



EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

AMALIA CASTRO ARDILA

ING. JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS  
BÁSICAS TECNOLOGÍA E INGENIERÍA PROGRAMA DE INGENIERA DE SISTEMAS

2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

PRESIDENTE DEL JURADO

---

JURADO

---

JURADO

Bogotá, 2020

## DEDICATORIA

A DIOS esencialmente quien me ha dotado de sabiduría y templanza para lograr esta meta académica, a mis hijos Daniela y Dilan quienes siempre me han acompañado en este proceso de formación y que con su paciencia entendieron y aceptaron las horas de trabajo dedicadas a mi formación.

A mi esposo y mi madre quien han sido testigos de este sueño y esta etapa en mi vida, a todos ellos por brindarme su apoyo incondicional, con el cual hoy culmino este proceso tan enriquecedor para mí.

## CONTENIDO

<b>INTRODUCCIÓN</b>	<b>7</b>
<b>OBJETIVO GENERAL</b>	<b>8</b>
<b>OBJETIVOS ESPECÍFICOS</b>	<b>8</b>
<b>DESARROLLO DEL PROYECTO</b>	<b>8</b>
Diseño Propuesto Packet Tracer Escenario 1	9
<b>ANÁLISIS DEL DESARROLLO DEL PROYECTO</b>	<b>10</b>
<b>Parte 1: verificar la conectividad de red básica</b>	<b>11</b>
Pinging Packet tracer	11
<b>Acceso seguro a los Routers</b>	<b>12</b>
<b>Verificación del acceso exclusivo desde la estación de administración PC</b>	<b>13</b>
<b>Tabla de Enrutamiento. Router 1</b>	<b>16</b>
<b>Tabla de Enrutamiento. Router 2</b>	<b>16</b>
<b>Tabla de Enrutamiento. Router 3</b>	<b>17</b>
Parte 3: Configuración de Enrutamiento.	21
<b>Comprobación de la red instalada.</b>	<b>29</b>
<b>Escenario 2</b>	<b>32</b>
Diseño Grafico Packet Tracer Escenario 2	32
<b>Configuración inicial Router:</b>	<b>33</b>
Estructura Grafica	35
<b>Se configuran las VLAN para cada Switch:</b>	<b>38</b>
Punto 2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca	41
<b>Punto 4. El enrutamiento deberá tener autenticación.</b>	<b>44</b>
<b>Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.</b>	<b>47</b>
Listas de control de acceso:	47
<b>CONCLUSIONES</b>	<b>62</b>
<b>BIBLIOGRAFÍA</b>	<b>63</b>



## RESUMEN

Acotar la información suministrada para la posterior ejecución en la realización de la implementación en los escenarios propuestos, no solo es la oportunidad de integrar los conocimientos adquiridos en la formación, sino a su vez la forma pedagógica de promover la participación activa en la gesta de soluciones.

La dinámica de integrar cada uno de los pasos propuestos en la realización de una simulación, lleva a que como futuros líderes de proyectos, se coloque a prueba la experticia de acuerdo a las necesidades.

La capacidad de resolución para los problemas que presentan las redes es una necesidad latente en el sector de la tecnología, dada a la amplia demanda que en la actualidad se generaliza, pero que en muchas ocasiones se pormenoriza por falta de capacitación y certificación en la ejecución de los mismos.

Sea esta la oportunidad de consolidar la formación adquirida, los conocimientos y dedicación a la resolución de dichos problemas.

## ABSTRACT

To limit the information provided for the subsequent execution in the implementation of the proposed scenarios, it is not only the opportunity to integrate the knowledge acquired in the training, but also the pedagogical way to promote active participation in the development of solutions.

The dynamics of integrating each one of the proposed steps in the realization of a simulation, leads to the fact that as future project leaders, the expertise is approved according to the needs.

The ability to solve network problems is a latent need in the technology sector, given the wide demand that is currently widespread, but that is often detailed due to lack of training and certification in the execution of the same .

This is the opportunity to consolidate the acquired training, knowledge and dedication to problem solving.

## INTRODUCCIÓN

Planificar la realización de los escenarios sugeridos, consolida la conceptualización general de la formación académica del diplomado de profundización CISCO (diseño e implementación de soluciones integradas LAN / WAN) siendo esta una oportunidad enriquecedora para la postulación de ideales en la resolución de casos problemas usualmente convencionales en el campo de las redes.

La herramienta de simulación packet tracer es ideal en la dinámica propuesta ya que su interfaz amigable en la ejecución de comandos y propuestas diseñadas sujetas a las indicaciones, se complementan de forma tal que la realización de los escenarios complejos sea lúdica e interactiva.

Sin embargo lo anteriormente mencionado no cobraría un fundamento esencial si se carece de conocimientos elementales que van desde la topología de las redes hasta las configuraciones más avanzadas de las mismas, sin dar paso a la duda esta formación va concatenada eslabón tras eslabón pues si desde su fase inicial no se dejan claras las diversas conjeturas que se presenten, pues se caería en una serie de errores que llevados a la práctica en la industria equivaldrían a pérdidas sustanciales de tiempo y dinero.

## 2. OBJETIVOS

### OBJETIVO GENERAL

Caracterizar cada uno de los escenarios propuestos, sujetos a los lineamientos establecidos.

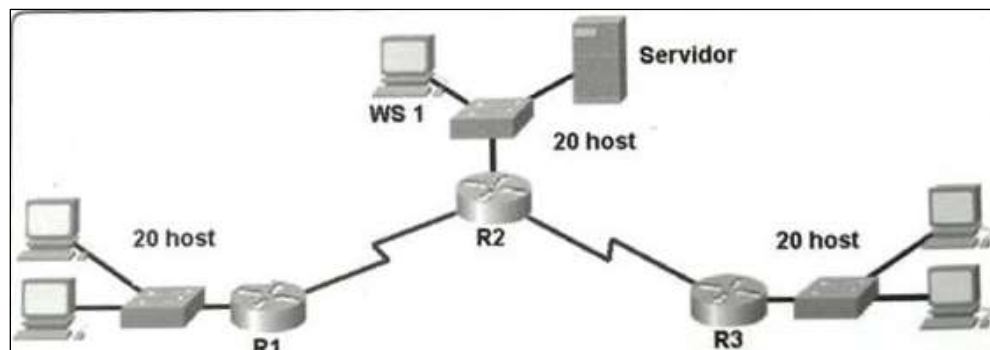
### OBJETIVOS ESPECÍFICOS

- Describir el paso a paso de los escenarios realizados junto a su emulación.
- Diseñar una propuesta gráfica apoyada del programa packet tracer.
- Evidenciar la configuración de los dispositivos en el programa packet tracer.
- Verificar las conexiones de los casos sugeridos.

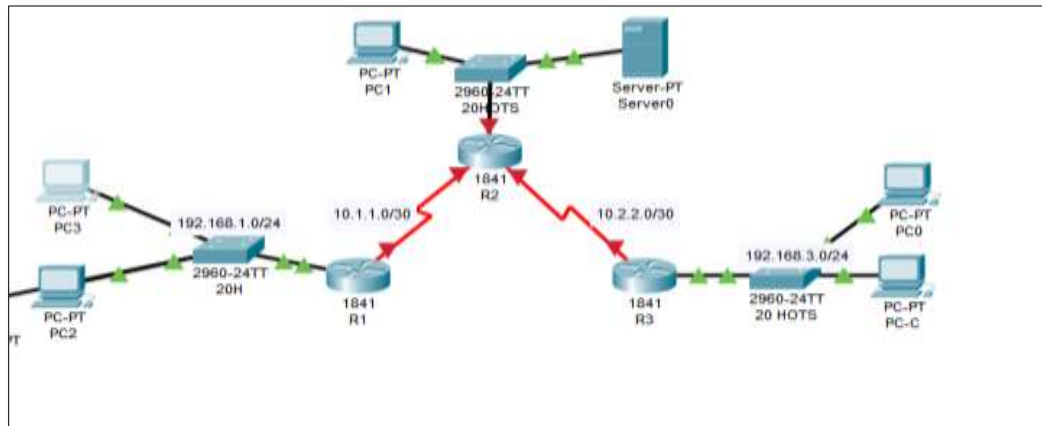
### DESARROLLO DEL PROYECTO

#### Escenario 1

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







Diseño Propuesto Packet Tracer Escenario 1

#### Topología de red

Los requerimientos solicitados son los siguientes:

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

No	Subred	Primera dirección de host	Ultima dirección de host	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

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

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

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

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

**Parte 6: Configuración final.**

## ANÁLISIS DEL DESARROLLO DEL PROYECTO

### Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

El acceso a los enrutadores R1, R2 y R3 solo debe permitirse desde PC-C, la estación de administración. PC-C también se utiliza para realizar pruebas de conectividad a PC-A, un servidor que proporciona servicios DNS, SMTP, FTP y HTTPS.

El procedimiento operativo estándar es aplicar ACL en los enrutadores de borde para mitigar las amenazas comunes en función de la dirección IP de origen y / o de destino. En esta actividad, crea ACL en los enrutadores de borde R1 y R3 para lograr este objetivo. A continuación, verifica la funcionalidad de ACL de los hosts internos y externos. Los enrutadores se han pre configurado con lo siguiente:

Rutina de seguridad ingreso a la programación de los router, clave de ingreso

```
enable secret ciscounad2019
service password-encryption
banner motd "solo acceso autorizado"
line console 0
password classunad2019
login
exit
```

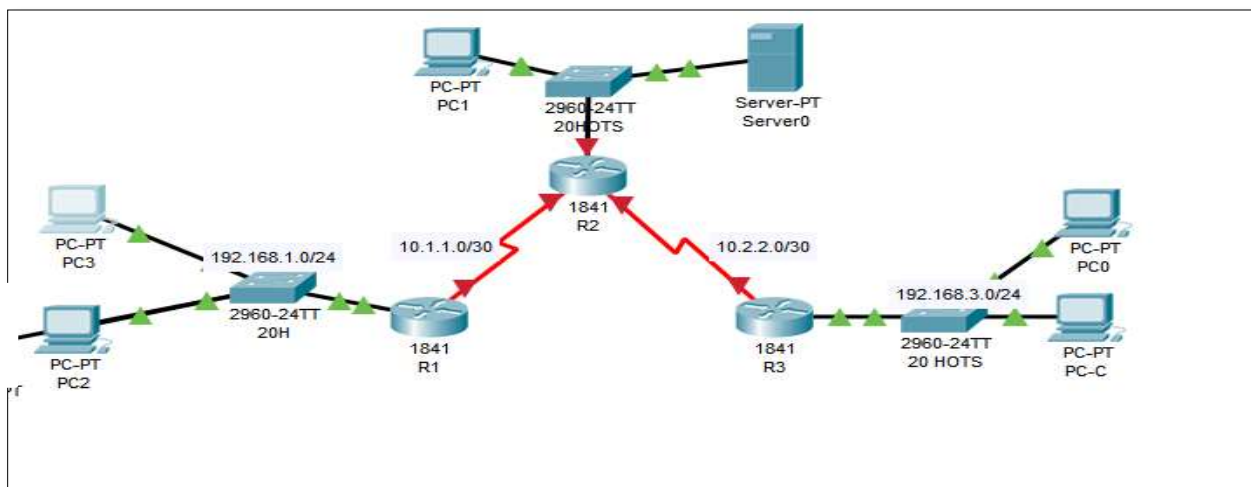
```
line vty 0 15
```

```
password class
```

login

end

Realizar la conexión física de los equipos con base en la topología de red



Parte 1: verificar la conectividad de red básica

Paso 1: desde la PC, verifique la conectividad con PC y R2.

```
Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

SERVER>
```

