Desarrollo de la Práctica Final
Diplomado y Profundización – Cisco Networking Academy
Diseño e Implementación de Soluciones Integradas LAN/WAN

Jayson Andrés Leyton Sarmiento

Giovanni Alberto Bracho
Tutor

Curso: 203092 A Grupo: 614

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería
Facatativá - Cundinamarca
2020

Resumen

Como es bien sabido las telecomunicaciones en el transcurso de la historia han realizado grandes aportes y acortado distancias en los diferentes oficios que el hombre desarrolla en la tierra y en el espacio, de forma concreta las telecomunicaciones son una forma de comunicarnos electrónicamente a distancia, actualmente las grandes compañías y hasta las mismas personas desean ahorrar tiempo automatizando sus procesos, los cuales les permite concentrarse en otros aspectos que les resultan importantes.

La constante necesidad que han generado los seres humanos de poder acceder a la información en cualquier momento y en cualquier lugar, han promovido que, según estimaciones de Cisco para el siguiente año es que la cantidad total de datos que se transfieren por la red serán algo más de 600 Zetta Bytes en el año, por ende y en definitiva la convergencia de la red tiene un papel fundamental en hacer llegar la información con más rapidez y más seguridad a los consumidores finales.

Por medio de un convenio entre la Universidad Nacional Abierta y a Distancia UNAD y la CISCO networking Academy, se realizó el diplomado “diseño e implementación de redes LAN/WAN” dividido en dos módulos el CCNA 1 y CCNA 2 en donde se han adquirido conocimientos de cómo funcionan las redes de forma física y lógica hasta temas más complejos como el diseño y la implementación de redes realizando conectividad entre dispositivos que se encuentran a grandes distancias.

Abstract

As it is well known, telecommunications throughout history have made great contributions and shortened distances in the different trades that man develops on the earth and in space, specifically, telecommunications are a way of communicating electronically at a distance, currently, large companies and even the same people want to save time by automating their processes which allow them to focus on other aspects that are important to them.

The constant need that human beings have generated to be able to access information at any time and in any places, have promoted that, according to Cisco estimates for the following year, the total amount of data that is transferred through the network will be just over 600 Zetta Bytes in the year, therefore and ultimately the convergence of the network has a fundamental role in delivering the information faster and safer to the final consumers.

Through an agreement between Universidad Nacional Abierta y a Distancia UNAD and the CISCO networking Academy, the course “diseño e implementación de redes LAN/WAN” was done and it was divided into two modules CCNA 1 and CCNA 2 where knowledge of how networks work physically and logically has been acquired to more complex topics such as the design and implementation of networks, making connectivity between devices that are at great distances.

TABLA DE CONTENIDO

INTRODUCCION

Por medio del siguiente trabajo llamado “examen final de habilidades prácticas”, el cual pertenece al Diplomado de profundización CISCO, “diseño e implementación de soluciones integradas de redes LAN/WAN” nos permite ampliar los conocimientos bases que se obtuvieron a través de la carrera Ingeniería de Sistemas, dicho informe está conformado por una red de computadores simulada por medio de la aplicación Packet Tracer, el propósito principal del diplomado y la plataforma es ser aplicado como un sistema educativo para aprender por descubrimiento.

Se abordaran dos escenarios en donde se aplicaran las respectivas técnicas para la comprensión y resolución de problemas que podemos tener en situaciones de la vida real entre ellos la inicialización y configuración inicial de dispositivos de red como routers, servidores, switches, teléfonos, puntos de acceso y computadores; Implementación de routing, configuración de OSPF, creación de VLANS, implementación de DHCP, NAT y verificación de las ACL.

Con la terminación de dicho diplomado el futuro ingeniero de sistemas expondrá por medio de este la redacción del paso a paso en el desarrollo de los dos escenarios presentados junto con ilustraciones y códigos ejecutados en la aplicación Packet Tracer nombrada anteriormente.

