

PRUEBA DE HABILIDADES PRACTICAS CCNP

JUAN MIGUEL MEJIA

UNIVERSIDAD ABIERTA Y DISTANCIA
ESCUELA BASICA DE TECNOLOGIAS E INGENIERIAS (ECBTI)
INGENIERA DE SISTEMAS
PEREIRA, RISARALDA
2021

PRUEBAS DE HABILIDADES PRACTICAS

JUAN MIGUEL MEJIA

DIPLOMADO CCNA DE CISCO CON MIRAS DE OPTAR POR EL TITULO DE
INGENIERIA DE SISTEMAS

PhD JUAN CARLOS VESGA FERREIRA DOCENTE ASOCIADO ECBTI

UNIVERSIDAD ABIERTA Y DISTANCIA
ESCUELA BASICA DE TECNOLOGIAS E INGENIERIAS (ECBTI)
INGENIERA DE SISTEMAS
PEREIRA, RISARALDA
2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN	7
2. OBJETIVOS.....	8
2.1 OBJETIVO GENERAL	8
2.2 OBJETIVOS ESPECÍFICOS	8
3. PLANTEAMIENTO DEL PROBLEMA	9
3.1 DEFINICION DEL PROBLEMA,.....	9
4. INTRODUCCIÓN	12
4.1 MATERIALES	12
4.2 METODOLOGIA.....	12
5 DESARROLLO DEL PROYECTO	20
5.1 ANÁLISIS Y DEL DESARROLLO DEL PROYECTO	20
5.1.1 ESCENARIO 1	20
5.1.2 ESCENARIO 2	48
CONCLUSIONES	75
BIBLIOGRAFIA	76

TABLA DE ILUSTRACIONES

Ilustración 1. Escenario 1	9
Ilustración 2. Escenario 2.....	10
Ilustración 3. Topología de Infraestructura Escenario 1	20
Ilustración 4. Conexiones físicas.....	21
Ilustración 5.Tabla enrutamiento Medellín	24
Ilustración 6. Tabla de Enrutamiento Bogotá	24
Ilustración 7. Tabla de Enrutamiento Cali	25
Ilustración 8.Salidas balanceo de cargas Medellín	25
Ilustración 9.Salidas Balanceo de Cargas. Bogotá	26
Ilustración 10. Salidas balanceo de cargas. Cali.....	26
Ilustración 11. Diagnóstico de vecinos. Medellín	27
Ilustración 12. Diagnósticos de vecinos -1. Bogotá.....	27
Ilustración 13.Diagnósticos de vecinos -2. Bogotá.....	28
Ilustración 14. Diagnóstico de vecinos. Cali.....	29
Ilustración 15. Salida prueba de conectividad.....	30
Ilustración 16. Tabla de enrutamiento. Medellín	32
Ilustración 17. Tabla de enrutamiento. Bogotá.....	32
Ilustración 18.Tabla de Enrutamiento. Cali	33
Ilustración 19. Prueba de conectividad de la Red. Medellín	34
Ilustración 20. Prueba de conectividad Red. Bogotá	35
Ilustración 21. Topología Escenario 2.....	48
Ilustración 22. Salida Prueba de conexión.....	52
Ilustración 23. Salida para validación de configuración	52
Ilustración 24. Salida prueba validación NAT y PAT	53
Ilustración 25. Tabla de enrutamiento Bucaramanga.....	55
Ilustración 26. Tabla e enrutamiento. Tunja.....	56
Ilustración 27. Tabla de Enrutamiento. Cundinamarca	57
Ilustración 28. Salidas exitosas. Pruebas VLAN 20	58
Ilustración 29. Dirección IP VLAN 30. Cundinamarca.....	59
Ilustración 30.Bloqueo de tráfico hacia equipos en Tunja.....	60
Ilustración 31.Permiso de conexión hacia internet.....	60
Ilustración 32. Pruebas VLAN30. Tunja	61
Ilustración 33. Bloqueo otras ciudades y permisos de conexión.....	62
Ilustración 34. IP VLAN20. Tunja	63
Ilustración 35. Permiso de Accesos VLAN20 Cundinamarca y VLAN10 Bucaramanga.....	63

Ilustración 36. Bloqueo trafico.....	64
Ilustración 37. IP VLAN30 Bucaramanga.....	64
Ilustración 38. Salida exitosa VLAN10	65
Ilustración 39. Bloqueo del tráfico adicional.....	65
Ilustración 40. IP VLAN10. Bucaramanga.....	66
Ilustración 41. PING rechazo internet	66
Ilustración 42. PING VLAN20 Cundinamarca	67
Ilustración 43. PING VLAN20 Tunja.....	67
Ilustración 44. Rechazo VLAN10 Gateway. Bucaramanga.....	69
Ilustración 45. RechazoVLAN10 Gateway. Tunja	70
Ilustración 46.Rechazo VLAN20 a su Gateway. Cundinamarca	71
Ilustración 47. Salida exitosa servidor interno.....	71
Ilustración 48. Configuración de redes internas	73

ÍNDICE DE TABLAS

Tabla 1. Configuración básica.....	23
Tabla 2. Comprobación de la Red instalada. Escenario 1	47

1. INTRODUCCIÓN

Realizaremos dos ejercicios con miras a dar solución a diferentes situaciones planteadas en escenarios complejos, el objetivo de este trabajo es lograr obtener una correcta aplicación de conocimientos adquiridos durante el diplomado CCNA. Utilizaremos una herramienta tecnología para la construcción y diseño de las diferentes soluciones y se explicara de manera detallada el procedimiento realizado en cada escenario propuesto.

Crearemos configuraciones en simuladores de dispositivos Cisco y realizaremos configuraciones en estaciones de trabajo cliente por medio de las cuales podremos realizar las diferentes validaciones de comunicación y funcionalidad; también realizaremos las respectivas adecuaciones de seguridad y todo el proceso documental del ejercicio.

2. OBJETIVOS

2.1 OBJETIVO GENERAL.

Mediante el desarrollo de diferentes configuraciones en equipos de comunicación CISCO, pretendemos resolver algunas necesidades de 2 empresas con redes a nivel a nacional. El propósito de este ejercicio es entregar la solución y su respectiva documentación.

2.2 OBJETIVOS ESPECÍFICOS

- Crear una red de sucursales para una compañía con 3 sedes a nivel nacional con las debidas normas de configuración y topología de red.
- Realizar e implementar el correcto diseño de una topología de red que permita dar solución de conectividad a una red ethernet en una compañía por medio de una salida a internet a través de sus dispositivos interconectados.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICION DEL PROBLEMA

- Escenario 1:

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el administrador de la red 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.

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.

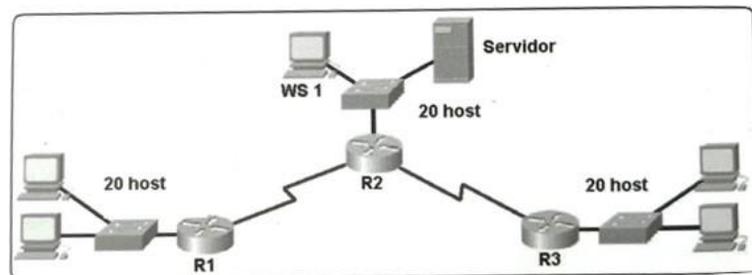


Ilustración 1. Escenario 1

- Escenario 2:

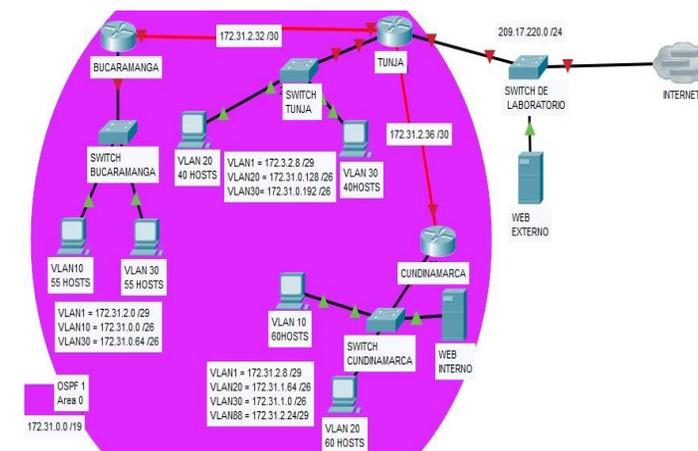


Ilustración 2. Escenario 2

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

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.

4. INTRODUCCIÓN

4.1 MATERIALES

Para el desarrollo del presente proyecto utilizamos diferentes herramientas tanto ofimáticas como técnicas especializadas, a continuación, las mas relevantes:

- Packet tracer.
- Google Chrome.
- Notepad.
- Microsoft Office.

4.2 METODOLOGIA

Durante el desarrollo del ejercicio para el segundo escenario, se necesitaron realizar algunas configuraciones para los routers de cada nodo, los cuales se detallan a continuación:

- Router Tunja:

```
TUNJA#show ru
TUNJA#show running-config
Building configuration...

Current configuration : 2970 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname TUNJA
!
login block-for 30 attempts 10 within 60
!
!
enable secret 5 $1$mERr$oc/Jnu9htDuoTn8ejwwR11
enable password 7 0802455D0A165747405A290A2B29282D
!
!
aaa new-model
!
aaa authentication login default local
!
!
no ip cef
```

```

no ipv6 cef
!
!
username miguel password 7 0802455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524R0GC-
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
ip address 172.3.2.9 255.255.255.248
ip access-group 104 in
duplex auto
speed auto
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 172.31.0.129 255.255.255.192
ip access-group 102 in
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 172.31.0.193 255.255.255.192
ip access-group 101 in
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 209.17.220.1 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface Serial0/3/0
bandwidth 1000
ip address 172.31.2.37 255.255.255.252
ip ospf message-digest-key 1 md5 CISCO
ip ospf 1 area 0
ip nat inside
!
interface Serial0/3/1
bandwidth 1000
ip address 172.31.2.34 255.255.255.252
ip ospf message-digest-key 1 md5 CISCO
ip ospf 1 area 0
ip nat inside
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 172.3.2.9
log-adjacency-changes
area 0 authentication message-digest
passive-interface default

```

```

no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.63 area 0
network 172.31.0.192 0.0.0.63 area 0
network 209.17.220.0 0.0.0.255 area 0
!
ip nat pool public_access 209.17.220.15 209.17.220.15 netmask 255.255.255.0
ip nat inside source list 1 pool public_access overload
ip nat inside source static 172.31.2.26 209.17.220.10
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 1 permit 172.0.0.0 0.0.0.255
access-list 101 permit ip 172.31.0.192 0.0.0.63 host 209.17.220.2
access-list 101 permit udp any any
access-list 101 permit ospf any any
access-list 101 permit ip 172.31.0.192 0.0.0.63 172.31.1.64 0.0.0.63
access-list 101 deny ip 172.31.0.192 0.0.0.63 any
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
access-list 102 permit udp any any
access-list 102 permit ospf any any
access-list 102 deny ip 172.31.0.128 0.0.0.63 any
access-list 4 permit 172.3.2.8 0.0.0.7
access-list 104 deny ip 172.3.2.8 0.0.0.7 172.0.0.0 0.255.255.255
access-list 104 permit ip 172.3.2.8 0.0.0.7 any
!
!
line con 0
!
line aux 0
!
line vty 0 4
access-class 4 in
password 7 0802455D0A165747405A
!
!
end
TUNJA#

```

- Router Bucaramanga:

```

BUCARAMANGA#show running-config
Building configuration...

Current configuration : 2923 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!