Pinging Packet tracer

```
SERVER>ssh -l SSHadmin 192.168.2.1
Open
Password:

R2#
```

Paso 2: desde PC verifica la conectividad con PC y R2t.  
 Desde el símbolo del sistema, haga ping a PC-A (192.168.1.3)

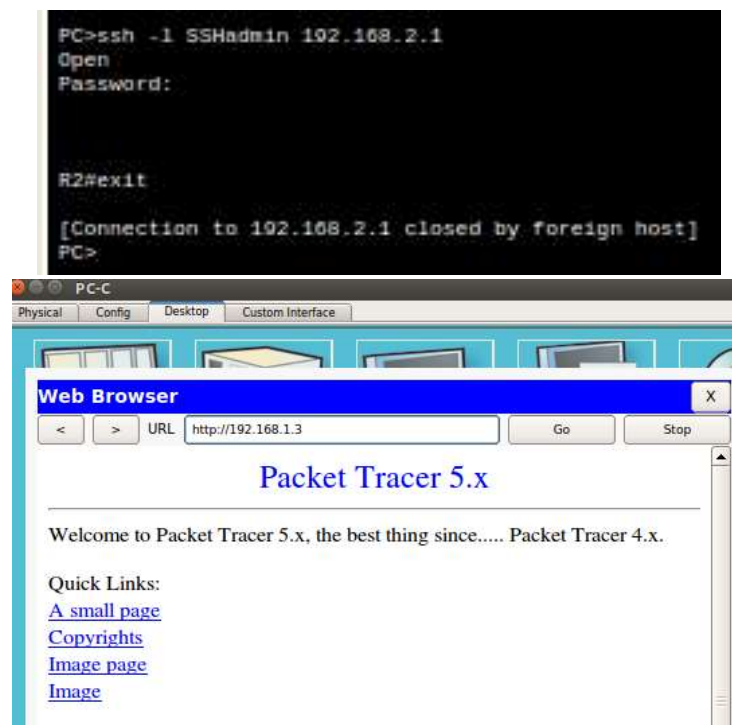
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Desde el símbolo del sistema, establezca una sesión SSH a la interfaz R2 Lo0 (192.168.2.1) utilizando un nombre de usuario SSHadmin y contraseña ciscosshpa55.  
 PC> ssh -l SSHadmin 192.168.2.1



### Acceso seguro a los Routers

Utilice el comando access-list para crear una ACL IP numerada en R1, R2 y R3.  
 R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0 R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0 R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3 0.0.0.0
R1(config)#
```

Lo mismo en R2 y R3

Paso 2: Aplicar ACL 10 al tráfico de entrada en las líneas VTY.

Utilice el comando access-class para aplicar la lista de acceso al tráfico entrante en las líneas VTY.

Con do show run verifico las líneas vty

```
line vty 0 4
password 7 082245508A101303081B0D517F
login local
transport input ssh
```

Ingreso a la configuración de las líneas vty

```
R1(config)#line vty 0 4
R1(config-line)#
```

Aplico el comando para aplicar la lista de acceso

```
R1(config-line)#access-class 10 in
R1(config-line)#
```

Hacemos lo mismo en R2 y R3

R1(config-line)# access-class 10 in R2(config-line)# access-class 10 in R3(config-line)# access-class 10 in

### Verificación del acceso exclusivo desde la estación de administración PC

```
[Connection to 192.168.2.1 closed by foreign host]
PC>ssh -l SSHAdmin 192.168.2.1
Open
Password:
R2#
```

Establezca una sesión SSH a 192.168.2.1

```
[Connection to 192.168.2.1 closed by foreign host]
SERVER>ssh -l SGHAdmin 192.168.2.1
% Connection refused by remote host
SERVER>
```

Configurar la topología de red, de acuerdo con las **Configuraciones básicas de los Routers**

### Router MEDELLIN

```

Router>enable
Router#configure terminal Router(config)#no ip domain-lookup Router(config)#hostname
MEDELLIN MEDELLIN(config)#no ip domain-lookup MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco MEDELLIN(config-line)#login MEDELLIN(config-line)#line
vty 0 15 MEDELLIN(config-line)#password cisco MEDELLIN(config-line)#login MEDELLIN(config-
line)#exit MEDELLIN(config)#enable secret class
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd $Prohibido el acceso a personas no autorizadas $
MEDELLIN(config)#interface Serial0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224 MEDELLIN(config-if)# No
Shutdown
MEDELLIN(config-if)# MEDELLIN(config-if)#exit MEDELLIN(config)#interface Serial0/1/0
MEDELLIN(config-if)#ip address 192.168.1.68 255.255.255.224 MEDELLIN(config-if)# No
Shutdown
MEDELLIN(config-if)# MEDELLIN(config-if)#exit MEDELLIN(config)#interface FA0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224 MEDELLIN(config-if)# No
Shutdown
MEDELLIN(config-if)#

```

### Router BOGOTA

```

Router>enable Router#configure terminal
Router(config)#no ip domain-lookup Router(config)#hostname BOGOTA BOGOTA(config)#no ip
domain-lookup BOGOTA(config)#line console 0 BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 15 BOGOTA(config-line)#password cisco BOGOTA(config-
line)#login BOGOTA(config-line)#exit BOGOTA(config)#enable secret class
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd $Prohibido el acceso a personas no autorizadas $
BOGOTA(config)#interface Serial0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224 BOGOTA(config-if)# No Shutdown
BOGOTA(config-if)# BOGOTA(config-if)#exit
BOGOTA(config)#interface Serial0/1/0 BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224 BOGOTA(config-if)# No Shutdown
BOGOTA(config-if)# BOGOTA(config-if)#exit BOGOTA(config)#interface FA0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224 BOGOTA(config-if)# No Shutdown
BOGOTA(config-if)#

```

### Router CALI

```

Router>enable Router#configure terminal

```

```
Router(config)#no ip domain-lookup Router(config)#hostname CALI CALI(config)#no ip domain-lookup CALI(config)#line console 0 CALI(config-line)#password cisco CALI(config-line)#login
```

```
CALI(config-line)#line vty 0 15 CALI(config-line)#password cisco CALI(config-line)#login
CALI(config-line)#exit CALI(config)#enable secret class
CALI(config)#service password-encryption
CALI(config)#banner motd $Prohibido el acceso a personas no autorizadas $
CALI(config)#interface Serial0/0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224 CALI(config-if)# No Shutdown
CALI(config-if)# CALI(config-if)#exit
CALI(config)#interface Serial0/1/0 CALI(config-if)#clock rate 128000
CALI(config-if)#ip address 192.168.1.34 255.255.255.224
CALI(config-if)# No Shutdown CALI(config-if)#
CALI(config-if)#exit CALI(config)#interface Fa0/0 CALI(config-if)#clock rate 128000
CALI(config-if)#ip address 192.168.1.65 255.255.255.224 CALI(config-if)# No Shutdown
CALI(config-if)#
```

Siguientes especificaciones.

Parte 1: Asignación de direcciones IP:

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

Asignar una dirección IP a la red.

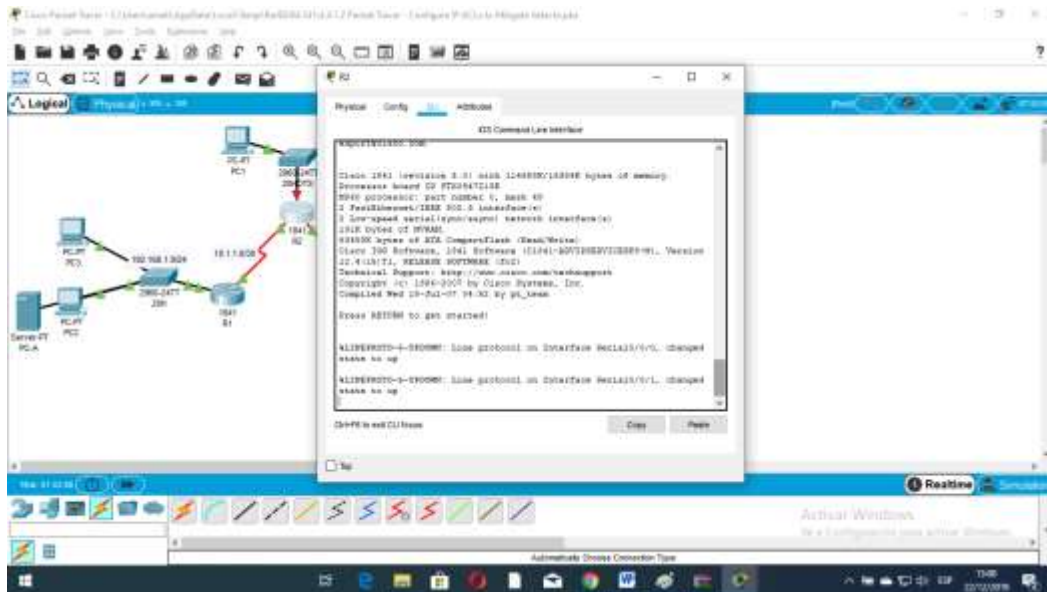
Parte 2: Configuración Básica.

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

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.



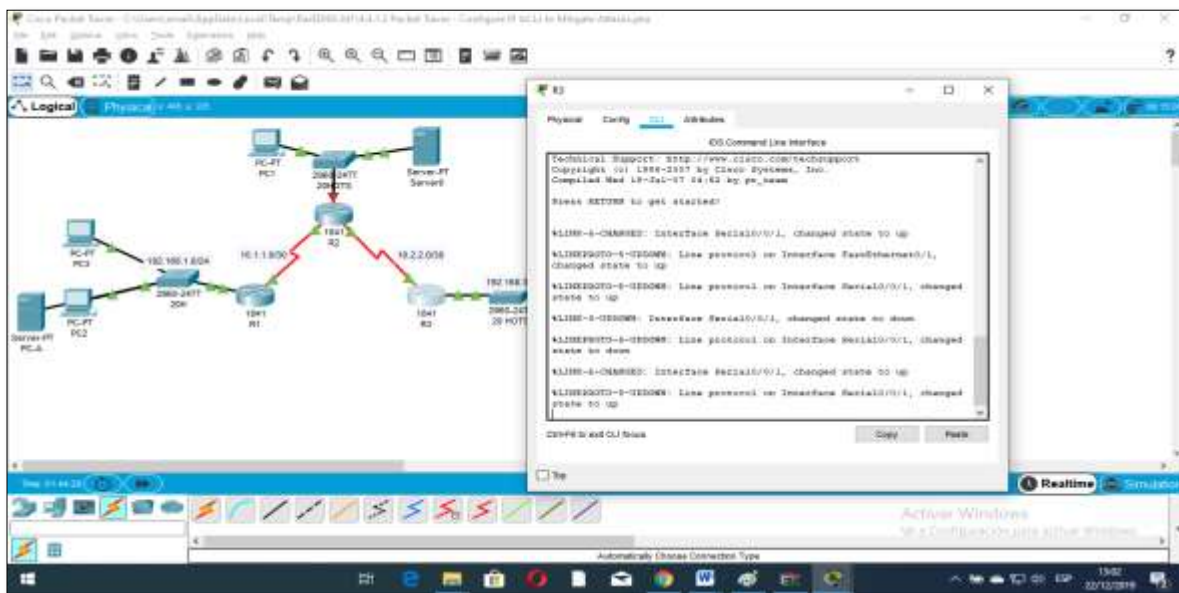




%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

### Tabla de Enrutamiento. Router 3



%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

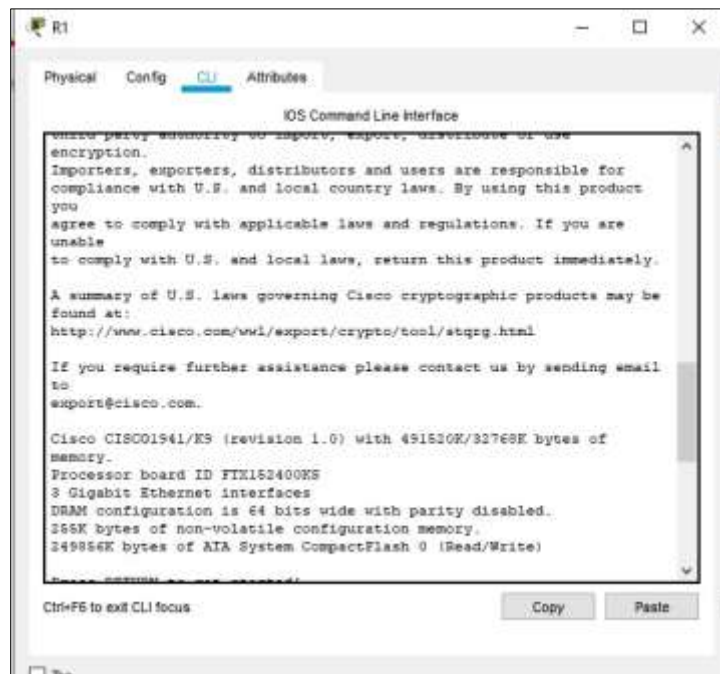
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Verificar el balanceo de carga que presentan los routers.

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

Obsérvese en los routers R1 y R2 cierta similitud.



R1>enable

R1#show ip config

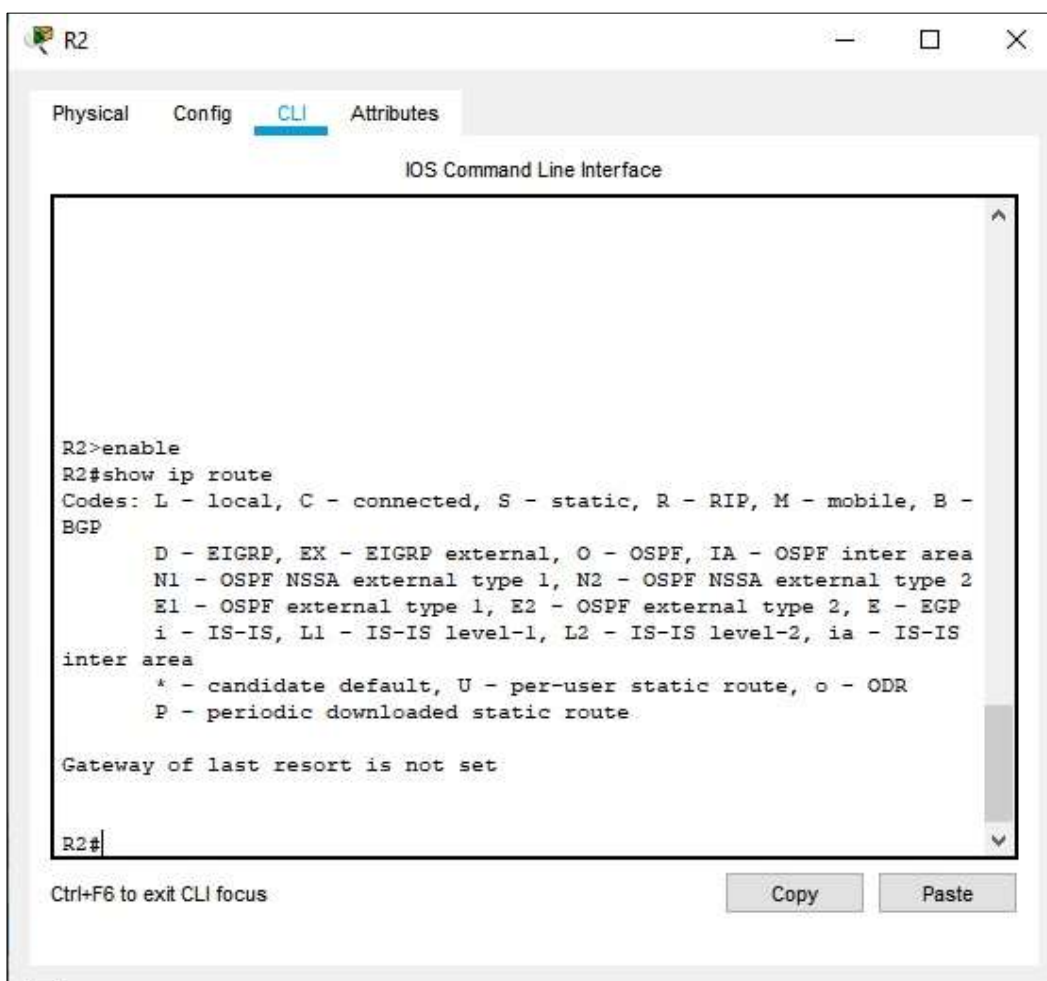
^

% Invalid input detected at '^' marker.

R1#show ip route

Codes: L - local, C - connected, S - static, 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



R2>enable

R2#show ip route

Codes: L - local, C - connected, S - static, 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

R2#

Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

hacemos con la consola de comandos asignando una ip al serial.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interfase serial 0/0/0
      ^
% Invalid input detected at '^' marker.

Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.15.0 255.255.255.0
Bad mask /24 for address 192.168.15.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

Realizar un diagnóstico de vecinos usando el comando cdp.