OBJETIVOS

Objetivo General

Aplicar todos los conocimientos adquiridos a través de la carrera y en el diplomado de profundización para identificar y aplicar una correcta solución a los dos escenarios implementados por la Cisco Networking Academy, cabe resaltar que dichos escenarios pueden darse en la vida real, por ende se deben aplicar habilidades teóricas y prácticas.

Se debe aplicar una correcta documentación e inserción de ilustraciones que conlleven a un correcto entendimiento de la solución de aplicada a cada escenario.

Objetivos Específicos

- Diseñar, analizar y seleccionar los dispositivos adecuados de acuerdo a la topología de red y esquemas de direccionamiento solicitado.
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores y computadores.
- Implementar una óptima seguridad en los Switch, creación de Vlans e inter Vlan Routing.
- Determinar la configuración necesaria para la implementación de EIGRP, que es un protocolo dinámico de Routing.
- Configurar y verificar listas de control de acceso ACL
- Configurar el enrutamiento OSPF con la autenticación en cada router.
- Verificar por medio de trazas o comando PING la óptima conectividad de la red, realizar pruebas entre dispositivos verificando correcto funcionamiento.

Evaluación – Prueba de Habilidades Prácticas CCNA

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros**.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer o GNS3.**

• Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL y OBLIGATORIA.

• Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

Descripción de escenarios propuestos para la prueba de habilidades

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 establece dos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología de red

Los requerimientos solicitados son los siguientes:

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

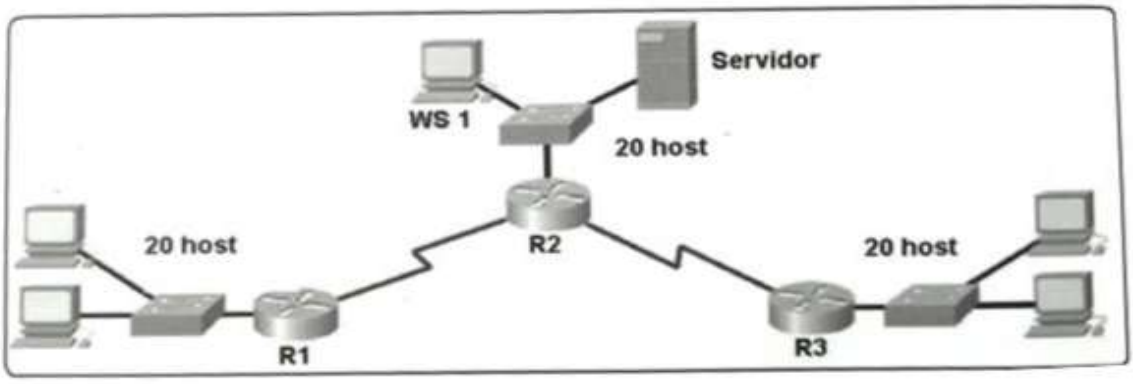
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

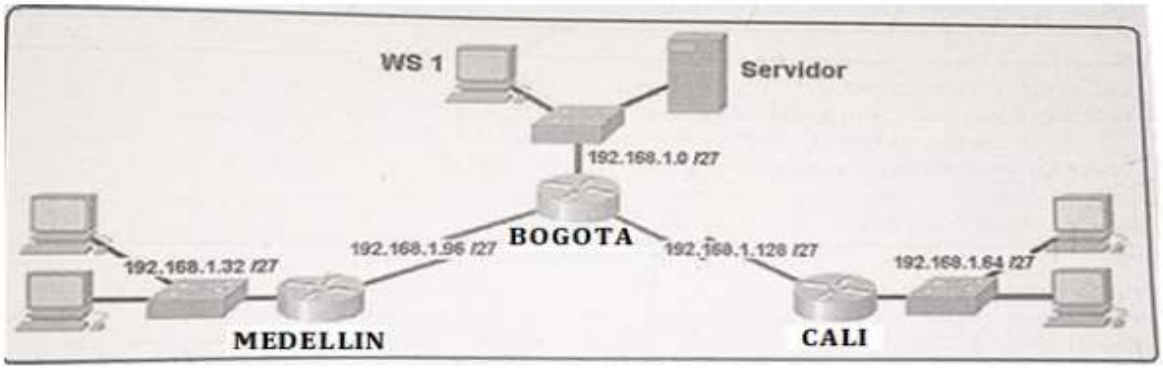
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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

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

Parte 6: Configuración final.





Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Como primera instancia se seleccionan los dispositivos que se utilizaran en la implementación de la red en Packet Tracer, dichos dispositivos son:

- 3 Router CISCO 1841
- 5 PC´S
- 1 Servidor
- 3 Switches Cisco Catalyst 2950 series
- Cables de red

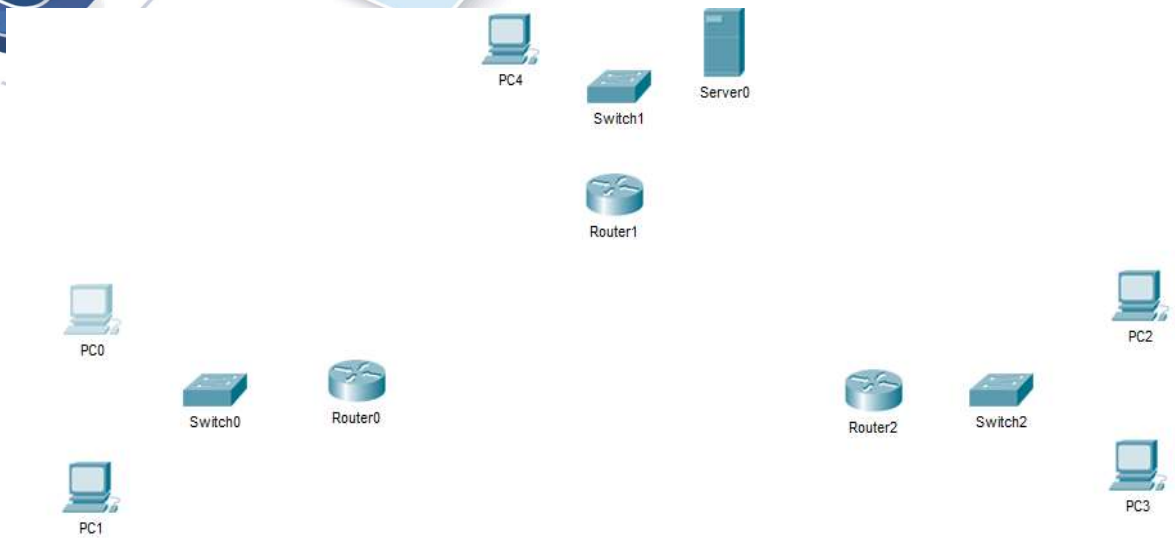


Ilustración 1: Implementando la red

Para cada uno de los routers se debe apagar el dispositivo en la pestaña Physical y dar clic como se muestra en la siguiente ilustración.

Ilustración 2: Apagado de router cisco 1841

Seguido de esto damos clic en la pestaña llamada **MODULES** que está dentro de la pestaña Physical y seleccionamos **WIC-1T** esto para permitir la conectividad **WAN** entre los demás routers.

