

Prueba de habilidades prácticas CCNA

Diplomado de profundización CISCO
(Diseño e implementación de soluciones integradas LAN
/ WAN)

Laura Yiset Vivas Hurtado

Universidad Nacional Abierta a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería

Programa de Ingeniería de Sistemas
Diplomado de Profundización CISCO

Santiago de Cali

Diciembre de 2019

Prueba de habilidades prácticas CCNA

Diplomado de profundización CISCO
(Diseño e implementación de soluciones integradas LAN
/ WAN)

Laura Yiset Vivas Hurtado

Universidad Nacional Abierta a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería

Programa de Ingeniería de Sistemas
Diplomado de Profundización CISCO

Santiago de Cali

Diciembre de 2019

CONTENIDO

Tabla de contenido

INTRODUCCIÓN	10
1. OBJETIVOS	11
1.1. Objetivo General.....	11
1.2. Objetivos Específicos.....	11
2. DESARROLLO DE LOS ESCENARIOS	12
2.1. Escenario 1	12
2.1.1. Parte 1: Asignación De Direcciones IP.....	12
2.1.2. Parte 2: Configuración Básica	20
2.1.3. Parte 3: Configuración De Enrutamiento	32
2.1.4. Parte 4: Configuración De Las Listas De Control De Acceso ..	36
2.1.5. Parte 5: Comprobación De La Red Instalada	41
2.2. Escenario 2	44
2.2.1. Configuración De Equipos.....	45
2.2.2. DHCP	49
2.2.3. NAT Estático Y NAT De Sobrecarga (PAT).....	50
2.2.4. El Enrutamiento Con Autenticación	50
2.2.5. Listas De Control De Acceso.....	51
2.2.6. VLSM.....	52
3. CONCLUSIONES	53
4. BIBLIOGRAFÍA	54

LISTA DE TABLAS

- Tabla 1. Tabla de redes y SubRedes.
Tabla 2. Asignación de los parámetros básicos y la detección de vecinos.
Tabla 3. Comprobación total de los dispositivos y su funcionamiento en la red.
Tabla 4. VLSM (Direccionamientos).

LISTA DE FIGURAS

- Figura 1. Escenario 1 Cada de host en la red.
Figura 2. Escenario 1 topología de la red.
Figura 3. Conexión física de la topología.
Figura 4. Topología de la Red.
Figura 5. Configuración del Equipo Lan de Medellín
Figura 6. Configuración del Equipo WS 1
Figura 7. Configuración del Servidor
Figura 8. Configuración del Equipo Lan de Cali
Figura 9. Diagnósticos de vecinos de Router Bogotá
Figura 10. Diagnósticos de vecinos de Router Medellín
Figura 11. Diagnósticos de vecinos de Router Cali
Figura 12. Ping del tramo de la ruta del Router de Medellín
Figura 13. Ping del tramo de la ruta del Router de Bogotá con WS 1
Figura 14. Ping del tramo de la ruta del Router de Bogotá con servidor
Figura 15. Ping del tramo de la ruta del Router de Cali
Figura 16. Ping de la Lan de Medellín al Router de Medellín y Bogotá
Figura 16: Ping de WS1 al servidor, router de Bogotá y Cali
Figura 17. Pin del servidor a la Lan de Bogotá y el router.
Figura 18. Ping de la Lan de Cali a router de Cali.
Figura 19. Ping de la Lan de Medellín a la Lan de Cali y el servidor.
Figura 20. Ping del WS 1 al router de Medellín y Cali
Figura 21. Vecindad Eigrp del Router Bogotá
Figura 22. Vecindad Eigrp del Router Medellín
Figura 23. Vecindad Eigrp del Router Cali
Figura 24. Tabla de enrutamiento Bogotá
Figura 25. Tabla de enrutamiento Medellín.
Figura 26. Tabla de enrutamiento Cali.
Figura 27. Prueba de conectividad de los puntos de red entre sí.
Figura 28. Habilitar el Router de Medellín para establecer conexiones Telnet.
Figura 29. Ingreso desde el router Bogotá al de Medellín por telnet.
Figura 30. Ingreso desde el router Cali al de Medellín por telnet.
Figura 31. Ingreso desde el router Medellín al de Bogotá por telnet.
Figura 32. Ingreso desde el router Cali al de Bogotá por telnet.
Figura 33. Ingreso desde el router Bogotá al de Cali por telnet.
Figura 34. Ingreso desde el router Medellín al de Cali por telnet.

- Figura 35. Ping de WS 1 al router de Bogotá y del Servidor al Router de Bogotá
- Figura 36. Ping a los LAN de Bogotá y Cali
- Figura 37. Ping a los LAN de Bogotá y Medellín
- Figura 38. Telnet Router Medellin – Router Cali
- Figura 39. Telnet Servidor – Router Medellin
- Figura 40. Telnet Lan Medellin – Router Cali
- Figura 41. Telnet Lan Cali – Router Cali
- Figura 42. Telnet Lan Cali – Router Medellin
- Figura 43. Ping Lan Cali -WS 1
- Figura 44. Ping Lan Medellin -WS 1
- Figura 45. Ping Lan Medellín- Lan Cali
- Figura 46. Escenario 2 topología de la red
- Figura 47. Conexiones Físicas de la Topología de Red
- Figura 48. Host de Bucaramanga
- Figura 49. Host Y Servidor de Cundinamarca
- Figura 50. Configuración NAT
- Figura 51. VLAN Router Tunja
- Figura 52. Lista de acceso de Router Cundinamarca

Glosario

RED: Es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

ROUTER: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red.

SWITCHER: Un switch es un dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un PC, una impresora, una televisión, una consola o cualquier aparato que posea una tarjeta Ethernet o Wifi.

OSPF: Open Shortest Path First es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

EIGRP: (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia.

ACL: Una lista de control de acceso o ACL, es un concepto de seguridad informática usado para fomentar la separación de privilegios.

CCNA: (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet.

TFTP: Son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP.

DCHP: El protocolo de configuración dinámica de host 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 en una red para que puedan comunicarse con otras redes IP.

NAT: Network Address Translación), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles

PAT: Port Address Translation (PAT) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.

VLSM: Máscara de subred de tamaño variable.

RESUMEN

Este trabajo a través de dos escenarios de una empresa refleja todos los temas que se vieron en el diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN), utilizando herramientas como Packet Tracer que nos permite simular en tiempo real y en escenario reales cualquier problema o planteamiento de redes como en este caso.

Para el desarrollo de esta actividad se utilizó la guía enviada por el tutor del diplomado, con el fin de poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking del estudiante.

Para la solución de la red se utilizó switches, routers, terminales (PC, servidores) y diferentes configuraciones como Vlan, Nat, Eigrp, Ospf etc. Realizando los enrutamientos necesarios para lograr el desarrollo de cada escenario propuesto.

Palabras claves: Cisco. Red, Lan y Wan, Switches, Routers.

SUMMARY

This work through two scenarios of a company reflects all the issues that were seen in the cisco deepening diploma (design and implementation of integrated LAN / WAN solutions), using tools such as Packet Tracer that allows us to simulate in real time and on stage real any problem or network approach as in this case.

For the development of this activity the guide sent by the tutor of the diploma was used, in order to test the levels of understanding and solution of problems related to various aspects of student Networking.

Switches, routers, terminals (PCs, servers) and different configurations such as Vlan, Nat, Eigrp, Ospf etc. were used to solve the network. Making the necessary routing to achieve the development of each proposed scenario.

Keywords: Cisco. Red, Lan and Wan, Switches, Routers.

INTRODUCCIÓN

Hoy en día, como mucha facilidad podemos conectarnos o contactarnos con cualquier persona o dispositivo al rededor del mundo y eso es gracias a los avances tecnológicos de este nuevo siglo XXI.

Con este trabajo se pretender colocar en prácticas las habilidades y los conocimientos adquiridos en el desarrollo del diplomado de profundización cisco, tocando temas como planificación e implementación de redes pequeñas con una variedad de aplicaciones y software que nos ayudan a simular escenarios reales de nuestro diario vivir dentro de nuestras profesiones.

En esta actividad veremos configuración de routers e switches entre otros equipos, con diferentes situaciones dentro de una red, realizando el procedimiento paso a paso y apoyándonos de herramientas como Packet Tracer.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Realizar la prueba de habilidades prácticas, como parte de las actividades evaluativas del Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas Lan / Wan).

1.2. OBJETIVOS ESPECÍFICOS

- Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas por el estudiante a lo largo del diplomado.
- poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking del estudiante.
- Registrar la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante el desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip router, entre otros.
- Realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

2. DESARROLLO DE LOS ESCENARIOS

2.1. 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.

