

## **DIPLOMADO DE PROFUNDIZACIÓN CISCO**

**Actividad final**

**Presentado a:  
DIEGO EDINSON RAMIREZ**

**Entregado por:  
Herick Gerardo Pérez**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
Diciembre 2019**

## CONTENIDO

|   |    |
|---|----|
| RESUMEN .....   | 3  |
| ABSTRACT .....  | 4  |
| INSTRUCCIÓN .....   | 5  |
| OBJETIVOS .....   | 6  |
| <b>Escenario 1</b> .....  | 7  |
| Parte 2: Configuración Básica. ....                             | 11 |
| Parte 3: Configuración de Enrutamiento.....                     | 22 |
| Parte 4: Configuración de las listas de Control de Acceso. .... | 28 |
| Parte 5: Comprobación de la red instalada. ....                 | 32 |
| <b>Escenario 2</b> .....  | 40 |
| CONCLUSIONES .....  | 48 |
| REFERENCIAS BIBLIOGRÁFICAS .....                                | 49 |

## RESUMEN

Luego del estudio de los capítulos de la plataforma de cisco y la realización de las actividades requeridas durante el desarrollo de la asignatura, realizando la ejecución del plan de pruebas para la configuración y comunicación de los diferentes elementos que compongan la topología de cada escenario procedemos a crear el presente documento, que se realiza con el fin de presentar el desarrollo de los ejercicios de la prueba final de habilidades, para dar solución a estos escenarios se requirió aplicar los conceptos y habilidades adquiridos durante el desarrollo de los diferentes capítulos y actividades vistos, mediante los cuales se obtuvo la información sobre los diferentes elementos que conforman una red, protocolos de enrutamiento, parámetros de seguridad y acceso en diferentes dispositivos en la red, además de las configuraciones OSPF, EIGRP, implementación DHCP, NAT, verificación de ACL. Estos escenarios se diseñaron y configuraron según la topología y requerimientos básicos dados, en la aplicación Packet Tracer que permite construir y ejecutar topologías de red.

En el escenario 1 se monta y desarrolla un red que requiere de la aplicación de los conocimientos en cuanto a configuración de los hosts necesarios y en una tabla la cual contiene el direccionamiento de cada uno de ellos, así como los servicios ACL, EIGRP, enlaces troncales y la implementación de las configuraciones.

En cuanto al escenario 2, se requerirá la aplicación de conocimientos y competencias en la implementación del enrutamiento VLAN, OSPF, Servicio DHCP y configuración de NAT estáticos y de sobrecarga, adicionalmente administrar los accesos a través de una lista de control de acceso

## ABSTRACT

After studying the chapters of the cisco platform and carrying out the activities required during the development of the subject, carrying out the test plan for the configuration and communication of the different elements that make up the topology of each scenario we proceed to To create this document, which is carried out in order to present the development of the final skills test exercises, to solve these scenarios, it was required to apply the concepts and skills acquired during the development of the different chapters and activities seen, through which information was obtained on the different elements that make up a network, routing protocols, security parameters and access on different devices in the network, in addition to the OSPF, EIGRP, DHCP implementation, NAT, ACL verification settings. These scenarios were designed and configured according to the topology and basic requirements given, in the Packet Tracer application that allows the construction and execution of network topologies.

In scenario 1, a network is developed and developed that requires the application of knowledge in terms of configuration of the necessary hosts and in a table which contains the address of each of them, as well as the ACL, EIGRP services, links Trunks and the implementation of the configurations.

As for scenario 2, the application of knowledge and skills in the implementation of VLAN routing, OSPF, DHCP service and static and overload NAT configuration will be required, additionally managing access through an access control list

## INSTRUCCIÓN

Es común que nuestro entorno diario usemos las redes de datos como medio de trabajo, para aprender, jugar y trabajar, estas cuentan con gran diversidad, ya que pueden variar según diferentes aspectos como la necesidad, tipo o tamaño, y pueden ir desde pequeñas redes locales hasta grandes estructuras globales, para atender las necesidades de comunicación de datos de cientos o hasta miles de computadoras.

Actualmente la administración y procesamiento de datos en las empresas han creado la necesidad de buscar y capacitar al personal idóneo para cumplir y ser competitivos laboralmente. Cisco, por medio de la información de CNNA, ofrece las herramientas para el aprendizaje en diseño y soporte de redes, otorgando las habilidades necesarias, para que el personal se desempeñe en este campo.

Por tanto, el siguiente informe, recoge la información obtenida durante el transcurso del diplomado y la realización de los laboratorios entregados y en este se hacen las observaciones, especificaciones técnicas, las limitaciones y las conclusiones surgidas tras el desarrollo, análisis y comprensión de las actividades propuestas, para alcanzar la certificación en el diplomado de profundización Cisco.

El programa de simulación de redes permitirá a los estudiantes experimentar con el comportamiento de la red y resolver los problemas de los elementos que no puedan conectarse, para permitir el tráfico entre estos. Para el uso de esta herramienta se requiere la aceptación de la licencia de usuario y la autorización del propietario que nos ha dado la universidad. El modo de operación con Packet Tracer es muy sencillo, ya que es un programa muy intuitivo y permite a los usuarios seleccionar los dispositivos que forman la red, los diferentes tipos de conector. Y en cada una de estas conexiones aparecerá un indicador de conectividad a nivel físico que podrá estar rojo (no hay conectividad), naranja (la interface está en proceso de inicio) o verde (la interfaz está operativa). La configuración de los parámetros de red será el reto a afrontar de cada estudiante con respecto a cada practica propuesta y lograr que la topología propuesta funcione.

## OBJETIVOS

### **GENERAL**

Hacer uso de los conocimientos, conceptos y prácticas adquiridos durante el diplomado para dar solución a los escenarios y posteriormente describir los parámetros y los objetos de la aplicación a través de las simulaciones de Packet Tracer.

### **ESPECÍFICOS**

- Entender la guía la prueba y hacer la definición de los elementos y propiedades de los objetos tal cual se solicita para cada caso.
- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores y Hosts.
- Solucionar los interrogantes incluidos en los laboratorios
- Garantizar que funcionen las simulaciones y la documentación del proceso sea clara.

## Escenario 1

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

### Topología de red

Los requerimientos solicitados son los siguientes:

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

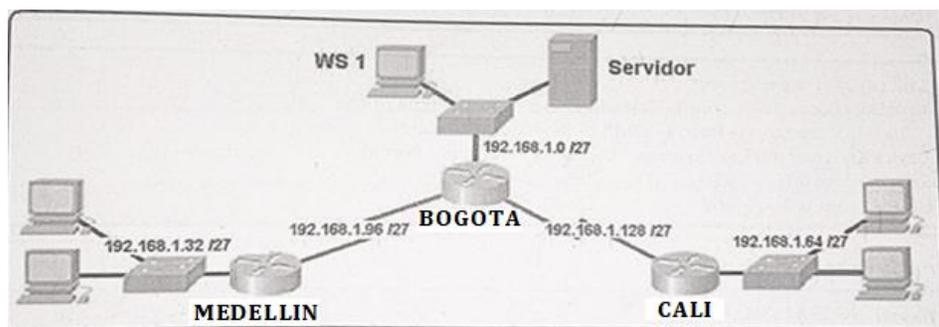
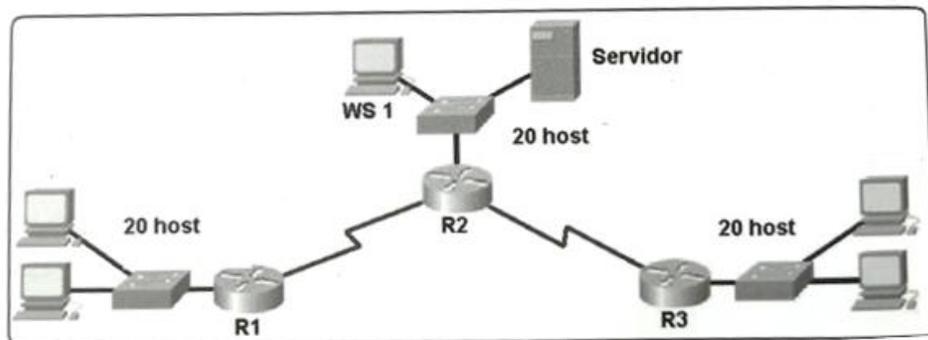
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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

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

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

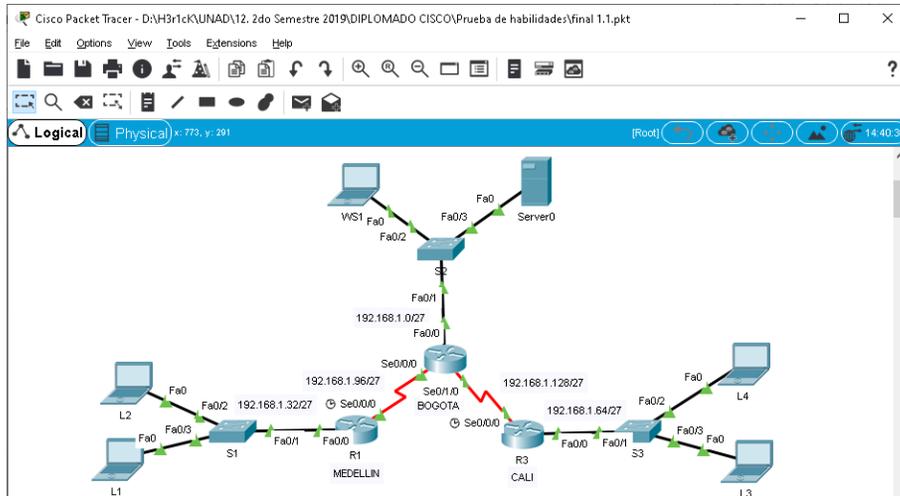
Parte 6: Configuración final.



## Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración
  - Realizar la conexión física de los equipos con base en la topología de red
- RTA:** Se realiza el montaje del diseño en la plataforma Packet tracer con los equipos listos para su configuración. Imagen a continuación una vez montados los elementos.



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

### Parte 1: Asignación de direcciones IP:

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

**RTA:** se calcula la máscara de red se usará  $255.255.255.224 = 27$

b. Asignar una dirección IP a la red.

**Proceso:** Se selecciona cada Router y se usa la opción de CLI para ingresar y ejecutar el conjunto de comandos de configuración básicos y de interfaz.

Pasos realizados para configurar los parámetros básicos:

- Cambiar nombre
- Desactivar la búsqueda del DNS
- Asignar contraseña del modo EXEC
- Asignar contraseña de consola y la contraseña de vty.
- Configurar aviso (MOTD)
- Configurar logging synchronous

Pasos para configuración de la interfaz

- Configurar la dirección IP

- Establecer frecuencia de reloj, si aplica

### **Comandos ejecutados en el Router R1:**

#### **Se configuran los parámetros básicos**

```
Router>enable
Router#conf terminal
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable pass class
R1(config)#line vty 0 15
R1(config-line)#password code
R1(config-line)#login
R1(config-line)#banner motd #uso permitido solo a usuarios registrados#
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exit
```

#### **Se configura configuración de interfaz**

```
R1#conf terminal
R1(config)# int fa0/0
R1(config-if)#ip address 192.168.1.33 255.255.255.224
R1(config-if)#exit
R1(config)# int s0/0/0
R1(config-if)#ip address 192.168.1.99 255.255.255.224
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
```

### **Comandos ejecutados en el Router R2:**

#### **Se configuran los parámetros básicos**

```
Router>enable
Router#conf terminal
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable pass class
R2(config)#line vty 0 15
R2(config-line)#password code
R2(config-line)#login
R2(config-line)#banner motd #uso permitido solo a usuarios registrados#
R2(config)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exit
```

### **Se configura configuracion de interfaz**

```
R2#conf terminal
R2(config)# int s0/0/0
R2(config-if)#ip address 192.168.1.98 255.255.255.224
R2(config-if)#exit
R2(config)# int fa0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.224
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)# int s0/1/0
R2(config-if)#ip address 192.168.1.130 255.255.255.224
R2(config-if)#no shutdown
R2(config-if)#exit
```

### **Comandos ejecutados en el Router R3:**

#### **Se cofiguan los parámetros básicos**

```
Router>enable
Router#conf terminal
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#enable pass class
R3(config)#line vty 0 15
R3(config-line)#password code
R3(config-line)#login
R3(config-line)#banner motd #uso permitido solo a usuarios registrados#
R3(config)#line con 0
R3(config-line)#logging synchronous
R3(config-line)#exit
```

#### **Se configura configuracion de interfaz**

```
R3#conf terminal
R3(config)# int fa0/0
R3(config-if)#ip address 192.168.1.65 255.255.255.224
R3(config-if)#exit
R3(config)# int s0/0/0
R3(config-if)#ip address 192.168.1.131 255.255.255.224
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
R3(config-if)#exit
```

## Parte 2: Configuración Básica.

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

|  | R3           | R3            | R3            |
|--|--------------|---------------|---------------|
| Nombre de Host                         | MEDELLIN     | BOGOTA        | CALI          |
| Dirección de Ip en interfaz Serial 0/0 | 192.168.1.99 | 192.168.1.98  | 192.168.1.131 |
| Dirección de Ip en interfaz Serial 0/1 |              | 192.168.1.130 |               |
| Dirección de Ip en interfaz FA 0/0     | 192.168.1.33 | 192.168.1.1   | 192.168.1.65  |
| Protocolo de enrutamiento              | Eigrp        | Eigrp         | Eigrp         |
| Sistema Autónomo                       | 200          | 200           | 200           |
| Afirmaciones de red                    | 192.168.1.0  | 192.168.1.0   | 192.168.1.0   |