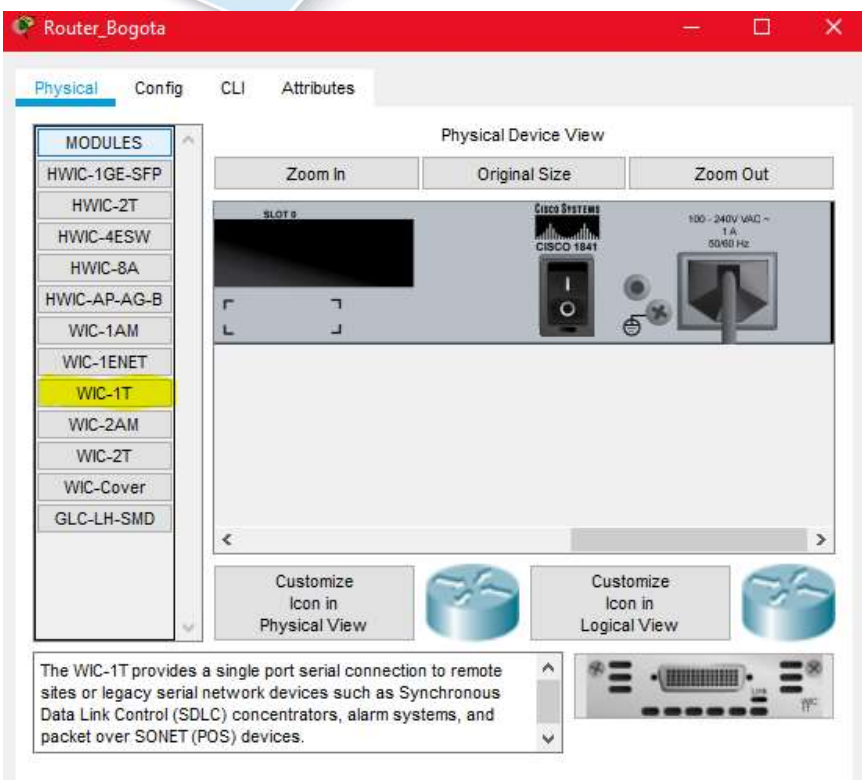


Ilustración 3: Selección WIC-1T

Una vez seleccionado el módulo **WIC-1T** lo arrastramos al Slot 0 y Slot 1 del router y debe quedar como en la siguiente ilustración.

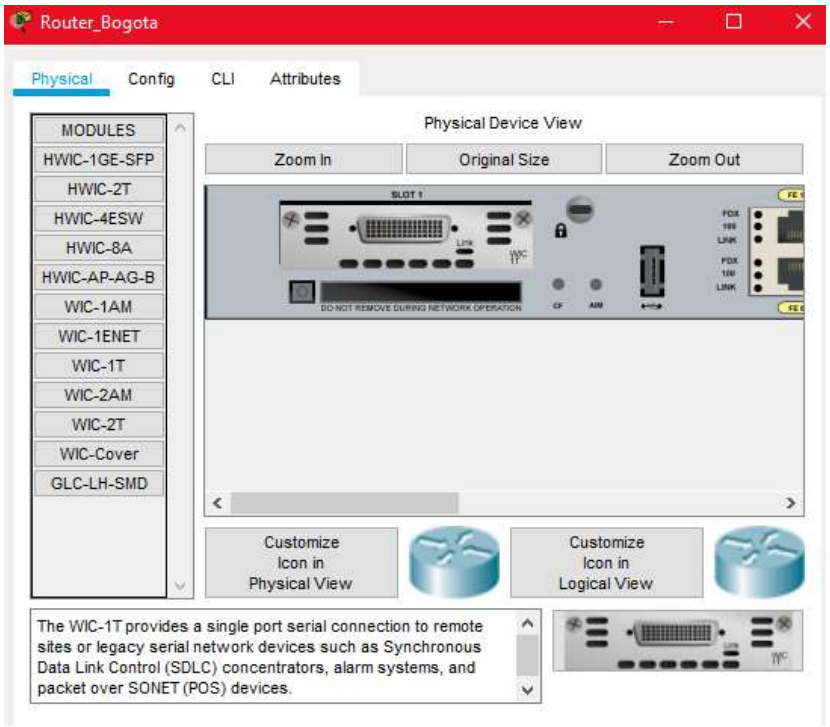


Ilustración 4: Modulo WIC-1T en Slot 1

Una vez instaladas las tarjetas en los routers, encendemos los routers y comenzamos con la configuración inicial de cada uno de los mismos. En dicha configuración se le asigna un nombre al router, contraseñas de seguridad y mensaje de seguridad de conexión no autorizada a los mismos.

