

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

**TRABAJO FINAL: PRUEBA DE HABILIDADES CCNA**

**PRESENTADO A: JOSE IGNACIO CARDONA**

**PRESENTADO POR:**

**DIEGO ALEJANDRO CANDAMIL**

**GRUPO: 203092\_16**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD  
PROGRAMA DE INGENIERÍA DE SISTEMAS  
DICIEMBRE DE 2019**

## Contenido

Resumen .....	3
Abstract .....	3
Introducción .....	4
Objetivos.....	4
Objetivos específicos.....	4
ESCENARIO 1 .....	5
Desarrollo .....	5
Parte 1: Asignación de direcciones IP.....	6
Parte 2: Configuración Básica.....	6
Parte 3: Configuración de Enrutamiento.....	10
Parte 4: Configuración de las listas de Control de Acceso.....	12
Parte 5: Comprobación de la red instalada.....	13
ESCENARIO 2 .....	15
Desarrollo .....	15
Aspectos a tener en cuenta .....	24
Conclusiones.....	25
Lista de referencias .....	26

## Resumen

En este documento encontrará el desarrollo de dos escenarios propuestos para demostrar el desarrollo de competencias y habilidades adquiridas durante el Diplomado en Profundización CCNA. Los escenarios abarcan temas básicos, pasando por intermedios y avanzados de networking, como lo son configuración inicial de los routers, seguridad y encriptación de credenciales de acceso, enrutamiento (EIGRP y OSPF), servicios DHCP, IP Helper, Telnet, creación de VLANs y seguridad con ACLs, entre otros. Por otro lado, se demuestra el uso del comandos de configuración de los dispositivos CISCO, empleando la herramienta de simulación Packet Tracer de la misma empresa.

## Abstract

In this document you will find the development of two scenarios proposed to demonstrate the development of skills and abilities acquired during the CCNA Deepening Diploma. The scenarios cover basic topics, including intermediate and advanced networking, such as initial configuration of routers, security and encryption of access credentials, routing (EIGRP and OSPF), DHCP services, IP Helper, Telnet, creation of VLANs and security with ACLs, among others. On the other hand, the use of the configuration commands of the CISCO devices is demonstrated, using the Packet Tracer simulation tool of the same company.

## Introducción

El buen uso de redes en organizaciones es importante en la actualidad teniendo en cuenta que todos los procesos deben estar interconectados en la misma. La importancia de demostrar este conocimiento mediante la resolución de dos escenarios es lo que me lleva a exponer lo aprendido en esta etapa. Cada uno tiene retos y conocimientos diferentes, los cuales podrán ver a continuación que lo poco y mucho que aprendí ha sido para mí muy importante darlo a conocer mediante este documento.

## Objetivos

### Objetivo general

Realizar la actividad teniendo en cuenta las habilidades y competencias adquiridas durante el curso.

### Objetivos específicos

- Realizar los respectivos escenarios siguiendo los lineamientos.
- Poner a prueba los conocimientos adquiridos durante las unidades 1 y 2 de CCNA
- Realizar redes a través de las herramientas packet tracer y así mismo probar su conexión



### 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.

- RTA:

Dirección de Red	Primera Utilizable	Ultima Utilizable	Dirección Broadcast
192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red.

- RTA:

BOGOTÁ	Se0/0/0	192.168.1.97/27
	Se0/0/1	192.168.1.129/27
	Fa0/0	192.168.1.1/27
MEDELLÍN	Se0/0/0	192.168.1.98/27
	Fa0/0	192.168.1.33/27
CALI	Se0/0/0	192.168.1.130/27
	Fa0/0	192.168.1.65/27
Servidor	Interfaz	192.168.1.2/27
	Gateway	192.168.1.1/27
WS1	Interfaz	192.168.1.3/27
	Gateway	192.168.1.1/27
PC1	Interfaz	192.168.1.34/27
	Gateway	192.168.1.33/27
PC2	Interfaz	192.168.1.35/27
	Gateway	192.168.1.33/27
PC3	Interfaz	192.168.1.66/27
	Gateway	192.168.1.65/27
PC4	Interfaz	192.168.1.67/27
	Gateway	192.168.1.65/27

### 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	<b>MEDELLIN</b>	<b>BOGOTA</b>	<b>CALI</b>
Dirección de Ip en interfaz Serial 0/0	192.168.1.98	192.168.1.97	192.168.1.130
Dirección de Ip en interfaz Serial 0/1		192.168.1.129	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	<b>Eigrp</b>	<b>Eigrp</b>	<b>Eigrp</b>
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.

