DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRUEBA HABILIDADES PRACTICAS

PRESENTADO A
EFRAIN ALEJANDRO PEREZ

PRESENTADO POR
Ricardo Rodríguez Suárez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CEAD JOSE ACEVEDO Y GOMEZ

DICIEMBRE de 2019

Tabla de contenido

TABLA CONTENIDO IMAGENES

RESUMEN

Para la opción de grado, la UNAD a dispuesto como una de las opciones de grado, el Diplomado en profundización CISCO en Diseño e implementación de redes integradas LAN y WAN.

Mediante el cual se ven los diferentes conceptos, desde lo básico en redes LAN, hasta conceptos avanzados de enrutamiento aplicando políticas de seguridad, todo lo aprendido durante este diplomado, deberá aplicarse en este trabajo de habilidades prácticas.

Para ello se plantean dos escenarios para el diseño e implementación de redes LAN y WAN, en el primer escenario deberemos asegurar el acceso a los equipos como switches y routers, aplicando conceptos de subredes y separando las mismas, aplicando listas de control de acceso para implementar las políticas y configuración indicadas en el escenario 1, todo esto usando direccionamiento IP estático.

Para el escenario 2, tendremos que diseñar e implementar políticas de seguridad de acceso a los equipos activos de red como switches y routers, así como segmentación de redes LAN usando para ellos IPV4, se usan VLAN para el control de tráfico entre las diferentes redes, así como el uso de navegación hacia Internet por medio de NAT, se utilizara para las direcciones IP DHCP, este último configurado en el router de Tunja y asignando dirección IP de manera automática a las redes de Cundinamarca y Bucaramanga, finalmente se implementaran ACL para el control de tráfico y seguridad de acuerdo a las especificaciones del escenario 2.

GLOSARIO

LAN: se conoce como red LAN (siglas del inglés: Local Área Network, que traduce Red de Área Local) a una red informática cuyo alcance se limita a un espacio físico reducido, como una casa, un departamento o a lo sumo un edificio.

WAN: es la sigla de Wide Area Network, una expresión en lengua inglesa que puede traducirse como Red de Área Amplia. Esto quiere decir que la red WAN es un tipo de red que cubre distancias de entre unos 100 y unos 1.000 kilómetros, lo que le permite brindar conectividad a varias ciudades o incluso a un país entero.

IP: Un protocolo es un conjunto de normas que rigen el funcionamiento de las cosas en una determinada tecnología, por lo que de esta forma se consigue que exista algún tipo de estandarización. Cuando hablamos de comunicaciones de red, un protocolo es el conjunto de normas que rigen cómo los paquetes de comunicación se transmiten a través de la red. Cuando tienes un protocolo, puedes estar seguro de que todas las máquinas de una red (o del mundo, cuando se trata de Internet), por muy diferentes que sean, hablan el mismo idioma y pueden integrarse en cualquier sistema.

ACL: es la sigla en inglés de Access Control List, (lista de control de acceso), es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física

DHCP: El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo.

ABSTRACT

After seeing throughout the semester, the concepts of LAN and WAN telecommunications networks, developing at each stage the workshops designed on the CISCO platform, where various topics were configured and resolved, from a basic configuration of PC, Server, Switch, Router, etc., through more advanced configurations such as applying access security to the aforementioned devices until finally reaching the interconnection of LAN and WAN networks.

We learned the importance of designing a network, in which IP addressing using is very important, especially for administration issues of the implemented networks. The segmentation of the network using specific techniques, such as network sounding, as well as the use of routing protocols, use of VLANs between networks, creation of access security between networks using for them Access Control Lists (ACL), we They have given the tools as future engineers, in order to put this knowledge into practice, in the final development of this skill practice.

We can from a completely feasible and real scenarios, design practically from scratch, with little information some networks and solve the problems raised, applying all the concepts and skills acquired throughout this diploma, to finally deliver the scenarios indicated in this work, totally solved.

INTRODUCCION

Luego de ver durante todo el semestre, los conceptos de redes de telecomunicaciones LAN y WAN, desarrollando en cada etapa los talleres diseñados en la plataforma CISCO, donde se configuraron y resolvieron temas diversos, desde una configuración básica de equipos PC, |Servidor, Switch, Router, etc, pasando por configuraciones más avanzadas como aplicar seguridad de acceso a los dispositivos antes mencionados hasta llegar finalmente a la interconexión de redes LAN y WAN.

Aprendimos la importancia del diseño de una red, en el cual el direccionamiento IP usando es muy importante, sobre todo para temas de administración de las redes implementadas. La segmentación de la red usando técnicas específicas, como el soneteo de red, así como el uso de protocolos de enrutamientos, uso de VLAN entre redes, creación de seguridad de acceso entre redes utilizando para ellos Listas de control de Acceso (ACL), nos han dado las herramientas como futuros ingenieros, para poder colocar en práctica estos conocimientos, en el desarrollo final de esta práctica de habilidades.

Podremos desde unos escenarios totalmente factibles y reales, diseñar prácticamente de cero, con poca información algunas redes y resolver los problemas planteados, aplicando todos los conceptos y habilidades adquiridas a lo largo de este diplomado, para finalmente entregar resulto los escenarios indicados en el presente trabajo, totalmente solucionados.

.

OBJETIVOS

OBJETIVO GENERAL

- Poner en en práctica los conocimientos adquiridos, en los ejercicios del Diplomado de redes CISCO, con el desarrollo de este trabajo de habilidades prácticas.

OBJETIVOS ESPECIFICOS

- Poner en práctica los conceptos adquiridos durante el semestre en la plataforma CISCO NETCAT.
- Usar packet tracert o GNS3 para el desarrollo de las actividades propuestas.
- Configurar los diferentes escenarios propuestos.
- Realizar pruebas de los escenarios ya configurados.
- Documentar las pruebas de los escenarios desarrollados.
- Solucionar los diferentes problemas que se presenten durante las configuraciones indicadas en cada escenario propuesto.
- Tomar las evidencias necesarias para el desarrollo e implementación de cada escenario propuesto.

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

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

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

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

Parte 6: Configuración final.

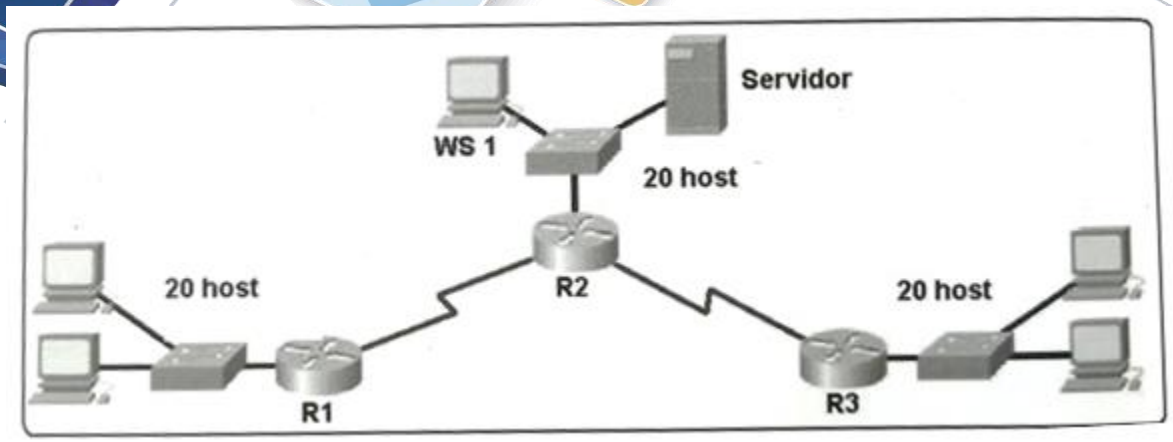

IMAGEN 1 ECENERIO 1

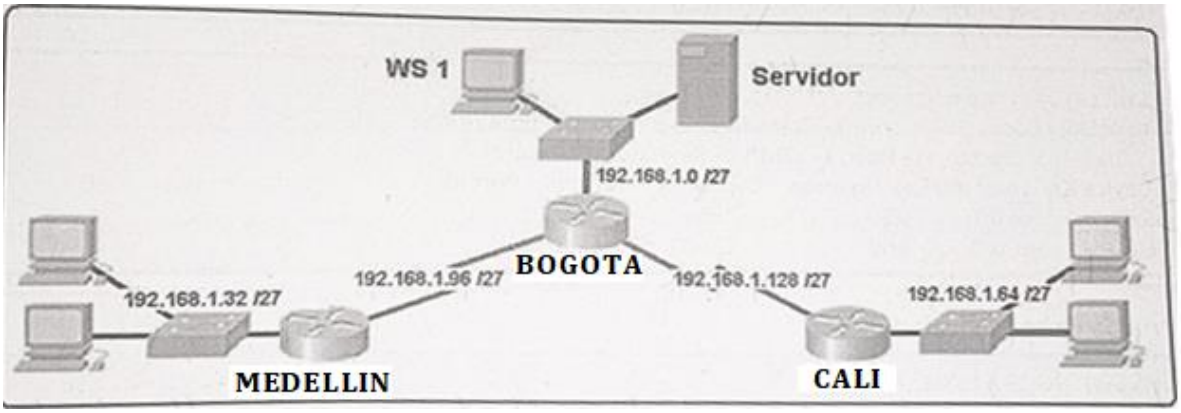

IMAGEN 2 ESCENARIO 1.1

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

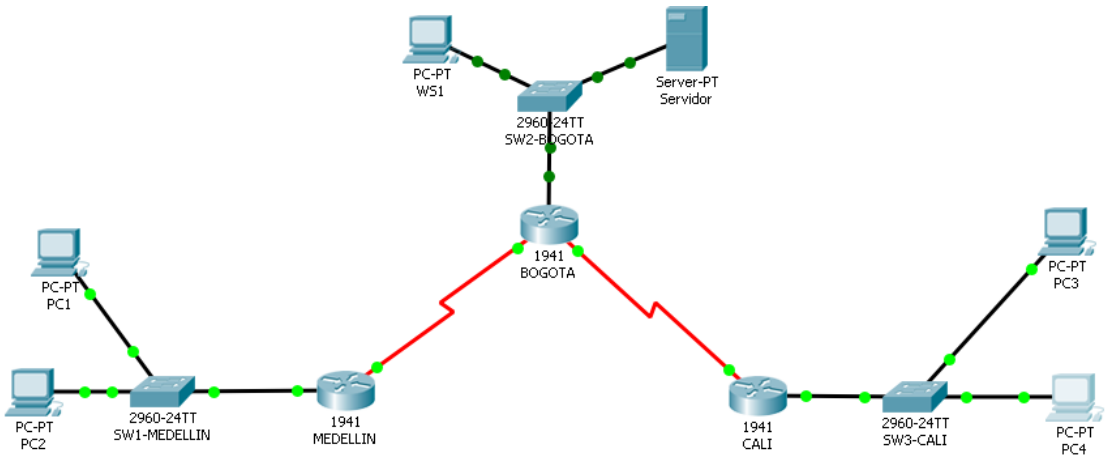

IMAGEN 3 ESCENARIO 1 DISEÑO FÍSICO RED

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

Parte 1: Asignación de direcciones IP:

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

Se realiza el subneteo de la rede de acuerdo a la información facilitada, dividiendo la red en 8 subredes, se adjunta la tabla de direccionamiento IP utilizado para el primer escenario.

SUBDIVISION RED

RED 192.168.1.0/27 : 8 SUBREDES		
1.	RED	192.168.1.0/27
	IP	192.168.1.1 - 192.168.1.30
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.31
	Hosts	30
2.	RED	192.168.1.32/27
	IP	192.168.1.33 - 192.168.1.62
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.63
	Hosts	30
3.	RED	192.168.1.64/27
	IP	192.168.1.65 - 192.168.1.94
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.95
	Hosts	30
4.	RED	192.168.1.96/27
	IP	192.168.1.97 - 192.168.1.126
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.127
	Hosts	30
5.	RED	192.168.1.128/27
	IP	192.168.1.129 - 192.168.1.158

	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.159
	Hosts	30
6.	RED	192.168.1.160/27
	IP	192.168.1.161 - 192.168.1.190
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.191
	Hosts	30
7.	RED	192.168.1.192/27
	IP	192.168.1.193 - 192.168.1.222
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.223
	Hosts	30
8.	RED	192.168.1.224/27
	IP	192.168.1.225 - 192.168.1.254
	Mascara Red	255.255.255.224
	Broadcast:	192.168.1.255
	Hosts	30

a. Asignar una dirección IP a la red.

LA IP DE LA RED es **192.168.1.0/27**

Parte 2: Configuración Básica.

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

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

Se realiza la configuración básica de los equipos activos de red, como rputer y Switches, controlando el acceso a los dispositivos con clave y encriptando esas claves, se adjunta las pantallas de configuración por cada dispositivo:

ROUTER MEDELLIN

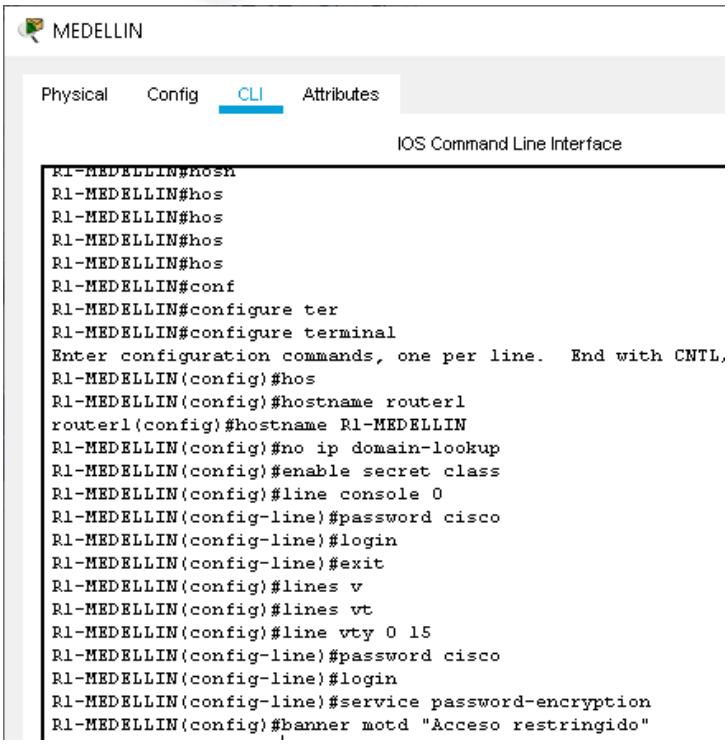

IMAGEN 4 CONFIGURACIÓN ROUTER MEDELLÍN

router1(config)#hostname R1-MEDELLIN
R1-MEDELLIN(config)#no ip domain-lookup
R1-MEDELLIN(config)#enable secret class
R1-MEDELLIN(config)#line console 0
R1-MEDELLIN(config-line)#password cisco
R1-MEDELLIN(config-line)#login
R1-MEDELLIN(config-line)#exit
R1-MEDELLIN(config)#lines v
R1-MEDELLIN(config)#lines vt
R1-MEDELLIN(config)#line vty 0 15
R1-MEDELLIN(config-line)#password cisco
R1-MEDELLIN(config-line)#login
R1-MEDELLIN(config-line)#service password-encryption
R1-MEDELLIN(config)#banner motd "Acceso restringido"
R1-MEDELLIN(config)#

ROUTER MEDELLIN CONFIGURACION DIRECCIONAMIENTO IP

R1-MEDELLIN(config-if)#interface serial 0/0/0
R1-MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
R1-MEDELLIN(config-if)#no shutdown

R1-MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

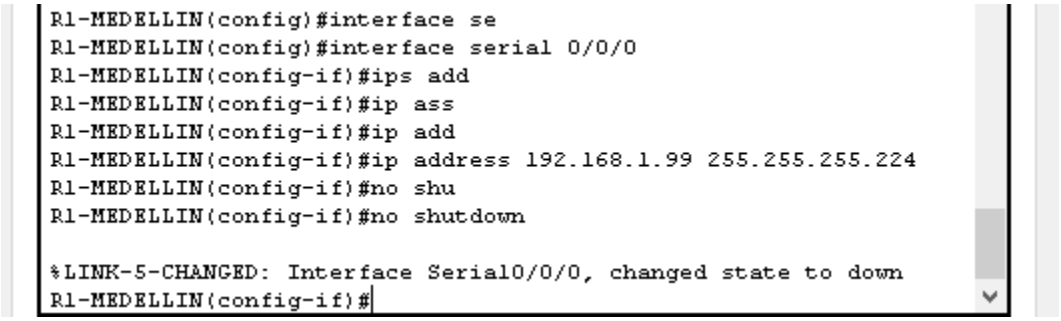

IMAGEN 5 CONFIGURACIÓN DIRECCIONAMIENTO IP ROUTER MEDELLÍN

R1-MEDELLIN(config-if)#interface gigabitEthernet 0/0
R1-MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
R1-MEDELLIN(config-if)#no shutdown

R1-MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

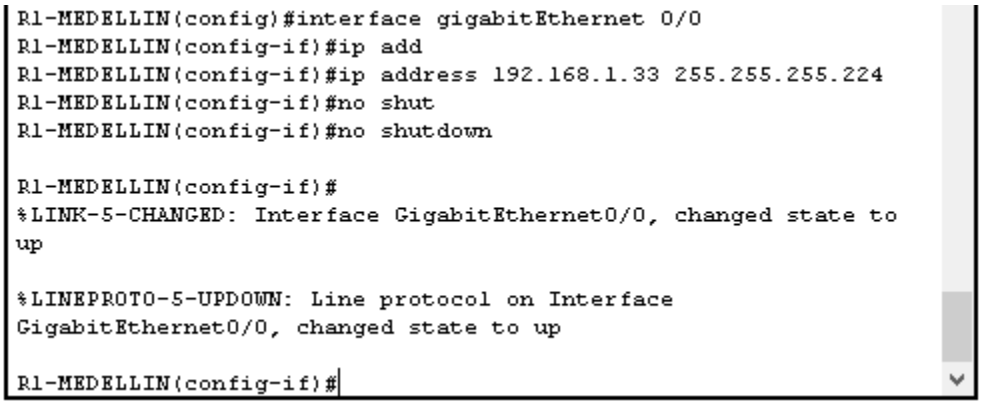

IMAGEN 6 CONFIGURACIÓN IP ROUTER MEDELLÍN

```
router2(config)#hostname R2-BOGOTA
R2-BOGOTA(config)#no ip domain-lookup
R2-BOGOTA(config)#enable secret class
R2-BOGOTA(config)#line console 0
R2-BOGOTA(config-line)#password cisco
R2-BOGOTA(config-line)#login
R2-BOGOTA(config-line)#exit
R2-BOGOTA(config)#line vty 0 15
R2-BOGOTA(config-line)#password cisco
R2-BOGOTA(config-line)#login
R2-BOGOTA(config-line)#service password-encryption
R2-BOGOTA(config)#banner motd "Acceso restringido"
R2-BOGOTA(config)#
```

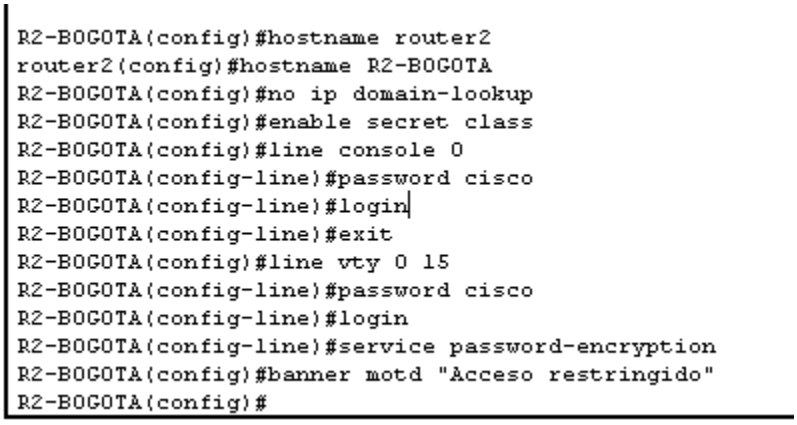

IMAGEN 7 CONFIGURACIÓN SEGURIDAD ACCESO ROUTER BOGOTA

R2-BOGOTA(config-if)#interface serial 0/0/0
R2-BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
R2-BOGOTA(config-if)#no shutdown