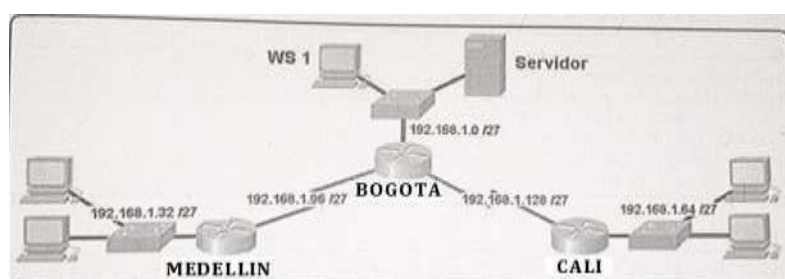


Figura 1. Escenario 1 Cada de host en la red.

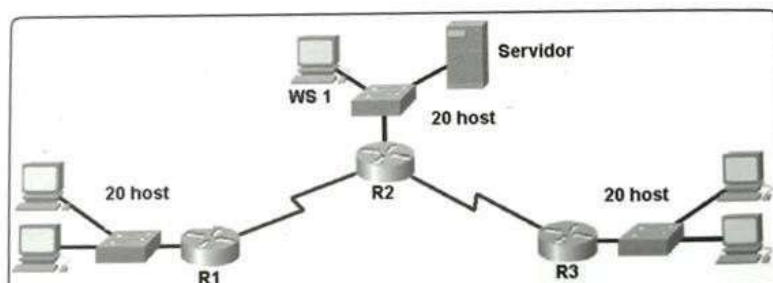


Figura 2. Escenario 1 topología de la red.

Topología de red

Los requerimientos solicitados son los siguientes:

2.1.1. Parte 1: Asignación De Direcciones IP

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

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

Configuración Básica De Los Routers

Router Bogota

```
Router>enable
Router#config t
Router(config)#hostname BOGOTA
BOGOTA(config)#line con 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#enable secret cisco
BOGOTA(config)#username admin privilege 15 password admin
BOGOTA(config)#ip domain-name cisco.com
BOGOTA(config)#crypto key generate rsa
The name for the keys will be: BOGOTA.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
BOGOTA(config)#line vty 0 4
*Mar 1 0:10:56.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
BOGOTA(config-line)#login local
BOGOTA(config-line)#transport
input ssh BOGOTA(config-
line)#do write Building
configuration...
[OK]
BOGOTA(config-line)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#exit
BOGOTA con0 is now
available Press RETURN to
get started.
BOGOTA(config-line)#
BOGOTA#exit
User Access
Verification
```

```
Password:
BOGOTA>enable
Password:
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#
```

Router Medellin

```
Router>enable
Router#config
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#enable secret cisco
MEDELLIN(config)#username admin privilege 15 password admin
MEDELLIN(config)#ip domain-name cisco.com
MEDELLIN(config)#crypto key generate rsa
The name for the keys will be: MEDELLIN.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
MEDELLIN(config)#line vty 0 4
*Mar 1 0:27:23.774: %SSH-5-ENABLED: SSH 1.99 has been enabled
MEDELLIN(config-line)#login local
MEDELLIN(config-line)#transport
input ssh MEDELLIN(config-
line)#do write Building
configuration...
[OK]
MEDELLIN(config-line)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#exit
MEDELLIN con0 is now
available Press RETURN
to get started. User
Access Verification
```

```
Password:
MEDELLIN>enable
Password:
MEDELLIN#
```

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#line con 0
CALI(config-line)#password cisco
CALI(config-line)#login
```

Router Cali

```
CALI(config-line)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#enable secret cisco
CALI(config)#username admin privilege 15 password admin
CALI(config)#ip domain-name cisco.com
CALI(config)#crypto key generate rsa
The name for the keys will be: CALI.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CALI(config)#line vty 0 4
*Mar 1 0:43:38.653: %SSH-5-ENABLED: SSH 1.99 has been enabled
CALI(config-line)#login local
CALI(config-line)#transport
input ssh CALI(config-
line)#do write Building
configuration...
[OK]
CALI(config-line)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#exit
CALI con0 is now
available Press
RETURN to get
started. User Access
Verification Password:
```

```
CALI>enable
Password:
Password:
CALI#
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#enable secret cisco
S1(config)#username admin privilege 15 password admin
S1(config)#ip domain-name cisco.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S1(config)#line vty 0 4
*Mar 1 1:5:39.553: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#login local
S1(config-line)#transport
input ssh S1(config-
line)#do write Building
configuration...
[OK]
S1(config-line)#exit
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#enable secret cisco
S2(config)#username admin privilege 15 password admin
```



```
S2(config)#ip domain-name cisco.com
S2(config)#crypto key generate rsa
The name for the keys will be: S2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S2(config)#line vty 0 4
*Mar 1 1:23:9.701: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-line)#login local
S2(config-line)#transport
input ssh S2(config-
line)#do write Building
configuration...
[OK]
S2(config-line)#exit
```

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#enable secret cisco
S3(config)#username admin privilege 15 password admin
S3(config)#ip domain-name cisco.com
S3(config)#crypto key generate rsaGG
The name for the keys will be: S3.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than
512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S3(config)#line vty 0 4
*Mar 1 1:32:20.151: %SSH-5-ENABLED: SSH 1.99 has been enabled
S3(config-line)#login local
S3(config-line)#transport
input ssh S3(config-
line)#do write Building
configuration...
[OK]
S3(config-line)#exit
```

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

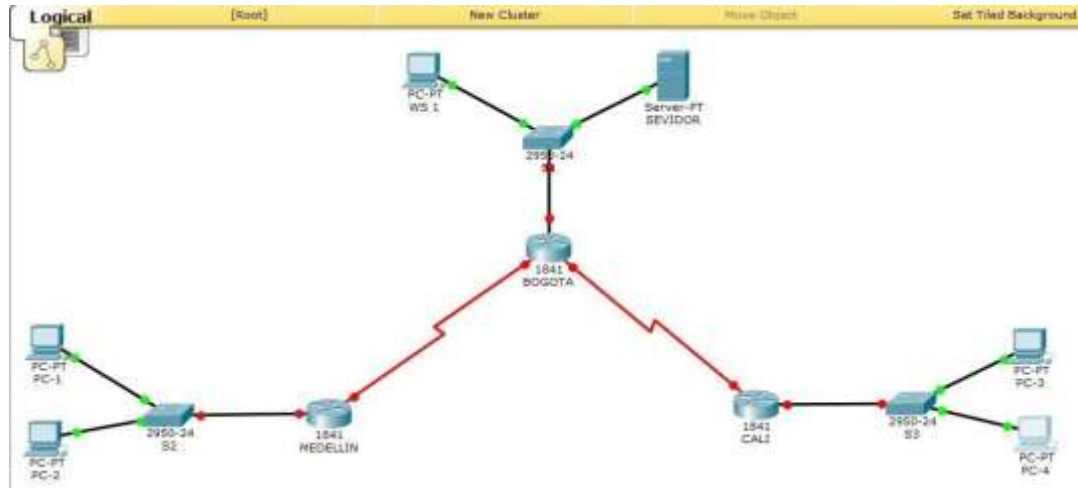


Figura 3. Conexión física de la topología

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

Se toman prestados 3 bits, se crean 8 subredes. $2^3=8$ subredes

Red 0	Red	192.168.1.000	0 0000	192.168.1.0
	Primero	192.168.1.000	0 0001	192.168.1.1
	Ultima	192.168.1.000	1 1110	192.168.1.30
	Broadcast	192.168.1.000	1 1111	192.168.1.31
Red 1	Red	192.168.1.001	0 0000	192.168.1.32
	Primero	192.168.1.001	0 0001	192.168.1.33
	Ultima	192.168.1.001	1 1110	192.168.1.62
	Broadcast	192.168.1.001	1 1111	192.168.1.63
Red 2	Red	192.168.1.010	0 0000	192.168.1.64
	Primero	192.168.1.010	0 0001	192.168.1.65
	Ultima	192.168.1.010	1 1110	192.168.1.94
	Broadcast	192.168.1.010	1 1111	192.168.1.95
Red 3	Red	192.168.1.011	0 0000	192.168.1.96
	Primero	192.168.1.011	0 0001	192.168.1.97
	Ultima	192.168.1.011	1 1110	192.168.1.126
	Broadcast	192.168.1.011	1 1111	192.168.1.127
Red 4	Red	192.168.1.100	0 0000	192.168.1.128
	Primero	192.168.1.100	0 0001	192.168.1.129
	Ultima	192.168.1.100	1 1110	192.168.1.158

	Broadcast	192.168.1.100	1 1111	192.168.1.159
Red 5	Red	192.168.1.101	0 0000	192.168.1.160
	Primero	192.168.1.101	0 0001	192.168.1.161
	Ultima	192.168.1.101	1 1110	192.168.1.190
	Broadcast	192.168.1.101	1 1111	192.168.1.191
Red 6	Red	192.168.1.110	0 0000	192.168.1.192
	Primero	192.168.1.110	0 0001	192.168.1.193
	Ultima	192.168.1.110	1 1110	192.168.1.222
	Broadcast	192.168.1.110	1 1111	192.168.1.223
Red 7	Red	192.168.1.111	0 0000	192.168.1.224
	Primero	192.168.1.111	0 0001	192.168.1.225
	Ultima	192.168.1.111	1 1110	192.168.1.254
	Broadcast	192.168.1.111	1 1111	192.168.1.255

Tabla 1. Tabla de redes y SubRedes.

b. Asignar una dirección IP a la red.

