

**DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN) (OPCI - (203092A_614)**

DIANA LUCIA AVILA TASCÓN

GRUPO 203092_17

TUTOR

JOSE IGNACIO CARDONA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS
PALMIRA
DICIEMBRE, 2019**

Contenido

Resumen	3
Abstract	4
Introducción	5
Objetivos	6
Desarrollo de los escenarios	7
Escenario 1	7
Topología de red	7
Desarrollo	8
Parte 1: Asignación de direcciones IP:	11
Parte 2: Configuración Básica.	13
Parte 3: Configuración de Enrutamiento.	19
Parte 4: Configuración de las listas de Control de Acceso.	23
Parte 5: Comprobación de la red instalada.	25
Escenario 2	26
1. Configuración básica.....	26
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca	35
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).	37
4. El enrutamiento deberá tener autenticación.	39
5. Listas de control de acceso	41
Conclusiones	47
Bibliografía	48

Resumen

El presente trabajo representa un escenario de red en el cual se aplican los conceptos vistos en el diplomado de redes CISCO CNNAI y CNNAII, esto con el fin de demostrar nuestros conocimientos adquiridos en topología de redes, así mismo la asignación de direcciones ip a los diferentes componentes de la red. En el desarrollo del escenario también se configura enrutamiento EIGRP y listas de control de acceso (ACL), por último, se comprueba que la red instalada funcione correctamente, cumpliendo así lo requerido en el planteamiento del problema. También se adjunta el archivo .pkt de la solución y configuración de la red.

Palabras claves: CNNA, ACL, EIGRP, protocolo, enrutamiento.

Abstract

The present work represents a network scenario in which the concepts seen in the CISCO CNAI and CNAII network diploma will be detected, this in order to demonstrate our knowledge acquired in network topology, as well as the assignment of ip addresses to the different network components. In the development of the scenario, EIGRP routing and access control lists (ACL) are also configured, finally, it is verified that the network is installed correctly, thus fulfilling what is required in the problem statement. The .pkt file of the solution and the network configuration are also attached.

Keywords: CNA, ACL, EIGRP, protocol, routing.

Introducción

El escenario planteado para solucionar se realiza de forma individual y consiste en construir una red en packet tracer según las orientaciones de la guía de pruebas de habilidades CNNA, la cual indica que hay una empresa que posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde se 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.

En este trabajo se detallan los comandos utilizados para cada configuración e imágenes de resultados obtenidos por la ejecución de algún comando en particular y que brinda información del componente en el que se está trabajando.

Objetivos

Colocar en practica los conocimientos adquiridos en el curso de CNNAI y CNNAII a través del escenario planteado.

Demostrar el paso a paso de la configuración de cada componente en la red construida.

Verificar que los resultados obtenidos sean los esperados para dar la solución a la problemática planteada.

Desarrollo de los escenarios

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

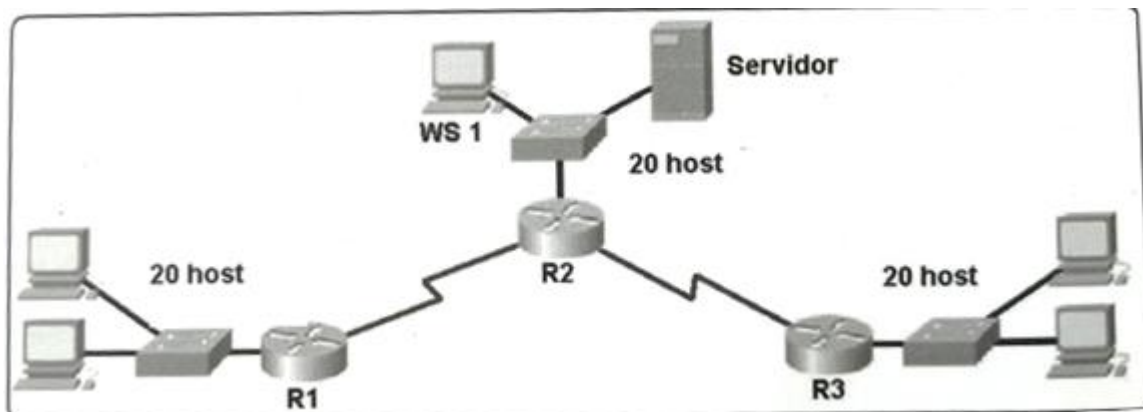
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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

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

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

Parte 6: Configuración final.



Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Configuración Router Medellín

El siguiente código configura nombre del router, encripta la contraseña y crea el mensaje de acceso restringido a los usuarios no autorizados.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Ro_Medellin
Ro_Medellin(config)#enable secret cisco
Ro_Medellin(config)#service password-encryption
Ro_Medellin(config)#banner motd "Restringido, solo acceso autorizado"
Ro_Medellin(config)#line console 0
Ro_Medellin(config-line)#password 0
Ro_Medellin(config-line)#login
Ro_Medellin(config-line)#exit
Ro_Medellin(config)#line vty 0 15
Ro_Medellin(config-line)#password class
Ro_Medellin(config-line)#login
Ro_Medellin(config-line)#end
Ro_Medellin#
```

Configuración Router Bogotá

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Ro_Bogota
Ro_Bogota(config)#enable secret cisco
Ro_Bogota(config)#service password-encryption
Ro_Bogota(config)#banner motd "Restringido, solo acceso a personal autorizado"
Ro_Bogota(config)#line console 0
Ro_Bogota(config-line)#password 0
Ro_Bogota(config-line)#login
Ro_Bogota(config-line)#exit
Ro_Bogota(config)#line vty 0 15
Ro_Bogota(config-line)#password class
```



```
Ro_Bogota(config-line)#login
Ro_Bogota(config-line)#end
Ro_Bogota#
```

Configuración Router Cali

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Ro_Cali
Ro_Cali(config)#enable secret cisco
Ro_Cali(config)#service password-encryption
Ro_Cali(config)#banner motd "Restringido, solo personal autorizado"
Ro_Cali(config)#line console 0
Ro_Cali(config-line)#password 0
Ro_Cali(config-line)#login
Ro_Cali(config-line)#exit
Ro_Cali(config)#line vty 0 15
Ro_Cali(config-line)#password class
Ro_Cali(config-line)#login
Ro_Cali(config-line)#end
Ro_Cali#
```

Configuración Switch Medellín

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw_Medillin
Sw_Medillin(config)#enable secret class
Sw_Medillin(config)#line console 0
Sw_Medillin(config-line)#password cisco
Sw_Medillin(config-line)#login
Sw_Medillin(config-line)#exit
Sw_Medillin(config)#service password-encryption
Sw_Medillin(config)#banner motd "Acceso no Autorizado"
Sw_Medillin(config)#exit
Sw_Medillin#
```