R2-BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2-BOGOTA(config-if)#interface serial 0/0/1
R2-BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
R2-BOGOTA(config-if)#no shutdown
R2-BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

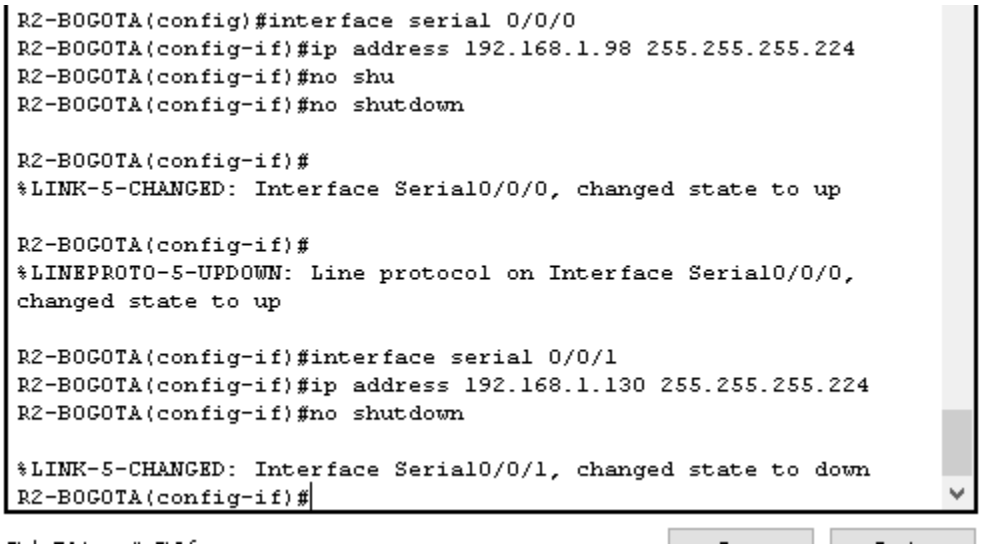

IMAGEN 8 CONFIGURACIÓN DIRECCIONAMIENTO IP RPUTER BOGOTÁ

R2-BOGOTA(config-if)#interface gigabitEthernet 0/0
R2-BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
R2-BOGOTA(config-if)#no shutdown
R2-BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

```
R2-BOGOTA(config)#interface gigabitEthernet 0/0
R2-BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
R2-BOGOTA(config-if)#no sh
R2-BOGOTA(config-if)#no shutdown

R2-BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R2-BOGOTA(config-if)#
```

IMAGEN 9 CONFIGURACIÓN IP RPUTER BOGOTÁ

ROUTER CALI

router3(config)#hostname R3-CALI
R3-CALI(config)#no ip domain-lookup
R3-CALI(config)#enable secret class
R3-CALI(config)#line console 0
R3-CALI(config-line)#password cisco
R3-CALI(config-line)#login
R3-CALI(config-line)#exit
R3-CALI(config)#line vty 0 15
R3-CALI(config-line)#password cisco
R3-CALI(config-line)#login
R3-CALI(config-line)#service password-encryption
R3-CALI(config)#banner motd "Acceso restringido"
R3-CALI(config)#

```
R3-CALI(config)#hostname router3
router3(config)#hostname R3-CALI
R3-CALI(config)#no ip domain-lookup
R3-CALI(config)#enable secret class
R3-CALI(config)#line console 0
R3-CALI(config-line)#password cisco
R3-CALI(config-line)#login
R3-CALI(config-line)#exit
R3-CALI(config)#line vty 0 15
R3-CALI(config-line)#password cisco
R3-CALI(config-line)#login
R3-CALI(config-line)#service password-encryption
R3-CALI(config)#banner motd "Acceso restringido"
R3-CALI(config)#
```

IMAGEN 10 CONFIGURACIÓN SEGURIDAD ACCESO ROUTER CALÍ

ROUTER CALI CONFIGURACION DIRECCIONAMIENTO IP

```
R3-CALI(config-if)#interface serial 0/0/0
R3-CALI(config-if)#ip add
R3-CALI(config-if)#ip address 192.168.1.131 255.255.255.224
R3-CALI(config-if)#no sh
R3-CALI(config-if)#no shutdown

R3-CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

```
R3-CALI(config-if)#interface serial 0/0/0
R3-CALI(config-if)#ip add
R3-CALI(config-if)#ip address 192.168.1.131 255.255.255.224
R3-CALI(config-if)#no sh
R3-CALI(config-if)#no shutdown

R3-CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

IMAGEN 11 CONFIGURACIÓN DIRECCIONAMIENTO IP ROUTER CALI

```
R3-CALI(config-if)#interface gigabitEthernet 0/0
R3-CALI(config-if)#ip address 192.168.1.65 255.255.255.224
R3-CALI(config-if)#no sh
R3-CALI(config-if)#no shutdown

R3-CALI(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
R3-CALI(config-if)#interface gigabitEthernet 0/0
R3-CALI(config-if)#ip address 192.168.1.65 255.255.255.224
R3-CALI(config-if)#no sh
R3-CALI(config-if)#no shutdown

R3-CALI(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

IMAGEN 12 CONFIGURACIÓN IP ROUTER CALI

SWITCH MEDELLIN

switch1(config)#hostname SW1-MEDELLLIN
SW1-MEDELLLIN(config)#no ip domain-lookup
SW1-MEDELLLIN(config)#enable secret class
SW1-MEDELLLIN(config)#line console 0
SW1-MEDELLLIN(config-line)#password cisco
SW1-MEDELLLIN(config-line)#login
SW1-MEDELLLIN(config-line)#exit
SW1-MEDELLLIN(config)#line vty 0 15
SW1-MEDELLLIN(config-line)#password cisco
SW1-MEDELLLIN(config-line)#login
SW1-MEDELLLIN(config-line)#service password-encryption
SW1-MEDELLLIN(config)#banner motd "Acceso restringido"
SW1-MEDELLLIN(config)#

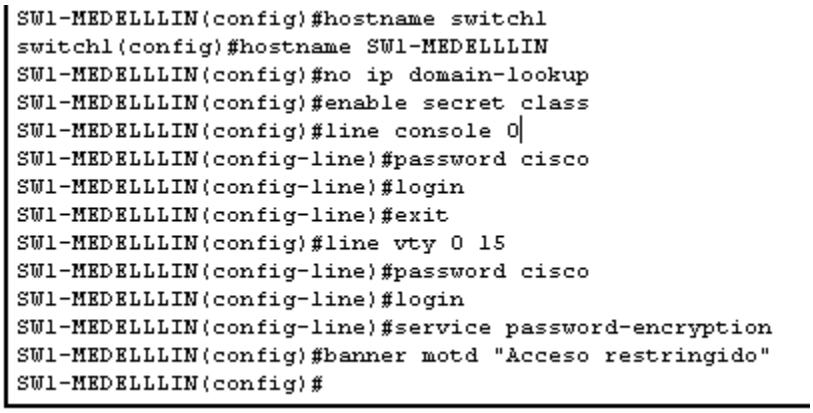

IMAGEN 13 CONFIGURACIÓN SEGURIDAD ACCESO SWITCH MEDELLÍN

SWITCH MEDELLIN CONFIGURACION DIRECCIONAMIENTO IP

SW1-MEDELLLIN(config-if)#interface vlan 1
SW1-MEDELLLIN(config-if)#ip address 192.168.1.34 255.255.255.224
SW1-MEDELLLIN(config-if)#no shutdown

SW1-MEDELLLIN(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

```
SW1-MEDELLLIN(config)#interface vlan 1
SW1-MEDELLLIN(config-if)#ip address 192.168.1.34 255.255.255.224
SW1-MEDELLLIN(config-if)#no shut
SW1-MEDELLLIN(config-if)#no shutdown

SW1-MEDELLLIN(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up

SW1-MEDELLLIN(config-if)#
```

IMAGEN 14 CONFIGURACIÓN IP VLAN 1 SWITCH MEDELLÍN

SWITCH BOGOTA CONFIGURACION DIRECCIONAMIENTO IP

SW2-BOGOTA(config)#no ip domain-lookup
SW2-BOGOTA (config)#enable secret class
SW2-BOGOTA (config)#line console 0
SW2-BOGOTA (config-line)#password cisco
SW2-BOGOTA (config-line)#login
SW2-BOGOTA (config-line)#exit
SW2-BOGOTA (config)#line vty 0 15
SW2-BOGOTA (config-line)#password cisco
SW2-BOGOTA (config-line)#login
SW2-BOGOTA (config-line)#service password-encryption
SW2-BOGOTA (config)#banner motd "Porhibido el Acceso no
A"
SW2-BOGOTA (config)#
SW2-BOGOTA(config-if)#interface vlan 1
SW2-BOGOTA(config-if)#ip address 192.168.1.2 255.255.255.224
SW2-BOGOTA (config-if)#no shutdown

SW2-BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

```
R2-BOGOTA(config-if)#hos
R2-BOGOTA(config-if)#exit
R2-BOGOTA(config)#hos
R2-BOGOTA(config)#hostname SW2-BOGOTA
SW2-BOGOTA(config)#no ip domain-lookup
SW2-BOGOTA(config)#enable secret class
SW2-BOGOTA(config)#line console 0
SW2-BOGOTA(config-line)#password cisco
SW2-BOGOTA(config-line)#login
SW2-BOGOTA(config-line)#line vty 0 15
SW2-BOGOTA(config-line)#password cisco
SW2-BOGOTA(config-line)#login
SW2-BOGOTA(config-line)#exit
SW2-BOGOTA(config)#service password-encryption
SW2-BOGOTA(config)#banner motd "Prohibido el Acceso no
Autorizado"
SW2-BOGOTA(config)#enable secret classinterface vlan 1
SW2-BOGOTA(config)#line console 0
SW2-BOGOTA(config-line)#exit
SW2-BOGOTA(config)#interface vlan 1
SW2-BOGOTA(config-if)#ip address 192.168.1.2 255.255.255.224
SW2-BOGOTA(config-if)#no sh
SW2-BOGOTA(config-if)#no shutdown
SW2-BOGOTA(config-if)#
```

IMAGEN 15 CONFIGURACIÓN SEGURIDAD ACCESO SWITCH BOGOTÁ Y VLAN 1

SWITCH CALI CONFIGURACION Y DIRECCIONAMIENTO IP

SW3-CALI(config)#no ip domain-lookup
SW3-CALI (config)#enable secret class
SW3-CALI (config)#line console 0
SW3-CALI (config-line)#password cisco
SW3-CALI (config-line)#login
SW3-CALI (config-line)#exit
SW3-CALI (config)#line vty 0 15
SW3-CALI (config-line)#password cisco
SW3-CALI (config-line)#login
SW3-CALI (config-line)#service password-encryption
SW3-CALI (config)#banner motd "Porhibido el Acceso no
A"
SW3-CALI (config)#
SW3-CALI (config-if)#interface vlan 1
SW3-CALI (config-if)#ip address 192.168.1.66 255.255.255.224
SW3-CALI (config-if)#no shutdown

SW3-CALI (config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname SW3-CALI
SW3-CALI(config)#no ip domain-lookup
SW3-CALI(config)#enable secret class
SW3-CALI(config)#line console 0
SW3-CALI(config-line)#password cisco
SW3-CALI(config-line)#login
SW3-CALI(config-line)#line vty 0 15
SW3-CALI(config-line)#password cisco
SW3-CALI(config-line)#login
SW3-CALI(config-line)#exit
SW3-CALI(config)#service password-encryption
SW3-CALI(config)#banner motd "Prohibido el Acceso no Autorizado"
SW3-CALI(config)#interface vlan 1
SW3-CALI(config-if)#ip address 192.168.1.66 255.255.255.224
SW3-CALI(config-if)#no sh
SW3-CALI(config-if)#no shutdown

SW3-CALI(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

IMAGEN 16 CONFIGURACIÓN SEGURIDAD ACCESO SWITCH CALI Y VLAN 1

PC1 CONFIGURACION DIRECCIONAMIENTO IP HOST MEDELLIN

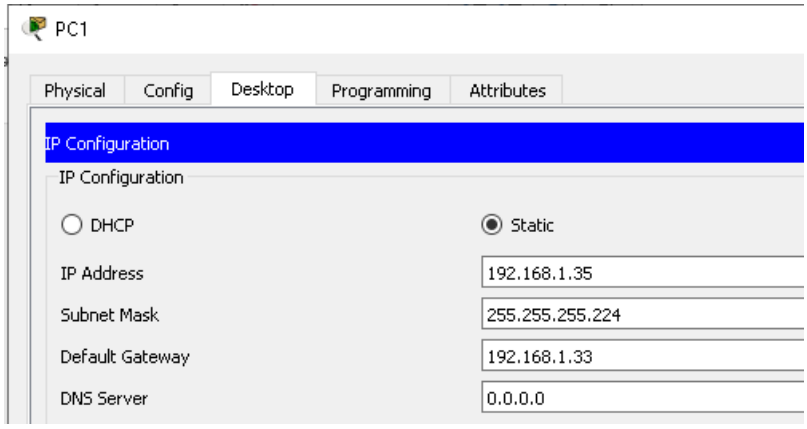

IMAGEN 17 CONFIGURACIÓN IP PC1 MEDELLÍN

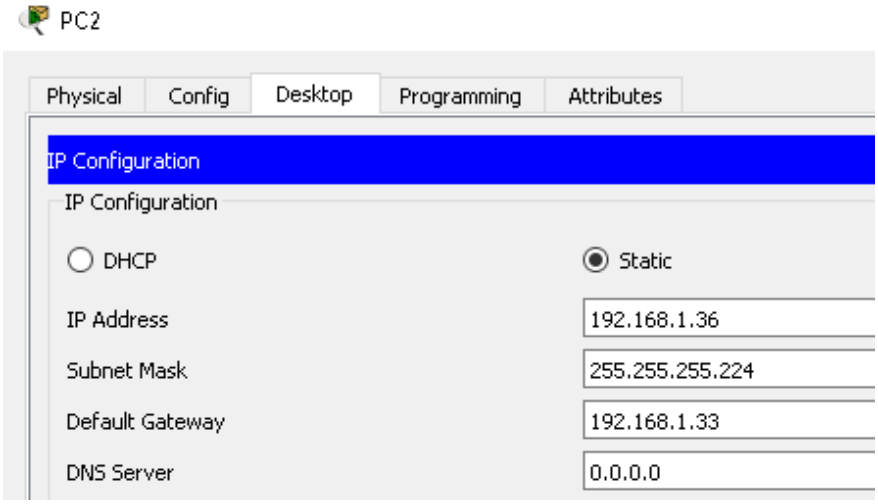

IMAGEN 18 CONFIGURACIÓN PC2 MEDELLÍN

PC3 CONFIGURACION DIRECCIONAMIENTO IP HOST CALI

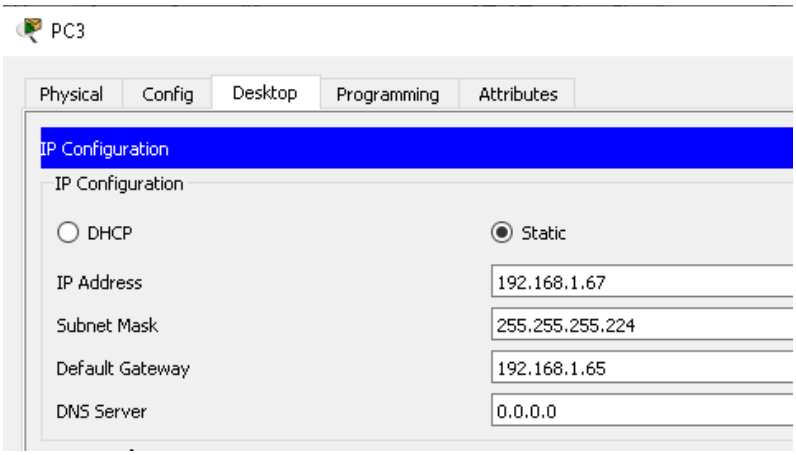

IMAGEN 19 CONFIGURACIÓN IP PC3 CALI

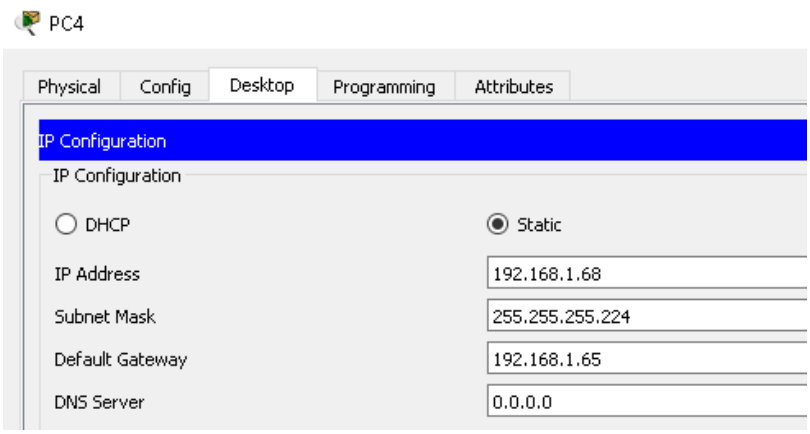

IMAGEN 20 CONFIGURACIÓN IP PC4 CALI

PC3 CONFIGURACION DIRECCIONAMIENTO IP HOST BOGOTA

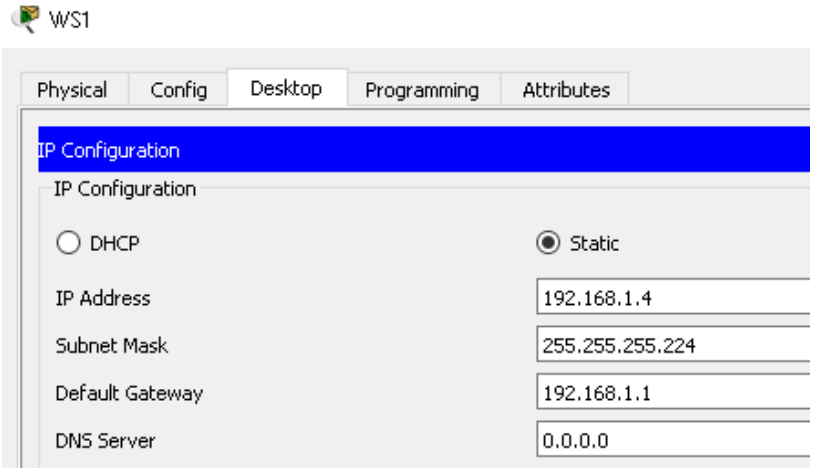

IMAGEN 21 CONFIGURACIÓN IP PC WS1 BOGOTÁ

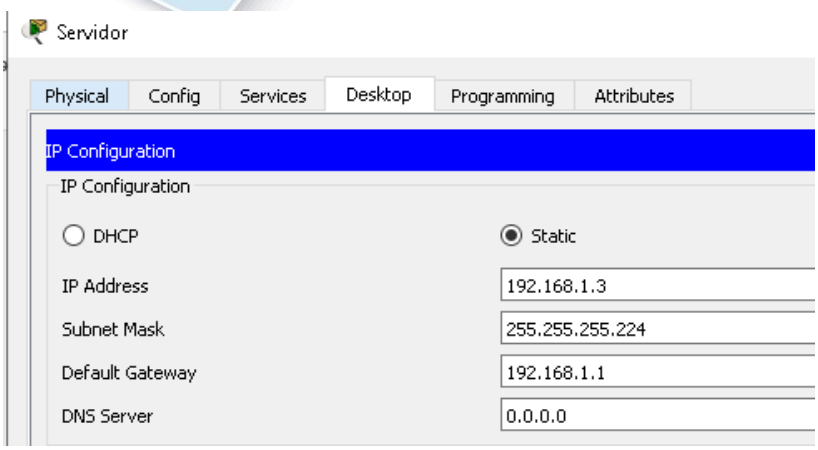

IMAGEN 22 CONFIGURACIÓN IP SERVIDOR BOGOTÁ

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

Se verifica la tabla de enrutamiento en el router de MEDELLIN

R1-MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:27:12, 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, 00:18:35, 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, 00:20:47, Serial0/0/0

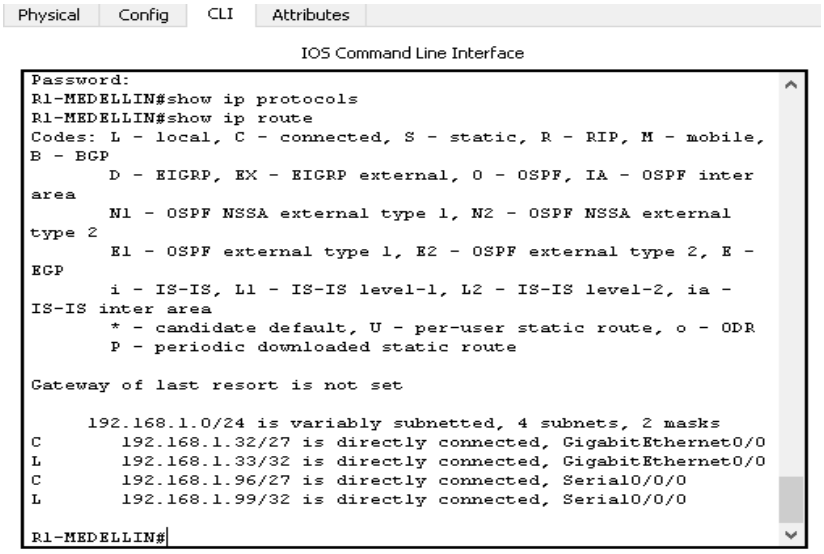

IMAGEN 23 TABLA ENRUTAMIENTO ROUTER MEDELLÍN

Se verifica la tabla de enrutamiento en el router de BOGOTA

R2-BOGOTA>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:31:50, Serial0/0/0
D 192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:20:45, 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

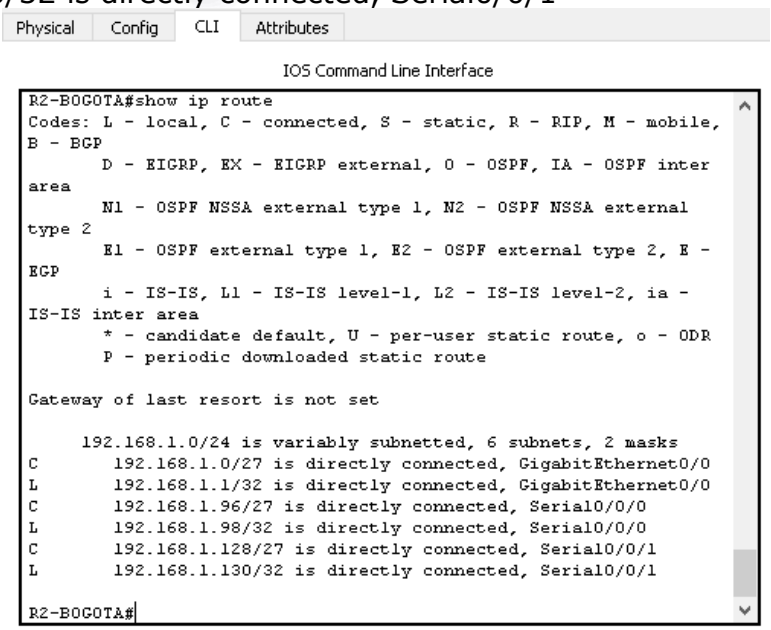

IMAGEN 24 TABLA DE ENRUTAMIENTO ROUTER BOGOTÁ

Se verifica la tabla de enrutamiento en el router de CALI

R3-CALI>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:23:24, Serial0/0/0
D 192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:23:24, 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, 00:23:24, 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

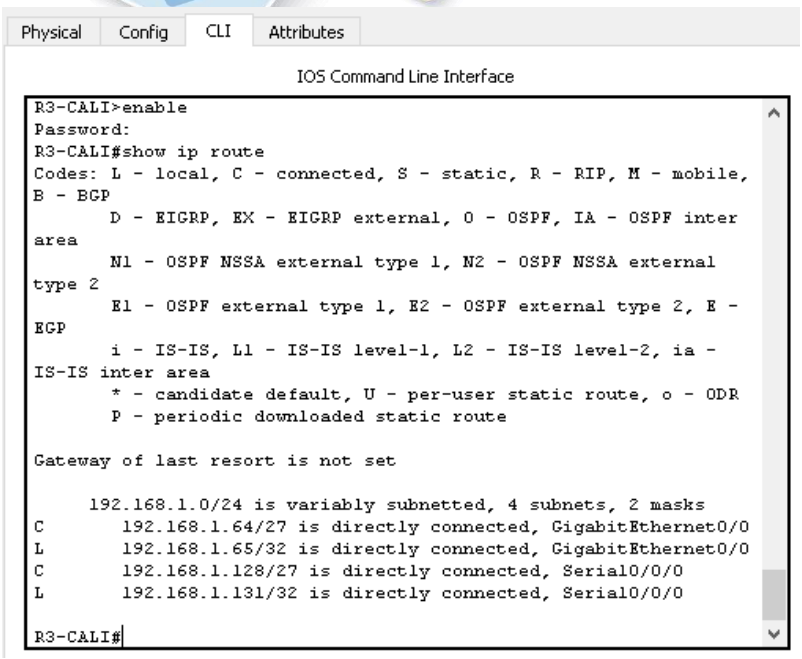

IMAGEN 25 TABLA ENRUTAMIENTO ROUTER CALI

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

En este Punto no se puede verificar Balanceo, es un entorno Virtual y adicional los equipos no tiene enlaces redundantes para poder realizar el balaceo.

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

SE REALIZA EL DIAGNOSTICO DE VECINOS USANDO EL COMANDO CDP EN LOS ROUTERS

R1-MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW1-MEDELLLIN
Gig 0/0 131 S 2960 Gig 0/1
R2-BOGOTA Ser 0/0/0 167 R C1900 Ser 0/0/0