La IP de la red es 192.168.1.0 /27

Topología Con Las Redes Asignadas

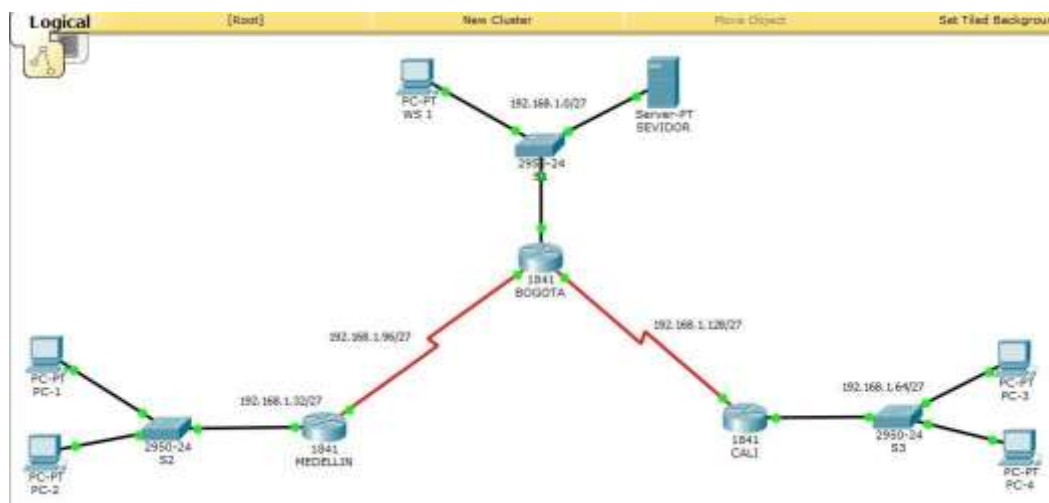


Figura 4. Topología de la Red.

2.1.2. Parte 2: Configuración Básica

Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectado

	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

Tabla 2. Asignación de los parámetros básicos y la detección de vecinos. a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

Router Bogotá

```

BOGOTA>enable
Password:
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface Serial0/1/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
BOGOTA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0,
changed state to up
BOGOTA(config-if)#interface Serial0/1/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224

```

```
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
BOGOTA(config-if)#interface FastEthernet0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
BOGOTA(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA(config-if)#exit
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip def
BOGOTA (config)#ip default-gateway 192.168.1.0
```

Router Medellin

```
User Access
Verification Password:
MEDELLIN>enable
Password:
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface Serial0/1/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN(config)#interface FastEthernet0/0
MEDELLIN(config-if)# ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip def
MEDELLIN(config)#ip default-gateway 192.168.1.0
```

```
User Access
Verification
```

Router Cali

Password:

```
CALI>enable
```

Password:

```
CALI #configure terminal
```

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

```
CALI (config)#interface Serial0/1/0
```

```
CALI (config-if)#ip address 192.168.1.131 255.255.255.224
```

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

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

```
CALI (config)#interface FastEthernet0/0
```

```
CALI (config-if)# ip address 192.168.1.65 255.255.255.224
```

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

```
CALI (config-if)#clock rate 128000
```

```
CALI (config)#exit
```

```
CALI #
```

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

```
CALI #config t
```

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

```
CALI (config)#ip def
```

```
CALI (config)#ip default-gateway 192.168.1.0
```

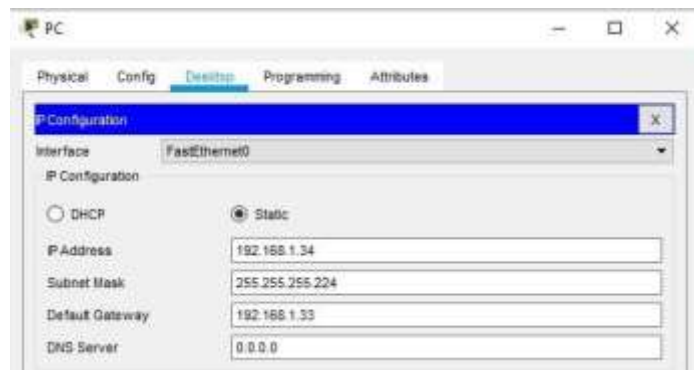


Figura 5. Configuración del Equipo Lan de Medellín

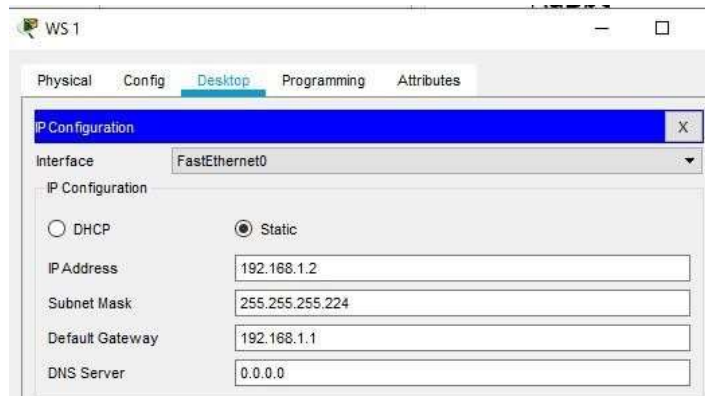


Figura 6. Configuración del Equipo WS 1



Figura 7. Configuración del Servidor



Figura 8. Configuración del Equipo Lan de Cali

- 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.

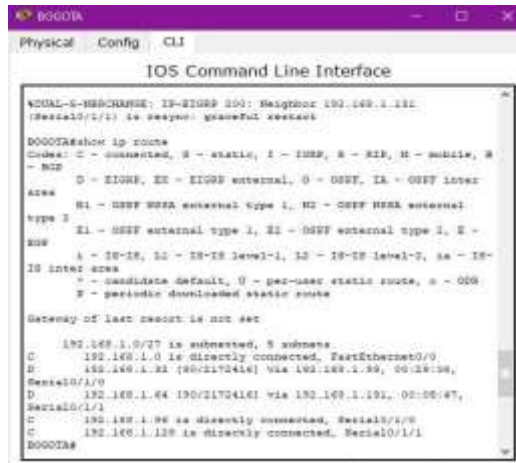


Figura 9. Diagnósticos de vecinos de Router Bogotá



Figura 10. Diagnósticos de vecinos de Router Medellín



Figura 11. Diagnósticos de vecinos de Router Cali

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

```
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#route eigrp 200
BOGOTA(config-router)#var
BOGOTA(config-router)#variance 4
BOGOTA(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99
(Serial0/1/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.131
(Serial0/1/1) is up: new adjacency
```

```
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#route eigrp 200
MEDELLIN(config-router)#vai
MEDELLIN(config-router)#vari
MEDELLIN(config-router)#variance 4
MEDELLIN(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98
(Serial0/1/0) is up: new adjacency
```

```
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#route eigrp 200
CALI(config-router)#var
CALI(config-router)#variance
CALI(config-router)#variance 4
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130
(Serial0/1/0) is up: new adjacency
```

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

```
BOGOTA#show cdp nei
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
Switch         Gig 0/0/0      168       S           2960      Fas 0/2
MEDELLIN      Ser 0/1/0      149       R           ISR4300   Ser 0/1/0
CALI           Ser 0/1/1      159       R           ISR4300   Ser 0/1/0
BOGOTA#
```