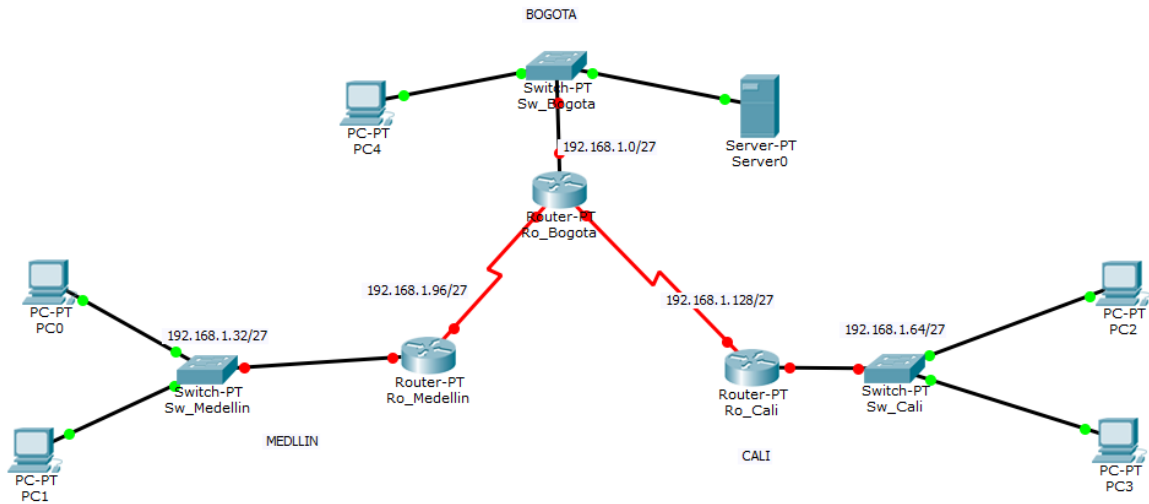
Configuración Switch Bogotá

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw_Bogota
Sw_Bogota(config)#enable secret class
Sw_Bogota(config)#line console 0
Sw_Bogota(config-line)#password cisco
Sw_Bogota(config-line)#login
Sw_Bogota(config-line)#exit
Sw_Bogota(config)#service password-encryption
Sw_Bogota(config)#banner motd "Acceso no Autorizado"
Sw_Bogota(config)#exit
Sw_Bogota#
```

Configuración Switch Cali

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw_Cali
Sw_Cali(config)#enable secret class
Sw_Cali(config)#line console 0
Sw_Cali(config-line)#password cisco
Sw_Cali(config-line)#login
Sw_Cali(config-line)#exit
Sw_Cali(config)#service password-encryption
Sw_Cali(config)#banner motd "Acceso no Autorizado"
Sw_Cali(config)#exit
Sw_Cali#
```

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



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

Parte 1: Asignación de direcciones IP:

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

Red Bogotá

Network: 192.168.1.0/27 Calculo binario: 11000000.10101000.00000001.000 00000
 Netmask: 255.255.255.224 Calculo binario: 11111111.11111111.11111111.111 00000
 Host Min: 192.168.1.1 Calculo binario: 11000000.10101000.00000001.000 00001
 Host Max: 192.168.1.30 Calculo binario: 11000000.10101000.00000001.000 11110
 Broadcast: 192.168.1.31 Calculo binario: 11000000.10101000.00000001.000 11111

Red Medellín

Network: 192.168.1.32/27 Calculo binario: 11000000.10101000.00000001.001 00000

Netmask: 255.255.255.224 Calculo binario: 11111111.11111111.11111111.11100000

Host Min: 192.168.1.33 Calculo binario: 11000000.10101000.00000001.00100001

Host Max: 192.168.1.62 Calculo binario: 11000000.10101000.00000001.00111110

Broadcast: 192.168.1.63 Calculo binario: 11000000.10101000.00000001.00111111

Red Cali

Network: 192.168.1.64/27 Calculo binario: 11000000.10101000.00000001.01000000

Netmask: 255.255.255.224 Calculo binario: 11111111.11111111.11111111.11100000

Host Min: 192.168.1.65 Calculo binario: 11000000.10101000.00000001.01000001

Host Max: 192.168.1.94 Calculo binario: 11000000.10101000.00000001.01011110

Broadcast: 192.168.1.95 Calculo binario: 11000000.10101000.00000001.01011111

El mismo cálculo se realiza para la ampliación de subredes:

Subred 1

Network: 192.168.1.96/27

Host Min: 192.168.1.97

Host Max: 192.168.1.126

Broadcast: 192.168.1.127

Subred 2

Network: 192.168.1.128/27

Host Min: 192.168.1.129

Host Max: 192.168.1.158

Broadcast: 192.168.1.159

Subred 3

Network: 192.168.1.160/27

Host Min: 192.168.1.161

Host Max: 192.168.1.190

Broadcast: 192.168.1.191

Subred 4

Network: 192.168.1.192/27

Host Min: 192.168.1.193

Host Max: 192.168.1.222

Broadcast: 192.168.1.223

Subred 5

Network: 192.168.1.224/27

Host Min: 192.168.1.225

Host Max: 192.168.1.254

Broadcast: 192.168.1.255

Subredes en uso: 3

Subredes calculadas para ampliación: 5

Total subredes: 8

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 2/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 3/0		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Se utilizan los siguientes comando para configurar las direcciones ip en los puertos de los router.

Router Bogotá

```
Ro_Bogota>enable
```

```
Password:
```

```
Ro_Bogota#conf t
```

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

```
Ro_Bogota(config)#int s2/0
```

```
Ro_Bogota(config-if)#ip address 192.168.1.98 255.255.255.224
```

```
Ro_Bogota(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
```

```
Ro_Bogota(config-if)#exit
```

```
Ro_Bogota(config)#int s3/0
```

```
Ro_Bogota(config-if)#ip address 192.168.1.130 255.255.255.224
```

```
Ro_Bogota(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial3/0, changed state to down
```

```
Ro_Bogota(config-if)#exit
```

```
Ro_Bogota(config)#int s3/0
```

```
Ro_Bogota(config-if)#ip address 192.168.1.130 255.255.255.224
```

```
Ro_Bogota(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial3/0, changed state to down
```

```
Ro_Bogota(config-if)#exit
```

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

```
Ro_Bogota(config-if)#ip address 192.168.1.1 255.255.255.224
```

```
Ro_Bogota(config-if)#exit
```

Router Medellín

```
Ro_Medellin>enable
```

```
Password:
```

```
Ro_Medellin#conf t
```

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

```
Ro_Medellin(config)#int s2/0
```

```
Ro_Medellin(config-if)#ip address 192.168.1.99 255.255.255.224
```

```
Ro_Medellin(config-if)#no shutdown
```

```
Ro_Medellin(config-if)#
```

```
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
```

```
Ro_Medellin(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

```
Ro_Medellin(config-if)#exit
Ro_Medellin(config)#int fa0/0
Ro_Medellin(config-if)#ip address 192.168.1.33 255.255.255.224
Ro_Medellin(config-if)#no shutdown
```

```
Ro_Medellin(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

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

```
Ro_Medellin(config-if)#exit
```

Router Cali

```
Ro_Cali>enable
Password:
Ro_Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cali(config)#int s2/0
Ro_Cali(config-if)#ip address 192.168.1.131 255.255.255.224
Ro_Cali(config-if)#no shutdown
```

```
Ro_Cali(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
```

```
Ro_Cali(config-if)#exit
Ro_Cali(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

```
Ro_Cali(config)#int fa0/0
Ro_Cali(config-if)#ip address 192.168.1.65 255.255.255.224
Ro_Cali(config-if)#no shutdown
```

```
Ro_Cali(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

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

- 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.