- RTA:

```
Bogota#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/1
```

```
Medellin#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 2 subnets
C       192.168.1.32 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0/0
```

```

Cali#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, Serial0/0/0
  
```

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

RTA:

```

Bogota#sh ip route 192.168.1.129
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/1
    Route metric is 0, traffic share count is 1

Bogota#sh ip route 192.168.1.97
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
    Route metric is 0, traffic share count is 1
  
```

```

Medellin#sh ip route 192.168.1.33
Routing entry for 192.168.1.32/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
    Route metric is 0, traffic share count is 1

Medellin#sh ip route 192.168.1.98
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
    Route metric is 0, traffic share count is 1
  
```

```

Cali#sh ip route 192.168.1.129
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
    Route metric is 0, traffic share count is 1

Cali#sh ip route 192.168.1.65
Routing entry for 192.168.1.64/27
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
    Route metric is 0, traffic share count is 1
  
```



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

RTA:

```
Bogota#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
Switch         Fas 0/0         136       S           2960      Fas 0/1
Cali           Ser 0/0/1       144       R           C1841     Ser 0/0/0
Medellin       Ser 0/0/0       146       R           C1841     Ser 0/0/0
Bogota#
```

```
Medellin#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
Switch         Fas 0/0         143       S           2960      Fas 0/1
Bogota         Ser 0/0/0       143       R           C1841     Ser 0/0/0
Medellin#
```

```
Cali#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
Switch         Fas 0/0         166       S           2960      Fas 0/1
Bogota         Ser 0/0/0       166       R           C1841     Ser 0/0/1
Cali#
```

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

RTA:

```
Bogota#ping 192.168.1.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms

Bogota#ping 192.168.1.130
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

```
Medellin#ping 192.168.1.97
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.97, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/6 ms
```

```
Cali#ping 192.168.1.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms
```

### Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

RTA:

```
Router(config)#router eigrp 1 Router(config-
router)#network [IP DE RED] Router(config-
router)#no auto-summary Router(config-
router)#exit
```

b. Verificar si existe vecindad con los routers configurados con EIGRP.

RTA:

```
Bogota#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme    Capability   Platform    Port ID
Switch           Fas 0/0        155        S            2960        Fas 0/1
Cali              Ser 0/0/1      163        R            C1841       Ser 0/0/0
Medellin         Ser 0/0/0      165        R            C1841       Ser 0/0/0
```

```
Medellin#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme    Capability   Platform    Port ID
Switch           Fas 0/0        126        S            2960        Fas 0/1
Bogota           Ser 0/0/0      126        R            C1841       Ser 0/0/0
```

```
Cali#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme    Capability   Platform    Port ID
Switch           Fas 0/0        151        S            2960        Fas 0/1
Bogota           Ser 0/0/0      151        R            C1841       Ser 0/0/1
```

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

RTA:

```
Bogota#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
C    192.168.1.0 is directly connected, FastEthernet0/0
D    192.168.1.32 [90/2172416] via 192.168.1.98, 00:05:14, Serial0/0/0
D    192.168.1.64 [90/2172416] via 192.168.1.130, 00:04:05, Serial0/0/1
C    192.168.1.96 is directly connected, Serial0/0/0
C    192.168.1.128 is directly connected, Serial0/0/1
```

```

Medellin#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.97, 00:06:10, Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.97, 00:05:01, Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/2681856] via 192.168.1.97, 00:06:10, Serial0/0/0

```