```

```

hostname BUCARAMANGA
!
login block-for 30 attempts 5 within 60
!
!
enable secret 5 $1$mERr$oc/Jnu9htDuoTn8ejwwR11
enable password 7 0802455D0A165747405A290A2B29282D
!
!
ip dhcp excluded-address 172.31.0.1
ip dhcp excluded-address 172.31.0.65
!
ip dhcp pool vlan10
network 172.31.0.0 255.255.255.192
default-router 172.31.0.1
dns-server 8.8.8.8
ip dhcp pool vlan30
network 172.31.0.64 255.255.255.192
default-router 172.31.0.65
dns-server 8.8.8.8
!
!
aaa new-model
!
aaa authentication login default local
!
!
no ip cef
no ipv6 cef
!
!
username miguel password 7 0802455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524Y7QC-
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
ip address 172.31.2.1 255.255.255.248
ip access-group 104 in
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 172.31.0.1 255.255.255.192
ip access-group 101 in
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 172.31.0.65 255.255.255.192
ip access-group 102 in
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!

```

```

interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
no ip address
ip ospf message-digest-key 1 md5 CISCO
clock rate 2000000
shutdown
!
interface Serial0/3/1
bandwidth 1000
ip address 172.31.2.33 255.255.255.252
ip ospf message-digest-key 1 md5 CISCO
ip ospf 1 area 0
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 172.31.2.1
log-adjacency-changes
area 0 authentication message-digest
passive-interface default
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
network 172.31.2.0 0.0.0.7 area 0
network 172.31.0.0 0.0.0.63 area 0
network 172.31.0.64 0.0.0.63 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 102 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
access-list 102 deny ip 172.31.0.64 0.0.0.63 172.0.0.0 0.255.255.255
access-list 102 permit ip 172.31.0.64 0.0.0.63 any
access-list 102 permit udp any any
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
access-list 101 permit udp any any
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.64 0.0.0.63
access-list 101 deny ip 172.31.0.0 0.0.0.63 any
access-list 4 permit 172.31.2.0 0.0.0.7
access-list 104 deny ip 172.31.2.0 0.0.0.7 172.0.0.0 0.255.255.255
access-list 104 permit ip 172.31.2.0 0.0.0.7 any
!
!
line con 0
!
line aux 0
!

```

```
line vty 0 4
access-class 4 in
password 7 0802655D0A165747405A
!
!
end
BUCARAMANGA#
```

- Router Cundinamarca:

```
CUNDINAMARCA#show running-config
Building configuration...
```

```
Current configuration : 3630 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname CUNDINAMARCA
!
login block-for 30 attempts 5 within 60
!
!
enable secret 5 $1$mERr$oc/Jnu9htDuoTn8ejwwR11
enable password 7 0802455D0A165747405A290A2B29282D
!
!
ip dhcp excluded-address 172.31.2.9
ip dhcp excluded-address 172.31.1.65
ip dhcp excluded-address 172.31.1.1
ip dhcp excluded-address 172.31.2.25
!
ip dhcp pool vlan20
network 172.31.1.64 255.255.255.192
default-router 172.31.1.65
dns-server 8.8.8.8
ip dhcp pool vlan30
network 172.31.1.0 255.255.255.192
default-router 172.31.1.1
dns-server 8.8.8.8
ip dhcp pool vlan88
network 172.31.2.24 255.255.255.248
default-router 172.31.2.25
dns-server 8.8.8.8
!
!
aaa new-model
!
aaa authentication login default local
!
!
no ip cef
no ipv6 cef
!
!
username miguel password 7 0802455D0A16
!
!
```

```

license udi pid CISCO2911/K9 sn FTX1524S9N2-
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
ip address 172.31.2.9 255.255.255.248
ip access-group 104 in
duplex auto
speed auto
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 172.31.1.65 255.255.255.192
ip access-group 101 in
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 172.31.1.1 255.255.255.192
ip access-group 102 in
!
interface GigabitEthernet0/0.88
encapsulation dot1Q 88
ip address 172.31.2.25 255.255.255.248
ip access-group 103 in
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
bandwidth 1000
ip address 172.31.2.38 255.255.255.252
ip ospf message-digest-key 1 md5 CISCO
ip ospf 1 area 0
clock rate 2000000
!
interface Serial0/3/1
no ip address
ip ospf message-digest-key 1 md5 CISCO
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 172.31.2.9
log-adjacency-changes
area 0 authentication message-digest
passive-interface default
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1

```

```

no passive-interface GigabitEthernet0/0.20
network 172.31.2.8 0.0.0.7 area 0
network 172.31.2.24 0.0.0.7 area 0
network 172.31.1.64 0.0.0.63 area 0
network 172.31.1.0 0.0.0.63 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 102 deny ip 172.31.1.0 0.0.0.63 172.3.2.8 0.0.0.7
access-list 102 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 102 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
access-list 102 permit ip 172.31.1.0 0.0.0.63 any
access-list 102 permit udp any any
access-list 102 permit ospf any any
access-list 101 permit ip 172.31.1.64 0.0.0.63 172.3.2.8 0.0.0.7
access-list 101 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
access-list 101 permit ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.0.63
access-list 101 permit udp any any
access-list 101 permit ospf any any
access-list 101 deny ip 172.31.1.64 0.0.0.63 any
access-list 4 permit 172.31.2.8 0.0.0.7
access-list 4 permit 172.31.2.24 0.0.0.7
access-list 103 deny ip 172.31.2.24 0.0.0.7 172.0.0.0 0.255.255.255
access-list 103 permit ip any any
access-list 104 deny ip 172.31.2.8 0.0.0.7 172.0.0.0 0.255.255.255
access-list 104 permit ip any any
!
!
line con 0
!
line aux 0
!
line vty 0 4
access-class 4 in
password 7 0802455D0A165747405A
!
!
end
CUNDINAMARCA#

```

5 DESARROLLO DEL PROYECTO

Después de realizar los respectivos análisis y varios diseños, se procedió a la configuración de las herramientas y equipos de comunicación que nos permitieron desarrollar los ejercicios de manera satisfactoria. A continuación, se detalla el proceso de solución para cada uno de los escenarios problema.

5.1 ANÁLISIS Y DEL DESARROLLO DEL PROYECTO.

5.1.1 ESCENARIO 1:

Con el fin de llevar a cabo la resolución de este punto, se diseña la siguiente infraestructura haciendo uso de “Packet Tracer”, el cual emula las 3 sedes:

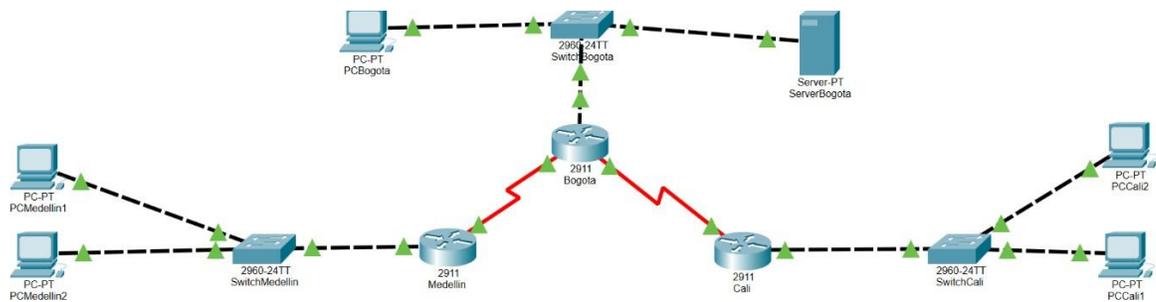


Ilustración 3. Topología de Infraestructura Escenario 1

Se elige router Cisco 2911 y se adicionan módulos de puertos seriales y módulos con puertos FastEthernet. Las interconexiones entre Medellín, Bogotá y Cali se realizan con conexiones seriales DTE dado que así aparecen las graficas del laboratorio. Se hace uso de Switches 2960 para conectar los equipos internamente en cada sede.

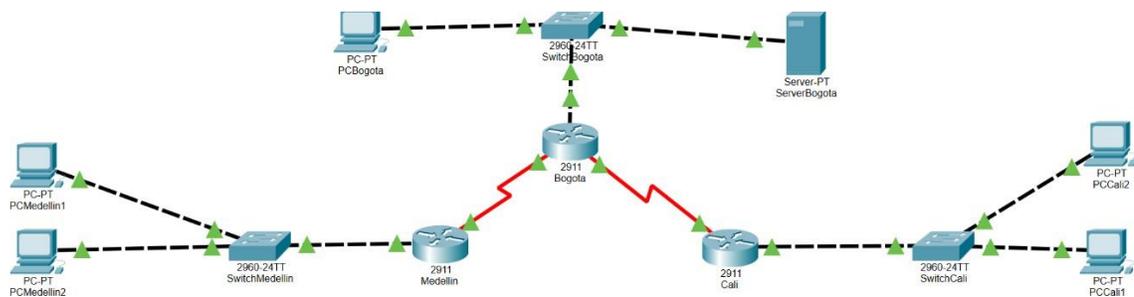
Se cambia el nombre de cada Router por: MEDELLIN, BOGOTA y CALI, y se asignan claves de seguridad mediante los siguientes comandos y se cifran los password en cada router:

- (config)#hostname BOGOTA
- (config)#enable secret Cisco2021*
- (config)#enable secret Cisco2021Enable
- (config)#service password-encryption

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

Respuesta:

La conexión física se muestra a continuación. Se hace uso de cables Seriales DTE para interconexión entre las sedes; MEDELLIN, BOGOTA y CALI. Se hace uso de cable cruzado para conectar los router a los switches y los equipos de punto final a los switches, como se muestra en la grafica de “Packet Tracer”.



Configurar la topología de red, de acuerdo con las 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.

