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

## PRUEBA DE HABILIDADES PRÁCTICAS

## TAREA 11

**MATEO SEBASTIAN MOLINA ARIAS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**

**ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA**

**INGENIERÍA ELECTRÓNICA**

**BOGOTÁ**

**2019**

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

## PRUEBA DE HABILIDADES PRÁCTICAS

## TAREA 11

**MATEO SEBASTIAN MOLINA ARIAS**

**INFORME**

**Opción de grado para Ingeniería Electrónica**

**DIRECTOR**

**JUAN CARLOS VESGA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**

**ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA**

**INGENIERÍA ELECTRÓNICA**

**BOGOTÁ**

**2019**

## Dedicatoria

Este proyecto se lo dedico primeramente a mi Padre Dios, a Jesús mi amigo, y al Espíritu Santo mi consuelo, quienes son uno, es decir, al Dios Eterno, pues es El quien me permite vivir, esforzarme y culminar esta carrera satisfactoriamente; también se lo dedico a mi Papá y a mi Mamá, quienes son mi familia, y siempre me apoyaron; y por ultimo a la UNAD y a sus asesores, docentes, tutores, y directivos.

**Agradecimiento**

Le agradezco primeramente a Dios, por darme sabiduría, ideas, creatividad, por darme la vida, la oportunidad, por darme un excelente Padre y una excelente Madre, y lo más importante, por darme la oportunidad de conocerlo, de hablarle, por escucharme, y fortalecerme, a fin de que además de muchas otras cosas, permitirme culminar exitosamente esta primera carrera universitaria.

También, ni más faltaba, agradezco a mi Papá y a mi Mamá, por su ayuda, su apoyo, porque me soportaron, comprendieron, y siempre estuvieron allí para mí.

Y por último, sin restarle importancia, a la UNAD, por ser una de las pioneras en la educación superior en la modalidad a distancia y virtual, pues gracias a esta institución y su constante innovación, he logrado culminar esta carrera.

**Contenido**

pág

## Lista de figuras

pág

## Lista de tablas

pág

## Resumen

Se comienza analizando el planteamiento y obteniendo una topología lógica, según las necesidad de cantidad de usuarios, conexiones, y uso de la red; para luego continuar configurando los parámetros básicos de seguridad y direccionamiento de cada router y switch, así como los parámetros básicos de servicios y direccionamiento de los PC y servidores, pasando por el enrutamiento dinámico, DHCP, NAT, hasta listas de control de acceso ACL. Primero se tiene una red WAN con 3 routers con interfaces Ethernet y Serial, en donde primero se configuran los routers con configuraciones básicas y de contraseñas, además del direccionamiento, luego se desarrollan verificación de dispositivos vecinos, rutas, y conectividad en ciertos tramos, para luego configurar el protocolo de enrutamiento dinámico EIGRP, el cual permite que exista conectividad en todos los tramos, allí también se verifican vecinos EIGRP y se verifican las tablas de enrutamiento, para verificar que se agregaron rutas dinámicamente por EIGRP con el indicativo D; luego, una vez que se cuenta con conectividad total, se restringen ciertos paquetes, para implementar seguridad en la red, en donde ciertas redes LAN no pueden acceder a otras, excepto al servidor ubicado en una de esas LAN, esto se logra al implementar listas de control de acceso ACL, en ciertas interfaces, en determinadas direcciones, y a determinados protocolos y servicios.

Adicionalmente se tiene una red MAN, la cual accede a internet en la oficina central, por medio de una red Ethernet; allí se implementan políticas de seguridad un poco más fuertes, incluso desde la configuración básica de los routers, al implementar acceso con usuarios y contraseñas, un máximo de intentos para acceder, un máximo tiempo de permanencia, y un servidor tftp para hacer backups de cada router remotamente, también, se establece autenticación en el protocolo de enrutamiento dinámico OSPF al tener que configurar una misma contraseña en cada interfaz que se conecta con el vecino OSPF el cual deber tener configurada la misma contraseña; en esta red se configura un router como servidor DHCP solo para 2 de las 3 redes LAN; también se configura NAT para traducir las direcciones de la MAN, a una dirección IP global interna (publica), con la cual se accede a internet, implementando NAT y PAT; y finalmente se aplican listas de control de acceso ACL, principalmente a fin de que cada VLAN solo acceda a terminados sectores y servicios

## Abstract

It begins by analyzing the problem and the logical topology, according to the need of number of users, connections, and use of the network; and then configuring the basic security and addressing parameters of each router and switch, as well as the basic services and addressing parameters of the PCs and servers, through dynamic routing, DHCP, NAT, up to ACL access control lists. First there is a WAN network with 3 routers with Ethernet and Serial interfaces, where first the routers with basic configurations and passwords are configured, in addition to the addressing, then, continue with verification of neighboring devices, the routes, and connectivity are verified in certain sections, to then configure the EIGRP dynamic routing protocol, which allows full connectivity in all sections, there, the EIGRP neighbors are verified and routing tables are verified, to verify that routes were dynamically added by EIGRP with the callsign D; then, once full connectivity is available, certain packets need to be restricted to implement network security, where, certain LAN networks cannot access others, except to the server located on one of those LANs, this is achieved by implementing of lists ACL access control, on certain interfaces, on certain addresses, and on certain protocols and services.

Additionally, there is a MAN network, which accesses the Internet in the head office, through an Ethernet network; there, a little stronger security policies are implemented, even from the basic configuration of the routers, when implementing access with users and passwords, a maximum of attempts to access, a maximum time of permanence, and a tftp server to make backups of each Router remotely, then, also establishes authentication in the OSPF dynamic routing protocol by having to configure the same password on each interface that it's connects to the OSPF neighbor, which must be the same password configured; then, in this network a router is configured as a DHCP server only for 2 of the 3 LAN networks; NAT is also configured to translate the addresses of the network MAN, to an internal (public) global IP address, with which the internet is accessed, implementing NAT and PAT; and finally ACL access control lists are applied, mainly so that each VLAN only accesses to a determinate sectors and services.

## Introducción

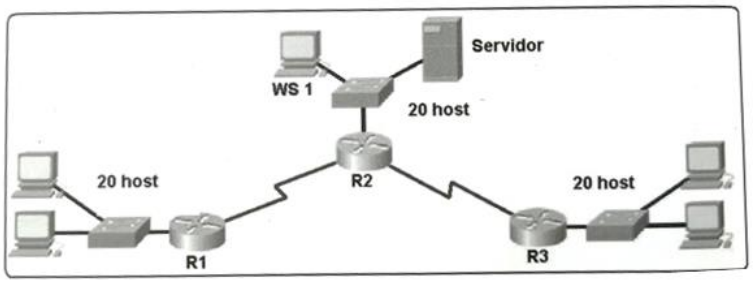
Las redes de telecomunicaciones son bastante complejas si se requiere que sean optimas y efectivas, comenzando por la creación de VLAN's, pasando por los protocolos de enrutamiento, hasta implementar políticas de seguridad para restringir el acceso desde y hacia ciertas zonas de la red, e incluso restringir las conexiones externas para ciertas subredes. Además, existen muchas configuraciones adicionales, tanto en la configuración básica, como en el enrutamiento, para añadir cierto nivel de seguridad; incluso las listas de acceso ACL se pueden configurar de diferentes maneras, a fin añadir seguridad a la red, sin comprometer rendimiento. Con todo esto se analizan prácticamente, aspectos y comandos necesarios y opcionales, como DHCP, NAT, contraseñas, enrutamiento EIGRP y OSPF, aplicables a los routers cisco, y configuraciones de VLAN que se aplican a los switch.

## Objetivos

- Analizar e implementar las topologías lógicas, al conectar cada interfaz de router y switch, por medio del cable puerto apropiado.
- Subnetear o dividir una dirección de red, en varias parte iguales o variables en base a los requerimientos de hosts.
- Poner en práctica comandos básicos de configuración de routers Cisco.
- Poner en practica comandos de verificación de configuración y conectividad en roters Cisco.
- Poner en práctica comandos de configuración de enrutamiento dinámico en routers Cisco.
- Poner en práctica comandos para configuración de DHCP y NAT en routers Cisco.
- Analizar direcciones IP de red o de host, de origen y destino, a fin de aplicar listas de control de acceso ACL, en routers Cisco.