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

**Proceso:** Se ingresa procede a seleccionar cada uno de los Router para ejecutar el comando show ip route, y de esta manera verificar la configuración de enrutamiento para cada caso, se adjuntan imágenes de evidencia

### Comandos ejecutados en el Router R1:

```
R1>enable
Password:
R1#sh ip route
```

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

uso solo para usuarios autorizados
R1>enable
Password:
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
      BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

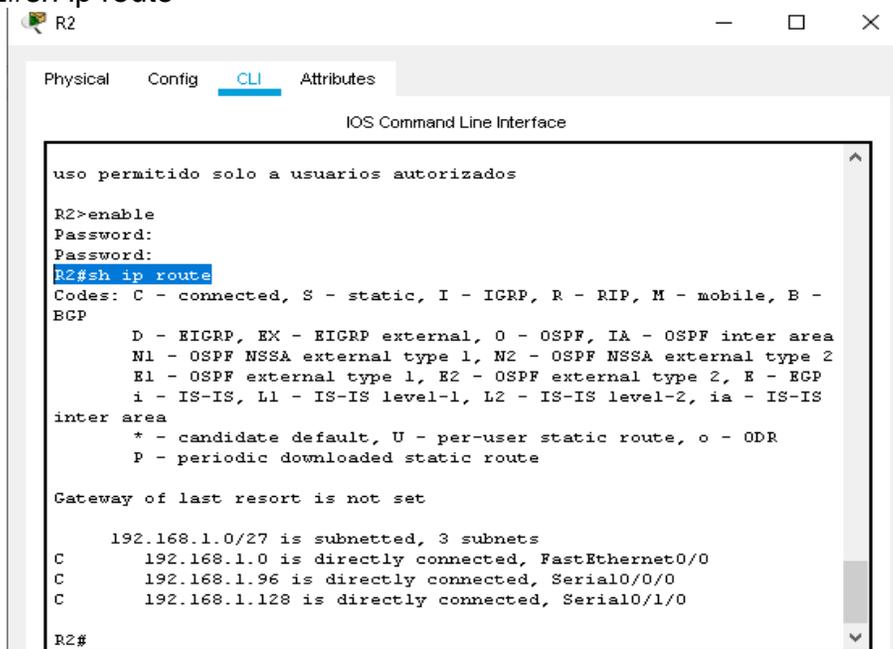
      192.168.1.0/27 is subnetted, 2 subnets
      C      192.168.1.32 is directly connected, FastEthernet0/0
      C      192.168.1.96 is directly connected, Serial0/0/0

R1#

```

## Comandos ejecutados en el Router R2:

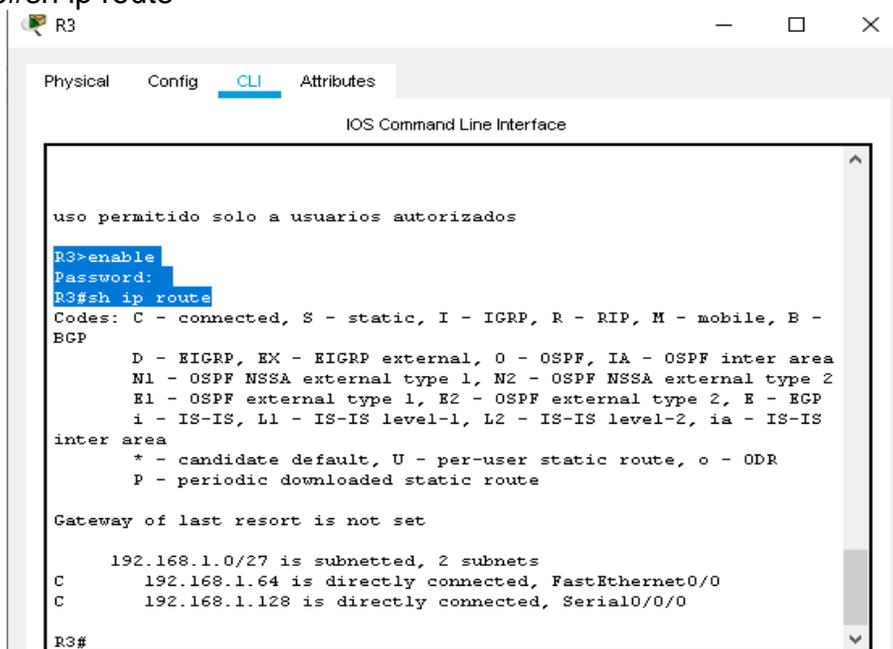
```
R2>enable  
Password:  
R2#sh ip route
```



```
R2  
Physical Config CLI Attributes  
IOS Command Line Interface  
uso permitido solo a usuarios autorizados  
R2>enable  
Password:  
Password:  
R2#sh ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -  
BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS  
inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route  
Gateway of last resort is not set  
192.168.1.0/27 is subnetted, 3 subnets  
C 192.168.1.0 is directly connected, FastEthernet0/0  
C 192.168.1.96 is directly connected, Serial0/0/0  
C 192.168.1.128 is directly connected, Serial0/1/0  
R2#
```

## Comandos ejecutados en el Router R3:

```
R3>enable  
Password:  
R3#sh ip route
```



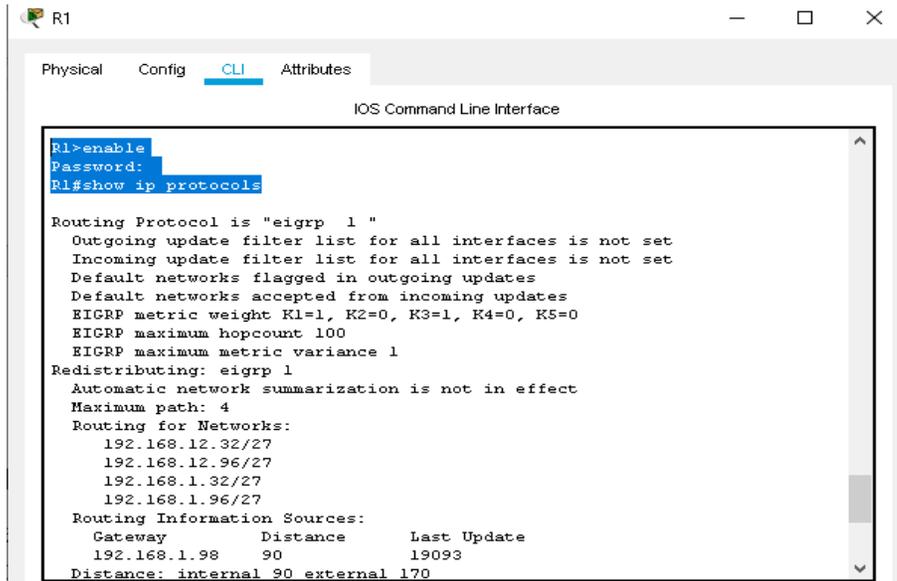
```
R3  
Physical Config CLI Attributes  
IOS Command Line Interface  
uso permitido solo a usuarios autorizados  
R3>enable  
Password:  
R3#sh ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -  
BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS  
inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route  
Gateway of last resort is not set  
192.168.1.0/27 is subnetted, 2 subnets  
C 192.168.1.64 is directly connected, FastEthernet0/0  
C 192.168.1.128 is directly connected, Serial0/0/0  
R3#
```

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

**Proceso:** Se selecciona cada Router y en la opción CLI se ingresa el comando `show ip protocols` que muestra varios de los parámetros y otra información acerca del estado actual de cualquier proceso activo de protocolo de routing configurado en el router.

**Comandos ejecutados en el Router R1:**

```
R1>enable  
Password:  
R1#show ip protocols
```



**Comandos ejecutados en el Router R2:**

```
R2>enable  
Password:  
R1#show ip protocols
```

```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2>enable
Password:
R2#show ip protocols

Routing Protocol is "eigrp 1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
    Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.96/27
    192.168.1.128/27
    192.168.1.0/27
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.1.131    90           54800313
```

### Comandos ejecutados en el Router R3:

```
R3>enable
Password:
R3#show ip protocols
```

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3>enable
Password:
R3#show ip protocols

Routing Protocol is "eigrp 1 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
    Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.64/27
    192.168.1.128/27
  Routing Information Sources:
    Gateway         Distance      Last Update
  192.168.1.130    90           146660223
  Distance: internal 90 external 170

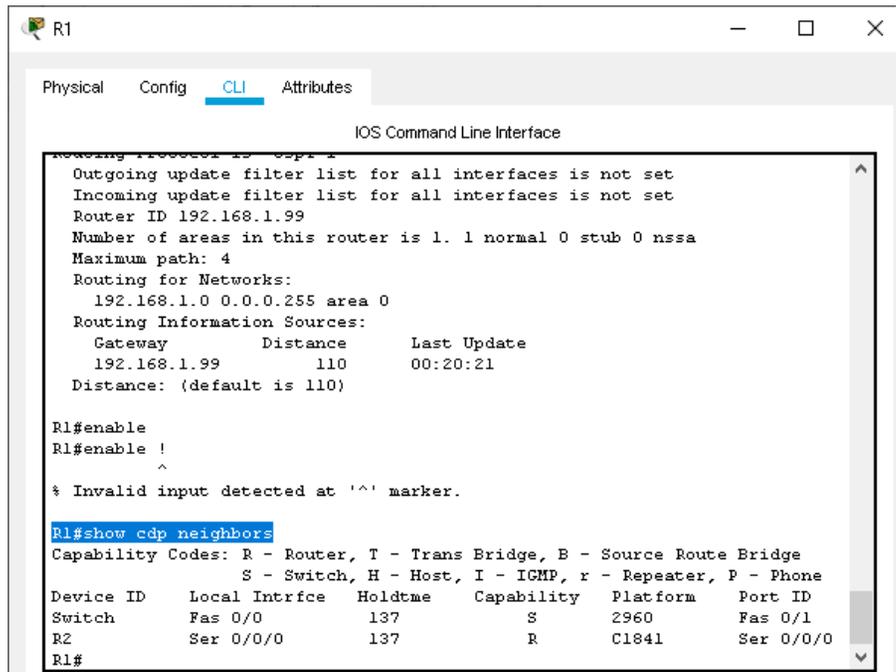
R3#
```

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

**Proceso:** Se selecciona cada Router y posteriormente se usa el comando show cdp neighbors para obtener información para la operación de los dispositivos Cisco de distribución y la capa de acceso

**Comandos ejecutados en el Router R1:**

R1#show cdp neighbors



**Comandos ejecutados en el Router R2:**

R2#show cdp neighbors

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.1.99
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.1.0 0.0.0.255 area 0
Routing Information Sources:
 Gateway      Distance      Last Update
 192.168.1.99    110          00:20:21
Distance: (default is 110)

R1#enable
R1#enable !
^
% Invalid input detected at '^' marker.

R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - ICMP, r - Repeater, P - Phone
Device ID      Local Infrfce  Holdtme    Capability  Platform  Port ID
Switch         Fas 0/0       137        S           2960      Fas 0/1
R2             Ser 0/0/0     137        R           C1841     Ser 0/0/0
R1#

```

**Comandos ejecutados en el Router R3:**  
**R3#show cdp neighbors**

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
Outgoing update filter list for all interferences is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 1
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 192.168.1.64/27
 192.168.1.128/27
Routing Information Sources:
 Gateway      Distance      Last Update
 192.168.1.130 90            146660223
Distance: internal 90 external 170

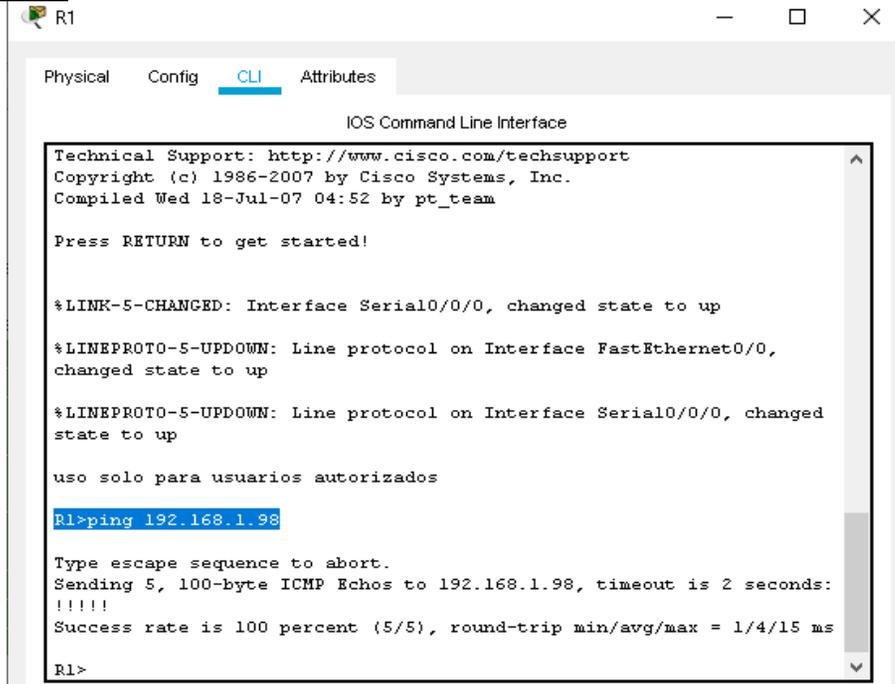
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - ICMP, r - Repeater, P - Phone
Device ID      Local Infrfce  Holdtme    Capability  Platform  Port ID
Switch         Fas 0/0       140        S           2960      Fas 0/1
R2             Ser 0/0/0     150        R           C1841     Ser 0/1/0
R3#

```

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

**Proceso:** Se usa la sección de CLI o el CMD para realizar PING de un tramo a otro

## Ping R1 a R2



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
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

Press RETURN to get started!