Respuesta:

El direccionamiento IP seleccionado para cada sede es el siguiente:

- **BOGOTA**
 - Red interna: 192.168.1.0/27
 - Red con Medellín: 192.168.1.96/27
 - Red con Cali: 192.168.1.128/27
- **MEDELLIN**
 - Red interna: 192.168.1.32/27
 - Red con Bogotá: 192.168.1.96/27
- **CALI**
 - Red interna: 192.168.1.64/27
 - Red con Bogotá: 192.168.1.128/27

Se lleva a cabo la configuración del direccionamiento IP de cada uno de los router mediante la configuración de los siguientes comandos, manejando un subneting de mascara 27, para un total de 30 hosts disponibles en cada red:

```
BOGOTA(config)#interface serial 0/3/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#exit
BOGOTA#Config terminal
BOGOTA(config)#interface serial 0/3/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#exit
BOGOTA(config)#interface gigabitEthernet 0/0
BOGOTA(config-if)#ip add
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
```

```
CALI(config)#interface serial 0/3/1
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#exit
CALI(config)#interface gigabitEthernet 0/0
CALI(config-if)#ip add
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
```

```
MEDELLIN(config)#interface serial 0/3/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#exit
MEDELLIN(config)#interface gigabitEthernet 0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
```

Parte 2: Configuración Básica.

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

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/3/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/3/1		192.168.1.130	
Dirección de Ip en interfaz GE 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento Sistema Autónomo	Eigrp 200	Eigrp 200	Eigrp 200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Tabla 1. Configuración básica

Nota: Se modifica la tabla con base en la nomenclatura de los módulos agregados a los Routers dentro del laboratorio.

Respuesta:

Una vez configurado el direccionamiento IP de los routers, se procede a configurar el protocolo de enturamiento EIGRP mediante los siguientes comandos:

```
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.0 255.255.255.0
```

```
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.0 255.255.255.0
```

```
CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.0 255.255.255.0
```

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.

Respuesta:

A continuación, se muestra la tabla de enrutamiento de cada uno del los routers en donde podemos observar enrutamiento aprendido dinámicamente:

- **MEDELLIN**

```

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, 6 subnets, 2 masks
D       192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:04:55, Serial0/3/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/3/0
L       192.168.1.99/32 is directly connected, Serial0/3/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:04:42, Serial0/3/0

```

Ilustración 5. Tabla enrutamiento Medellín

- BOGOTA

```

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, 7 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 [90/2170112] via 192.168.1.99, 00:07:35, Serial0/3/0
C       192.168.1.96/27 is directly connected, Serial0/3/0
L       192.168.1.98/32 is directly connected, Serial0/3/0
C       192.168.1.128/27 is directly connected, Serial0/3/1
L       192.168.1.130/32 is directly connected, Serial0/3/1

```

Ilustración 6. Tabla de Enrutamiento Bogotá

- CALI

```

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, 2 subnets, 2 masks
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0

CALI#

```

Ilustración 7. Tabla de Enrutamiento Cali

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

Respuesta:

Para llevar a cabo esta verificación, hacemos uso del comando “show IP route” seleccionando la red 192.168.1.0 en cada uno de los routers:

- **MEDELLIN:** Podemos observar que la red 192.168.1.0/27 es aprendida mediante EIGRP y hay un “Redistributing” via eigrp 200

```

MEDELLIN#show ip route 192.168.1.0
Routing entry for 192.168.1.0/24, 6 known subnets
  Attached (4 connections)
    Variably subnetted with 2 masks
    Redistributing via eigrp 200, eigrp 200, eigrp 200, eigrp 200
D       192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:10:56, Serial0/3/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
        192.168.1.33/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/3/0
        192.168.1.99/32 is directly connected, Serial0/3/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:10:56, Serial0/3/0

MEDELLIN#

```

Ilustración 8. Salidas balanceo de cargas Medellín

- **BOGOTA:** Podemos observar el “Redistributing” vía eigrp 200

```

BOGOTA#show ip route 192.168.1.0
Routing entry for 192.168.1.0/24, 7 known subnets
  Attached (6 connections)
    Variably subnetted with 2 masks
    Redistributing via eigrp 200, eigrp 200, eigrp 200, eigrp 200
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D       192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:21:04, Serial0/3/0
C       192.168.1.96/27 is directly connected, Serial0/3/0
       192.168.1.98/32 is directly connected, Serial0/3/0
C       192.168.1.128/27 is directly connected, Serial0/3/1
       192.168.1.130/32 is directly connected, Serial0/3/1
BOGOTA#

```

Ilustración 9. Salidas Balanceo de Cargas. Bogotá

- CALI:

```

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 [90/2170112] via 192.168.1.130, 00:00:29, Serial0/3/0
D       192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:00:29, Serial0/3/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:00:29, Serial0/3/0
C       192.168.1.128/27 is directly connected, Serial0/3/0
L       192.168.1.131/32 is directly connected, Serial0/3/0
CALI#

```

Ilustración 10. Salidas balanceo de cargas. Cali

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

Respuesta:

Para responder este punto vamos a hacer uso del siguiente comando “**show cdp neighbors details**”, esto con el fin de obtener información de dispositivos vecinos de manera detallada.

- **MEDELLIN:** Podemos ver información del switch interno en Medellín e información del router de Bogotá.

```

MEDELLIN#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 136

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

MEDELLIN#

```

Ilustración 11. Diagnóstico de vecinos. Medellín

- **BOGOTA:** Podemos ver información del router de Medellín y Cali, y del switch interno.

```

BOGOTA#show cdp neighbors detail

Device ID: MEDELLIN
Entry address(es):
  IP address : 192.168.1.99
Platform: cisco C2900, Capabilities: Router
Interface: Serial10/3/0, Port ID (outgoing port): Serial10/3/0
Holdtime: 169

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

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

```

Ilustración 12. Diagnósticos de vecinos -1. Bogotá

```
Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 139

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: CALI
Entry address(es):
Platform: cisco C2900, Capabilities: Router
Interface: Serial0/3/1, Port ID (outgoing port): Serial0/3/0
Holdtime: 151

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
```

Ilustración 13. Diagnósticos de vecinos -2. Bogotá

- **CALI:** Podemos ver información del switch interno de Cali y el router de Bogotá.

```

CALI#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 138

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 : 192.168.1.130
Platform: cisco C2900, Capabilities: Router
Interface: Serial0/3/0, Port ID (outgoing port): Serial0/3/1
Holdtime: 140

Version :
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full

```

Ilustración 14. Diagnóstico de vecinos. Cali

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

Respuesta:

A continuación, se comparte la imagen de una prueba ping desde el Router de Bogotá hacia la interfaz de la red interna del Router de Medellín (192.168.1.33) y a la red interna del Router de Cali, comprobando conexión y enrutamiento exitoso.

```

BOGOTA#ping 192.168.1.33

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/18 ms

BOGOTA#ping 192.168.1.65

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.65, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms

BOGOTA#|

```

Ilustración 15. Salida prueba de conectividad

Parte 3: Configuración de Enrutamiento.

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

Respuesta:

Se procede a configurar el enrutamiento EIGRP en cada uno de los routers mediante los siguientes comandos, con el AS igual a 200:

```

MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.0 255.255.255.0

```

```

BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.0 255.255.255.0

```

```

CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.0 255.255.255.0

```

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

Respuesta:

Para solucionar este requerimiento, hacemos uso del comando “**show ip eigrp neighbors**”, en cada uno de los Routers:

- **MEDELLIN:** Se identifica un vecino en el AS 200 detectado por la interfaz serial 0/3/0, el cual corresponde al router de Bogotá.

```
MEDELLIN#show ip eigrp neighbors 200
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT  RTO  Q   Seq
   (sec)             (ms)          Cnt  Num
0   192.168.1.98     Se0/3/0       11   01:35:49  40   1000 0   15
MEDELLIN#
```

- **BOGOTA:** Se identifican dos vecinos en el AS 200 detectados por la interfaz serial 0/3/0 y la interfaz serial 0/3/1, los cuales corresponden al router de Medellín y Cali respectivamente.

```
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT  RTO  Q   Seq
   (sec)             (ms)          Cnt  Num
0   192.168.1.99     Se0/3/0       10   01:38:47  40   1000 0   19
1   192.168.1.131   Se0/3/1       13   00:28:54  40   1000 0   7
BOGOTA#
```

- **CALI:** Se identifica un vecino en el AS 200 correspondiente al Router de Bogotá.

```
CALI#sho ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT  RTO  Q   Seq
   (sec)             (ms)          Cnt  Num
0   192.168.1.130   Se0/3/0       12   00:31:07  40   1000 0   16
CALI#
```

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

Respuesta:

Con el fin de realizar una comprobación del enrutamiento dentro de cada router, haremos uso del comando “show IP route”, el cual nos detalla la tabla de enrutamiento de cada router.

- MEDELLIN

```
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 [90/2170112] via 192.168.1.98, 01:48:49, Serial0/3/0
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 [90/2682112] via 192.168.1.98, 00:38:57, Serial0/3/0
C       192.168.1.96/27 is directly connected, Serial0/3/0
L       192.168.1.99/32 is directly connected, Serial0/3/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 01:48:49, Serial0/3/0

MEDELLIN#
```

Ilustración 16. Tabla de enrutamiento. Medellín

- BOGOTA

```
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 [90/2170112] via 192.168.1.99, 01:51:25, Serial0/3/0
D       192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:41:33, Serial0/3/1
C       192.168.1.96/27 is directly connected, Serial0/3/0
L       192.168.1.98/32 is directly connected, Serial0/3/0
C       192.168.1.128/27 is directly connected, Serial0/3/1
L       192.168.1.130/32 is directly connected, Serial0/3/1

BOGOTA#
```

Ilustración 17. Tabla de enrutamiento. Bogotá

- **CALI**

```
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 [90/2170112] via 192.168.1.130, 00:40:41, Serial0/3/0
D       192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:40:41, Serial0/3/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:40:41, Serial0/3/0
C       192.168.1.128/27 is directly connected, Serial0/3/0
L       192.168.1.131/32 is directly connected, Serial0/3/0

CALI#
```

Ilustración 18.Tabla de Enrutamiento. Cali

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.

Respuesta:

Esta prueba la haremos desde el “PCCali1” el cual tiene direccionamiento IP 192.168.1.70, primero realizando un PING hacia el “PCMedellin1” el cual está ubicado en Medellín y tiene direccionamiento IP 192.168.1.40, como podemos ver en la siguiente imagen, garantizamos la IP desde donde se esta enviando el PING y su destino en Medellín. El PING responde de manera exitosa.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::20D:BDFF:FE75:7D86
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.70
    Subnet Mask.....: 255.255.255.224
    Default Gateway.....: ::
                                     192.168.1.65

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                     0.0.0.0

C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=3ms TTL=253
Reply from 192.168.1.33: bytes=32 time=3ms TTL=253
Reply from 192.168.1.33: bytes=32 time=3ms TTL=253
Reply from 192.168.1.33: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

Ilustración 19. Prueba de conectividad de la Red. Medellín

La segunda prueba solicitada, la realizamos nuevamente desde el PCCali1 pero esta vez hacia el servidor en Bogotá. El servidor tiene direccionamiento IP 192.168.1.10. Como vemos en la siguiente prueba el PING es exitoso, garantizando así conectividad entre ambas sedes.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::20D:BDFF:FE75:7D86
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.70
    Subnet Mask.....: 255.255.255.224
    Default Gateway.....: ::
                                     192.168.1.65

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                     0.0.0.0

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=3ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

Ilustración 20. Prueba de conectividad Red. Bogotá

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.