# 1. ESCENARIO 1

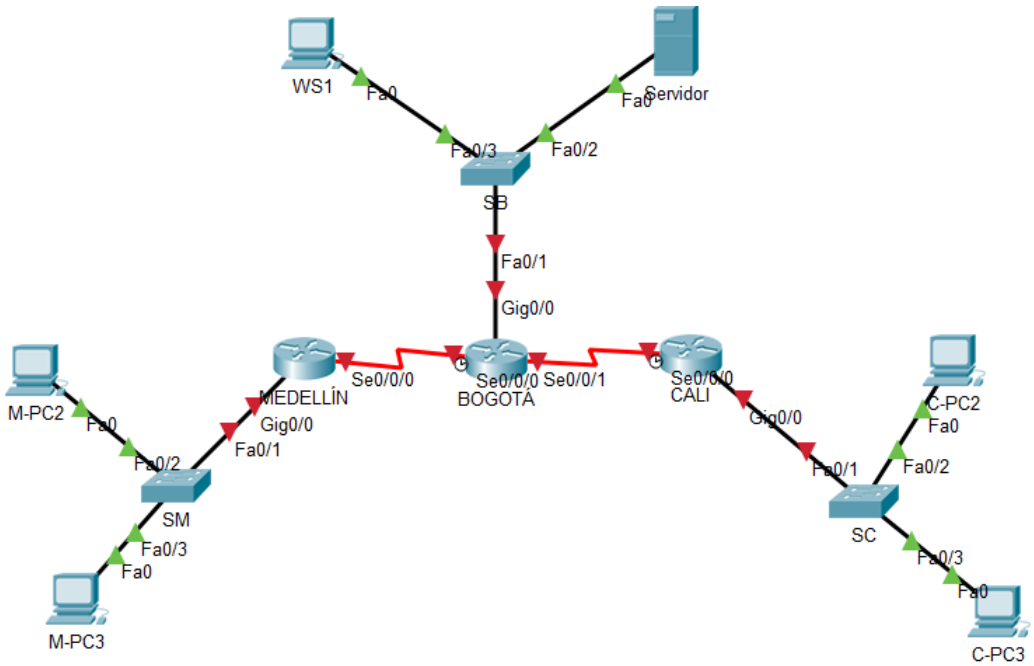
Figura 1




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.

**Se procede a implementar y conectar la anterior topología, en el software de simulación PacketTracer 7.2.2:**

Figura 2



## 1.1 Asignación de direcciones IP

Se utiliza la dirección IP 192.168.1.0/24 para dividir en subredes, y crear una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa:

Se divide en ocho partes, en redes /27, con la máscara de subred 255.255.255.224:

192.168.1.0/27

192.168.1.32/27

192.168.1.64/27

192.168.1.96/27

192.168.1.128/27

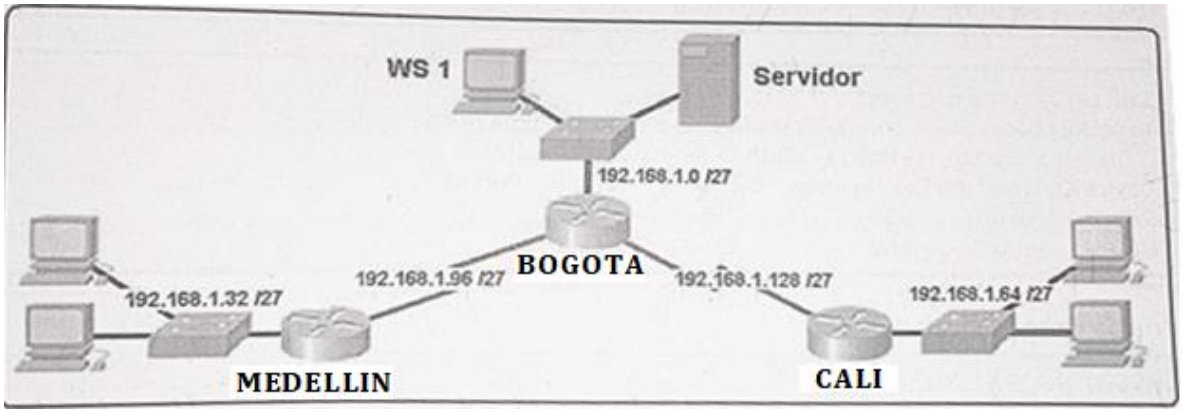
192.168.1.160/27

192.168.1.192/27

192.168.1.224/27

Ahora se aplican a los 5 segmentos de red actuales:

Figura 3



## 1.2 Configuración Básica

**a. Ahora se completa la tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.**

Tabla 1

| | 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 GB 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 |

Comandos utilizados para la configuración inicial y de interfaces de cada router:

**R1: MEDELLIN**

```
enable
conf t
hostname MEDELLIN
line con 0
password sede1
login
logging synchronous
line vty 0 15
password sedevty1
login
logging synchronous
exit
enable password adminr1
service password-encryption
interface s0/0/0
ip address 192.168.1.99 255.255.255.224
no shutdown
interface g0/0
ip address 192.168.1.33
no shutdown
end
copy run start
```

**R2: BOGOTA**

```
enable
conf t
hostname BOGOTA
line con 0
password sede2
login
```

```
logging synchronous
line vty 0 15
password sedevty2
login
logging synchronous
exit
enable password adminr2
service password-encryption
interface s0/0/0
ip address 192.168.1.98 255.255.255.224
clock rate 1000000
no shutdown

hostname CALI
line con 0
password sede3
login
logging synchronous
line vty 0 15
password sedevty3
login
logging synchronous
exit
interface s0/0/1
ip address 192.168.1.130 255.255.255.224
no shutdown
interface g0/0
ip address 192.168.1.1
no shutdown
end
copy run start
```

### R3: CALI

```
enable
conf t

enable password adminr3
service password-encryption
interface s0/0/0
ip address 192.168.1.131 255.255.255.224
clock rate 1000000
no shutdown
interface g0/0
ip address 192.168.1.65
no shutdown
end
copy run start
```

### También se aplica una configuración básica los switches:

### SM:

```
enable
conf t
hostname SM
line con 0
password sede1
login
logging synchronous
exit
enable password admins1
service password-encryption
exit
copy run start
```

### SB:

```
enable
conf t
```

```
hostname SB
line con 0
password sede2
login
logging synchronous
exit
enable password admins2
service password-encryption
exit
copy run start
```

**SC:**

```
enable
conf t
hostname SC
line con 0
password sede3
login
logging synchronous
exit
enable password admins3
service password-encryption
exit
copy run start
```

**b. Ahora se verifica la tabla de enrutamiento:**

Con el comando `show ip route`:

