PRUEBA DE HABILIDADES PRACTICAS – DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRALES LAN/WAN)

EDWARDS ANDRE RUIZ BELTRAN

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
ZIPAQUIRA
2019

PRUEBA DE HABILIDADES PRACTICAS – DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRALES LAN/WAN)

EDWARDS ANDRE RUIZ BELTRAN

PRUEBA DE HABILIDADES PRACTICAS DIPLOMADO DE PROFUNDIZACION CISCO

GIOVANNI ALBERTO BRACHO
TUTOR ECBTI
NANCY AMPARO GUACA G
TUTORA ECBTI

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
ZIPAQUIRA
2019

CONTENIDO

Pag

GLOSARIO

DIRECION IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en red (elemento de comunicación / conexión) de un dispositivo (computadora, Tablet, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

DIRECCIÓN IPv4: Protocolo de Internet versión 4. Estas direcciones constan de 32 bits (0 al 31) particionadas en cuatro grupos de ocho bits cada uno llamados octetos

ENCRIPCION: Proceso de codificar un mensaje de manera que sea incomprensible a usuarios no autorizados. Cuando son recuperados por usuarios autorizados, los mensajes codificados son entonces reconvertido (esto se conoce como decodificado) en un texto significativo. La salida codificada se llama ci-phertext (texto cifrado).

INTERNET: Cuando se usa como nombre y se escribe con i minúscula “internet” es una abreviación para red interconectada, que se refiere a una colección de redes interconectadas que funcionan como una sola red. Cuando se usa con nombre propio y se escribe con I mayúscula “Internet”, se refiere a la red interconectada mas grande del mundo, que consiste en cientos de miles de redes interconectadas en todo el mundo y se basa en un conjunto de estándares de red TCP/IP.

RED: agrupación de sistemas y equipos de cómputo, que se encuentran regidos por protocolos de comunicación, sistemas de direccionamiento, transporte, conmutación y transmisión de información cuya principal función es la optimización de los recursos informáticos y permitir el fácil acceso a la información.

RED DE AREA LOCAL (LAN): Red que interconecta sistemas de computo y equipos de comunicación dentro de un área geográfica de tamaño moderado. Estas redes pueden incluir un cuarto, varios cuartos dentro de un edificio, varios edificios de un campus universitario o un sector empresarial. Estas redes suelen tener un rango máximo de 10 Km de radio.

ROUTER: Originalmente se identificaba con el termino Gateway, sobre todo en referencia a la red de Internet. El Router es el responsable de discernir cual es el camino mas adecuado para la transmisión de mensajes en una red de datos.

SWITCH: Dispositivo lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o mas host pasando datos de un segmento de red a otro de acuerdo con la dirección MAC de destino.

RESUMEN

El Diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integrales LAN / WAN), nos proporcionó un sin número de conocimientos nuevos acerca de las redes LAN / WAN, conocimientos que serán de gran valor para nuestro crecimiento profesional y vida laboral en el ámbito de las redes o áreas de TI afines. Por mi parte tenia los conceptos teóricos de lo que era una red de datos, pero nunca había tenido la oportunidad de trabajar con una herramienta de diseño de redes y en el presente Diplomado pude hacerlo y con esto pude comprender como funciona realmente una red de datos, como se configura un Router, un Switch y cuál es su funcionalidad en el interior de una red de datos. Conceptos que si no son aterrizados en la practicas pueden ser muy ambiguos y generar confusión.

ABSTRACT

The Diploma of deepening CISCO (Design and Implementation of LAN / WAN Integral Solutions), provided us with several new knowledges about LAN / WAN networks, knowledge that will be of great value for our professional growth and working life in the field of networks or related IT areas. For my part I had the theoretical concepts of what a data network was, but I had never had the opportunity to work with a network design tool and in this Diploma I could do it and with this I could understand how a data network really works, how to configure a Router, a Switch and what is its functionality inside a data network. Concepts that if they are not landed in practice can be very ambiguous and generate confusion.

1. INTRODUCCION

Con el presente trabajo practico se pretende poner en práctica cada uno de los conocimientos y destrezas adquiridas durante el desarrollo del Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones Integrales LAN / WAN). Para poner en prácticas los conocimientos y habilidades de cada estudiante del Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones LAN / WAN), se proponen dos escenarios reales con unos requerimientos mínimos de configuración y operatividad que se deberán cumplir para garantizar la operatividad de las redes de datos propuestas.

El presente trabajo se realizará de forma individual por cada uno de los integrantes del Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones LAN / WAN) ya que como su nombre lo indica es una prueba de habilidades prácticas. El presente trabajo se entregará en el entorno de seguimiento y evaluación en las fechas establecidas para su entrega.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Poner en práctica las habilidades y conocimientos adquiridos durante el desarrollo del Diplomado de Profundización CISCO (Diseño e Implementación de soluciones integrales LAN / WAN)

2.2 OBJETIVOS ESPECÍFICOS

- Desplegar la configuración requerida y pertinente para cada uno de los equipos de red del escenario 1.
- Desplegar la configuración requerida y pertinente para cada uno de los equipos de red del escenario 2.
- Detectar fortalezas y falencias para configurar los diferentes equipos de red de cada uno de los escenarios propuestos.
- Subnetear cada una de las redes propuestas de acuerdo con los requerimientos de los escenarios propuestos.

3. ESCENARIO 1

Una empresa posee sucursales 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 si cada uno de los dispositivos que conforman 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.

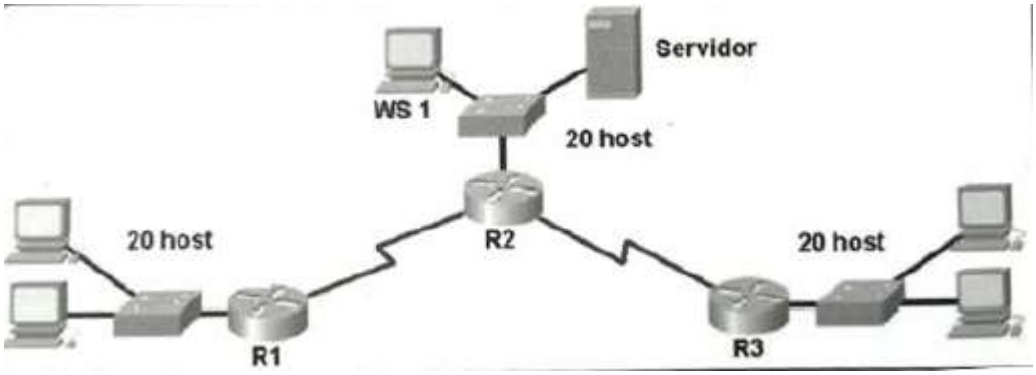

Figura 1. Topología física del escenario 1.

Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección IP 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 los 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.

3.1. CONFIGURACION INICIAL.

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 del SW para la ciudad de Medellín.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-MEDELLIN01
SW-MEDELLIN01(config)#no ip domain-lookup
SW-MEDELLIN01(config)#enable secret class
SW-MEDELLIN01(config)#line con 0
SW-MEDELLIN01(config-line)#password cisco
SW-MEDELLIN01(config-line)#login
SW-MEDELLIN01(config-line)#logging synchronous
SW-MEDELLIN01(config-line)#line vty 0 15
SW-MEDELLIN01(config-line)#password cisco
SW-MEDELLIN01(config-line)#login
SW-MEDELLIN01(config-line)#logging synchronous
SW-MEDELLIN01(config-line)#exit
SW-MEDELLIN01(config)#service password-encryption
SW-MEDELLIN01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-MEDELLIN01(config)# exit
SW-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración del SW para la ciudad de Cali.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CALI01
SW-CALI01(config)#no ip domain-lookup
```

```
SW-CALI01(config)#enable secret class
SW-CALI01(config)#line con 0
SW-CALI01(config-line)#password cisco
SW-CALI01(config-line)#login
SW-CALI01(config-line)#logging synchronous
SW-CALI01(config-line)#line vty 0 15
SW-CALI01(config-line)#password cisco
SW-CALI01(config-line)#login
SW-CALI01(config-line)#logging synchronous
SW-CALI01(config-line)#exit
SW-CALI01(config)#service password-encryption
SW-CALI01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-CALI01(config)#exit
SW-CALI01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración del SW para la ciudad de Bogotá.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BOGOTA01
SW-BOGOTA01(config)#no ip domain-lookup
SW-BOGOTA01(config)#enable secret class
SW-BOGOTA01(config)#line con 0
SW-BOGOTA01(config-line)#password cisco
SW-BOGOTA01(config-line)#login
SW-BOGOTA01(config-line)#logging synchronous
SW-BOGOTA01(config-line)#line vty 0 15
SW-BOGOTA01(config-line)#password cisco
SW-BOGOTA01(config-line)#login
SW-BOGOTA01(config-line)#logging synchronous
SW-BOGOTA01(config-line)#exit
SW-BOGOTA01(config)#service password-encryption
SW-BOGOTA01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-BOGOTA01(config)#exit
SW-BOGOTA01#copy running-config startup-config
```

Destination filename [startup-config]?
Building configuration...
[OK]

Configuración Router para la ciudad de Medellín

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-MEDELLIN01
R-MEDELLIN01(config)#no ip domain-lookup
R-MEDELLIN01(config)#enable secret class
R-MEDELLIN01(config)#line con 0
R-MEDELLIN01(config-line)#password cisco
R-MEDELLIN01(config-line)#login
R-MEDELLIN01(config-line)#logging synchronous
R-MEDELLIN01(config-line)#line vty 0 15
R-MEDELLIN01(config-line)#password cisco
R-MEDELLIN01(config-line)#login
R-MEDELLIN01(config-line)#logging synchronous
R-MEDELLIN01(config-line)#exit
R-MEDELLIN01(config)#service password-encryption
R-MEDELLIN01(config)#login block-for 30 attempts 2 within 120
R-MEDELLIN01(config)#banner motd #Unauthorized access is strictly prohibited#
R-MEDELLIN01(config)#exit
R-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Configuración Router para la ciudad de Cali.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-CALI01
R-CALI01(config)#no ip domain-lookup
R-CALI01(config)#enable secret class
R-CALI01(config)#line con 0