```

R1
Physical  Config  CLI  Attributes
IOS Command Line Interface

Press RETURN to get started.

R1>enable
R1#show cdp neigh
R1#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
R1#
  
```

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

```

Packet Tracer SERVER Command Line 1.0
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

SERVER>
  
```

### Parte 3: Configuración de Enrutamiento.

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

```

Physical Config CLI
IOS Command Line Interface
#0000-5-#R#CHANGE. IP-SIGNS 1. Neighbor 192.168.10.9 (Serial0/0/1) is up. New ad
jacency
R3 (config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#vr
Building configuration...
[OK]
R3#sh ip ne
R3#sh ip top
R3#sh ip ne
R3#sh ip e
R3#sh ip eigrp ne
R3#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.10.5 Se0/0/0 13 00:01:04 40 1000 0 10
1 192.168.10.9 Se0/0/1 13 00:01:04 40 1000 0 10

R3#sh ip eigrp t
R3#sh ip eigrp to
Copy Paste

```

Show ip eigrp topology: Este comando me indica la topología que voy a tener en la red donde me indica la letra P es el código de la topología a la red que se está dirigiendo tal como P 192.168.1.0/24 al primer AS y su FD es 28160 como se ve en la siguiente imagen:

```

Physical Config CLI
IOS Command Line Interface
R3#sh ip eigrp t
R3#sh ip eigrp to
R3#sh ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       s - Reply status

P 192.168.1.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 216960
   via Connected, Serial0/0/0
P 192.168.10.2/24, 1 successors, FD is 216960
   via Summary (216960/0), Null0
P 192.168.10.8/30, 1 successors, FD is 216960
   via Connected, Serial0/0/1
P 192.16.0.0/16, 2 successors, FD is 2172416
   via 192.168.10.5 (2172416/28160), Serial0/0/0
   via 192.168.10.9 (2172416/28160), Serial0/0/1
P 10.0.0.0/8, 1 successors, FD is 2681920
   via 192.168.10.9 (2681920/216960), Serial0/0/1
R3#
Copy Paste

```

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

	R1	R2	R3
<b>Nombre de Host</b>	MEDELLIN	BOGOTA	CALI
<b>Dirección de Ip en interfaz Serial 0/0</b>	192.168.1.99	192.168.1.98	<b>192.168.1.131</b>
<b>Dirección de Ip en interfaz Serial 0/1</b>	192.168.1.68	192.168.1.130	<b>192.168.1.34</b>
<b>Dirección de Ip en interfaz FA 0/0</b>	192.168.1.33	192.168.1.1	<b>192.168.1.65</b>
<b>Protocolo de enrutamiento</b>	Eigrp	Eigrp	<b>Eigrp</b>
<b>Sistema Autónomo</b>	200	200	<b>200</b>
<b>Afirmaciones de red</b>	<b>192.168.1.0</b>	<b>192.168.1.0</b>	<b>192.168.1.0</b>

Verificar si existe vecindad con los routers configurados con EIGRP.

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

```
BOGOTA#show 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
R       192.168.1.32 [120/1] via 192.168.1.99, 00:00:02, Serial0/0/0
        [120/1] via 192.168.1.131, 00:00:17, Serial0/1/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 03:17:51, Serial0/1/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/1/0
```

Bogota#show ip route

Codes: L - local, C - connected, S - static, 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

192.168.1.0/24 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, 00:59:15, Serial0/1/0

D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:59:14, Serial0/1/1

C 192.168.1.96/27 is directly connected, Serial0/1/0 L 192.168.1.98/32 is directly connected, Serial0/1/0 C 192.168.1.128/27 is directly connected, Serial0/1/1

L 192.168.1.130/32 is directly connected, Serial0/1/1

Medellin#show ip route

Codes: L - local, C - connected, S - static, 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

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks

D 192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:57:09, Serial0/1/0

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, 00:57:08, Serial0/1/0

C 192.168.1.96/27 is directly connected, Serial0/1/0 L 192.168.1.99/32 is directly connected, Serial0/1/0

D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:57:09, Serial0/1/0

Cali#show ip route



Codes: L - local, C - connected, S - static, 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

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks  
 D 192.168.1.0/27 [90/2172416] via 192.168.1.130, 01:00:17, Serial0/1/0 D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 01:00:17, Serial0/1/0  
 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, 01:00:17, Serial0/1/0  
 C 192.168.1.128/27 is directly connected, Serial0/1/0  
 L 192.168.1.131/32 is directly connected, Serial0/1/0

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.

```
MEDELLIN#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 164

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
-----

Device ID: BOGOTA
Entry address(es):
  IP address : 192.168.1.98
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 164

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
```

Medellin>en

Medellin#show ip route 192.168.1.131 Routing entry for 192.168.1.128/27

Known via "eigrp 200", distance 90, metric 2681856, type internal Redistributing via eigrp 200

Last update from 192.168.1.98 on Serial0/1/0, 00:23:15 ago Routing Descriptor Blocks:

\* 192.168.1.98, from 192.168.1.98, 00:23:15 ago, via Serial0/1/0 Route metric is 2681856, traffic share count is 1

Total delay is 40000 microseconds, minimum bandwidth is 1544 Kbit Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 1

Medellin#show ip route 192.168.1.1 Routing entry for 192.168.1.0/27

Known via "eigrp 200", distance 90, metric 2172416, type internal Redistributing via eigrp 200

Last update from 192.168.1.98 on Serial0/1/0, 00:25:32 ago Routing Descriptor Blocks:

\* 192.168.1.98, from 192.168.1.98, 00:25:32 ago, via Serial0/1/0 Route metric is 2172416, traffic share count is 1

Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 1

Cali>en

Cali#show ip route 192.168.1.33 Routing entry for 192.168.1.32/27

Known via "eigrp 200", distance 90, metric 2684416, type internal Redistributing via eigrp 200

Last update from 192.168.1.130 on Serial0/1/0, 00:26:43 ago Routing Descriptor Blocks:

\* 192.168.1.130, from 192.168.1.130, 00:26:43 ago, via Serial0/1/0 Route metric is 2684416, traffic share count is 1

Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 2 Bogota>en

Bogota#show ip route 192.168.1.33 Routing entry for 192.168.1.32/27

Known via "eigrp 200", distance 90, metric 2172416, type internal Redistributing via eigrp 200

Last update from 192.168.1.99 on Serial0/1/0, 00:27:29 ago Routing Descriptor Blocks:

\* 192.168.1.99, from 192.168.1.99, 00:27:29 ago, via Serial0/1/0 Route metric is 2172416, traffic share count is 1

Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 1

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

Medellin>en Medellin#config t

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