Figura 4

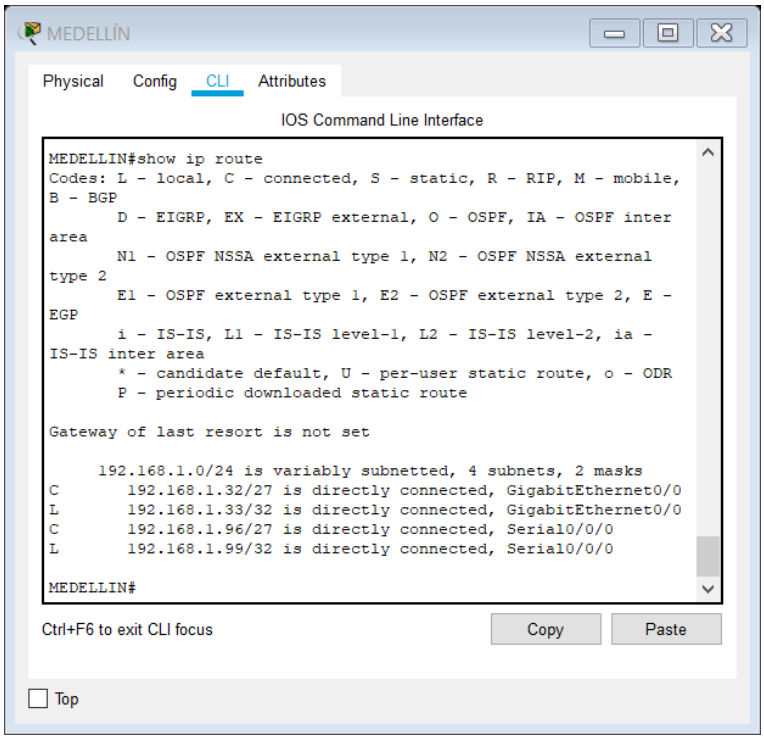


Figura 5

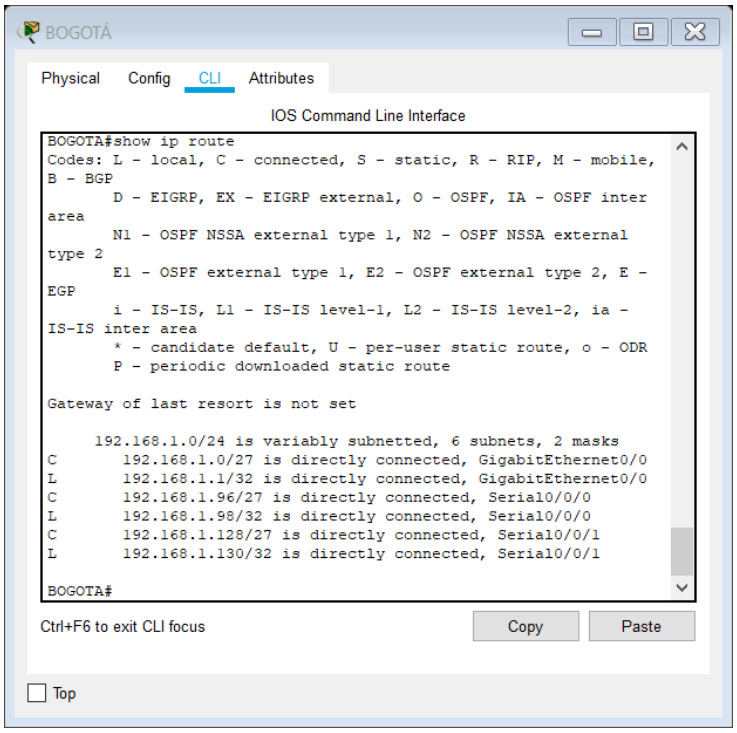
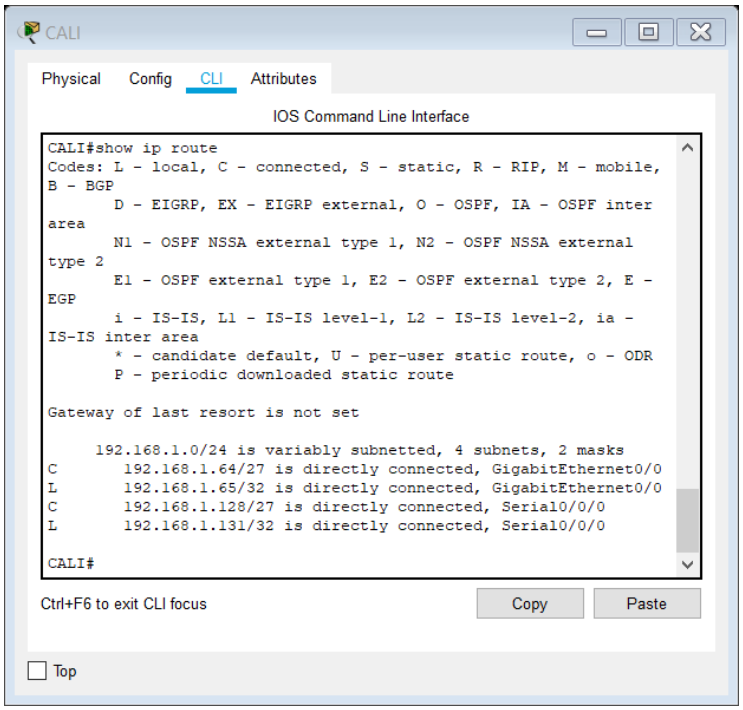



Figura 6



En las tablas de enrutamiento, se observa que efectivamente cada router tiene ruta para cada red configurada en las interfaces del router; pero claramente se observa que no existen rutas si la red no está conectada local o directamente.

**c. Ahora se verifica el balanceo de carga que presentan los routers:**

Figura 7

```
MEDELLIN#show ip route 192.168.1.96
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#show ip route 192.168.1.32
Routing entry for 192.168.1.32/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0
      Route metric is 0, traffic share count is 1

MEDELLIN#
```

Figura 8

```
BOGOTA#show ip route 192.168.1.96
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

BOGOTA#show ip route 192.168.1.128
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#show ip route 192.168.1.2
Routing entry for 192.168.1.0/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0
      Route metric is 0, traffic share count is 1

BOGOTA#
```

Figura 9

```
CALI#show ip route 192.168.1.128
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#show ip route 192.168.1.64
Routing entry for 192.168.1.64/27
Known via "connected", distance 0, metric 0 (connected, via
interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet0/0
      Route metric is 0, traffic share count is 1

CALI#
```

Se observa que como existen dos rutas para una misma red, y como todas las rutas son conectadas directa o localmente, estas tienen una distancia administrativa de 0 y una métrica también de 0.

**d. Ahora se realiza un diagnóstico de vecinos usando el comando cdp:**

Primero se verifica que cdp este activo en los equipos:

Routers:

Figura 10

```
MEDELLIN#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
MEDELLIN#
```

Figura 11

```
BOGOTA#show cdp
% CDP is not enabled
BOGOTA#
```

Figura 12

```
CALI#show cdp
% CDP is not enabled
CALI#
```

Switches:

Figura 13

```
SM#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
SM#
```

Figura 14

```
SB#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
SB#
```

Figura 15

```
SC#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
SC#
```

Ahora se activa globalmente (en donde se encontraba desactivado, es decir el router de BOGOTA y MEDELLIN) con el comando `cdp run`:

Figura 16

```
CALI(config)#cdp run
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console

CALI#
```

Figura 17

```
BOGOTA(config)#cdp run
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#
```

Ahora si se verifican los vecinos con el comando `show cdp neighbors`:

Switches:

Figura 18

```
SM#show 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
MEDELLIN     Fas 0/1          177            R       C1900       Gig 0/0
SM#
```

Figura 19

```
SB#show 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
BOGOTA       Fas 0/1          176            R       C1900       Gig 0/0
SB#
```

Figura 20

```
SC#show 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
CALI         Fas 0/1          178            R       C1900       Gig 0/0
SC#
```

Routers:

Figura 21

```
MEDELLIN#show 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
SM           Gig 0/0          129            S       2960        Fas 0/1
BOGOTA       Ser 0/0/0        160            R       C1900       Ser 0/0/0
MEDELLIN#
```

Figura 22

```
BOGOTA#show 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
SB           Gig 0/0          172            S       2960        Fas 0/1
MEDELLIN     Ser 0/0/0        179            R       C1900       Ser 0/0/0
CALI         Ser 0/0/1        124            R       C1900       Ser 0/0/0
BOGOTA#
```

Figura 23

```
CALI#show 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
BOGOTA       Ser 0/0/0        171            R       C1900       Ser 0/0/1
SC           Gig 0/0          140            S       2960        Fas 0/1
CALI#
```

Se observa que efectivamente, en cada router se informan los dispositivos conectados, en que interfaz local están conectados, desde que interfaz del vecino

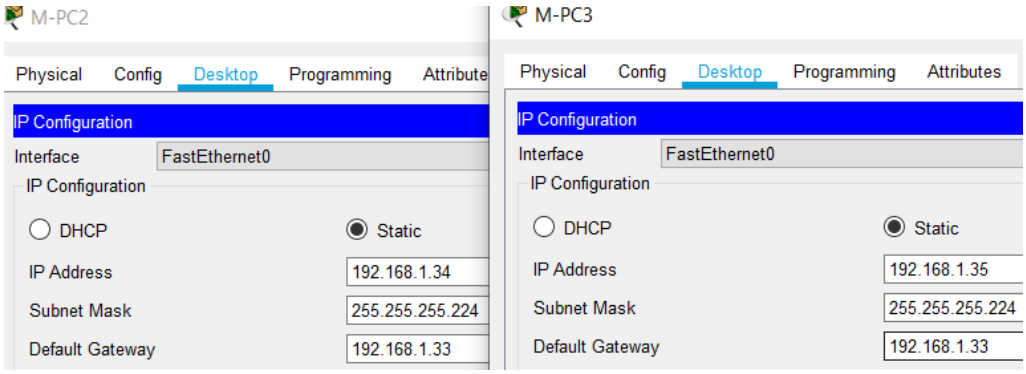
se conectaron, el tipo de dispositivos y el modelo, y el tiempo que se guardan los paquetes cdp recibidos; en donde lo anterior corresponde con la topología lógica.

**e. Y finalmente se realiza una prueba de conectividad en cada tramo de la ruta usando el comando ping:**

Ahora después de ya tener configurados los routers, se procede a configurar las PC, según las direcciones de red e interfaces G0/0 de los routers:

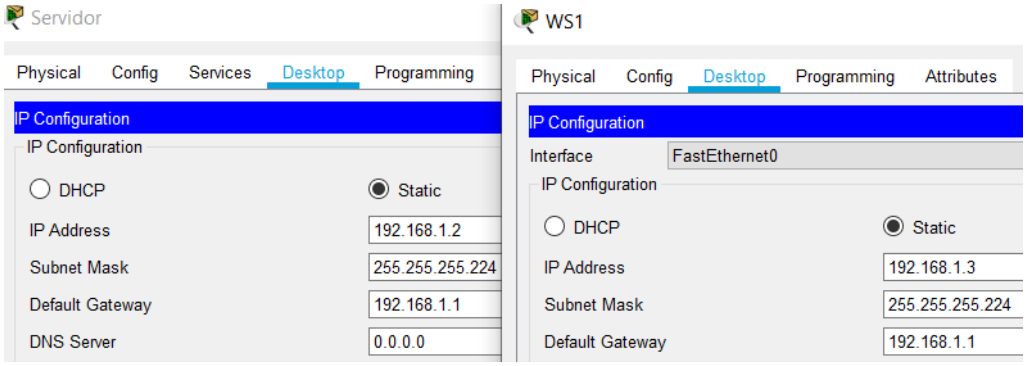
Sede MEDELLIN:

Figura 24



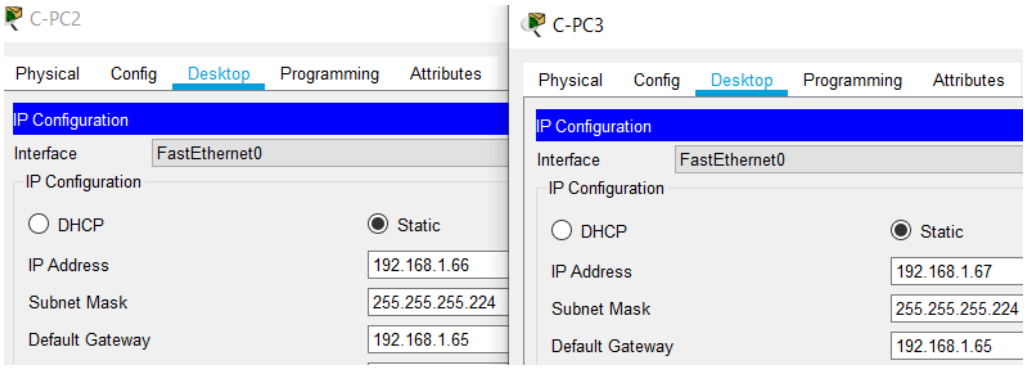

Sede BOGOTA:

Figura 25




Sede CALI:

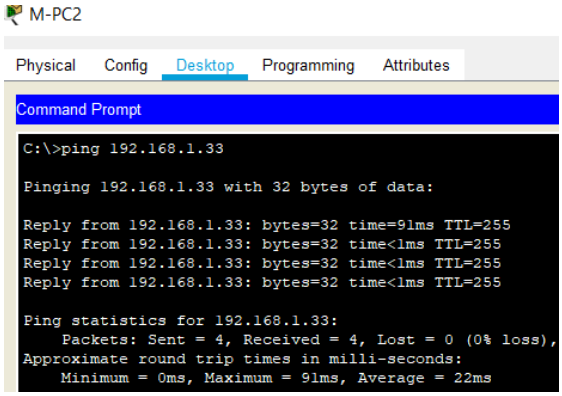
Figura 26




Ahora, se prueba la conectividad de cada tramo:

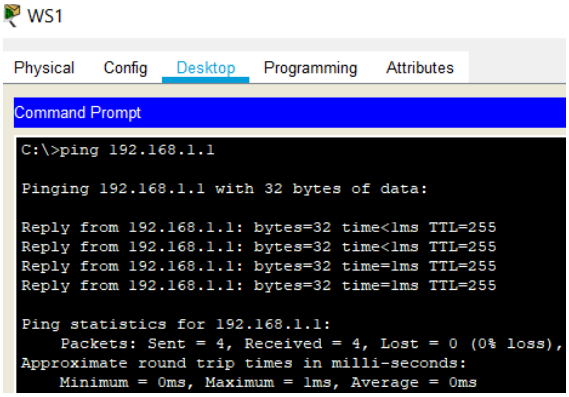
De un PC al Gateway en la red de MEDELLIN:

Figura 27



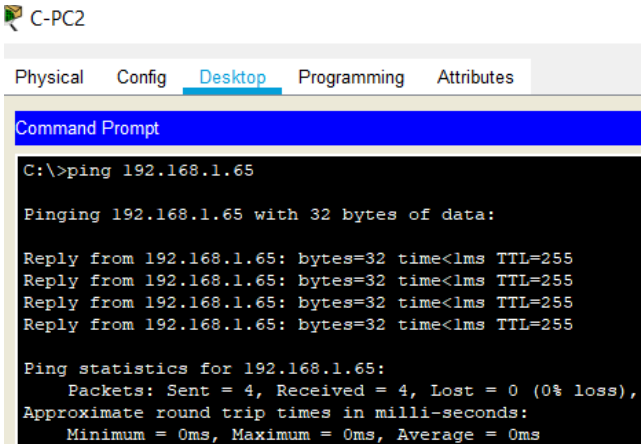

De un PC al Gateway en la red de BOGOTA:

Figura 28




De un PC al Gateway en la red de CALI:

Figura 29




Del router BOGOTA al router MEDELLIN:

Figura 30

```
BOGOTA>ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/12 ms

BOGOTA>
```

Del router BOGOTA al router CALI:

Figura 31

```
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 = 6/8/11 ms

BOGOTA>
```

## 1.3 Configuración de Enrutamiento

**a. Se configura el protocolo EIGRP en cada router, con los siguientes comandos:**

### R1 MEDELLIN:

```
enable
conf t
router eigrp 200
no auto-summary
network 192.168.1.32
network 192.168.1.96
end
copy run start
```

### R2 BOGOTA:

```
enable
conf t
router eigrp 200
no auto-summary
network 192.168.1.96
network 192.168.1.0
network 192.168.1.128
end
copy run start
```

### R3 CALI:

```
enable
conf t
router eigrp 200
no auto-summary
network 192.168.1.128
network 192.168.1.64
end
copy run start
```

**b. Ahora se verifican los vecinos EIGRP de cada router:**

Figura 32

```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt  Num
0   192.168.1.98    Se0/0/0         10   00:14:22  40     1000  0   5

MEDELLIN#
```

Figura 33

```
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt  Num
0   192.168.1.99    Se0/0/0         11   00:15:01  40     1000  0   7
1   192.168.1.131   Se0/0/1         11   00:13:04  40     1000  0   7

BOGOTA#
```

Figura 34

```
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt  Num
0   192.168.1.130   Se0/0/0         10   00:13:24  40     1000  0   6

CALI#
```

Se observa que efectivamente los routers MEDELLIN y CALI tienen un vecino EIGRP, y el router BOGOTA tiene 2

vecinos, lo cual corresponde con la topología lógica y los routers configurados con EIGRP; se observa el proceso 1 (porque todos los routers fueron configurados con un proceso EIGRP 1), la interfaz local a la que esta conectado el vecino EIGRP, y demás información de secuencia, tiempo desde que se descubrió, etc.

**c. Ahora se procede a verificar que efectivamente se hallan agregado las rutas dinámicas EIGRP (D) a las tablas de enrutamiento de cada router, con el comando `show ip route`:**

Figura 35

```
Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:19:26, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:17:30, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:19:26, Serial0/0/0

MEDELLIN#
```

Figura 36

```
Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D       192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:19:39, Serial0/0/0
D       192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:17:43, Serial0/0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1

BOGOTA#
```

Figura 37

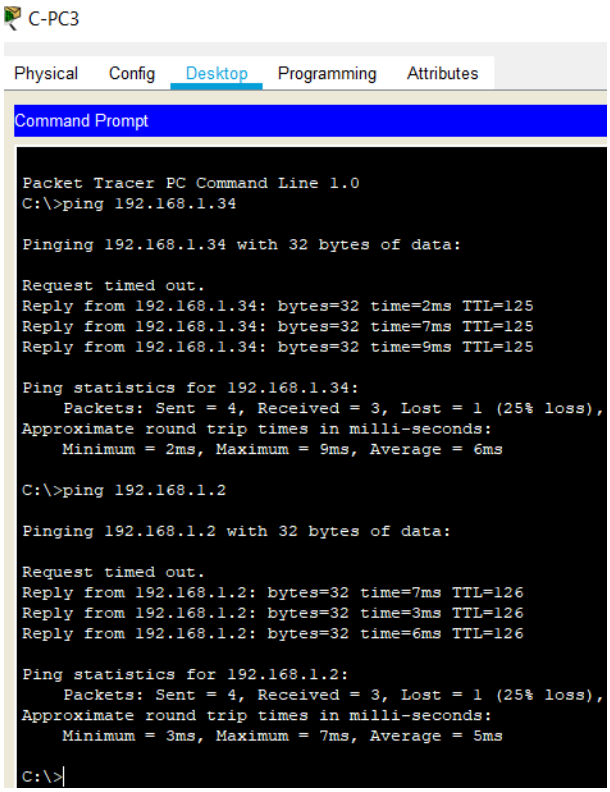
```
Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:17:53, Serial0/0/0
D       192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:17:53, Serial0/0/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:17:53, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0

CALI#
```

Se observa que efectivamente se agregaron las rutas EIGRP (D), con distancia administrativa de 90, y una métrica esperada.

**d. Y ahora, verificamos que exista conectividad entre las 3 redes LAN ethernet:**

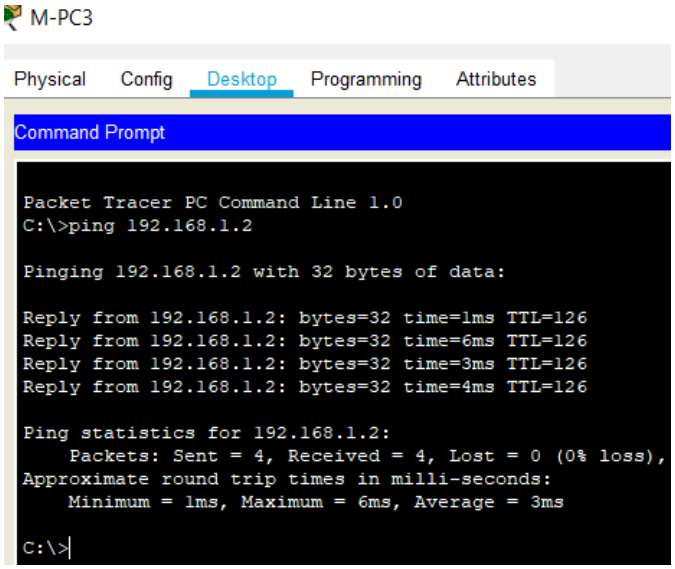
Se realiza ping desde el C-PC3(192.168.1.67) de la red de CALI, hacia el M-PC2(192.168.1.34) de la red de MEDELLIN, y hacia el Servidor(192.168.1.2) de la red de BOGOTA:

Figura 38



Y ahora, se realiza ping desde el M-PC3(192.168.1.35) de la red de MEDELLIN, hacia el hacia el Servidor(192.168.1.2) de la red de BOGOTA:

Figura 39



## 1.4 Configuración de listas de Control de Acceso

Ahora, se configuran listas de control de acceso en base a los siguientes requerimientos:

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

**a. Primero, se permite el acceso desde las LAN de MEDELLIN y CALI, hacia el Servidor, y con el deny implícito se negará el resto de tráfico:**

Con los siguientes comandos, en los routers MEDELLIN CALI, se configura una ACL extendida, en dirección entrante en las interfaces g0/0, permitiendo el tráfico con cualquier dirección IP de origen y con la dirección de host de destino 192.168.1.2: (**se aplican los mismos comandos en ambos routers**)

```
enable

conf t

ip access-list extended MSERVER (cambia el nombre para CALI, a CSERVER)

permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0

exit

int g0/0

ip access-group MSERVER in

end
```

Con la configuración anterior, se bloquean todos los paquetes que ingresan a la interfaz g0/0 del router MEDELLIN y CALI, excepto los que tiene dirección IP de destino el Servidor de la LAN de BOGOTA; con lo cual **las estaciones de trabajo en las LAN de MEDELLIN y CALI no tienen acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor**, y además **ningún dispositivo externo (fuera de la subred respectiva) puede conectarse con las estaciones mencionadas**, debido a que los paquetes de respuesta con dirección IP de destino que no sea la del servidor, serán bloqueados.