```
R-CALI01(config-line)#password cisco
R-CALI01(config-line)#login
R-CALI01(config-line)#logging synchronous
R-CALI01(config-line)#line vty 0 15
R-CALI01(config-line)#password cisco
R-CALI01(config-line)#login
R-CALI01(config-line)#logging synchronous
R-CALI01(config-line)#exit
R-CALI01(config)#service password-encryption
R-CALI01(config)#login block-for 30 attempts 2 within 120
R-CALI01(config)#banner motd #Unauthorized access is strictly prohibited#
R-CALI01(config)#exit
R-CALI01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración Router para la ciudad de Bogotá.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-BOGOTA01
R-BOGOTA01(config)#no ip domain-lookup
R-BOGOTA01(config)#enable secret class
R-BOGOTA01(config)#line con 0
R-BOGOTA01(config-line)#password cisco
R-BOGOTA01(config-line)#login
R-BOGOTA01(config-line)#logging synchronous
R-BOGOTA01(config-line)#line vty 0 15
R-BOGOTA01(config-line)#password cisco
R-BOGOTA01(config-line)#login
R-BOGOTA01(config-line)#logging synchronous
R-BOGOTA01(config-line)#exit
R-BOGOTA01(config)#service password-encryption
R-BOGOTA01(config)#login block-for 30 attempts 2 within 120
R-BOGOTA01(config)#banner motd #Unauthorized access is strictly prohibited#
R-BOGOTA01(config)#exit
R-BOGOTA01#copy running-config startup-config
```

Destination filename [startup-config]?
Building configuration...
[OK]

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

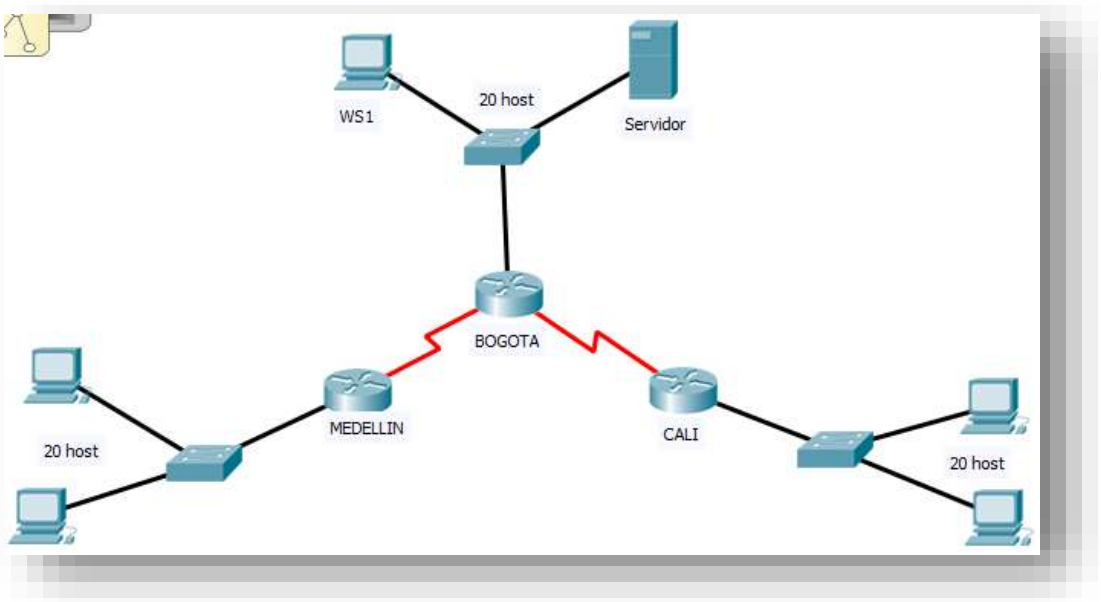

Figura 2. Configurar la topología de red, de acuerdo con las siguientes especificaciones.

3.2. ASIGNACIÓN DE DIRECCIONAMIENTO IP

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

   Para la topología propuesta se trabajará la red 192.168.1.0/24. Con esta **/24** podemos crear 8 segmentos de subred para abarcar 20 hosts en cada uno de ellos.

RED	Gateway	Broadcast	Host
192.168.1.0/27	192.168.1.1	192.168.1.31	20
192.168.1.32/27	192.168.1.33	192.168.1.63	20
192.168.1.64/27	192.168.1.65	192.168.1.95	20
192.168.1.96/27	192.168.1.97	192.168.1.127	20
192.168.1.128/27	192.168.1.129	192.168.1.159	20

192.168.1.160/27	192.168.1.161	192.168.1.191	20
192.168.1.192/27	192.168.1.193	192.168.1.223	20
192.168.1.224/27	192.168.1.225	192.168.1.255	20

Tabla 1. Segmentación de la red 192.168.1.0/24

b. Asignar una dirección IP a la red.

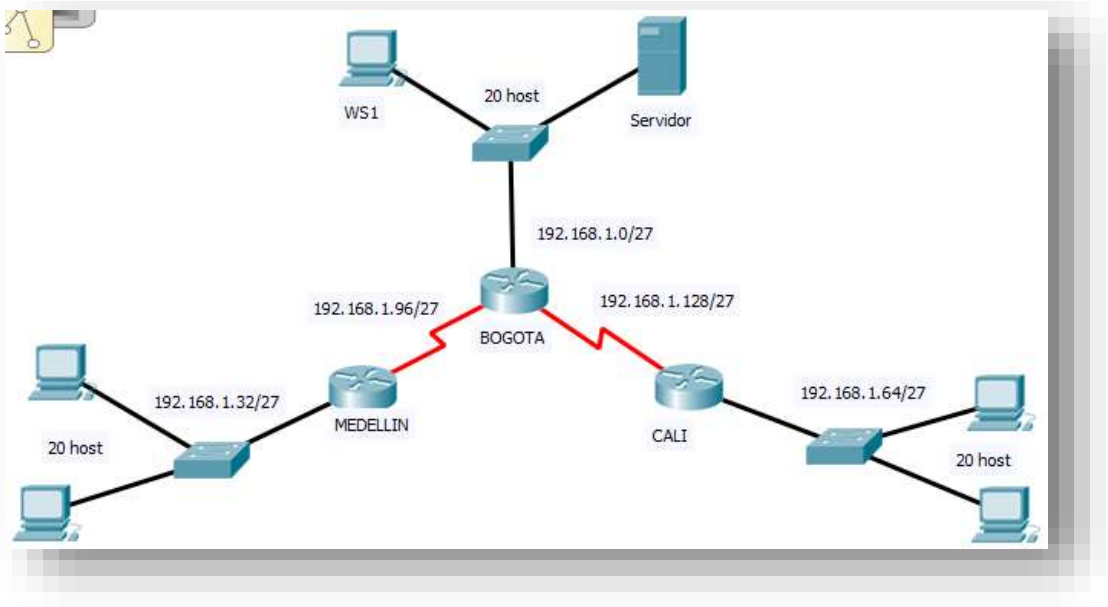

Figura 3. Asignación de redes a la topología propuesta.

3.3. CONFIGURACIÓN DE DIRECCIONAMIENTO IP

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

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	N/A	192.168.1.130	N/A
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

Tabla 2. Configuración IP para las interfaces de los Router.

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

Configuración de interfaces en el Router de la ciudad de Medellín

```
R-MEDELLIN01>enable
Password:
R-MEDELLIN01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-MEDELLIN01(config)#interface G0/0
R-MEDELLIN01(config-if)#no shutdown
R-MEDELLIN01(config-if)#ip address 192.168.1.33 255.255.255.224
R-MEDELLIN01(config-if)#standby 1 ip 192.168.1.35
R-MEDELLIN01(config-if)#interface S0/0/0
R-MEDELLIN01(config-if)#no shutdown
R-MEDELLIN01(config-if)#ip address 192.168.1.99 255.255.255.224
R-MEDELLIN01(config-if)#clock rate 64000
R-MEDELLIN01(config-if)#no shut down
R-MEDELLIN01(config-if)#end
R-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R-MEDELLIN01#show ip interface brief
```

Interface	IP-Address	OK? Method	Status	Protocol
GigabitEthernet0/0	192.168.1.33	YES manual	up	up
GigabitEthernet0/1	unassigned	YES unset	administratively down	down
Serial0/0/0	192.168.1.99	YES manual	up	up
Serial0/0/1	unassigned	YES unset	administratively down	down
Vlan1	unassigned	YES unset	administratively down	down

Configuración de interface VLAN 1 en el Switch de la ciudad de Medellín

```
SW-MEDELLIN01#configure terminal
SW-MEDELLIN01(config)#interface vlan 1
SW-MEDELLIN01(config-if)#no shutdown
SW-MEDELLIN01(config-if)#ip address 192.168.1.34 255.255.255.224
SW-MEDELLIN01(config-if)#ip default-gateway 192.168.1.33
SW-MEDELLIN01(config)#end
SW-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración de interfaces en el Router de la ciudad de Bogotá

```
R-BOGOTA01>enable
Password:
R-BOGOTA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-BOGOTA01(config)#interface S0/0/0
R-BOGOTA01(config-if)#no shutdown
R-BOGOTA01(config-if)#ip address 192.168.1.98 255.255.255.224
R-BOGOTA01(config-if)#interface S0/0/1
R-BOGOTA01(config-if)#no shutdown
R-BOGOTA01(config-if)#ip address 192.168.1.130 255.255.255.224
R-BOGOTA01(config-if)#interface G0/0
R-BOGOTA01(config-if)#no shutdown
R-BOGOTA01(config-if)#ip address 192.168.1.1 255.255.255.224
R-BOGOTA01(config-if)#standby 1 ip 192.168.1.5
R-BOGOTA01(config-if)#end
R-BOGOTA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R-BOGOTA01#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	Administratively down	down
Serial0/0/0	192.168.1.98	YES	manual	up	up
Serial0/0/1	192.168.1.130	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Configuración de interface VLAN 1 en el Switch de la ciudad de Bogotá.

```
SW-BOGOTA01#configure terminal
SW-BOGOTA01(config)#interface vlan 1
SW-BOGOTA01(config-if)#no shutdown
SW-BOGOTA01(config-if)#ip address 192.168.1.2 255.255.255.224
SW-BOGOTA01(config-if)#ip default-gateway 192.168.1.1
SW-BOGOTA01(config)#end
SW-BOGOTA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

[OK]

Configuración de interfaces en el Router de la ciudad de Cali.

```
R-CALI01>enable
Password:
R-CALI01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CALI01(config)#interface S0/0/0
R-CALI01(config-if)#no shutdown
R-CALI01(config-if)#ip address 192.168.1.131 255.255.255.224
R-CALI01(config-if)#clock rate 64000
R-CALI01(config-if)#no shutdown
R-CALI01(config-if)#interface G0/0
R-CALI01(config-if)#no shutdown
R-CALI01(config-if)#ip address 192.168.1.65 255.255.255.224
R-CALI01(config-if)#standby 1 ip 192.168.1.67
R-CALI01(config-if)#end
R-CALI01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

R-CALI01#show ip interface brief

Interface	IP-Address	OK? Method	Status	Protocol
GigabitEthernet0/0	192.168.1.65	YES manual	up	up
GigabitEthernet0/1	unassigned	YES unset	administratively down	down
Serial0/0/0	192.168.1.131	YES manual	up	up
Serial0/0/1	unassigned	YES unset	administratively down	down
Vlan1	unassigned	YES unset	administratively down	down

Configuración de interface VLAN 1 en el Switch de la ciudad de Bogotá.

```
SW-CALI01#configure terminal
SW-CALI01(config)#interface vlan 1
SW-CALI01(config-if)#no shutdown
SW-CALI01(config-if)#ip address 192.168.1.66 255.255.255.224
SW-CALI01(config-if)#ip default-gateway 192.168.1.65
SW-CALI01(config)#end
SW-CALI01#copy running-config startup-config
```

Destination filename [startup-config]?
Building configuration...
[OK]

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

Balanceo de cargas para el Router de la ciudad de Medellín.

R-MEDELLIN01#show ip route 192.168.1.32
Routing entry for 192.168.1.32/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via GigabitEthernet0/0
    Route metric is 0, traffic share count is 1

R-MEDELLIN01#show ip route 192.168.1.96
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Serial0/0/0
    Route metric is 0, traffic share count is 1

Balanceo de cargas para el Router de la ciudad de Bogotá.

R-BOGOTA01#show ip route 192.168.1.0
Routing entry for 192.168.1.0/24, 6 known subnets
Attached (6 connections)
Variably subnetted with 2 masks
C   192.168.1.0/27 is directly connected, GigabitEthernet0/0
        192.168.1.1/32 is directly connected, GigabitEthernet0/0
C   192.168.1.96/27 is directly connected, Serial0/0/0
        192.168.1.98/32 is directly connected, Serial0/0/0
C   192.168.1.128/27 is directly connected, Serial0/0/1
        192.168.1.130/32 is directly connected, Serial0/0/1

R-BOGOTA01#show ip route 192.168.1.96
Routing entry for 192.168.1.96/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

* directly connected, via Serial0/0/0
Route metric is 0, traffic share count is 1

R-BOGOTA01#show ip route 192.168.1.128
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Serial0/0/1
Route metric is 0, traffic share count is 1

Balanceo de cargas para el Router de la ciudad de Bogotá.

R-CALI01#show ip route 192.168.1.128
Routing entry for 192.168.1.128/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Serial0/0/0
Route metric is 0, traffic share count is 1

R-CALI01#show ip route 192.168.1.64
Routing entry for 192.168.1.64/27
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via GigabitEthernet0/0
Route metric is 0, traffic share count is 1

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

Diagnóstico de vecinos para el Router de la ciudad de Medellín.

R-MEDELLIN01#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 Interface	Holdtme	Capability	Platform	Port ID
R-BOGOTA01	Ser 0/0/0	173	R	C1900	Ser 0/0/0

R-MEDELLIN01#

Diagnóstico de vecinos para el Router de la ciudad de Bogotá.

R-BOGOTA01#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-BOGOTA01	Gig 0/0	130	S	2960	Gig 0/1
R-MEDELLIN01	Ser 0/0/0	149	R	C1900	Ser 0/0/0
R-CALI01	Ser 0/0/1	130	R	C1900	Ser 0/0/0

Diagnóstico de vecinos para el Router de la ciudad de Cali.

R-CALI01#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-CALI01	Gig 0/0	123	S	2960	Gig 0/1
R-BOGOTA01	Ser 0/0/0	149	R	C1900	Ser 0/0/1

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

Prueba de conectividad entre dos estaciones de trabajo ubicados en la ciudad de Medellín.