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

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

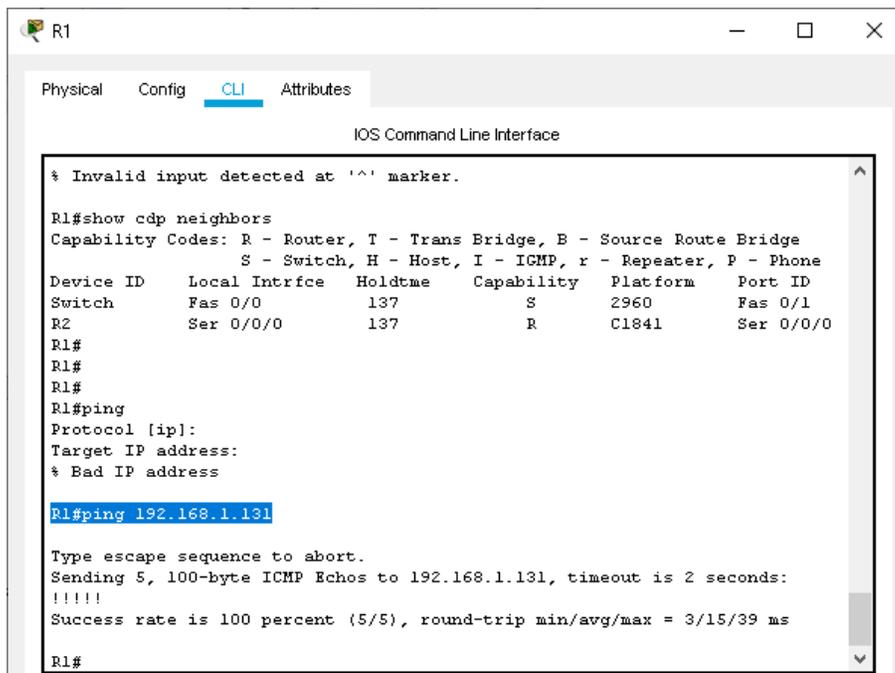
uso solo para usuarios autorizados

R1>ping 192.168.1.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/15 ms

R1>
```

## Ping R1 a R3



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

% Invalid input detected at '^' marker.

R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - ICMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme  Capability  Platform  Port ID
Switch         Fas 0/0        137      S           2960      Fas 0/1
R2             Ser 0/0/0      137      R           C1841     Ser 0/0/0
R1#
R1#
R1#
R1#ping
Protocol [ip]:
Target IP address:
% Bad IP address

R1#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 = 3/15/39 ms

R1#
```

## Ping R2 a R1

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Routing for Networks:
Routing Information Sources:
  Gateway         Distance       Last Update
Distance: (default is 110)

R2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - ICMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme    Capability  Platform  Port ID
Switch           Fas 0/0       138        S           2960      Fas 0/1
R1               Ser 0/0/0     157        R           C1841     Ser 0/0/0
R3               Ser 0/1/0     139        R           C1841     Ser 0/0/0
R2#
R2#
R2#
R2#
R2#
R2#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 = 1/7/14 ms

R2#

```

### Ping R2 a R3

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Switch           Fas 0/0       138        S           2960      Fas 0/1
R1               Ser 0/0/0     157        R           C1841     Ser 0/0/0
R3               Ser 0/1/0     139        R           C1841     Ser 0/0/0
R2#
R2#
R2#
R2#
R2#
R2#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 = 1/7/14 ms

R2#
R2#
R2#ping 192.168.1.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms

R2#

```

### Ping R3 a R1

```
R3
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

uso permitido solo a usuarios autorizados

R3>enable
Password:
R3#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 = 2/7/13 ms

R3#
```

## Ping R3 a R2

```
R3
Physical Config CLI Attributes
IOS Command Line Interface

uso permitido solo a usuarios autorizados

R3>enable
Password:
R3#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 = 2/7/13 ms

R3#
R3#
R3#
R3#
R3#ping 192.168.1.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/11 ms

R3#
```

## Ping L1 a L2

The screenshot shows a network device configuration window titled 'L1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a Command Prompt window. The Command Prompt shows a successful ping to 192.168.1.66, followed by a ping to 192.168.1.35. The ping to 192.168.1.35 shows 4 successful replies with 0% loss and an average round trip time of 0ms.

```
Command Prompt
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

## Ping L1 a L3

The screenshot shows a network device configuration window titled 'L1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a Command Prompt window. The Command Prompt shows a successful ping to 192.168.1.35, followed by a ping to 192.168.1.67. The ping to 192.168.1.67 shows 4 replies, but the first one timed out, resulting in a 25% loss rate and an average round trip time of 2ms.

```
Command Prompt
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.67

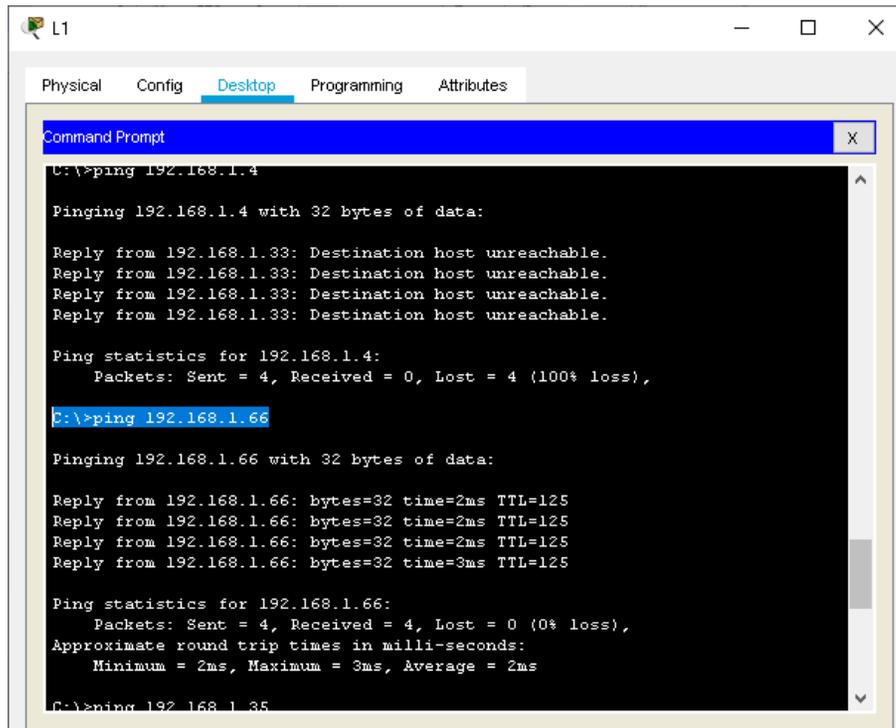
Pinging 192.168.1.67 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
```

## Ping L1 a L4



```
L1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66

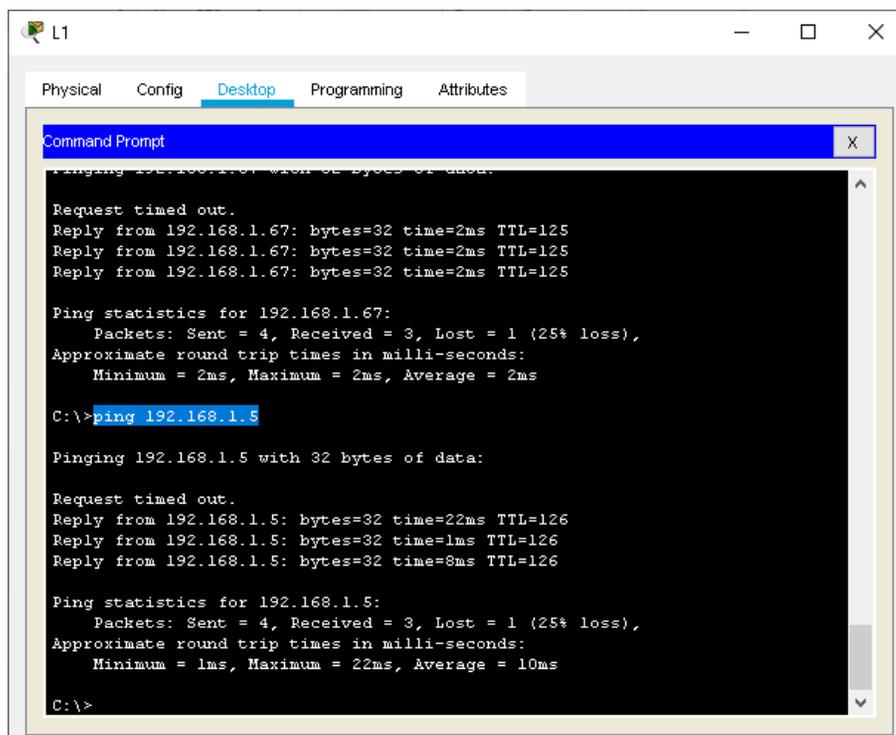
Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=2ms TTL=125
Reply from 192.168.1.66: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>ping 192.168.1.35
```

## Ping L1 a WS1



```
L1
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.67 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125
Reply from 192.168.1.67: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ping 192.168.1.5

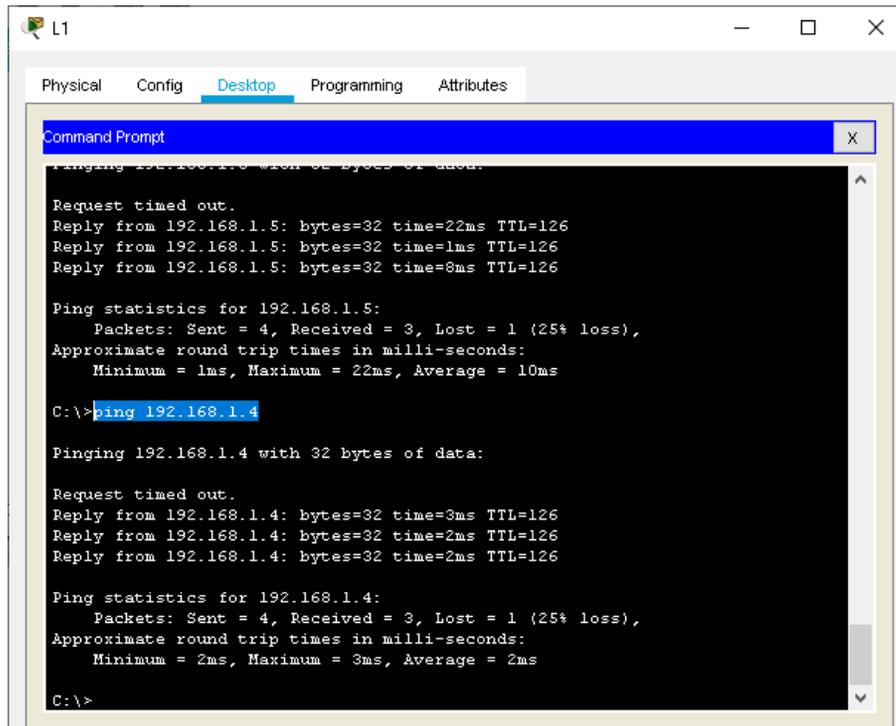
Pinging 192.168.1.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.5: bytes=32 time=22ms TTL=126
Reply from 192.168.1.5: bytes=32 time=1ms TTL=126
Reply from 192.168.1.5: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 22ms, Average = 10ms

C:\>
```

## Ping L1 a Server0



```
L1
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.5 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.5: bytes=32 time=22ms TTL=126
Reply from 192.168.1.5: bytes=32 time=1ms TTL=126
Reply from 192.168.1.5: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 22ms, Average = 10ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.4: bytes=32 time=3ms TTL=126
Reply from 192.168.1.4: bytes=32 time=2ms TTL=126
Reply from 192.168.1.4: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

### Parte 3: Configuración de Enrutamiento.

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

**Proceso:** Se selecciona cada Router y en la opción CLI se ingresa a la opción de Configuration Terminal, posteriormente se usa el comando Router Eigrp + un identificador en este caso el número 1. Ahora por medio del comando Do Show Ip Route se buscan los elementos que tengan el estado (C – connected), los cuales agregaremos al protocolo de enrutamiento Eigrp.