Respuesta:

Con el fin de asegurar la conexión telnet entre los router, se crea una lista de acceso en cada router y se asigna esta lista de acceso mediante el comando “access-class” a la interfaz “line vty 0 4”, permitiendo únicamente la conexión desde los routers externos, así:

MEDELLIN

- MEDELLIN(config)#access-list 1 permit host 192.168.1.98
- MEDELLIN(config)#access-list 1 permit host 192.168.1.131
- MEDELLIN(config)# line vty 0 4
- MEDELLIN(config-line)#access-class 1 in

BOGOTA

- BOGOTA(config)#access-list 1 permit host 192.168.1.99
- BOGOTA (config)#access-list 1 permit host 192.168.1.131
- BOGOTA (config)# line vty 0 4
- BOGOTA (config-line)#access-class 1 in

CALI

- CALI(config)#access-list 1 permit host 192.168.1.98
- CALI (config)#access-list 1 permit host 192.168.1.130
- CALI (config)# line vty 0 4
- CALI (config-line)#access-class 1 in

Con el fin de restringir la conectividad de la red, a que solo los routers tengan conexión a toda la red y el resto de dispositivos NO, se lleva a cabo la siguiente configuración de listas de acceso en los equipos:

ROUTER MEDELLIN

```
ip access-list extended 101
access-list 101 permit ip host 192.168.1.98 192.168.1.0 0.0.0.255
access-list 101 permit ip host 192.168.1.131 192.168.1.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.99
access-list 101 permit eigrp any any
```

```
{Asignación de lista de acceso a interfaz en sentido inbound}
interface serial 0/3/0
```

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

ROUTER BOGOTA

```
ip access-list extended 101
access-list 101 permit IP host 192.168.1.99 192.168.1.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.98
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.99
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.131
access-list 101 permit eigrp any any
ip access-list extended 102
access-list 102 permit IP host 192.168.1.131 192.168.1.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.130
access-list 102 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.99
access-list 102 permit eigrp any any
```

{Asignación de lista de acceso a interfaz en sentido inbound}

```
interface serial 0/3/0
```

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

{Asignación de lista de acceso a interfaz en sentido inbound}

```
interface serial 0/3/1
```

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

ROUTER CALI

```
ip access-list extended 101
access-list 101 permit ip host 192.168.1.99 192.168.1.0 0.0.0.255
access-list 101 permit ip host 192.168.1.130 192.168.1.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.131
access-list 101 permit eigrp any any
```

{Asignación de lista de acceso a interfaz en sentido inbound}

```
interface serial 0/3/0
```

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

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

Respuesta:

El servidor cuenta con direccionamiento IP estático 192.168.1.10. Se procede a agregar las siguientes listas de acceso en los routers con el fin de otorgar los permisos requeridos. Estos permisos se otorgan mediante los siguientes comandos:

BOGOTA

```
access-list 101 permit IP 192.168.1.0 0.0.0.255 host 192.168.1.10  
access-list 102 permit IP 192.168.1.0 0.0.0.255 host 192.168.1.10
```

MEDELLIN

```
access-list 101 permit ip host 192.168.1.10 192.168.1.0 0.0.0.255
```

CALI

```
access-list 101 permit ip host 192.168.1.10 192.168.1.0 0.0.0.255
```

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

Respuesta:

Con el fin de dar cumplimiento con este requerimiento, se crea una lista de acceso para controlar el tráfico desde la red interna de Cali y Medellín, permitiendo solo cada segmento interno de cada sede, poder acceder a la dirección IP del servidor en Bogotá con IP 192.168.1.10. De igual manera se crean las listas de acceso para garantizar los permisos de conexión de cada router. Los comandos utilizados son los siguientes:

MEDELLIN

```
ip access-list extend 102  
permit ip 192.168.1.0 0.0.0.31 host 192.168.1.10  
permit ip 192.168.1.32 0.0.0.31 host 192.168.1.99  
permit ip 192.168.1.32 0.0.0.31 host 192.168.1.131
```

{Se asigna la lista de acceso a la interfaz conectada a la red interna}

```

interface giga 0/0
ip access-group 102 in
CALI
ip access-list extend 102
permit ip 192.168.1.64 0.0.0.31 host 192.168.1.10
permit ip 192.168.1.64 0.0.0.31 host 192.168.1.99
permit ip 192.168.1.64 0.0.0.31 host 192.168.1.130

```

{Se asigna la lista de acceso a la interfaz conectada a la red interna}

```

interface giga 0/0
ip access-group 102 in

```

Parte 5: 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.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	<p>Exitoso</p> <pre> MEDELLIN>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: </pre>
	WS_1	Router BOGOTA	<p>Rechazado</p> <pre> C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::290:21FF:FEB3:343C IPv6 Address: :: IPv4 Address: 192.168.1.11 Subnet Mask: 255.255.255.224 Default Gateway: :: 192.168.1.1 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address: :: IPv6 Address: :: IPv4 Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: :: 0.0.0.0 C:\>telnet 192.168.1.1 Trying 192.168.1.1 ... % Connection refused by remote host C:\> </pre>

	Servidor	Router CALI	<p style="text-align: center;">Rechazado</p> <pre>C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::205:5EFF:FEAA:C30 IPv6 Address: :: IPv4 Address: 192.168.1.10 Subnet Mask: 255.255.255.224 Default Gateway: :: 192.168.1.1 C:\>telnet 192.168.1.131 Trying 192.168.1.131 ... % Connection refused by remote host C:\></pre>
	Servidor	Router MEDELLIN	<p style="text-align: center;">Rechazado</p> <pre>C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::205:5EFF:FEAA:C30 IPv6 Address: :: IPv4 Address: 192.168.1.10 Subnet Mask: 255.255.255.224 Default Gateway: :: 192.168.1.1 C:\>telnet 192.168.1.99 Trying 192.168.1.99 ... % Connection refused by remote host C:\></pre>
TELNET	LAN del Router MEDELLIN	Router CALI	<p style="text-align: center;">Rechazado</p> <pre>C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::201:64FF:FEA6:D7BD IPv6 Address: :: IPv4 Address: 192.168.1.41 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.1.33 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address: :: IPv6 Address: :: IPv4 Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: :: 0.0.0.0 C:\> C:\> C:\>telnet 192.168.1.131 Trying 192.168.1.131 ... % Connection timed out; remote host not responding</pre>
	LAN del Router CALI	Router CALI	Rechazado

			<pre> C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix...: Link-local IPv6 Address...: FE80::20D:BDFE:FE75:7D86 IPv6 Address...: :: IPv4 Address...: 192.168.1.70 Subnet Mask...: 255.255.255.224 Default Gateway...: :: 192.168.1.65 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address...: :: IPv6 Address...: :: IPv4 Address...: 0.0.0.0 Subnet Mask...: 0.0.0.0 Default Gateway...: :: 0.0.0.0 C:\>telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding C:\>telnet 192.168.1.131 Trying 192.168.1.131 ... % Connection timed out; remote host not responding </pre>
	<p>LAN del Router MEDELLIN</p>	<p>Router MEDELLIN</p>	<p style="text-align: center;">Rechazado</p> <pre> C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix...: Link-local IPv6 Address...: FE80::201:64FF:FEA6:D7BD IPv6 Address...: :: IPv4 Address...: 192.168.1.41 Subnet Mask...: 255.255.255.0 Default Gateway...: :: 192.168.1.33 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address...: :: IPv6 Address...: :: IPv4 Address...: 0.0.0.0 Subnet Mask...: 0.0.0.0 Default Gateway...: :: 0.0.0.0 C:\>telnet 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\>telnet 192.168.1.99 Trying 192.168.1.99 ... % Connection timed out; remote host not responding </pre>
	<p>LAN del Router CALI</p>	<p>Router MEDELLIN</p>	<p style="text-align: center;">Rechazado</p>

			<pre> C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::20D:BDFE:FE75:7D86 IPv6 Address: :: IPv4 Address: 192.168.1.70 Subnet Mask: 255.255.255.224 Default Gateway: :: 192.168.1.65 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address: :: IPv6 Address: :: IPv4 Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: :: 0.0.0.0 C:\>telnet 192.168.1.99 Trying 192.168.1.99 ... % Connection timed out; remote host not responding </pre>
<p style="text-align: center;">PING</p>	<p style="text-align: center;">LAN del Router CALI</p>	<p style="text-align: center;">WS_1</p>	<p style="text-align: center;">Rechazado</p> <pre> C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::20D:BDFE:FE75:7D86 IPv6 Address: :: IPv4 Address: 192.168.1.70 Subnet Mask: 255.255.255.224 Default Gateway: :: 192.168.1.65 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address: :: IPv6 Address: :: IPv4 Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: :: 0.0.0.0 C:\>ping 192.168.1.11 Pinging 192.168.1.11 with 32 bytes of data: Reply from 192.168.1.65: Destination host unreachable. Ping statistics for 192.168.1.11: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), </pre>
	<p style="text-align: center;">LAN del Router MEDELLIN</p>	<p style="text-align: center;">WS_1</p>	<p style="text-align: center;">Rechazado</p>

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::201:64FF:FEA6:D7BD
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.41
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                192.168.1.33

Bluetooth Connection:

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::201:64FF:FEA6:D7BD
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.41
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                192.168.1.33

Bluetooth Connection:

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=2ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

	LAN del Router MEDELLIN	LAN del Router CALI	<p style="text-align: center;">Rechazado</p> <pre> C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::201:64FF:FEA6:D7BD IPv6 Address: :: IPv4 Address: 192.168.1.41 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.1.33 Bluetooth Connection: Connection-specific DNS Suffix...: Link-local IPv6 Address: :: IPv6 Address: :: IPv4 Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: :: 0.0.0.0 C:\>ping 192.168.1.70 Pinging 192.168.1.70 with 32 bytes of data: Reply from 192.168.1.33: Destination host unreachable. Ping statistics for 192.168.1.70: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), </pre>
PING	LAN del Router CALI	Servidor	Exitoso

**LAN del
Router
MEDELLIN**

Servidor

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::20D:BDFE:FE75:7D86
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.70
    Subnet Mask.....: 255.255.255.224
    Default Gateway.....: ::
                                     192.168.1.65

Bluetooth Connection:

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                     0.0.0.0

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=2ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Exitoso