```

Cali#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

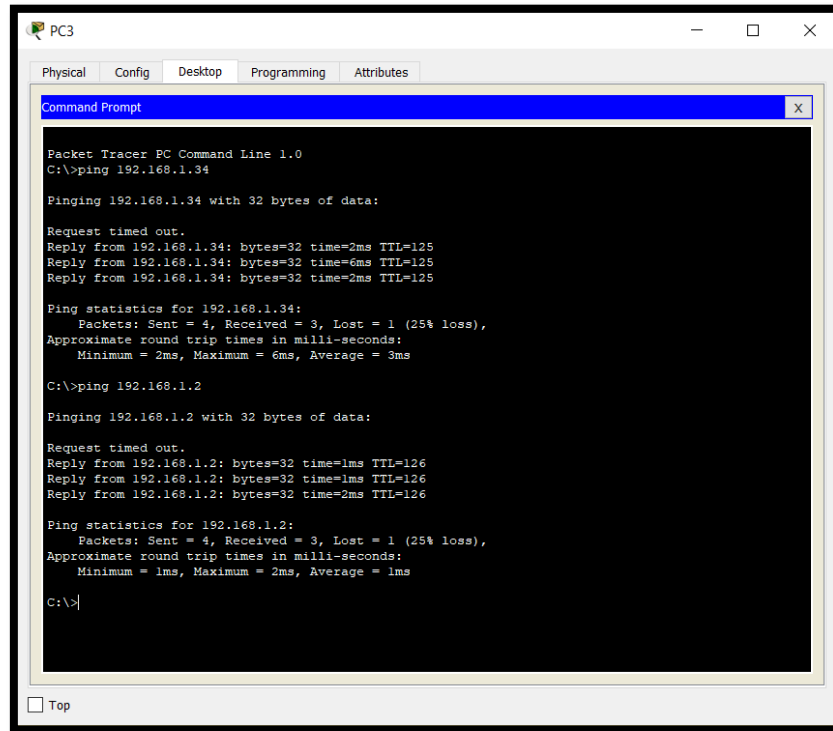
Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.129, 00:05:41, Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.129, 00:05:41, Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.129, 00:05:41, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

```

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.

RTA:



#### 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:

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

a. 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.

RTA:

```
Bogota (Config)# access-list 1 deny host 192.168.1.3
```

```
Bogota (Config)# access-list 1 permit any
```

```
Bogota (Config)# int fa0/0
```

```
Bogota (Config-if)# ip access-group 1 in
```

b. 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. RTA:

```
Medellin (Config)# access-list 1 permit host 192.168.1.2
```

```
Medellin (Config)# access-list 1 deny any
```

```
Medellin (Config)# int fa0/0
```

Medellin (Config-if)# ip access-group 1 in

### 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.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Ok
	WS_1	Router BOGOTA	
	Servidor	Router CALI	Ok
	Servidor	Router MEDELLIN	Ok
TELNET	LAN del Router MEDELLIN	Router CALI	
	LAN del Router CALI	Router CALI	Ok
	LAN del Router MEDELLIN	Router MEDELLIN	Ok
	LAN del Router CALI	Router MEDELLIN	Ok
PING	LAN del Router CALI	WS_1	unreachable
	LAN del Router MEDELLIN	WS_1	unreachable
	LAN del Router MEDELLIN	LAN del Router CALI	unreachable
PING	LAN del Router CALI	Servidor	Ok
	LAN del Router MEDELLIN	Servidor	Ok
	Servidor	LAN del Router MEDELLIN	Ok
	Servidor	LAN del Router CALI	Ok
	Router CALI	LAN del Router MEDELLIN	Ok
	Router MEDELLIN	LAN del Router CALI	Ok

```
Medellin#telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

Password:
Cali>
```

```
C:\>
C:\>telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

Password:
Cali>
```

```
C:\>
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...Open

User Access Verification

Password:
Medellin>
```

PC4

```

Physical  Config  Desktop  Programmin
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

Password:
Password:
Cali>exit
    
```

PC2

```

Physical  Config  Desktop  Programmin
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...Open

User Access Verification

Password:
Medellin>
    
```

PC4

```

Physical  Config  Desktop  Program
Command Prompt
snmpget      SNMP GET
snmpgetbulk  SNMP GET BULK
snmpset      SNMP SET
ssh          ssh client
telnet       Telnet client
tracert      Trace route to des
C:\>
C:\>
C:\>quit
C:\>exit
exit