```
C:\>ping 192.168.1.37

Pinging 192.168.1.37 with 32 bytes of data:

Reply from 192.168.1.37: bytes=32 time=2ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Figura 4. Ping desde la PC con IP 192.168.1.36 a la Pc con IP 192.168.1.37

```
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=14ms TTL=128
Reply from 192.168.1.36: bytes=32 time=1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 4ms
```

Figura 5. Ping desde la PC con IP 192.168.1.37 a la Pc con IP 192.168.1.36

Prueba de conectividad entre la estación de trabajo WS1 y el servidor ubicados en la ciudad de Bogotá.

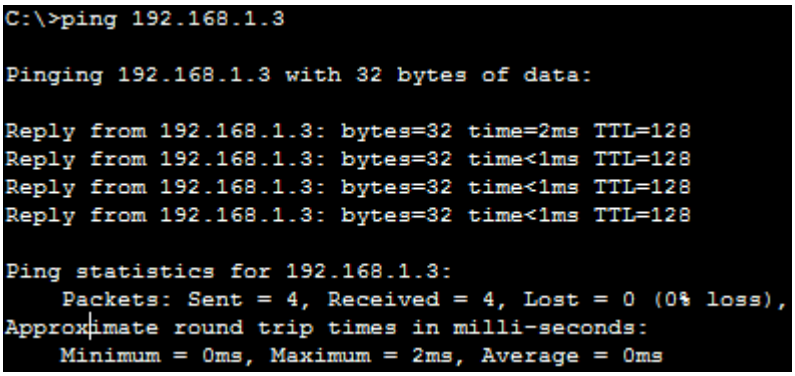

Figura 6. Ping desde la estación de trabajo WS1 con IP 192.168.1.4 al Servidor con IP 192.168.1.3

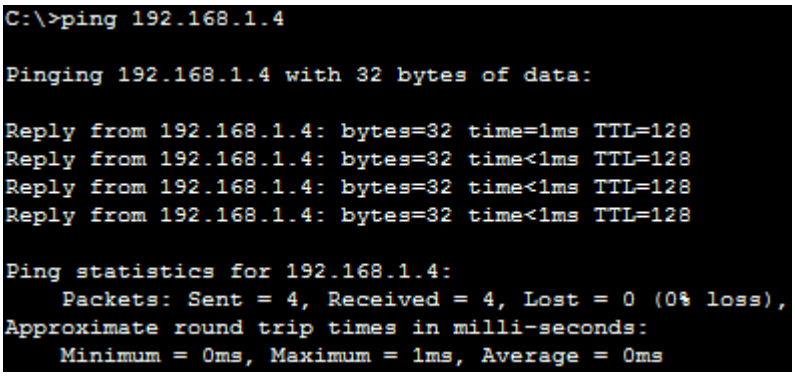

Figura 7. Ping desde el Servidor con IP 192.168.1.3 a la estación de trabajo WS1 con IP 192.168.1.4

Prueba de conectividad entre dos estaciones de trabajo ubicados en la ciudad de Cali.

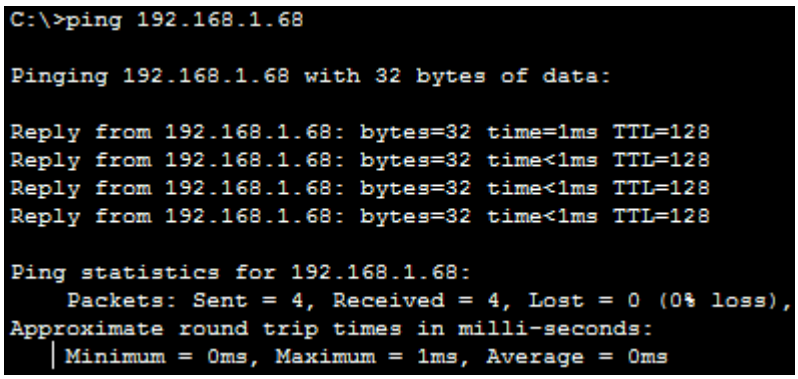

Figura 8. Ping desde la PC con IP 192.168.1.69 a la Pc con IP 192.168.1.68

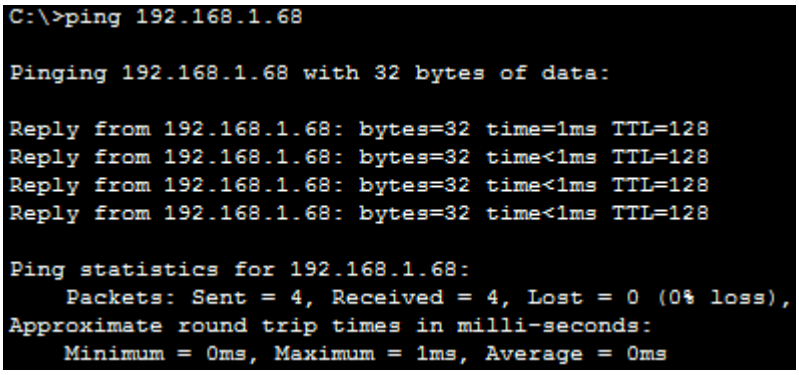

Figura 9. Ping desde la PC con IP 192.168.1.69 a la Pc con IP 192.168.1.68

3.4. CONFIGURACIÓN DE ENRUTAMIENTO.

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

Protocolo de enrutamiento EIGRP en R-MEDELLIN

R-MEDELLIN01(config)#router eigrp 200
R-MEDELLIN01(config-router)#network 192.168.1.32 0.0.0.31
R-MEDELLIN01(config-router)#network 192.168.1.96 0.0.0.31
R-MEDELLIN01(config-router)#no auto-summary
R-MEDELLIN01(config-router)#exit
R-MEDELLIN01(config)#

Protocolo de enrutamiento EIGRP en R-BOGOTA

R-BOGOTA01(config)#router eigrp 200
R-BOGOTA01(config-router)#network 192.168.1.96 0.0.0.31
R-BOGOTA01(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) is up: new adjacency

R-BOGOTA01(config-router)#network 192.168.1.0 0.0.0.31
R-BOGOTA01(config-router)#network 192.168.1.128 0.0.0.31
R-BOGOTA01(config-router)#exit
R-BOGOTA01(config)#

Protocolo de enrutamiento EIGRP en R-CALI

```
R-CALI01(config)#router eigrp 200
R-CALI01(config-router)#network 192.168.1.128 0.0.0.31
R-CALI01(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is
up: new adjacency

R-CALI01(config-router)#network 192.168.1.64 0.0.0.31
R-CALI01(config-router)#exit
R-CALI01(config)
```

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

Vecindad para el Router de la ciudad de Bogotá.

```
R-BOGOTA01#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-BOGOTA01	Gig 0/0	177	S	2960	Gig 0/1
R-MEDELLIN01	Ser 0/0/0	132	R	C1900	Ser 0/0/0
R-CALI01	Ser 0/0/1	140	R	C1900	Ser 0/0/0

```
R-BOGOTA01#
```

Vecindad para el Router de la ciudad de Medellín.

```
R-MEDELLIN01#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-MEDELLIN01	Gig 0/0	156	S	2960	Gig 0/1
R-BOGOTA01	Ser 0/0/0	56	R	C1900	Ser 0/0/0

```
R-MEDELLIN01#
```

Vecindad para el Router de la ciudad de Cali.

```
R-CALI01#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-CALI01	Gig 0/0	164	S	2960	Gig 0/1
R-BOGOTA01	Ser 0/0/0	164	R	C1900	Ser 0/0/1

R-CALI01#

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

Tabla de enrutamiento para el Router de la ciudad de Bogotá.

```
R-BOGOTA01#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, 00:17:24, Serial0/0/0
D      192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:17:22, Serial0/0/1
C      192.168.1.96/27 is directly connected, Serial0/0/0
L      192.168.1.98/32 is directly connected, Serial0/0/0
C      192.168.1.128/27 is directly connected, Serial0/0/1
L      192.168.1.130/32 is directly connected, Serial0/0/1

R-BOGOTA01#
```

Tabla de enrutamiento para el Router de la ciudad de Cali.

```
R-CALI01#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, 00:26:12, Serial0/0/0
D       192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:26:12, Serial0/0/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:26:12, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0
R-CALI01#
```

Tabla de enrutamiento para el Router de la ciudad de Medellín.

```
R-MEDELLIN01#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, 00:31:28, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2682112] via 192.168.1.98, 00:31:26, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:31:28, Serial0/0/0
```

R-MEDELLIN01#

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.

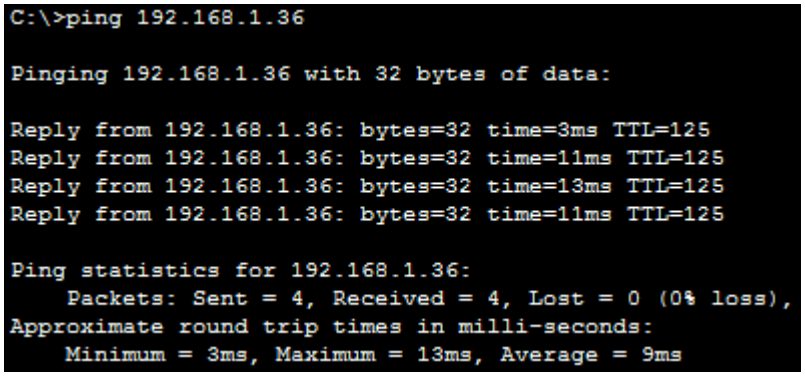

Figura 10- Ping desde la LAN del Router de CALI hacia un host en la LAN de MEDELLIN

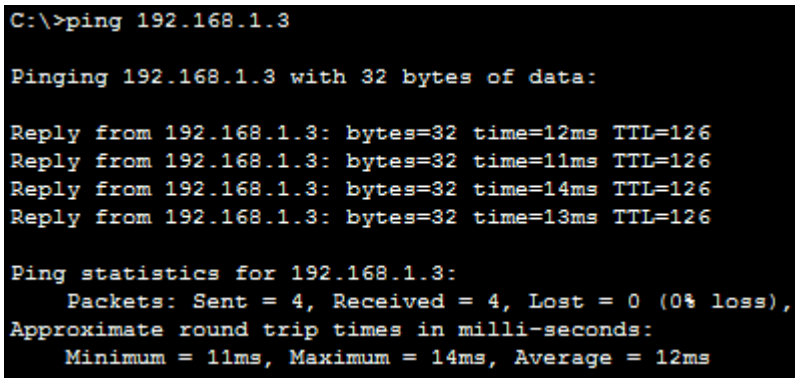

Figura 11. Ping desde la LAN del Router de CALI hacia el server

3.5. 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 Router.

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

Configuración ACL en el Router de la ciudad de Medellín (R-MEDELLIN01).