```
R1-MEDELLIN#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform
Port ID
SW1-MEDELLLIN
              Gig 0/0          163            S       2960
Gig 0/1
R2-BOGOTA     Ser 0/0/0        163            R       C1900
Ser 0/0/0
R1-MEDELLIN#
```

IMAGEN 26 VERICACIÓN VECINOS ROUTER MEDELLÍN

R2-BOGOTA>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW2-BOGOTA Gig 0/0 173 S 2960 Gig 0/1
R1-MEDELLIN Ser 0/0/0 137 R C1900 Ser 0/0/0
R3-CALI Ser 0/0/1 149 R C1900 Ser 0/0/0

```
R2-BOGOTA#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform
Port ID
SW2-BOGOTA    Gig 0/0          175            S       2960
Gig 0/1
R3-CALI       Ser 0/0/1        175            R       C1900
Ser 0/0/0
R1-MEDELLIN   Ser 0/0/0        175            R       C1900
Ser 0/0/0
R2-BOGOTA#
```

IMAGEN 27 VERIFIACIÓN VECINOS ROUTER BOGOTÁ

R3-CALI>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW3-CALI Gig 0/0 134 S 2960 Gig 0/1
R2-BOGOTA Ser 0/0/0 122 R C1900 Ser 0/0/1

```
R3-CALI#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform
Port ID
SW3-CALI      Gig 0/0          131            S       2960
Gig 0/1
R2-BOGOTA     Ser 0/0/0        131            R       C1900
Ser 0/0/1
R3-CALI#
```

IMAGEN 28 VERIFICACIÓN VECINOS ROUTER CALI

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

REALIZAMOS PING DESDE LOS HOST DE MEDELLIN A ROUTER DE MEDELLIN PARA VALIDAR CONECTIVIDAD.

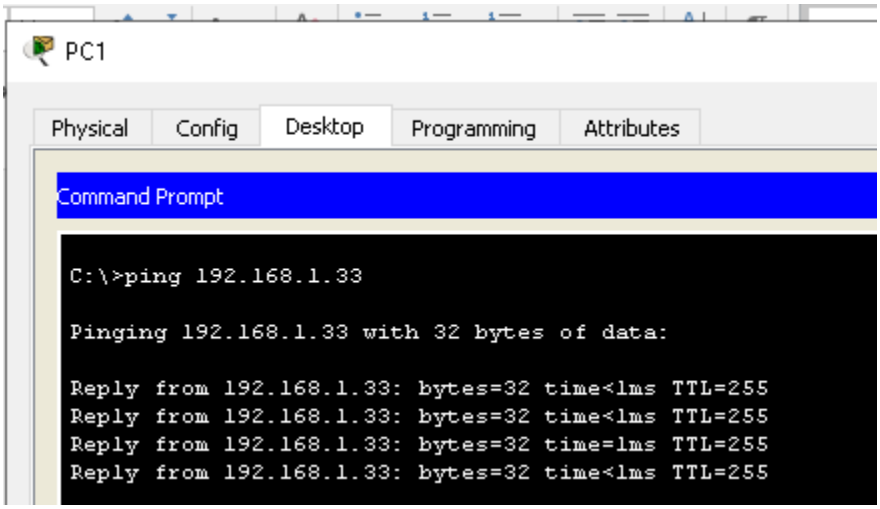

IMAGEN 29 VERIFICACIÓN CONECTIVIDAD PC1 A ROUTER MEDELLÍN

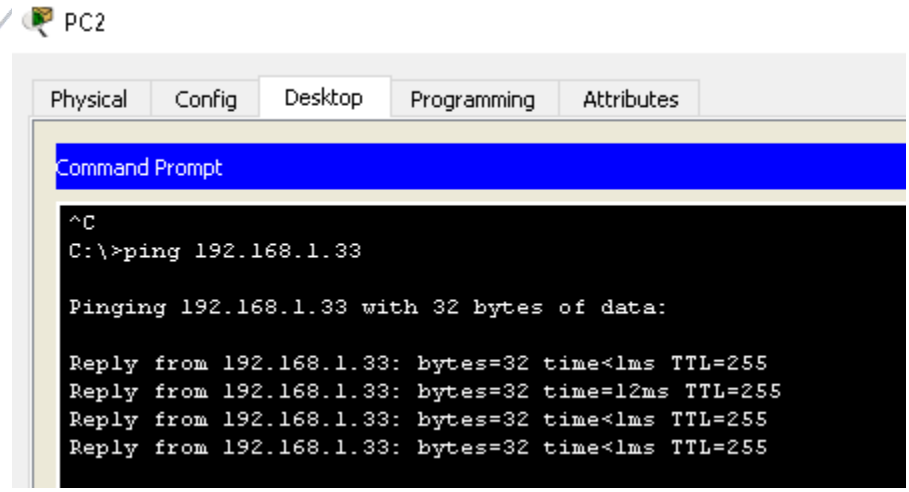

IMAGEN 30 VERIFICACIÓN CONECTIVIDAD PC2 A ROUTER MEDELLÍN

REALIZAMOS PING DESDE LOS HOST DE CALI A ROUTER DE CALI PARA VALIDAR CONECTIVIDAD.

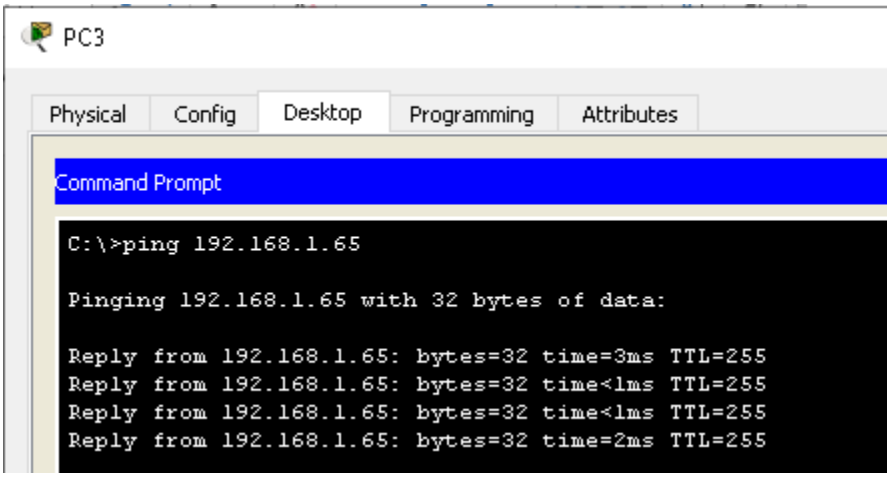

IMAGEN 31 VERIFICACIÓN CONECTIVIDAD PC3 A ROUTER CALI

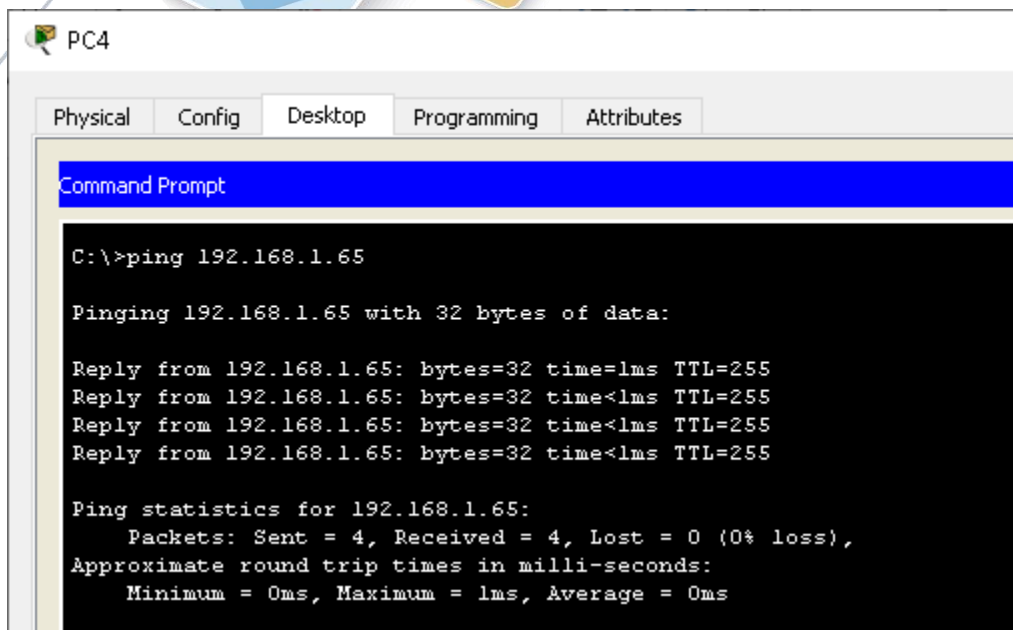

IMAGEN 32 VERIFICACIÓN CONECTIVIDAD PC4 A ROUTER CALÍ

REALIZAMOS PING DESDE LOS HOST DE BOGOTA A ROUTER DE BOGOTA PARA VALIDAR CONECTIVIDAD.

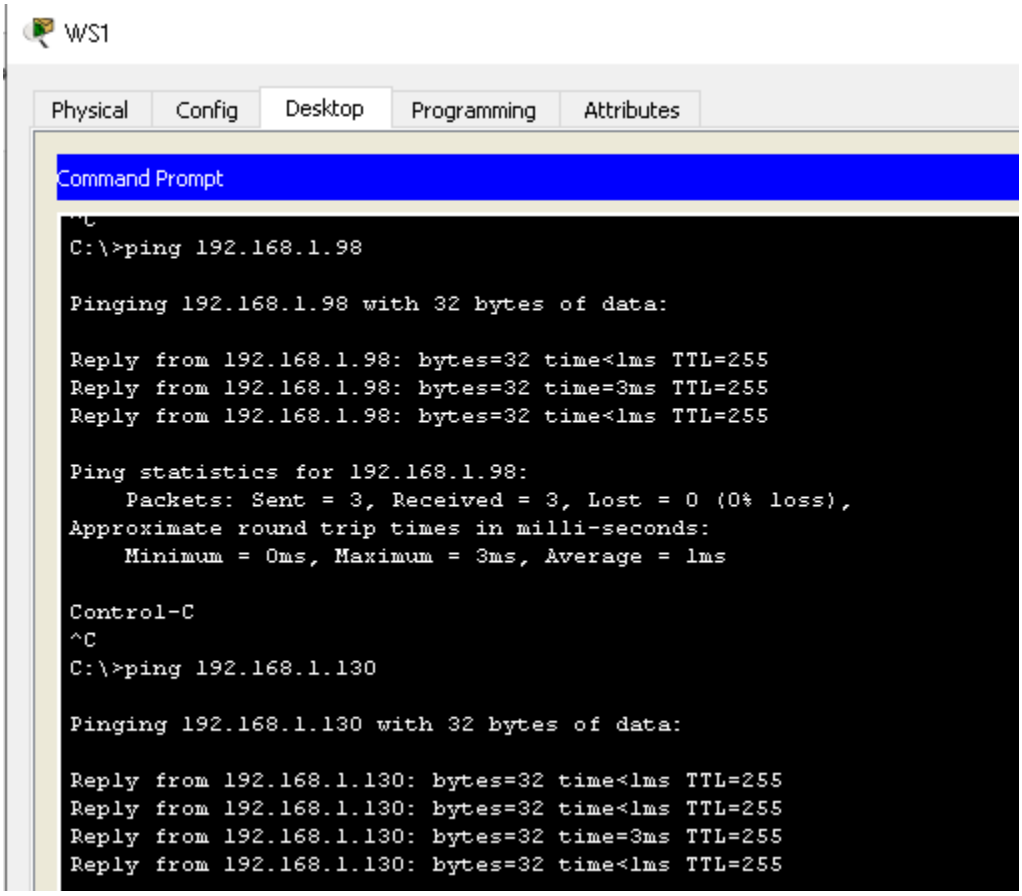

IMAGEN 33 VERIFICAR CONECTIVIDAD PC WS1 A ROUTER BOGOTA

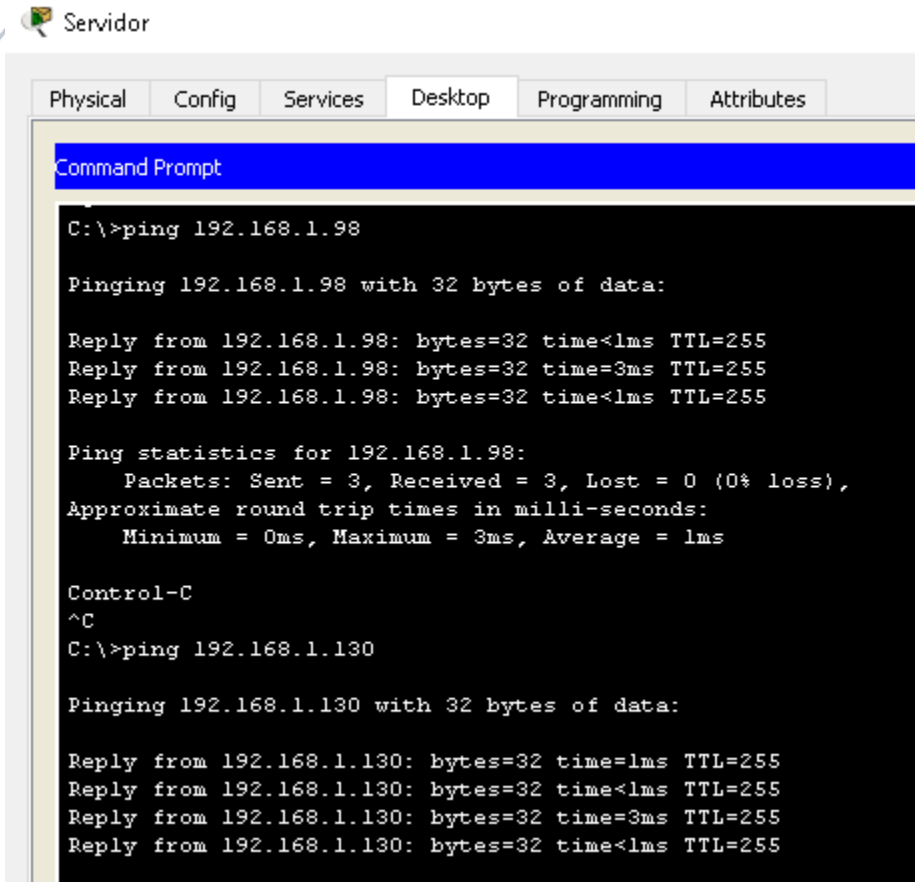

IMAGEN 34 VERIFICACIÓN CONECTIVIDAD SERVIDOR A ROUTER BOGOTÁ

Parte 3: Configuración de Enrutamiento.

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

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE MEDELLIN.

R1-MEDELLIN(config-router)#no auto-summary
R1-MEDELLIN(config-router)#net
R1-MEDELLIN(config-router)#network 192.168.1.33 255.255.255.224
R1-MEDELLIN(config-router)#network 192.168.1.99 255.255.255.224
R1-MEDELLIN(config-router)#

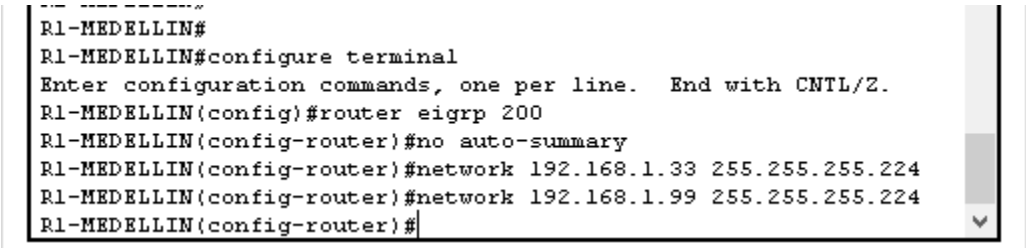

IMAGEN 35 CONFIGURACIÓN PROTOCOLO ENRUTAMIENTO EIGRP ROUTER MEDELLÍN

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE BOGOTA.

Enter configuration commands, one per line. End with CNTL/Z.
R2-BOGOTA(config)#router eigrp 200
R2-BOGOTA(config-router)#no auto-summary
R2-BOGOTA(config-router)#network 192.168.1.1 255.255.255.224
R2-BOGOTA(config-router)#network 192.168.1.98 255.255.255.224