**b. Segundo, se debe garantizar que de la LAN de BOGOTA solo el servidor pueda acceder a toda la red, y que WS1 solo acceda a su subred:**

Con los siguientes comandos, en el **router BOGOTA**, se configura una ACL extendida, en dirección entrante en las interface

s g0/0, permitiendo solo el tráfico con la dirección IP de origen de host 192.168.1.2 y con la cualquier dirección IP de destino:

```
enable

conf t

ip access-list extended BSERVER

permit ip 192.168.1.2 0.0.0.0 0.0.0.0 255.255.255.255

exit

int g0/0

ip access-group BSERVER in

end
```

Con la configuración anterior, se permite que en la interface g0/0 solo entre el tráfico con dirección de origen 192.168.1.2, el resto se deniega, **por tanto, WS1 no podrá salir de su subred, pero el Servidor sí.**

**c. Y tercero, los routers además de establecer conexiones Telnet con los demás routers (para lo cual deben tener configuradas sus líneas vty), los routers, deben poder acceder a todos los dispositivos:**

Con los siguientes comandos, en el cada router, se añade a las ACL extendidas configuradas en dirección entrante en las interfaces g0/0, 3 opciones permit permitiendo también solamente el tráfico con cualquier dirección IP de origen y con la dirección de host de destino de cada router (dirección IP del router de su interfaz más cercana a cada LAN, es decir, por ejemplo en la red LAN de MEDELLIN, se permiten paquetes con la dirección de destino, de la interfaz g0/0 de ese router, de la interfaz s0/0/0 de BOGOTA, y de la interfaz s0/0/0 de CALI):

**Router MEDELLIN:**

```
enable

conf t

ip access-list extended MSERVER

permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0

permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0

permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
```

```
end
copy run start
```

### Router BOGOTA:

```
enable
conf t
ip access-list extended BSERVER
permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
end
copy run start
```

### Router CALI:

```
enable
conf t
ip access-list extended CSERVER
permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
permit ip 0.0.0.0 255.255.255.255 192.168.130.1 0.0.0.0
permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
end
copy run start
```

Con la configuración anterior, se permite el tráfico con dirección de destino de algún router, es decir, de la interfaz de router más cercana a cada LAN, que es desde la cual se generaría una conexión desde determinado router hacia determinada LAN.

## 1.5 Comprobación de la red instalada

**a. Se comprueba que la configuración de las listas de acceso fue exitosa en cada router, con el comando `show access-list`:**

Figura 40

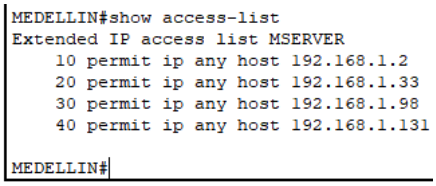



Figura 41

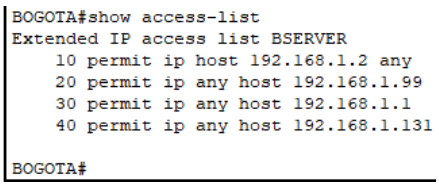
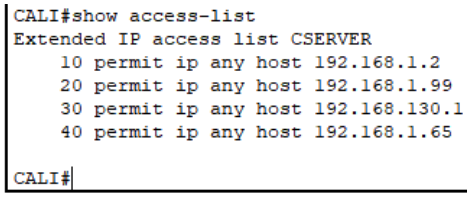



Figura 42




**b. Se realizan las siguientes pruebas, para verificar que cumpla con los requisitos se seguridad y conectividad:**

**OK:** Exitoso

**Fail:** Fallido (Destination host unreachable, es decir que fue bloqueado, en este caso por las ACL configuradas).

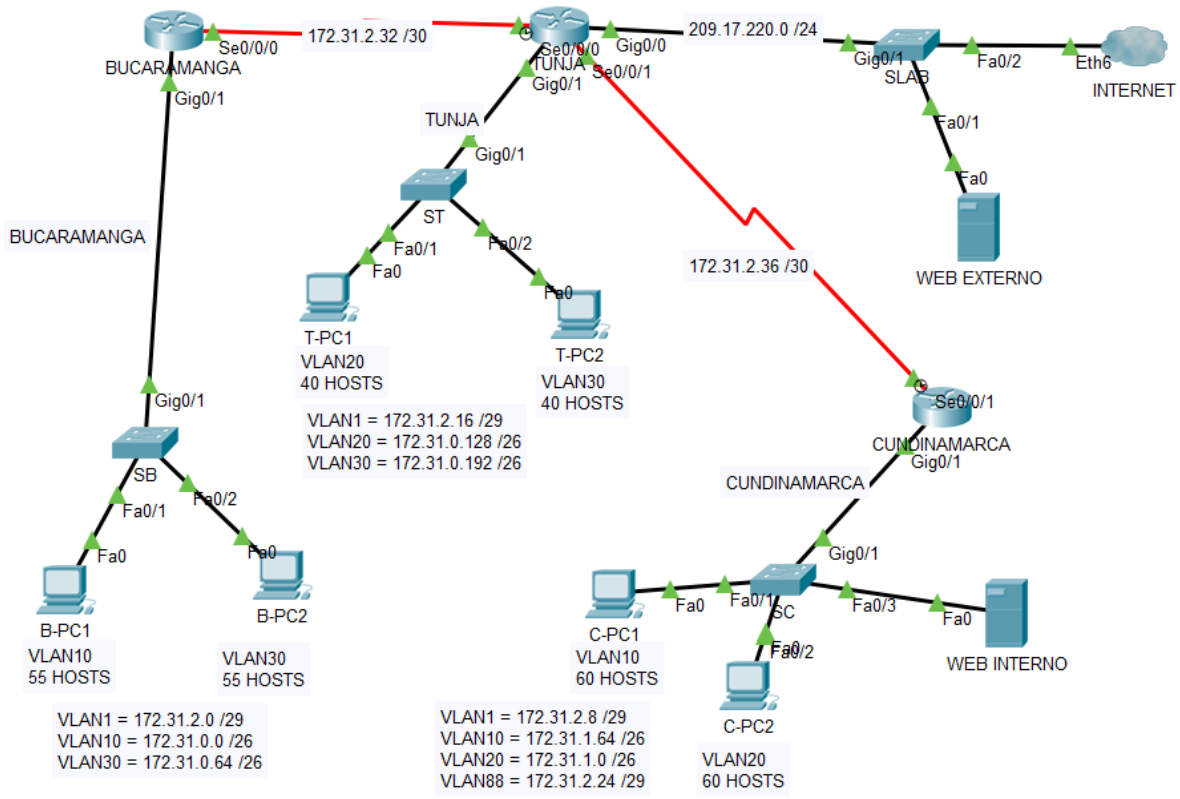
Tabla 2

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

# 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.

Figura 43



## 2.1 Configuración básica y Segura

a. **Aquí se configuran todos los routers, según los siguientes requerimientos:**
   - Configuración básica.
   - Autenticación local con AAA.
   - Cifrado de contraseñas.
   - Un máximo de intentos para acceder al router.
   - Máximo tiempo de acceso al detectar ataques.

El requerimiento de **"Establecer un servidor TFTP y almacenar todos los archivos necesarios de los routers.",** se deberá ejecutar manualmente con el comando `copy tftp...`, cuando exista conectividad con el servidor WEB INTERNO, y preferiblemente después de configurar todo. En la **Parte 6**, se describen los comandos utilizados.