```
Medellin(config)#line vty 0 Medellin(config-line)#pass cisco Medellin(config-line)#login
Medellin(config-line)#service password-encryption Medellin(config)#end
```

Bogota>en Bogota#config t

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

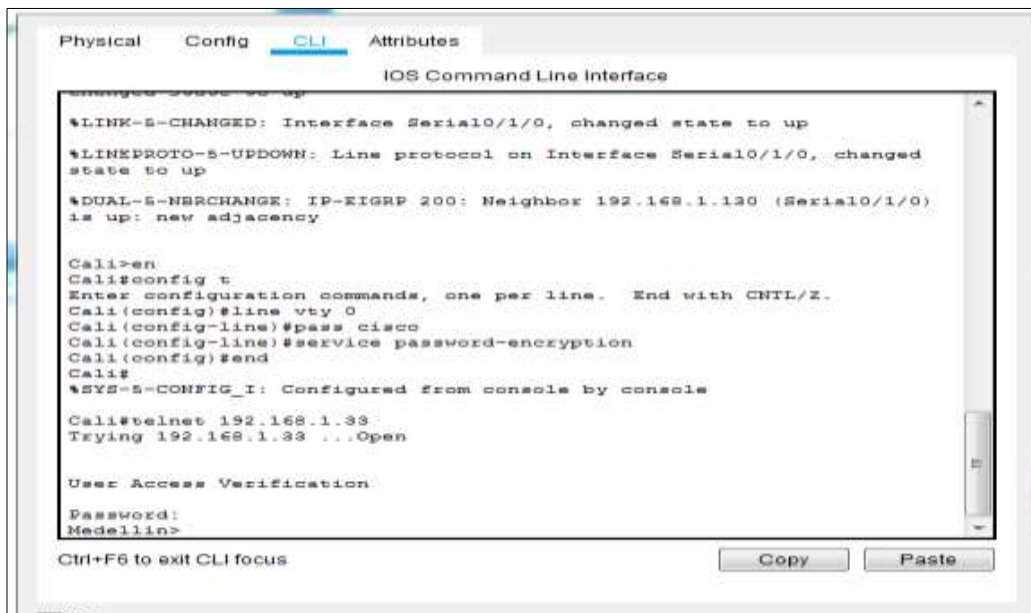
```
Bogota(config)#line vty 0 Bogota(config-line)#pass cisco
Bogota(config-line)#service password-encryption Bogota(config)#wr
```

Cali>en Cali#config t

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

```
Cali(config)#line vty 0 Cali(config-line)#pass cisco
Cali(config-line)#service password-encryption Cali(config)#end.
```

Ingreso desde Router Cali a router Medellín y Bogotá a través de Telnet



The screenshot shows a Cisco IOS CLI window with tabs for Physical, Config, CLI (selected), and Attributes. The terminal output is as follows:

```

Cali#config t
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#line vty 0
Cali(config-line)#pass cisco
Cali(config-line)#service password-encryption
Cali(config)#end
Cali#
%SYS-5-CONFIG_I: Configured from console by console

Cali#telnet 192.168.1.33
Trying 192.168.1.33 ...Open

User Access Verification

Password:
Medellin>exit

[Connection to 192.168.1.33 closed by foreign host]
Cali#
Cali#telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

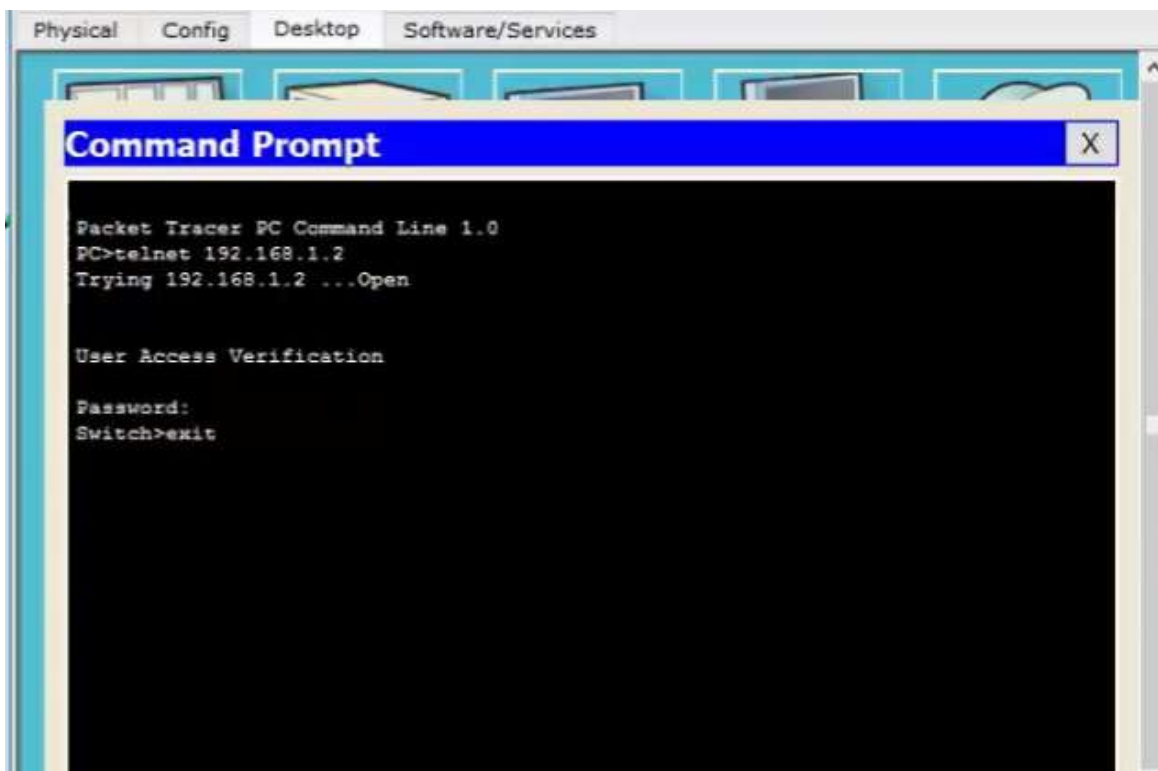
Password:
Bogota>
  
```

At the bottom of the window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

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:

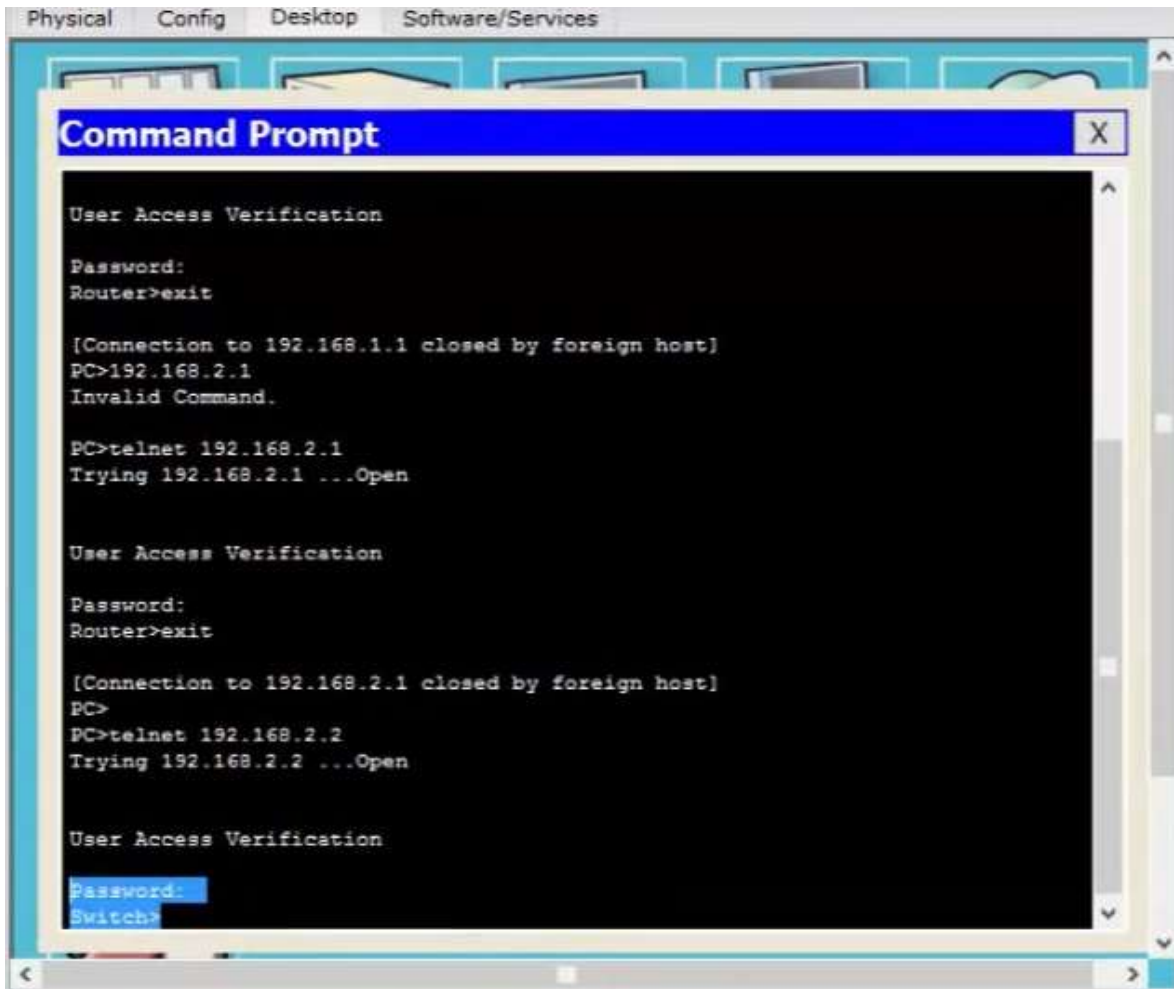
Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.



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.



```
Physical  Config  Desktop  Software/Services

Command Prompt

User Access Verification

Password:
Router>exit

[Connection to 192.168.1.1 closed by foreign host]
PC>192.168.2.1
Invalid Command.