			<pre> C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Link-local IPv6 Address.....: FE80::201:64FF:FEA6:D7BD IPv6 Address.....: :: IPv4 Address.....: 192.168.1.41 Subnet Mask.....: 255.255.255.0 Default Gateway.....: :: 192.168.1.33 Bluetooth Connection: Connection-specific DNS Suffix.: Link-local IPv6 Address.....: :: IPv6 Address.....: :: IPv4 Address.....: 0.0.0.0 Subnet Mask.....: 0.0.0.0 Default Gateway.....: :: 0.0.0.0 C:\>ping 192.168.1.10 Pinging 192.168.1.10 with 32 bytes of data: Reply from 192.168.1.10: bytes=32 time=2ms TTL=126 Reply from 192.168.1.10: bytes=32 time=3ms TTL=126 Reply from 192.168.1.10: bytes=32 time=3ms TTL=126 Reply from 192.168.1.10: bytes=32 time=1ms TTL=126 Ping statistics for 192.168.1.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 3ms, Average = 2ms </pre>
	<p align="center">Servidor</p>	<p align="center">LAN del Router MEDELLIN</p>	<p align="center">Exitoso</p> <pre> C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Link-local IPv6 Address.....: FE80::205:5EFF:FEAA:C30 IPv6 Address.....: :: IPv4 Address.....: 192.168.1.10 Subnet Mask.....: 255.255.255.224 Default Gateway.....: :: 192.168.1.1 C:\>ping 192.168.1.40 Pinging 192.168.1.40 with 32 bytes of data: Reply from 192.168.1.40: bytes=32 time=17ms TTL=126 Reply from 192.168.1.40: bytes=32 time=2ms TTL=126 Reply from 192.168.1.40: bytes=32 time=1ms TTL=126 Reply from 192.168.1.40: bytes=32 time=7ms TTL=126 Ping statistics for 192.168.1.40: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 17ms, Average = 6ms </pre>

	<p align="center">Servidor</p>	<p align="center">LAN del Router CALI</p>	<p align="center">Exitoso</p> <pre> C:\>ipconfig FastEthernet0 Connection: (default port) Connection-specific DNS Suffix. : Link-local IPv6 Address : FE80::205:5EFF:FEAA:C30 IPv6 Address : :: IPv4 Address. : 192.168.1.10 Subnet Mask : 255.255.255.224 Default Gateway : 192.168.1.1 C:\>ping 192.168.1.70 Pinging 192.168.1.70 with 32 bytes of data: Reply from 192.168.1.70: bytes=32 time=16ms TTL=126 Reply from 192.168.1.70: bytes=32 time=1ms TTL=126 Reply from 192.168.1.70: bytes=32 time=1ms TTL=126 Reply from 192.168.1.70: bytes=32 time=2ms TTL=126 Ping statistics for 192.168.1.70: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 16ms, Average = 5ms </pre>
	<p align="center">Router CALI</p>	<p align="center">LAN del Router MEDELLIN</p>	<p align="center">Exitoso</p> <pre> CALI#ping 192.168.1.40 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.40, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/19/58 ms CALI#ping 192.168.1.41 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.41, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/12 ms CALI# </pre>
	<p align="center">Router MEDELLIN</p>	<p align="center">LAN del Router CALI</p>	<p align="center">Exitoso</p> <pre> MEDELLIN#ping 192.168.1.70 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.70, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/17/61 ms MEDELLIN#ping 192.168.1.71 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.71, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 3/9/12 ms MEDELLIN# </pre>

Tabla 2. Comprobación de la Red instalada. Escenario 1

5.1.2 ESCENARIO 2:

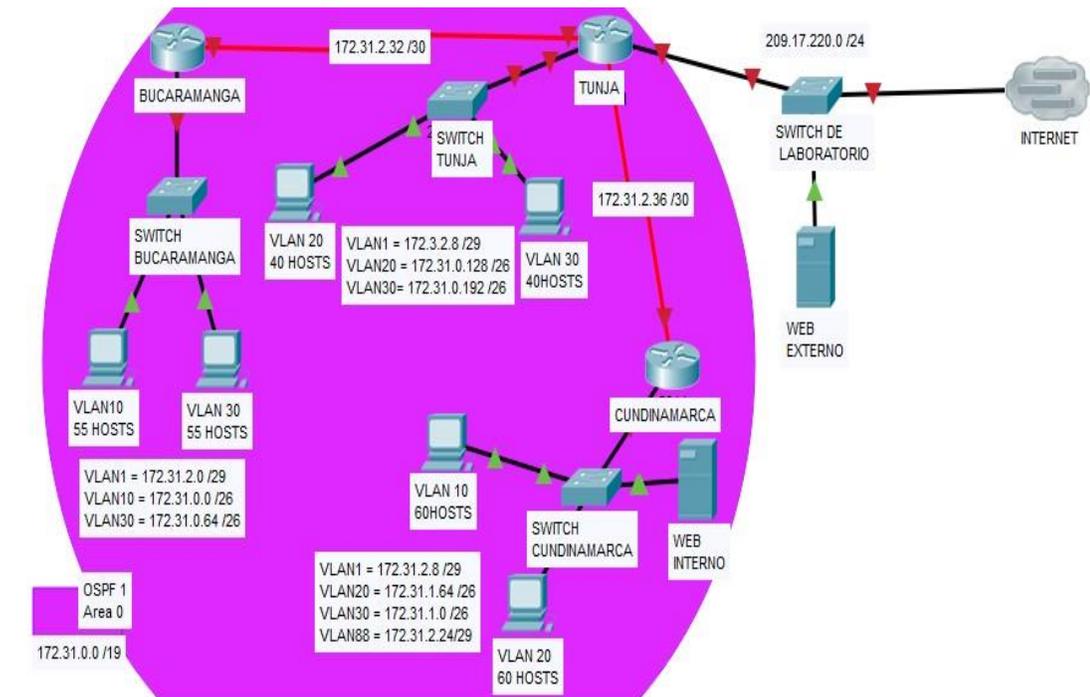


Ilustración 21. Topología Escenario 2

Los siguientes son los requerimientos necesarios:

6 Todos los routers deberán tener los siguiente:

- **Configuración básica.**
 - Se configura el nombre a cada router según su ubicación: BUCARAMANGA, CUNDINAMARCA y TUNJA.
 - Se habilita solicitud de password para el modo “Enable”.
 - Se crea usuario local administración del equipo “miguel.mejia”
 - Se activa el cifrado de contraseñas en la configuración del router.
 - Se configuran vlan en los switches según la gráfica. Los puertos de conexión entre cada y switch y el router se configura en modo troncal “trunk”.
- **Autenticación local con AAA.**
 - Se procede a crear un usuario interno “miguel.mejia” con su respectivo password.

- Se habilita la autenticación AAA para autenticación local mediante los siguientes comandos:
 - aaa new-model
 - aaa authentication login default local
- **Cifrado de contraseñas.**
 - Para llevar a cabo este requerimiento hacemos uso del siguiente comando en todos los routers “service password-encryption”.
- **Un máximo de intentos para acceder al router.**
 - Hacemos uso del siguiente comando “login block-for 30 attempts 5 within 60”, el cual, si se presentan 5 intentos de autenticación fallidos, el login se bloqueará por 30 segundos.
- **Máximo tiempo de acceso al detectar ataques.**
- **Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.**
 - Se elige como servidor TFTP el servidor web externo y mediante el siguiente comando se almacenan los archivos de configuración de cada router.

```
BUCARAMANGA#copy running-config tftp:
Address or name of remote host []? 209.17.220.2
Destination filename [BUCARAMANGA-config]?

Writing running-config...!!
[OK - 2923 bytes]

2923 bytes copied in 0.052 secs (56211 bytes/sec)
BUCARAMANGA#
```

```
TUNJA#copy running-config tftp:
Address or name of remote host []? 209.17.220.2
Destination filename [TUNJA-config]?

Writing running-config...!!
[OK - 2970 bytes]

2970 bytes copied in 0.001 secs (2970000 bytes/sec)
TUNJA#
```

```
CUNDINAMARCA#copy running-config tftp:
Address or name of remote host []? 209.17.220.2
Destination filename [CUNDINAMARCA-config]?

Writing running-config...!!
[OK - 3630 bytes]

3630 bytes copied in 0.002 secs (1815000 bytes/sec)
CUNDINAMARCA#
```

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

Respuesta:

Para dar cumplimiento con este punto, llevamos a cabo la siguiente configuración de DHCP en los routers de BUCARAMANGA y CUNDINAMARCA. Los comandos ejecutados son los siguientes:

BUCARAMANGA

- Excluimos del dhcp las direcciones IP correspondientes al Gateway-Router:
 - o ip dhcp excluded-address 172.31.0.1
 - o ip dhcp excluded-address 172.31.0.65
- Configuramos el DHCP para la vlan10 "ip dhcp pool vlan10"
 - o network 172.31.0.0 255.255.255.192
 - o default-router 172.31.0.1
 - o dns-server 8.8.8.8
- Configuramos el DHCP para la vlan30 "ip dhcp pool vlan30"
 - o network 172.31.0.64 255.255.255.192
 - o default-router 172.31.0.65
 - o dns-server 8.8.8.8

CUNDINAMARCA

- Excluimos del dhcp las direcciones IP correspondientes al Gateway-Router:
 - o ip dhcp excluded-address 172.31.2.9
 - o ip dhcp excluded-address 172.31.1.65
 - o ip dhcp excluded-address 172.31.1.1
 - o ip dhcp excluded-address 172.31.2.25
- Configuramos el DHCP para la vlan20 "ip dhcp pool vlan20"
 - o network 172.31.1.64 255.255.255.192
 - o default-router 172.31.1.65
 - o dns-server 8.8.8.8
- Configuramos el DHCP para la vlan20 "ip dhcp pool vlan30"
 - o network 172.31.1.0 255.255.255.192
 - o default-router 172.31.1.1
 - o dns-server 8.8.8.8
- Configuramos el DHCP para la vlan88 "ip dhcp pool vlan88"
 - o network 172.31.2.24 255.255.255.248
 - o default-router 172.31.2.25
 - o dns-server 8.8.8.8

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

Respuesta:

Se lleva a cabo la configuración de un NAT estático para publicar hacia internet en el router de TUNJA el web server interno (Con IP 172.31.2.26) ubicado en CUNDINAMARCA. Se usa como dirección IP publica 209.17.220.10 y los comandos utilizados son los siguientes:

TUNJA

```
TUNJA(config)#interface serial 0/3/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/3/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#interface gigabitEthernet 0/2
TUNJA(config-if)#ip nat outside
```

```
TUNJA(config)#ip nat inside source static 172.31.2.26 209.17.220.10
```

Una vez se configura este NAT estático se realizan pruebas de conexión telnet por el puerto 80 desde el router de TUNJA a la IP real del server y esta conexión es exitosa:

```
TUNJA#telnet 172.31.2.26 80
Trying 172.31.2.26 ...Open
```

Y se realiza una prueba de conexión exitosa desde el servidor WebExterno a la IP publica usada en el NAT Statico:

```
Packet Tracer SERVER Command Line 1.0
C:\>
C:\>
C:\>telnet 209.17.220.10 80
Trying 209.17.220.10 ...Open

[Connection to 209.17.220.10 closed by foreign host]
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BAFF:FE3D:8348
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 209.17.220.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
                                209.17.220.1
```

Ilustración 22. Salida Prueba de conexión

Continuamos con la configuración del PAT para toda la red interna. Esta configuración se lleva a cabo en el router de TUNJA y los comandos utilizados son los siguientes:

TUNJA

```
TUNJA(config)#access-list 1 permit 172.0.0.0 0.0.0.255
TUNJA(config)#ip nat pool public_access 209.17.220.15 209.17.220.15 netmask
255.255.255.0
TUNJA(config)#ip nat inside source list 1 pool public_access overload
```

Con el fin de validar la correcta configuración y funcionamiento del PAT, realizamos pruebas de conexión desde un PC interno en la red de Bucaramanga, dando un PING y un TELNET al puerto 80 al servidor WebExterno, ambas pruebas fueron exitosas:

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>telnet 209.17.220.2 80
Trying 209.17.220.2 ...Open
```

Ilustración 23. Salida para validación de configuración

Validamos con el siguiente comando “show ip nat statistics” y “show ip nat translations” y vemos que tanto el NAT estatico como el PAT están funcionando correctamente:

```
TUNJA#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/2
Inside Interfaces: Serial0/3/0 , Serial0/3/1
Hits: 6 Misses: 9
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.0
   start 209.17.220.15 end 209.17.220.15
   type generic, total addresses 1 , allocated 0 (0%), misses 0
TUNJA#show ip nat tra
TUNJA#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.17.220.10        172.31.2.26       ---                ---
tcp  209.17.220.10:80    172.31.2.26:80    209.17.220.2:1025  209.17.220.2:1025
TUNJA#
```

Ilustración 24. Salida prueba validación NAT y PAT

9 El enrutamiento deberá tener autenticación.

Respuesta:

Se lleva a cabo la configuración del enrutamiento OSPF con autenticación en los 3 Routers. La configuración llevada a cabo es la siguiente:

BUCARAMANGA

```
interface Serial 0/3/1
ip ospf 1 area 0
ip ospf authentication-key C15c0
```

```
router ospf 1
network 172.31.2.0 0.0.0.7 area 0
network 172.31.0.0 0.0.0.63 area 0
network 172.31.0.64 0.0.0.63 area 0
area 0 authentication
```

TUNJA

```
interface Serial 0/3/1
ip ospf 1 area 0
```

```
ip ospf authentication-key C15c0
interface Serial 0/3/0
ip ospf 1 area 0
ip ospf authentication-key C15c0
```

```
router ospf 1
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.63 area 0
network 172.31.0.192 0.0.0.63 area 0
network 209.17.220.0 0.0.0.255 area 0
area 0 authentication
```

CUNDINAMARCA

```
interface Serial 0/3/0
ip ospf 1 area 0
ip ospf authentication-key Cisco2021
router ospf 1
network 172.31.2.8 0.0.0.7 area 0
network 172.31.2.24 0.0.0.7 area 0
network 172.31.1.64 0.0.0.63 area 0
network 172.31.1.0 0.0.0.63 area 0
area 0 authentication
```

Una vez configurado el protocolo de enrutamiento, podemos observar la tabla de enrutamiento en cada uno de los routers. Podemos observar las rutas aprendidas mediante OSPF:

BUCARAMANGA

```

BUCARAMANGA#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

    172.3.0.0/29 is subnetted, 1 subnets
O      172.3.2.8/29 [110/101] via 172.31.2.34, 00:04:56, Serial0/3/1
    172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
C      172.31.0.0/26 is directly connected, GigabitEthernet0/0.10
L      172.31.0.1/32 is directly connected, GigabitEthernet0/0.10
C      172.31.0.64/26 is directly connected, GigabitEthernet0/0.30
L      172.31.0.65/32 is directly connected, GigabitEthernet0/0.30
O      172.31.0.128/26 [110/101] via 172.31.2.34, 00:04:56, Serial0/3/1
O      172.31.0.192/26 [110/101] via 172.31.2.34, 00:04:56, Serial0/3/1
O      172.31.1.0/26 [110/201] via 172.31.2.34, 00:04:07, Serial0/3/1
O      172.31.1.64/26 [110/201] via 172.31.2.34, 00:04:07, Serial0/3/1
C      172.31.2.0/29 is directly connected, GigabitEthernet0/0
L      172.31.2.1/32 is directly connected, GigabitEthernet0/0
O      172.31.2.8/29 [110/201] via 172.31.2.34, 00:04:07, Serial0/3/1
O      172.31.2.24/29 [110/201] via 172.31.2.34, 00:04:07, Serial0/3/1
C      172.31.2.32/30 is directly connected, Serial0/3/1
L      172.31.2.33/32 is directly connected, Serial0/3/1
O      172.31.2.36/30 [110/200] via 172.31.2.34, 00:04:56, Serial0/3/1
O      209.17.220.0/24 [110/101] via 172.31.2.34, 00:04:56, Serial0/3/1

BUCARAMANGA#

```

Ilustración 25. Tabla de enrutamiento Bucaramanga

TUNJA

```
TUNJA#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

172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.3.2.8/29 is directly connected, GigabitEthernet0/0
L    172.3.2.9/32 is directly connected, GigabitEthernet0/0
172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
O    172.31.0.0/26 [110/101] via 172.31.2.33, 00:08:08, Serial0/3/1
O    172.31.0.64/26 [110/101] via 172.31.2.33, 00:08:08, Serial0/3/1
C    172.31.0.128/26 is directly connected, GigabitEthernet0/0.20
L    172.31.0.129/32 is directly connected, GigabitEthernet0/0.20
C    172.31.0.192/26 is directly connected, GigabitEthernet0/0.30
L    172.31.0.193/32 is directly connected, GigabitEthernet0/0.30
O    172.31.1.0/26 [110/101] via 172.31.2.38, 00:07:19, Serial0/3/0
O    172.31.1.64/26 [110/101] via 172.31.2.38, 00:07:19, Serial0/3/0
O    172.31.2.0/29 [110/101] via 172.31.2.33, 00:08:08, Serial0/3/1
O    172.31.2.8/29 [110/101] via 172.31.2.38, 00:07:19, Serial0/3/0
O    172.31.2.24/29 [110/101] via 172.31.2.38, 00:07:19, Serial0/3/0
C    172.31.2.32/30 is directly connected, Serial0/3/1
L    172.31.2.34/32 is directly connected, Serial0/3/1
C    172.31.2.36/30 is directly connected, Serial0/3/0
L    172.31.2.37/32 is directly connected, Serial0/3/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.17.220.0/24 is directly connected, GigabitEthernet0/2
L    209.17.220.1/32 is directly connected, GigabitEthernet0/2
```

Ilustración 26. Tabla e enrutamiento. Tunja

CUNDINAMARCA

CUNDINAMARCA#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

```
172.3.0.0/29 is subnetted, 1 subnets
O   172.3.2.8/29 [110/101] via 172.31.2.37, 00:08:14, Serial0/3/0
172.31.0.0/16 is variably subnetted, 16 subnets, 4 masks
O   172.31.0.0/26 [110/201] via 172.31.2.37, 00:08:14, Serial0/3/0
O   172.31.0.64/26 [110/201] via 172.31.2.37, 00:08:14, Serial0/3/0
O   172.31.0.128/26 [110/101] via 172.31.2.37, 00:08:14, Serial0/3/0
O   172.31.0.192/26 [110/101] via 172.31.2.37, 00:08:14, Serial0/3/0
C   172.31.1.0/26 is directly connected, GigabitEthernet0/0.30
L   172.31.1.1/32 is directly connected, GigabitEthernet0/0.30
C   172.31.1.64/26 is directly connected, GigabitEthernet0/0.10
L   172.31.1.65/32 is directly connected, GigabitEthernet0/0.10
O   172.31.2.0/29 [110/201] via 172.31.2.37, 00:08:14, Serial0/3/0
C   172.31.2.8/29 is directly connected, GigabitEthernet0/0
L   172.31.2.9/32 is directly connected, GigabitEthernet0/0
C   172.31.2.24/29 is directly connected, GigabitEthernet0/0.88
L   172.31.2.25/32 is directly connected, GigabitEthernet0/0.88
O   172.31.2.32/30 [110/200] via 172.31.2.37, 00:08:14, Serial0/3/0
C   172.31.2.36/30 is directly connected, Serial0/3/0
L   172.31.2.38/32 is directly connected, Serial0/3/0
O   209.17.220.0/24 [110/101] via 172.31.2.37, 00:08:14, Serial0/3/0
```

Ilustración 27. Tabla de Enrutamiento. Cundinamarca

10 Listas de control de acceso:

- **Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.**
 - Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.20 del Router de CUNDINAMARCA:

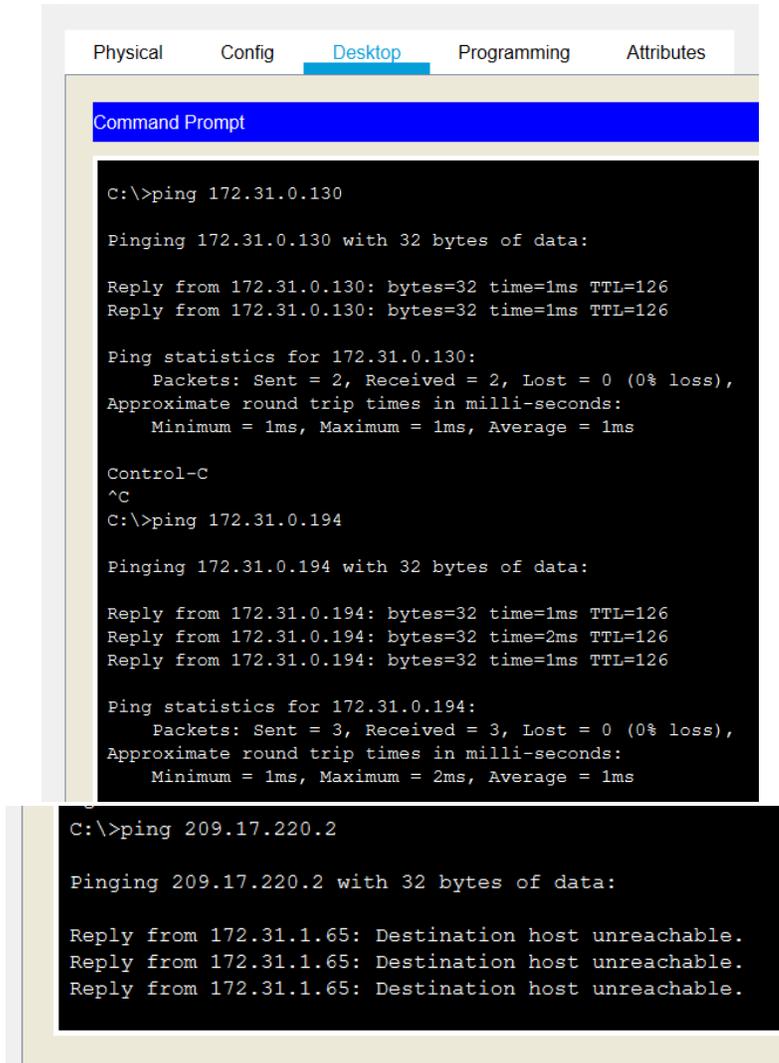
Extended IP access list 102