```
R2-BOGOTA#conf
R2-BOGOTA#configure ter
R2-BOGOTA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2-BOGOTA(config)#router eigrp 200
R2-BOGOTA(config-router)#no auto-summary
R2-BOGOTA(config-router)#network 192.168.1.1 255.255.255.224
R2-BOGOTA(config-router)#network 192.168.1.98 255.255.255.224
R2-BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99
(Serial0/0/0) is up: new adjacency

R2-BOGOTA(config-router)#network 192.168.1.130 255.255.255.224
R2-BOGOTA(config-router)#network 192.168.1.130 255.255.255.224
R2-BOGOTA(config-router)#
```

IMAGEN 36 CONFIGURACIÓN PROTOCOLO EIGRP ROUTER BOGOTÁ

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE CALI.

R3-CALI(config)#router eigrp 200
R3-CALI(config-router)#no auto-summary
R3-CALI(config-router)#network 192.168.1.65 255.255.255.224
R3-CALI(config-router)#network 192.168.1.131 255.255.255.224

```
R3-CALI#configure ter
R3-CALI#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3-CALI(config)#
R3-CALI(config)#
R3-CALI(config)#router eigrp 200
R3-CALI(config-router)#no auto-summary
R3-CALI(config-router)#network 192.168.1.65 255.255.255.224
R3-CALI(config-router)#network 192.168.1.131 255.255.255.224
R3-CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130
(Serial0/0/0) is up: new adjacency

R3-CALI(config-router)#
```

IMAGEN 37 CONFIGURACIÓN PROTOCOLO EIGRP ROUTER CALI

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

SE VERIFICA VECINDAD EN EL ROUTER DE MEDELLIN.

R1-MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW1-MEDELLLIN
Gig 0/0 151 S 2960 Gig 0/1
R2-BOGOTA Ser 0/0/0 128 R C1900 Ser 0/0/0

```
R1-MEDELLIN#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme     Capability   Platform
Port ID
SW1-MEDELLLIN
              Gig 0/0          163             S       2960
Gig 0/1
R2-BOGOTA     Ser 0/0/0        163             R       C1900
Ser 0/0/0
R1-MEDELLIN#
```

IMAGEN 38 VERIFICACIÓN VECINDAD ROUTER MEDELLÍN

SE VERIFICA VECINDAD EN EL ROUTER DE BOGOTA

R2-BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW2-BOGOTA Gig 0/0 147 S 2960 Gig 0/1
R1-MEDELLIN Ser 0/0/0 172 R C1900 Ser 0/0/0

R3-CALI Ser 0/0/1 124 R C1900 Ser 0/0/0

```
R2-BOGOTA#enable Show cdp neighbors
                 ^
% Invalid input detected at '^' marker.

R2-BOGOTA#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform
Port ID
SW2-BOGOTA    Gig 0/0          135            S       2960
Gig 0/1
R3-CALI       Ser 0/0/1        135            R       C1900
Ser 0/0/0
R1-MEDELLIN   Ser 0/0/0        135            R       C1900
Ser 0/0/0
R2-BOGOTA#
```

IMAGEN 39 VERIFICACIÓN VECINDAD ROUTER BOGOTÁ

SE VERIFICA VECINDAD EN EL ROUTER DE CALI

R3-CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
SW3-CALI Gig 0/0 160 S 2960 Gig 0/1
R2-BOGOTA Ser 0/0/0 149 R C1900 Ser 0/0/1

```
R3-CALI#Show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce   Holdtme    Capability   Platform
Port ID
SW3-CALI      Gig 0/0          163            S       2960
Gig 0/1
R2-BOGOTA     Ser 0/0/0        163            R       C1900
Ser 0/0/1
R3-CALI#
```

IMAGEN 40 VERIFICACIÓN VECINDAD ROUTER CALI

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

SE VERIFICA TABLA DE ENRUTAMIENT EN EL ROUTER DE MEDELLIN.

```
R1-MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:39:07,
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, 00:30:30,
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, 00:32:42,
Serial0/0/0
```

```
R1-MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:07:14,
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, 00:04:43,
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, 00:06:59,
Serial0/0/0

R1-MEDELLIN#
```

IMAGEN 41 VERIFICACIÓN TABLA ENRUTAMIENTO ROUTER MEDELLÍN

SE VERIFICA TABLA DE ENRUTAMIENT EN EL ROUTER DE BOGOTA.

R2-BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:42:10,
Serial0/0/0
D 192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:31:05,
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

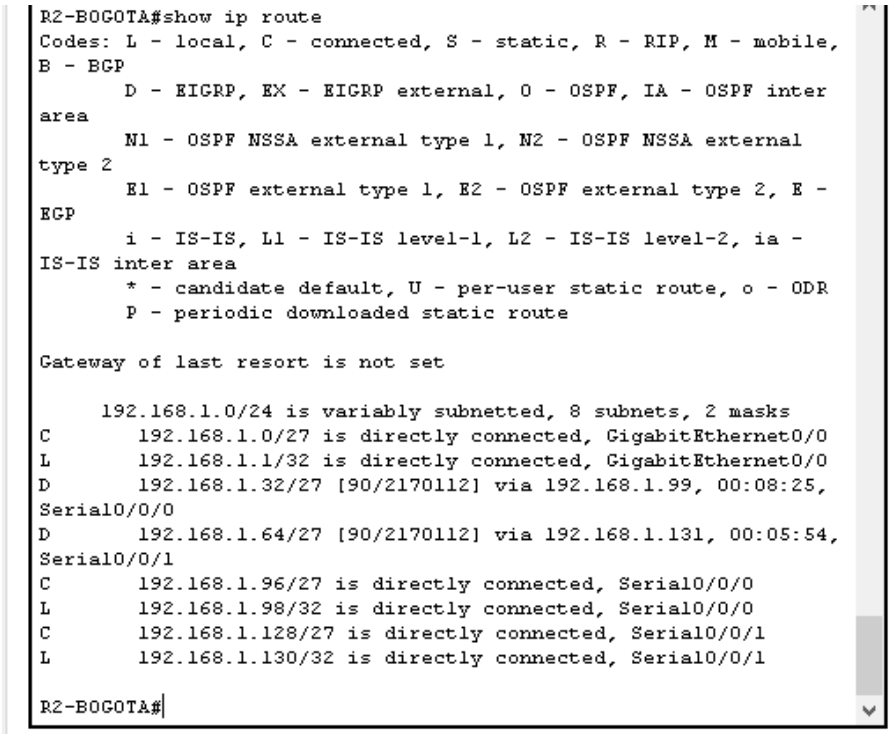

IMAGEN 42 VERIFICACIÓN TABLA ENRUTAMIENTO ROUTER BOGOTÁ

SE VERIFICA TABLA DE ENRUTAMIENT EN EL ROUTER DE CALI.

R3-CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

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

D 192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:33:26, Serial0/0/0
D 192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:33:26, 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, 00:33:26, 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

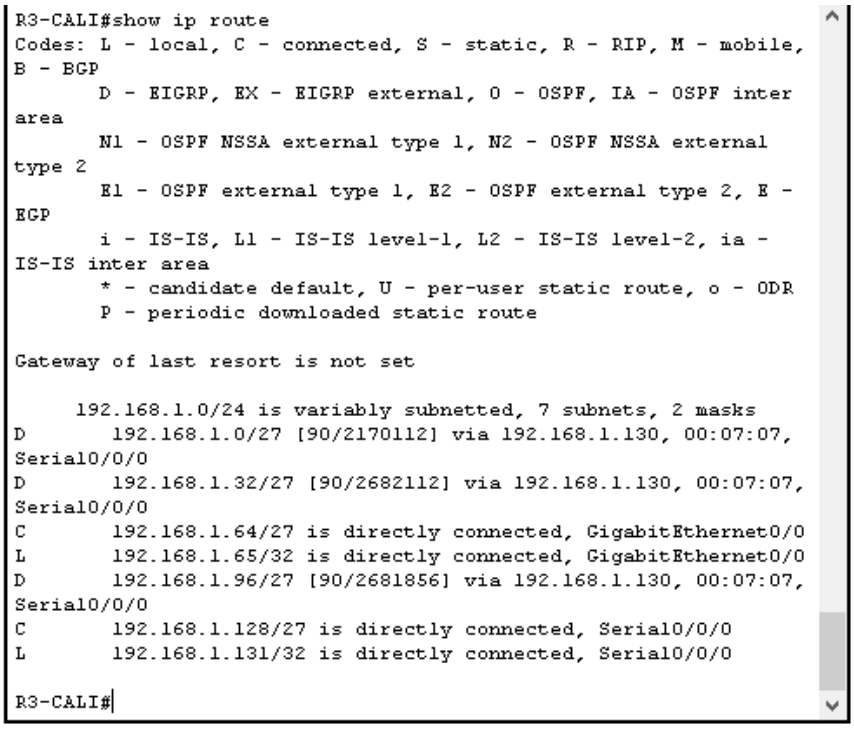

IMAGEN 43 VERIFICACIÓN TABLA ENRUTAMIENTO ROUTER CALI

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

SE VERIFICA CONECTIVIDAD DESDE EL PC 4 DE LA RED DE CALI HACIA UN PC DE LA RED DE MEDELLIN.

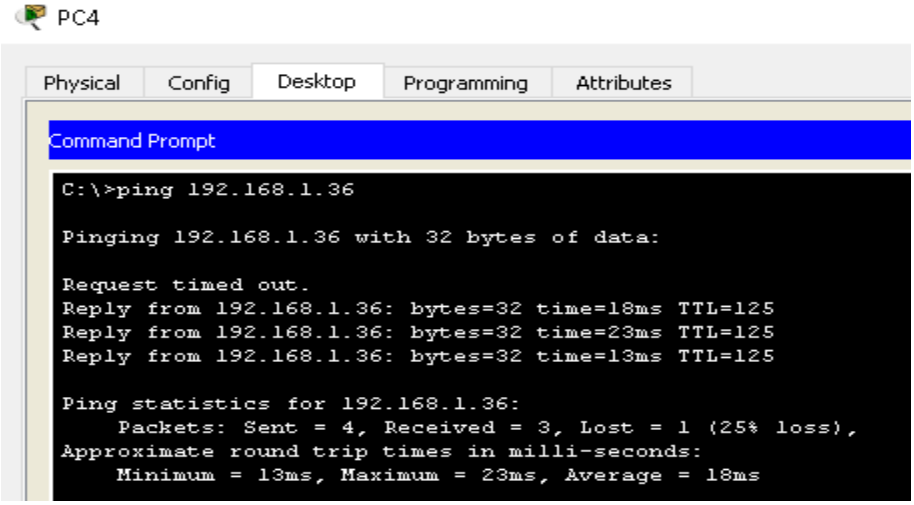

IMAGEN 44 PRUEBA CONECTIVIDAD PC4 CALI A RED MEDELLÍN

SE VERIFICA CONECTIVIDAD DESDE EL PC 4 DE LA RED DE CALI HACIA EL SERVIDOR DE LA RED DE BOGOTA.

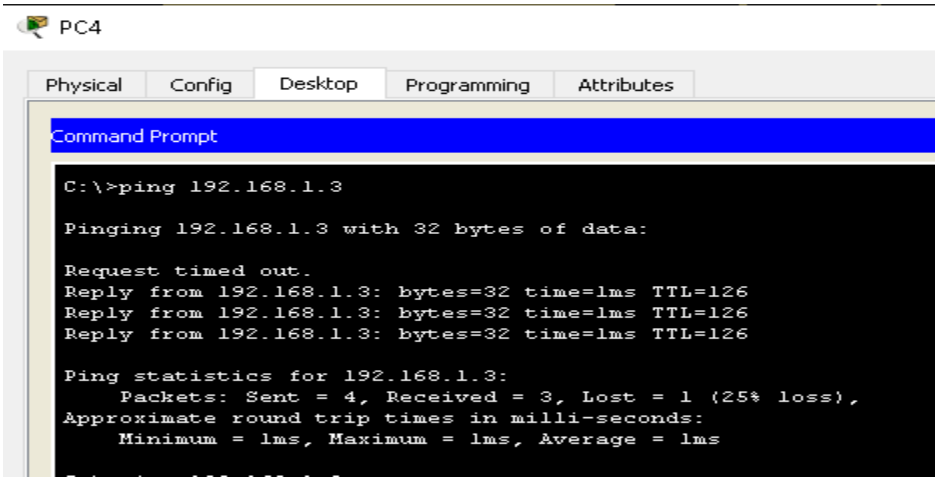

IMAGEN 45 PRUEBA CONECTIVIDAD PC4 RED CALI A LA RED DE BOGOTÁ

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

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

Las condiciones para crear las ACL son las siguientes:

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

LAS CONEXIONES A TELNET SE HABILITARON EN LOS ROUTERS CON LA CONFIGURACION DE LINE VTY **AL INICIIO DE CONFIGURACIÓN DEL ESCENARIO.**

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.

SE CONFIGURA UNA ACL ESTATICA QUE SOLO PERMITA QUE EL SERVIDOR PUEDA CONECTARESE CON LAS DEMAS REDES Y LOS DEMAS HOST DE LA RED DE BOGOTA NO PODRAN CONECTARSE SINO A SU RED INTERNA.

```
R2-BOGOTA(config)#access-list 1 per
R2-BOGOTA(config)#access-list 1 permit 192.168.1.3
R2-BOGOTA(config)#int
R2-BOGOTA(config)#interface g
R2-BOGOTA(config)#interface gigabitEthernet 0/0
R2-BOGOTA(config-if)#ip access
   R2-BOGOTA(config-if)#ip access-group 1 out
```

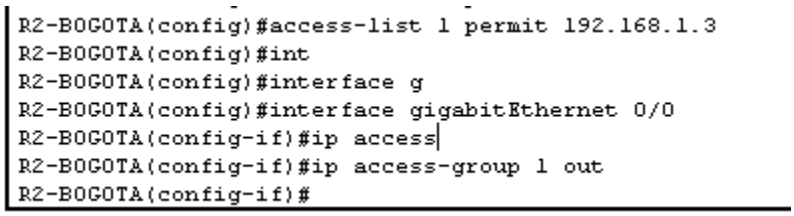

IMAGEN 46 CONFIGURACIÓN ACLE ROUTER BOGOTÁ

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

SE CONFIGURA UNA ACL EXTENDIDAD **EN EL RPUTER DE MEDELLIN, PARA QUE SOLO PERMITA QUE LOS HOST DE ESA RED PUEDAN SACAR TRAFICO DE RED SOLO AL SERVIDOR, PERMITIR EL TRAFICO TELNET**

R1-MEDELLIN(config)#access-list 1 permit 192.168.1.3
R1-MEDELLIN(config)#in
R1-MEDELLIN(config)#interface g
R1-MEDELLIN(config)#interface gigabitEthernet 0/0
R1-MEDELLIN(config-if)#ip acca
R1-MEDELLIN(config-if)#ip acc
R1-MEDELLIN(config-if)#ip access-group 1 o
R1-MEDELLIN(config-if)#ip access-group 1 out

R1-MEDELLIN(config)#access-list 100 per
R1-MEDELLIN(config)#access-list 100 permit tcp 192.168.1.32 0.0.0.255 host 192.168.1.3 eq 23
R1-MEDELLIN(config)#interface gigabitEthernet 0/0
R1-MEDELLIN(config-if)#ip access-group 100 out

```
R1-MEDELLIN(config)#acc
R1-MEDELLIN(config)#access-list 100 per
R1-MEDELLIN(config)#access-list 100 permit tcp 192.168.1.32 0.0.0.255 host
192.168.1.3 eq 23
R1-MEDELLIN(config)#interface gigabitEthernet 0/0
R1-MEDELLIN(config-if)#ip access-group 100 out
R1-MEDELLIN(config-if)#
```

IMAGEN 47 CONFIGURACIÓN ACL ROUTER BOGOTÁ

SE CONFIGURA UNA ACL EXTENDIDAD EN EL RPUTER DE CALI, PARA QUE SOLO PERMITA QUE LOS HOST DE ESA RED PUEDAN SACAR TRAFICO DE RED SOLO AL SERVIDOR DE BOGOTA Y DENIEGUE LA

SALIDA DEL RESTO DE TRAFICO DE RES A LAS REDES DE MEDELLIN Y BOGOTA.

R3-CALI(config)#access-list 1 permit 192.168.1.3
R3-CALI(config)#int
R3-CALI(config)#interface g
R3-CALI(config)#interface gigabitEthernet 0/0
R3-CALI(config-if)#ip ac
R3-CALI(config-if)#ip access-group 1 ou
R3-CALI(config-if)#ip access-group 1 out

R3-CALI(config)#access-list 100 per
R3-CALI(config)#access-list 100 permit tcp 192.168.1.32 0.0.0.255 host 192.168.1.3 eq 23
R3-CALI(config)#interface gigabitEthernet 0/0
R3-CALI(config-if)#ip access-group 100 out
R3-CALI(config-if)#