#### Comandos ejecutados en el Router R1:

```
R1>enable
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#do sh ip rout
R1(config-router)#network 192.168.1.32 0.0.0.31
R1(config-router)#network 192.168.1.96 0.0.0.31
R1(config-router)#no auto-summary
R1(config-router)#exit
```

#### Comandos ejecutados en el Router R2:

```
R2>enable
R2#conf term
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#router eigrp 1  
R2(config-router)#do sh ip rou  
R2(config-router)#network 192.168.1.0 0.0.0.31  
R2(config-router)#network 192.168.1.96 0.0.0.31  
R2(config-router)#network 192.168.1.128 0.0.0.31  
R2(config-router)#no auto-summary  
R2(config-router)#exit
```

**Comandos ejecutados en el Router R3:**

```
R3>enable  
R3#conf term  
Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)#router eigrp 1  
R3(config-router)#do sh ip rou  
R3(config-router)#network 192.168.1.64 0.0.0.31  
R3(config-router)#network 192.168.1.128 0.0.0.31  
R3(config-router)#no auto-summary  
R3(config-router)#exit
```

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

**Proceso:** Se selecciona cada Router y en la opción CLI se ingresa Show Ip Eigrp Neighbors el cual permite ver el estado de los EIGRP dinámicos o estáticos.

**Comandos ejecutados en el Router R1:**

Physical Config **CLI** Attributes

IOS Command Line Interface

Press RETURN to get started.

uso solo para usuarios autorizados

```
R1>enable
Password:
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address      Interface    Hold Uptime    SRTT  RT0  Q  Seq
   (sec)         (ms)         (sec)          (ms)  Cnt  Num
0  192.168.1.98  Se0/0/0     11  03:25:29    40   1000  0  35
```

### Comandos ejecutados en el Router R2:

Physical Config **CLI** Attributes

IOS Command Line Interface

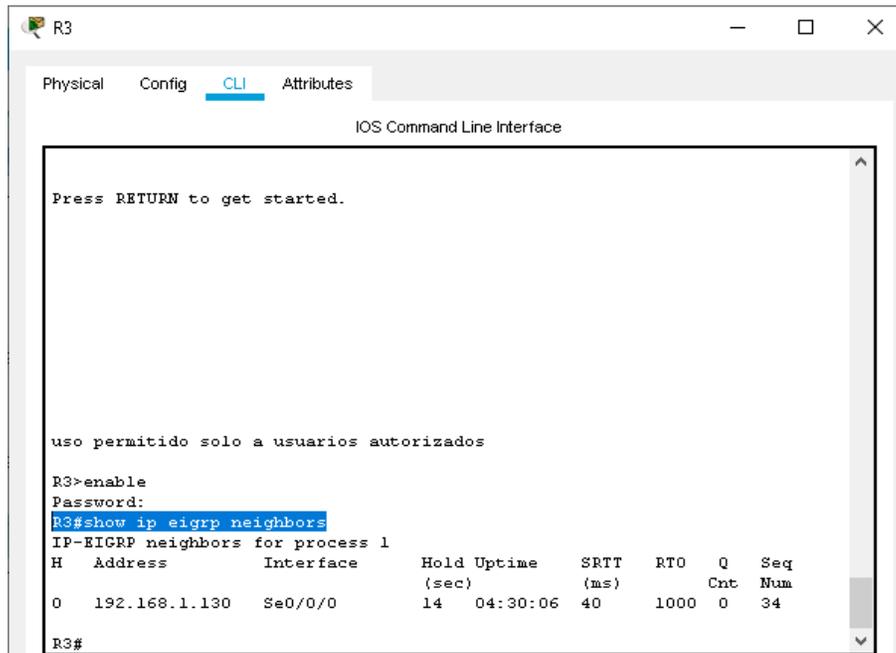
Press RETURN to get started.

uso permitido solo a usuarios autorizados

```
R2>enable
Password:
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address      Interface    Hold Uptime    SRTT  RT0  Q  Seq
   (sec)         (ms)         (sec)          (ms)  Cnt  Num
0  192.168.1.131 Se0/1/0     11  04:28:52    40   1000  0  44
1  192.168.1.99  Se0/0/0     14  03:34:34    40   1000  0  7

R2#
```

## Comandos ejecutados en el Router R3:



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

uso permitido solo a usuarios autorizados

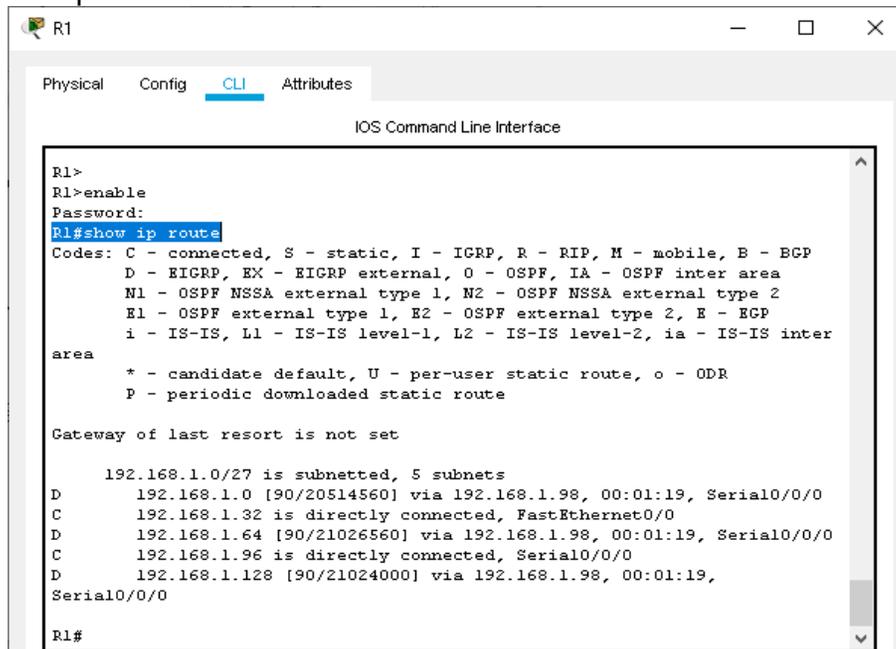
R3>enable
Password:
R3#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H  Address          Interface      Hold Uptime    SRTT  RT0  Q  Seq
  (sec)              (ms)          Cnt  Num
0  192.168.1.130     Se0/0/0       14   04:30:06  40   1000 0  34

R3#
```

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

## Comandos ejecutados en el Router R1:

```
R1>enable
Password:
R1#sh ip route
```



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

R1>
R1>enable
Password:
R1#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
D    192.168.1.0 [90/20514560] via 192.168.1.98, 00:01:19, Serial0/0/0
C    192.168.1.32 is directly connected, FastEthernet0/0
D    192.168.1.64 [90/21026560] via 192.168.1.98, 00:01:19, Serial0/0/0
C    192.168.1.96 is directly connected, Serial0/0/0
D    192.168.1.128 [90/21024000] via 192.168.1.98, 00:01:19,
Serial0/0/0

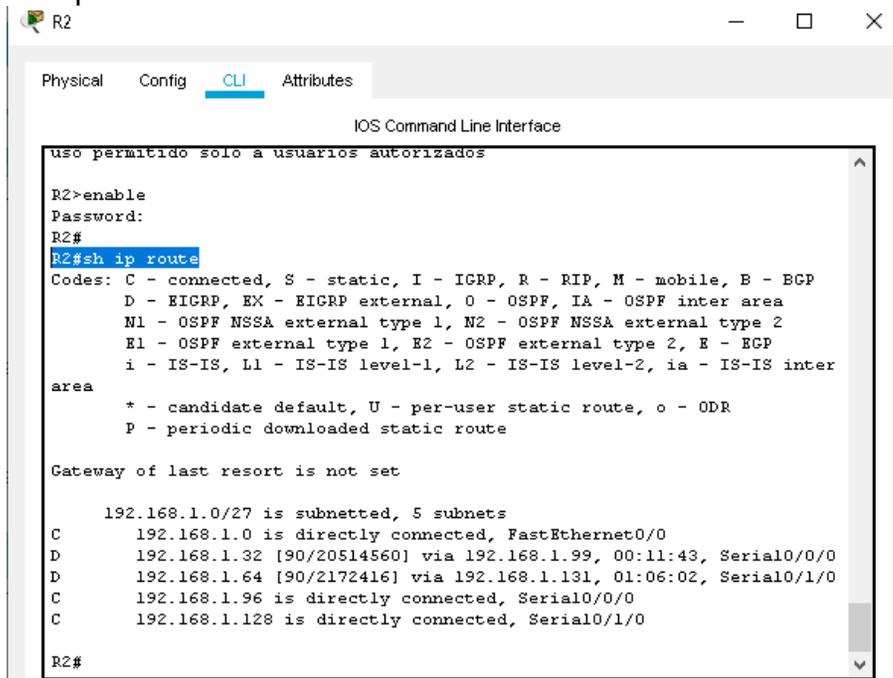
R1#
```

## Comandos ejecutados en el Router R2:

R2>enable

Password:

R2#sh ip route



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
uso permitido solo a usuarios autorizados
R2>enable
Password:
R2#
R2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
C    192.168.1.0 is directly connected, FastEthernet0/0
D    192.168.1.32 [90/20514560] via 192.168.1.99, 00:11:43, Serial0/0/0
D    192.168.1.64 [90/2172416] via 192.168.1.131, 01:06:02, 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

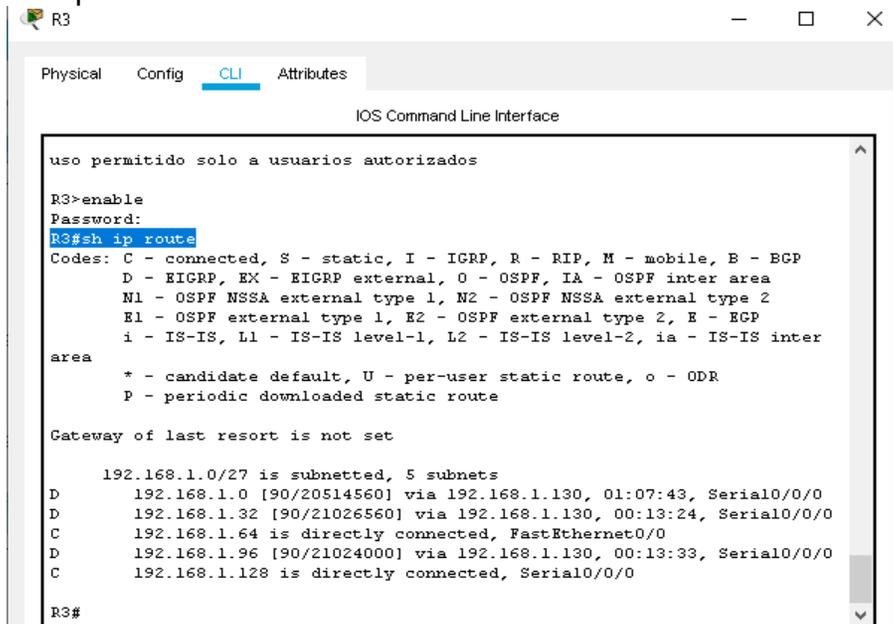
R2#
```

## Comandos ejecutados en el Router R3:

R3>enable

Password:

R3#sh ip route



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
uso permitido solo a usuarios autorizados
R3>enable
Password:
R3#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

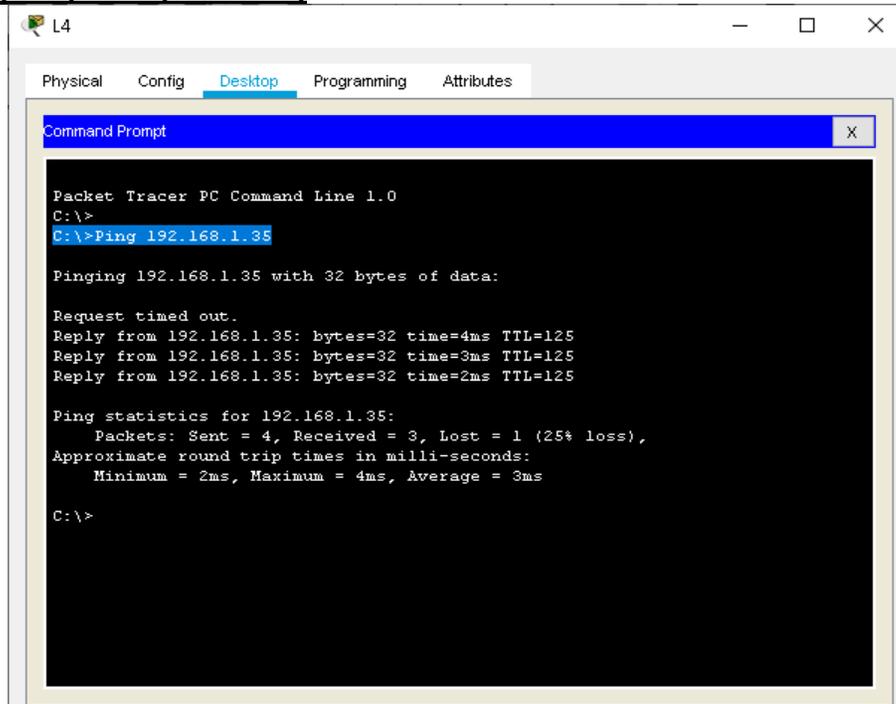
Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D    192.168.1.0 [90/20514560] via 192.168.1.130, 01:07:43, Serial0/0/0
D    192.168.1.32 [90/21026560] via 192.168.1.130, 00:13:24, Serial0/0/0
C    192.168.1.64 is directly connected, FastEthernet0/0
D    192.168.1.96 [90/21024000] via 192.168.1.130, 00:13:33, Serial0/0/0
C    192.168.1.128 is directly connected, Serial0/0/0

R3#
```

