line)#login
SWTU(config-line)#line vty 0 15
SWTU(config-line)#password cisco
SWTU(config-line)#login
SWTU(config)#line console 0
SWTU(config-line)#logging synchronous

```



CONCLUSIONES

- El tipo de topología utilizada afecta al tipo y capacidades del hardware de red, su administración y las posibilidades de expansión futura.
- La configuración inicial de la topología por medio de la ACL de los router permite mitigar los ataques de forma remota
- El Subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet. Esto se traduce en que el router que establece la conexión entre la red e Internet se especifica como dirección única, aunque puede que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.
- La configuración ACL permite el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al Router mediante telnet o SSH.

BIBLIOGRAFIA

- CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>
- CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>
- CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>
- Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>
- Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm
- 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>
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>