Nota: Los seriales planteados en la tabla según la guía inicial, fueron modificados a los que reflejan en esta tabla, dado que los router seleccionados para la configuración de la red con contienen esos números de serial planteados en la guía, por eso se ajusta la tabla.

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

Verificando balanceo en Router Cali

```

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

Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, Serial2/0
Ro_Cali#

```

Verificando balanceo en Router Medellin

```

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

Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 2 subnets
C       192.168.1.32 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial2/0
Ro_Medellin#

```

Verificando balanceo en Router Bogotá

```

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

Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial2/0
C       192.168.1.128 is directly connected, Serial3/0
Ro_Bogota#

```

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

Verificando Diagnóstico de vecinos en el Router Medellín

```

Ro_Medellin#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability   Platform    Port ID
Sw_Medillin     Fas 0/0         145        S            PT3000      Fas 0/1
Ro_Bogota       Ser 2/0         156        R            PT1000      Ser 2/0
Ro_Medellin#

```

Verificando en el Router Cali

```

Ro_Cali#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability   Platform    Port ID
Ro_Bogota       Ser 2/0         165        R            PT1000      Ser 3/0
Sw_Cali         Fas 0/0         147        S            PT3000      Fas 0/1
Ro_Cali#

```

Verificando en el Router Bogotá

```

Ro_Bogota#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability   Platform    Port ID
Ro_Medellin   Ser 2/0        156       R            PT1000      Ser 2/0
Ro_Cali       Ser 3/0        149       R            PT1000      Ser 2/0
Switch        Fas 0/0        167       S            PT3000      Fas 0/1
Ro_Bogota#

```

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

Ping del Ro_Medellin a la ip 192.168.1.98 (Ro_Bogota)

```

Ro_Medellin#ping 192.168.1.98

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

Ro_Medellin#

```

Ping del Ro_Bogota a la ip 192.168.1.99 (Ro_Medellin)

```

Ro_Bogota#ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

```

Ping del Ro_Bogota a la ip 192.168.1.131 (Ro_Cali)

```

Ro_Bogota#ping 192.168.1.131

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

```

Ping del Ro_Cali a la ip 192.168.1.130 (Ro_Bogota)

```
Ro_Cali#ping 192.168.1.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
```

Parte 3: Configuración de Enrutamiento.

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

Protocolo de Enrutamiento para Ro_Bogota

```
Ro_Bogota>enable
Password:
Ro_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bogota(config)#router eigrp 240
Ro_Bogota(config-router)#network 192.168.1.96
Ro_Bogota(config-router)#network 192.168.1.0
Ro_Bogota(config-router)#network 192.168.1.28
Ro_Bogota(config-router)#
```

Protocolo de Enrutamiento para Ro_Medellin

User Access Verification

Password:

```
Ro_Medellin>enable
Password:
Ro_Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Medellin(config)#router eigrp 240
Ro_Medellin(config-router)#network 192.168.1.32
Ro_Medellin(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 240: Neighbor 192.168.1.98 (Serial2/0) is up: new
adjacency

Ro_Medellin(config-router)#network 192.168.1.96
Ro_Medellin(config-router)#
```

Protocolo de Enrutamiento para Ro_Cali

```

User Access Verification

Password:

Ro_Cali>enable
Password:
Ro_Cali#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ro_Cali(config)#router eigrp 240
Ro_Cali(config-router)#network 192.168.1.128
Ro_Cali(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 240: Neighbor 192.168.1.130 (Serial2/0) is up: new
adjacency

Ro_Cali(config-router)#network 192.168.1.64
Ro_Cali(config-router)#
  
```

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

Router Medellin Ro_Medellin

```

Ro_Medellin#show ip eigrp neighbors
IP-EIGRP neighbors for process 240
H   Address           Interface           Hold Uptime        SRTT    RTO    Q    Seq
   (sec)              (ms)              Cnt  Num
0   192.168.1.98       Se2/0              12   00:02:43   40    1000  0    6
Ro_Medellin#
  
```

Router Bogotá Ro_Bogota

```

Ro_Bogota#show ip eigrp neighbors
IP-EIGRP neighbors for process 240
H   Address           Interface           Hold Uptime        SRTT    RTO    Q    Seq
   (sec)              (ms)              Cnt  Num
0   192.168.1.131      Se3/0              11   00:11:19   40    1000  0    7
1   192.168.1.99       Se2/0              13   00:09:26   40    1000  0    7
Ro_Bogota#
  
```

Router Bogotá Ro_Cali

```

Ro_Cali#show ip eigrp neighbors
IP-EIGRP neighbors for process 240
H   Address           Interface           Hold Uptime        SRTT    RTO    Q    Seq
   (sec)              (ms)              Cnt  Num
0   192.168.1.130      Se2/0              14   00:12:30   40    1000  0    5
Ro_Cali#
  
```

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

Tabla de enrutamiento Ro_Bogota

```

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/20514560] via 192.168.1.99, 00:17:41, Serial2/0
D       192.168.1.64 [90/20514560] via 192.168.1.131, 00:19:34, Serial3/0
C       192.168.1.96 is directly connected, Serial2/0
C       192.168.1.128 is directly connected, Serial3/0
Ro_Bogota#

```

Tabla de enrutamiento Ro_Cali

```

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.130, 00:26:29, Serial2/0
D       192.168.1.32 [90/21026560] via 192.168.1.130, 00:24:35, Serial2/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/21024000] via 192.168.1.130, 00:26:29, Serial2/0
C       192.168.1.128 is directly connected, Serial2/0
Ro_Cali#

```

Tabla de enrutamiento Ro_Medellin

```

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.98, 00:25:58, Serial2/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/21026560] via 192.168.1.98, 00:25:58, Serial2/0
C       192.168.1.96 is directly connected, Serial2/0
D       192.168.1.128 [90/21024000] via 192.168.1.98, 00:25:58, Serial2/0
Ro_Medellin#

```

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

Ping desde el PC3 (red Cali) hacia el PC 1 (red Medellin)

```

PC>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms

PC>

```

Ping desde el PC3 (red Cali) hacia el servidor (red Bogotá)

```

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=13ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 5ms

PC>

```

Se comprueba que la conectividad con entre las redes Cali, Medellín y Bogotá está funcionando correctamente.

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.