d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

### Ping L4 (Cali) a L2 (Medellin)



```
L4
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>
C:\>Ping 192.168.1.35

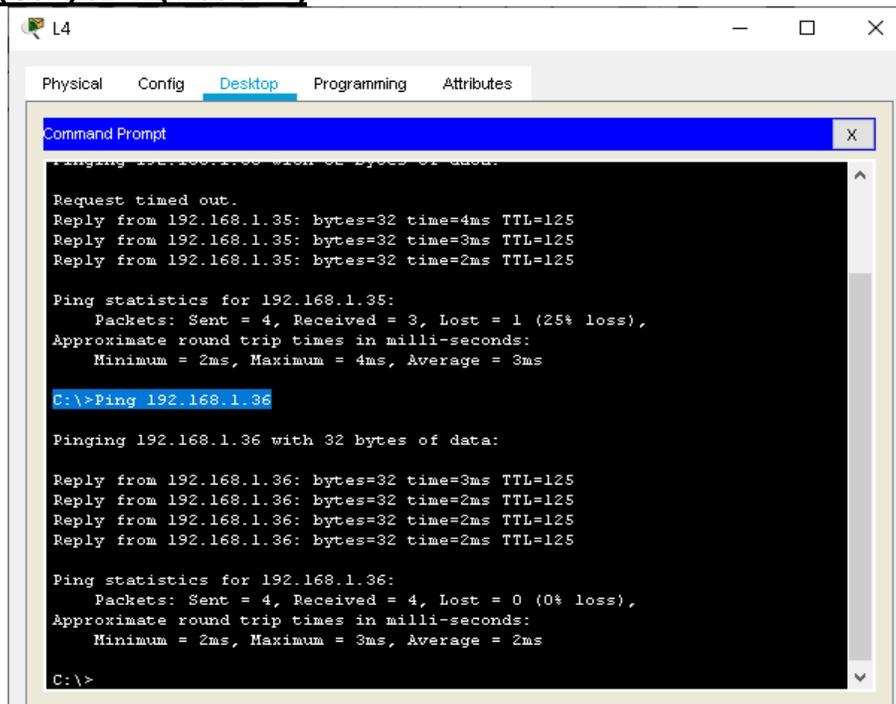
Pinging 192.168.1.35 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.35: bytes=32 time=4ms TTL=125
Reply from 192.168.1.35: bytes=32 time=3ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\>
```

### Ping L4 (Cali) a L1 (Medellin)



```
L4
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.35 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.35: bytes=32 time=4ms TTL=125
Reply from 192.168.1.35: bytes=32 time=3ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\>Ping 192.168.1.36

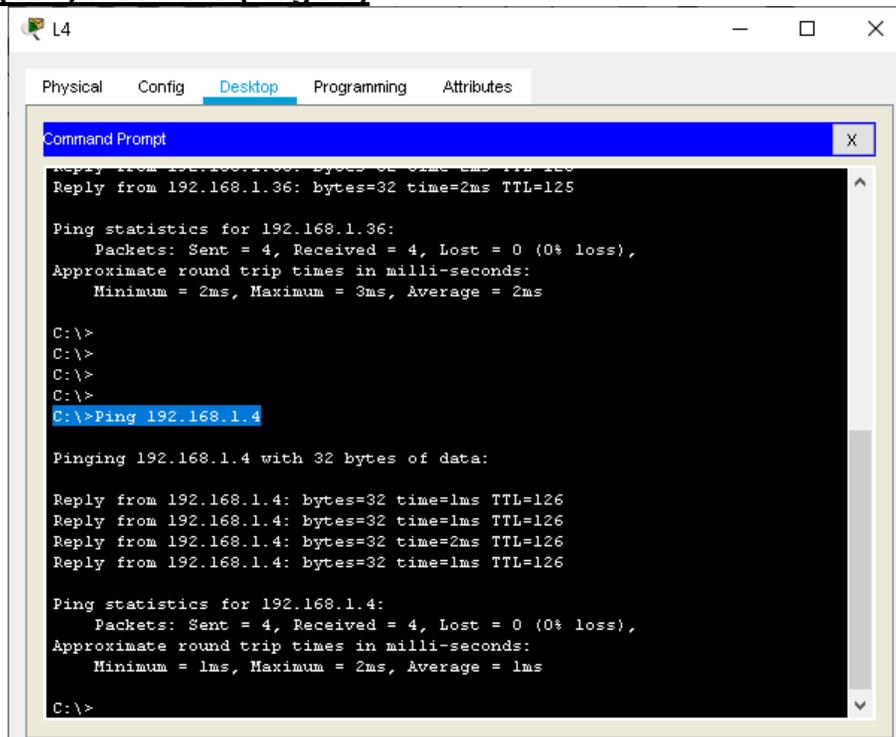
Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=3ms TTL=125
Reply from 192.168.1.36: bytes=32 time=2ms TTL=125
Reply from 192.168.1.36: bytes=32 time=2ms TTL=125
Reply from 192.168.1.36: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

## Ping L4 (Cali) a Server0 (Bogota)



```
L4
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.36: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=1ms TTL=126
Reply from 192.168.1.4: bytes=32 time=1ms TTL=126
Reply from 192.168.1.4: bytes=32 time=2ms TTL=126
Reply from 192.168.1.4: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
```

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

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

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

**Proceso:** Se selecciona cada Router y en la opción CLI se ingresa el comando Telnet con la IP de cada uno de los otros routers, se comparte evidencia de conexión

### **Comandos de conexión telnet Router R3 a R2:**

```
R3>enable
Password:
R3#telne
R3#telnet 192.168.1.1
```

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

Openuso permitido solo a usuarios autorizados

R3>enable
Password:
R3#telne
R3#telnet 192.168.1.1
Trying 192.168.1.1 ...Openuso permitido solo a usuarios autorizados

User Access Verification

Password:
R2>
```

### Comandos de conexión telnet Router R3 a R1:

```
R3>enable
Password:
R3#telnet 192.168.1.99
```

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3#telne
R3#telnet 192.168.1.1
Trying 192.168.1.1 ...Openuso permitido solo a usuarios autorizados

User Access Verification

Password:
R2>exit

[Connection to 192.168.1.1 closed by foreign host]
R3#telnet 192.168.1.99
Trying 192.168.1.99 ...Openuso solo para usuarios autorizados

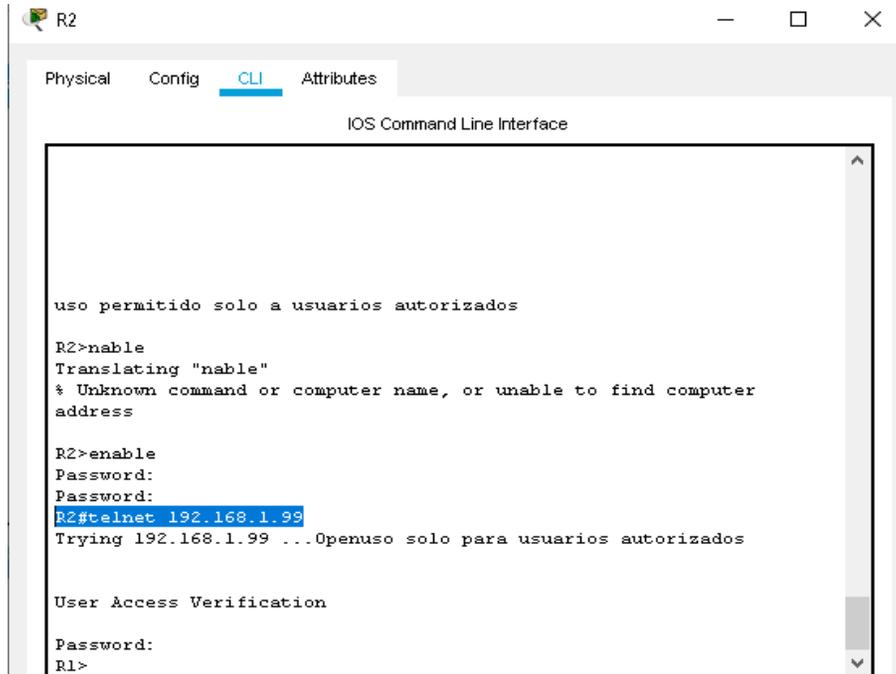
User Access Verification

Password:
Password:
R1> (You have open connections) [confirm]

[Connection to 192.168.1.99 closed by foreign host]
R3#
```

### Comandos de conexión telnet Router R2 a R1:

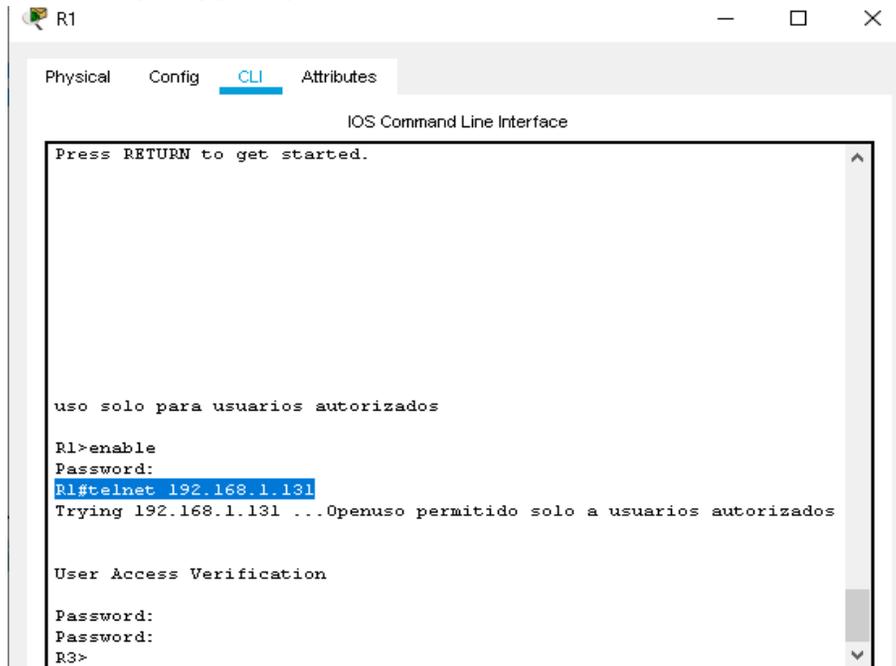
```
R2>enable  
Password:  
R2#telnet 192.168.1.99
```



```
R2  
Physical Config CLI Attributes  
IOS Command Line Interface  
uso permitido solo a usuarios autorizados  
R2>enable  
Translating "enable"  
% Unknown command or computer name, or unable to find computer  
address  
R2>enable  
Password:  
Password:  
R2#telnet 192.168.1.99  
Trying 192.168.1.99 ...Openuso solo para usuarios autorizados  
User Access Verification  
Password:  
R1>
```

### Comandos de conexión telnet Router R1 a R3:

```
R1>enable  
Password:  
R1#telnet 192.168.1.131
```



```
R1  
Physical Config CLI Attributes  
IOS Command Line Interface  
Press RETURN to get started.  
uso solo para usuarios autorizados  
R1>enable  
Password:  
R1#telnet 192.168.1.131  
Trying 192.168.1.131 ...Openuso permitido solo a usuarios autorizados  
User Access Verification  
Password:  
Password:  
R3>
```

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

**Proceso:** Se selecciona cada Router y en la opción CLI se ingresa los comandos El proceso de creación de una ACL se lleva a cabo creando la lista que para este caso llamaremos acceso y posteriormente asociándola a la IP a la cual se le permitirá el acceso, y posteriormente se define el filtro bien sea de entrada o salida.

#### **Comandos de ACL Router R1**

```
R1>enable
Password:
R1#conf t
R1(config)#ip access-list extended acceso
R1(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.4 0.0.0.0
R1(config-ext-nacl)#exit
R1(config)#int f0/0
R1(config-if)#ip access-group 1 in
R1(config-if)#
```

#### **Comandos de ACL Router R2**

```
R2>enable
Password:
R2#conf t
R2(config)#ip access-list extended acceso
R2(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.4 0.0.0.0
R2(config-ext-nacl)#exit
R2(config)#int f0/0
R2(config-if)#ip access-group 1 in
R2(config-if)#
```

#### **Comandos de ACL Router R3**

```
R3>enable
Password:
R3#conf t
R3(config)#ip access-list extended acceso
R3(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.4 0.0.0.0
R3(config-ext-nacl)#exit
R3(config)#int f0/0
R3(config-if)#ip access-group 1 in
R3(config-if)#
```

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

#### **Comandos de ACL Router R1**

```
R1>enable
Password:
R1#conf t
R1(config)#ip access-list extended acceso
R1(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0
R1(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
R1(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131
0.0.0.0
R1(config-ext-nacl)#
```

#### **Comandos de ACL Router R2**

```
R2>enable
Password:
R2#conf t
R2(config)#ip access-list extended acceso
R2(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
R2(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
R2(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.130
0.0.0.0
R2(config-ext-nacl)#
```

#### **Comandos de ACL Router R3**

```
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip access-list extended acceso
R3(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131
0.0.0.0
R3(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
R3(config-ext-nacl)#
```

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

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

##### **Ping Server0(Bogota) a L2 (Medellin)**