```
R-MEDELLIN01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.3
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.1
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.98
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.130
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.65
R-MEDELLIN01(config)#access-list 10 permit 192.168.1.131
R-MEDELLIN01(config)#line vty 0 4
R-MEDELLIN01(config-line)#access-class 10 in
R-MEDELLIN01(config-line)#exit
R-MEDELLIN01(config)#line vty 5 15
R-MEDELLIN01(config-line)#access-class 10 in
R-MEDELLIN01(config-line)#end
R-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-MEDELLIN01#
```

Configuración ACL en el Router de la ciudad de Bogotá (R-BOGOTA01).

```
R-BOGOTA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-BOGOTA01(config)#access-list 10 permit 192.168.1.3
R-BOGOTA01(config)#access-list 10 permit 192.168.1.33
R-BOGOTA01(config)#access-list 10 permit 192.168.1.99
R-BOGOTA01(config)#access-list 10 permit 192.168.1.65
R-BOGOTA01(config)#access-list 10 permit 192.168.1.131
R-BOGOTA01(config)#line vty 0 4
R-BOGOTA01(config-line)#access-class 10 in
R-BOGOTA01(config-line)#line vty 5 15
R-BOGOTA01(config-line)#access-class 10 in
R-BOGOTA01(config-line)#end
R-BOGOTA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

R-BOGOTA01#

Configuración ACL en el Router de la ciudad de Cali (R-CALI01).

```
R-CALI01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CALI01(config)#access-list 10 permit 192.168.1.3
R-CALI01(config)#access-list 10 permit 192.168.1.33
R-CALI01(config)#access-list 10 permit 192.168.1.99
R-CALI01(config)#access-list 10 permit 192.168.1.1
R-CALI01(config)#access-list 10 permit 192.168.1.98
R-CALI01(config)#access-list 10 permit 192.168.1.130
R-CALI01(config)#line vty 0 4
R-CALI01(config-line)#access-class 10 in
R-CALI01(config-line)#line vty 5 15
R-CALI01(config-line)#access-class 10 in
R-CALI01(config-line)#end
R-CALI01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-CALI01#
```

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.

Para restringir el acceso de las estaciones de trabajo a los dispositivos de red que se encuentran fuera de su red se ha establecido la lista de acceso "**access-list standard 20**", esta lista de acceso niega el acceso a **telnet** para las estaciones de trabajo de la LAN. Esta lista de acceso permite acceso a telnet para el servidor ubicado en la ciudad de Bogotá, todos los Routers, Switches de la red. Como las direcciones IP de las interfaces de los Router y el servidor son estáticas la ACL se crea por IP.

Configuración ACL (Access-list standard 20) en SW-BOGOTA

```
SW-BOGOTA01(config)#ip access-list standard 20
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.3
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.1
```

```
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.98
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.130
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.99
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.34
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.33
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.131
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.66
SW-BOGOTA01(config-std-nacl)#permit host 192.168.1.65
SW-BOGOTA01(config-std-nacl)#exit
SW-BOGOTA01(config)#line vty 0 15
SW-BOGOTA01(config-line)#access-class 20 in
SW-BOGOTA01(config-line)#end
SW-BOGOTA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BOGOTA01#
```

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

Configuración ACL (Access-list standard 20) en SW-MEDELLIN

```
SW-MEDELLIN01(config)#ip access-list standard 20
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.3
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.2
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.1
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.98
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.130
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.66
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.65
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.131
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.33
SW-MEDELLIN01(config-std-nacl)#permit host 192.168.1.99
SW-MEDELLIN01(config-std-nacl)#exit
SW-MEDELLIN01(config)#line vty 0 15
SW-MEDELLIN01(config-line)#access-class 20 in
SW-MEDELLIN01(config-line)#end
```

```
SW-MEDELLIN01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-MEDELLIN01#
```

Configuración ACL (Access-list standard 20) en el SW-CALI

```
SW-CALI01(config)#ip access-list standar 20
SW-CALI01(config-std-nacl)#permit host 192.168.1.3
SW-CALI01(config-std-nacl)#permit host 192.168.1.2
SW-CALI01(config-std-nacl)#permit host 192.168.1.1
SW-CALI01(config-std-nacl)#permit host 192.168.1.98
SW-CALI01(config-std-nacl)#permit host 192.168.1.130
SW-CALI01(config-std-nacl)#permit host 192.168.1.34
SW-CALI01(config-std-nacl)#permit host 192.168.1.33
SW-CALI01(config-std-nacl)#permit host 192.168.1.99
SW-CALI01(config-std-nacl)#permit host 192.168.1.65
SW-CALI01(config-std-nacl)#permit host 192.168.1.131
SW-CALI01(config-std-nacl)#exit
SW-CALI01(config)#line vty 0 15
SW-CALI01(config-line)#access-class 20 in
SW-CALI01(config-line)#end
SW-CALI01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-CALI01#
```

3.6. VERIFICACIÓN DE LA RED.

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

Telnet desde el Router de la ciudad de Medellín al Router de la ciudad de Bogotá.

```
R-MEDELLIN01#telnet 192.168.1.1
Trying 192.168.1.1 ...OpenUnauthorized access is strictly prohibited
```

User Access Verification

Password:
R-BOGOTA01>enable
Password:
R-BOGOTA01#

Telnet desde el Router de la ciudad de Bogotá al Router de la ciudad de Cali.

R-BOGOTA01#telnet 192.168.1.131
Trying 192.168.1.131 ...OpenUnauthorized access is strictly prohibited

User Access Verification

Password:
R-CALI01>enable
Password:
R-CALI01#

Telnet desde el Router de la ciudad de Cali al Router de la ciudad de Medellín.

R-CALI01#telnet 192.168.1.99
Trying 192.168.1.99 ...OpenUnauthorized access is strictly prohibited

User Access Verification

Password:
R-MEDELLIN01>enable
Password:
R-MEDELLIN01#

b. Comprobar y completar la siguiente tabla de direcciones de prueba para confirmar el óptimo funcionamiento de la red.

ORIGEN		DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	OK
	WS_1	**Router BOGOTA**	Refused
	Servidor	**Router CALI**	OK
	Servidor	**Router MEDELLIN**	OK

TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Refused
	LAN del Router CALI	**Router CALI**	Refused
	LAN del Router MEDELLIN	**Router MEDELLIN**	Refused
	LAN del Router CALI	**Router MEDELLIN**	Refused
PING	**LAN del Router CALI**	**WS_1**	OK
	LAN del Router MEDELLIN	**WS_1**	OK
	LAN del Router MEDELLIN	**LAN del Router CALI**	OK
PING	**LAN del Router CALI**	**Servidor**	OK
	LAN del Router MEDELLIN	**Servidor**	OK
	Servidor	**LAN del Router MEDELLIN**	OK
	Servidor	**LAN del Router CALI**	OK
	Router CALI	**LAN del Router MEDELLIN**	OK
	Router MEDELLIN	**LAN del Router CALI**	OK

Tabla 3. Tabla de pruebas de conectividad para la red.

4. ESCENARIO 2

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

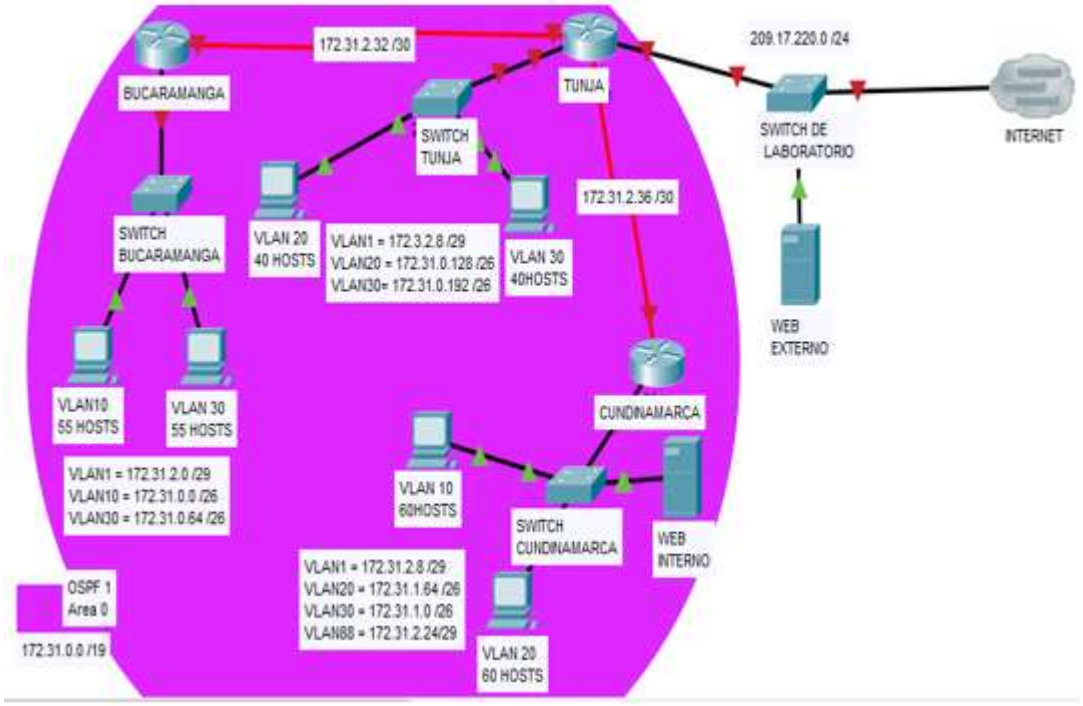

Figura 12. Topología escenario 2.

4.1. CONFIGURACIÓN INICIAL

Cada uno de los Router del escenario propuesto deben cumplir con los siguientes requerimientos de configuración.

- ✓ Configuración básica.
- ✓ Autenticación local con AAA.
- ✓ Cifrado de contraseñas.
- ✓ Un máximo tiempo de acceso al detectar ataques.
- ✓ Establecer un servidor TFTP y almacenar todos los archivos necesarios de los Router.

Configuración de los equipos de red para la sede de Bucaramanga.