```
R3-CALI(config)#access-list 100 permit ip 192.168.1.32 0.0.0.255 host 192.168.1.3
R3-CALI(config)#inte
R3-CALI(config)#interface g
R3-CALI(config)#interface gigabitEthernet 0/0
R3-CALI(config-if)#ip acc
R3-CALI(config-if)#ip access-group 100 out
R3-CALI(config-if)#
```

IMAGEN 48 CONFIGURACIÓN ACL ROUTER CALI

Parte 5: Comprobación de la red instalada.

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

SE REALIZAN PRUENAS DESDE UN HOST DE LA RED DE MEDELLIN PARA COMPROBAR QUE LA ACL QUEDO BIEN CONFIGURADA Y NO PERMITE TRAFICO DE RED HACIA LA RED DE BOGOTA.

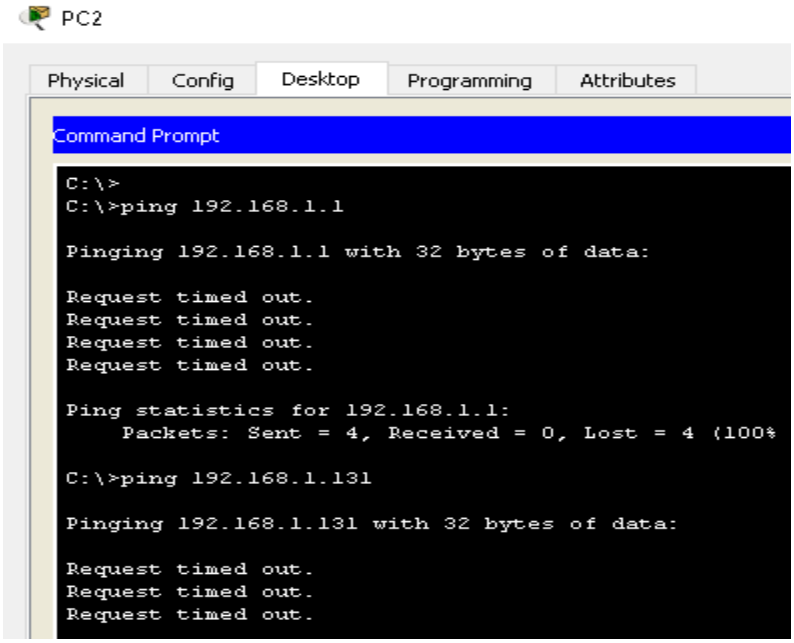

IMAGEN 49 VERIFICACIÓN ACL DESDE PC2 MEDELLÍN A RED BOGOTÁ

SE REALIZAN PRUEBAS DESDE UN HOST DE LA RED DE MEDELLIN PARA COMPROBAR QUE LA ACL QUEDO BIEN CONFIGURADA Y NO PERMITE TRAFICO DE RED HACIA LA RED DE CALI.

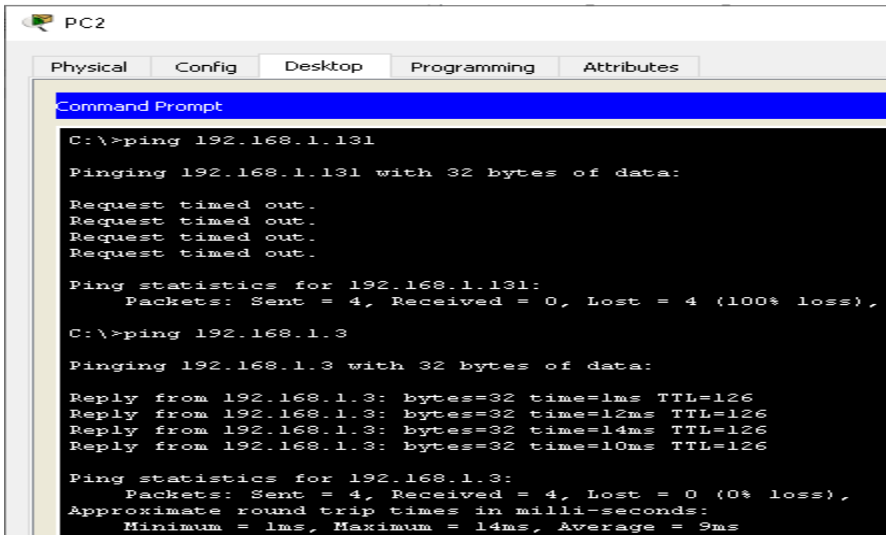

IMAGEN 50 PRUEBAS ACL RED MEDELLÍN PC2 A RED DE CALI

SE REALIZAN PRUENAS DESDE EL HOST SERVIDOR DE LA RED DE BOGOTA PARA COMPROBAR QUE LA ACL QUEDO BIEN CONFIGURADA Y QUE PERMITE TRAFICO HACIA LAS REDES DE MEDELLIN Y CALI.

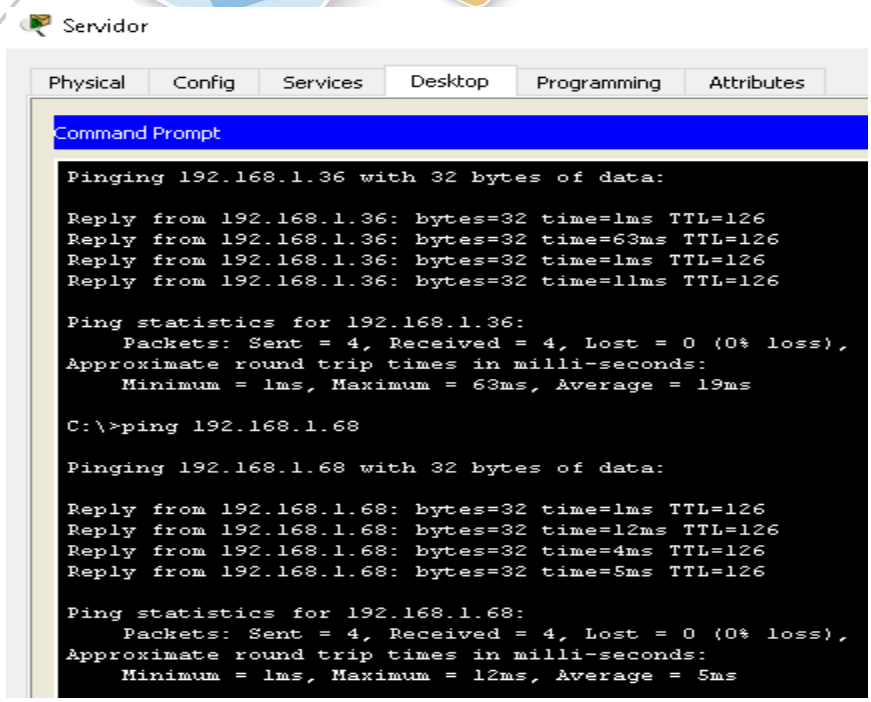

IMAGEN 51 PRUEBAS ACL SERVIDOR BOGOTÁ A LAS REDES DE MEDELLÍN Y CALI

SE REALIZAN PRUENAS DESDE EL HOST WS1 DE LA RED DE BOGOTA PARA COMPROBAR QUE LA ACL QUEDO BIEN CONFIGURADA Y QUE NO PERMITE TRAFICO DESDE LOS OTROS HOSTS HACIA LAS REDES DE MEDELLIN Y CALI, SOLO PERMITE TRAFICO EN SU PROPIA RED.

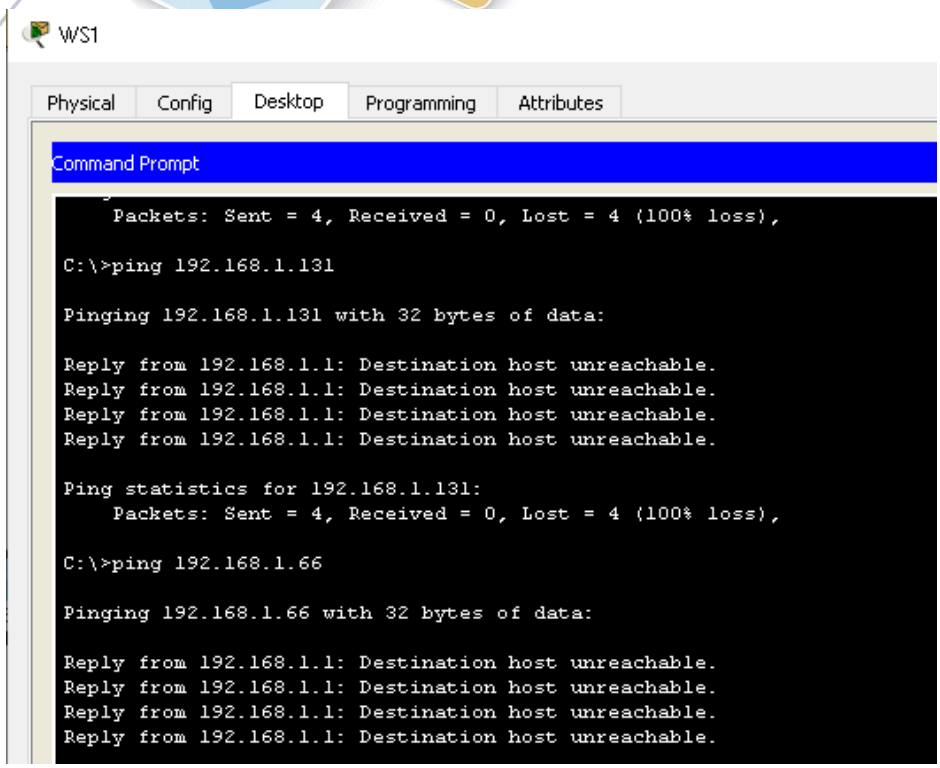

IMAGEN 52 PRUEBAS ACL BOGOTA PC WS1 A RED INTERNA

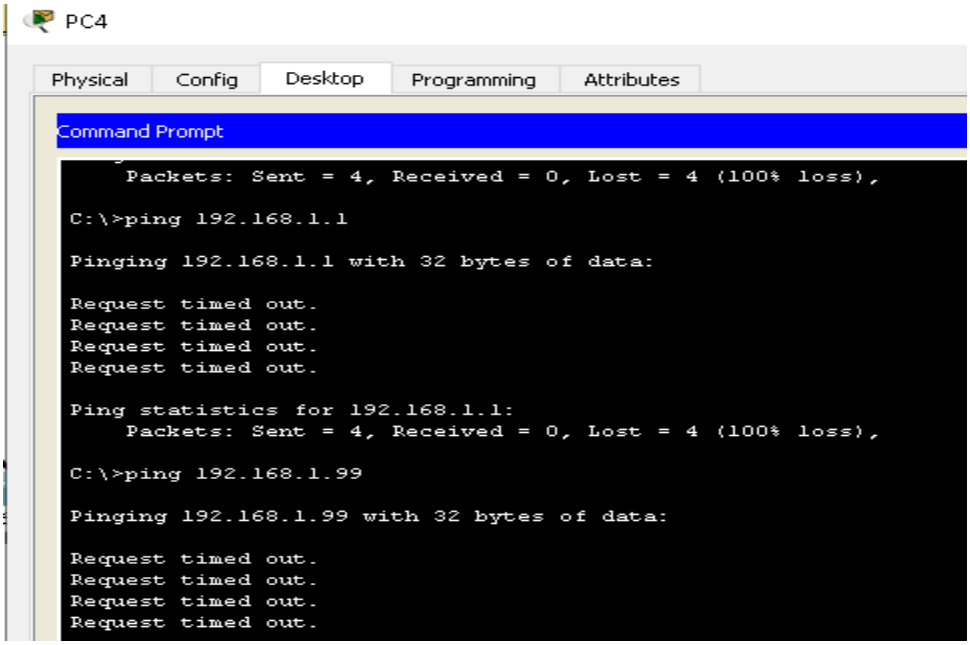

IMAGEN 53 PRUEBA ACL RED CALI A RED BOGOTA

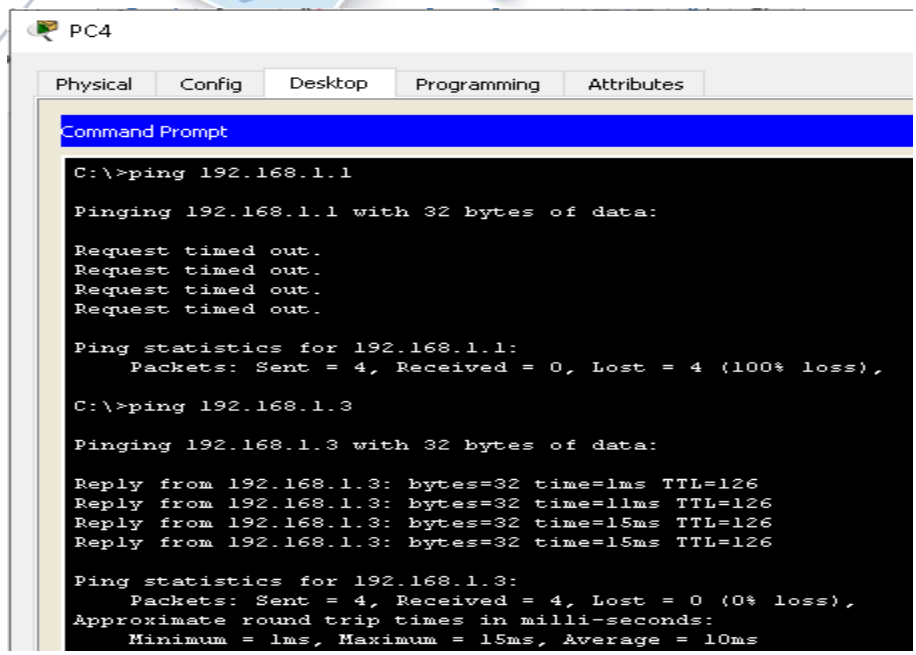

IMAGEN 54 PRUEBA ACL PC4 A RED INTERNA

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

SE REALIZAN LAS PRUEBAS DE CONECTIVIDAD OBTENIENDO LOS SIGUIENTES RESULTADOS.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	ACCESO OK
	WS_1	Router BOGOTA	ACCESO OK
	Servidor	Router CALI	ACCESO OK
	Servidor	Router MEDELLIN	ACCESO OK
TELNET	LAN del Router MEDELLIN	Router CALI	ACCESO DENEGADO
	LAN del Router CALI	Router CALI	ACCESO OK
	LAN del Router MEDELLIN	Router MEDELLIN	ACCESO OK
	LAN del Router CALI	Router MEDELLIN	ACCESO DENEGADO
PING	LAN del Router CALI	WS_1	ACCESO DENEGADO
	LAN del Router MEDELLIN	WS_1	ACCESO DENEGADO

	LAN del Router MEDELLIN	**LAN del Router CALI**	ACCESO DENEGADO
PING	**LAN del Router CALI**	**Servidor**	ACCESO OK
	LAN del Router MEDELLIN	**Servidor**	ACCESO OK
	Servidor	**LAN del Router MEDELLIN**	ACCESO OK
	Servidor	**LAN del Router CALI**	ACCESO OK
	Router CALI	**LAN del Router MEDELLIN**	ACCESO DENEGADO
	Router MEDELLIN	**LAN del Router CALI**	ACCESO DENEGADO

Escenario 2

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

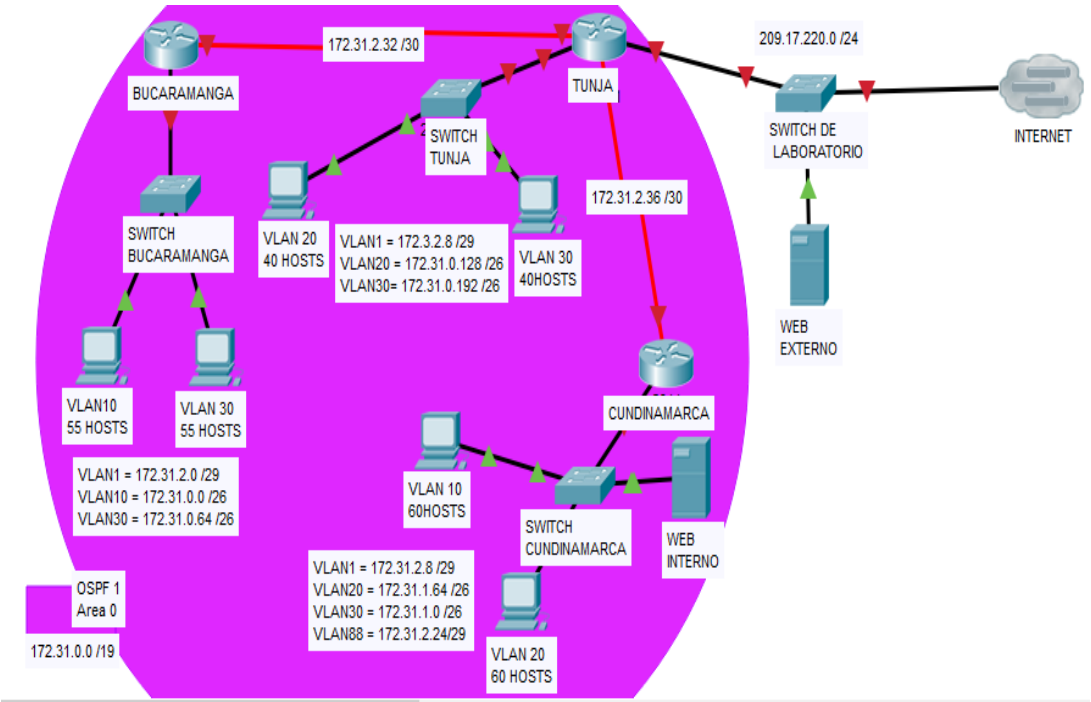

IMAGEN 55 ESCENARIO 2 PROPUESTA

Desarrollo

Los siguientes son los requerimientos necesarios:

1.Todos los routers deberán tener los siguiente:

•Configuración básica.

•Autenticación local con AAA.

•Cifrado de contraseñas.

•Un máximo de internos para acceder al router.

•Máximo tiempo de acceso al detectar ataques.

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

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

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

4. El enrutamiento deberá tener autenticación.

5. Listas de control de acceso:

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

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

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

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

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

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

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

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

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

Aspectos a tener en cuenta

• Habilitar VLAN en cada switch y permitir su enrutamiento.

• Enrutamiento OSPF con autenticación en cada router.

• Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

• Configuración de NAT estático y de sobrecarga.

• Establecer una lista de control de acceso de acuerdo con los criterios señalados.

• Habilitar las opciones en puerto consola y terminal virtual

DEACUERDO A LOS DATOS DEL DIRECCIONAMIENTO IP UTILIZAREMOS LA SIGUIENTE TABLA DE DIRECCIONAMIENTO IP

Se usa VLSM: se utiliza la dirección 172.31.0.0 /18 para el direccionamiento

TRABAJO RICANDO SUARES								
BUCARAMANGA			**TUNJA**			**CUNDINAMARCA**		
Vlan 10	Red 172.31.0.0/26		vlan 20	Red 172.31.0.128/26		vlan 10	Red 172.31.1.0/26	
GW	172.31.0.1		GW	172.31.0.129		GW	172.31.1.1	
vlan 30	Red 172.31.0.64/26		vlan 30	Red 172.31.0.192/26		vlan 20	Red 172.31.1.64/26	
GW	172.31.0.65		GW	172.31.0.193		GW	172.31.1.65	
						vlan 30	Red_192.168.10.0/24	
						GW	192.168.10.1	
vlan 2	10.130.200.0/29		vlan 2	10.130.200.8/29		vlan 2	10.130.200.16/29	
B/MANGA To TUNJA								
172.31.2.32/30								
Int Se0/0/0	172.31.2.33		Int Se0/0/0	172.31.2.34				
			TUNJA To C/MARCA					
			172.31.2.36/30					
			Int Se0/0/1	172.31.2.37		Int Se0/0/0	172.31.2.38	

SEGUDAMENTE DEBEMOS AGREGAR A LOS ROUTER UNA TARJETA SERIAL PARA PODER COMUNICARSE CON LOS OTROS ROUTERS.

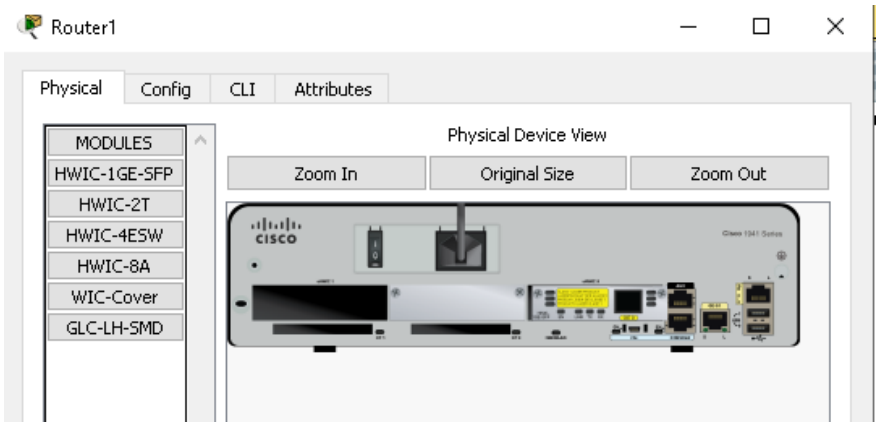

IMAGEN 56 ADICIÓN TARJETA INTERFACES SERIALES

SE REALIZAN LAS CONFIGURACIONES INDICADAS DE ACCESO Y SEGURIDAD EN EL ROUTER DE BUCARAMANGA.