C:\>
C:\>
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...Open

User Access Verification

Password:
Medellin>
    
```

```

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

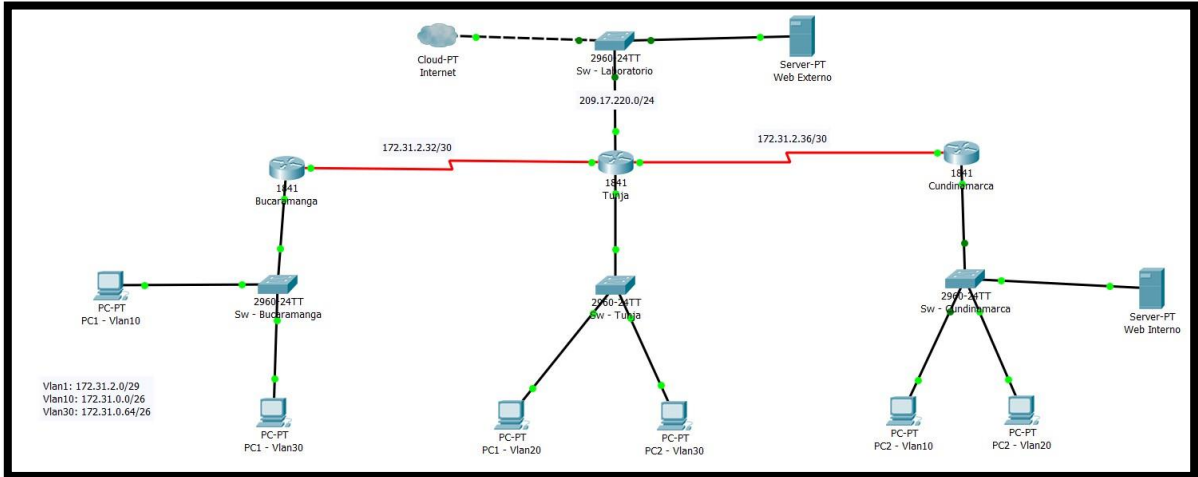
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
    
```

Ping desde PC4

## ESCENARIO 2



## Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

- Configuración básica.
- Autenticación local con AAA.

RTA:

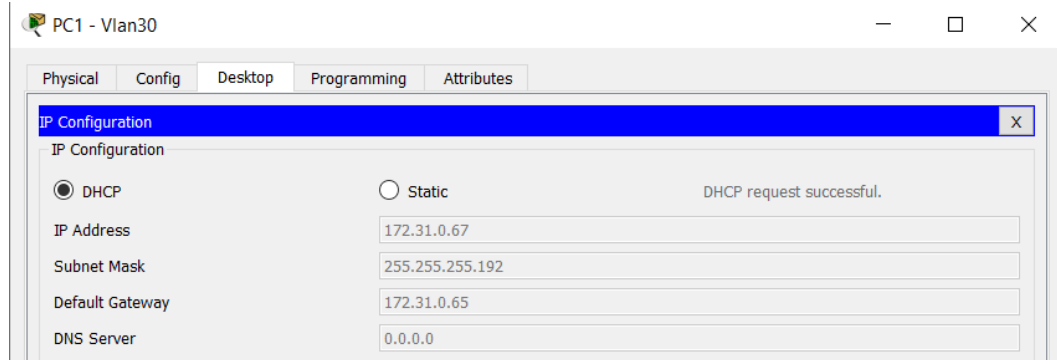
```
Router (config)#aaa new-model
Router (config)#username cisco secret cisco
Router (config)#aaa authentication login default local
Router (config)#aaa authentication login default enable
Router (config)#enable secret cisco
Router (config)#aaa authentication login console local
Router (config)#line console 0
Router (config-line)#login authentication console
Router (config-line)#exit
Router (config)#aaa authentication login vty enable
Router (config)#line vty 0 4
Router (config-line)#password cisco
Router (config-line)#login authentication vty
Router (config-line)#end
```

- Cifrado de contraseñas.  
RTA: Router(config)#service password-encryption
- Un máximo de intentos para acceder al router.  
RTA: Router(config)#login block-for 30 attempts 3 within 30
- Máximo tiempo de acceso al detectar ataques.  
RTA: Router(config)#login block-for 30 attempts 3 within 30

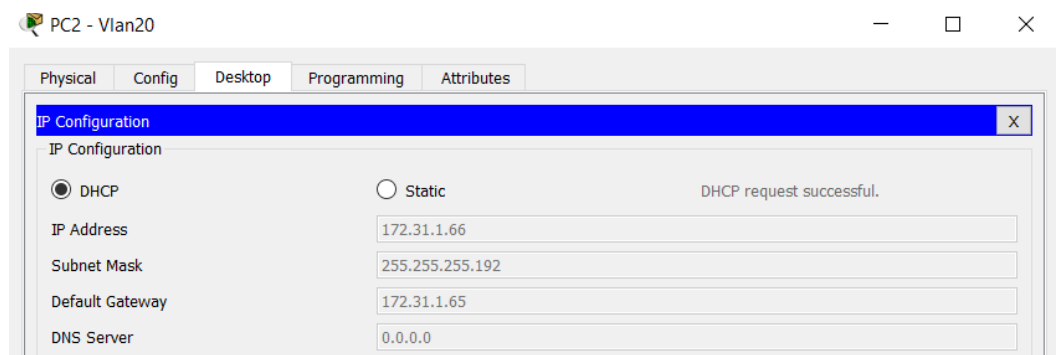
- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca.

RTA:

PC1 – Vlan30 Bucaramanga



PC2 – Vlan20 Cundinamarca



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

RTA:

```
NAT -> Tunja(config)#ip nat inside source static 209.17.220.2 5.5.5.5
```

```
Tunja(config)#interface fa0/1
```

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

```
Tunja(config)#interface se0/0/0 Tunja
```

```
(config-if)#ip nat outside
```

```
Tunja (config)#ip route 0.0.0.0 0.0.0.0 se0/0/0
```

```
PAT -> Tunja(config)# access-list 1 permit 172.31.0.0 0.0.0.127
```

```
Tunja(config)# ip nat inside source list 1 interface fa0/1 overload
```

```
Tunja(config)#interface fa0/1
```



```
Tunja(config-if)# ip nat outside
Tunja(config)#interface se0/0/0
Tunja(config-if)#ip nat inside
```

```
Tunja#
Tunja#sh ip nat translations
Pro  Inside global      Inside local      Outside local
-----
Outside global
icmp 209.17.220.1:1    172.31.0.67:1    209.17.220.2:1
209.17.220.2:1
icmp 209.17.220.1:2    172.31.0.67:2    209.17.220.2:2
209.17.220.2:2
icmp 209.17.220.1:3    172.31.0.67:3    209.17.220.2:3
209.17.220.2:3
icmp 209.17.220.1:4    172.31.0.67:4    209.17.220.2:4
209.17.220.2:4
---  5.5.5.5            209.17.220.2    ---            ---
```

4. El enrutamiento deberá tener autenticación.

RTA:

```
Router(config)#router ospf 1
Router(config-router)#network 172.31.2.32 255.255.255.252 area 1
```

*Y acá se repitió el mismo proceso con las demás direcciones de red en los 3 routers.*

```
Router(config-router)#exit
```

```
Tunja#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O       172.31.0.0/26 [110/65] via 172.31.2.34, 01:18:26, Serial0/0/0
O       172.31.0.64/26 [110/65] via 172.31.2.34, 01:18:26, Serial0/0/0
C       172.31.0.128/26 is directly connected, FastEthernet0/0.20
C       172.31.0.192/26 is directly connected, FastEthernet0/0.30
O       172.31.1.0/26 [110/65] via 172.31.2.38, 01:12:26, Serial0/0/1
O       172.31.1.64/26 [110/65] via 172.31.2.38, 01:12:44, Serial0/0/1
O       172.31.2.0/29 [110/65] via 172.31.2.34, 01:18:26, Serial0/0/0
C       172.31.2.8/29 is directly connected, FastEthernet0/0.1
O       172.31.2.16/29 [110/65] via 172.31.2.38, 01:13:08, Serial0/0/1
C       172.31.2.32/30 is directly connected, Serial0/0/0
C       172.31.2.36/30 is directly connected, Serial0/0/1
C       209.17.220.0/24 is directly connected, FastEthernet0/1
S*    0.0.0.0/0 is directly connected, Serial0/0/0
```

5. Listas de control de acceso:

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

RTA:

```
Cundinamarca(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63
172.31.0.128 0.0.0.63
```

```
Cundinamarca(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63
172.31.0.192 0.0.0.63
Cundinamarca(config)#access-list 101 deny ip any any
Cundinamarca(config)#int fa0/0 Cundinamarca(config-
if)#ip access-group 101 in
```

```
Cundinamarca#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
 20 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
 30 deny ip any any (50 match(es))
Extended IP access list 102
 10 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
 20 deny ip any any
```

- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

RTA:

```
Cundinamarca(config)#access-list 102 permit ip 172.31.1.0 0.0.0.63
209.17.220.2 0.0.0.255
```

```
Cundinamarca(config)#access-list 102 deny ip any any
Cundinamarca(config)#int fa0/0 Cundinamarca(config-
if)#ip access-group 102 in
```

```
Cundinamarca#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
 20 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
 30 deny ip any any (50 match(es))
Extended IP access list 102
 10 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
 20 deny ip any any
```

- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

RTA:

```
Tunja(config)#access-list 102 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
Tunja(config)#access-list 102 permit tcp 172.31.0.192 0.0.0.63 any eq 20
Tunja(config)#access-list 102 permit tcp 172.31.0.192 0.0.0.63 any eq www
Tunja(config)#access-list 102 deny ip any any
Tunja(config)#int fa0/0
Tunja(config-if)#ip access-group 102 in
```

```
Tunja#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
 20 deny ip any any
 30 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Extended IP access list 102
 10 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
 20 permit tcp 172.31.0.192 0.0.0.63 any eq 20
 30 permit tcp 172.31.0.192 0.0.0.63 any eq www
 40 deny ip any any
```

- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

RTA:

```
Tunja(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.1.64
0.0.0.63
```

```
Tunja(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63
```

```
Tunja(config)#access-list 101 deny ip any any
```

```
Tunja(config)#int fa0/0
```

```
Tunja(config-if)#ip access-group 101 in
```

```
Tunja#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
 20 deny ip any any
 30 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Extended IP access list 102
 10 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
 20 permit tcp 172.31.0.192 0.0.0.63 any eq 20
 30 permit tcp 172.31.0.192 0.0.0.63 any eq www
 40 deny ip any any
```

- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

RTA:

```
Bucaramanga(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63
209.17.220.2 0.0.0.255
```

```
Bucaramanga(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
```

```
Bucaramanga(config)#access-list 101 deny ip any any
```

```
Bucaramanga(config)#int fa0/0
```

```
Bucaramanga(config-if)#ip access-group 101 in
```

```
Bucaramanga#sh access-lists
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list 101
 10 permit ip 172.31.0.64 0.0.0.63 209.17.220.0 0.0.0.255
 20 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
 30 deny ip any any
Extended IP access list 102
 10 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
 20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
 30 deny ip any any
```

- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

RTA:

```
Bucaramanga(config)#access-list 102 permit ip 172.31.0.0 0.0.0.63 172.31.1.64
0.0.0.63
```

```
Bucaramanga(config)#access-list 102 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
```

```
Bucaramanga(config)#access-list 102 deny ip any any
```

```
Bucaramanga(config)#int fa0/0
```

```
Bucaramanga(config-if)#ip access-group 102 in
```

```
Bucaramanga#sh access-lists
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list 101
 10 permit ip 172.31.0.64 0.0.0.63 209.17.220.0 0.0.0.255
 20 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
 30 deny ip any any
Extended IP access list 102
 10 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
 20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
 30 deny ip any any
```

- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

RTA:

```
Bucaramanga(config)#access-list 104 deny ip 172.31.0.0 0.0.0.63 172.31.1.0
0.0.0.63
```

```
Bucaramanga(config)#access-list 104 permit ip any any
```

```
Bucaramanga(config)#int fa0/0
```

```
Bucaramanga(config-if)#ip access-group 104 in
```

```
Bucaramanga#sh access-lists
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list 101
 10 permit ip 172.31.0.64 0.0.0.63 209.17.220.0 0.0.0.255
 20 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
 30 deny ip any any
Extended IP access list 102
 10 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
 20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
 30 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.0 0.0.0.7 172.31.2.0 0.0.0.7
 20 permit ip 172.31.2.0 0.0.0.7 172.31.2.8 0.0.0.7
 30 permit ip 172.31.2.0 0.0.0.7 172.31.2.16 0.0.0.7
 40 permit ip 172.31.2.0 0.0.0.7 209.17.220.0 0.0.0.255
 50 deny ip any any
Extended IP access list 104
 10 deny ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
 20 permit ip any any
```

```
Tunja(config)#access-list 104 deny ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
```

```
Tunja(config)#access-list 104 deny ip 172.31.0.192 0.0.0.63 172.31.0.64 0.0.0.63
```

```
Tunja(config)#access-list 104 permit ip any any
```

```
Tunja(config)#int fa0/0
```

```
Tunja(config-if)#ip access-group 104 in
```

```
Tunja#sh acc
Extended IP access list 101
 10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
 20 deny ip any any
 30 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Extended IP access list 102
 10 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
 20 permit tcp 172.31.0.192 0.0.0.63 any eq 20
 30 permit tcp 172.31.0.192 0.0.0.63 any eq www
 40 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.8 0.0.0.7 172.31.2.8 0.0.0.7
 20 permit ip 172.31.2.8 0.0.0.7 172.31.2.0 0.0.0.7
 30 permit ip 172.31.2.8 0.0.0.7 172.31.2.16 0.0.0.7
 40 permit ip 172.31.2.8 0.0.0.7 209.17.220.0 0.0.0.255
Extended IP access list 104
 10 deny ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
 20 deny ip 172.31.0.192 0.0.0.63 172.31.0.64 0.0.0.63
 30 permit ip any any
```