**Comandos en BUCARAMANGA:**

```
enable
conf t
hostname BUCARAMANGA
enable password adminr1
service password-encryption
login block-for 300 attempts 2 within 30
aaa new-model
aaa authentication login ADMINSAAA local enable
username Barran1 secret Barran1
line con 0
logging synchronous
login authentication ADMINSAAA
exec-timeout 10
line vty 0 15
logging synchronous
login authentication ADMINSAAA
exec-timeout 3
exit
interface s0/0/0
ip address 172.31.2.33 255.255.255.252
no shutdown
interface g0/1.1
encapsulation dot1q 1
ip address 172.31.2.1 255.255.255.248
interface g0/1.10
encapsulation dot1q 10
ip address 172.31.0.1 255.255.255.192
interface g0/1.30
encapsulation dot1q 30
ip address 172.31.0.65 255.255.255.192
interface g0/1
no shutdown
end
```

```
copy run start
```

## Comandos en TUNJA:

```
enable
conf t
hostname TUNJA
enable password adminr2
service password-encryption
login block-for 300 attempts 2 within 30
aaa new-model
aaa authentication login ADMINSAAA local enable
username Tunj1 secret Tunj1
line con 0
logging synchronous
login authentication ADMINSAAA
exec-timeout 10
line vty 0 15
logging synchronous
login authentication ADMINSAAA
exec-timeout 3
exit
interface s0/0/0
ip address 172.31.2.34 255.255.255.252
clock rate 1000000
no shutdown
interface s0/0/1
ip address 172.31.2.37 255.255.255.252
no shutdown
interface g0/0
ip address 209.17.220.1 255.255.255.0
no shutdown
interface g0/1.1
encapsulation dot1q 1
ip address 172.3.2.9 255.255.255.248
interface g0/1.20
encapsulation dot1q 20
ip address 172.31.0.129 255.255.255.192
interface g0/1.30
encapsulation dot1q 30
ip address 172.31.0.193 255.255.255.192
interface g0/1
no shutdown
end
copy run start
```

## Comandos CUNDINAMARCA:

```
enable
conf t
hostname CUNDINAMARCA
enable password adminr3
service password-encryption
login block-for 300 attempts 2 within 30
aaa new-model
aaa authentication login ADMINSAAA local enable
username Cund1 secret Cund1
line con 0
logging synchronous
login authentication ADMINSAAA
exec-timeout 10
line vty 0 15
logging synchronous
login authentication ADMINSAAA
exec-timeout 3
exit
interface s0/0/1
ip address 172.31.2.38 255.255.255.252
```

```
clock rate 1000000
no shutdown
interface g0/1.1
encapsulation dot1q 1
ip address 172.31.2.9 255.255.255.248
interface g0/1.10
encapsulation dot1q 10
ip address 172.31.1.65 255.255.255.192
interface g0/1.20
encapsulation dot1q 20
ip address 172.31.1.1 255.255.255.192
interface g0/1.88
encapsulation dot1q 88
ip address 172.31.2.25 255.255.255.248
interface g0/1
no shutdown
end
copy run start
```

## 2.2 VLAN y DHCP

**a. Primero, se configuran las VLAN en cada switch, permitiendo también su enrutamiento al asignarles una dirección IP:**

Con los siguientes comandos, se asigna IP a cada VLAN, y luego se asignan las respectivas VLAN a los puertos:

### Switch BUCARAMANGA:

```
enable
conf t
hostname SB
vlan 1
name VLAN1
vlan 10
name VLAN10
vlan 30
name VLAN30
exit
int VLAN1
ip address 172.31.2.2 255.255.255.248
no shutdown
int VLAN10
ip address 172.31.0.2 255.255.255.192
no shutdown
int VLAN30
ip address 172.31.0.66 255.255.255.192
no shutdown
int f0/1
switchport mode access
switchport access vlan 10
int f0/2
switchport mode access
switchport access vlan 30
int g0/1
switchport mode trunk
end
copy run start
```

### Switch TUNJA:

```
enable
conf t
hostname ST
vlan 1
name VLAN1
vlan 20
name VLAN20
vlan 30
name VLAN30
exit
int VLAN1
ip address 172.3.2.10 255.255.255.248
no shutdown
int VLAN20
ip address 172.31.0.130 255.255.255.192
no shutdown
int VLAN30
```

```
ip address 172.31.0.194 255.255.255.192
no shutdown
int f0/1
switchport mode access
switchport access vlan 20
int f0/2
switchport mode access
switchport access vlan 30
int g0/1
switchport mode trunk
end
copy run start
```

### Switch CUNDINAMARCA:

```
enable
conf t
hostname SC
vlan 1
name VLAN1
vlan 10
name VLAN20
vlan 20
name VLAN30
vlan 88
name VLAN88
exit
int VLAN1
ip address 172.31.2.10 255.255.255.248
no shutdown
int VLAN10
ip address 172.31.1.66 255.255.255.192
no shutdown
int VLAN20
ip address 172.31.1.2 255.255.255.192
no shutdown
int VLAN88
ip address 172.31.2.26 255.255.255.248
no shutdown
int f0/1
switchport mode access
switchport access vlan 10
int f0/2
switchport mode access
switchport access vlan 20
int f0/3
switchport mode access
switchport access vlan 88
int g0/1
switchport mode trunk
end
copy run start
```

**b. Ahora, se configura el servicio DHCP en el router TUNJA, y la retransmisión en los router BUCARAMANGA y CUNDINAMARCA:**

Con los siguientes comandos en el router TUNJA, primero, se excluyen las direcciones IP que se configuraron en los routers y en las VLAN de los switch; luego se configura un pool para cada VLAN de BUCARAMANGA y CUNDINAMARCA, un total de 7 pools, para dar direcciones IP a BUCARAMANGA y CUNDINAMARCA, pero a TUNJA no:

```
enable
conf t
```

```
ip dhcp excluded-address 172.31.2.11

ip dhcp excluded-address 172.31.2.1 172.31.2.2

ip dhcp excluded-address 172.31.0.1 172.31.0.2

ip dhcp excluded-address 172.31.0.65 172.31.0.66

ip dhcp excluded-address 172.31.2.9 172.31.2.10

ip dhcp excluded-address 172.31.1.65 172.31.1.66

ip dhcp excluded-address 172.31.1.1 172.31.1.2

ip dhcp excluded-address 172.31.2.25 172.31.2.26

ip dhcp pool LANBV1

network 172.31.2.0 255.255.255.248

default-router 172.31.2.1

ip dhcp pool LANBV10

network 172.31.0.0 255.255.255.192

default-router 172.31.0.1

ip dhcp pool LANBV30

network 172.31.0.64 255.255.255.192

default-router 172.31.0.65

ip dhcp pool LANCV1

network 172.31.2.8 255.255.255.248

default-router 172.31.2.9

ip dhcp pool LANCV10

network 172.31.1.64 255.255.255.192

default-router 172.31.1.65

ip dhcp pool LANCV20

network 172.31.1.0 255.255.255.192

default-router 172.31.1.1

ip dhcp pool LANCV88

network 172.31.2.24 255.255.255.248

default-router 172.31.2.25

end

copy run sta
```

Ahora, con los siguientes comandos se configura la retransmisión de DHCP en las subinterfaces g0/1 del router BUCARAMANGA y CUNDINAMARCA

**Router BUCARAMANGA:**

```
enable

conf t

int g0/1.1

ip helper-address 172.31.2.34

int g0/1.10

ip helper-address 172.31.2.34

int g0/1.30

ip helper-address 172.31.2.34

end

copy run start
```

**Router CUNDINAMARCA:**

```
enable

conf t

int g0/1.1

ip helper-address 172.31.2.37

int g0/1.10

ip helper-address 172.31.2.37

int g0/1.20

ip helper-address 172.31.2.37

int g0/1.88

ip helper-address 172.31.2.37

end

copy run start
```

## 2.3 Enrrutamiento OSPF

**a. Se configura el protocolo de enrutamiento OSPF de área 0 en cada router:**

Con los siguientes comandos, se activa OSPF, se anuncian las redes conectadas por las cuales también se anuncia OSPF, se configura la interfaz LAN como pasiva, para que por allí no se anuncie OSPF; y se indica que para todas las red de área 0, se utilice autenticación:

### Router BUCARRAMANGA:

```
enable
conf t
router ospf 1
router-id 1.1.1.1
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.0 0.0.0.7 area 0
network 172.31.0.1 0.0.0.63 area 0
network 172.31.0.64 0.0.0.63 area 0
passive-interface g0/1
area 0 authentication
end
copy run start
```

### Router TUNJA:

```
enable
conf t
router ospf 1
router-id 2.2.2.2
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.36 0.0.0.3 area 0
network 209.17.220.0 0.0.0.255 area 0
network 172.3.2.8 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
passive-interface g0/1
area 0 authentication
end
copy run start
```

### Router CUDINAMARCA:

```
enable
conf t
router ospf 1
router-id 3.3.3.3
network 172.31.2.36 0.0.0.3 area 0
network 172.31.2.8 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 172.31.2.24 0.0.0.7 area 0
passive-interface g0/1
area 0 authentication
end
```

```
copy run start
```

**b. Con los siguientes comandos, se configura una clave OSPF en las interfaces por las cuales se anuncia OSPF, la cual debe coincidir con el otro router, para que permanezca o se establezca la adyacencia de vecinos OSPF:**

### Router BUCARAMANGA:

```
enable
conf t
int s0/0/0
ip ospf authentication-key osintepf
end
copy run start
```

### Router TUNJA:

```
enable
conf t
int s0/0/0
ip ospf authentication-key osintepf
int s0/0/1
ip ospf authentication-key osintepf
end
copy run start
```

### Router CUNDINAMARCA:

```
enable
conf t
int s0/0/0
ip ospf authentication-key osintepf
end
copy run start
```

## 2.4 NAT y PAT

a. Aquí se configura la traducción por dirección de red (NAT) estática para el servidor, y la NAT de sobrecarga con traducción por dirección de puerto (PAT) para el resto de los equipos:

Los siguientes comandos se aplican en el router TUNJA, debido a que este router TUNJA es como la puerta de salida de la red Ethernet hacia internet; en estos comandos, primero se configura una traducción estática para el servidor, luego una ACL para determinar las direcciones IP a traducir (todas las de la red 172.31.0.0 /16), luego se asigna esa ACL (como las IP locales internas), a una traducción NAT con overload (para que, como solo se configura una IP global interna, se traduzcan todos los paquetes, por PAT), asignando como IP global interna la dirección IP de la interfaz g0/0; y finalmente se configuran las interfaces y subinterfaces como internas (ip nat inside), excepto la g0/0 la cual será externa (ip nat outside), para así identificar donde se realizara la traducción:

```
enable

conf t

ip nat inside source static 172.31.2.11
209.17.220.5

ip access-list standard PAT-ACL

permit 172.31.0.0 0.0.255.255

exit

ip nat inside source list PAT-ACL
interface g0/0 overload

int g0/0

ip nat outside

int s0/0/0

ip nat inside

int s0/0/1

ip nat inside

int g0/1.1

ip nat inside

int g0/1.20

ip nat inside

int g0/1.30

ip nat inside

end

copy run start
```

b. Ahora, se deberá configurar una ruta estática como ruta predeterminada en el router TUNJA, para que los paquetes con una dirección IP desconocida (es decir, que no se encuentra en las tablas de enrutamiento), salgan por la interfaz g0/0 a internet:

Los siguientes comandos se aplican en el router TUNJA, allí se crea una ruta estática predeterminada, con interfaz de salida g0/0; y luego en proceso OSPF 1, se indica que se propague información predeterminada, como la ruta que se acabo de crear, esto para que todos puedan acceder a internet, sin tener que configurar una ruta estática predeterminada en cada router:

```
enable

conf t

ip route 0.0.0.0 0.0.0.0 g0/0

router ospf 1

default-information originate

end

copy run start
```

## 2.5 Listas de control de acceso (ACL)

a. Se configuran ACL (listas de control de acceso), para restringir el acceso de determinadas VLAN a determinadas áreas de la red e incluso a internet, en base a los siguientes requerimientos:

- **Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja, y a la VLAN 10 de Bucaramanga.** (ACL: Extendida, con opciones permit y deny especificas)
- **Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.** (ACL: Extendida, con opciones deny específicas, y una opción permit general)
- **Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.** (ACL: Extendida, con opciones permit especificas)
- **Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.** (ACL: Extendida, con opciones permit y deny especificas)
- **Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.** (ACL: Extendida, con opciones deny específicas, y una opción permit general)
- **Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.** (ACL: Extendida, con opciones permit y deny especificas)
- **Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad, ni a los routers.**
- **Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet**.

A continuación, se describen los comandos utilizados para configurar las ACL en cada router a fin de cumplir con los requerimientos; para un mejor entendimiento, se ha subrayado con un color cada requerimiento, el cual coincide con el color de los comandos utilizados para cumplir dicho requerimiento; también se subrayaron los requerimientos agregados, a fin de que se cumplan otros; y finalmente entre paréntesis se describe el tipo y forma de ACL utilizada:

## Router BARRANQUILLA:

```
enanble

conf t

ip access-list extended ACLV1

deny ip 172.31.2.0 0.0.0.7 172.31.0.64 0.0.0.63

deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

permit ip any any

exit

int g0/1.1

ip access-group ACLV1 in

exit

ip access-list extended ACLV10

deny ip 172.31.0.0 0.0.0.63 172.31.2.0 0.0.0.7

deny ip 172.31.0.0 0.0.0.63 172.31.0.64 0.0.0.63

deny ip 172.31.0.0 0.0.0.63 host 172.31.1.1

deny ip 172.31.0.0 0.0.0.63 host 172.31.0.129

permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63

permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

permit udp any any eq bootps

exit

int g0/1.10

ip access-group ACLV10 in

exit

ip access-list extended ACLV30

deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7

deny ip 172.31.0.64 0.0.0.63 host 172.31.0.65

deny ip 172.31.0.64 0.0.0.63 host 172.31.0.1

deny ip 172.31.0.64 0.0.0.63 host 172.31.1.65

deny ip 172.31.1.64 0.0.0.63 172.31.2.33 0.0.0.3

deny ip 172.31.1.64 0.0.0.63 172.31.2.36 0.0.0.3

deny ip 172.31.0.64 0.0.0.63 172.31.2.16 0.0.0.7

deny ip 172.31.0.64 0.0.0.63 172.31.0.128 0.0.0.63

deny ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63

deny ip 172.31.0.64 0.0.0.63 172.31.2.8 0.0.0.7

deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63

deny ip 172.31.0.64 0.0.0.63 172.31.2.24 0.0.0.7

permit ip any any

exit

int g0/1.30

ip access-group ACLV30 in

end

copy running startup
```

## Router TUNJA:

```
enable

conf t

ip access-list extended ACLV1

deny ip 172.31.2.16 0.0.0.7 172.31.0.128 0.0.0.63

deny ip 172.31.2.16 0.0.0.7 172.31.0.192 0.0.0.63

permit ip any any

exit

int g0/1.1

ip access-group ACLV1 in

exit

ip access-list extended ACLV20
```

```
deny ip 172.31.0.128 0.0.0.63 host 172.31.1.1

deny ip 172.31.0.128 0.0.0.63 host 172.31.0.1

permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63

permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

exit

int g0/1.20

ip access-group ACLV20 in

exit

ip access-list extended ACLV30

permit tcp 172.31.0.192 0.0.0.63 any eq ftp

permit tcp 172.31.0.192 0.0.0.63 any eq www

exit

int g0/1.30

ip access-group ACLV30 in

end

copy running startup
```

## Router CUNDINAMARCA:

```
enable

conf t

ip access-list extended ACLV1

deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

deny ip 172.31.2.8 0.0.0.7 172.31.1.0 0.0.0.63

deny ip 172.31.2.8 0.0.0.7 172.31.2.24 0.0.0.7

permit ip any any

exit

int g0/1.1

ip access-group ACLV1 in

exit

ip access-list extended ACLV10

deny ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7

deny ip 172.31.1.64 0.0.0.63 172.31.1.0 0.0.0.63

deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7

deny ip 172.31.1.64 0.0.0.63 host 172.31.1.65

deny ip 172.31.1.64 0.0.0.63 host 172.31.2.1

deny ip 172.31.1.64 0.0.0.63 host 172.31.0.1

deny ip 172.31.1.64 0.0.0.63 host 172.31.0.65

deny ip 172.31.1.64 0.0.0.63 172.31.2.33 0.0.0.3

deny ip 172.31.1.64 0.0.0.63 172.31.2.36 0.0.0.3

deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7

deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63

deny ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63

permit ip any any

exit

int g0/1.10

ip access-group ACLV10 in

exit

ip access-list extended ACLV20

deny ip 172.31.1.0 0.0.0.63 host 172.31.1.1

deny ip 172.31.1.0 0.0.0.63 host 172.31.2.17

deny ip 172.31.1.0 0.0.0.63 host 172.31.0.129

deny ip 172.31.1.0 0.0.0.63 host 172.31.0.193

deny ip 172.31.1.0 0.0.0.63 host 172.31.0.1
```

```
permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7

permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63

permit ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63

permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63

permit udp any any eq bootps

exit

int g0/1.20

ip access-group ACLV20 in

exit

ip access-list extended ACLV88

deny ip 172.31.2.24 0.0.0.7 172.31.2.8 0.0.0.7

deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

deny ip 172.31.2.24 0.0.0.7 172.31.1.0 0.0.0.63

permit ip any any

exit

int g0/1.88

ip access-group ACLV88 in

end

end

copy running startup
```

## 2.6 Verificación y Respaldo

**a. A continuación, en base a las anteriores configuraciones, se realizan ciertas verificaciones, para corroborar la conectividad y la seguridad:**

Tabla 3

| | Origen | | | Destino | | | R | T |
|---|---|---|---|---|---|---|---|---|
| | Red | Nombre | IP | Red | Nombre | IP | | |
| 1 | Bucaram... | VLAN10 | 172.31.0.3 | Cundina... | VLAN20 | 172.31.1.3 | OK | P |
| 2 | Bucaram... | VLAN10 | 172.31.0.3 | Cundina... | VLAN10 | 172.31.1.67 | Fail | P |
| 3 | Tunja | VLAN30 | 172.31.0.195 | Externa | WebExterno | 209.17.220.5 | OK | FTP |
| 4 | Cundina... | VLAN88 | 172.31.2.27 | Bucaram... | Router | 172.31.2.33 | OK | TE |
| 5 | Cundina... | VLAN20 | 172.31.1.3 | Bucaram... | VLAN30 | 172.31.0.67 | Fail | P |