Figura 12 Ping del tramo de la ruta del Router de Medellín

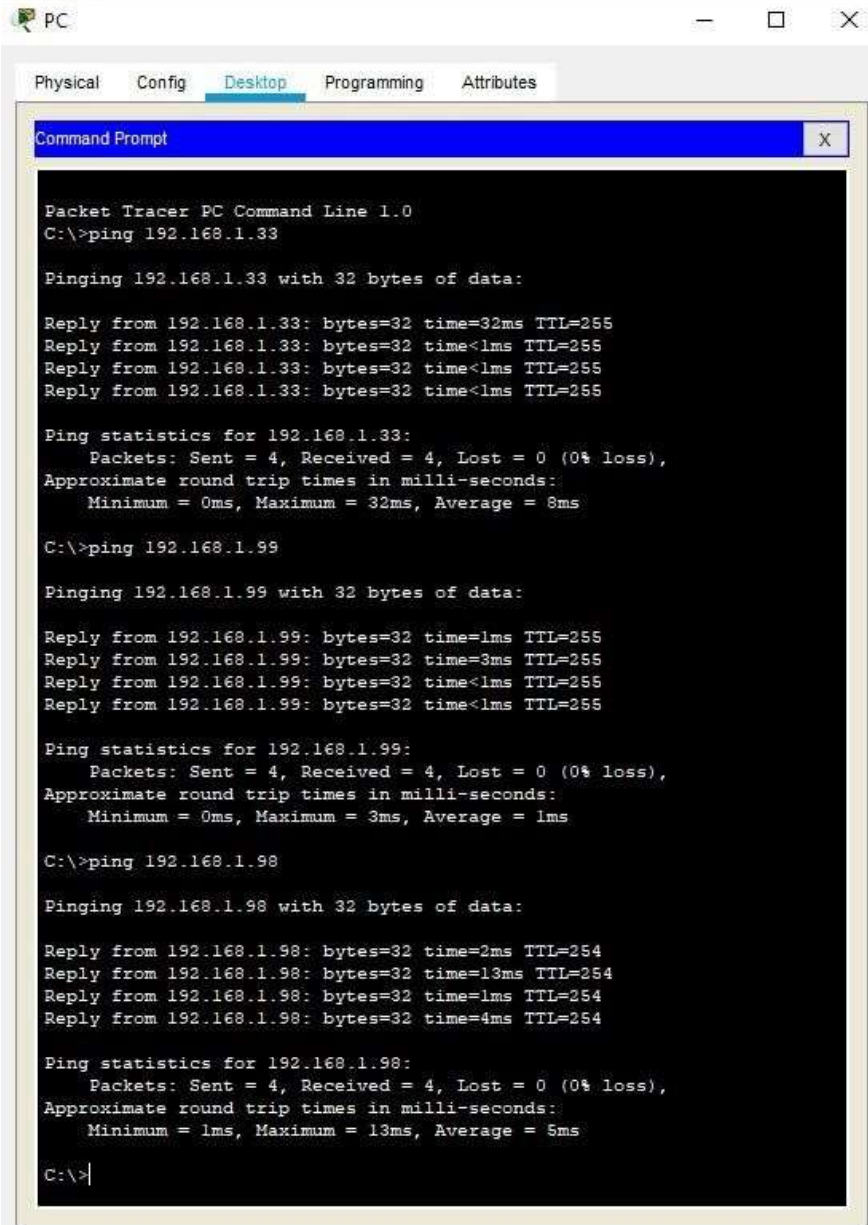
```
MEDELLIN#show cdp nei
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
Switch         Gig 0/0/0      129       S           2960      Fas 0/2
BOGOTA         Ser 0/1/0      151       R           ISR4300   Ser 0/1/0
MEDELLIN#
```

Figura 13 Ping del tramo de la ruta del Router de Bogotá con WS

```
CALI#show cdp nei
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
Switch         Gig 0/0/0      150       S           2960      Fas 0/1
BOGOTA         Ser 0/1/0      159       R           ISR4300   Ser 0/1/1
CALI#
```

Figura 14 Ping del tramo de la ruta del Router de Bogotá con servidor

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



```
PC
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=32ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 32ms, Average = 8ms

C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

Reply from 192.168.1.99: bytes=32 time=1ms TTL=255
Reply from 192.168.1.99: bytes=32 time=3ms TTL=255
Reply from 192.168.1.99: bytes=32 time<1ms TTL=255
Reply from 192.168.1.99: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.1.98

Pinging 192.168.1.98 with 32 bytes of data:

Reply from 192.168.1.98: bytes=32 time=2ms TTL=254
Reply from 192.168.1.98: bytes=32 time=13ms TTL=254
Reply from 192.168.1.98: bytes=32 time=1ms TTL=254
Reply from 192.168.1.98: bytes=32 time=4ms TTL=254

Ping statistics for 192.168.1.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 5ms

C:\>
```

Figura 15. Ping del tramo de la ruta del Router de Cali

The image shows a Packet Tracer PC Command Line window titled 'WS 1'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=12ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=3ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>ping 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Reply from 192.168.1.131: bytes=32 time=40ms TTL=254
Reply from 192.168.1.131: bytes=32 time=10ms TTL=254
Reply from 192.168.1.131: bytes=32 time=1ms TTL=254
Reply from 192.168.1.131: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 40ms, Average = 13ms