```
Cundinamarca(config)#access-list 104 deny ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
```

```
Cundinamarca(config)#access-list 104 deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
```

```
Cundinamarca(config)#access-list permit ip any any
```

```
Cundinamarca(config)#access-list 104 permit ip any any
```

Cundinamarca(config)#int fa0/0

Cundinamarca(config-if)#ip access-group 104 in

```
Cundinamarca#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
 20 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
 30 deny ip any any (632 match(es))
Extended IP access list 102
 10 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
 20 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.16 0.0.0.7 172.31.2.16 0.0.0.7
 20 permit ip 172.31.2.16 0.0.0.7 172.31.2.0 0.0.0.7
 30 permit ip 172.31.2.16 0.0.0.7 172.31.2.8 0.0.0.7
 40 permit ip 172.31.2.16 0.0.0.7 209.17.220.0 0.0.0.255
Extended IP access list 104
 10 deny ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
 20 deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
 30 permit ip any any
```

- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

RTA:

Bucaramanga(config)#access-list 103 permit ip 172.31.2.0 0.0.0.7 172.31.2.1 0.0.0.7

Bucaramanga(config)#access-list 103 permit ip 172.31.2.0 0.0.0.7 172.31.2.9 0.0.0.7

Bucaramanga(config)#access-list 103 permit ip 172.31.2.0 0.0.0.7 172.31.2.17 0.0.0.7

Bucaramanga(config)#access-list 103 permit ip 172.31.2.0 0.0.0.7 209.17.220.2 0.0.0.255

Bucaramanga(config)#access-list 103 deny ip any any

Bucaramanga(config)#int fa0/0

Bucaramanga(config-if)#ip access-group 103 in

```
Bucaramanga#sh access-lists
Extended IP access list sl_def_acl
 0 deny tcp any any eq telnet
 0 deny tcp any any eq www
 0 deny tcp any any eq 22
 0 permit tcp any any eq 22
Extended IP access list 101
 10 permit ip 172.31.0.64 0.0.0.63 209.17.220.0 0.0.0.255
 20 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
 30 deny ip any any
Extended IP access list 102
 10 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
 20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
 30 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.0 0.0.0.7 172.31.2.0 0.0.0.7
 20 permit ip 172.31.2.0 0.0.0.7 172.31.2.8 0.0.0.7
 30 permit ip 172.31.2.0 0.0.0.7 172.31.2.16 0.0.0.7
 40 permit ip 172.31.2.0 0.0.0.7 209.17.220.0 0.0.0.255
 50 deny ip any any
```

```
Tunja(config)#access-list 103 permit ip 172.31.2.8 0.0.0.7 172.31.2.90.0.0.7
Tunja(config)#access-list 103 permit ip 172.31.2.8 0.0.0.7 172.31.2.10.0.0.7
Tunja(config)#access-list 103 permit ip 172.31.2.8 0.0.0.7 172.31.2.17 0.0.0.7
Tunja(config)#access-list 103 permit ip 172.31.2.8 0.0.0.7 209.17.220.2
0.0.0.255
Tunja(config)#int fa0/0
Tunja(config-if)#ip access-group 103 in
```

```
Tunja#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
 20 deny ip any any
 30 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Extended IP access list 102
 10 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
 20 permit tcp 172.31.0.192 0.0.0.63 any eq 20
 30 permit tcp 172.31.0.192 0.0.0.63 any eq www
 40 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.8 0.0.0.7 172.31.2.8 0.0.0.7
 20 permit ip 172.31.2.8 0.0.0.7 172.31.2.0 0.0.0.7
 30 permit ip 172.31.2.8 0.0.0.7 172.31.2.16 0.0.0.7
 40 permit ip 172.31.2.8 0.0.0.7 209.17.220.0 0.0.0.255
```