Comandos utilizados para el Ro_Bogota

```

Ro_Bogota>enable
Password:
Ro_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bogota(config)#int fa0/0
Ro_Bogota(config-if)#ip access-group 102 in
Ro_Bogota(config-if)#access-list 102 permit tcp any any eq telnet
Ro_Bogota(config)#

```

Comandos utilizados para el Ro_Medellin

```

Password:

Ro_Medellin>enable
Password:

```

```
Ro_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Medellin(config)#int fa0/0
Ro_Medellin(config-if)#ip access-group 102 in
Ro_Medellin(config-if)#access-list 102 permit tcp any any eq telnet
Ro_Medellin(config)#
```

Comandos utilizados para el Ro_Cali

Password:

```
Ro_Cali>enable
Password:
Ro_Cali#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cali(config)#int fa0/0
Ro_Cali(config-if)#ip access-group 102 in
Ro_Cali(config-if)#access-list 102 permit tcp any any eq telnet
Ro_Cali(config)#
```

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

Comandos utilizados en el Ro_Bogota

```
Ro_Bogota>enable
Password:
Ro_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bogota(config)#int fa0/0
Ro_Bogota(config-if)#ip access-group 1 in
Ro_Bogota(config-if)#access-list 1 deny host 192.168.1.3
Ro_Bogota(config)#int fa0/0
Ro_Bogota(config-if)#access-list 1 permit any
Ro_Bogota(config)#
```

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

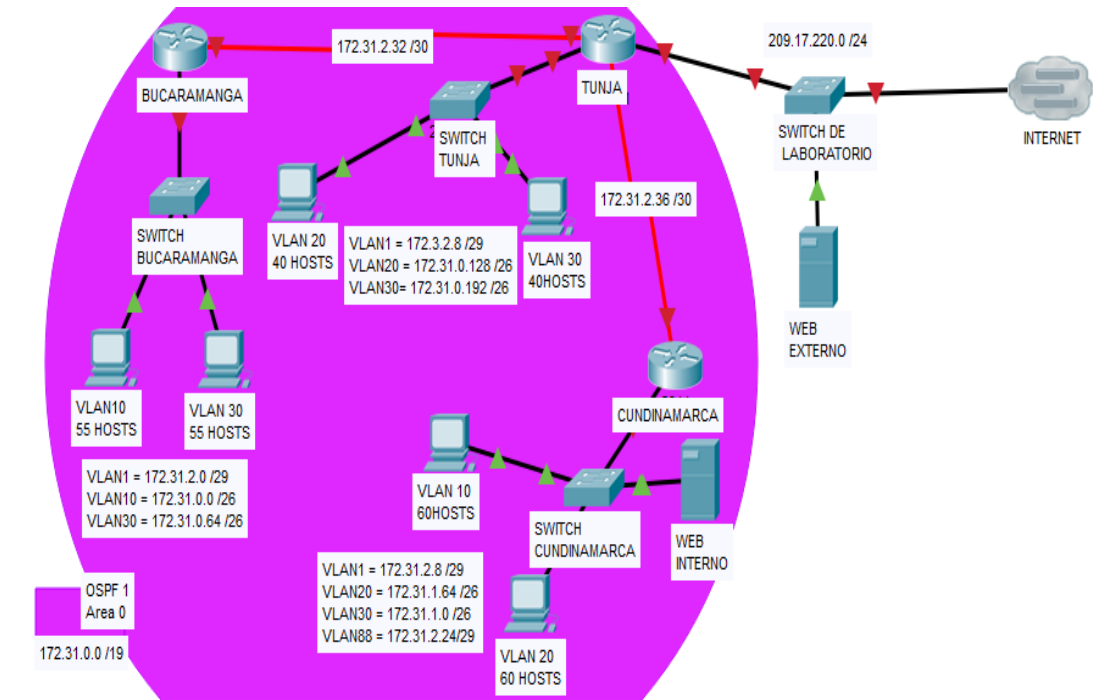
Parte 5: Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Conecta
	WS_1	Router BOGOTA	Conecta
	Servidor	Router CALI	Conecta
	Servidor	Router MEDELLIN	Conecta
TELNET	LAN del Router MEDELLIN	Router CALI	No conecta
	LAN del Router CALI	Router CALI	Conecta
	LAN del Router MEDELLIN	Router MEDELLIN	Conecta
	LAN del Router CALI	Router MEDELLIN	No conecta
PING	LAN del Router CALI	WS_1	No conecta
	LAN del Router MEDELLIN	WS_1	No conecta
	LAN del Router MEDELLIN	LAN del Router CALI	No conecta
PING	LAN del Router CALI	Servidor	Conecta
	LAN del Router MEDELLIN	Servidor	Conecta
	Servidor	LAN del Router MEDELLIN	Conecta
	Servidor	LAN del Router CALI	Conecta
	Router CALI	LAN del Router MEDELLIN	No conecta
	Router MEDELLIN	LAN del Router CALI	No conecta

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.



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

1. Configuración básica.

Router Bucaramanga

```
Router>enable
Router#configure terminal
Router(config)#hostname Ro_Bucaramanga
Ro_Bucaramanga(config)#
Ro_Bucaramanga(config)#interface Serial2/0
Ro_Bucaramanga(config-if)#ip address 172.31.2.33 255.255.0.0
```

Ro_Bucaramanga(config-if)#ip address 172.31.2.33 255.255.255.252

Se debe configurar el **Sw_Bucaramanga** para asignar las vlan al router Ro_Bucaramanga

```
Switch(config-if)#exit
Switch(config)#interface vlan1
Switch(config-if)#ip address 172.31.2.1
Switch(config-if)#ip address 172.31.2.1 255.255.255.248
Switch(config-if)#

Switch(config)#interface vlan10
Switch(config-if)#ip address 172.31.0.0 255.255.255.192
Bad mask /26 for address 172.31.0.0
Switch(config-if)#ip address 172.31.0.1 255.255.255.192
Switch(config-if)#exit
Switch(config)#interface vlan30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#ip address 172.31.0.65 255.255.255.192
Switch(config-if)#exit
Switch(config)#
```

Configurando el Router **Ro_Bucaramanga** para que haya comunicación con las 3 vlans.

```
Ro_Bucaramanga(config)#int fa0/0.1
Ro_Bucaramanga(config-subif)#encapsulation dot1Q 2
Ro_Bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#int fa0/0.2
Ro_Bucaramanga(config-subif)#encapsulation dot1Q 3
Ro_Bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#int fa0/0.3
Ro_Bucaramanga(config-subif)#encapsulation dot1Q 4
Ro_Bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#
```

Posteriormente encendemos el puerto fa0/0 para la comunicación con el Sw_Bucaramanga, utilizando los siguientes comandos:

```
Ro_Bucaramanga(config)#int fa0/0
Ro_Bucaramanga(config-if)#no shutdown
Ro_Bucaramanga(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up
Ro_Bucaramanga(config-if)#
```

Router Tunja

```
Router>enable
Router#configure terminal
Router(config)#hostname Ro_Tunja
Ro_Bucaramanga(config)#
Ro_Bucaramanga(config)#interface Serial2/0
Ro_Bucaramanga(config-if)#ip address 172.31.2.34 255.255.0.0
Ro_Bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
Ro_Tunja(config-if)#exit
Ro_Tunja(config)#interface Serial3/0
Ro_Tunja(config-if)#ip address 172.31.2.37 255.255.255.252
Ro_Tunja(config-if)#
```

Se debe configurar el **Sw_Tunja** para asignar las vlan al router Ro_Tunja

```
Switch(config)#interface vlan1
Switch(config-if)#ip address 172.3.2.9 255.255.255.248
Switch(config-if)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface vlan20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#exit
Switch(config)#interface vlan30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#ip address 172.31.0.193 255.255.255.192
Switch(config-if)#
```