PC>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification

Password:
Router>exit

[Connection to 192.168.2.1 closed by foreign host]
PC>
PC>telnet 192.168.2.2
Trying 192.168.2.2 ...Open

User Access Verification

Password:
Switch>
```

### Comprobación de la red instalada.

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

Physical Config **CLI** Attributes

IOS Command Line Interface

```

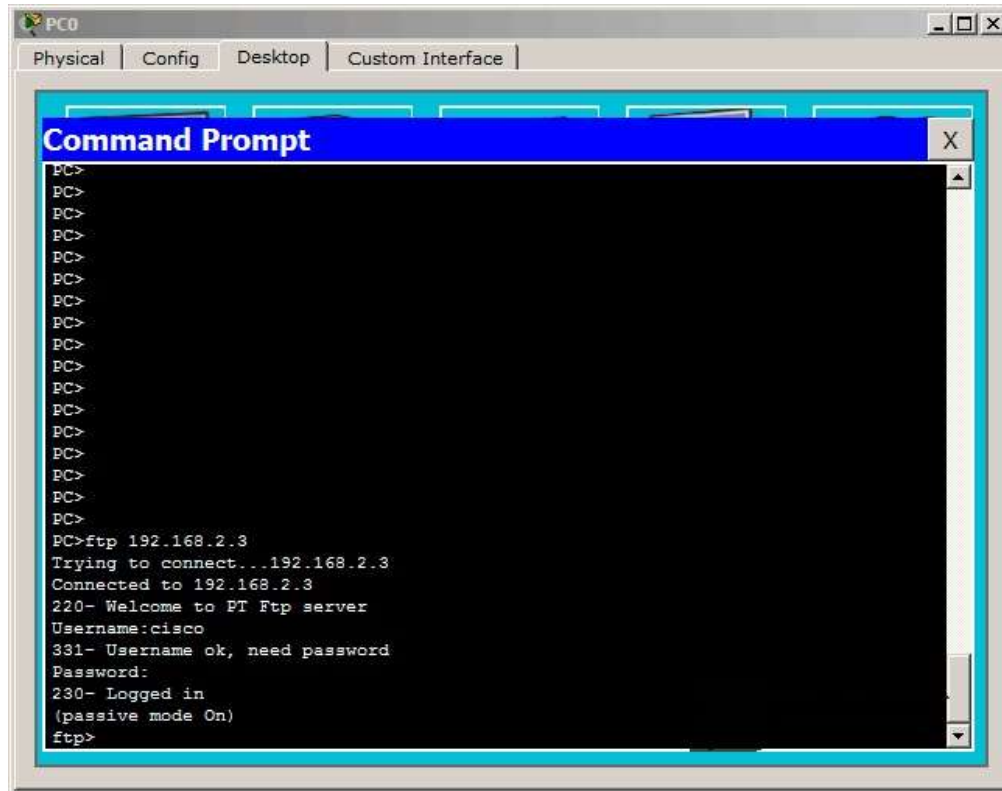
Press RETURN to get started:

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#router rip
R1(config-router)#access-list 1 permit 192.168.0.0
  
```

Ctrl+F6 to exit CLI focus

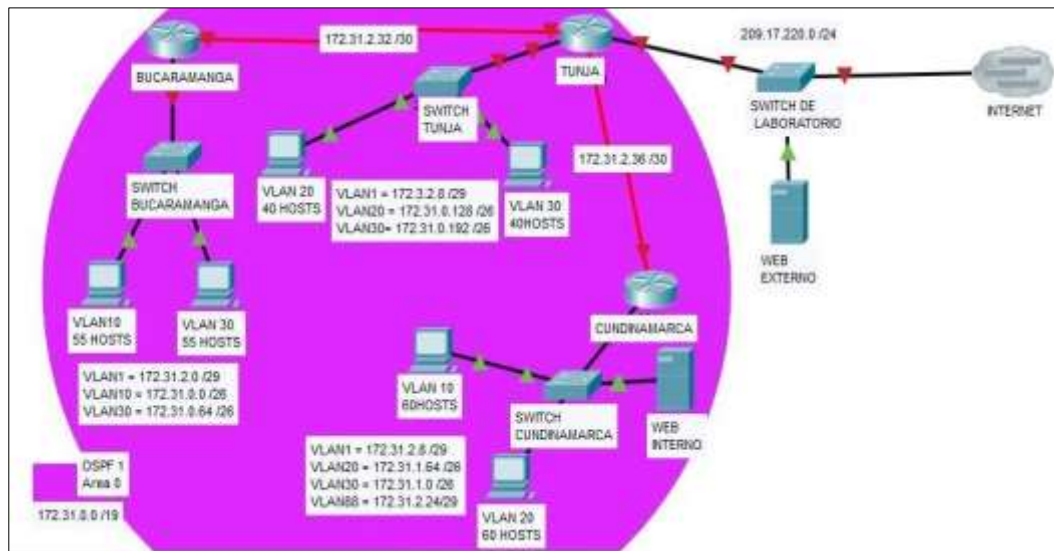
Copy Paste





## 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.



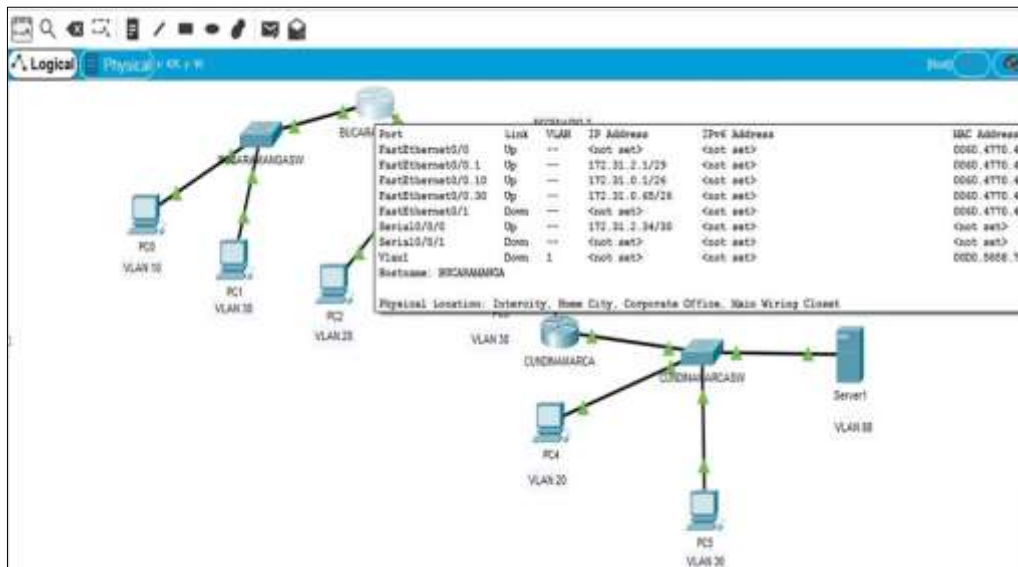
Diseño Grafico Packet Tracer Escenario 2

Los siguientes son los requerimientos necesarios:

Punto 1 Todos los routers deberán tener los siguientes:

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

Se realiza la configuración básica para cada router dándole un nombre a los routers con el comando hostname y sus respectivas contraseñas.



### Configuración inicial Router:

Bucaramanga

```

Router>enable Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA BUCARAMANGA(config)#enable
password cisco2019
BUCARAMANGA(config)#enable password cisco2019
BUCARAMANGA(config)#service password-encryption BUCARAMANGA(config)#login
block-for 150 attempts 3 within 20 BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login R1 local enable
    
```

```

BUCARAMANGA(config)#username          NOMBRE0          secret          R2
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#login authentication RED1 BUCARAMANGA(config-
line)#logging synchronous BUCARAMANGA(config-line)#exe-timeout 11

```

^

```
% Invalid input detected at '^' marker. BUCARAMANGA(config-line)#exec-timeout 11
```

```

BUCARAMANGA(config-line)#line vty 0 15 BUCARAMANGA(config-line)#login
authentication RED1 BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#exec-timeout 5 BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#interface s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shutdown

```

```

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BUCARAMANGA(config-if)#interface g0/1.1 BUCARAMANGA(config-
subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#interface g0/1.10 BUCARAMANGA(config-
subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#interface g0/1.30 BUCARAMANGA(config-
subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#interface g0/1
BUCARAMANGA(config-if)#no shutdown

```

```
BUCARAMANGA(config-if)#
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed
state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up
```

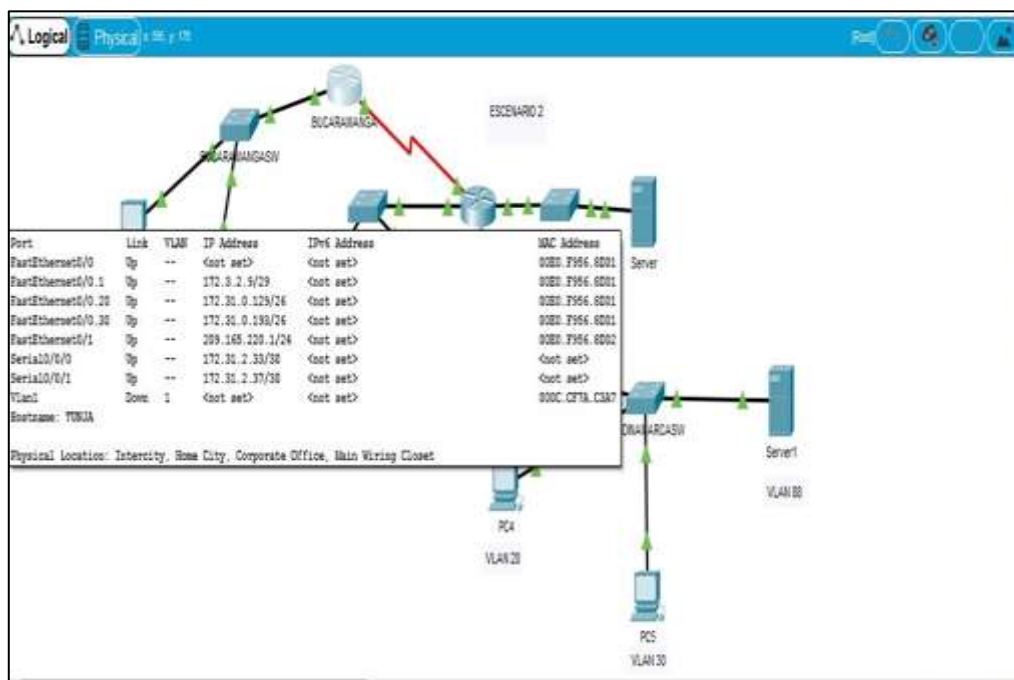
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed
state to up
```

%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed state to up

BUCARAMANGA(config-if)#end BUCARAMANGA#

%SYS-5-CONFIG\_I: Configured from console by console



Estructura Grafica

Tunja

Router>enable Router#conf t

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

Router(config)#hostname TUNJA

TUNJA(config)#enable password SISTEMAS1 TUNJA(config)#service password-encryption TUNJA(config)#login block-for 150 attempts 3 within 20 TUNJA(config)#aaa new-model

TUNJA(config)#aaa authentication login GERENCIA1 local enable

TUNJA(config)#username NOMBRE13 secret ADMIN2 TUNJA(config)#line con 0

TUNJA(config-line)#login authentication GERENCIA1 TUNJA(config-line)#logging synchronous TUNJA(config-line)#exec-timeout 11

TUNJA(config-line)#line vty 0 15

```
TUNJA(config-line)#login authentication GERENCIA1 TUNJA(config-line)#logging
synchronous TUNJA(config-line)#exec-timeout 5
TUNJA(config-line)#exit TUNJA(config)#interface s0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#clock rate 1000000 TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
TUNJA(config-if)#interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
TUNJA(config-if)#interface s0/0/1
```

```
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252 TUNJA(config-if)#no
shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down TUNJA(config-
if)#interface g0/0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0 TUNJA(config-if)#no
shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up
TUNJA(config-if)#interface g0/1.1 TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192 TUNJA(config-
subif)#interface g0/1.30
```

```
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192 TUNJA(config-
subif)#interface g0/1
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed
state to up
TUNJA(config-if)#end TUNJA#
%SYS-5-CONFIG_I: Configured from console by console TUNJA#
```