```
10 deny ip 172.31.1.0 0.0.0.63 172.3.2.8 0.0.0.7
20 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63 (7
match(es))
30 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63 (6
match(es))
40 permit ip 172.31.1.0 0.0.0.63 any (29 match(es))
50 permit udp any any (5 match(es))
60 permit ospf any any
```

```
interface GigabitEthernet0/0.20
  ip access-group 101 in
```

- Se hacen pruebas desde un equipo en la vlan 20 de CUNDINAMARCA y los resultados son exitosos:

PC2-VLAN20



```
Physical Config Desktop Programming Attributes
Command Prompt

C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

Control-C
^C
C:\>ping 172.31.0.194

Pinging 172.31.0.194 with 32 bytes of data:

Reply from 172.31.0.194: bytes=32 time=1ms TTL=126
Reply from 172.31.0.194: bytes=32 time=2ms TTL=126
Reply from 172.31.0.194: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.194:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
```

Ilustración 28. Salidas exitosas. Pruebas VLAN 20

- **Nota:** Se validan y crean las listas de acceso requeridas en el router de TUNJA, con el fin de dar los permisos de conexión requeridos.
- Los hosts de VLAN 30 (Se modifica VLAN10 por VLAN30 según la gráfica del ejercicio) en Cundinamarca si acceden a internet y no a la red interna de Tunja.

- Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.30 del Router de CUNDINAMARCA:

Extended IP access list 101

```

10 permit ip 172.31.1.64 0.0.0.63 172.3.2.8 0.0.0.7
20 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63 (58
match(es))
30 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63 (86
match(es))
40 permit ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.0.63 (4
match(es))
60 permit udp any any (3 match(es))
70 permit ospf any any
80 deny ip 172.31.1.64 0.0.0.63 any (2 match(es))

```

interface GigabitEthernet0/0.30

```
ip access-group 102 in
```

- Se hacen pruebas desde un equipo en la vlan 30 de CUNDINAMARCA y los resultados son exitosos. Bloqueando el PING hacia equipos en TUNJA y permitiendo el tráfico hacia internet:

- Dirección IP de equipo en VLAN30 de Cundinamarca.

```

C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::260:5CFF:FE59:A61B
IPv6 Address.....: ::
IPv4 Address.....: 172.31.1.2
Subnet Mask.....: 255.255.255.192
Default Gateway.....: ::
                        172.31.1.1

```

Ilustración 29. Dirección IP VLAN 30. Cundinamarca

- Bloqueo de tráfico hacia equipos en Tunja.

```
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.1.1: Destination host unreachable.

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.0.194

Pinging 172.31.0.194 with 32 bytes of data:

Reply from 172.31.1.1: Destination host unreachable.

Ping statistics for 172.31.0.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ilustración 30. Bloqueo de tráfico hacia equipos en Tunja

- Permiso de conexión hacia internet.

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Ilustración 31. Permiso de conexión hacia internet

- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
 - Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.30 del Router de TUNJA:

Extended IP access list 101

```
10 permit ip 172.31.0.192 0.0.0.63 host 209.17.220.2
30 permit udp any any
40 permit ospf any any
50 permit ip 172.31.0.192 0.0.0.63 172.31.1.64 0.0.0.63 (2
match(es))
60 deny ip 172.31.0.192 0.0.0.63 any
```

interface GigabitEthernet0/0.30

```
ip access-group 101 in
```

- Se hacen pruebas desde un equipo en la vlan 30 de TUNJA y los resultados son exitosos. Bloqueando el PING hacia equipos las otras ciudades y solo se permite el acceso al servidor ubicado en internet.
 - Dirección IP de equipo de pruebas en VLAN30 de Tunja.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:16FF:FE7D:7CA8
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 172.31.0.194
    Subnet Mask . . . . .: 255.255.255.192
    Default Gateway . . . . .:
                                172.31.0.193

Bluetooth Connection:
```

Ilustración 32. Pruebas VLAN30. Tunja

- Bloqueo de tráfico hacia otras ciudades y permisos de conexión hacia internet.

```

C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.193: Destination host unreachable.

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 209.17.220.2: bytes=32 time=1ms TTL=127
Reply from 209.17.220.2: bytes=32 time<1ms TTL=127
Reply from 209.17.220.2: bytes=32 time<1ms TTL=127
Reply from 209.17.220.2: bytes=32 time<1ms TTL=127

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Ilustración 33. Bloqueo otras ciudades y permisos de conexión

- **Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.**
 - Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.20 del Router de TUNJA:

Extended IP access list 102

```

10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
20 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
30 permit udp any any
40 permit ospf any any
50 deny ip 172.31.0.128 0.0.0.63 any

```

interface GigabitEthernet0/0.20

```
ip access-group 102 in
```

- Se hacen pruebas desde un equipo en la VLAN20 de TUNJA y los resultados son exitosos. Bloqueando el PING hacia equipos diferentes de la VLAN10 en Bucaramanga y la VLAN20 en Cundinamarca.
 - Dirección IP de equipo de pruebas en VLAN20 de Tunja.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::203:E4FF:FE30:9BCD
    IPv6 Address.....: ::
    IPv4 Address.....: 172.31.0.130
    Subnet Mask.....: 255.255.255.192
    Default Gateway.....: ::
                                172.31.0.129
```

Ilustración 34. IP VLAN20. Tunja

- Permisos de acceso a VLAN20 en Cundinamarca y VLAN10 en Bucaramanga.

```
C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=2ms TTL=126
Reply from 172.31.1.66: bytes=32 time=1ms TTL=126
Reply from 172.31.1.66: bytes=32 time=2ms TTL=126
Reply from 172.31.1.66: bytes=32 time=2ms TTL=126

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Request timed out.
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=10ms TTL=126

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 4ms
```

Ilustración 35. Permiso de Accesos VLAN20 Cundinamarca y VLAN10 Bucaramanga

- Bloqueo de tráfico hacia internet.

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 36. Bloqueo trafico

- **Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.**
 - Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.30 del Router de BUCARAMANGA:

Extended IP access list 102

```
10 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
20 deny ip 172.31.0.64 0.0.0.63 172.0.0.0 0.255.255.255
30 permit ip 172.31.0.64 0.0.0.63 any
40 permit udp any any (2 match(es))
```

interface GigabitEthernet0/0.30

```
ip access-group 102 in
```

- Se hacen pruebas desde un equipo en la VLAN30 de BUCARAMANGA y los resultados son exitosos. Permitiendo la conexión hacia internet y a la VLAN10, y bloqueando el resto de tráfico.
 - Dirección IP de equipo en la VLAN30 de Bucaramanga

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::202:17FF:FE14:94D2
IPv6 Address.....: ::
IPv4 Address.....: 172.31.0.66
Subnet Mask.....: 255.255.255.192
Default Gateway.....:
                        172.31.0.65
```

Ilustración 37. IP VLAN30 Bucaramanga

- Conexión a internet y hacia la VLAN10 es exitosa.

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.2: bytes=32 time=1ms TTL=127
Reply from 172.31.0.2: bytes=32 time<1ms TTL=127
Reply from 172.31.0.2: bytes=32 time<1ms TTL=127
Reply from 172.31.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ilustración 38. Salida exitosa VLAN10

- Bloqueo del resto de tráfico.

```
C:\>ping 172.31.0.193

Pinging 172.31.0.193 with 32 bytes of data:

Reply from 172.31.0.65: Destination host unreachable.

Ping statistics for 172.31.0.193:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 39. Bloqueo del tráfico adicional

- **Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.**
 - Se lleva a cabo la creación de la siguiente lista de acceso y se aplica en la subinterfaz giga0/0.10 del Router de BUCARAMANGA:

Extended IP access list 101

```
10 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 (3 match(es))
20 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
40 permit udp any any (2 match(es))
50 permit ip 172.31.0.0 0.0.0.63 172.31.0.64 0.0.0.63 (4 match(es))
60 deny ip 172.31.0.0 0.0.0.63 any
```

interface GigabitEthernet0/0.10

```
ip access-group 101 in
```

- Se hacen pruebas desde un equipo en la VLAN10 de BUCARAMANGA y los resultados son exitosos. Permitiendo la conexión hacia las VLAN20 de TUNJA y CUNDINAMARCA, y bloqueando el resto de tráfico incluyendo internet.
 - Dirección IP de equipo en VLAN10 de Bucaramanga.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::201:96FF:FEB5:27AA
IPv6 Address.....: ::
IPv4 Address.....: 172.31.0.2
Subnet Mask.....: 255.255.255.192
Default Gateway.....: ::
                        172.31.0.1
```

Ilustración 40. IP VLAN10. Bucaramanga

- PING a internet es rechazado.

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 41. PING rechazo internet

- PING a VLAN20 en Cundinamarca es exitoso.

```
C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=3ms TTL=125
Reply from 172.31.1.66: bytes=32 time=2ms TTL=125
Reply from 172.31.1.66: bytes=32 time=2ms TTL=125
Reply from 172.31.1.66: bytes=32 time=10ms TTL=125

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 4ms
```

Ilustración 42. PING VLAN20 Cundinamarca

- PING a VLAN20 en Tunja es exitoso.

```
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=2ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=2ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Ilustración 43. PING VLAN20 Tunja

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

Dado que, con la creación de las listas de acceso a las interfaces, aquel tráfico NO especificado será bloqueado. Igualmente, se hace una revisión sobre cada router para confirmar dicho bloqueo:

BUCARAMANGA: Dado que contamos con las siguientes listas de acceso configuradas en el router, las listas de acceso resaltadas en negro se encargan de bloquear el tráfico entre las VLAN del router de BUCARAMANGA que no se haya permitido explícitamente.

Extended IP access list 102

```
10 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
```

```
20 deny ip 172.31.0.64 0.0.0.63 172.0.0.0 0.255.255.255
30 permit ip 172.31.0.64 0.0.0.63 any
40 permit udp any any
```

Extended IP access list 101

```
10 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
20 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
40 permit udp any any (2 match(es))
50 permit ip 172.31.0.0 0.0.0.63 172.31.0.64 0.0.0.63
60 deny ip 172.31.0.0 0.0.0.63 any
```

TUNJA: Dado que contamos con las siguientes listas de acceso configuradas en el router, las listas de acceso resaltadas en negro se encargan de bloquear el tráfico entre las VLAN del router de TUNJA que no se haya permitido explícitamente.

Extended IP access list 101

```
10 permit ip 172.31.0.192 0.0.0.63 host 209.17.220.2
20 permit udp any any
30 permit ospf any any
40 permit ip 172.31.0.192 0.0.0.63 172.31.1.64 0.0.0.63
50 deny ip 172.31.0.192 0.0.0.63 any
```

Extended IP access list 102

```
10 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
20 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
30 permit udp any any
40 permit ospf any any
50 deny ip 172.31.0.128 0.0.0.63 any
```

CUNDINAMARCA: Dado que contamos con las siguientes listas de acceso configuradas en el router, las listas de acceso resaltadas en negro se encargan de bloquear el tráfico entre las VLAN del router de CUNDINAMARCA que no se haya permitido explícitamente.

Extended IP access list 102

```
10 deny ip 172.31.1.0 0.0.0.63 172.3.2.8 0.0.0.7
20 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
30 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
40 permit ip 172.31.1.0 0.0.0.63 any
50 permit udp any any (2 match(es))
60 permit ospf any any
```

Extended IP access list 101

```
10 permit ip 172.31.1.64 0.0.0.63 172.3.2.8 0.0.0.7
```

```

20 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63 (3
match(es))
30 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
40 permit ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.0.63 (5 match(es))
50 permit udp any any (2 match(es))
60 permit ospf any any
70 deny ip 172.31.1.64 0.0.0.63 any

```

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

Respuesta:

Se lleva a cabo la configuración de las siguientes listas de acceso en cada uno de los routers y se asigna esta lista de acceso a la interfaz TELNET (Line vty 0 4)

BUCARAMANGA

```

access-list 4 permit 172.31.2.0 0.0.0.7
line vty 0 4
access-class 4 in

```

Se valida realizando un telnet desde un equipo en la VLAN10 a su Gateway y este es rechazado.