Configurando el Router **Ro_Tunja** para que haya comunicación con las 3 vlans.

```

Ro_Tunja(config)#interface fa0/0.1
Ro_Tunja(config-subif)#encapsulation dot1Q 2
Ro_Tunja(config-subif)#ip address 172.31.2.9 255.255.255.248
Ro_Tunja(config-subif)#exit
Ro_Tunja(config)#int fa0/0.2
Ro_Tunja(config-subif)#encapsulation dot1Q 3
Ro_Tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
Ro_Tunja(config-subif)#exit
Ro_Tunja(config)#int fa0/0.3
Ro_Tunja(config-subif)#encapsulation dot1Q 4
Ro_Tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
Ro_Tunja(config-subif)#exit
Ro_Tunja(config)#

```

Posteriormente encendemos el puerto fa0/0 para la comunicación con el Sw_Tunja, utilizando los siguientes comandos:

```

Ro_Tunja(config)#int fa0/0
Ro_Tunja(config-if)#no shutdown
Ro_Tunja(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

```

Router Cundinamarca

```

Router>enable
Router#configure terminal
Router(config)#hostname Ro_Cundinamarca
Ro_Bucaramanga(config)#
Ro_Bucaramanga(config)#interface Serial2/0
Ro_Bucaramanga(config-if)#ip address 172.31.2.38 255.255.0.0
Ro_Bucaramanga(config-if)#ip address 172.31.2.38 255.255.255.252
Ro_Tunja(config-if)#exit

```

Se debe configurar el **Sw_Cundinamarca** para asignar las vlan al router Ro_Cundinamarca

```
Switch(config)#int vlan1
Switch(config-if)#ip address 172.31.2.9 255.255.255.248
Switch(config-if)#exit
Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip address 172.31.1.64 255.255.255.192
Bad mask /26 for address 172.31.1.64
Switch(config-if)#ip address 172.31.1.65 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 172.31.1.1 255.255.255.192
      ^
% Invalid input detected at '^' marker.

Switch(config)#int vlan 30
Switch(config-if)#ip address 172.31.1.1 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 88
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

Switch(config-if)#ip address 172.31.2.25 255.255.255.248
Switch(config-if)#exit
Switch(config)#
```

Configurando el Router **Ro_Cundinamarca** para que haya comunicación con las 3 vlans.

```
Ro_Cundinamarca(config)#int fa0/0.1
Ro_Cundinamarca(config-subif)#encapsulation dot1Q 2
Ro_Cundinamarca(config-subif)#ip address 172.31.2.9 255.255.255.248
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.2
Ro_Cundinamarca(config-subif)#encapsulation dot1Q 3
Ro_Cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.3
Ro_Cundinamarca(config-subif)#encapsulation dot1Q 4
Ro_Cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.4
Ro_Cundinamarca(config-subif)#encapsulation dot1Q 5
Ro_Cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#
```

Posteriormente encendemos el puerto fa0/0 para la comunicación con el Sw_Cundinamarca, utilizando los siguientes comandos:

```
Ro_Cundinamarca(config)#int fa0/0
Ro_Cundinamarca(config-if)#no shutdown
Ro_Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state to up
Ro_Cundinamarca(config-if)#
```

A continuación se muestra la imagen de la configuración de cada Router.

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	<not set>	<not set>	00E0.A399.44BB
FastEthernet0/0.1	Up	172.3.2.9/29	<not set>	00E0.A399.44BB
FastEthernet0/0.2	Up	172.31.0.129/26	<not set>	00E0.A399.44BB
FastEthernet0/0.3	Up	172.31.0.193/26	<not set>	00E0.A399.44BB
FastEthernet1/0	Up	<not set>	<not set>	0030.A30E.AE43
Serial2/0	Up	172.31.2.34/30	<not set>	<not set>
Serial3/0	Up	172.31.2.37/30	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0050.0F60.D347
FastEthernet5/0	Down	<not set>	<not set>	0050.0FA2.B067

Hostname: Ro_Tunja

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	<not set>	<not set>	00D0.FFD7.DB82
FastEthernet0/0.1	Up	172.31.2.9/29	<not set>	00D0.FFD7.DB82
FastEthernet0/0.2	Up	172.31.1.65/26	<not set>	00D0.FFD7.DB82
FastEthernet0/0.3	Up	172.31.1.1/26	<not set>	00D0.FFD7.DB82
FastEthernet0/0.4	Up	172.31.2.25/29	<not set>	00D0.FFD7.DB82
FastEthernet1/0	Down	<not set>	<not set>	000B.BEAA.A866
Serial2/0	Up	172.31.2.38/30	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0002.16CA.0415
FastEthernet5/0	Down	<not set>	<not set>	0060.70AC.657A

Hostname: Ro_Cundinamarca

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	<not set>	<not set>	00E0.A399.44BB
FastEthernet0/0.1	Up	172.3.2.9/29	<not set>	00E0.A399.44BB
FastEthernet0/0.2	Up	172.31.0.129/26	<not set>	00E0.A399.44BB
FastEthernet0/0.3	Up	172.31.0.193/26	<not set>	00E0.A399.44BB
FastEthernet1/0	Up	<not set>	<not set>	0030.A30E.AE43
Serial2/0	Up	172.31.2.34/30	<not set>	<not set>
Serial3/0	Up	172.31.2.37/30	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0050.0F60.D347
FastEthernet5/0	Down	<not set>	<not set>	0050.0FA2.B067

Hostname: Ro_Tunja

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

- Autenticación local con AAA.
- Cifrado de contraseñas.
- Un máximo de internos para acceder al router.
- Máximo tiempo de acceso al detectar ataques.

Ahora se procede a realizar la configuración de los routers, de manera que se coloca autenticación local con AAA, se hace cifrado de contraseña mediante rsa 1024 bytes. También se establece un máximo de intentos de 2 y un máximo de tiempo de espera de 60.

Ro_Bucaramanga

```
Ro_Bucaramanga>enable
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#line vty 0 4
Ro_Bucaramanga(config-line)#password cisco
Ro_Bucaramanga(config-line)#login
Ro_Bucaramanga(config-line)#exit
Ro_Bucaramanga(config)#enable secret cisco
Ro_Bucaramanga(config)#ip domain-name BUCARAMANGA.com
Ro_Bucaramanga(config)#crypto key generate rsa
The name for the keys will be: Ro_Bucaramanga.BUCARAMANGA.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Ro_Bucaramanga(config)#ip ssh time-out 60
*mar. 1 3:49:33.346: %SSH-5-ENABLED: SSH 1.99 has been enabled
Ro_Bucaramanga(config)#ip ssh authentication-retries 2
Ro_Bucaramanga(config)#aaa new-model
Ro_Bucaramanga(config)#line vty 0 4
Ro_Bucaramanga(config-line)#transport input ssh
Ro_Bucaramanga(config-line)#username Bucaramanga secret password
Ro_Bucaramanga(config)#
```