## Cundinamarca

```
Router>enable Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA CUNDINAMARCA(config)#enable
password CISCO321 CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#login block-for 150 attempts 3 within 20
CUNDINAMARCA(config)#aaa new-model CUNDINAMARCA(config)#aaa
authentication login CISCO50 local enable CUNDINAMARCA(config)#username
EQUI60 secret ADD55 CUNDINAMARCA(config)#line con 0
```

```
CUNDINAMARCA(config-line)#login authentication CISCO5 CUNDINAMARCA(config-
line)#logging synchronous CUNDINAMARCA(config-line)#exec-timeout 11
CUNDINAMARCA(config-line)#line vty 0 15 CUNDINAMARCA(config-line)#login
authentication CISCO5 CUNDINAMARCA(config-line)#logging
```

```
synchronous CUNDINAMARCA(config-line)#exec-timeout 5 CUNDINAMARCA(config-
line)#exit CUNDINAMARCA(config)#interface s0/0/1
%Invalid interface type and number CUNDINAMARCA(config)#interface s0/0/1
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#clock rate 1000000 CUNDINAMARCA(config-if)#no
shutdown
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
CUNDINAMARCA(config-if)#interface s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
CUNDINAMARCA(config-if)#interface s0/0/1 CUNDINAMARCA(config-if)#interface
g0/1.1 CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172..31.2.9 255.255.255.248
^
```

```
% Invalid input detected at '^' marker.
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#interface g0/1.20 CUNDINAMARCA(config-
subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#interface g0/1.30 CUNDINAMARCA(config-
subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#interface g0/1.88 CUNDINAMARCA(config-
subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#interface g0/1
CUNDINAMARCA(config-if)#no shutdown
```

```

CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.88, changed
state to up
CUNDINAMARCA(config-if)#end CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console CUNDINAMARCA#

```

### Se configuran las VLAN para cada Switch:

Se configuran las VLAN para cada switch con su respectivo número de la VLAN que se desea configurar con el comando config-vlan. También se le da un nombre a la VLAN con el comando name, estos pasos se registraron en los siguientes:

Bucaramanga

```

Switch>enable Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#vlan1
^
% Invalid input detected at '^' marker. Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed. Switch(config-vlan)#vlan 10
Switch(config-vlan)#name VLAN10 Switch(config-vlan)#vlan 30 Switch(config-
vlan)#name VLAN30 Switch(config-vlan)#exit Switch(config)#int VLAN1
Switch(config-if)#ip address 172.31.2.2 255.255.255.248 Switch(config-if)#no shutdown

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

```

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#int VLAN10 Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
Switch(config-if)#ip address 172.31.0.66 255.255.255.192 Switch(config-if)#no
shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#copy run start
Destination filename [startup-config]?

```

Tunja

```

Switch>enable Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed. Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20 Switch(config-vlan)#vlan 30 Switch(config-
vlan)#name VLAN30 Switch(config-vlan)#exit Switch(config)#int VLAN1
Switch(config-if)#ip address 172.3.2.10 255.255.255.248 Switch(config-if)#no shutdown
Switch(config-if)#int VLAN20
Switch(config-if)#ip address 172.31.0.130 255.255.255.192 Switch(config-if)#no
shutdown
Switch(config-if)#int VLAN30

Switch(config-if)#ip address 172.31.0.194 255.255.255.192 Switch(config-if)#no
shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20 Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#copy run start
Destination filename [startup-config]?

```



Cundinamarca

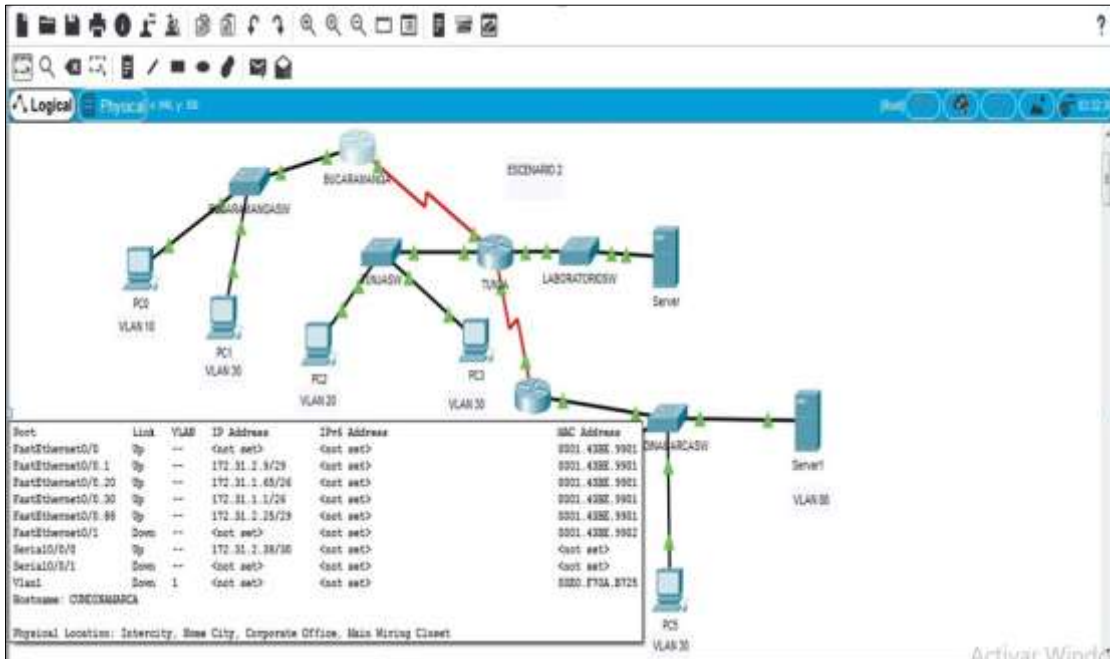
```

Switch>enable Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed. Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20 Switch(config-vlan)#vlan 30 Switch(config-
vlan)#name VLAN30 Switch(config-vlan)#vlan 88 Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit Switch(config)#int VLAN1
Switch(config-if)#ip address 172.31.2.10 255.255.255.248 Switch(config-if)#no
shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#int VLAN20 Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip address 172.31.1.66 255.255.255.192 Switch(config-if)#no
shutdown

Switch(config-if)#int VLAN30 Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
Switch(config-if)#ip address 172.31.1.2 255.255.255.192 Switch(config-if)#no shutdown
Switch(config-if)#int VLAN88 Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up
Switch(config-if)#ip address 172.31.2.26 255.255.255.248 Switch(config-if)#no
shutdown
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 20
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
Switch(config-if)#int f0/2
Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 30
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
Switch(config-if)#end Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#copy run start
Destination filename [startup-config]?

```



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

Se configuran los routers con el comando DHCP dándole la asignación de direcciones IP.

### DHCP en cada router:

Tunja

TUNJA>enable Password:

Password:

TUNJA#conf t

Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip dhcp excluded-address 172.31.2.1 172.31.2.2

TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.2

TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.66

TUNJA(config)#ip dhcp excluded-address 172.31.2.9 172.31.2.10

TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.66

TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.2

TUNJA(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.26 TUNJA(config)#ip dhcp excluded-address

172.31.2.11 TUNJA(config)#ip dhcp pool BucaramangaV1

```

TUNJA(dhcp-config)#network 172.31.2.0 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.1 TUNJA(dhcp-config)#ip dhcp pool
BucaramangaV10 TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1 TUNJA(dhcp-config)#ip dhcp pool
BucaramangaV30 TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65 TUNJA(dhcp-config)#ip dhcp pool
CundinamarcaV1 TUNJA(dhcp-config)#network 172.31.2.8 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.9 TUNJA(dhcp-config)#ip dhcp pool
CundinamarcaV20 TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65 TUNJA(dhcp-config)#ip dhcp pool
CundinamarcaV30 TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1 TUNJA(dhcp-config)#ip dhcp pool
CundinamarcaV88 TUNJA(dhcp-config)#network 172.31.2.24 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.25 TUNJA(dhcp-config)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy run start
Destination filename [startup-config]?

```

Bucaramanga

```

BUCARAMANGA>enable Password:
Password:
BUCARAMANGA#conf t

```

```

Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int g0/1.1
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.10

```

```

BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.30 BUCARAMANGA(config-subif)#ip helper-
address 172.31.2.34
BUCARAMANGA(config-subif)#end BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

```

```

BUCARAMANGA#copy run start Destination filename [startup-config]?

```

Cundinamarca

```

CUNDINAMARCA>enable Password:
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/1.1
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.20 CUNDINAMARCA(config-subif)#ip helper-
address 172.31.2.37 CUNDINAMARCA(config-subif)#int g0/1.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.88 CUNDINAMARCA(config-subif)#ip helper-
address 172.31.2.37 CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#copy run start Destination filename [startup-config]?

```

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

Se realiza la configuración con el comando NAT estático el cual se mapea una dirección IP privada con una publica de forma estática, para esto se realiza con el comando ip nat inside source static.

```

TUNJA>enable Password:
Password:
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip nat
inside source static 172.31.2.11 209.17.220
TUNJA(config)#ip access-list standart COLOMBIA
^

```

```

% Invalid input detected at '^' marker. TUNJA(config)#ip access-list standard
COLOMBIA TUNJA(config-std-nacl)#permit 172.31.0.0 0.0.255.255 TUNJA(config-std-
nacl)#exit
TUNJA(config)#ip nat inside source list COLOMBIA interface g0/0 overload
TUNJA(config)#int g0/0
TUNJA(config-if)#ip nat outside TUNJA(config-if)#int s0/0/0 TUNJA(config-if)#ip nat
inside TUNJA(config-if)#int s0/0/1 TUNJA(config-if)#ip nat inside TUNJA(config-if)#int
g0/1.1 TUNJA(config-subif)#ip nat inside TUNJA(config-subif)#int g0/1.20
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up

```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed
state to up
```

```
TUNJA(config-subif)#ip nat inside TUNJA(config-subif)#int g0/1.30 TUNJA(config-
subif)#ip nat inside TUNJA(config-subif)#end TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
TUNJA#copy run start
Destination filename [startup-config]?
```

Configuración de ruta estática predeterminada:

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip route
0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate TUNJA(config-router)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy run start
Destination filename [startup-config]? Building configuration...
[OK]
```

Punto 4. El enrutamiento deberá tener autenticación.

A continuación se realiza el enrutamiento a cada router.

Bucaramanga

```
BUCARAMANGA>enable Password:
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 100
BUCARAMANGA(config-router)#router-id 1.1.1.1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.0.1 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#passive-interface g0/1 BUCARAMANGA(config-
router)#area 0 authentication BUCARAMANGA(config-router)#exit
```

```

BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication-key osinterpf
%OSPF: Warning: The password/key will be truncated to 8 characters
BUCARAMANGA(config-if)#copy run start
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config-if)#no ip ospf authentication-key osinterpf
BUCARAMANGA(config-if)#ip ospf authentication-key ACOSPF
BUCARAMANGA(config-if)#copy run start
^
% Invalid input detected at '^' marker. BUCARAMANGA(config-if)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy run start Destination filename [startup-config]? Building
configuration...
[OK]

```

Tunja

```

TUNJA>enable Password: TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#router
ospf 100
TUNJA(config-router)#router - id 2.2.2.2
^
% Invalid input detected at '^' marker. TUNJA(config-router)#router-id 2.2.2.2
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0 TUNJA(config-
router)#passive-interface g0/1

```

```

TUNJA(config-router)#area 0 authentication TUNJA(config-router)#exit
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication-key ACOSPF TUNJA(config-if)#
06:53:23: %OSPF-5-ADJCHG: Process 100, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done

```

```

TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip ospf authentication-key ACOSPF TUNJA(config-if)#copy run start
^
% Invalid input detected at '^' marker. TUNJA(config-if)#end
TUNJA#

```

%SYS-5-CONFIG\_I: Configured from console by console