```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.1.5:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.35:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 192.168.1.67
Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
```

## Ping Server0(Bogota) a L3(Cali)

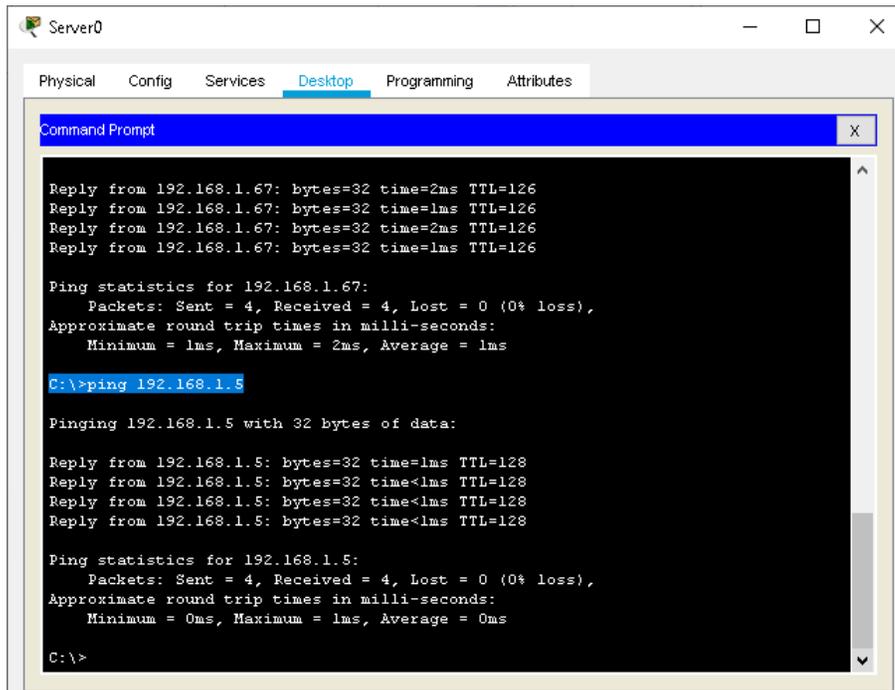
```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.35:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 192.168.1.67
Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.67:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
```

## Ping Server0(Bogota) a WS1(Cali)



The screenshot shows a Packet Tracer PC window titled "Server0" with tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of a ping command to 192.168.1.5, which is successful. The output includes four replies with 32 bytes of data and a TTL of 128, with round trip times of 1ms. The statistics show 4 packets sent, 4 received, and 0% loss.

```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=2ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.1.5

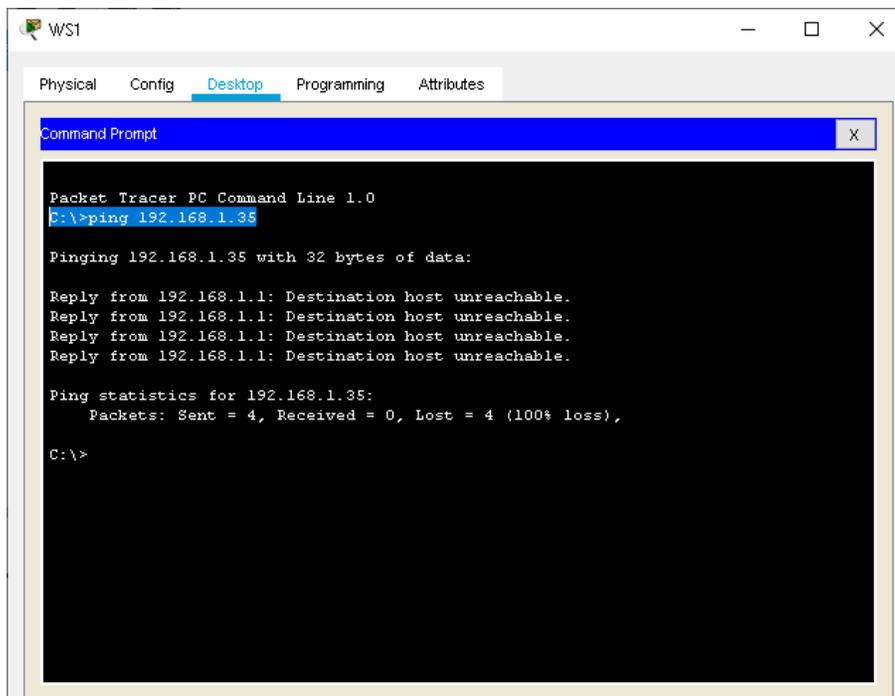
Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

## Ping WS1(Bogota) a L2(Medellin)



The screenshot shows a Packet Tracer PC window titled "WS1" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of a ping command to 192.168.1.35, which fails. The output shows four replies from 192.168.1.1 indicating that the destination host is unreachable. The statistics show 4 packets sent, 0 received, and 100% loss.

```
WS1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
E:\>ping 192.168.1.35

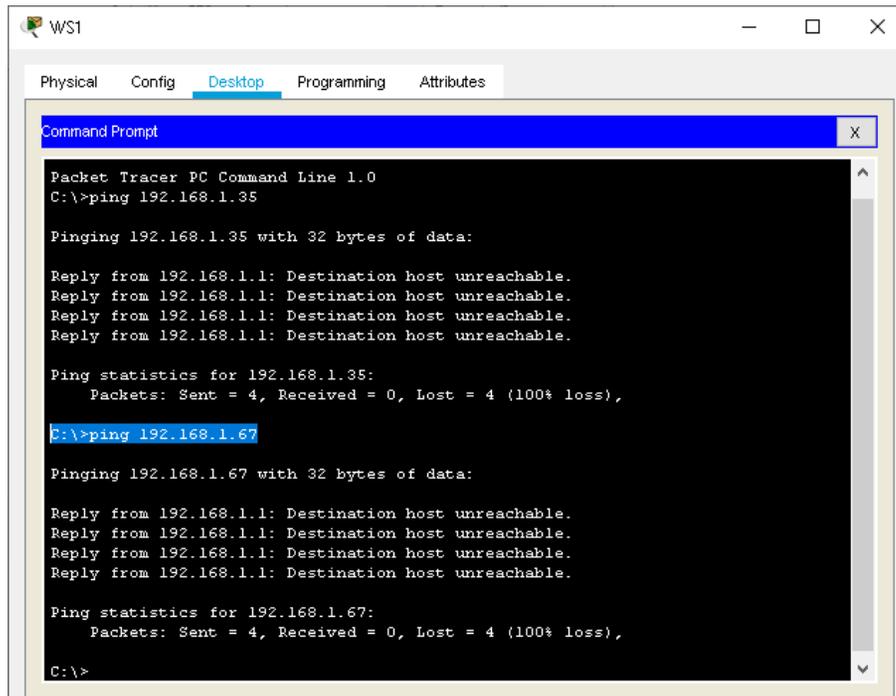
Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Ping WS1(Bogota) a L3(Cali)



```
WS1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.67

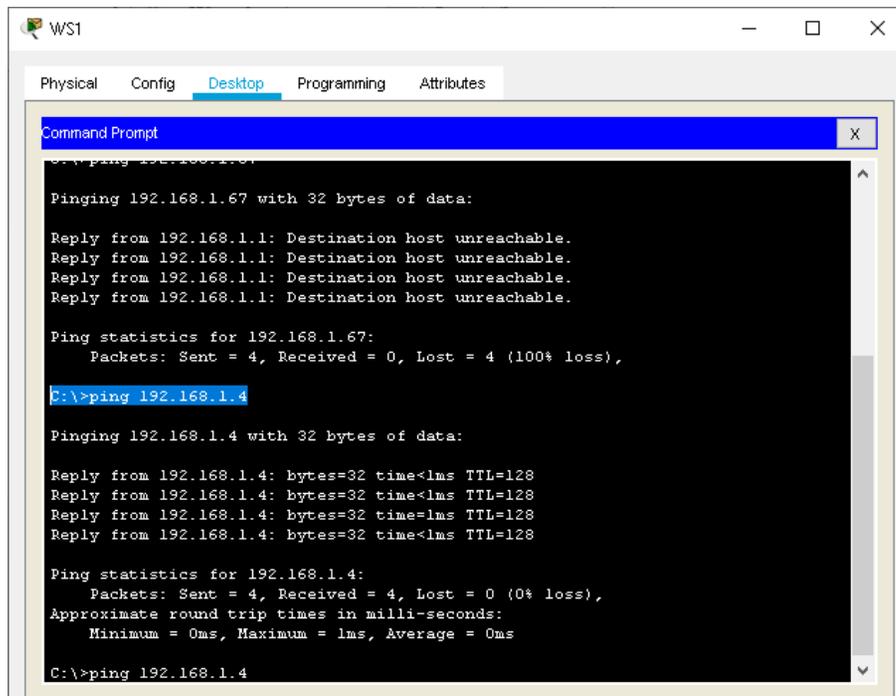
Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Ping WS1(Bogota) a Server0(Bogota)



```
WS1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.4

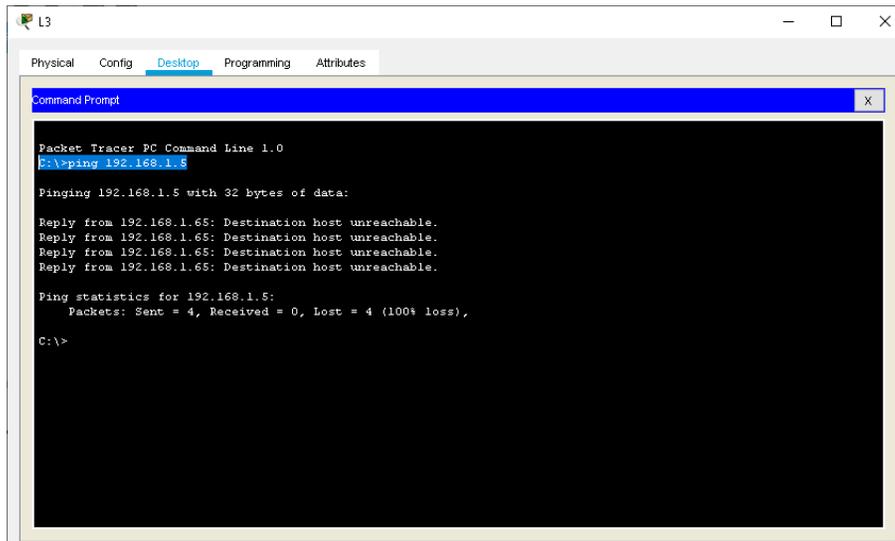
Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

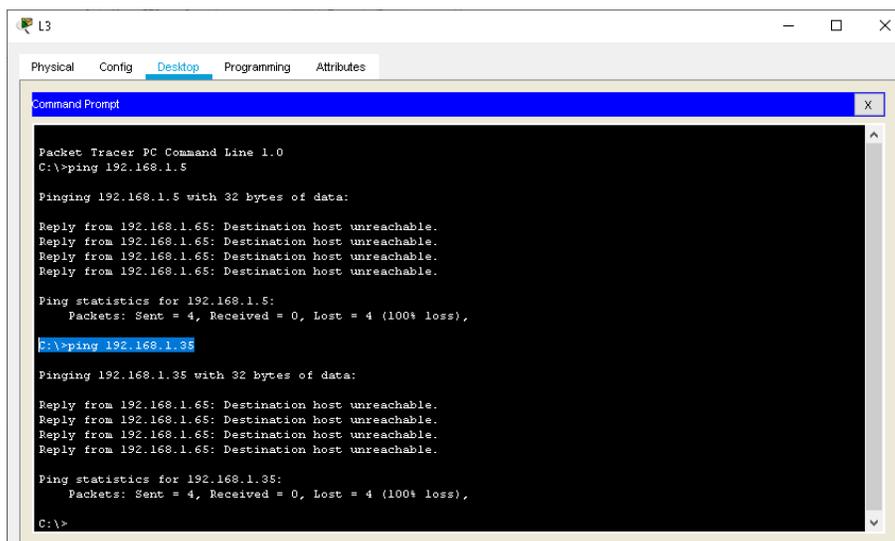
C:\>ping 192.168.1.4
```

## Ping L3(Cali) a WS1 (Bogota)



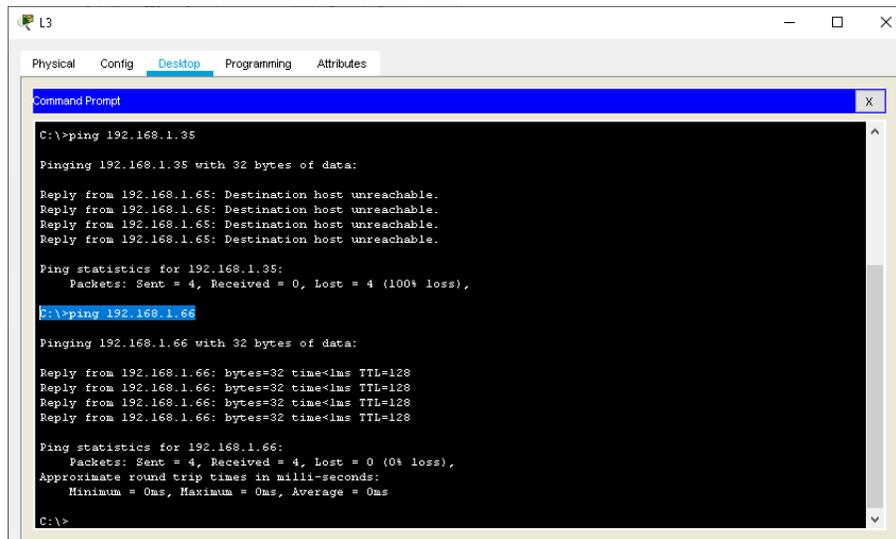
```
L3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.65: Destination host unreachable.
Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

## Ping L3(Cali) a L2 (Medellin)