R = Resultado esperado

T = Tipo de prueba

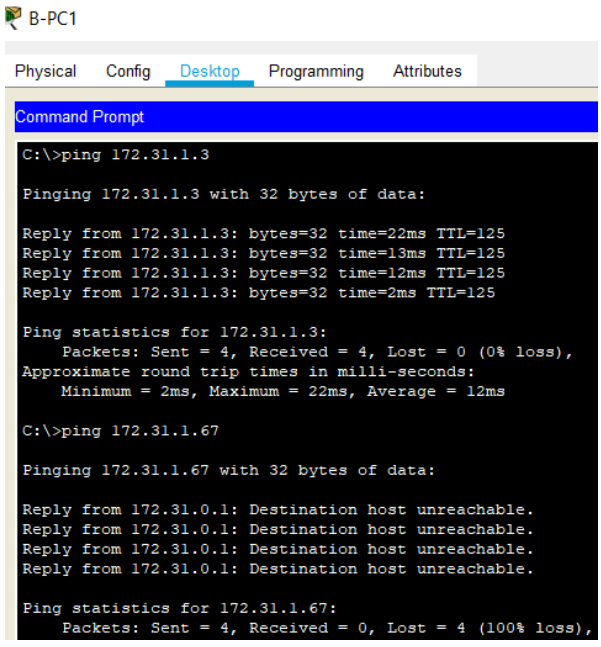
P = Ping

FTP = Acceso a servidor FTP

TE = Telnet

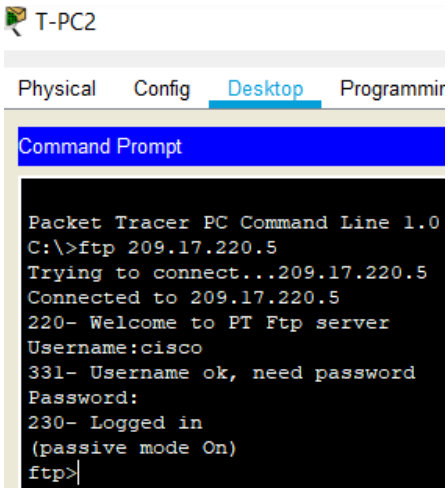
**No. 1 y No. 2**

Figura 44



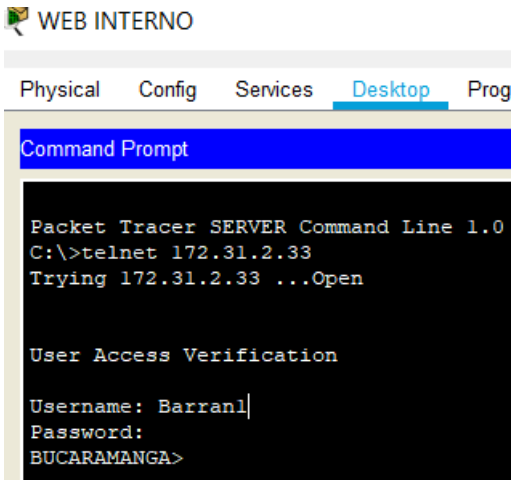
**No. 3**

Figura 45



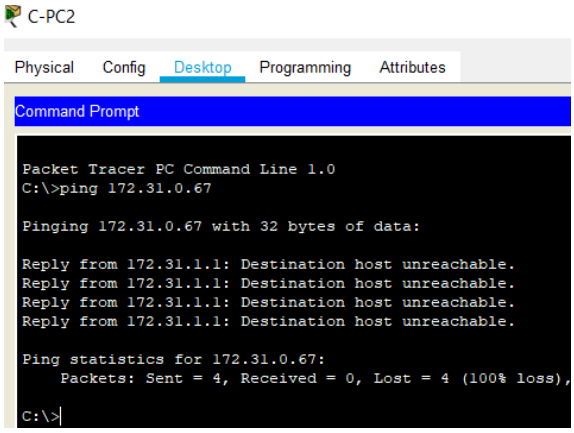

**No. 4**

Figura 46




**No. 5**

Figura 47




**b. Después de que se configuraron los routers y de que existió conectividad con el servidor WEB INTERNO; se proceden a ingresar los siguientes comandos en cada router, para guardar una copia de respaldo de la configuración de inicio, y una copia de respaldo del IOS:**

## Router BUCARAMANGA:

```
copy run start
copy startup-config tftp
172.31.2.27
Respaldo_RB_startup
copy flash: tftp:
c1900-universalk9-mz.SPA.151-4.M4.bin
172.31.2.27
Respaldo_RB_IOS
```

## Router TUNJA:

```
copy run start
copy startup-config tftp
172.31.2.27
Respaldo_RT_startup
copy flash: tftp:
c1900-universalk9-mz.SPA.151-4.M4.bin
172.31.2.27
Respaldo_RT_IOS
```

## Router CUNDINAMARCA:

```
copy run start
copy startup-config tftp
172.31.2.27
Respaldo_RC_startup
copy flash: tftp:
c1900-universalk9-mz.SPA.151-4.M4.bin
172.31.2.27
Respaldo_RC_IOS
```

## Conclusiones

- ✓ Al final, se tienen 2 redes funcionando completa y seguramente en base a los requerimientos, en donde se observó que existen configuraciones adicionales a las famosas contraseñas, como límite de intentos de acceso, usuario y contraseña, y tiempo máximo de permanencia.
- ✓ Se conocieron comandos de verificación muy útiles, como la verificación de vecinos cdp y EIGRP, los cuales permiten verificar determinada configuración, y conocer algunas características de los equipos conectados, aunque no se tenga acceso físico a estos.
- ✓ Los protocolos de enrutamiento dinámico, permiten el anuncio de las redes conectadas al router, y así cada router al anunciar sus redes, todos terminan conociendo todas las redes y rutas disponibles para enviar paquetes, con la ventaja de que si se agregan o se quitan rutas, todos los routers lo sabrán en breve tiempo; adicionalmente OSPF cuenta con autenticación, la cual consiste en configurar una misma contraseña en cada interfaz que se conecta con el vecino OSPF, en donde el vecino OSPF tener configurada la misma contraseña, para que exista adyacencia.
- ✓ En DHCP, si se quiere evitar que una red acceda a estos servicios, existen múltiples opciones, desde no configurar un pool para estas redes, no configurar la retransmisión, hasta bloquear el trafico DHCP en determinada interfaz de router, en donde esta ultima es la más efectiva, ya que no permite que se utilicen innecesariamente recursos de red, en paquetes DHCP que no tendrán éxito.
- ✓ NAT y PAT, son servicios interesantes, ya que traducen múltiples direcciones IP locales internas, en una sola dirección global interna, gracias a PAT, al asignar a cada paquete una dirección de puerto diferente; también es posible configurar varias direcciones IP globales internas, pero es más efectiva solo una, con NAT de sobrecarga (a través de PAT).
- ✓ Las listas de control de acceso ACL, tienen multiplicidad de configuraciones, desde ACL estándar, hasta ACL extendidas, también es posible especificar protocolos, interfaces, y si se filtran paquetes entrantes o salientes; por otro lado se observó que se debe tener muy en cuenta que tipo de paquetes circulan por la red, a la hora de aplicar este filtro, no vaya a ser que por ejemplo se terminen bloqueando servicios deseados (si es que así se desean) como DHCP, FTP, SSH, etc.

## Bibliografía


- Alani, M. M. (2017). Guide to Cisco Routers Configuration : Becoming a Router Geek (Vol. Second edition). Cham: Springer. Recuperado de http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsebk&AN=1516705&lang=es&site=eds-live&scope=site
- Boronat Seguí, F. (2013). Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Recuperado de http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edselb&AN=edselb.3217412&lang=es&site=eds-live&scope=site
- Chappell, L. (2000). Router commands. Network World, 17(36), 48. Retrieved from https://search-proquest-com.bibliotecavirtual.unad.edu.co/docview/215968015?accountid=48784
- 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). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1
- Cisco. (s. f.). Ejemplo de Configuración de Filtro ACL de Punto de Acceso. Recuperado 15 de diciembre de 2019, de Cisco website: https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/68097-accesspt.html
- Cisco. (s. f.). Ejemplo de Configuración de Filtro ACL de Punto de Acceso. Recuperado 15 de diciembre de 2019, de Cisco website: https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-lan-wlan/68097-accesspt.html
- 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 Packet Tracer (7.2.2) [software]. (2019). Fabricante: Cisco.
- J. S. y K. [Javier Reyes]. (2013, Mayo 21). Respaldo y Recuperacion IOS y CONFIG Router CISCO. Recuperado de https://www.youtube.com/watch?v=eIpqqMN81yQ&t=178s
- Granda, J. [Jorge Granda]. (2017, Junio 15). Autenticación, acceso y contabilización AAA local y remoto. Recuperado de https://www.youtube.com/watch?v=g-JHks7nljE&t=459s

- Lammle, T. (2008). Todd Lammle's CCNA IOS Commands Survival Guide. Indianapolis, Ind: Sybex. Recuperado de http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=218603&lang=es&site=eds-live&scope=site
- Mario, L. [mariontechacademy]. (2013, Noviembre 11). CS071 21.02 OSPF - Configuracion OSPF en Packet Tracer. Recuperado de https://www.youtube.com/watch?v=lw-IekHi9eY&t=31s
- Mario, L. [mariontechacademy]. (2013, Noviembre 20). CS071 22.05 VLSM - Ejemplo VLSM y EIGRP Packet Tracer. Recuperado de https://www.youtube.com/watch?v=iFGKRIjJWYs&t=376s