```

C:\>IPCONFIG

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::201:96FF:FEB5:27AA
    IPv6 Address...: ::
    IPv4 Address...: 172.31.0.2
    Subnet Mask...: 255.255.255.192
    Default Gateway...: ::
                                     172.31.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: ::
    IPv6 Address...: ::
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    Default Gateway...: ::
                                     0.0.0.0

C:\>telnet 172.31.0.1
Trying 172.31.0.1 ...
% Connection timed out; remote host not responding

```

Ilustración 44. Rechazo VLAN10 Gateway. Bucaramanga

TUNJA

```
access-list 4 permit 172.3.2.8 0.0.0.7
line vty 0 4
access-class 4 in
```

Se valida realizando un telnet desde un equipo en la VLAN10 a su Gateway y este es rechazado.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::203:E4FF:FE30:9BCD
IPv6 Address.....: ::
IPv4 Address.....: 172.31.0.130
Subnet Mask.....: 255.255.255.192
Default Gateway.....: ::
                               172.31.0.129

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                               0.0.0.0

C:\>telnet 172.31.0.129
Trying 172.31.0.129 ...
% Connection timed out; remote host not responding
C:\>
```

Ilustración 45. Rechazo VLAN10 Gateway. Tunja

CUNDINAMARCA

```
access-list 4 permit 172.31.2.8 0.0.0.7
access-list 4 permit 172.31.2.24 0.0.0.7
line vty 0 4
access-class 4 in
```

Se valida realizando un telnet desde un equipo en la VLAN20 a su Gateway y este es rechazado. Sin embargo, el telnet desde el servidor interno es exitoso.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::203:E4FF:FE30:9BCD
    IPv6 Address.....: ::
    IPv4 Address.....: 172.31.0.130
    Subnet Mask.....: 255.255.255.192
    Default Gateway.....: ::
                                172.31.0.129

Bluetooth Connection:

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                                0.0.0.0

C:\>telnet 172.31.0.129
Trying 172.31.0.129 ...
% Connection timed out; remote host not responding
C:\>
```

Ilustración 46.Rechazo VLAN20 a su Gateway. Cundinamarca

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::20A:F3FF:FED5:55C3
    IPv6 Address.....: ::
    IPv4 Address.....: 172.31.2.26
    Subnet Mask.....: 255.255.255.248
    Default Gateway.....: ::
                                172.31.2.25

C:\>telnet 172.31.2.25
Trying 172.31.2.25 ...Open

User Access Verification

Username:
% Username: timeout expired!
```

Ilustración 47. Salida exitosa servidor interno

Con el fin de restringir el tráfico desde la red de administración y desde la red de servidores solo a internet, procedemos a crear las siguientes listas de acceso en cada router y se asignan a la subinterfaz correspondiente. Las lógicas de estas listas de acceso es bloquear todo el tráfico hacia la red 172.0.0.0/24 y permitir el resto de tráfico.

BUCARAMANGA

```
ip access-list extend 104
  deny ip 172.31.2.0 0.0.0.7 172.0.0.0 0.255.255.255
  permit ip 172.31.2.0 0.0.0.7 any
```

```
interface gigabitEthernet 0/0
  ip access-group 104 in
```

TUNJA

```
ip access-list extend 104
  deny ip 172.3.2.8 0.0.0.7 172.0.0.0 0.255.255.255
  permit ip 172.3.2.8 0.0.0.7 any
```

```
interface gigabitEthernet 0/0
  ip access-group 104 in
```

CUNDINAMARCA

```
ip access-list extend 103
  deny ip 172.31.2.24 0.0.0.7 172.0.0.0 0.255.255.255
  permit ip any any
```

```
interface gigabitEthernet 0/0.88
  ip access-group 103 in
  ip access-list extend 104
  deny ip 172.31.2.8 0.0.0.7 172.0.0.0 0.255.255.255
  permit ip any any
```

```
interface gigabitEthernet 0/0
  ip access-group 104 in
```

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

Respuesta:

La configuración de cada sede al interior de la red, se lleva a cabo teniendo en cuenta la siguiente gráfica, en donde cada subred es configurada con el tipo y tamaño de mascara requerido en dicha gráfica:

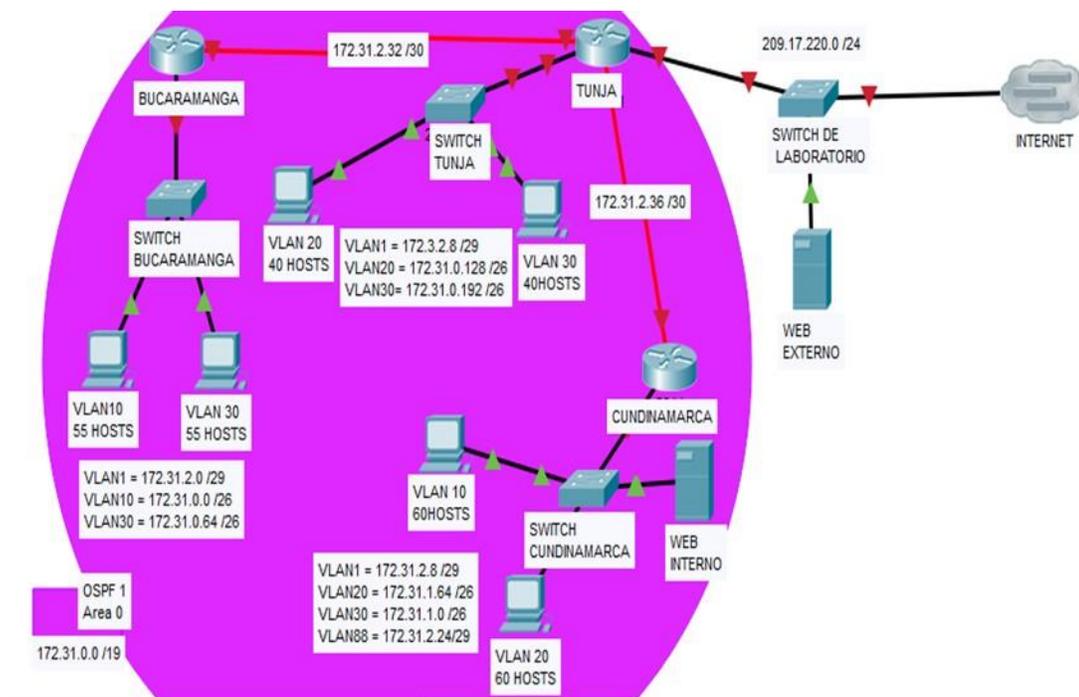


Ilustración 48. Configuración de redes internas

Aspectos a tener en cuenta

- **Habilitar VLAN en cada switch y permitir su enrutamiento.**
 - Se lleva a cabo la configuración de vlan en cada switch y cada vlan es asignada a un puerto donde se encuentra conectado un PC según la gráfica. Cada conexión entre los switches y cada router se lleva a cabo en modo trunk y la interfaz del router es virtualizada para que sea el Gateway de cada vlan.
- **Enrutamiento OSPF con autenticación en cada router.**
 - Se configura en cada una de las interfaces seriales el siguiente parámetro el cual solicita autenticación para el protocolo OSPF mediante el uso de los siguientes comandos “area 0 authentication message-digest” dentro de la configuración de “router ospf 1” y el “ip ospf message-digest-key 1 md5 CISCO” dentro de las interfaces seriales.
- **Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.**
 - Según el requerimiento del punto 2, se lleva a cabo la activación del DHCP en los routers de CUNDINAMARCA y BUCARAMANGA.
- **Configuración de NAT estático y de sobrecarga.**

- Se lleva a cabo la configuración requerida en el punto 3, sobre el router de TUNJA ya que este es el dispositivo que da conexión con internet.
- **Establecer una lista de control de acceso de acuerdo con los criterios señalados.**
 - Se lleva a cabo la configuración de listas de acceso las cuales operan correctamente. Se adjuntan imágenes de las pruebas y el en archivo .pkt adjunto se puede validar dicho funcionamiento.
- **Habilitar las opciones en puerto consola y terminal virtual**
 - Se procede a habilitar ambos puertos y se asegura el acceso del terminal mediante lista de acceso. Proceso explicado anteriormente.

CONCLUSIONES

Se realiza un escenario completo de configuraciones con las herramientas expuestas, cada escenario presento un nivel complejidad diferente lo que hace del ejercicio una base sólida en la práctica de las diferentes funcionalidades y herramientas que presenta cada equipo en la gama de comunicaciones CISCO; evidenciamos por ejemplo que en algunos modelos de dispositivos algunos comando variaban en su nomenclatura y algunos ya no existen en el firmware del dispositivo, esto nos permite ampliar de manera sustancial nuestros conocimientos técnicos de estos dispositivos.

Diferentes escenarios para diferentes soluciones, el modelo de ejercicio planteado trajo consigo unas configuraciones predeterminadas para el desarrollo del mismo, sin embargo, en el diseño que se planteó para la solución de ambos escenarios, aparecían diferentes formas de configuración apalancadas también en los diferentes tipos de dispositivos que se utilizaren para la solución final.

Al final se concluye que ambos escenarios, después de las diferentes evidencias adjuntas, quedan activos y cumplen con el objetivo del ejercicio de manera ideal.

BIBLIOGRAFIA

[1] Lamle Tobb, (2011, Abril 1) CCNA Cisco Certified Network Associate Study Guide, 7 th Edition, (p 640 – 801)

[2] Cisco (s.f.) Hoja de datos de los routers de servicios integrados de la serie Cisco 2900. Actualizado 22 de Agosto de 2017, de www.router-switch.com/pdf/cisco2911-k9-datasheet.pdf

[3] Cisco (s.f.) Configuración de ejemplo para la autenticación en OSPF. Actualizado 23 de Agosto de 2005, Id doc.13697, de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13697-25.html