C:\>
```

Figura 16. Ping de WS1 al servidor, router de Bogotá y Cali

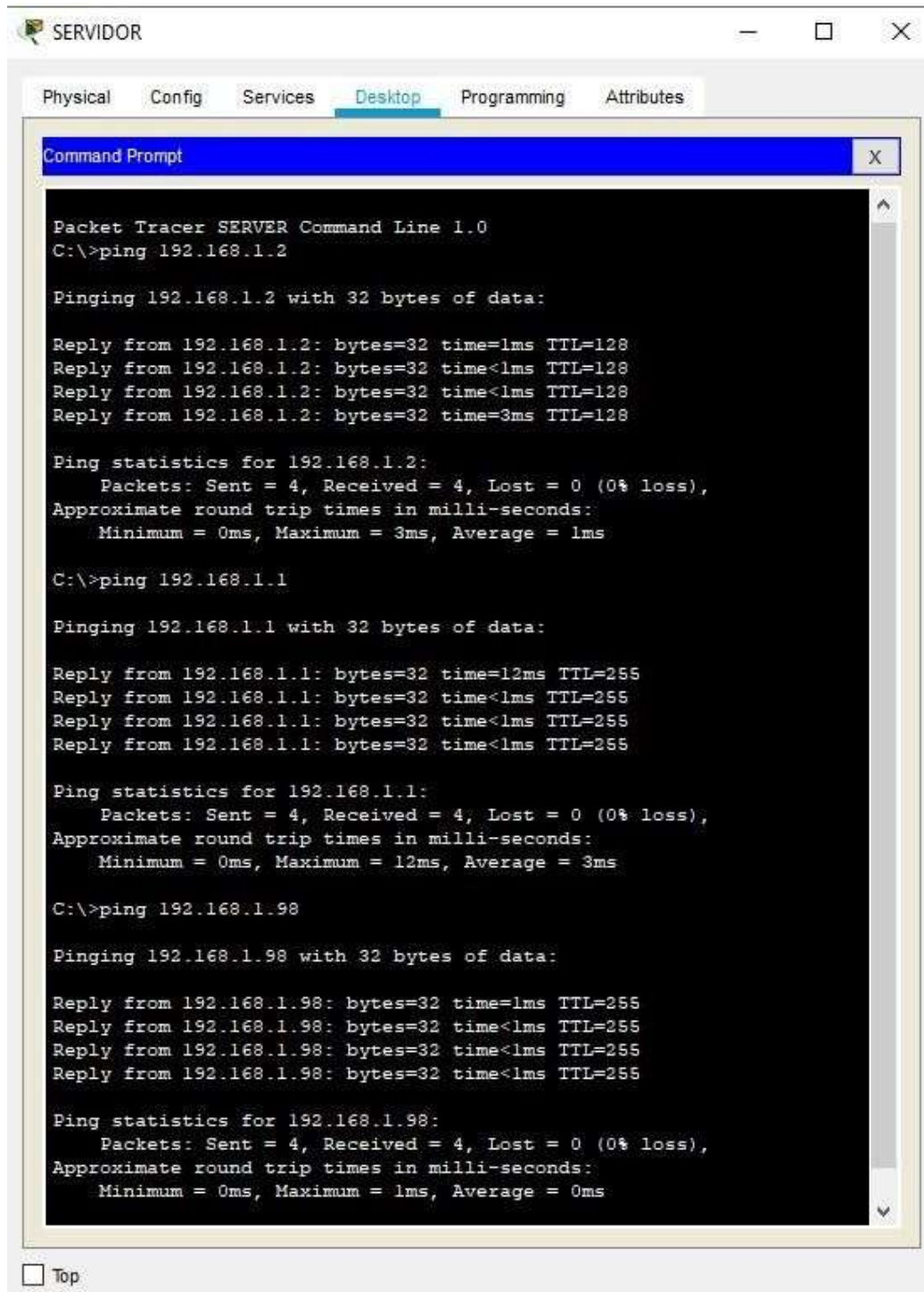


Figura 17. Ping del servidor a la Lan de Bogotá y el router.

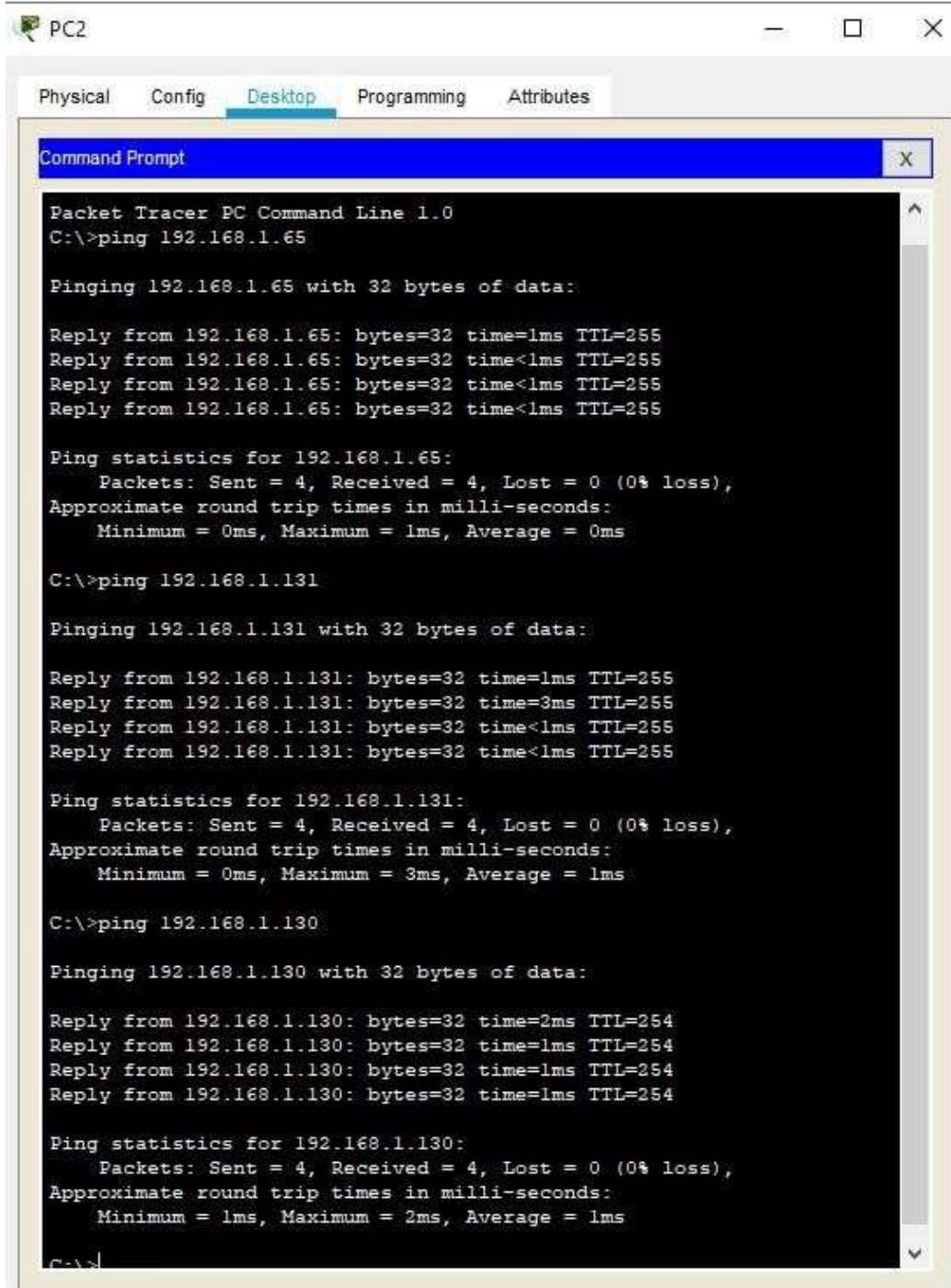


Figura 18. Ping de la Lan de Cali a router de Cali.

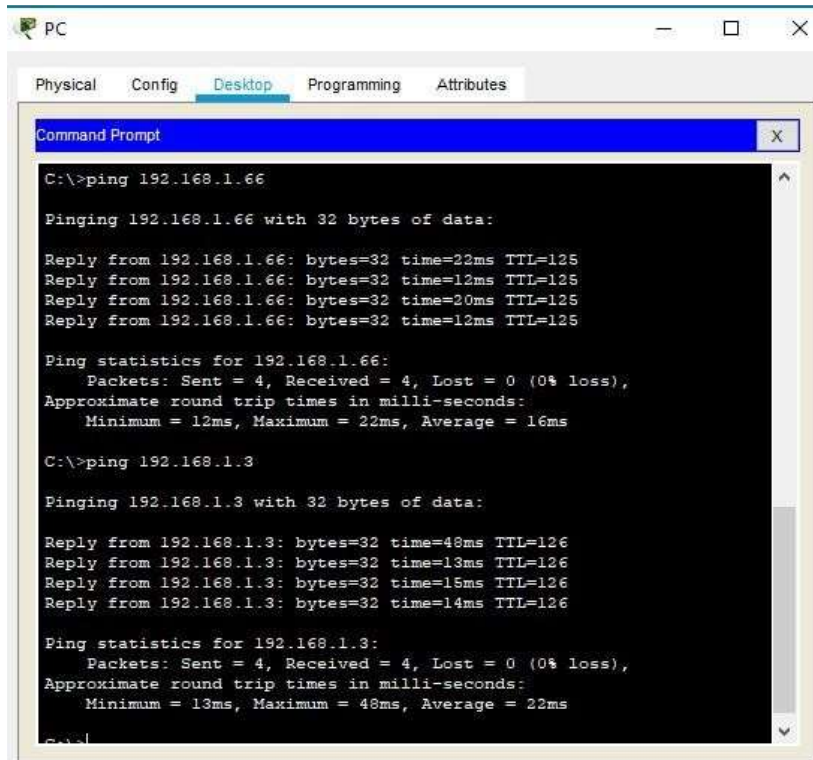


Figura 19. Ping de la Lan de Medellín a la Lan de Cali y el servidor.

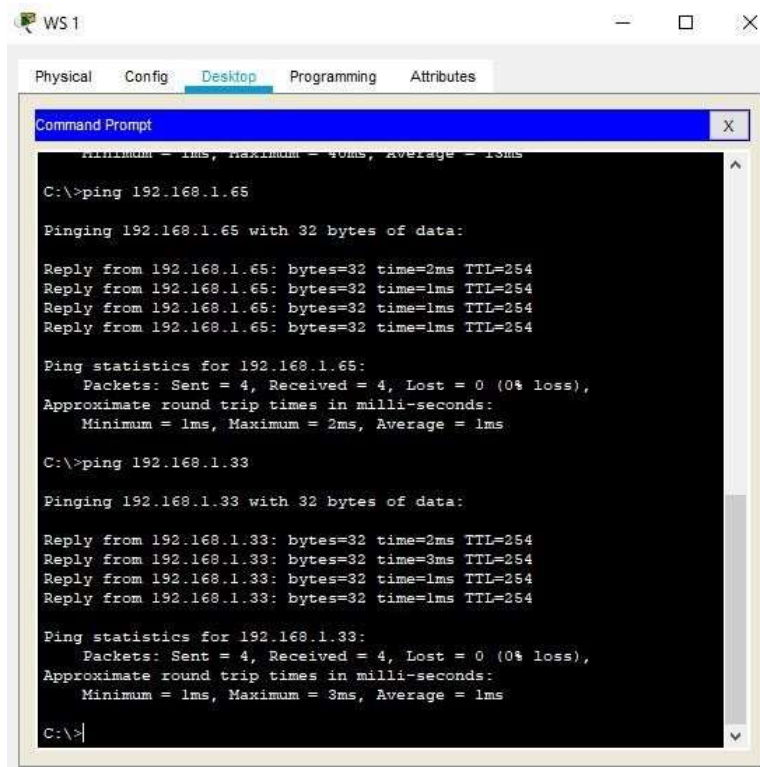


Figura 20. Ping del WS 1 al router de Medellín y Cali

2.1.3. Parte 3: Configuración De Enrutamiento

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

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

EIGRP Router Bogotá

```
BOGOTA(config)#route eigrp 200
BOGOTA(config-router)#net
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.96.0 0.0.0.31
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99
(Serial0/1/0) is up: new adjacency
BOGOTA(config-router)#network 192.168.128.0 0.0.0.31
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.131
(Serial0/1/1) is up: new adjacency
BOGOTA(config-router)#network 192.168.32.0 0.0.0.31
BOGOTA(config-router)#no au
BOGOTA(config-router)#no auto-
summary BOGOTA(config-
router)#do write Building
configuration...
[OK]
```

EIGRP Router Medellin

```
MEDELLIN(config)#route eigrp 200
MEDELLIN(config-router)#net
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98
(Serial0/1/0) is up: new adjacency
MEDELLIN(config-router)#network 192.168.1.128 0.0.0.31
MEDELLIN(config-router)# no auto-summary
```

EIGRP Router Cali

```
CALI(config)#route eigrp 200
CALI(config-router)#net
CALI(config-router)#network 192.168.96.0 0.0.0.31
CALI(config-router)#network 192.168.128.0 0.0.0.31
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.131
(Serial0/1/0) is up: new adjacency
```



```

CALI config-router)#network 192.168.64.0 0.0.0.31
CALI(config-router)#no au
CALI config-router)#no auto-
summary CALI(config-
router)#do write Building
configuration...
[OK]

```

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

```

User Access Verification

Password:

BOGOTA>enable
Password:
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
S1             Fas 0/0       157       S           2950      Fas 0/24
CALI           Ser 0/1/1     166       R           C1841     Ser 0/1/0
MEDELLIN      Ser 0/1/0     157       R           C1841     Ser 0/1/0
BOGOTA#

```

Figura 21. Vecindad Eigrp del Router Bogotá

```

User Access Verification

Password:

MEDELLIN>enable
Password:
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
S2             Fas 0/0       162       S           2950      Fas 0/24
BOGOTA        Ser 0/1/0     169       R           C1841     Ser 0/1/0
MEDELLIN#

```

Figura 22. Vecindad Eigrp del Router Medellín

```

User Access Verification

Password:

CALI>enable
Password:
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
S3             Fas 0/0       157        S           2950      Fas 0/24
BOGOTA        Ser 0/1/0     164        R           C1841     Ser 0/1/1
CALI#

```

Figura 23. Vecindad Eigrp del 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.