Ro_Tunja

```
Ro_Tunja>enable
Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#line vty 0 4
```



```
Ro_Tunja(config-line)#password cisco
Ro_Tunja(config-line)#login
Ro_Tunja(config-line)#exit
Ro_Tunja(config)#enable secret cisco
Ro_Tunja(config)#ip domain-name TUNJA.com
Ro_Tunja(config)#crypto key generate rsa
The name for the keys will be: Ro_Tunja.TUNJA.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Ro_Tunja(config)#ip ssh time-out 60
*mar. 1 4:0:54.820: %SSH-5-ENABLED: SSH 1.99 has been enabled
Ro_Tunja(config)#ip ssh authentication-retries 2
Ro_Tunja(config)#aaa new-model
Ro_Tunja(config)#line vty 0 4
Ro_Tunja(config-line)#transport input ssh
Ro_Tunja(config-line)#username Tunja secret password
Ro_Tunja(config)#
```

Ro_Cundinamarca

```
Ro_Cundinamarca>enable
Ro_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#line vty 0 4
Ro_Cundinamarca(config-line)#password cisco
Ro_Cundinamarca(config-line)#login
Ro_Cundinamarca(config-line)#exit
Ro_Cundinamarca(config)#enable secret cisco
Ro_Cundinamarca(config)#ip domain-name CUNDINAMARCA.com
Ro_Cundinamarca(config)#crypto key generate rsa
The name for the keys will be: Ro_Cundinamarca.CUNDINAMARCA.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Ro_Cundinamarca(config)#ip ssh time-out 60
*mar. 1 3:53:36.734: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
Ro_Cundinamarca(config)#ip ssh authentication-retries 2
Ro_Cundinamarca(config)#aaa new-model
Ro_Cundinamarca(config)#line vty 0 4
Ro_Cundinamarca(config-line)#transport input ssh
Ro_Cundinamarca(config-line)#username Cundinamarca secret password
Ro_Cundinamarca(config)#
```

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

```
Ro_Bucaramanga#dir flash
Directory of flash:/
```

```
3 -rw- 5571584 <no date> pt1000-i-mz.122-28.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml
```

```
64016384 bytes total (58188981 bytes free)
```

```
Ro_Bucaramanga#copy flash: tftp:
```

```
Source filename []? pt1000-i-mz.122-28.bin
```

```
Address or name of remote host []? 172.31.2.20
```

```
Destination filename [pt1000-i-mz.122-28.bin]?
```

```
Writing pt1000-i-mz.122-28.bin.....
```

```
[OK - 5571584 bytes]
```

```
5571584 bytes copied in 6.754 secs (4970000 bytes/sec)
```

```
Ro_Tunja#dir flash
Directory of flash:/
```

```
3 -rw- 5571584 <no date> pt1000-i-mz.122-28.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml
```

```
64016384 bytes total (58188981 bytes free)
```

```
Ro_Tunja#copy flash: tftp:
```

```
Source filename []? pt1000-i-mz.122-28.bin
```

```
Address or name of remote host []? 172.31.2.20
```

```
Destination filename [pt1000-i-mz.122-28.bin]?
```

```
Writing pt1000-i-mz.122-28.bin.....
```

```
[OK - 5571584 bytes]
```

```
5571584 bytes copied in 6.754 secs (4970000 bytes/sec)
```

```
Ro_Cundinamarca>enable
Password:
Ro_Cundinamarca#dir flash
Directory of flash:/

3 -rw- 5571584 <no date> pt1000-i-mz.122-28.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml

64016384 bytes total (58188981 bytes free)
Ro_Cundinamarca#copy flash: tftp:
Source filename []? pt1000-i-mz.122-28.bin
Address or name of remote host []? 172.31.2.20
Destination filename [pt1000-i-mz.122-28.bin]?
Writing pt1000-i-mz.122-28.bin.....
[OK - 5571584 bytes]
5571584 bytes copied in 6.754 secs (4970000 bytes/sec)
```

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

Configurando Router Tunja

```
Ro_Tunja>enable
Password:
Ro_Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#ip dhcp excluded-address 172.31.2.1 172.31.2.2
Ro_Tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.2
Ro_Tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.66
Ro_Tunja(config)#ip dhcp excluded-address 172.31.2.9 172.31.2.10
Ro_Tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.66
Ro_Tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.2
Ro_Tunja(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.26
Ro_Tunja(config)#ip dhcp excluded-address 172.31.2.11
Ro_Tunja(config)#ip dhcp pool lan_bucara_v1
Ro_Tunja(dhcp-config)#network 172.31.2.0 255.255.255.248
Ro_Tunja(dhcp-config)#default-router 172.31.0.0 255.255.255.255.192
^
% Invalid input detected at '^' marker.
```

```

Ro_Tunja(dhcp-config)#default-router 172.31.0.0 Ro_Tunja(dhcp-Ro_Tunja(dhcp-
config)#default-router 172.31.0.0 Ro_Tunja(dhcp-Ro_Tunja(dhcp-config)#default-router
172.31.0.0 Ro_Tunja(dhcp-config)#default-router 172.31.2.1
Ro_Tunja(dhcp-config)#ip dhcp pool lan_bucara_v10
Ro_Tunja(dhcp-config)#network 72.31.0.0 255.255.255.192
Ro_Tunja(dhcp-config)#default-router 172.31.0.1
Ro_Tunja(dhcp-config)#ip dhcp pool lan_bucara_v30
Ro_Tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
Ro_Tunja(dhcp-config)#default-router 172.31.0.65
Ro_Tunja(dhcp-config)#ip dhcp pool lan_cundi_v1
Ro_Tunja(dhcp-config)#network 172.31.2.8 255.255.255.248
Ro_Tunja(dhcp-config)#default-router 172.31.2.9
Ro_Tunja(dhcp-config)#ip dhcp pool lan_cundi_v20
Ro_Tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
Ro_Tunja(dhcp-config)#default-router 172.31.1.65
Ro_Tunja(dhcp-config)#ip dhcp pool lan_cundi_v30
Ro_Tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
Ro_Tunja(dhcp-config)#default-router 172.31.1.1
Ro_Tunja(dhcp-config)#ip dhcp pool lan_cundi_v88
Ro_Tunja(dhcp-config)#network 172.31.2.24 255.55.255.248
172.23.2.24 / 255.55.255.248 is an invalid network.
Ro_Tunja(dhcp-config)#network 172.31.2.24 255.255.255.248
Ro_Tunja(dhcp-config)#default-router 172.31.2.25
Ro_Tunja(dhcp-config)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console

```

Ro_Tunja#

Configurando Router Bucaramanga

```

Ro_Bucaramanga>enable
Password:
Ro_Bucaramanga#int fa0/0.1
^
% Invalid input detected at '^' marker.
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#int fa0/0.1
Ro_Bucaramanga(config-subif)#ip helper-address 172.31.2.34
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#int fa0/0.2
Ro_Bucaramanga(config-subif)#ip helper-address 172.31.2.34
Ro_Bucaramanga(config-subif)#exit

```

```
Ro_Bucaramanga(config)#int fa0/0.3
Ro_Bucaramanga(config-subif)#ip helper-address 172.31.2.34
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#exit
Ro_Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

Ro_Bucaramanga#
```