```
L3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.65: Destination host unreachable.
Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.65: Destination host unreachable.
Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

## Ping L3(Cali) a L4(Cali)



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66

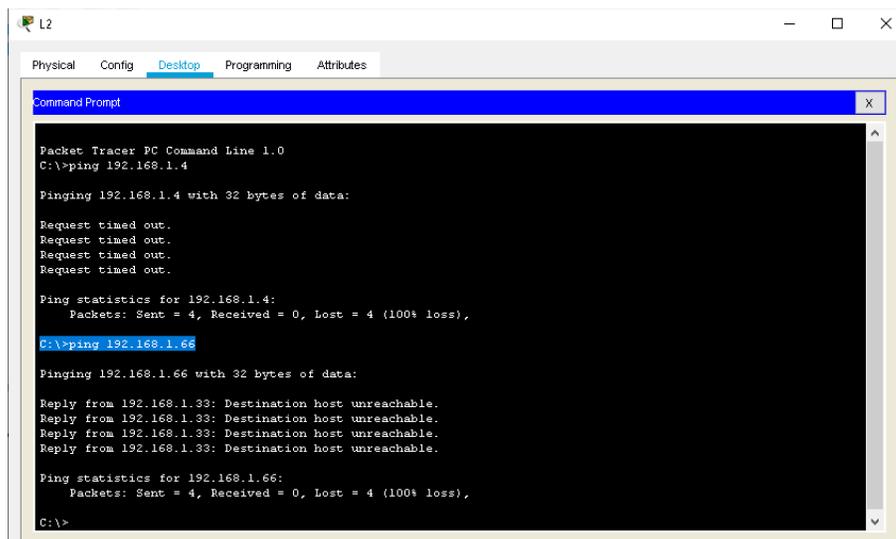
Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

## Ping L2(Medellin) a L4(Cali)



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

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

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66

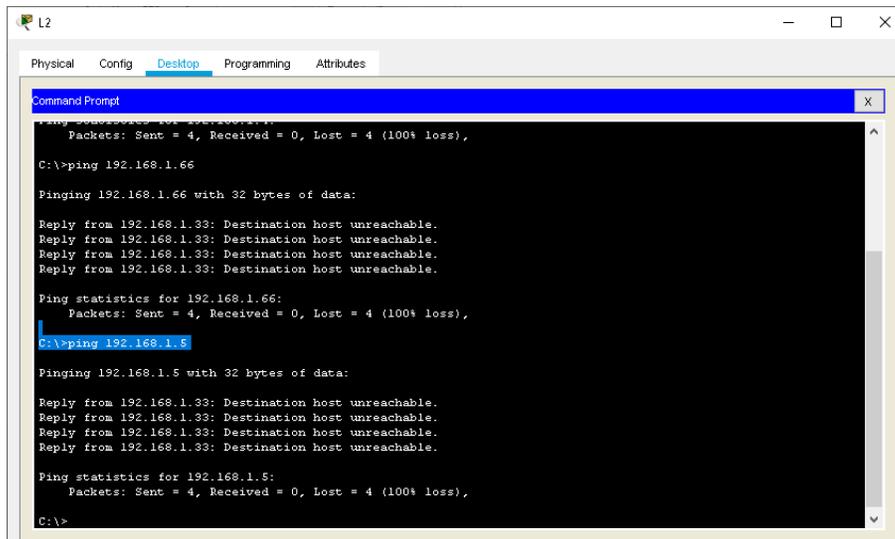
Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Ping L2(Medellin) a WS1(Bogota)



```
Command Prompt
C:\>ping 192.168.1.66
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.

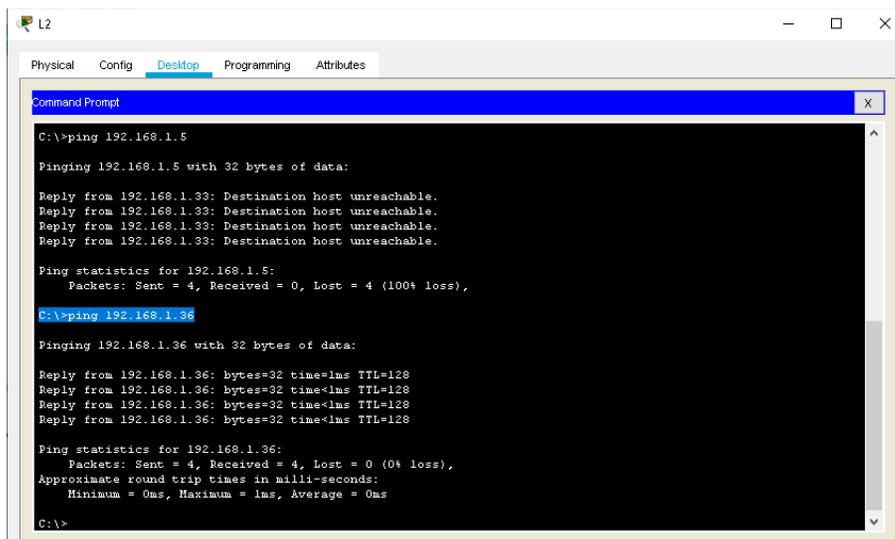
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Ping L2(Medellin) a L1(Medellin)



```
Command Prompt
C:\>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.36
Pinging 192.168.1.36 with 32 bytes of data:
Reply from 192.168.1.36: bytes=32 time=1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

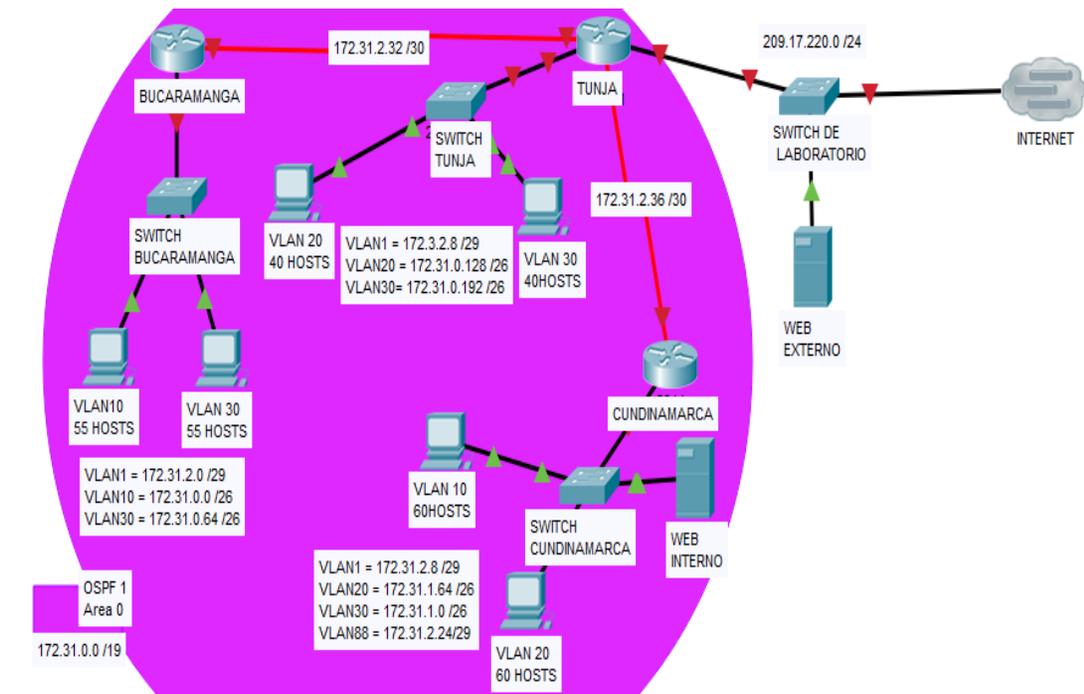
**Conclusion del proceso:** el Server0 puede comunicarse con todos los host, pero los host de cada ciudad no pueden conectarse con otros fuera de su red.

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

|               | <b>ORIGEN</b>                  | <b>DESTINO</b>                 | <b>RESULTADO</b>             |
|---------------|--------------------------------|--------------------------------|------------------------------|
| <b>TELNET</b> | <b>Router MEDELLIN</b>         | <b>Router CALI</b>             | Se conecta                   |
|               | <b>WS_1</b>                    | <b>Router BOGOTA</b>           | No se conecta, time out      |
|               | <b>Servidor</b>                | <b>Router CALI</b>             | No se conecta, time out      |
|               | <b>Servidor</b>                | <b>Router MEDELLIN</b>         | No se conecta, time out      |
| <b>TELNET</b> | <b>LAN del Router MEDELLIN</b> | <b>Router CALI</b>             | No se conecta, time out      |
|               | <b>LAN del Router CALI</b>     | <b>Router CALI</b>             | No se conecta, time out      |
|               | <b>LAN del Router MEDELLIN</b> | <b>Router MEDELLIN</b>         | No se conecta, time out      |
|               | <b>LAN del Router CALI</b>     | <b>Router MEDELLIN</b>         | No se conecta, time out      |
| <b>PING</b>   | <b>LAN del Router CALI</b>     | <b>WS_1</b>                    | No se conecta, time out      |
|               | <b>LAN del Router MEDELLIN</b> | <b>WS_1</b>                    | No se conecta, time out      |
|               | <b>LAN del Router MEDELLIN</b> | <b>LAN del Router CALI</b>     | Se conecta Ping 5/5          |
| <b>PING</b>   | <b>LAN del Router CALI</b>     | <b>Servidor</b>                | No se conecta, time out      |
|               | <b>LAN del Router MEDELLIN</b> | <b>Servidor</b>                | No se conecta, time out      |
|               | <b>Servidor</b>                | <b>LAN del Router MEDELLIN</b> | Destination host unreachable |
|               | <b>Servidor</b>                | <b>LAN del Router CALI</b>     | Destination host unreachable |
|               | <b>Router CALI</b>             | <b>LAN del Router MEDELLIN</b> | Destination host unreachable |
|               | <b>Router MEDELLIN</b>         | <b>LAN del Router CALI</b>     | Se conecta Ping 5/5          |

## Escenario 2

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



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
  - Configuración básica.
  - Autenticación local con AAA.
  - Cifrado de contraseñas.
  - Un máximo de internos para acceder al router.
  - Máximo tiempo de acceso al detectar ataques.
  - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).
4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:

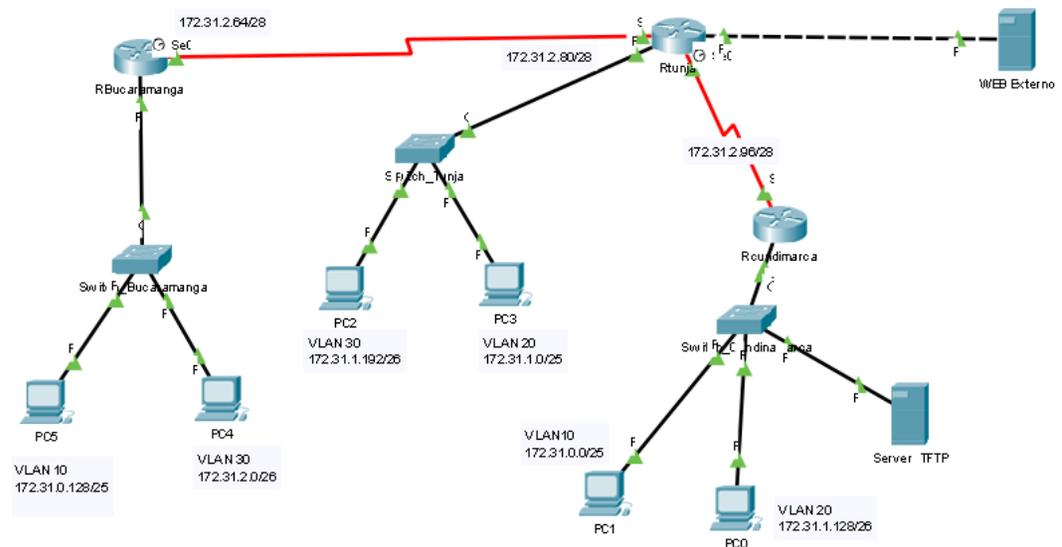
- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
- Los hosts de VLAN 20 en Tunja solo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

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

**Aspectos a tener en cuenta**

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

## Desarrollo



**Proceso:** Se procede a realizar las configuraciones básicas de los equipos que conforman la red.

Configuración de parametros basico.