```
router1(config)#hostname R-BMANGA
R-BMANGA(config)#no ip domain-lookup
R-BMANGA(config)#enable secret class
R-BMANGA(config)#line console 0
R-BMANGA(config-line)#password cisco
R-BMANGA(config-line)#login
R-BMANGA(config-line)#exit
R-BMANGA(config)#lines v
R-BMANGA(config)#lines vt
R-BMANGA(config)#line vty 0 15
R-BMANGA(config-line)#password cisco
R-BMANGA(config-line)#login
R-BMANGA(config-line)#service password-encryption
R-BMANGA(config)#banner motd "Acceso restringido"
R-BMANGA(config)# login block-for 300 attempts 5 within 30
```

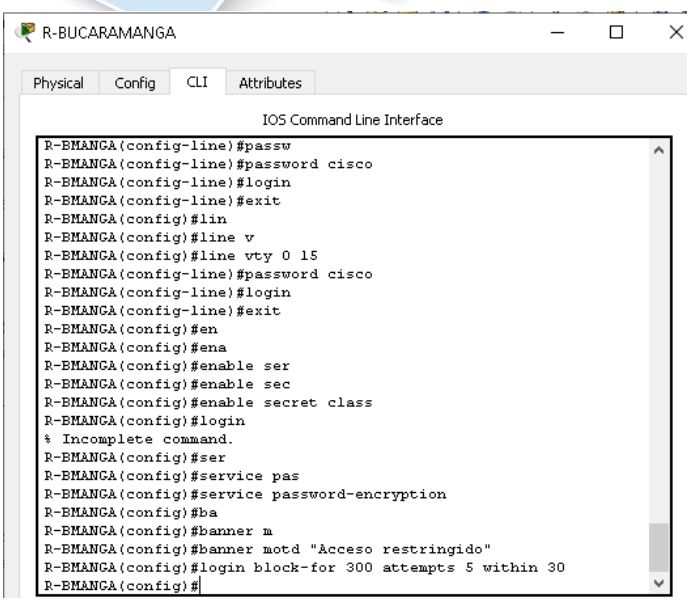

IMAGEN 57 CONFIGURACIÓN SEGURIDAD ACCESO ROUTER BUCARAMANGA

DE ACUERDO A LA TABLA DE DIRECCIONAMIENTO IP REALIZAMOS LA CONFIGURACION DE LAS INTERFACES DE RED EN EL ROUTER DE BUCARAMANGA, SE CONFIGURA EL DCHP CON USO DE IPHELPERT

R-BMANGA(config)#interface gigabitEthernet 0/0
R-BMANGA(config-if)#interface gigabitEthernet 0/0.2
R-BMANGA(config-subif)#en
R-BMANGA(config-subif)#encapsulation do
R-BMANGA(config-subif)#encapsulation dot1Q 2
R-BMANGA(config-subif)#ip address 10.130.200.2 255.255.255.240
R-BMANGA(config)#interface gigabitEthernet 0/0
R-BMANGA(config-if)#interface gigabitEthernet 0/0.10
R-BMANGA(config-subif)#en
R-BMANGA(config-subif)#encapsulation do
R-BMANGA(config-subif)#encapsulation dot1Q 10
R-BMANGA(config-subif)#ip address 172.131.0.1 255.255.255.192
R-BMANGA(config-subif)# ip helper-address 172.31.2.34
R-BMANGA(config-if)#interface gigabitEthernet 0/0.30
R-BMANGA(config-subif)# description VLAN30
R-BMANGA(config-subif)#encapsulation do
R-BMANGA(config-subif)#encapsulation dot1Q 30
R-BMANGA(config-subif)# ip address 172.31.0.65 255.255.255.192
R-BMANGA(config-subif)# ip helper-address 172.31.2.34

R-BMANGA(config-subif)# interface Serial0/0/0
R-BMANGA(config-subif)# ip address 172.31.2.33 255.255.255.252

```
R-BMANGA(config)#interface GigabitEthernet0/0.10
R-BMANGA(config-subif)#encapsulation dot1Q 10
R-BMANGA(config-subif)#ip addre
R-BMANGA(config-subif)#ip address 172.31.0.1/26
                                  ^
% Invalid input detected at '^' marker.

R-BMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
R-BMANGA(config-subif)#interface GigabitEthernet0/0.2
R-BMANGA(config-subif)#encapsulation dot1Q 2
R-BMANGA(config-subif)#ip address 10.130.200.2 255.255.255.248
R-BMANGA(config-subif)#interface GigabitEthernet0/0.10
R-BMANGA(config-subif)#ip helper-address 172.31.2.34
R-BMANGA(config-subif)#interface GigabitEthernet0/0.30
R-BMANGA(config-subif)#description VLAN30
R-BMANGA(config-subif)#encapsulation dot1Q 30
R-BMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
R-BMANGA(config-subif)#ip helper-address 172.31.2.34
R-BMANGA(config-subif)#ip helper-address 172.31.2.34
R-BMANGA(config-subif)#interface Serial0/0/0
R-BMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
R-BMANGA(config-if)#ip ospf authentication-key 7 08021D0A0A4
%OSPF: Warning: The password/key will be truncated to 8 characters
R-BMANGA(config-if)#interface Serial0/0/1
R-BMANGA(config-if)#
```

IMAGEN 58 CONFIGURACIÓN DIRECCIONAMIENTO IP ROUTER BUCARAMANGA

REALIZAMOS LA CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF CON AUTENTICACION EN EL ROUTER DE BUCARAMANGA.

R-BMANGA(config-subif)#router ospf 1
R-BMANGA(config-subif)# log-adjancency-changes
R-BMANGA(config-subif)# area 0 authentication
R-BMANGA(config-subif)# network 172.31.0.0 0.0.0.63 area 0
R-BMANGA(config-subif)# network 172.31.0.64 0.0.0.63 area 0
R-BMANGA(config-subif)# network 172.31.2.32 0.0.0.3 area 0
R-BMANGA(config-subif)# network 10.130.200.0 0.0.0.7 area 0

```
R-BMANGA(config-if)#router ospf 1
R-BMANGA(config-router)#log-adjacency-changes
R-BMANGA(config-router)#area 0 authentication
R-BMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
R-BMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
R-BMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
R-BMANGA(config-router)#network 10.130.200.0 0.0.0.7 area 0
R-BMANGA(config-router)#
```

IMAGEN 59 CONFIGURACIÓN PROTOCOLO OSPF ROUTER BUCARAMANGA

```
switch(config)#hostname SW-BAMANGA
SW-BAMANGA(config)#no ip domain-lookup
SW-BAMANGA(config)#enable secret class
SW-BAMANGA(config)#line console 0
SW-BAMANGA(config-line)#password cisco
SW-BAMANGA(config-line)#login
SW-BAMANGA(config-line)#exit
SW-BAMANGA(config)#line vty 0 15
SW-BAMANGA(config-line)#password cisco
SW-BAMANGA(config-line)#login
SW-BAMANGA(config-line)#service password-encryption
SW-BAMANGA(config)#banner motd "Acceso restringido"
```

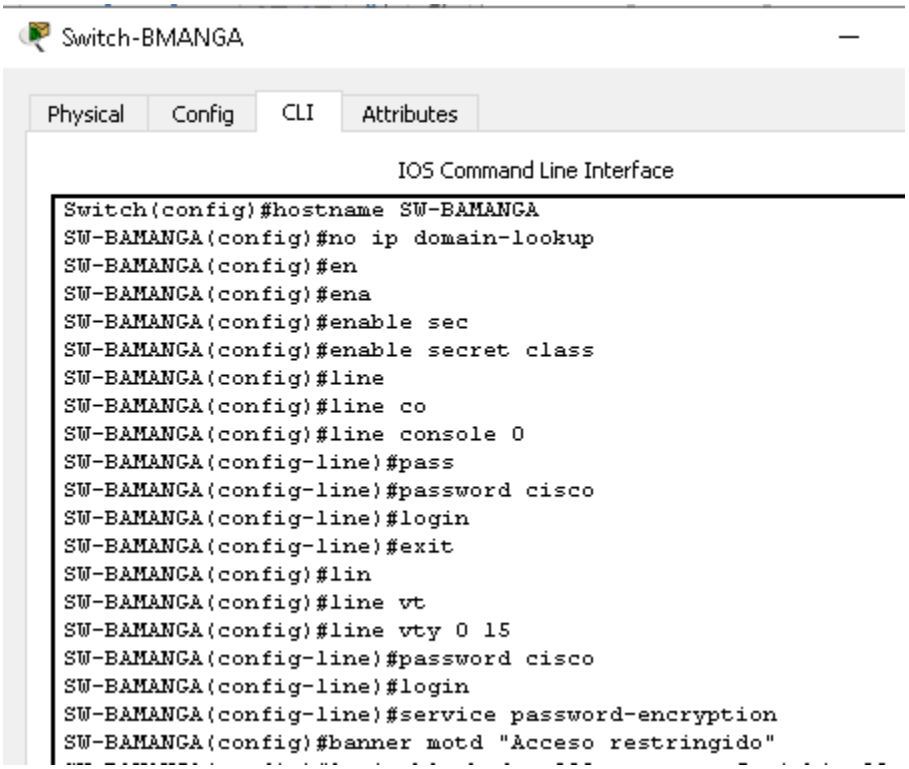

IMAGEN 60 CONFIGURACIÓN SEGURIDAD ACCESSO SWITCH BUCARAMANGA

DE ACUERDO AL ESCENARIO SE CONFIGURAN LAS VLAN EN EL SWITCH DE BUCARAMANGA, DE ACUERDO A LAS NECESIDADES INDICADAS, SE HABILITA EN TRAFICO ENTRE VLAN POR MEDIO DE TRONCALES.

```
SW-BAMANGA(config)#vlan 10
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config)# interface FastEthernet0/1
SW-BAMANGA(config-if)# description PC_VLAN10
SW-BAMANGA(config-if)# switchport access vlan 10
SW-BAMANGA(config-if)# switchport mode access
SW-BAMANGA(config-if)# interface FastEthernet0/2
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config)#vlan 30
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config-vlan)# description PC_VLAN30
SW-BAMANGA(config-if)# switchport access vlan 30
SW-BAMANGA(config-if)# switchport mode access
SW-BAMANGA(config-if)# interface FastEthernet0/3
SW-BAMANGA(config-if)# description PC_GESTION
SW-BAMANGA(config)#vlan 2
SW-BAMANGA(config-vlan)#exit

SW-BAMANGA(config-vlan)# switchport access vlan 2
SW-BAMANGA(config-if)# switchport mode access
SW-BAMANGA(config-if)# interface GigabitEthernet0/1
SW-BAMANGA(config-if)# description CX to RT_B/MANGA
SW-BAMANGA(config-if)# switchport trunk allowed vlan 2,10,30
SW-BAMANGA(config-if)# switchport mode trunk
SW-BAMANGA(config-vlan)# interface Vlan2
SW-BAMANGA(config-if)# ip address 10.130.200.1 255.255.255.248
SW-BAMANGA(config-if)#no shutdown
SW-BAMANGA(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

```
SW-BAMANGA(config)#interface FastEthernet0/1
SW-BAMANGA(config-if)#description PC_VLAN10
SW-BAMANGA(config-if)#VLAN10
                     ^
% Invalid input detected at '^' marker.

SW-BAMANGA(config-if)#exit
SW-BAMANGA(config)#VLAN 10
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config)#interface FastEthernet0/1
SW-BAMANGA(config-if)#switchport access vlan 10
SW-BAMANGA(config-if)#switchport mode access
SW-BAMANGA(config-if)#exit
SW-BAMANGA(config)#VLAN 30
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config)#interface FastEthernet0/2
SW-BAMANGA(config-if)#description PC_VLAN30
SW-BAMANGA(config-if)#switchport access vlan 30
SW-BAMANGA(config-if)#switchport mode access
SW-BAMANGA(config-if)#exit
SW-BAMANGA(config)#VLAN 2
SW-BAMANGA(config-vlan)#exit
SW-BAMANGA(config)#interface FastEthernet0/3
SW-BAMANGA(config-if)#description PC_GESTION
SW-BAMANGA(config-if)#switchport access vlan 2
SW-BAMANGA(config-if)#switchport mode access
SW-BAMANGA(config-if)#interface GigabitEthernet0/1
SW-BAMANGA(config-if)#description CX to RT_B/MANGA
SW-BAMANGA(config-if)#switchport trunk allowed vlan 2,10,30
SW-BAMANGA(config-if)#switchport mode trunk
SW-BAMANGA(config-if)#interface Vlan2
SW-BAMANGA(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

SW-BAMANGA(config-if)#interface Vlan2
```

IMAGEN 61 CONFIGURACIÓN DIRECCIONAMIENTO IP Y VLAN SWITCH BUCARAMANGA

SE CONFOGIURA LA VLAN 2 PARA ADMINSITRACIÓN DELSWITCH DE BUCARAMANGA Y SE ADICIONA EL GATEWAY.

SW-BAMANGA(config-if)#interface Vlan2
SW-BAMANGA(config-if)#exit
SW-BAMANGA(config)#ip default-gateway 10.130.200.2

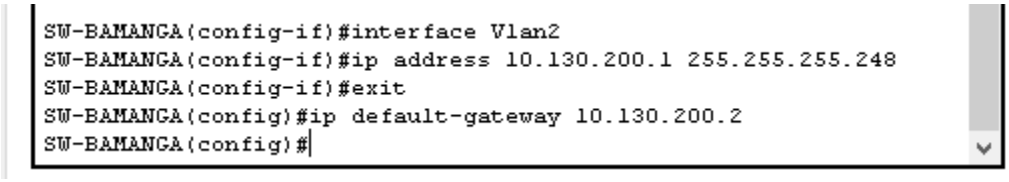

IMAGEN 62 CONFIGURACIÓN VLAN ADMINISTRACIÓN BUCARAMANGA

SE REALIZAN LAS CONFIGURACIONES BASICAS INDICADAS DE ACCESO Y SEGURIDAD EN EL ROUTER DE TUNJA.

Router2(config)#hostname R-TUNJA
R-TUNJA(config)#no ip domain-lookup
R-TUNJA(config)#enable secret class
R-TUNJA(config)#line console 0
R-TUNJA(config-line)#password cisco
R-TUNJA(config-line)#login
R-TUNJA(config-line)#exit
R-TUNJA(config)#lines v
R-TUNJA(config)#lines vt
R-TUNJA(config)#line vty 0 15
R-TUNJA(config-line)#password cisco
R-TUNJA(config-line)#login
R-TUNJA(config-line)#service password-encryption
R-TUNJA(config)#banner motd "Acceso restringido"
R-TUNJA(config)# login block-for 300 attempts 5 within 30

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R-TUNJA
R-TUNJA(config)#no ip domain-lookup
R-TUNJA(config)#en
R-TUNJA(config)#ena
R-TUNJA(config)#enable se
R-TUNJA(config)#enable secret class
R-TUNJA(config)#line console 0
R-TUNJA(config-line)#password cisco
R-TUNJA(config-line)#login
R-TUNJA(config-line)#line v
R-TUNJA(config-line)#exit
R-TUNJA(config)#line
R-TUNJA(config)#line v
R-TUNJA(config)#line vty 0 15
R-TUNJA(config-line)#password cisco
R-TUNJA(config-line)#login
R-TUNJA(config-line)#service password-encryption
R-TUNJA(config)#banner motd "Acceso restringido"
R-TUNJA(config)#login block-for 300 attempts 5 within 30
```

IMAGEN 63 CONFIGURACIÓN SEGURIDAD ACCESO ROUTER TUNJA

DE ACUERDO A LA TABLA DE DIRECCIONAMIENTO IP REALIZAMOS LA CONFIGURACION DE LAS INTERFACES DE RED EN EL ROUTER DE TUNJA, SE CONFIGURA NAT DE SOBRECARGA PAT, PARA EVITAR EL USO DE DIRECCIONES IP PUBLICAS EN LA RED INTERNA Y QUE SE REALICE LA TRADUCCION DE DIRECCIONES POR UNA SOLA IP Y PARA EL WEB SERVER NAT ESTATICO.