Configurando router Cundinamarca

```
Ro_Cundinamarca>enable
Password:
Ro_Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#int fa0/0.1
Ro_Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.2
Ro_Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.3
Ro_Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#int fa0/0.4
Ro_Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Ro_Cundinamarca(config-subif)#exit
Ro_Cundinamarca(config)#exit
Ro_Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console

Ro_Cundinamarca#
```

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

Configurando Router Tunja

```
Ro_Tunja>enable
Password:
Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#ip nat inside source static 172.31.2.11 209.17.220.7
```

```

Ro_Tunja(config)#ip access-list standart COLOMBIA
^
% Invalid input detected at '^' marker.
Ro_Tunja(config)#ip access-list standard COLOMBIA
Ro_Tunja(config-std-nacl)#permit 172.31.0.0 0.0.255.255
Ro_Tunja(config-std-nacl)#exit
Ro_Tunja(config)#ip nat inside source list COLOMBIA int fa0/0 overload
Ro_Tunja(config)#int fa0/0
Ro_Tunja(config-if)#ip nat outside
Ro_Tunja(config-if)#int s2/0
Ro_Tunja(config-if)#ip nat outside
Ro_Tunja(config-if)#int s3/0
Ro_Tunja(config-if)#ip nat inside
Ro_Tunja(config-if)#int fa0/0.1
Ro_Tunja(config-subif)#ip nat inside
Ro_Tunja(config-subif)#int fa0/0.2
Ro_Tunja(config-subif)#ip nat inside
Ro_Tunja(config-subif)#int fa0/0.3
Ro_Tunja(config-subif)#ip nat inside
Ro_Tunja(config-subif)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console

Ro_Tunja#

```

A continuación se realiza la configuración de la ruta estática predeterminada.

```

Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#ip route 0.0.0.0 0.0.0.0 fa0/0
Ro_Tunja(config)#router ospf 1
Ro_Tunja(config-router)#default-information originate
Ro_Tunja(config-router)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console

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

```

4. El enrutamiento deberá tener autenticación.

Configuración de servidor Bucaramanga

```
Ro_Bucaramanga>enable
Password:
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#router ospf 100
Ro_Bucaramanga(config-router)#router-id 1.1.1.1
Ro_Bucaramanga(config-router)#network 172.31.2.31 0.0.0.3 area0
^
% Invalid input detected at '^' marker.
Ro_Bucaramanga(config-router)#network 172.31.2.31 0.0.0.3 area 0
Ro_Bucaramanga(config-router)#network 172.31.2.0 0.0.0.7 area 0
Ro_Bucaramanga(config-router)#network 172.31.0.1 0.0.0.63 area 0
Ro_Bucaramanga(config-router)#network 172.31.0.64 0.0.0.63 area 0
Ro_Bucaramanga(config-router)#passive-interface fa0/1
%Invalid interface type and number
Ro_Bucaramanga(config-router)#passive-interface fa0/0
Ro_Bucaramanga(config-router)#area 0 authentication
Ro_Bucaramanga(config-router)#exit
Ro_Bucaramanga(config)#int s2/0
Ro_Bucaramanga(config-if)#ip ospf authentication-key osinterpf
%OSPF: Warning: The password/key will be truncated to 8 characters
Ro_Bucaramanga(config-if)#no ip ospf authentication-key osinterpf
Ro_Bucaramanga(config-if)#ip ospf authentication-key DianaOspf
%OSPF: Warning: The password/key will be truncated to 8 characters
Ro_Bucaramanga(config-if)#end
Ro_Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

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

Configuración de servidor Tunja

```
Ro_Tunja>enable
Password:
Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Ro_Tunja(config)#router ospf 100
Ro_Tunja(config-router)#router-id 2.2.2.2
Ro_Tunja(config-router)#network 172.31.2.32 0.0.0.3 area 0
Ro_Tunja(config-router)#network 172.31.2.36 0.0.0.3 area 0
Ro_Tunja(config-router)#network 209.17.220.0 0.0.0.255 area 0
Ro_Tunja(config-router)#network 172.31.2.8 0.0.0.7 area 0
Ro_Tunja(config-router)#network 172.31.0.128 0.0.0.63 area 0
Ro_Tunja(config-router)#network 172.3.2.8 0.0.0.7 area 0
Ro_Tunja(config-router)#network 172.31.0.192 0.0.0.63 area 0
Ro_Tunja(config-router)#passive-interface fa0/0
Ro_Tunja(config-router)#area 0 authentication
Ro_Tunja(config-router)#exit
Ro_Tunja(config)#int s2/0
Ro_Tunja(config-if)#ip ospf authentication-key DianaOspf
%OSPF: Warning: The password/key will be truncated to 8 characters
Ro_Tunja(config-if)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Configuración de servidor Cundinamarca

```
Ro_Cundinamarca>enable
Password:
Ro_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#router ospf 100
Ro_Cundinamarca(config-router)#router-id 3.3.3.3
Ro_Cundinamarca(config-router)#network 172.31.2.36 0.0.0.3 area 0
Ro_Cundinamarca(config-router)#network 172.31.2.8 0.0.0.7 area 0
Ro_Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area 0
Ro_Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area Ro_Cundinamarca(config-
router)#network 172.31.1.0 0.0.0.63 area 0
Ro_Cundinamarca(config-router)#network 172.31.2.24 0.0.0.7 area 0
Ro_Cundinamarca(config-router)#passive-interface fa0/0
Ro_Cundinamarca(config-router)#area 0 authentication
Ro_Cundinamarca(config-router)#exit
Ro_Cundinamarca(config)#
```



```
00:44:19: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Serial2/0 from LOADING to FULL,
Loading Done
```

```
Ro_Cundinamarca(config)#int s2/0
Ro_Cundinamarca(config-if)#ip ospf authentication-key DianaOspf
%OSPF: Warning: The password/key will be truncated to 8 characters
Ro_Cundinamarca(config-if)#end
Ro_Cundinamarca#
```

5. Listas de control de acceso

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

```
Ro_Cundinamarca>enable
Password:
Ro_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#router ospf 100
Ro_Cundinamarca(config-router)#router-id 3.3.3.3
Ro_Cundinamarca(config-router)#network 172.31.2.36 0.0.0.3 area 0
Ro_Cundinamarca(config-router)#network 172.31.2.8 0.0.0.7 area 0
Ro_Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area 0
Ro_Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area Ro_Cundinamarca(config-
router)#network 172.31.1.0 0.0.0.63 area 0
Ro_Cundinamarca(config-router)#network 172.31.2.24 0.0.0.7 area 0
Ro_Cundinamarca(config-router)#passive-interface fa0/0
Ro_Cundinamarca(config-router)#area 0 authentication
Ro_Cundinamarca(config-router)#exit
Ro_Cundinamarca(config)#
00:44:19: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Serial2/0 from LOADING to FULL,
Loading Done
```

```
Ro_Cundinamarca(config)#int s2/0
Ro_Cundinamarca(config-if)#ip ospf authentication-key DianaOspf
%OSPF: Warning: The password/key will be truncated to 8 characters
Ro_Cundinamarca(config-if)#end
Ro_Cundinamarca#
```