```
TUNJA#copy run start
Destination filename [startup-config]? Building configuration...
[OK]
```

CUNDINAMARCA

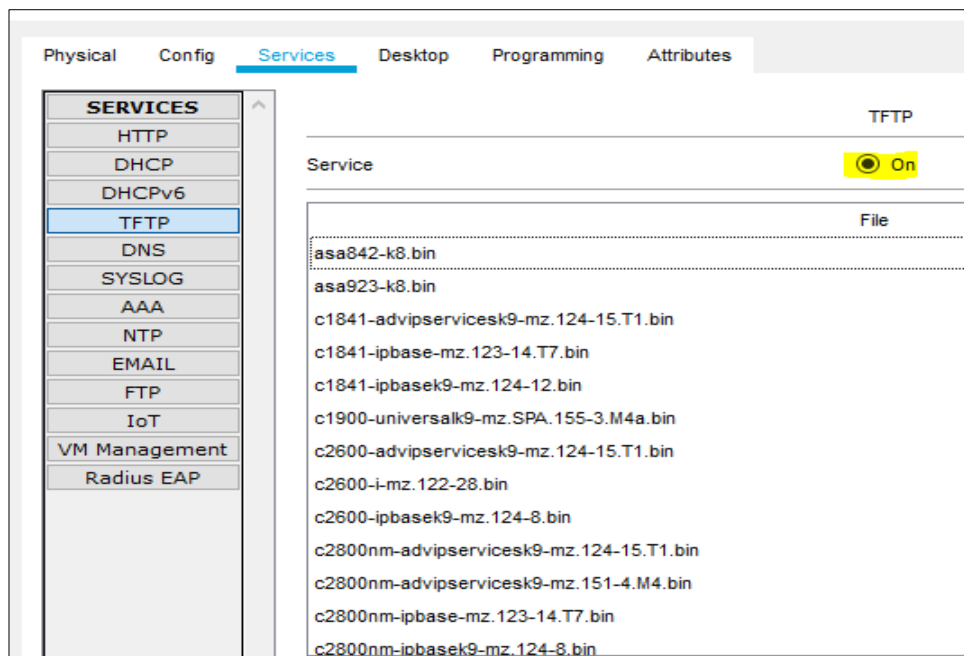
```
CUNDINAMARCA>enable Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 100
CUNDINAMARCA(config-router)#router-id 3.3.3.3
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#passive-interface g0/1 CUNDINAMARCA(config-
router)#area 0 authentication CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication-key ACOSPF
CUNDINAMARCA(config-if)#copy run start
^
% Invalid input detected at '^' marker. CUNDINAMARCA(config-if)#end
CUNDINAMARCA#
```

%SYS-5-CONFIG\_I: Configured from console by console

```
CUNDINAMARCA#copy run start Destination filename [startup-config]? Building
configuration...
```

[OK]

**Establezca un servidor TFTP** y almacene todos los archivos necesarios de los routers.



**Listas de control de acceso:**

A continuación se parametrizan los accesos  
 Para esto se realiza con el comando ip access-list extended.

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

```

Username: NOMBRE6 Password:
CUNDINAMARCA>enable Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV30 CUNDINAMARCA(config-
ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.128
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.192
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#exit CUNDINAMARCA(config)#int g0/1.30
CUNDINAMARCA(config-subif)#ip access-group LANCV30 in
CUNDINAMARCA(config-subif)#end
    
```



```
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV20 CUNDINAMARCA(config-
ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.128
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.192
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#permit ip any any CUNDINAMARCA(config-ext-
nacl)#exit CUNDINAMARCA(config)#int g0/1.20 CUNDINAMARCA(config-subif)#ip
access-group LANCV20 in CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
TUNJA>enable Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip
access-list extended LANTV30
TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq
ftp
TUNJA(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq
www
TUNJA(config-ext-nacl)#exit

TUNJA(config)#int g0/1.30
TUNJA(config-subif)#ip access-group LANTV30 in TUNJA(config-subif)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip access-
list extended LANTV20
TUNJA(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
TUNJA(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config-ext-nacl)#exit
TUNJA(config)#int g0/1.20
TUNJA(config-subif)#ip access-group LANTV20 in TUNJA(config-subif)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

```

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

```

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV30 BUCARAMANGA(config-ext-
nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.16
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.128
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.192
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.8
0.0.0.7
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.64
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.0
0.0.0.63
BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.24
0.0.0.7
BUCARAMANGA(config-ext-nacl)#permit ip any any BUCARAMANGA(config-ext-
nacl)#exit BUCARAMANGA(config)#int g0/1.30 BUCARAMANGA(config-subif)#ip access-
group LANBV30
% Incomplete command.
BUCARAMANGA(config-subif)#ip access-group LABV30 in
BUCARAMANGA(config-subif)#end

```

```
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
BUCARAMANGA#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV10 BUCARAMANGA(config-ext-
nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.1.0
0.0.0.63
BUCARAMANGA(config-ext-nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.0.128
0.0.0.63
BUCARAMANGA(config-ext-nacl)#exit BUCARAMANGA(config)#int g0/1.10
BUCARAMANGA(config-subif)#ip access-group LANBV10 in BUCARAMANGA(config-
subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
CUNDINAMARCA>enable
```

```
Password:
```

```
CUNDINAMARCA#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV20 CUNDINAMARCA(config-
ext-nacl)#no permit ip any any CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64
0.0.0.63 172.31.2.8
0.0.0.7
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.1.0
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.24
0.0.0.7
CUNDINAMARCA(config-ext-nacl)#permit ip any any CUNDINAMARCA(config-ext-
nacl)#end CUNDINAMARCA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
CUNDINAMARCA#show access-list 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 LANCV30
10 permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7
20 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
30 permit ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63

```

```

Extended IP access list LANCV20
10 deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
20 deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
30 deny ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
40 deny ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7
50 deny ip 172.31.1.64 0.0.0.63 172.31.1.0 0.0.0.63
60 deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
70 permit ip any any

```

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

```

Username: NOMBRE0 Password:
BUCARAMANGA>enable Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip access-list extended LANBV30 BUCARAMANGA(config-ext-nacl)#no permit ip any any BUCARAMANGA(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
BUCARAMANGA(config-ext-nacl)#permit ip any any BUCARAMANGA(config-ext-nacl)#end BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

```

```

BUCARAMANGA#show access-list 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 LANBV30
10 deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
20 deny ip 172.31.0.64 0.0.0.63 172.31.2.16 0.0.0.7
30 deny ip 172.31.0.64 0.0.0.63 172.31.0.128 0.0.0.63
40 deny ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63
50 deny ip 172.31.0.64 0.0.0.63 172.31.2.8 0.0.0.7
60 deny ip 172.31.0.64 0.0.0.63 172.31.1.64 0.0.0.63
70 deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
80 deny ip 172.31.0.64 0.0.0.63 172.31.2.24 0.0.0.7
90 permit ip any any

```

Extended IP access list LANBV10

```
10 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
```

```
20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 BUCARAMANGA#
```

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

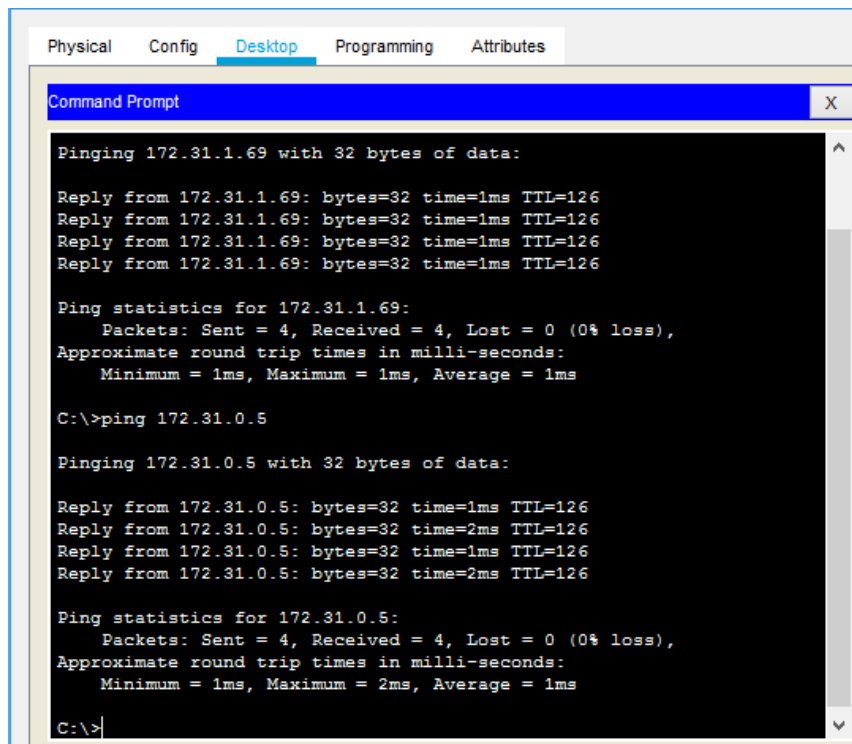
```
TUNJA(config-subif)#access-list 152 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
```

```
TUNJA(config)#access-list 152 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
```

```
TUNJA(config)#int g0/0.20
```

```
TUNJA(config-subif)#ip access-group 152 in
```

```
TUNJA(config-subif)#
```



```

Physical  Config  Desktop  Programming  Attributes
Command Prompt
Approximate round trip times in milliseconds:
  Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>ping 172.31.0.69

Pinging 172.31.0.69 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 172.31.0.69:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.1.5

Pinging 172.31.1.5 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 172.31.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

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

```
BUCARAMANGA(config)#access-list 151 permit ip 172.31.0.64 0.0.0.63
209.165.220.0 0.0.0.255
```

```
BUCARAMANGA(config)#int g0/0.30 BUCARAMANGA(config-subif)#ip access-group 151
in BUCARAMANGA(config-subif)#
```

```

Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 209.165.220.5

Pinging 209.165.220.5 with 32 bytes of data:

Reply from 209.165.220.5: bytes=32 time=2ms TTL=126
Reply from 209.165.220.5: bytes=32 time=11ms TTL=126
Reply from 209.165.220.5: bytes=32 time=11ms TTL=126
Reply from 209.165.220.5: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>ping 172.31.0.131

Pinging 172.31.0.131 with 32 bytes of data:

Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.

Ping statistics for 172.31.0.131:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

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

```
BUCARAMANGA(config-subif)#access-list 152 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
```

```
BUCARAMANGA(config)#
```

```
BUCARAMANGA(config)#access-list 152 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
```

```
BUCARAMANGA(config)#int g0/0.10 BUCARAMANGA(config-subif)#ip access-group 152
in BUCARAMANGA(config-subif)#
```

```

Physical  Config  Desktop  Programming  Attributes
Command Prompt
Pinging 172.31.1.69 with 32 bytes of data:

Reply from 172.31.1.69: bytes=32 time=3ms TTL=125
Reply from 172.31.1.69: bytes=32 time=5ms TTL=125
Reply from 172.31.1.69: bytes=32 time=3ms TTL=125
Reply from 172.31.1.69: bytes=32 time=5ms TTL=125

Ping statistics for 172.31.1.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\>ping 172.31.0.131

Pinging 172.31.0.131 with 32 bytes of data:

Reply from 172.31.0.131: bytes=32 time=2ms TTL=126
Reply from 172.31.0.131: bytes=32 time=11ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>

```

```

Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 172.31.0.131

Pinging 172.31.0.131 with 32 bytes of data:

Reply from 172.31.0.131: bytes=32 time=2ms TTL=126
Reply from 172.31.0.131: bytes=32 time=11ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>ping 209.165.220.5

Pinging 209.165.220.5 with 32 bytes of data:

Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 209.165.220.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```