Configuración del SW instalado en la sede de Bucaramanga.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BUCARAMANGA
SW-BUCARAMANGA01(config)#no ip domain-lookup
SW-BUCARAMANGA01(config)#enable secret class
SW-BUCARAMANGA01(config)#line con 0
SW-BUCARAMANGA01(config-line)#password cisco
SW-BUCARAMANGA01(config-line)#login
SW-BUCARAMANGA01(config-line)#loggin synchronous
SW-BUCARAMANGA01(config-line)#line vty 0 15
SW-BUCARAMANGA01(config-line)#password cisco
SW-BUCARAMANGA01(config-line)#login
SW-BUCARAMANGA01(config-line)#loggin synchronous
SW-BUCARAMANGA01(config-line)#exit
SW-BUCARAMANGA01(config)#service password-encryption
SW-BUCARAMANGA01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-BUCARAMANGA01(config)#exit
SW-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BUCARAMANGA01#
```

Configuración de la Vlan 1 en el SW de Bucaramanga para poder tener gestión del equipo

```
SW-BUCARAMANGA01(config)#interface vlan 1
SW-BUCARAMANGA01(config-if)#description Vlan1
SW-BUCARAMANGA01(config-if)#no shutdown
SW-BUCARAMANGA01(config-if)#ip address 172.31.2.3 255.255.255.248
SW-BUCARAMANGA01(config-if)#ip default-gateway 172.31.2.1
SW-BUCARAMANGA01(config-if)#end
SW-BUCARAMANGA01#copy running-config startup-config
```

Destination filename [startup-config]?
Building configuration...
[OK]
SW-BUCARAMANGA01#

Creación de las Vlan 10 y Vlan 30 presentes en la red LAN de la sede de Bucaramanga.

Creación Vlan 10 en el SW-BUCARAMANGA01

SW-BUCARAMANGA01(config)#interface vlan 10
SW-BUCARAMANGA01(config-if)#description Vlan10
SW-BUCARAMANGA01(config-if)#exit
SW-BUCARAMANGA01(config)#

Creación Vlan 30 en el SW-BUCARAMANGA01

SW-BUCARAMANGA01(config)#interface vlan 30
SW-BUCARAMANGA01(config-if)#description Vlan30
SW-BUCARAMANGA01(config-if)#exit
SW-BUCARAMANGA01(config)# do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BUCARAMANGA01(config)#exit

Asignación de las Vlan 10 y Vlan 30 en los puertos del SW-BUCARAMANGA01, para efectos del presente trabajo solo se va a configurar la interface Fa0/1 con la Vlan 10 y la interface fa0/2 con la Vlan 30. Los demás puertos se dejarán en modo shutdown.

SW-BUCARAMANGA01(config)#interface f0/1
SW-BUCARAMANGA01(config-if)#switchport mode access
SW-BUCARAMANGA01(config-if)#switchport access Vlan 10
SW-BUCARAMANGA01(config-if)#exit

SW-BUCARAMANGA01(config)#interface f0/2
SW-BUCARAMANGA01(config-if)#switchport mode access
SW-BUCARAMANGA01(config-if)#switchport access Vlan 30

SW-BUCARAMANGA01(config-if)#exit

SW-BUCARAMANGA01(config)#interface range f0/3-24
SW-BUCARAMANGA01(config-if-range)#shutdown
SW-BUCARAMANGA01(config-if-range)#end
SW-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BUCARAMANGA01#

Para poder permitir el ruteo entre las Vlan y poder interconectar las demás sedes requerimos de un Router para salir de la sede y el puerto que nos va a realizar esta interconexión debe ser un puerto troncal o Trunk (puerto de transporte)

Configuración de la Interface Ga0/1 como puerto Trunk

SW-BUCARAMANGA01(config)#interface G0/1
SW-BUCARAMANGA01(config-if)#switchport mode trunk
SW-BUCARAMANGA01(config-if)#switchport trunk allowed vlan 1,20,30,1002-1005
SW-BUCARAMANGA01(config-if)#end
SW- BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW- BUCARAMANGA01#

Configuración del Router instalado en la sede de Bucaramanga, el cual se etiquetará como R-BUCARAMANGA01.

Router>enable
Router#configure terminal
Router(config)#hostname R-BUCARAMANGA01
R-BUCARAMANGA01(config)#no ip domain-lookup
R-BUCARAMANGA01(config)#enable secret class
R-BUCARAMANGA01(config)#line con 0
R-BUCARAMANGA01(config-line)#password cisco
R-BUCARAMANGA01(config-line)#login
R-BUCARAMANGA01(config-line)#loggin synchronous

```
R-BUCARAMANGA01(config-line)#line vty 0 15
R-BUCARAMANGA01(config-line)#password cisco
R-BUCARAMANGA01(config-line)#login
R-BUCARAMANGA01(config-line)#loggin synchronous
R-BUCARAMANGA01(config-line)#exit
R-BUCARAMANGA01(config)#login block-for 30 attempts 2 within 120
R-BUCARAMANGA01(config)#service password-encryption
R-BUCARAMANGA01(config)#banner motd #Unauthorized access is strictly prohibited#
R-BUCARAMANGA01(config)#interface S0/0/0
R-BUCARAMANGA01(config-if)#no shutdown
R-BUCARAMANGA01(config-if)#ip address 172.31.2.34 255.255.255.252
R-BUCARAMANGA01(config-if)#clock rate 64000
R-BUCARAMANGA01(config-if)#end
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-BUCARAMANGA01#
```

Configuramos el Router para que nos permita realizar ruteo entre las diferentes Vlan. Adicionalmente debemos levantar la interface Ga0/0 que por default se encuentra en modo shutdown.

```
R-BUCARAMANGA01(config)#interface G0/0
R-BUCARAMANGA01(config-if)#no shutdown
R-BUCARAMANGA01(config-if)#exit

R-BUCARAMANGA01(config)#interface G0/0.1
R-BUCARAMANGA01(config-subif)#encapsulation dot1Q 1 Native
R-BUCARAMANGA01(config-subif)#ip address 172.31.2.2 255.255.255.248
R-BUCARAMANGA01(config-subif)#standby 1 ip 172.31.2.1
R-BUCARAMANGA01(config-subif)#exit

R-BUCARAMANGA01(config)#interface G0/0.10
R-BUCARAMANGA01(config-subif)#encapsulation dot1Q 10
R-BUCARAMANGA01(config-subif)#ip address 172.31.0.2 255.255.255.192
R-BUCARAMANGA01(config-subif)#standby 10 ip 172.31.0.1
R-BUCARAMANGA01(config-subif)#exit
```

```
R-BUCARAMANGA01(config)#interface G0/0.30
R-BUCARAMANGA01(config-subif)#encapsulation dot1Q 30
R-BUCARAMANGA01(config-subif)#ip address 172.31.0.66 255.255.255.192
R-BUCARAMANGA01(config-subif)#standby 30 ip 172.31.0.65
R-BUCARAMANGA01(config-subif)#exit

R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración de los equipos de red para la sede de Tunja.

Configuración del SW instalado en la sede de Tunja.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname
Switch(config)#hostname SW-TUNJA01
SW-TUNJA01(config)#no ip domain-lookup
SW-TUNJA01(config)#enable secret class
SW-TUNJA01(config)#line con 0
SW-TUNJA01(config-line)#password cisco
SW-TUNJA01(config-line)#login
SW-TUNJA01(config-line)#loggin synchronous
SW-TUNJA01(config-line)#line vty 0 15
SW-TUNJA01(config-line)#password cisco
SW-TUNJA01(config-line)#login
SW-TUNJA01(config-line)#loggin synchronous
SW-TUNJA01(config-line)#exit
SW-TUNJA01(config)#service password-encryption
SW-TUNJA01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-TUNJA01(config)#exit
SW-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

SW-TUNJA01#

Configuración de la Vlan 1 en el SW de Tunja para poder tener gestión del equipo

SW-TUNJA01(config)#interface vla 1
SW-TUNJA01(config-if)#description Vlan1
SW-TUNJA01(config-if)#no shutdown
SW-TUNJA01(config-if)#ip address 172.31.2.11 255.255.255.248
SW-TUNJA01(config-if)#ip default-gateway 172.31.2.9
SW-TUNJA01(config-if)#end
SW-TUNJA01# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-TUNJA01(config)#

Creación de la Vlan 20 y la Vlan 30 presentes en la red LAN de la sede de Tunja.

Creación Vlan 20 en el SW-TUNJA01

SW-TUNJA01(config)#interface vlan 20
SW-TUNJA01(config-vlan)#description Vlan20
SW-TUNJA01(config-vlan)#exit
SW-TUNJA01(config)#do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-TUNJA01(config)#

Creación Vlan 30 en el SW-TUNJA01

SW-TUNJA01(config)#interface vlan 30
SW-TUNJA01(config-vlan)#description Vlan30
SW-TUNJA01(config-vlan)#exit
SW-TUNJA01(config)#do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-TUNJA01(config)#exit

Asignación de la Vlan 20 y la Vlan 30 en las interfaces del SW-TUNJA01, para efectos del presente trabajo solo se va a configurar la interface Fa0/1 con la Vlan 20 y la interface fa0/2 con la Vlan 30. Los demás puertos se dejarán en modo shutdown.

```
SW- TUNJA01 (config)#interface f0/1
SW- TUNJA01 (config-if)#switchport mode access
SW- TUNJA01 (config-if)#switchport access Vlan 20
SW- TUNJA01 (config-if)#exit

SW- TUNJA01 (config)#interface f0/2
SW- TUNJA01 (config-if)#switchport mode access
SW- TUNJA01 (config-if)#switchport access Vlan 30
SW- TUNJA01 (config-if)#exit

SW-TUNJA01(config)#interface range f0/3-24
SW- TUNJA01 (config-if-range)#shutdown
SW- TUNJA01 (config-if-range)#end
SW- TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW- TUNJA01#
```

Para poder permitir el ruteo entre las Vlan y poder interconectar las demás sedes requerimos de un Router para salir de la sede y el puerto que nos va a realizar esta interconexión debe ser un puerto troncal o Trunk (puerto de transporte)

Configuración de la Interface Ga0/1 como puerto Trunk

```
SW-TUNJA01(config)#interface G0/1
SW-TUNJA01(config-if)#switchport mode trunk
SW-TUNJA01(config-if)#switchport trunk allowed vlan 1,20,30,1002-1005
SW-TUNJA01(config-if)#end
SW-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-TUNJA01#
```

Configuración del Router instalado en la sede de Tunja, el cual se etiquetará como R-TUNJA01.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-TUNJA01
R-TUNJA01(config)#no ip domain-lookup
R-TUNJA01(config)#enable secret class
R-TUNJA01(config)#line con 0
R-TUNJA01(config-line)#password cisco
R-TUNJA01(config-line)#login
R-TUNJA01(config-line)#loggin synchronous
R-TUNJA01(config-line)#line vty 0 15
R-TUNJA01(config-line)#password cisco
R-TUNJA01(config-line)#login
R-TUNJA01(config-line)#loggin synchronous
R-TUNJA01(config-line)#exit
R-TUNJA01(config)#login block-for 30 attempts 2 within 120
R-TUNJA01(config)#service password-encryption
R-TUNJA01(config)#banner motd #Unauthorized access is strictly prohibited#
R-TUNJA01(config)#exit
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-TUNJA01#
```

Configuración de las interfaces del R-TUNJA01

```
R-TUNJA01(config)#interface G0/0
R-TUNJA01(config-if)#no shutdown
R-TUNJA01(config-if)#ip address 209.17.220.1 255.255.255.0
R-TUNJA01(config-if)#exit
R-TUNJA01(config)#interface G0/1
R-TUNJA01(config-if)#ip address 172.31.2.9 255.255.255.248
R-TUNJA01(config-if)#exit
R-TUNJA01(config)#interface S0/0/0
R-TUNJA01(config-if)#no shutdown
```

```
R-TUNJA01(config-if)#ip address 172.31.2.33 255.255.255.252
R-TUNJA01(config-if)#exit
R-TUNJA01(config)#interface S0/0/1
R-TUNJA01(config-if)#no shutdown
R-TUNJA01(config-if)#ip address 172.31.2.37 255.255.255.252
R-TUNJA01(config-if)#end
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuramos el Router para que nos permita realizar ruteo entre las diferentes Vlan. Adicionalmente debemos levantar la interface Ga0/1 que por default se encuentra en modo shutdown.

```
R-TUNJA01(config)#interface G0/1
R-TUNJA01(config-if)#no shutdown
R-TUNJA01(config-if)#exit

R-TUNJA01(config)#interface G0/1.1
R-TUNJA01(config-subif)#encapsulation dot1Q 1 Native
R-TUNJA01(config-subif)#ip address 172.31.2.10 255.255.255.248
R-TUNJA01(config-subif)#standby 1 ip 172.31.2.9
R-TUNJA01(config-subif)#exit

R-TUNJA01(config)#interface G0/1.20
R-TUNJA01(config-subif)#encapsulation dot1Q 20
R-TUNJA01(config-subif)#ip address 172.31.0.130 255.255.255.192
R-TUNJA01(config-subif)#standby 20 ip 172.31.0.129
R-TUNJA01(config-subif)#exit

R-TUNJA01(config)#interface G0/1.30
R-TUNJA01(config-subif)#encapsulation dot1Q 30
R-TUNJA01(config-subif)#ip address 172.31.0.194 255.255.255.192
R-TUNJA01(config-subif)#standby 30 ip 172.31.0.193
R-TUNJA01(config-subif)#end

R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
```

Building configuration...
[OK]

Configuración de los equipos de red para la sede de Cundinamarca.