```
R-TUNJA (config)#interface gigabitEthernet 0/0.2
R-TUNJA (config-subif)#en
R-TUNJA (config-subif)#encapsulation do
R-TUNJA (config-subif)#encapsulation dot1Q 2
R-TUNJA (config-subif)#ip address 10.130.200.10 255.255.255.248
R-TUNJA (config-if)#interface gigabitEthernet 0/0.20
R-TUNJA (config-subif)# description VLAN20
R-TUNJA (config-subif)#encapsulation do
R-TUNJA (config-subif)#encapsulation dot1Q 20
R-TUNJA (config-subif)#ip address 172.31.0.129 255.255.255.192
R-TUNJA (config-subif)#ip access-group 103 in
R-TUNJA (config-subif)# ip nat inside
R-TUNJA (config-if)#interface gigabitEthernet 0/0.30
R-TUNJA (config-subif)# description VLAN30
R-TUNJA (config-subif)#encapsulation do
```

```
R-TUNJA (config-subif)#encapsulation dot1Q 30
R-TUNJA (config-subif)# ip address 172.31.0.193 255.255.255.192
R-TUNJA (config-subif)# ip access-group 102 in
R-TUNJA (config-subif)# ip nat inside
R-TUNJA (config-subif)# interface GigabitEthernet0/1
R-TUNJA (config-if)# ip address 209.17.220.1 255.255.255.0
R-TUNJA (config-if)# ip nat outside
R-TUNJA (config-if)# duplex auto
R-TUNJA (config-if)# speed auto
R-TUNJA (config-if)# interface Serial0/0/0
R-TUNJA (config-if)# ip address 172.31.2.34 255.255.255.252
R-TUNJA (config-if)# ip nat inside
R-TUNJA (config-if)# interface Serial0/0/1
R-TUNJA (config-if)# ip address 172.31.2.37 255.255.255.252
R-TUNJA (config-if)#ip nat inside
R-TUNJA (config-if)# router ospf 1
R-TUNJA (config-router)# log-adjacency-changes
R-TUNJA (config- router)# area 0 authentication
R-TUNJA (config- router)# network 172.31.0.128 0.0.0.63 area 0
R-TUNJA (config- router)# network 172.31.0.192 0.0.0.63 area 0
R-TUNJA (config- router)# network 172.31.2.32 0.0.0.3 area 0
R-TUNJA (config- router)# network 172.31.2.36 0.0.0.3 area 0
R-TUNJA (config- router)# network 209.17.220.0 0.0.0.255 area 0
R-TUNJA (config- router)# network 10.130.200.8 0.0.0.7 area 0
R-TUNJA (config- router)# ip nat inside source list 10 interface
GigabitEthernet0/1 overload
R-TUNJA (config- router)# ip nat inside source static 192.168.10.2
209.17.220.1
```

R-TUNJA (config- router)# ip classless

```
R-TUNJA(config-subif)#encapsulation dot1Q 20
R-TUNJA(config-subif)#
R-TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
R-TUNJA(config-subif)#ip access-group 103 in
R-TUNJA(config-subif)#ip nat inside
R-TUNJA(config-subif)#interface GigabitEthernet0/0.30
R-TUNJA(config-subif)#description VLAN30
R-TUNJA(config-subif)#encapsulation dot1Q 30
R-TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
R-TUNJA(config-subif)#ip access-group 102 in
R-TUNJA(config-subif)#ip nat inside
R-TUNJA(config-subif)#interface GigabitEthernet0/1
R-TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
R-TUNJA(config-if)#ip nat outside
R-TUNJA(config-if)#duplex auto
R-TUNJA(config-if)#speed auto
R-TUNJA(config-if)#interface Serial0/0/0
R-TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
R-TUNJA(config-if)#ip nat inside
R-TUNJA(config-if)#interface Serial0/0/1
R-TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
R-TUNJA(config-if)#ip nat inside
R-TUNJA(config-if)#router ospf 1
R-TUNJA(config-router)#log-adjacency-changes
R-TUNJA(config-router)#area 0 authentication
R-TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
R-TUNJA(config-router)# network 172.31.0.192 0.0.0.63 area 0
R-TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
R-TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R-TUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
R-TUNJA(config-router)#network 10.130.200.8 0.0.0.7 area 0
R-TUNJA(config-router)#
```

IMAGEN 64 CONFIGURACIÓN DIRECCIONAMIENTO ROUTER TUNKJA CON NAT Y OSPF

SE CONFIGURA EL DCHP POOL EN ROUTER DE TUNJA DE ACUERDO A LAS INDICACIONES DEL ESCANARIO USABDO LAS VLAN INDICADAS UNICAMEN ASIGNARA IP PARA LOS EQUIPOS DE LA RED DE BUCARAMANGA Y CUNDINAMARCA.

R-TUNJA (config)# ip dhcp pool VLAN10-B/MANGA
R-TUNJA (dhcp-config)# network 172.31.0.0 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.0.1
R-TUNJA (dhcp-config)# ip dhcp pool VLAN30-B/MANGA
R-TUNJA (dhcp-config)# network 172.31.0.64 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.0.65
R-TUNJA (dhcp-config)# ip dhcp pool VLAN10-C/MARCA
R-TUNJA (dhcp-config)# network 172.31.1.0 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.1.1
R-TUNJA (dhcp-config)# ip dhcp pool VLAN20-C/MARCA
R-TUNJA (dhcp-config)# network 172.31.1.64 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.1.65

R-TUNJA (dhcp-config)# ip dhcp pool VLAN20-TUNJA
R-TUNJA (dhcp-config)# network 172.31.0.128 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.0.129
R-TUNJA (dhcp-config)# ip dhcp pool VLAN30-TUNJA
R-TUNJA (dhcp-config)# network 172.31.0.192 255.255.255.192
R-TUNJA (dhcp-config)# default-router 172.31.0.193

```
R-TUNJA(config)#ip dhcp pool VLAN10-B/MANGA
R-TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
R-TUNJA(dhcp-config)#default-router 172.31.0.1
R-TUNJA(dhcp-config)#ip dhcp pool VLAN30-B/MANGA
R-TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
R-TUNJA(dhcp-config)#default-router 172.31.0.65
R-TUNJA(dhcp-config)#ip dhcp pool VLAN10-C/MARCA
R-TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
R-TUNJA(dhcp-config)#default-router 172.31.1.1
R-TUNJA(dhcp-config)#ip dhcp pool VLAN20-C/MARCA
R-TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
```

IMAGEN 65 CONFIGURACIÓN DHCP POOL ROUTER TUNJA

SE CONFIGURAN LAS ACL DE ACUERDO A LAS INDICACIONES DEL ESCENARIO 2, EN EL ROUTER DE TUNJA , LOS EQUIPOS DE LA VLAN 20 EN TUNJA SOLO ACCEDEN A LA VLAN 20 DE CUNDINAMARCA Y A LA VLAN 10 DE BUCARAMANGA, LOS HOST DE LA VLAN 30 DE TUNJA SOLO ACCEDEN A SERVIDORES WEB Y FTP DE INTERNET.

R-TUNJA (config)#access-list 102 permit ip 172.31.0.192 0.0.0.63 host 209.17.220.100
R-TUNJA (config)# access-list 102 deny ip any any
R-TUNJA (config)# access-list 103 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
R-TUNJA (config)# access-list 103 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
R-TUNJA (config)# access-list 103 deny ip any any

```
R-TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R-TUNJA(config)#access-list 102 permit ip 172.31.0.192 0.0.0.63 host 209.17.220.100
R-TUNJA(config)#access-list 102 deny ip any any
R-TUNJA(config)#access-list 103 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
R-TUNJA(config)#access-list 103 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
R-TUNJA(config)#access-list 103 deny ip any any
R-TUNJA(config)#
```

IMAGEN 66 CONFIGURACIÓN ACL ROUTER TUNJA

SE CONFIGURA EL SWITCH DE TUNJA CON LOS PARAMETROS BASICO DE SEGURIDAD Y DE ACCESO, DE ACUERDO A LO SOLICITADO EN EL ESCENARIO 2.

Switch(config)# hostname SW-TUNJA
SW-TUNJA(config-subif)# no ip domain-lookup
SW-TUNJA(config-subif)#enable secret class
SW-TUNJA(config-subif)#line console 0
SW-TUNJA(config-line)# password cisco
SW-TUNJA(config-line)#login
SW-TUNJA(config-line)#exit
SW-TUNJA(config)#line vty 0 15
SW-TUNJA(config-line)# password cisco
SW-TUNJA(config-line)#login
SW-TUNJA(config-line)# service password-encryption
SW-TUNJA(config-line)# banner motd "Acceso restringido"

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-TUNJA
SW-TUNJA(config)#no ip domain-lookup
SW-TUNJA(config)#enable secret class
SW-TUNJA(config)#line console 0
SW-TUNJA(config-line)#password cisco
SW-TUNJA(config-line)#login
SW-TUNJA(config-line)#exit
SW-TUNJA(config)#line
SW-TUNJA(config)#line vt
SW-TUNJA(config)#line vty 0 15
SW-TUNJA(config-line)#password cisco
SW-TUNJA(config-line)#login
SW-TUNJA(config-line)#service password-encryption
SW-TUNJA(config)#banner motd "Acceso restringido"
```

IMAGEN 67 CONFIGURACIÓN SEGURIDAD ACCESO SWITCH TUNJA

SE CONFIGURA EL DIRECCIONAMIENTO IP, VLAN DE ACUERDO AL ESCENARIO 2, SE UTILIZA RUTEO ENTRE VLAN SWITCH TUNJA

SW-TUNJA(config-)# interface FastEthernet0/1
SW-TUNJA(config-subif)#exit
SW-TUNJA(config-)#vlan 20
SW-TUNJA(config-vlan)#exit

```
SW-TUNJA(config)# vlan 20
SW-TUNJA(config-vlan)#exit
SW-TUNJA(config)# interface FastEthernet0/1
SW-TUNJA(config-if)# witchport access vlan 20
SW-TUNJA(config-if)# switchport mode access
SW-TUNJA(config-if)# interface FastEthernet0/2
SW-TUNJA(config-if)# switchport access vlan 30
SW-TUNJA(config-if)# switchport mode access
SW-TUNJA(config-if)#exit
SW-TUNJA(config)#vlan 2
SW-TUNJA(config-vlan)#exit
SW-TUNJA(config-if)# interface FastEthernet0/3
SW-TUNJA(config-if)# description PC_GESTION
SW-TUNJA(config-if)# switchport access vlan 2
SW-TUNJA(config-if)# switchport mode access
SW-TUNJA(config-if)# interface GigabitEthernet0/1
SW-TUNJA(config-if)# description CX to RT_TUNJA
SW-TUNJA(config-if)# switchport trunk allowed vlan 2,20,30
SW-TUNJA(config-if)# switchport mode trunk
SW-TUNJA(config-if)# interface Vlan2
SW-TUNJA(config-vlan)# ip address 10.130.200.9 255.255.255.248
SW-TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

```
SW-TUNJA(config)#interface FastEthernet0/1
SW-TUNJA(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-TUNJA(config-if)#exit
SW-TUNJA(config)#vlan 20
SW-TUNJA(config-vlan)#exit
SW-TUNJA(config)#vlan 30
SW-TUNJA(config-vlan)#interface FastEthernet0/1
SW-TUNJA(config-if)#switchport access vlan 20
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#interface FastEthernet0/2
SW-TUNJA(config-if)#switchport access vlan 30
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#interface FastEthernet0/3
SW-TUNJA(config-if)#description PC_GESTION
SW-TUNJA(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
SW-TUNJA(config-if)#exit
SW-TUNJA(config)#vlan 2
SW-TUNJA(config-vlan)#interface FastEthernet0/3
SW-TUNJA(config-if)#switchport access vlan 2
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#interface GigabitEthernet0/1
SW-TUNJA(config-if)#description CX to RT_TUNJA
SW-TUNJA(config-if)#switchport trunk allowed vlan 2,20,30
SW-TUNJA(config-if)#switchport mode trunk
SW-TUNJA(config-if)#interface Vlan2
SW-TUNJA(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

IMAGEN 68 CONFIGURACIÓN DIRECCIONAMIENTO IP Y VLAN SWITCH TUNJA

SE CONFIGURA EL GATEWAY EN EL SWITCH DE TUNJA.

SW-TUNJA(config-if)# ip default-gateway 10.130.200.10

```
SW-TUNJA(config-if)#ip address 10.130.200.9 255.255.255.248
SW-TUNJA(config-if)#exit
SW-TUNJA(config)#ip default-gateway 10.130.200.10
SW-TUNJA(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

IMAGEN 69 CONFIGURACIÓN DEFAULT GATEWAY SWITCH TUNJA

SE CREA LA VLAN 2 PARA GESTION, EN EL SWITCH DE INTERNET

SW-INTERNET(config-if)# interface Vlan2
SW- INTERNET (config-if)# ip address 200.17.220.2 255.255.255.0
SW- INTERNET (config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan2, changed state to up

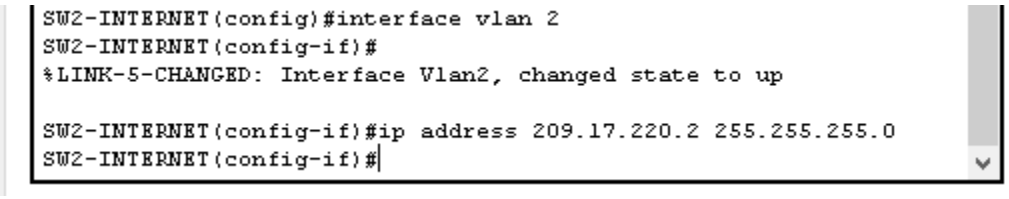

IMAGEN 70 CONFIGURACIÓN VLAN ADMINISTRACIÓN TUNJA

SE CONFIGUTA DIRECCIONAMIENTO NAT TIPO PAT EN EL WEB SERVER EXTERNO DE LA RED DE TUNJA, USANDO PARA ELLO IP PUBLICA.

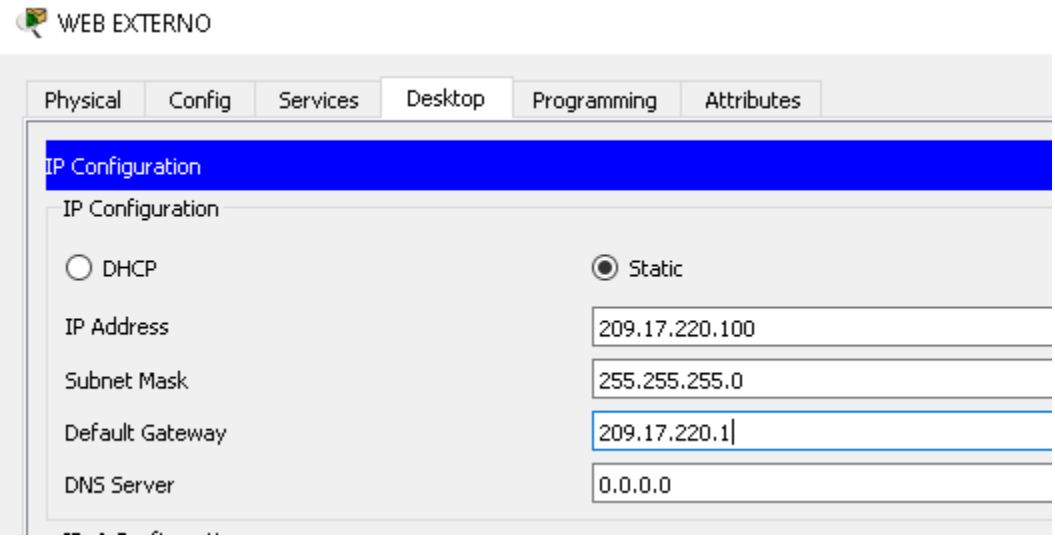

IMAGEN 71 CONFIGURACIÓN IP WEB SERVER EXTERNO

SE CONFIGURA LOS PARAMETROS BASICO Y DE SEGURIDAD DE ACUERDO A LO INDICADO EN EL ESCENARIO EN EL ROUTER DE CUNDINAMARCA.

Router3(config)#hostname R-CNMARCA
R-CNMARCA(config)#no ip domain-lookup
R-CNMARCA(config)#enable secret class
R-CNMARCA(config)#line console 0
R-CNMARCAconfig-line)#login
R-CNMARCA(config-line)#exit
R-CNMARCA(config)#lines v
R-CNMARCA(config)#lines vt
R-CNMARCA(config)#line vty 0 15
R-CNMARCA(config-line)#password cisco
R-CNMARCA(config-line)#login
R-CNMARCA(config-line)#service password-encryption
R-CNMARCA(config)#banner motd "Acceso restringido"
R-CNMARCA(config)# login block-for 300 attempts 5 within 30

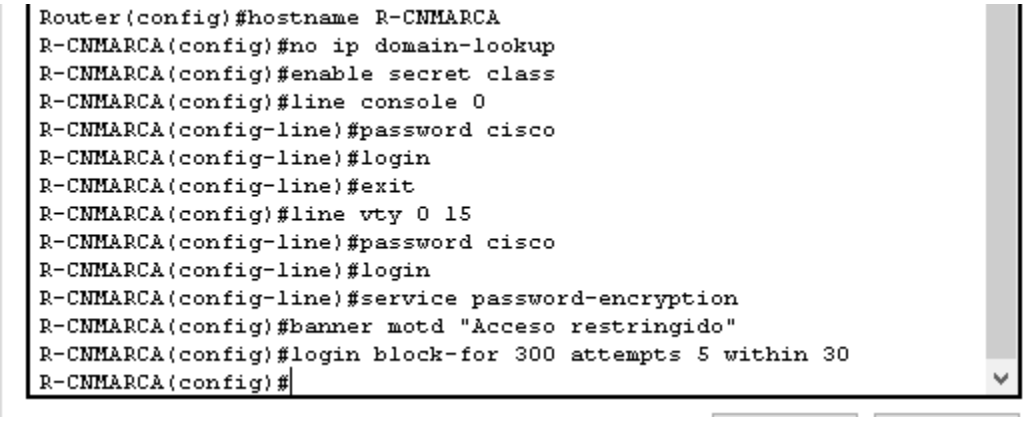

IMAGEN 72 CONFIGURACIÓN SEGURIDAD ACCESO ROUTER CUNDINAMARCA

SE CONFIGURAN EL DIRECCIONAMIENTO IP EN LAS INTERFACES, EN EL ROUTER DE CUNDINAMARCA, ADICIONAL SE CONFIGURA EL USO DE DHCP CON IPHELPER.

R- CNMARCA(config)#interface gigabitEthernet 0/0.2
R- CNMARCA(config-subif)#en
R- CNMARCA(config-subif)#encapsulation do
R- CNMARCA(config-subif)#encapsulation dot1Q 2
R- CNMARCA(config-subif)#ip address 10.130.200.17 255.255.255.248
R- CNMARCA(config-if)#interface gigabitEthernet 0/0.10
R- CNMARCA(config-subif)# description VLAN20
R- CNMARCA(config-subif)#encapsulation do
R- CNMARCA(config-subif)#encapsulation dot1Q 10
R- CNMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
R- CNMARCA(config-subif)#ip access-group 101 in
R- CNMARCA(config-if)#interface gigabitEthernet 0/0.20
R- CNMARCA(config-subif)# description VLAN20
R- CNMARCA(config-subif)#encapsulation do
R- CNMARCA(config-subif)#encapsulation dot1Q 20
R- CNMARCA(config-subif)# ip address 172.31.65. 255.255.255.192
R- CNMARCA(config-subif)# ip helper-address 172.31.2.37
R- CNMARCA(config-subif)# ip access-group 100 in
R- CNMARCA(config-if)#interface gigabitEthernet 0/0.30
R- CNMARCA(config-subif)# description VLAN30
R- CNMARCA(config-subif)#encapsulation do
R- CNMARCA(config-subif)#encapsulation dot1Q 30
R- CNMARCA(config-subif)# ip address 192.168.10.1 255.255.255.0
R- CNMARCA(config-if)# interface Serial0/0/0
R- CNMARCA(config-if)# ip address 172.31.2.38 255.255.255.252