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

```
BUCARAMANGA(config-subif)#access-list 153 deny ip 172.31.2.0 0.0.0.7
172.31.0.0 0.0.0.63
```

```
BUCARAMANGA(config)#access-list 153 deny ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
```

```
BUCARAMANGA(config)#access-list 153 permit ip any any BUCARAMANGA(config)#int
g0/0.10 BUCARAMANGA(config-subif)#ip access-group 153 out BUCARAMANGA(config-
subif)#
```

```
TUNJA#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#access-list
153 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
```

```
TUNJA(config)#access-list 153 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
```

```
TUNJA(config)#access-list 153 permit ip any any
```

```
TUNJA(config)#int g0/0.20
```

```
TUNJA(config-subif)#ip access-group 153 out TUNJA(config-subif)#
```

```
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.8 0.0.0.7 172.31.1.64
0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.1.0 0.0.0.63 172.31.1.64
0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.24 0.0.0.7 172.31.1.64
0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 153 permit ip any any CUNDINAMARCA(config)#int
g0/0.20 CUNDINAMARCA(config-subif)#ip access-group 153 out
CUNDINAMARCA(config-subif)#
```

```
Physical Config Desktop Programming Attributes
Command Prompt X
Pinging 172.31.0.131 with 32 bytes of data:
Reply from 172.31.0.131: bytes=32 time=2ms TTL=126
Reply from 172.31.0.131: bytes=32 time=11ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>ping 209.165.220.5

Pinging 209.165.220.5 with 32 bytes of data:

Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 209.165.220.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Physical Config Desktop Programming Attributes
Command Prompt X
Pinging 172.31.1.5 with 32 bytes of data:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.1.5

Pinging 172.31.1.5 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 172.31.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

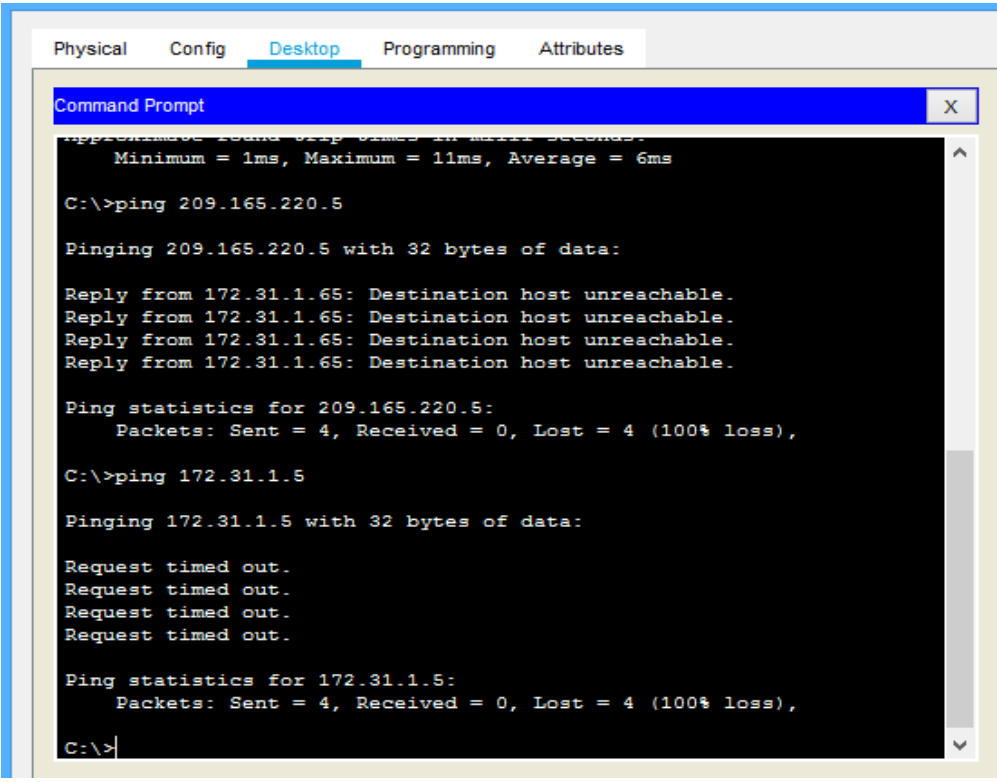
C:\>ping 172.31.0.195

Pinging 172.31.0.195 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 172.31.0.195:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



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

```

BUCARAMANGA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#access-class 9 in
  
```

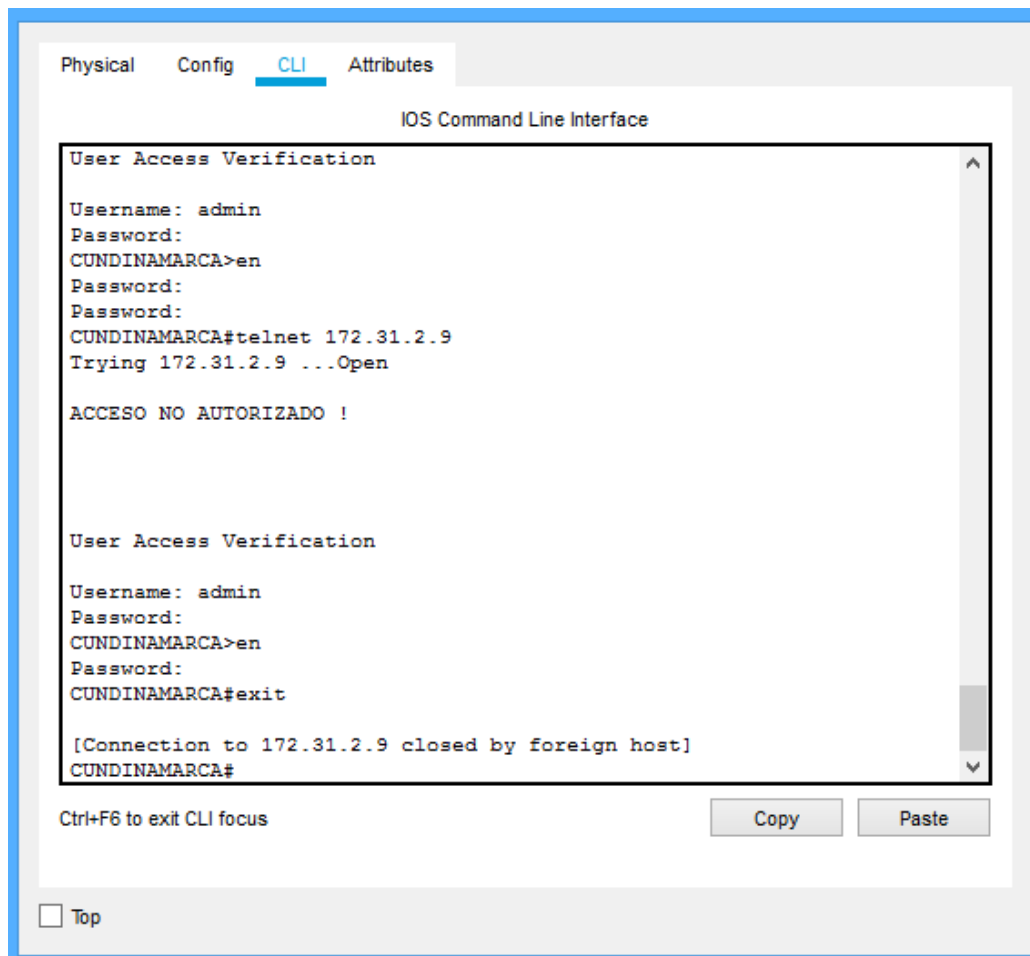
```

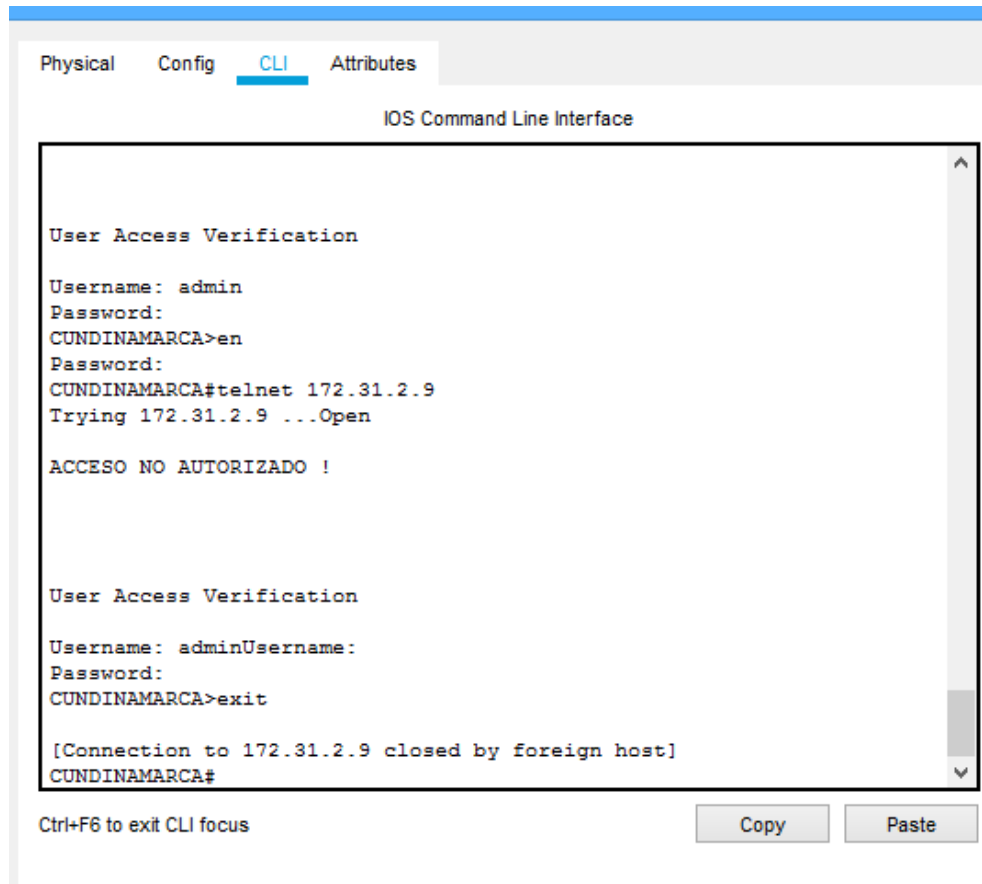
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#access-list
9 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 4
TUNJA(config-line)#access-class 9 in TUNJA(config-line)#
  
```

```

CUNDINAMARCA(config-subif)#access-list 9 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#access-class 9 in CUNDINAMARCA(config-line)#

```





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

```

BUCARAMANGA(config-if)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
  
```

```

CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#
  
```

```

00:25:02: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
CUNDINAMARCA(config-router)#end TUNJA(config-if)#router ospf 1
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0 TUNJA(config-router)#
00:19:40: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from
LOADING to FULL, Loading Done

```

```

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0 TUNJA(config-router)#end

```

## CONCLUSIONES

La realización de los anteriores escenarios ejemplificados en el programa packet tracer fueron la oportunidad de colocar a prueba los valores académicos adquiridos en la formación del diplomado, el análisis sobre el criterio de la formulación de un plano y la resolución de códigos básicos en el programa permiten evidenciar la complejidad de la realización de los mismos.

Realizar diferentes planteamientos previos ante los escenarios sugeridos es una oportunidad de situaciones que en el contexto laboral se palpan a diario, adquirir un vocabulario nuevo ligado al ámbito de las redes y que va de la mano con el área de ingeniería de sistemas es sin duda la resolución final de los saberes optados en la formación.

## BIBLIOGRAFÍA

Albritton, J. (1999). *Cisco IOS essentials*. New York: McGraw-Hill.

Cisco Press. (1998). *Cisco IOS WAN solutions*. [Place of publication not identified].

Download The Packet Tracer Simulator Tool & Find Courses | Networking Academy. (2019). Retrieved 24 December 2019, from <https://www.netacad.com/courses/packet-tracer>

Temática: Enrutamiento entre VLANs

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>