```

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/2172416] via 192.168.1.99, 00:11:44, Serial0/1/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:11:42, Serial0/1/1
C       192.168.1.96 is directly connected, Serial0/1/0
C       192.168.1.128 is directly connected, Serial0/1/1
-----

```

Figura 24. Tabla de enrutamiento Bogotá.

```

User Access Verification

Password:

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 00:15:19, Serial0/1/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 00:15:17, Serial0/1/0
C       192.168.1.96 is directly connected, Serial0/1/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 00:15:19, Serial0/1/0
MEDELLIN#

```

Figura 25. Tabla de enrutamiento Medellín.

```

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

Gateway of last resort is not set

    192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 00:16:12, Serial0/1/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:16:12, Serial0/1/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 00:16:12, Serial0/1/0
C       192.168.1.128 is directly connected, Serial0/1/0
CALI#

```

Figura 26. Tabla de enrutamiento Cali.

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

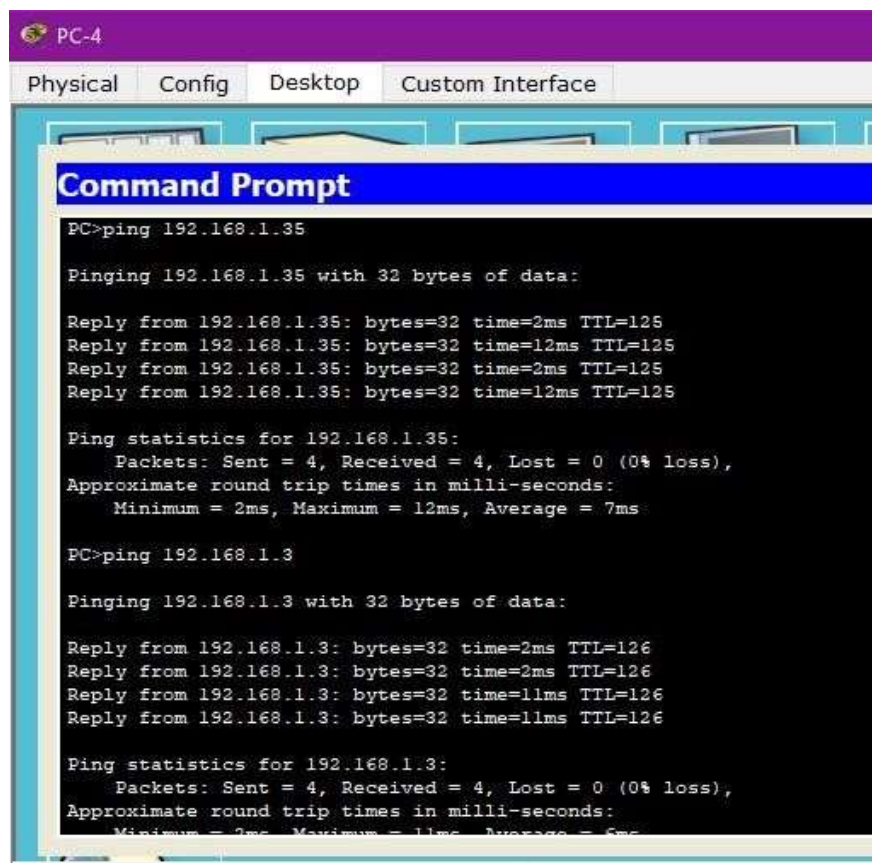


Figura 27. Prueba de conectividad de los puntos de red entre sí.

2.1.4. Parte 4: Configuración De Las Listas De Control De Acceso

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

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

Telnet Medellin

```
MEDELLIN#enable
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#trans
MEDELLIN(config-line)#transport input all
```

```
MEDELLIN#enable
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#trans
MEDELLIN(config-line)#transport input all
```

Figura 28. Habilitar el Router de Medellín para establecer conexiones Telnet

```
BOGOTA#
BOGOTA#telnet 192.168.1.99
Trying 192.168.1.99 ...Open

User Access Verification

Password:
MEDELLIN>enable
Password:
MEDELLIN#exit

[Connection to 192.168.1.99 closed by foreign host]
BOGOTA#config
```

Figura 29. Ingreso desde el router Bogotá al de Medellín por telnet.

```

User Access Verification

Password:

CALI>enable
Password:
CALI#ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/18 ms

CALI#telnet 192.168.1.99
Trying 192.168.1.99 ...Open

User Access Verification

Password:
Password:
MEDELLIN>enable
Password:
MEDELLIN#

```

Figura 30. Ingreso desde el router Cali al de Medellín por telnet.

Telnet Bogota

```

BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#tran
BOGOTA(config-line)#transport input all
BOGOTA(config-line)#exit
BOGOTA(config)#

```

```

User Access Verification

Password:

MEDELLIN>enable
Password:
MEDELLIN#telnet 192.168.1.98
Trying 192.168.1.98 ...Open

User Access Verification

Password:
BOGOTA>enable
Password:
BOGOTA#

```

Figura 31. Ingreso desde el router Medellín al de Bogotá por telnet.

```
CALI#telnet 192.168.1.98
Trying 192.168.1.98 ...Open

User Access Verification

Password:
BOGOTA>enable
Password:
BOGOTA#
```

Figura 32. Ingreso desde el router Cali al de Bogotá por telnet.

```
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#line vty 4 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#trans
CALI(config-line)#transport input all
CALI(config-line)#
```

```
User Access Verification

Password:
BOGOTA>enable
Password:
BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

Password:
CALI>enable
Password:
CALI#
```

Figura 33. Ingreso desde el router Bogotá al de Cali por telnet.

```
MEDELLIN#telnet 192.168.1.65
Trying 192.168.1.65 ...Open

User Access Verification

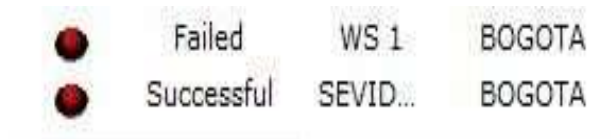
Password:
CALI>enable
Password:
CALI#
```

Figura 34. Ingreso desde el router Medellín al de Cali por telnet.

- 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.

Creamos listas de acceso para administrar el acceso a la red.

```
User Access Verification
Password: BOGOTA>enable Password:
BOGOTA#acce
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#acce
BOGOTA(config)#access-list 1 per
BOGOTA(config)#access-list 1 permit 192.168.1.3
BOGOTA(config)#access-list 1 deny 192.168.1.2
BOGOTA(config)#int
BOGOTA(config)#interface fas
BOGOTA(config)#interface fastEthernet 0/0
BOGOTA(config-if)#ip acc
BOGOTA(config-if)#ip access-group 1 in
BOGOTA(config-if)#
```



●	Failed	WS 1	BOGOTA
●	Successful	SEVID...	BOGOTA

Figura 35. Ping de WS 1 al router de Bogotá y del Servidor al Router de Bogotá

- d. 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.
- e.

LAN de MEDELLIN

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	SEVID...	PC-1	ICMP		0.000	N	0
	Failed	PC-1	WS 1	ICMP		0.000	N	1
	Failed	PC-1	PC-3	ICMP		0.000	N	2
	Failed	PC-1	PC-4	ICMP		0.000	N	3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC-2	SEVIDOR	ICMP		0.000	N	0
	Failed	PC-2	WS 1	ICMP		0.000	N	1
	Failed	PC-2	PC-3	ICMP		0.000	N	2
	Failed	PC-2	PC-4	ICMP		0.000	N	3

Figura 36. Ping a los LAN de Bogotá y Cali

LAN de CALI

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC-3	SEVIDOR	ICMP		0.000	N	0
	Failed	PC-3	WS 1	ICMP		0.000	N	1
	Failed	PC-3	PC-1	ICMP		0.000	N	2
	Failed	PC-3	PC-2	ICMP		0.000	N	3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC-4	SEVIDOR	ICMP		0.000	N	0
	Failed	PC-4	WS 1	ICMP		0.000	N	1
	Failed	PC-4	PC-1	ICMP		0.000	N	2
	Failed	PC-4	PC-2	ICMP		0.000	N	3

Figura 37. Ping a los LAN de Bogotá y Medellín

2.1.5.

Parte 5: Comprobación De La Red Instalada

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Default
	WS_1	Router BOGOTA	Successful
	Servidor	Router CALI	Successful
	Servidor	Router MEDELLIN	Successful
TELNET	LAN del Router MEDELLIN	Router CALI	Default
	LAN del Router CALI	Router CALI	Default
	LAN del Router MEDELLIN	Router MEDELLIN	Default
	LAN del Router CALI	Router MEDELLIN	Default
PING	LAN del Router CALI	WS_1	Default
	LAN del Router MEDELLIN	WS_1	Default
	LAN del Router MEDELLIN	LAN del Router CALI	Default
PING	LAN del Router CALI	Servidor	Successful
	LAN del Router MEDELLIN	Servidor	Successful
	Servidor	LAN del Router MEDELLIN	Successful
	Servidor	LAN del Router CALI	Successful
	Router CALI	LAN del Router MEDELLIN	Default
	Router MEDELLIN	LAN del Router CALI	Default

Tabla 3. Comprobación total de los dispositivos y su funcionamiento en la red.