Configuración del SW instalado en la sede de Cundinamarca.

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CUNDINAMARCA01
SW-CUNDINAMARCA01(config)#no ip domain-lookup
SW-CUNDINAMARCA01(config)#enable secret class
SW-CUNDINAMARCA01(config)#line con 0
SW-CUNDINAMARCA01(config-line)#password cisco
SW-CUNDINAMARCA01(config-line)#login
SW-CUNDINAMARCA01(config-line)#loggin synchronous
SW-CUNDINAMARCA01(config-line)#line vty 0 15
SW-CUNDINAMARCA01(config-line)#password cisco
SW-CUNDINAMARCA01(config-line)#login
SW-CUNDINAMARCA01(config-line)#loggin synchronous
SW-CUNDINAMARCA01(config-line)#exit
SW-CUNDINAMARCA01(config)#service password-encryption
SW-CUNDINAMARCA01(config)#banner motd #Unauthorized access is strictly prohibited#
SW-CUNDINAMARCA01(config)#exit
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-CUNDINAMARCA01#

Configuración de la Vlan 1 en el SW de Cundinamarca para poder tener gestión remota del equipo

SW-CUNDINAMARCA01(config)#interface vlan 1
SW-CUNDINAMARCA01(config-if)#description Vlan1
SW-CUNDINAMARCA01(config-if)#no shutdown
SW-CUNDINAMARCA01(config-if)#ip address 172.31.2.19 255.255.255.248

SW-CUNDINAMARCA01(config-if)#ip default-gateway 172.31.2.17
SW-CUNDINAMARCA01(config)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-CUNDINAMARCA01#

Creación de la Vlan 20, la Vlan 30 y Vlan 88 presentes en la red LAN de la sede de Cundinamarca.

Creación Vlan 20 en el SW-CUNDINAMARCA01

SW-CUNDINAMARCA01(config)#interface vlan 20
SW-CUNDINAMARCA01(config-if)#description Vlan20
SW-CUNDINAMARCA01(config-if)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Creación Vlan 30 en el SW-CUNDINAMARCA01

SW-CUNDINAMARCA01(config)#interface vlan 30
SW-CUNDINAMARCA01(config-if)#description Vlan30
SW-CUNDINAMARCA01(config-if)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Creación Vlan 88 en el SW-CUNDINAMARCA01

SW-CUNDINAMARCA01(config)#interface vlan 88
SW-CUNDINAMARCA01(config-if)#description Vlan88
SW-CUNDINAMARCA01(config-if)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

[OK]

Asignación de la Vlan 20 y la Vlan 30 en las interfaces del SW-CUNDINAMARCA01, para efectos del presente trabajo solo se va a configurar la interface Fa0/1 con la Vlan 20, la interface fa0/2 con la Vlan 30 y la interface G0/2 con la Vlan 88. Los demás puertos se dejarán en modo shutdown.

```
SW-CUNDINAMARCA01(config)#interface f0/1
SW-CUNDINAMARCA01(config-if)#switchport mode access
SW-CUNDINAMARCA01(config-if)#switchport access vlan 20
SW-CUNDINAMARCA01(config-if)#exit

SW-CUNDINAMARCA01(config)#interface f0/2
SW-CUNDINAMARCA01(config-if)#switchport mode access
SW-CUNDINAMARCA01(config-if)#switchport access vlan 30
SW-CUNDINAMARCA01(config-if)#exit

SW-CUNDINAMARCA01(config)#interface G0/2
SW-CUNDINAMARCA01(config-if)#switchport mode access
SW-CUNDINAMARCA01(config-if)#switchport access vlan 88
SW-CUNDINAMARCA01(config-if)#exit

SW-CUNDINAMARCA01(config)#interface range f0/3-24
SW-CUNDINAMARCA01(config-if-range)#shutdown
SW-CUNDINAMARCA01(config-if-range)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Para poder permitir el ruteo entre las Vlan y poder interconectar las demás sedes requerimos de un Router para salir de la sede y el puerto que nos va a realizar esta interconexión debe ser un puerto troncal o Trunk (puerto de transporte)

Configuración de la Interface Ga0/1 como puerto Trunk

```
SW-CUNDINAMARCA01(config)#interface G0/1
SW-CUNDINAMARCA01(config-if)#switchport mode trunk
```

SW-CUNDINAMARCA01(config-if)#switchport trunk allowed vlan 1,20,30,88,1002-1005
SW-CUNDINAMARCA01(config-if)#end
SW-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Configuración del Router instalado en la sede de Cundinamarca, el cual se etiquetará como R-CUNDINAMARCA01.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-CUNDINAMARCA01
R-CUNDINAMARCA01(config)#no ip domain-lookup
R-CUNDINAMARCA01(config)#enable secret class
R-CUNDINAMARCA01(config)#line con 0
R-CUNDINAMARCA01(config-line)#password cisco
R-CUNDINAMARCA01(config-line)#login
R-CUNDINAMARCA01(config-line)#loggin synchronous
R-CUNDINAMARCA01(config-line)#line vty 0 15
R-CUNDINAMARCA01(config-line)#password cisco
R-CUNDINAMARCA01(config-line)#login
R-CUNDINAMARCA01(config-line)#loggin synchronous
R-CUNDINAMARCA01(config-line)#exit
R-CUNDINAMARCA01(config)#login block-for 30 attempts 2 within 120
R-CUNDINAMARCA01(config)#service password-encryption
R-CUNDINAMARCA01(config)#banner motd #Unauthorized access is strictly prohibited#
R-CUNDINAMARCA01(config)#

Configuración de las interfaces del R-CUNDINAMARCA01

R-CUNDINAMARCA01(config)#interface S0/0/0
R-CUNDINAMARCA01(config-if)#no shutdown
R-CUNDINAMARCA01(config-if)#ip address 172.31.2.38 255.255.255.252
R-CUNDINAMARCA01(config-if)#clock rate 64000
R-CUNDINAMARCA01(config)#exit

```
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuramos el Router para que nos permita realizar ruteo entre las diferentes Vlan. Adicionalmente debemos levantar la interface Ga0/0 que por default se encuentra en modo shutdown.

```
R-CUNDINAMARCA01(config)#interface G0/0
R-CUNDINAMARCA01(config-if)#no shutdown
R-CUNDINAMARCA01(config)#

R-CUNDINAMARCA01(config)#interface G0/0.1
R-CUNDINAMARCA01(config-subif)#encapsulation dot1Q 1 Native
R-CUNDINAMARCA01(config-subif)#ip address 172.31.2.18 255.255.255.248
R-CUNDINAMARCA01(config-subif)#standby 1 ip 172.31.2.17
R-CUNDINAMARCA01(config-subif)#exit

R-CUNDINAMARCA01(config)#interface G0/0.20
R-CUNDINAMARCA01(config-subif)#encapsulation dot1Q 20
R-CUNDINAMARCA01(config-subif)#ip address 172.31.1.66 255.255.255.192
R-CUNDINAMARCA01(config-subif)#standby 20 ip 172.31.1.65
R-CUNDINAMARCA01(config-subif)#exit

R-CUNDINAMARCA01(config)#interface G0/0.30
R-CUNDINAMARCA01(config-subif)#encapsulation dot1Q 30
R-CUNDINAMARCA01(config-subif)#ip address 172.31.1.2 255.255.255.192
R-CUNDINAMARCA01(config-subif)#standby 30 ip 172.31.1.1
R-CUNDINAMARCA01(config-subif)#exit

R-CUNDINAMARCA01(config)#interface G0/0.88
R-CUNDINAMARCA01(config-subif)#encapsulation dot1Q 88
R-CUNDINAMARCA01(config-subif)#ip address 172.31.2.26 255.255.255.248
R-CUNDINAMARCA01(config-subif)#standby 88 ip 172.31.2.25
R-CUNDINAMARCA01(config-subif)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

[OK]
R-CUNDINAMARCA01#

4.2. ENRUTAMIENTO OSPF CON AUTENTICACIÓN

En el presente escenario vamos a realizar enrutamiento OSPF cifrado para garantizar seguridad en la red. Este enrutamiento nos permite mitigar ataques a la red mediante bucles generados por tablas de routing falsas que podría crear una persona que logre alcanzar la interfaz WAN de la red.

Enrutamiento OSPF para el Router instalado en la sede de Bucaramanga

```
R-BUCARAMANGA01#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

       172.31.0.0/16 is variably subnetted, 8 subnets, 4 masks
C         172.31.0.0/26 is directly connected, GigabitEthernet0/0.10
L         172.31.0.2/32 is directly connected, GigabitEthernet0/0.10
C         172.31.0.64/26 is directly connected, GigabitEthernet0/0.30
L         172.31.0.66/32 is directly connected, GigabitEthernet0/0.30
C         172.31.2.0/29 is directly connected, GigabitEthernet0/0.1
L         172.31.2.2/32 is directly connected, GigabitEthernet0/0.1
C         172.31.2.32/30 is directly connected, Serial0/0/0
L         172.31.2.34/32 is directly connected, Serial0/0/0
```

Con el comando show ip route podemos observar las redes que se encuentran conectadas al Router de la sede de Cundinamarca. Una vez determinadas las redes conectadas al Router procedemos a configurar el enrutamiento OSPF.

```
R-BUCARAMANGA01#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R-BUCARAMANGA01(config)#router ospf 1
R-BUCARAMANGA01(config-router)#router-id 2.2.2.2
R-BUCARAMANGA01(config-router)#network 172.31.0.0 0.0.0.63 area 0
R-BUCARAMANGA01(config-router)#network 172.31.0.64 0.0.0.63 area 0
R-BUCARAMANGA01(config-router)#network 172.31.2.0 0.0.0.7 area 0
R-BUCARAMANGA01(config-router)#network 172.31.2.32 0.0.0.3 area 0
R-BUCARAMANGA01(config-router)#end
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Enrutamiento OSPF para el Router instalado en la sede de Tunja

```
R-TUNJA01#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

       172.31.0.0/16 is variably subnetted, 10 subnets, 4 masks
C            172.31.0.128/26 is directly connected, GigabitEthernet0/1.20
L            172.31.0.130/32 is directly connected, GigabitEthernet0/1.20
C            172.31.0.192/26 is directly connected, GigabitEthernet0/1.30
L            172.31.0.194/32 is directly connected, GigabitEthernet0/1.30
C            172.31.2.8/29 is directly connected, GigabitEthernet0/1.1
L            172.31.2.10/32 is directly connected, GigabitEthernet0/1.1
C            172.31.2.32/30 is directly connected, Serial0/0/0
L            172.31.2.33/32 is directly connected, Serial0/0/0
C            172.31.2.36/30 is directly connected, Serial0/0/1
L            172.31.2.37/32 is directly connected, Serial0/0/1
       209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C           209.17.220.0/24 is directly connected, GigabitEthernet0/0
```

```
L        209.17.220.1/32 is directly connected, GigabitEthernet0/0

R-TUNJA01(config)#router ospf 1
R-TUNJA01(config-router)#router-id 1.1.1.1
R-TUNJA01(config-router)#network 172.31.0.128 0.0.0.63 area 0
R-TUNJA01(config-router)#network 172.31.0.192 0.0.0.63 area 0
R-TUNJA01(config-router)#network 172.31.2.8 0.0.0.7 area 0
R-TUNJA01(config-router)#network 172.31.2.32 0.0.0.3 area 0
R-TUNJA01(config-router)#network 172.31.2.36 0.0.0.3 area 0
R-TUNJA01(config-router)#network 209.17.220.0 0.0.0.255 area 0
R-TUNJA01(config-router)#end
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Enrutamiento OSPF para el Router instalado en la sede de Cundinamarca.