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

```

Ro_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#ip access-list extended LANV20
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.0.191 0.0.0.63
Ro_Cundinamarca(config-ext-nacl)#permit ip any any
Ro_Cundinamarca(config-ext-nacl)#exit
Ro_Cundinamarca(config-subif)#int fa0/0.2
Ro_Cundinamarca(config-subif)#ip access-group LANV20 in
Ro_Cundinamarca(config-subif)#end
Ro_Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console
Ro_Cundinamarca#

```

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

```

Ro_Tunja>enable
Password:
Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#ip access-list extended LANV30
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq
% Incomplete command.
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq ftp
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.192 0.0.0.63 0.0.0.0 255.255.255.255 eq www
Ro_Tunja(config-ext-nacl)#exit
Ro_Tunja(config)#int fa0/0.3
Ro_Tunja(config-subif)#ip access-group LANV30 in
Ro_Tunja(config-subif)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
Ro_Tunja#

```

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

```
Ro_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Tunja(config)#ip access-list extended LANV20
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.0.63 172.31.1.0 0.0.0.63
^
% Invalid input detected at '^' marker.
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
Ro_Tunja(config-ext-nacl)#permit tcp 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Ro_Tunja(config-ext-nacl)#exit
Ro_Tunja(config)#int fa0/0.2
Ro_Tunja(config-subif)#ip access-group LANV20 in
Ro_Tunja(config-subif)#end
Ro_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
```

Ro_Tunja#

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

```
Ro_Bucaramanga>enable
Password:
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#ip access-list extended LANV30
^
% Invalid input detected at '^' marker.
Ro_Bucaramanga(config)#ip access-list extended LANV30
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.16 0.0.0.7
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.8 0.0.0.7
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.64 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.24 0.0.0.7
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.128 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#permit ip any any
Ro_Bucaramanga(config-ext-nacl)#exit
Ro_Bucaramanga(config)#int fa0/0.3
Ro_Bucaramanga(config-subif)#ip access-group LANV30 in
Ro_Bucaramanga(config-subif)#end
```

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

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

```
Ro_Bucaramanga>enable
Password:
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#ip access-list extended LANV10
Ro_Bucaramanga(config-ext-nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
Ro_Bucaramanga(config-ext-nacl)#exit
Ro_Bucaramanga(config)#int fa0/0.1
Ro_Bucaramanga(config-subif)#ip access-group LANV10 in
Ro_Bucaramanga(config-subif)#exit
Ro_Bucaramanga(config)#exit
Ro_Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Ro_Bucaramanga#
```

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

```
Ro_Cundinamarca>enable
Password:
Ro_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Cundinamarca(config)#access-list 3 permit 172.31.0.0
Ro_Cundinamarca(config)#interface se2/0
Ro_Cundinamarca(config-if)#ip access-group 3 in
Ro_Cundinamarca(config-if)#exit
Ro_Cundinamarca(config)#ip access-list extended LANV20
Ro_Cundinamarca(config-ext-nacl)#no permit any any
^
% Invalid input detected at '^' marker.
Ro_Cundinamarca(config-ext-nacl)#no permit ip any any
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.1.0 0.0.0.63
Ro_Cundinamarca(config-ext-nacl)#deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
Ro_Cundinamarca(config-ext-nacl)#permit ip any any
Ro_Cundinamarca(config-ext-nacl)#end
Ro_Cundinamarca#
```

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

```
Ro_Cundinamarca#show access-list
Extended IP access list LANV30
10 permit ip 172.31.1.0 0.0.0.63 172.31.2.16 0.0.0.7
20 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
30 permit ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
Extended IP access list LANV20
10 deny ip 172.31.1.64 0.0.0.63 172.31.2.16 0.0.0.7
20 deny ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
30 deny ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7
40 deny ip 172.31.1.64 0.0.0.63 172.31.1.0 0.0.0.63
50 deny ip 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7
60 permit ip any any
Standard IP access list 3
10 permit host 172.31.0.0
Ro_Cundinamarca#
```

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

```
Ro_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Ro_Bucaramanga(config)#ip access-list extended LANV30
Ro_Bucaramanga(config-ext-nacl)#no permit ip any any
Ro_Bucaramanga(config-ext-nacl)#deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
Ro_Bucaramanga(config-ext-nacl)#permit ip any any
Ro_Bucaramanga(config-ext-nacl)#end
Ro_Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Ro_Bucaramanga#show access-list
Extended IP access list LANV30
10 deny ip 172.31.0.64 0.0.0.63 172.31.2.0 0.0.0.7
20 deny ip 172.31.0.64 0.0.0.63 172.31.2.16 0.0.0.7
30 deny ip 172.31.0.64 0.0.0.63 172.31.2.128 0.0.0.63
40 deny ip 172.31.0.64 0.0.0.63 172.31.2.192 0.0.0.63
50 deny ip 172.31.0.64 0.0.0.63 172.31.2.8 0.0.0.7
60 deny ip 172.31.0.64 0.0.0.63 172.31.1.64 0.0.0.63
70 deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
80 deny ip 172.31.0.64 0.0.0.63 172.31.2.24 0.0.0.7
90 deny ip 172.31.0.64 0.0.0.63 172.31.0.128 0.0.0.63
100 deny ip 172.31.0.64 0.0.0.63 172.31.0.192 0.0.0.63
110 permit ip any any
```

```
Extended IP access list LANV10
10 permit ip 172.31.0.0 0.0.0.63 172.31.1.0 0.0.0.63
20 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
Ro_Bucaramanga#
```

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

Aspectos a tener en cuenta

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

Conclusiones

Es importante tener el conocimiento para subnetear la red, ya que este es el punto inicial para configurar una red y si al momento de construir las subredes se realiza de una manera no apropiada, se puede desperdiciar direcciones que no van a ser utilizadas o es posible que la red sea lenta por una configuración innecesaria.

Una red puede ser vulnerada de diferentes maneras, por ello es importante colocar varios niveles de seguridad, así como se colocó claves de acceso a los Routers y los Switch, de manera que sólo los usuarios que estén autorizados (que tengan la clave) puedan acceder a realizar configuraciones y obtener información.

Para complementar la seguridad se utiliza las listas de control de acceso (ACL) en cada router, de manera que haya mayor control en el acceso entre los equipos de la red.

Bibliografía

- Ariganello, E. (s.f.). *Blog CNNA. Configuración de EIGRP*. Obtenido de <https://aprenderedes.com/2006/10/configuracion-de-eigrp/>
- Ariganello, E. (s.f.). *Blog CNNA. Aprende redes. Proceso de configuración de ACL*. Obtenido de <https://aprenderedes.com/2006/11/proceso-de-configuracion-de-acl/>
- Cisco. (2014). *Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación*. Obtenido de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>
- Cisco. (s.f.). *Configurar ACL de IP de uso general*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html#anc5
- Prieto, R. (s.f.). *Blog. Configuración de ACLs con Packet Tracer*. Obtenido de <https://www.raulprietofernandez.net/blog/packet-tracer/configuracion-de-acls-con-packet-tracer>