- Cambiar nombre
- Desactivar la búsqueda del DNS
- Asignar contraseña del modo EXEC
- Asignar contraseña de consola y la contraseña de vty.
- Configurar aviso (MOTD)
- Configurar logging synchronous

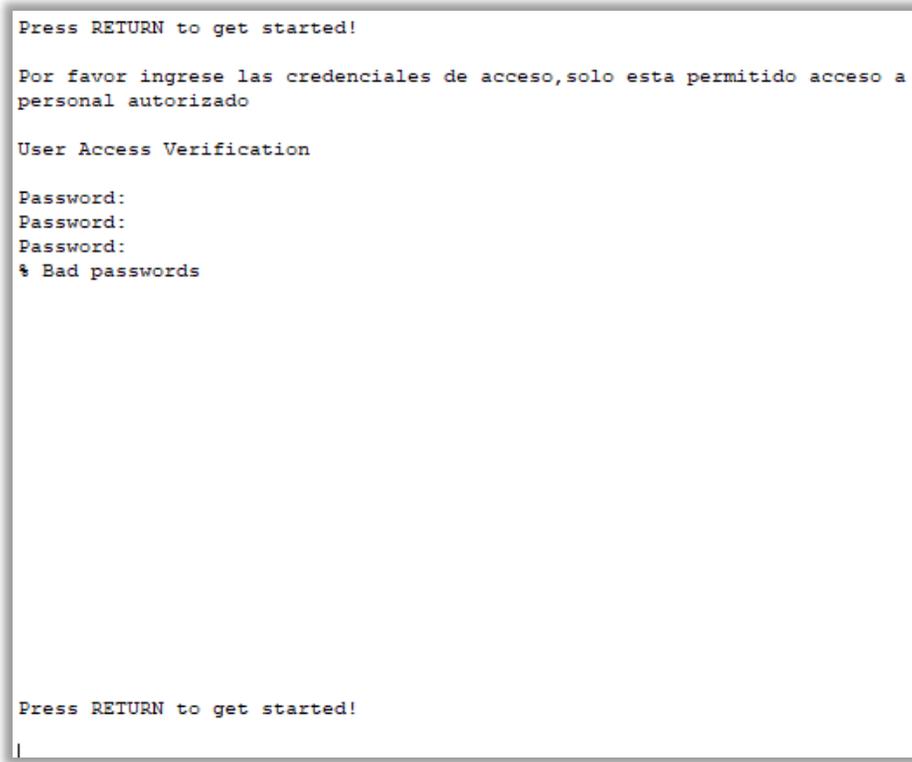
Pasos para configuracion de la interfaz

- Configurar la dirección IP
- Establecer frecuencia de reloj, si aplica

### Configuración básica Switch Cundinamarca:

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#hostname SWcundinamarca
SWcundinamarca(config)#line console 0
SWcundinamarca(config-line)#password
SWcundinamarca(config-line)#login
SWcundinamarca(config)#line vty 0 15
SWcundinamarca(config-line)#password
```

```
SWcundinamarca(config-line)#login
SWcundinamarca(config)#write
Building configuration...
[OK]
SWcundinamarca(config)#service password-encryption
SWcundinamarca(config)#banner motd #Por favor ingrese las credenciales
de acceso,solo esta permitido acceso a personal autorizado#
SWcundinamarca(config)#
```



```
Press RETURN to get started!

Por favor ingrese las credenciales de acceso,solo esta permitido acceso a
personal autorizado

User Access Verification

Password:
Password:
Password:
⚡ Bad passwords

Press RETURN to get started!
|
```

### Configuración básica de Switch Tunja

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#hostname SWtunja
SWtunja(config)#line console 0
SWtunja(config-line)#password
SWtunja(config-line)#login
SWtunja(config)#line vty 0 15
SWtunja(config-line)#password
SWtunja(config-line)#login
SWtunja(config)#write
Building configuration...
[OK]
```

```
SWtunja(config)#service password-encryption
SWtunja(config)#banner motd #Por favor ingrese las credenciales de
acceso,solo esta permitido el acceso a personal autorizado#
```

### **Configuración básica de Switch Bucaramanga**

```
Switch(config)#hostname SWbucaramanga
SWbucaramanga(config)#line console 0
SWbucaramanga(config-line)#password
SWbucaramanga(config-line)#login
SWbucaramanga(config)#line vty 0 15
SWbucaramanga(config-line)#password
SWbucaramanga(config-line)#login
SWbucaramanga(config)#service password-encryption
SWbucaramanga(config)#no ip domain-lookup
SWbucaramanga(config)#baner motd #Por favor ingrese las credenciales
de acceso,solo esta permitido el acceso a personal autorizado#
SWbucaramanga#write
Building configuration...
[OK]
```

### **Configuración básica de Switch Laboratorio:**

```
Switch>
Switch>enable
Switch# conf terminal
Switch(config)#hostname SLab
SLab(config-if)#int vlan1
SLab(config-if)#ip add 209.17.220.1 255.255.255.0
```

### **Switch Cundinamarca creación de VLAN y asignación de interfaces**

```
SWcundinamarca(config)#vlan 10
SWcundinamarca(config-vlan)# name 10
SWcundinamarca(config)#interface vlan 10
SWcundinamarca(config)#interface range fa0/1-10
SWcundinamarca(config-if-range)#switchport mode access
SWcundinamarca(config-if-range)#switchport access vlan 10
SWcundinamarca(config-if-range)#do write
SWcundinamarca(config)#vlan 20
SWcundinamarca(config-vlan)#name 20
SWcundinamarca(config)#interface vlan 20
SWcundinamarca(config)#interface range fa0/11-18
SWcundinamarca(config-if-range)#switchport mode access
SWcundinamarca(config-if-range)#switchport access vlan 20
SWcundinamarca(config-if-range)#do write
SWcundinamarca(config)#vlan 1
```

```
SWcundinamarca(config-vlan)#interface vlan 1
SWcundinamarca(config-if)#interface gi0/1
SWcundinamarca(config-if)#switchport mode trunk
SWcundinamarca(config-if)#switchport access vlan 1
SWcundinamarca(config-if)#do write
```

### **Switch Tunja creación de VLAN y asignación de interfaces**

```
SWtunja(config)#vlan 20
SWtunja(config-vlan)#name 20t
SWtunja(config-vlan)#interface vlan 20
SWtunja(config)#interface range fa0/1-10
SWtunja(config-if-range)#switchport mode access
SWtunja(config-if-range)#switchport access vlan 20
SWtunja(config-if)#vlan 30
SWtunja(config-vlan)#name 30t
SWtunja(config-vlan)#interface vlan 30
SWtunja(config-if)#interface range fa0/11-18
SWtunja(config-if-range)#switchport mode access
SWtunja(config-if-range)#switchport access vlan 30
```

### **Switch Bucaramanga creación de VLAN y asignación de interfaces**

```
SWbucaramanga(config)#vlan 10
SWbucaramanga(config-vlan)#name 10b
SWbucaramanga(config-vlan)#interface vlan 10
SWbucaramanga(config-if)#interface range fa0/1-10
SWbucaramanga(config-if-range)#switchport mode access
SWbucaramanga(config-if-range)#switchport access vlan 10
SWbucaramanga(config)#vlan 30
SWbucaramanga(config-vlan)#name 30b
SWbucaramanga(config-vlan)#interface vlan 30
SWbucaramanga(config-vlan)#interface range fa0/11-18
SWbucaramanga(config-if-range)#switchport mode access
SWbucaramanga(config-if-range)#switchport access vlan 30
```

### **Configuración Router Cundinamarca**

```
Router>enable
Router#configure terminal
Router(config)#hostname rcundi
rcundi(config)#no ip domain-lookup
rcundi(config)#line console 0
rcundi(config-line)#password
rcundi(config-line)#login
rcundi(config-line)#banner motd #Ingrese las credenciales, solo se permite
acceso a personal autorizado#
```

### **Configuración Router Tunja**

```
Router>enable
Router#configure terminal
Router(config)#hostname rtunja
rcundi(config)#no ip domain-lookup
rcundi(config)#line console 0
rcundi(config-line)#password
rcundi(config-line)#login
rcundi(config-line)#banner motd #Ingrese las credenciales, solo se permite
acceso a personal autorizado#
```

### **Configuración Router Bucaramanga**

```
Router>enable
Router#configure terminal
Router(config)#hostname rbuca
rcundi(config)#no ip domain-lookup
rcundi(config)#line console 0
rcundi(config-line)#password
rcundi(config-line)#login
rcundi(config-line)#banner motd #Ingrese las credenciales, solo se permite
acceso a personal autorizado#
```

### **Asignación de direcciones IP rcundi y DHCP**

```
rcundi(config-if)#interface fa0/0.1
rcundi(config-subif)#encapsulation dot1q 1 native
rcundi(config-subif)#ip address 172.31.2.65 255.255.255.240
rcundi(config-subif)#interface fa0/0.10
rcundi(config-subif)#encapsulation dot1q 10
rcundi(config-subif)#ip address 172.31.0.1 255.255.255.128
rcundi(config-subif)#interface fa0/0.20
rcundi(config-subif)#encapsulation dot1q 20
rcundi(config-subif)#ip address 172.31.1.129 255.255.255.192
rcundi(config)#ip dhcp pool cundinamarca
rcundi(dhcp-config)#network 172.31.0.0 255.255.255.128
rcundi(dhcp-config)#default-router 172.31.0.1
rcundi(dhcp-config)#dns-server 8.8.8.8
rcundi(config)#ip dhcp pool vlan20
rcundi(dhcp-config)#network 172.31.1.128 255.255.255.192
rcundi(dhcp-config)#default-router 172.31.1.129
rcundi(dhcp-config)#dns-server 4.4.4.4
```



### Asignación de direcciones IP Tunja

```
rcundi(config-if)#interface fa0/0.1
rcundi(config-subif)#encapsulation dot1q 1 native
rcundi(config-subif)#ip address 172.31.2.65 255.255.255.240
rcundi(config-subif)#interface fa0/0.20
rcundi(config-subif)#encapsulation dot1q 20
rcundi(config-subif)#ip address 172.31.1.1 255.255.255.128
rcundi(config-subif)#interface fa0/0.30
rcundi(config-subif)#encapsulation dot1q 30
rcundi(config-subif)#ip address 172.31.1.193 255.255.255.192
```

### Asignación de direcciones IP Bucaramanga

```
rcundi(config-if)#interface fa0/0.1
rcundi(config-subif)#encapsulation dot1q 1 native
rcundi(config-subif)#ip address 172.31.2.65 255.255.255.240
rcundi(config-subif)#interface fa0/0.10
rcundi(config-subif)#encapsulation dot1q 20
rcundi(config-subif)#ip address 172.31.1.1 255.255.255.128
rcundi(config-subif)#interface fa0/0.20
rcundi(config-subif)#encapsulation dot1q 30
rcundi(config-subif)#ip address 172.31.1.193 255.255.255.192
rcundi(config)#ip dhcp pool cundinamarca
rcundi(dhcp-config)#network 172.31.0.0 255.255.255.128
rcundi(dhcp-config)#default-router 172.31.0.1
rcundi(dhcp-config)#dns-server 8.8.8.8
rcundi(config)#ip dhcp pool vlan20
rcundi(dhcp-config)#network 172.31.1.128 255.255.255.192
rcundi(dhcp-config)#default-router 172.31.1.129
rcundi(dhcp-config)#dns-server 4.4.4.4
```

## CONCLUSIONES

- El protocolo EIGRP permite incrementar el potencial de las redes, generando una reducción en el tiempo de convergencia y facilitando la liberación de enlaces de menor velocidad
- El uso de NAT es imprescindible en una organización ya que permite la administración de las redes de manera organizada y ha prolongado la vida de IPV4 entre tanto logra hacerse la transición mundial a IPV6.
- La configuración de NAT estática es la mejor solución para aquellos dispositivos y servicios de alto impacto y que no se pueden dejar a merced por ip's dinámicas. Una ACL es usada por seguridad como una forma de determinar los permisos de acceso apropiados a los elementos de una red
- Una ACL permite hacer control y filtrar el tráfico en los router de una red, administrando o el mismo de acuerdo a alguna condición que se requiera como una
- Durante el desarrollo del laboratorio se identifica el control que permite una ACL sobre el tráfico de una red, negando o permitiendo el mismo de acuerdo la ip del host configurado
- El uso del protocolo OSPF permite dividir sistemas grandes en partes diferentes donde cada una es una red o un conjunto de redes inmediatas las cuales permiten una mejor administración.
- Cuando las redes son grandes y se usa el protocolo OSPF, los router usados crean enlaces que relacionan a los nodos vecinos, estableciendo distintos tipos de relación con ellos.
- La interfaz pasiva son las cuales en las que el protocolo de enrutamiento no genera actualizaciones de enrutamiento por seguridad, evitando que los usuarios finales puedan acceder a información de la red que no sea conveniente.

## REFERENCIAS BIBLIOGRÁFICAS

- CISCO. (2014). *DHCP. Principios de Enrutamiento y Conmutación*. Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>
- CISCO. (2014). *Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación*. . Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>
- CISCO. (2014). *Listas de control de acceso. Principios de Enrutamiento y Conmutación*. Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>
- CISCO. (2014). *OSPF de una sola área. Principios de Enrutamiento y Conmutación*. . Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). *Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación*. . Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>
- Lammle, T. (2010). *CISCO Press (Ed). Cisco Certified Network Associate Study Guide*. . Obtenido de <https://1drv.ms/b/s!AmlJYei->
- Lucas, M. (2009). *Cisco Routers for the Desperate : Router and Switch Management, the Easy Way*. San Francisco: No Starch Press. . Obtenido de <https://1drv.ms/b/s!AmlJYei-NT1Im3L74BZ3bpMiXRx0>
- Odom, W. (2013). *CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide*. . Obtenido de <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>