```
R-CUNDINAMARCA01#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

       172.31.0.0/16 is variably subnetted, 10 subnets, 4 masks
C           172.31.1.0/26 is directly connected, GigabitEthernet0/0.30
L           172.31.1.2/32 is directly connected, GigabitEthernet0/0.30
C           172.31.1.64/26 is directly connected, GigabitEthernet0/0.20
L           172.31.1.66/32 is directly connected, GigabitEthernet0/0.20
C           172.31.2.16/29 is directly connected, GigabitEthernet0/0.1
L           172.31.2.18/32 is directly connected, GigabitEthernet0/0.1
C           172.31.2.24/29 is directly connected, GigabitEthernet0/0.88
L           172.31.2.26/32 is directly connected, GigabitEthernet0/0.88
C           172.31.2.36/30 is directly connected, Serial0/0/0
```

L 172.31.2.38/32 is directly connected, Serial0/0/0

R-CUNDINAMARCA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CUNDINAMARCA01(config)#router ospf 1
R-CUNDINAMARCA01(config-router)#router-id 3.3.3.3
R-CUNDINAMARCA01(config-router)#network 172.31.1.0 0.0.0.63 area 0
R-CUNDINAMARCA01(config-router)#network 172.31.1.64 0.0.0.63 area 0
R-CUNDINAMARCA01(config-router)#network 172.31.2.16 0.0.0.7 area 0
R-CUNDINAMARCA01(config-router)#network 172.31.2.24 0.0.0.7 area 0
R-CUNDINAMARCA01(config-router)#network 172.31.2.36 0.0.0.3 area 0
R-CUNDINAMARCA01(config-router)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Autenticación OSPF para el Router instalado en la sede de Bucaramanga.

R-BUCARAMANGA01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-BUCARAMANGA01(config)#interface S0/0/0
R-BUCARAMANGA01(config-if)#ip ospf message-digest-key 9 md5 RB-RT
R-BUCARAMANGA01(config-if)#ip ospf authentication message-digest
R-BUCARAMANGA01(config-if)#end

Para validar que se encuentre activa la autenticación ejecutamos el siguiente comando. Y podemos observar que efectivamente se encuentra activa (en color amarillo se resalta la activación de la autenticación OSPF)

R-BUCARAMANGA01#show ip ospf interface S0/0/0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.2.34/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:00
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 9

```
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Autenticación OSPF para el Router instalado en la sede de Tunja.

Como ya se configuro autentificación por OSPF el Router de Tunja solo va a detectar las redes que estén conectadas físicamente a él. A continuación, podemos observar que solo detecta la red de Cundinamarca porque en la interface que los interconecta no se ha configurado la autenticación OSPF

```
R-TUNJA01#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:31	172.31.2.38	Serial0/0/1

```
R-TUNJA01#
```

Procedemos a cifrar la interfaz S0/0/0 en el Router de Tunja

```
R-TUNJA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-TUNJA01(config)#interface S0/0/0
R-TUNJA01(config-if)#ip ospf message-digest-key 9 md5 RB-RT
R-TUNJA01(config-if)#ip ospf authentication message-digest
R-TUNJA01(config-if)#
00:22:32: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from
LOADING to FULL, Loading Done

R-TUNJA01(config-if)#end
```

Validamos que se activa la autenticación OSPF.

```
R-TUNJA01#show ip ospf interface S0/0/0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.2.33/30, Area 0
    Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
    Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
    Index 6/6, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
    Suppress hello for 0 neighbor(s)
    Message digest authentication enabled
    Youngest key id is 9
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Continuamos con la autenticación OSPF para la interface S0/0/1 del Router instalado en la sede de Tunja

```
R-TUNJA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-TUNJA01(config)#interface S0/0/1
R-TUNJA01(config-if)#ip ospf message-digest-key 9 md5 RC-RT
R-TUNJA01(config-if)#ip ospf authentication message-digest
R-TUNJA01(config-if)#end
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

R-TUNJA01#

Validamos que se encuentre activa la autenticación OSPF para la interface

R-TUNJA01#show ip ospf interface S0/0/1

Serial0/0/1 is up, line protocol is up
Internet address is 172.31.2.37/30, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 5/5, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 9
R-TUNJA01#

Autenticación OSPF para el Router instalado en la sede de Cundinamarca.

El Router de la sede de Tunja no va a detectar ningún Router vecino debido a que el Router de la Sede de Tunja ya tiene activa la autenticación OSPF en todas sus interfaces seriales. Para podernos conectar nuevamente a la red debemos activar la autenticación OSPF en el Router de la sede de Cundinamarca.

R-CUNDINAMARCA01#show ip ospf neighbor

R-CUNDINAMARCA01#

Configuración autenticación OSPF en la interface S0/0/0 del Router sede Cundinamarca.

R-CUNDINAMARCA01(config-if)#ip ospf message-digest-key 9 md5 RC-RT
R-CUNDINAMARCA01(config-if)#ip ospf authentication message-digest

```
R-CUNDINAMARCA01(config-if)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-CUNDINAMARCA01#
```

Validamos que se encuentre activa la autenticación OSPF y efectivamente se encuentra activa.

```
R-CUNDINAMARCA01#show ip ospf interface S0/0/0

    Serial0/0/0 is up, line protocol is up
    Internet address is 172.31.2.38/30, Area 0
    Process ID 1, Router ID 3.3.3.3, Network Type POINT-TO-POINT, Cost: 64
    Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
    Index 5/5, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
    Suppress hello for 0 neighbor(s)
    Message digest authentication enabled
    Youngest key id is 9
R-CUNDINAMARCA01#
```

Indagamos nuevamente Router vecinos y encontramos que ya detecta el Router de la sede de Tunja por la interface S0/0/0

```
R- CUNDINAMARCA01#show ip ospf neighbor
  Neighbor ID     Pri   State           Dead Time   Address         Interface
    1.1.1.1         0   FULL/ -         00:00:36    172.31.2.37     Serial0/0/0
R-CUNDINAMARCA01#
```

4.3. CONFIGURACIÓN DHCP

Configuramos como servidor DHCP el Router ubicado en la sede de Tunja. Este Router nos proporcionara direccionamiento IP por DHCP para las sedes de Cundinamarca y Bucaramanga.

Configuración interface S0/0/1 para el Router-TUNJA01, esta interface pertenece al enlace WAN entre la sede Tunja y la sede de Cundinamarca.

```
R-TUNJA01(config)#ip dhcp pool RedInterfaceS0/0/1
R-TUNJA01(dhcp-config)#network 172.31.2.36 255.255.255.252
R-TUNJA01(dhcp-config)#default-router 172.31.2.37
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.2.37 172.31.2.38
R-TUNJA01(config)#
```

Configuración interface S0/0/0 para el Router-TUNJA01, esta interface pertenece al enlace WAN entre la sede Tunja y la sede de Bucaramanga.

```
R-TUNJA01(config)#ip dhcp pool RedInterfaceS0/0/0
R-TUNJA01(dhcp-config)#network 172.31.2.32 255.255.255.252
R-TUNJA01(dhcp-config)#default-router 172.31.2.33
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.2.33 172.31.2.35
R-TUNJA01(config)#exit
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Publicamos las redes que recibirán direccionamiento IP por DHCP del Router ubicado en la sede de Tunja mediante ip helper-address.

Redes conectadas al Router de la sede de Bucaramanga para recibir direccionamiento IP mediante ip helper-address del R-TUNJA01.

```
R-TUNJA01(config)#ip dhcp pool RedBucaramangaVlan1
R-TUNJA01(dhcp-config)#network 172.31.2.0 255.255.255.248
R-TUNJA01(dhcp-config)#default-router 172.31.2.1
R-TUNJA01(dhcp-config)#ip dhcp excluded-address 172.31.2.1 172.31.2.3
```

```
R-TUNJA01(config)#exit

R-TUNJA01(config)#ip dhcp pool RedBucaramangaVlan10
R-TUNJA01(dhcp-config)#network 172.31.0.0 255.255.255.192
R-TUNJA01(dhcp-config)#default-router 172.31.0.1
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.3
R-TUNJA01(config)#ip dhcp pool RedBucaramangaVlan30
R-TUNJA01(dhcp-config)#network 172.31.0.64 255.255.255.192
R-TUNJA01(dhcp-config)#default-router 172.31.0.65
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.67
```

Redes conectadas al Router de la sede de Cundinamarca para recibir direccionamiento IP mediante ip helper-address del R_TUNJA01.

```
R-TUNJA01(config)#ip dhcp pool RedCundinamarcaVlan1
R-TUNJA01(dhcp-config)#network 172.31.2.16 255.255.255.248
R-TUNJA01(dhcp-config)#default-router 172.31.2.17
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.2.17 172.31.2.19

R-TUNJA01(config)#ip dhcp pool RedCundinamarcaVlan20
R-TUNJA01(dhcp-config)#network 172.31.1.64 255.255.255.192
R-TUNJA01(dhcp-config)#default-router 172.31.1.65
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.67

R-TUNJA01(config)#ip dhcp pool RedCundinamarcaVlan30
R-TUNJA01(dhcp-config)#network 172.31.1.0 255.255.255.192
R-TUNJA01(dhcp-config)#default-router 172.31.1.1
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.3

R-TUNJA01(config)#ip dhcp pool RedCundinamarcaVlan88
R-TUNJA01(dhcp-config)#network 172.31.2.24 255.255.255.248
R-TUNJA01(dhcp-config)#default-router 172.31.2.25
R-TUNJA01(dhcp-config)#exit
R-TUNJA01(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.27
```

```
R-TUNJA01#copy running-config st
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración del ip helper-address en el Router de la sede Cundinamarca.