```

User Access Verification

Password:

MEDELLIN>enable
Password:
MEDELLIN#telnet 192.168.1.65
Trying 192.168.1.65 ...
% Connection timed out; remote host not responding
MEDELLIN#

```

Figura 38. Telnet Router Medellin – Route Cali

```

PC>telnet 192.168.1.98
Trying 192.168.1.98 ...
% Connection timed out; remote host not responding
PC>

```

Figura 39. Telnet Servidor – Router Medellín

```

% Connection timed out; remote
SERVER>telnet 192.168.1.99
Trying 192.168.1.99 ... Open

User Access Verification

Password:
MEDELLIN>enable
Password:
MEDELLIN#

```

Figura 40. Telnet Lan Medellin – Router Cali

```

Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.65
Trying 192.168.1.65 ...
% Connection timed out; remote host not responding
PC>

```

Figura 41. Telnet Lan Cali – Router Cali

```

Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.99
Trying 192.168.1.99 ...
% Connection timed out; remote host not responding
PC>

```

Figura 42. Telnet Lan Cali – Router Medellín

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 43. Ping Lan Cali -WS 1

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 44. Ping Lan Medellin -WS 1

```
PC>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

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

Figura 45. Ping Lan Medellín- Lan Cali

2.2. Escenario 2

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

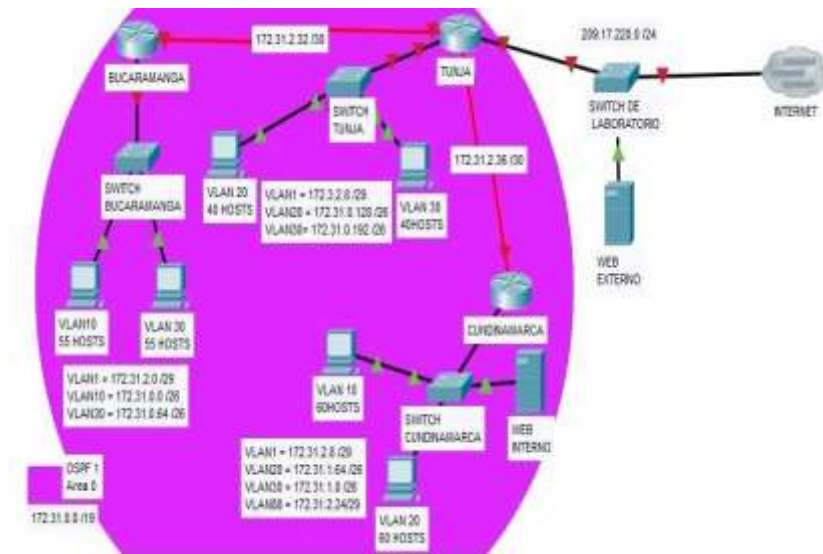


Figura 46. Escenario 2 topología de la red

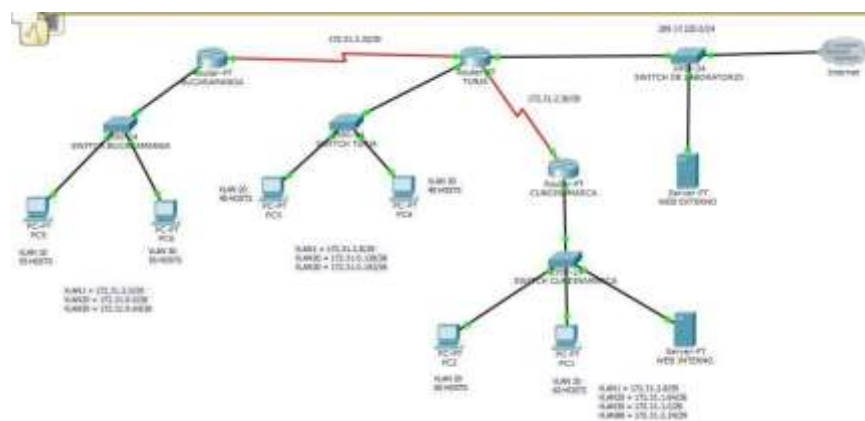


Figura 47. Conexiones Físicas de la Topología de Red

2.2.1. Configuración De Equipos

Configuración Básica.

Router Bucaramanga

```
Router>enable
Router#configure terminal
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable password cisco
BUCARAMANGA(config)#enable secret cisco1
BUCARAMANGA(config)#banner motd #Router de BUCARAMANGA#
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#exit
BUCARAMANGA#copy running-config startup-config
```

Router Tunja

```
Router>enable
Router#configure terminal
Router(config)#hostname BUCARAMANGA
TUNJA(config)#enable password cisco
TUNJA (config)#enable secret cisco1
TUNJA (config)#banner motd #Router de TUNJA #
TUNJA (config)#line console 0
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
TUNJA (config-line)#exit
TUNJA (config)#line vty 0 4
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
TUNJA (config-line)#exit
TUNJA (config)#service password-encryption
TUNJA (config)#exit
TUNJA #copy running-config startup-config
```

Router Cundinamarca

```
Router>enable
Router#configure terminal
Router(config)#hostname BUCARAMANGA
CUNDINAMARCA(config)#enable password cisco
```

```
CUNDINAMARCA (config)#enable secret cisco1
CUNDINAMARCA (config)#banner motd
CUNDINAMARCA (config)#line console 0
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#line vty 0 4
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#service password-encryption
CUNDINAMARCA (config)#exit
CUNDINAMARCA #copy running-config startup-config
```

Autenticación local con AAA.

Router Bucaramanga

```
BUCARAMANGA (config)#username laura secret cisco
BUCARAMANGA (config)#aaa new-model
BUCARAMANGA (config)#aaa authentication login default local
BUCARAMANGA (config)#line console 0
BUCARAMANGA (config-line)#login authentication default
BUCARAMANGA (config-line)#exit
BUCARAMANGA (config)#line vty 0 4
BUCARAMANGA (config-line)#login authentication default
BUCARAMANGA (config-line)#exit
BUCARAMANGA (config)#exit
BUCARAMANGA #
```

Router Tunja

```
TUNJA (config)#username laura secret cisco
TUNJA (config)#aaa new-model
TUNJA (config)#aaa authentication login default local
TUNJA (config)#line console 0
TUNJA (config-line)#login authentication default
TUNJA (config-line)#exit
TUNJA (config)#line vty 0 4
TUNJA (config-line)#login authentication default
TUNJA (config-line)#exit
TUNJA (config)#exit
TUNJA #
```

Router Cundinamarca

```
CUNDINAMARCA (config)#username laura secret cisco
CUNDINAMARCA (config)#aaa new-model
CUNDINAMARCA (config)#aaa authentication login default local
CUNDINAMARCA (config)#line console 0
```

```
CUNDINAMARCA (config-line)#login authentication default
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#line vty 0 4
CUNDINAMARCA (config-line)#login authentication default
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#exit
CUNDINAMARCA #
```

Cifrado De Contraseñas

Router Bucaramanga

```
BUCARAMANGA #configure terminal
BUCARAMANGA (config)#service password-encryption
BUCARAMANGA (config)#exit
```

Router Tunja

```
TUNJA #configure terminal
TUNJA (config)#service password-encryption
TUNJA (config)#exit
```

Router Cundinamarca

```
CUNDINAMARCA #configure terminal
CUNDINAMARCA (config)#service password-encryption
CUNDINAMARCA (config)#exit
```

Se establezca un servidor TFTP que almacene todos los archivos necesarios de los routers.