```
Cundinamarca(config)#access-list 103 permit ip 172.31.2.16 0.0.0.7
172.31.2.17 0.0.0.7
Cundinamarca(config)#access-list 103 permit ip 172.31.2.16 0.0.0.7 172.31.2.1
0.0.0.7
Cundinamarca(config)#access-list 103 permit ip 172.31.2.16 0.0.0.7 172.31.2.9
0.0.0.7
Cundinamarca(config)#access-list 103 permit ip 172.31.2.16 0.0.0.7
209.17.220.2 0.0.0.255
Cundinamarca(config)#int fa0/0
Cundinamarca(config-if)#ip access-group 103 in
```

```
Cundinamarca#sh access-lists
Extended IP access list 101
 10 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
 20 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
 30 deny ip any any (508 match(es))
Extended IP access list 102
 10 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
 20 deny ip any any
Extended IP access list 103
 10 permit ip 172.31.2.16 0.0.0.7 172.31.2.16 0.0.0.7
 20 permit ip 172.31.2.16 0.0.0.7 172.31.2.0 0.0.0.7
 30 permit ip 172.31.2.16 0.0.0.7 172.31.2.8 0.0.0.7
 40 permit ip 172.31.2.16 0.0.0.7 209.17.220.0 0.0.0.255
```

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

Dirección Red	Primera Utilizable	Ultima Utilizable	Dirección Broadcast

172.31.0.0	172.31.0.1	172.31.0.62	172.31.0.63
172.31.0.64	172.31.0.65	172.31.0.126	172.31.0.127
172.31.0.128	172.31.0.129	172.31.0.190	172.31.0.191
172.31.0.192	172.31.0.193	172.31.0.254	172.31.0.255
172.31.1.0	172.31.1.1	172.31.1.62	172.31.1.63
172.31.1.64	172.31.1.65	172.31.1.126	172.31.1.127

### 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.
- 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

Con el desarrollo de esta actividad, pude aclarar conceptos teóricos los cuales no tenía tan claros. Cada una de las actividades tenía su propio reto y progreso, el cual sino se llevaba en debido orden podía entorpecer o retrasar de forma relativa el adelanto de esta. Tema como la implementación de VLANs se encuentra bastante en las organizaciones y, es una buena manera de empezar a otorgar seguridad en una topología de red.

Un tema el cual me ha llamado la atención y logré establecer como conocimiento fue el configurar el router como servidor DHCP, es práctico y pude quitarme ese mal hábito de pensar que era complicado. El establecer enrutamiento dinámico es la mejor alternativa, desde luego cabe aclarar que se debe tener en claro el direccionamiento estático para temas muy puntuales, teniendo en cuenta que hay dispositivos o servicios los cuales debemos tener fijos, el leer, comprender y aprender OSPF es una ganancia para mí.

Por último, como administrador de red, el tema más prescindible o que debemos garantizar a nuestro cliente, es el tema de seguridad, algo tan sencillo y simple como poner o configurar una contraseña para el acceso al router, son cosas que se deben tener en cuenta, porque he tenido la oportunidad de conocer administradores que no tienen esta práctica y, también he conocido las consecuencias de no hacerlo.

Sin más, agradecer por todo lo aprendido con este trabajo final.

## Lista de referencias

- DevTics, D. (18 de abril del 2017). Configuración Encapsulamiento PPP. []. Recuperado de <http://devtics.blogspot.com>
- Del Barrio, David. (7 de enero 2012). Configurar un servidor de DHCP del IOS de Cisco | Packet Tracer. Taller del Bit Recuperado de <https://eltallerdelbit.com/servidor-dhcp-packet-tracer/>
- Gordon, A [Andrew Gordon]. (2012 febrero 19). Setting up a Loopback Address. [Video]. Recuperado de [https://www.youtube.com/watch?v=z9tMTc1\\_qYg](https://www.youtube.com/watch?v=z9tMTc1_qYg)
- Romero Goyzueta, C. A. [Christian Augusto Romero Goyzueta]. (2016 junio 30). How to Create a Cluster on Packet Tracer - Cómo Crear un Cluster en Packet Tracer. [Video]. Recuperado de <https://www.youtube.com/watch?v=14pVM2QgeDA>
- Perez, D. (29 de septiembre del 2018). Configuración de VLANs. []. Recuperado de <https://todopacketracer.com>
- Perez, D. (03 de marzo del 2012). Enrutamiento entre VLANs. []. Recuperado de <https://todopacketracer.com>
- Walton, A. (). Implementación Básica de OSPFv2 y OSPFv3. []. Recuperado de <https://ccnadesdecero.es>