```
R-CNMARCA(config)#interface GigabitEthernet0/0.2
R-CNMARCA(config-subif)#encapsulation dot1Q 2
R-CNMARCA(config-subif)#ip address 10.130.200.17 255.255.255.248
R-CNMARCA(config-subif)#interface GigabitEthernet0/0.10
R-CNMARCA(config-subif)#description VLAN10
R-CNMARCA(config-subif)#encapsulation dot1Q 10
R-CNMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
R-CNMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
R-CNMARCA(config-subif)#ip access-group 101 in
R-CNMARCA(config-subif)#interface GigabitEthernet0/0.20
R-CNMARCA(config-subif)#description VLAN20
R-CNMARCA(config-subif)#encapsulation dot1Q 20
R-CNMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
R-CNMARCA(config-subif)#ip helper-address 172.31.2.37
R-CNMARCA(config-subif)#ip access-group 100 in
R-CNMARCA(config-subif)#interface GigabitEthernet0/0.30
R-CNMARCA(config-subif)#encapsulation dot1Q 30
R-CNMARCA(config-subif)#ip address 192.168.10.1 255.255.255.0
R-CNMARCA(config-subif)#interface Serial0/0/0
R-CNMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
R-CNMARCA(config-if)#ip ospf authentication-key 7 08021D0A0A49
%OSPF: Warning: The password/key will be truncated to 8 characters
R-CNMARCA(config-if)#interface Serial0/0/1
R-CNMARCA(config-if)#
```

IMAGEN 73 CONFIGURACIÓN DIRECCIONAMIENTO IP ROUTER CUNDINAMARCA CON VLAN

SE CONFIGURA EL PROTOCOLO DE ENRUTAMIENTO OSFP CON AUTENTICACION EN EL ROUTER DE CUNDINAMARCA.

R- CNMARCA(config-if)# router ospf 1
R- CNMARCA(config-router)# log-adjacency-changes
R- CNMARCA(config- router)# area 0 authentication
R- CNMARCA(config- router)# network 172.31.2.36 0.0.0.3 area 0
R- CNMARCA(config- router)# network 172.31.1.0 0.0.0.63 area 0
R- CNMARCA(config- router)# network 172.31.1.64 0.0.0.63 area 0
R- CNMARCA(config- router)# network 192.168.10.0 0.0.0.255 area 0
R- CNMARCA(config- router network 10.130.200.16 0.0.0.7 area 0

```
R-CNMARCA(config)#router ospf 1
R-CNMARCA(config-router)#log-adjacency-changes
R-CNMARCA(config-router)#area 0 authentication
R-CNMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
R-CNMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
R-CNMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
R-CNMARCA(config-router)#network 192.168.10.0 0.0.0.255 area 0
R-CNMARCA(config-router)#network 10.130.200.16 0.0.0.7 area 0
R-CNMARCA(config-router)#
```

IMAGEN 74 CONFIGURACIÓN PROTOCOLO OSFP ROUTER CUNDINAMARCA

SE CONFIGURAN ALAS ACL, DE ACUERDO A ESPECIFICACIONES DEL ESCENARIO 2 EN EL ROUTER DE CUNDINAMARCA, LA VLAN 20 NO ACCEDE A INTERNET SOLO A LA RED INTERNA DE TUNJA, LA VLAN 10 DE CUNDINAMARCA ACCEDE A INERNET Y NO A LA RED INTERNA DE TUNJA

```
R-CNMARCA(config-router)#network 10.130.200.16 0.0.0.7 area 0
R-CNMARCA(config-router)#access-list 100 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
R-CNMARCA(config)#access-list 100 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
R-CNMARCA(config)#access-list 100 deny ip any any
R-CNMARCA(config)#access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
R-CNMARCA(config)#access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
R-CNMARCA(config)#access-list 101 permit ip any any
R-CNMARCA(config)#
```

IMAGEN 75 CONFIGURACIÓN ACL ROUTER CUNDINAMARCA

SE CONFIGURAN LOS PARAMETROS DE ACCESO Y SEGURIDAD BASICOS DEL SWITCH DE CUNDINAMARCA.

Switch(config)# hostname SW-CUNMARCA
SW-CUNMARCA(config-subif)# no ip domain-lookup
SW-CUNMARCA(config-subif)#enable secret class
SW-CUNMARCA(config-subif)#line console 0
SW-CUNMARCA(config-line)# password cisco
SW-CUNMARCA(config-line)#login
SW-CUNMARCA(config-line)#exit
SW-CUNMARCA(config)#line vty 0 15
SW-CUNMARCA(config-line)# password cisco
SW-CUNMARCA(config-line)#login
SW-CUNMARCA(config-line)# service password-encryption
SW-CUNMARCA(config-line)# banner motd “Acceso restringido”

```
SW-CUNMARCA(config)#no ip domain-lookup
SW-CUNMARCA(config)#enable secret class
SW-CUNMARCA(config)#line console 0
SW-CUNMARCA(config-line)#password cisco
SW-CUNMARCA(config-line)#exit
SW-CUNMARCA(config)#line vty 0 15
SW-CUNMARCA(config-line)#password cisco
SW-CUNMARCA(config-line)#login
SW-CUNMARCA(config-line)#exit
SW-CUNMARCA(config)#line console 0
SW-CUNMARCA(config-line)#login
SW-CUNMARCA(config-line)#service password-encryption
SW-CUNMARCA(config)#banner motd "Acceso restringido"
SW-CUNMARCA(config)#
```

IMAGEN 76 CONFIGURACIÓN SEGURIDAD ACCESO SWITCH CUNDINAMARCA

SE CONFIGURAN LAS VLAN EN EL SWITCH DE CUNDINAMARCA, DE ACUERDO A LOS REQUERIMIENTOS DEL ESCENARIO 2, SE CONFIGURA EL ENRUTAMIENTO ENTRE VLAN, SE CREA LA VLAN 2 PARA GESTION, SE CONFIGURA EL GATEWAY.

SW-CUNMARCA(config)# vlan 10
SW-CUNMARCA(config-vlan)#vlan 20
SW-CUNMARCA(config-vlan)#vlan 30
SW-CUNMARCA(config-vlan)# vlan 2
SW-CUNMARCA(config-vlan)# interface FastEthernet0/1
SW-CUNMARCA(config-if)# switchport access vlan 10
SW-CUNMARCA(config-if)# switchport mode access
SW-CUNMARCA(config-if)# interface FastEthernet0/2
SW-CUNMARCA(config-if)# witchport access vlan 20
SW-CUNMARCA(config-if)# switchport mode access
SW-CUNMARCA(config-if)# interface FastEthernet0/3
SW-CUNMARCA(config-if)# witchport access vlan 30
SW-CUNMARCA(config-if)# switchport mode access
SW-CUNMARCA(config-if)# interface FastEthernet0/4
SW-CUNMARCA(config-if)# description PC_GESTION
SW-CUNMARCA(config-if)# switchport access vlan 2
SW-CUNMARCA(config-if)# switchport mode access
SW-CUNMARCA(config-if)# interface GigabitEthernet0/1
SW-CUNMARCA(config-if)# description CX to RT_C/MARCA
SW-CUNMARCA(config-if)# switchport trunk allowed vlan 2,10,20,30
SW-CUNMARCA(config-if)# switchport mode trunk
SW-CUNMARCA(config-if)# interface Vlan2
SW-CUNMARCA(config-vlan)# ip address 10.130.200.18 255.255.255.248

SW-CUNMARCA(config-if)#no shutdown
%LINK-5-CHANGD: Interface Vlan2, changed state to up
SW-CUNMARCA(config)#ip default gateway 10.130.200.7

```
SW-CUNMARCA(config)#vlan 10
SW-CUNMARCA(config-vlan)#vlan 20
SW-CUNMARCA(config-vlan)#vlan 30
SW-CUNMARCA(config-vlan)#vlan 2
SW-CUNMARCA(config-vlan)#interface FastEthernet0/1
SW-CUNMARCA(config-if)#switchport access vlan 10
SW-CUNMARCA(config-if)#switchport mode access
SW-CUNMARCA(config-if)#interface FastEthernet0/2
SW-CUNMARCA(config-if)#switchport access vlan 20
SW-CUNMARCA(config-if)#switchport mode access
SW-CUNMARCA(config-if)#interface FastEthernet0/3
SW-CUNMARCA(config-if)#switchport access vlan 30
SW-CUNMARCA(config-if)#switchport mode access
SW-CUNMARCA(config-if)#interface FastEthernet0/4
SW-CUNMARCA(config-if)#description PC_GESTION
SW-CUNMARCA(config-if)#switchport access vlan 2
SW-CUNMARCA(config-if)#switchport mode access
SW-CUNMARCA(config-if)#interface GigabitEthernet0/1
SW-CUNMARCA(config-if)#description CX to RT_C/MARCA
SW-CUNMARCA(config-if)#switchport trunk allowed vlan 2,10,20,30
SW-CUNMARCA(config-if)#switchport mode trunk
SW-CUNMARCA(config-if)#interface Vlan2
SW-CUNMARCA(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

SW-CUNMARCA(config-if)#ip address 10.130.200.18 255.255.255.248
SW-CUNMARCA(config-if)#exit
SW-CUNMARCA(config)#ip default-gateway 10.130.200.17
SW-CUNMARCA(config)#
```

IMAGEN 77 CONFIGURACIÓN DIRECCIONAMIENTO IP Y VLAN SWITCH CUNDINAMARCA

SE CONFIGURA EL SERVIDOR DE AUTENTICACION AAA EN EL ROUTER DE CUNDINAMARCA.

```
R-CNMARCA(config)#aaa new-model
R-CNMARCA(config)#aa
R-CNMARCA(config)#aaa authe
R-CNMARCA(config)#aaa authentication mo
R-CNMARCA(config)#aaa authentication lo
R-CNMARCA(config)#aaa authentication login de
R-CNMARCA(config)#aaa authentication login default gr
R-CNMARCA(config)#aaa authentication login default group t
R-CNMARCA(config)#aaa authentication login default group tacacs+
R-CNMARCA(config)#
R-CNMARCA(config)#ta
R-CNMARCA(config)#tacacs-server hos
R-CNMARCA(config)#tacacs-server host 192.168.10.2 KEY class
```

IMAGEN 78 CONFIGURACIÓN SERVIDOR AUTENTICACION AAA

SE CONFIGURA EN EL SERVIDOR WEB INTERNO EL SERVICIO DE AUTENTICACION AAA, SE CREA EL CLIENTE, EL KEY, SE CREA UN USUARIO PARA PRUEBAS.

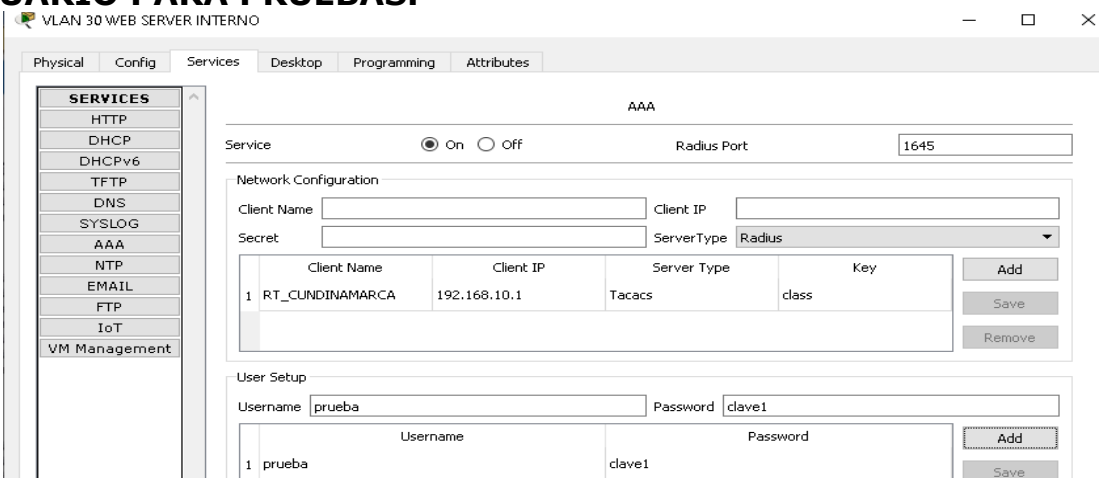

IMAGEN 79 CONFIGURACIÓN SERVIDOR WEB AUTENTICACIÓN AAA

SE CONFIGURA EL SERVIDOR DE AUTENTICACION AAA EN EL ROUTER DE TUNJA.

```
Enter configuration commands, one per line. End with CNTL/Z.
R-TUNJA(config)#aaa new-model
R-TUNJA(config)#aaa authentication login default group tacacs+
R-TUNJA(config)#tacacs-server host 192.168.10.2 key class
R-TUNJA(config)#
```

```
Username:
Username: prueba
Password:
R-TUNAJA>
```

IMAGEN 80 VERIFICACIÓN ACCESO CON AUTENTICACIÓN AAA ROUTER TUNJA

SE CONFIGURA EL SERVIDOR DE AUTENTICACION AAA EN EL ROUTER DE BUCARAMANGA.

R-BMANGA(config)#aaa new-model
R-BMANGA(config)#aaa authentication login default group tacacs+
R-BMANGA(config)#aaa authentication login default group tacacs+
R-BMANGA(config)# tacacs-server host 192.168.10.2 key class

IMAGEN 81 CONFIGURACIÓN ACCESO CON AUTENTICACIÓN AAA ROUTER BUCARAMANGA

SE REALIZA LA COPIA DE LOS ARCHIVOS DE CONFIGURACIÓN AL SERVIDOR TFTP MAS CERCA DEL ROUTER DE BUCARAMANGA.

SW-BAMANGA#copy running-config tftp
Address or name of remote host []? 209.17.220.100
Destination filename [SW-BAMANGA-confg]?

Writing running-config....!!
[OK - 1698 bytes]

1698 bytes copied in 3.092 secs (549 bytes/sec)
SW-BAMANGA#

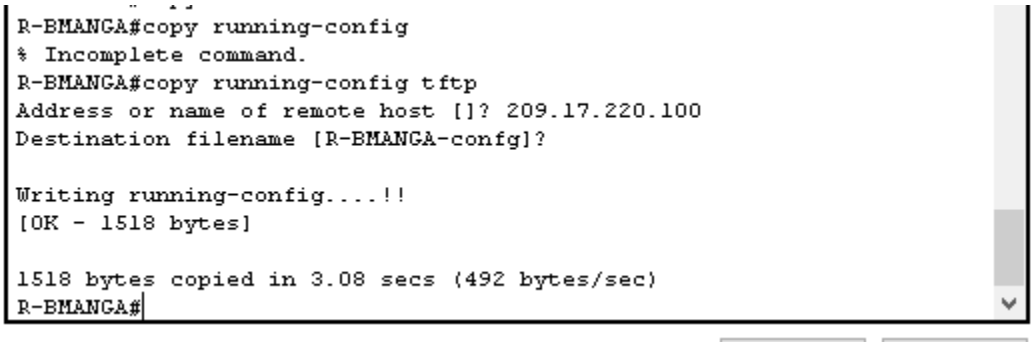

IMAGEN 82 COPIA DE ARCHISO DE SYSTEMA ROUTER BUCARAMANGA POR TFTP

SE REALIZA LA COPIA DE LOS ARCHIVOS DE CONFIGURACIÓN AL SERVIDOR TFTP MAS CERCA DEL ROUTER DE TUNJA.

R-TUNJA#copy running-config tftp
Address or name of remote host []? 192.168.10.2
Destination filename [R-TUNJA-confg]?

Writing running-config....!!
[OK - 2812 bytes]

2812 bytes copied in 3.125 secs (899 bytes/sec)
R-TUNJA#

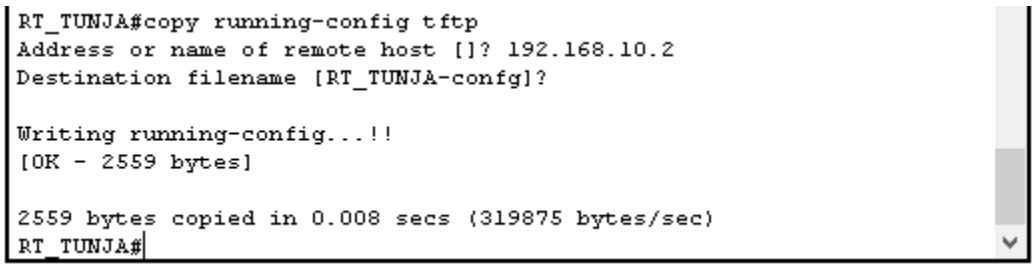

IMAGEN 83 COPIA ARCHISO SYSTEMA TFTP ROUTER TUNJA

SE REALIZA LA COPIA DE LOS ARCHIVOS DE CONFIGURACIÓN AL SERVIDOR TFTP MAS CERCA DEL ROUTER DE CUNDINAMARCA.

R-CNMARCA#copy running-config tftp
Address or name of remote host []? 209.17.220.100
Destination filename [R-CNMARCA-confg]?

Writing running-config...!!
[OK - 2264 bytes]

2264 bytes copied in 0.001 secs (2264000 bytes/sec)
R-CNMARCA#

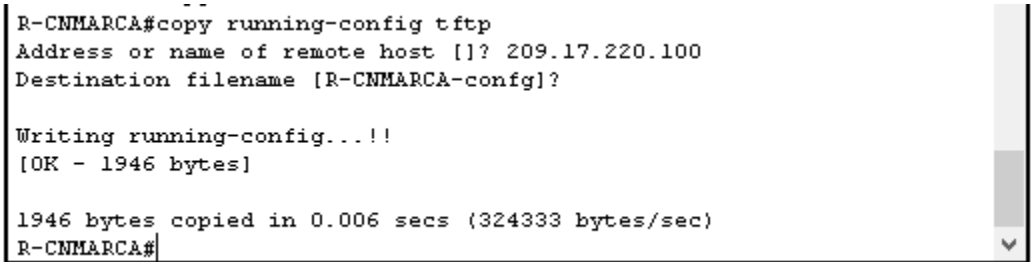

IMAGEN 84 COPIA ARCHISO SYSTEMA TFTP ROUTER CUNDINAMARCA

CONCLUSIONES.

Con este diplomado en CISCO, vimos los conceptos básicos de redes, así como conceptos avanzados en redes de comunicación tanto LAN como WAN, esto nos ayudará como profesionales en el diseño, implementación, soporte y solución de problema relacionados con redes locales LAN y de área extensa WAN.

Este diplomado se trabajó con base en la tecnología cisco, usando para ello el simulador de escenarios CISCO PACKET TRACERT y los laboratorios de CISCO NETLAB, lo que nos ayudó a poner en práctica los conocimientos que se fueron adquiriendo a través del desarrollo de cada Unidad correspondiente al diplomado en referencia, luego con ello pudimos diseñar los escenarios virtuales y solucionar los ejercicios planteados en cada parte de estas unidades, así como la aplicación de laboratorios de los diferentes temas vistos durante este diplomado.

Lo anterior me permitió adquirir los conocimientos necesarios, en el soporte y configuración de redes LAN y WAN, usando para ello equipos CISCO, esto es suma mente importante puesto que uno de los principales métodos de conexión para las comunicaciones, es el uso de estas redes, y los equipos CISCO, en el mundo de hoy día la tecnología sigue creciendo y avanzado a pasos agigantados, para que esto haya sido posible se ha utilizado las comunicaciones, para poder difundir estos conocimiento tecnológico a la humanidad, de manera confiable y rápida.

Las comunicaciones se han vuelta el pan de cada día, y con ellas podemos comunicarnos con nuestros seres queridos, compañeros de oficina, amigos, etc., desde cualquier parte del mundo y en tiempo real, esto hace que este diplomado de CISCO clave en nuestro futuro como profesionales, al ver la importancia de diseñar, implementar y soportar las comunicaciones de manera adecuada, con equipos de alto desempeño, que hacen que el mundo de hoy esta permanente mente comunicado.

REFERENCIAS

CISCO SYSTEM. (2017). Capítulo 1. Introducción a redes conmutadas. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#1.0.1.1

CISCO SYSTEM. (2017). Capítulo 2. Configuración y conceptos básicos de switching. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#2.0.1.1

CISCO SYSTEM. (2017). Capítulo 3. VLAN. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#3.0.1.1

CISCO SYSTEM. (2017). Capítulo 4. Conceptos de routing. Recuperado dehttps://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#4.0.1.1

CISCO SYSTEM. (2017). Capítulo 5. Enrutamiento entre VLAN. Recuperado dehttps://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#5.0.1.1

UNAD (2018). Comandos del IOS de CISCO para configurar Switch con el laboratorio remoto Smartlab [OVI]. Recuperado de http://hdl.handle.net/10596/21714