Router Bucaramanga

```
BUCARAMANGA#dir flash:
```

```
Directory of flash:/
```

```
 3 -rw- 33591768      <no date> c1841-advipservicesk9-mz.124-15.T1.bin
```

```
 2 -rw- 28282        <no date> sigdef-category.xml
```

```
 1 -rw- 227537       <no date> sigdef-default.xml 64016384 bytes
```

```
total (30168797 bytes free) BUCARAMANGA#copy flash: tftp:
```

```
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
```

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

```
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
```

```
Writing c1841-advipservicesk9-mz.124-
```

```
15.T1.bin. ....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
[OK – 33591768 bytes] 33591768 bytes copied in 6.754 secs (4970000 bytes/sec)
```

Router Tunja

```
TUNJA#dir flash:
Directory of flash:/
  3 -rw-  33591768      <no date> c1841-advipservicesk9-mz.124-
15.T1.bin
  2 -rw-    28282      <no date> sigdef-category.xml
  1 -rw-   227537      <no date> sigdef-default.xml 64016384 bytes
total (30168797 bytes free) TUNJA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing          c1841-advipservicesk9-mz.124-
15.T1.bin. ....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK – 33591768 bytes]
33591768 bytes copied in 6.754 secs (4970000 bytes/sec)
```

Router Cundinamarca

```
CUNDINAMARCA#dir flash:
Directory of flash:/
  3 -rw-  33591768      <no date> c1841-advipservicesk9-mz.124-
15.T1.bin
  2 -rw-    28282      <no date> sigdef-category.xml
  1 -rw-   227537      <no date> sigdef-default.xml 64016384 bytes
total (30168797 bytes free) CUNDINAMARCA #copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing          c1841-advipservicesk9-mz.124-
15.T1.bin. ....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK – 33591768 bytes] 33591768 bytes copied in 6.754 secs (4970000
bytes/sec)
```


2.2.2 DHCP

Se utiliza direcciones DHCP para los hosts de Bucaramanga y Cundinamarca utilizando DHCP POOL

DCHP POOL LAN BUCARAMANGA



Figura 48. Host de Bucaramanga

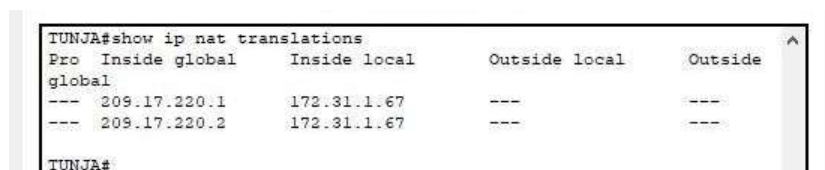
DCHP POOL LAN CUNDINAMARCA



Figura 49. Host Y Servidor de Cundinamarca

2.2.3 NAT Estático Y NAT De Sobrecarga (PAT)

```
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.2
TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
```



```
TUNJA#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside
global
---  209.17.220.1    172.31.1.67   ---            ---
---  209.17.220.2    172.31.1.67   ---            ---
TUNJA#
```

Figura 50. Configuración NAT

Configuración de la NAT con sobrecarga (PAT), se crea una access-list donde se colocan las direcciones que se desean que sean traducidas.

2.2.4 El Enrutamiento Con Autenticación.

```
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
TUNJA(config)#router ospf 1
TUNJA(config-router)#area 0 authentication
TUNJA(config-router)#
TUNJA(config)#router ospf 1
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.0 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.0 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.64 0.0.0.63 area 0
TUNJA(config-router)#
```

2.2.5 Listas De Control De Acceso

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

```
BUCARAMANGA (config)#access-list 1 permit 209.17.220.0
BUCARAMANGA (config)#access-list 1 permit host 172.31.0.0
BUCARAMANGA (config)#access-list 1 deny any
BUCARAMANGA (config)#interface fa0/0
BUCARAMANGA (config-if)#ip access-group 1 out
```

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

```
TUNJA(config)#access-list 2 permit 172.31.0.0
TUNJA(config)#interface fa0/0
TUNJA(config-if)#ip access-group 2 in
TUNJA(config-if)#
```

```
TUNJA#show access-list
Standard IP access list 1
 10 permit host 172.31.1.64
Standard IP access list 4
 10 deny 172.31.1.0 0.0.0.63
 20 permit any
Standard IP access list 3
 10 deny 172.31.1.64 0.0.0.63
 20 permit any (747 match(es))
Standard IP access list 10
 10 permit 172.31.0.0 0.0.63.255
```

Figura 51. VLAN Router Tunja

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

```
CUNDINAMARCA(config)#access-list 3 deny 172.31.0.192 0.0.0.63
CUNDINAMARCA(config)#access-list 3 permit any
CUNDINAMARCA(config)#interface fa0/0
CUNDINAMARCA(config-if)#ip access-group 3 out
CUNDINAMARCA(config-if)# exit
CUNDINAMARCA(config)#access-list 3 permit 172.31.0.0
CUNDINAMARCA(config)#interface se0/0/0
CUNDINAMARCA(config-if)#ip access-group 3 in
CUNDINAMARCA(config-if)#
```

```

Physical  Config  CLI  Attributes
IOS Command Line Interface
CUNDINAMARCA#show access-list
Standard IP access list 1
 10 deny 172.31.0.192 0.0.0.63
 20 permit any (2 match(es))
CUNDINAMARCA#

```

Figura 52. Lista de acceso de Router Cundinamarca

2.2.6 VLSM

Id	Host	Hosts encontrados	Dirección de red	Mascara de Sub red
1	55	62	172.31.0.0	255.255.255.192
2	55	62	172.31.0.64	255.255.255.192
3	40	62	172.31.0.128	255.255.255.192
4	40	62	172.31.0.192	255.255.255.192
5	60	62	172.31.1.0	255.255.255.192
6	60	62	172.31.1.64	255.255.255.192
7			172.31.1.128	
8			172.31.1.192	
9	6	6	172.31.2.0	255.255.255.248
10	6	6	172.31.2.8	255.255.255.248
11	6	6	172.31.2.16	255.255.255.248
12			172.31.2.24	
13	2	2	172.31.2.32	255.255.255.252
14	2	2	172.31.2.36	255.255.255.252

Tabla 4. VLSM (Direccionamientos)

Habilitamos los POOLS en los de Bucaramanga y Cundinamarca ingresamos en el modo de configuración del router Tunja, para permitir acceso al DHCP en las interfaces.

3. CONCLUSIONES

- Este trabajo me ayuda a evaluar los conocimientos que adquirí durante el diplomado de profundización de cisco, dándome cuenta de las habilidades y destrezas que tengo para la solución de problemas reales dentro del mundo de las redes.
- Aprendí a identificar más el procedimiento de enrutamiento de dispositivos dentro una red y cómo funciona él envío y la recepción de paquetes (dentro de una red).
- Afiance mis conocimientos en la configuración de dispositivos como el Router y Switches con todas las reglas de seguridad y optimización de las métricas para su buen funcionamiento.
- El aprender los protocolos de enrutamiento, el manejo de las Vlan y la seguridad que se utiliza en cada protocolo permite una segmentación adecuada de la red permitiendo el acceso rápido y seguro de la información en cualquier momento y lugar. Hoy en día cualquier empresa debe estar actualizada tecnológicamente, ofreciendo un servicio de alta calidad y disponibilidad.
- Con todos los ejercicios prácticos que se hicieron durante el diplomado aprendí a implantar las redes WAN y LAN dentro de una topología, haciendo enrutamiento dinámico y estático en el diseño de la misma, permitiendo una mejor administración de acceso y desempeño.
- Durante el diplomado utilizamos diferentes softwares para el desarrollo de los ejercicios de configuración e implementación de dispositivos y redes. En particular el simulador de Packet Tracer nos da la oportunidad de ver en tiempo real el diseño e implantación de diferentes escenarios de redes, ayudándome a colocar en práctica los conocimientos adquiridos.

4. BIBLIOGRAFÍA

Tanenbaum, Andrew S. (2003). Redes de ordenadores (Google Books) (4ª edición). Pearson Educación. ISBN 9789702601623. Consultado el 26 de enero de 2012. (la versión en línea solo ofrece una vista parcial del contenido).

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE

GRADO. {En línea}. {Consultado junio 2009}. Disponible en:
http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otros_trabajo_s_de_grado/compendio_de_tesis_y_otros_trabajos_de_grado.asp?Codigo= ESP.

Router. {En línea}. {Consultado diciembre 2019}. Disponible en:
<https://es.wikipedia.org/wiki/Router>

SWITCHER. {En línea}. {Consultado diciembre 2019}. Disponible en:
<https://www.aboutespanol.com/que-es-un-switch-841388>

OSPF . {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Open_Shortest_Path_First

EIGRP. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol
ACL. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Lista_de_control_de_acceso#cite_note-1

CNNA. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Certificaci%C3%B3n_Cisco

TFTP. {En línea}. {Consultado diciembre 2019}. Disponible en:
<https://es.wikipedia.org/wiki/TFTP>

DCHP. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

NAT. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

PAT. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/Port_address_translation

VLMS. {En línea}. {Consultado diciembre 2019}. Disponible en:
https://es.wikipedia.org/wiki/M%C3%A1scaras_de_subred_de_tama%C3%B1o_variable

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de <https://staticcourse-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>