```
R-CUNDINAMARCA01# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CUNDINAMARCA01(config)#interface S0/0/0
R-CUNDINAMARCA01(config-if)#ip helper-address 172.31.2.37
R-CUNDINAMARCA01(config-if)#exit
R-CUNDINAMARCA01(config)#interface G0/0.1
R-CUNDINAMARCA01(config-subif)#ip helper-address 172.31.2.37
R-CUNDINAMARCA01(config-subif)#exit
R-CUNDINAMARCA01(config)#interface G0/0.20
R-CUNDINAMARCA01(config-subif)#ip helper-address 172.31.2.37
R-CUNDINAMARCA01(config-subif)#exit
R-CUNDINAMARCA01(config)#interface G0/0.30
R-CUNDINAMARCA01(config-subif)#ip helper-address 172.31.2.37
R-CUNDINAMARCA01(config-subif)#exit
R-CUNDINAMARCA01(config)#interface G0/0.88
R-CUNDINAMARCA01(config-subif)#ip helper-address 172.31.2.37
R-CUNDINAMARCA01(config-subif)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración del ip helper-address en el Router de la sede Bucaramanga.

```
R-BUCARAMANGA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-BUCARAMANGA01(config)#interface S0/0/0
R-BUCARAMANGA01(config-if)#ip helper-address 172.31.2.33
R-BUCARAMANGA01(config-if)#exit
R-BUCARAMANGA01(config)#interface G0/0.1
R-BUCARAMANGA01(config-subif)#ip helper-address 172.31.2.33
```

```
R-BUCARAMANGA01(config-subif)#exit
R-BUCARAMANGA01(config)#interface G0/0.10
R-BUCARAMANGA01(config-subif)#ip helper-address 172.31.2.33
R-BUCARAMANGA01(config-subif)#exit
R-BUCARAMANGA01(config)#interface G0/0.30
R-BUCARAMANGA01(config-subif)#ip helper-address 172.31.2.33
R-BUCARAMANGA01(config-subif)#exit
```

Debido a las diferentes ACL que se han implementado en la red, se hace necesario crear una ACL que permita el DHCP mediante helper-address en la sede de Bucaramanga.

```
R-BUCARAMANGA01(config)#access-list 102 permit ip 172.31.0.0 0.0.0.63 172.31.2.32 0.0.0.3
R-BUCARAMANGA01(config)#access-list 102 permit ip 172.31.0.64 0.0.0.63 172.31.2.32 0.0.0.3
R-BUCARAMANGA01(config-subif)#access-list 102 permit ip 172.31.2.0 0.0.0.7 172.31.2.32 0.0.0.3

R-BUCARAMANGA01(config)#interface g0/0.1
R-BUCARAMANGA01(config-subif)#ip access-group 102 out
R-BUCARAMANGA01(config-subif)#exit
R-BUCARAMANGA01(config)#interface g0/0.10
R-BUCARAMANGA01(config-subif)#ip access-group 102 out
R-BUCARAMANGA01(config-subif)#exit
R-BUCARAMANGA01(config-subif)#interface g0/0.30
R-BUCARAMANGA01(config-subif)#ip access-group 102 out
R-BUCARAMANGA01(config-subif)#end
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

4.4. CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO

Se van a implementar una serie de ACL en los diferentes Router para aumentar la seguridad de la red y restringir los accesos a la misma.

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

```
R-CUNDINAMARCA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CUNDINAMARCA01(config)#access-list 100 deny tcp 172.31.1.64 0.0.0.63
209.17.220.0 0.0.0.255 eq 80
R-CUNDINAMARCA01(config)#access-list 100 deny tcp 172.31.1.64 0.0.0.63
209.17.220.0 0.0.0.255 eq 443
R-CUNDINAMARCA01(config)#access-list 100 permit ip 172.31.1.64 0.0.0.63
172.31.2.8 0.0.0.7
R-CUNDINAMARCA01(config)#access-list 100 permit ip 172.31.1.64 0.0.0.63
172.31.0.128 0.0.0.63
R-CUNDINAMARCA01(config)#access-list 100 permit ip 172.31.1.64 0.0.0.63
172.31.0.192 0.0.0.63
R-CUNDINAMARCA01(config)#interface S0/0/0
R-CUNDINAMARCA01(config-subif)#ip access-group 100 out
R-CUNDINAMARCA01(config-if)#exit
R-CUNDINAMARCA01(config)#access-list 101 deny tcp 172.31.1.64 0.0.0.63
172.31.2.24 0.0.0.7 eq 80
R-CUNDINAMARCA01(config)#access-list 101 deny tcp 172.31.1.64 0.0.0.63
172.31.2.24 0.0.0.7 eq 443
R-CUNDINAMARCA01(config)#access-list 101 permit ip any any
R-CUNDINAMARCA01(config)#interface G0/0.20
R-CUNDINAMARCA01(config-subif)#ip access-group 101 out
R-CUNDINAMARCA01(config-subif)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-CUNDINAMARCA01#
```

Validamos la creación y funcionamiento de la ACL creada

```
R-CUNDINAMARCA01#show access-list
Extended IP access list sl_def_acl
        0 deny tcp any any eq telnet
        0 deny tcp any any eq www
        0 deny tcp any any eq 22
```

0 permit tcp any any eq 22
Extended IP access list 100
10 deny tcp 172.31.1.64 0.0.0.63 209.17.220.0 0.0.0.255 eq www (12 match(es))
20 deny tcp 172.31.1.64 0.0.0.63 209.17.220.0 0.0.0.255 eq 443
30 permit ip 172.31.1.64 0.0.0.63 172.31.2.8 0.0.0.7 (16 match(es))
40 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63 (4 match(es))
50 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63 (4 match(es))
Extended IP access list 101
10 deny tcp 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7 eq www
20 deny tcp 172.31.1.64 0.0.0.63 172.31.2.24 0.0.0.7 eq 443
30 permit ip any any
R-CUNDINAMARCA01#

- ✓ Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

R-CUNDINAMARCA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-CUNDINAMARCA01(config)#access-list 102 permit tcp 172.31.1.0 0.0.0.63 172.31.2.24 0.0.0.7 eq 80
R-CUNDINAMARCA01(config)#access-list 102 permit tcp 172.31.1.0 0.0.0.63 172.31.2.24 0.0.0.7 eq 443
R-CUNDINAMARCA01(config)#access-list 102 permit ip any any
R-CUNDINAMARCA01(config)#interface G0/0.30
R-CUNDINAMARCA01(config-subif)#ip access-group 102 out

R-CUNDINAMARCA01(config)#access-list 103 permit tcp 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255 eq 80
R-CUNDINAMARCA01(config)#access-list 103 permit tcp 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255 eq 443
R-CUNDINAMARCA01(config-subif)#access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.2.8 0.0.0.7
R-CUNDINAMARCA01(config)#access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
R-CUNDINAMARCA01(config)#access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
R-CUNDINAMARCA01(config)#access-list 103 permit ip any any
R-CUNDINAMARCA01(config)#interface S0/0/0

R-CUNDINAMARCA01(config-if)#ip access-group 103 out
R-CUNDINAMARCA01(config-if)#end
R-CUNDINAMARCA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R-CUNDINAMARCA01#

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

R-TUNJA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255 eq ftp
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255 eq 80
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255 eq 443
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 172.31.2.24 0.0.0.7 eq ftp
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 172.31.2.24 0.0.0.7 eq 80
R-TUNJA01(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 172.31.2.24 0.0.0.7 eq 443
R-TUNJA01(config)#interface G0/1.30
R-TUNJA01(config-subif)#ip access-group 100 in
R-TUNJA01(config-subif)#end
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

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

R-TUNJA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-TUNJA01(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63

```
R-TUNJA01(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63
R-TUNJA01(config)#interface G0/1.20
R-TUNJA01(config-subif)#ip access-group 101 in
R-TUNJA01(config-subif)#end
R-TUNJA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

```
R-BUCARAMANGA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-BUCARAMANGA01(config)#access-list 100 permit tcp 172.31.0.64 0.0.0.63
209.17.220.0 0.0.0.255 eq 80
R-BUCARAMANGA01(config)#access-list 100 permit tcp 172.31.0.64 0.0.0.63
209.17.220.0 0.0.0.255 eq 443
R-BUCARAMANGA01(config)#access-list 100 permit tcp 172.31.0.64 0.0.0.63
172.31.2.24 0.0.0.7 eq 80
R-BUCARAMANGA01(config)#access-list 100 permit tcp 172.31.0.64 0.0.0.63
172.31.2.24 0.0.0.7 eq 443
R-BUCARAMANGA01(config)#access-list 100 permit ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
R-BUCARAMANGA01(config)#interface G0/0.30
R-BUCARAMANGA01(config-subif)#ip access-group 100 in
R-BUCARAMANGA01(config-subif)#end
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

```
R-BUCARAMANGA01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R-BUCARAMANGA01(config)#access-list 101 deny tcp 172.31.0.0 0.0.0.63
209.17.220.4 0.0.0.255 eq 80
R-BUCARAMANGA01(config)#access-list 101 deny tcp 172.31.0.0 0.0.0.63
209.17.220.4 0.0.0.255 eq 443
R-BUCARAMANGA01(config)#access-list 101 deny tcp 172.31.0.0 0.0.0.63
172.31.2.24 0.0.0.7 eq 80
R-BUCARAMANGA01(config)#access-list 101 deny tcp 172.31.0.0 0.0.0.63
172.31.2.24 0.0.0.7 eq 443
R-BUCARAMANGA01(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
R-BUCARAMANGA01(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
R-BUCARAMANGA01(config)#interface G0/0.10
R-BUCARAMANGA01(config-subif)#ip access-group 101 in
R-BUCARAMANGA01(config-subif)#end
R-BUCARAMANGA01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

CONCLUSIONES

Durante el desarrollo del presente trabajo pude comprender la funcionalidad de las ACL, para permitir o denegar tráfico entrante o saliente de una red o de una interface especifica.

La implementación de ACLs en una red son una buena estrategia de seguridad para proteger la red de datos de conexiones no autorizadas. Puesto que estas solo permiten acceso a la red a las direcciones MAC que se encuentren configuradas en la lista ACL creada; Una desventaja de usar estas ACL es que si se cuenta con un Scope de direcciones IP reducido las conexiones a la red de equipos no autorizados estarían copando las pocas direcciones IP disponibles del segmento de red. Estos equipos reciben direccionamiento IP, pero no tienen servicios de red.

Cuando una red cuenta con un Router y Switch capa 2, es recomendable hacer el Routing de capa 3 con el Router, puesto que este conoce las diferentes redes creadas en la misma y permite su salida a Internet o hacia otra red ubicada en otro espacio geográfico. Los Switch Cisco 2960 también permiten hacer Routing de capa 3, pero para esto se requiere hacer configuración de rutas estáticas y se tornaría algo engorrosa la configuración del enrutamiento al interior de la red.

Una gran estrategia para una empresa al momento de implementar o renovar su infraestructura de red seria usar como servidores DHCP los Router presentes en la infraestructura de red a implementar o actual; de esta manera se evitaría la compra de un servidor adicional u otro equipo para administrar el DHCP logrando reducir gastos y tiempos de implementación.

El protocolo de enrutamiento que se escoja para una red de datos garantizara la disponibilidad, seguridad, desempeño y eficiencia de esta, por eso se debe escoger muy bien el protocolo a implementar, a modo personal el protocolo de enrutamiento OSPF con autenticación me parece muy seguro y eficiente.

En una red de datos a nivel corporativo siempre se cuenta con un canal de comunicaciones Principal y un canal de Backup en caso de que el Principal falle; normalmente el canal de Backup es de un menor BW que el canal Principal. A modo personal recomendaría una configuración de canal Activo – Activo, que significa que ambos canales se encuentran operativos y no se necesita de un fallo en el canal de Principal para que el canal de Backup se active como sucede con la configuración

Activo - Pasivo. Adicionalmente recomiendo separa el tráfico de datos entre los dos canales de datos, lo que reduce ampliamente la saturación del canal Principal obviamente configurando un HSRP que migre los servicios del canal Principal al canal de Backup una vez este falle y viceversa para poder garantizar la operatividad de los diferentes servicios de red (Acceso a recursos compartidos, WIFI, Mensajería instantánea y no síncrona, Multimedia, etc.)

BIBLIOGRAFIA

LAMMLE, Todd. CCNA Cisco Certified Network Associate Deluxe Study Guide. John Wiley & Sons, 2011.

ARIGANELLO, Ernesto. REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada. Grupo Editorial RA-MA, 2016.

ODOM, Wendell. Ccent/ccna icnd1 official exam certification guide (ccent exam 640-822 and ccna exam 640-802). Cisco Press, 2007.

ODOM, Wendell. CCNA Routing and Switching ICND2 200-105 Official Cert Guide. Cisco Press, 2016.

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN51/es/index.html#5.0.1.1

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN51/es/index.html#6.0.1.1

UNAD (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9