Configuración router Bogotá

Router>enable

Router#configure terminal

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

Router(config)#hostname Bogota

Bogota(config)#no ip domain-lookup

Bogota(config)#enable secret class

Bogota(config)#line console 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)#exit

Bogota(config)#service password-encryption

Bogota(config)#banner motd # Se iniciaran acciones legales en caso de uso no autorizado de este dispositivo #

Bogota(config)#exit

Configuración router Medellin

Router>enable

Router#configure terminal

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

Router(config)#hostname Medellin

Medellin(config)#no ip domain-lookup

Medellin(config)#enable secret class

Medellin(config)#line console 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)#exit

Medellin(config)#service password-encryption

Medellin(config)#banner motd # Se iniciaran acciones legales en caso de uso no autorizado de este dispositivo #

Medellin(config)#exit

Configuración router Cali

Router>enable

Router#configure terminal

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

Router(config)#hostname Cali

Cali(config)#no ip domain-lookup

Cali(config)#enable secret class

Cali(config)#line console 0

Cali(config-line)#password cisco

Cali(config-line)#login

Cali(config-line)#line vty 0 4

Cali(config-line)#password cisco

Cali(config-line)#login

Cali(config-line)#exit

Cali(config)#service password-encryption

Cali(config)#banner motd # Se iniciaran acciones legales en caso de uso no autorizado de este dispositivo #

Cali(config)#exit

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

Seleccionamos cables de red y comenzamos a cablear la red, para la conexión entre routers se utiliza el cable serial DTE de color rojo, nuestra red queda de la siguiente manera:

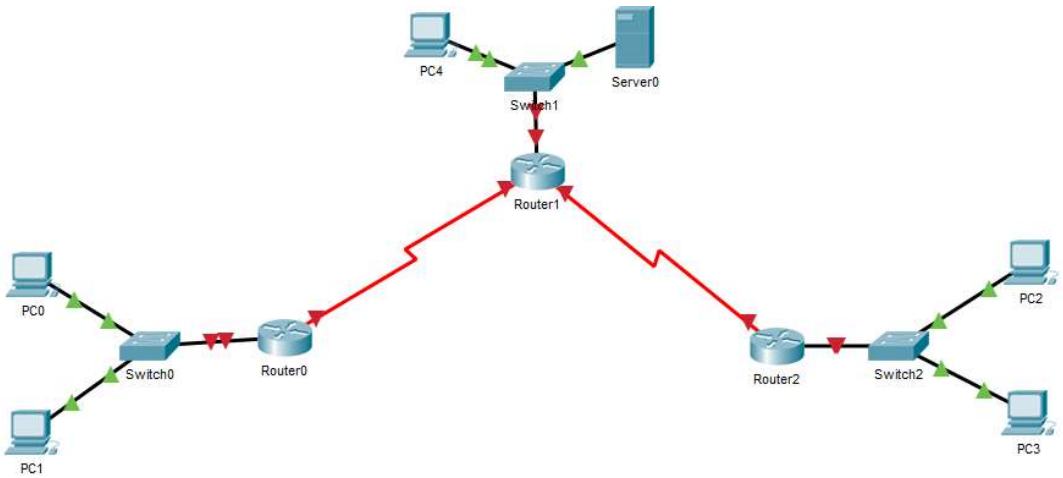


Ilustración 5: Cableado de la red

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

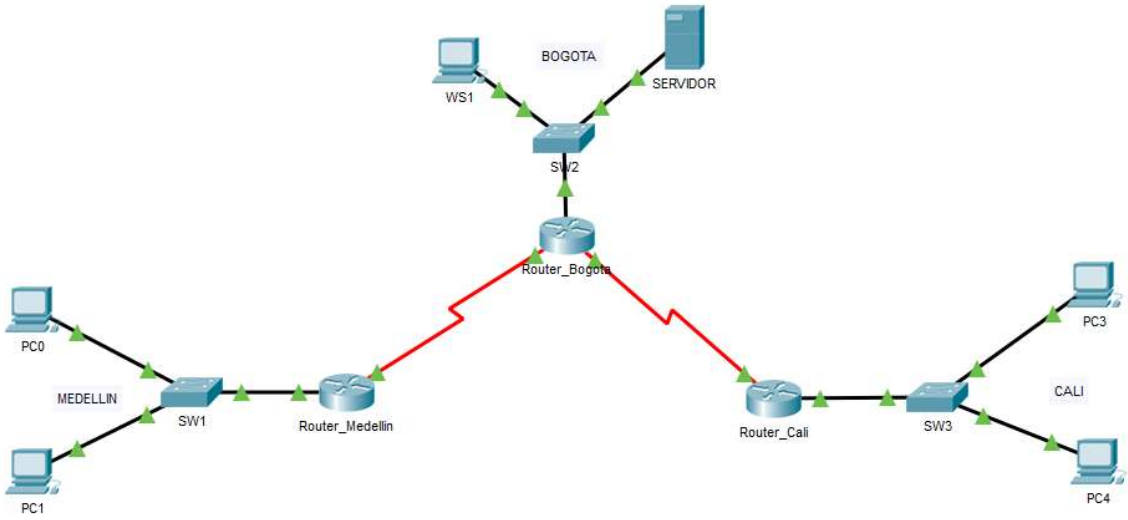


Ilustración 6: Red cableada

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**.**

Para realizar el subneteo tomamos como referencia las IP´s de la interfaz FA 0/0 en cada uno de los router entregadas en la tabla de configuración básica. Como podemos apreciar tiene saltos de 30 host cada una por tener mascara 27 por ende el subneting realizado queda de la siguiente manera:

	Bogotá	**Reservadas para crecimiento**	
IP Inicial	192.168.1.1	**IP inicial**	192.168.1.97
Mask	27 255.255.255.224	**Mask**	27 255.255.255.224
GW	192.168.1.1 192.168.1.2 al	**GW**	192.168.1.97 192.168.1.98 al
LAN	192.168.1.30	**LAN**	192.168.1.126

Medellín			
IP Inicial	192.168.1.33	**IP inicial**	192.168.1.129
Mask	27 255.255.255.224	**Mask**	27
GW	192.168.1.33 192.168.1.34 al	**GW**	192.168.1.129 192.168.1.130 al
LAN	192.168.1.62	**LAN**	192.168.1.158

Cali			
IP Inicial	192.168.1.65	**IP inicial**	192.168.1.161
Mask	27 255.255.255.224	**Mask**	27 255.255.255.224
GW	192.168.1.65 192.168.1.66 al	**GW**	192.168.1.161 192.168.1.162 al
LAN	192.168.1.94	**LAN**	192.168.1.190

b. Asignar una dirección IP a la red.

IP DE RED: 192.168.1.3

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

	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	192.168.1.97	192.168.1.130	192.168.1.129
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

Ahora teniendo la tabla de subnetting procedemos a realizar la configuración de dicho direccionamiento en cada uno de los routers.

Router Medellín

Medellin(config)#

Medellin(config)#interface Serial 0/0/0

Medellin(config-if)#ip ad

Medellin(config-if)#ip address 192.168.1.99 255.255.255.224

Medellin(config-if)#no sh

Medellin(config-if)#no shutdown

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

Medellin(config-if)#exit

Medellin(config)#interface fa

Medellin(config)#interface fastEthernet 0/0

Medellin(config-if)#ip ad

Medellin(config-if)#ip address 192.168.1.33 255.255.255.224

Medellin(config-if)#no sh

Medellin(config-if)#no shutdown

Medellin(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

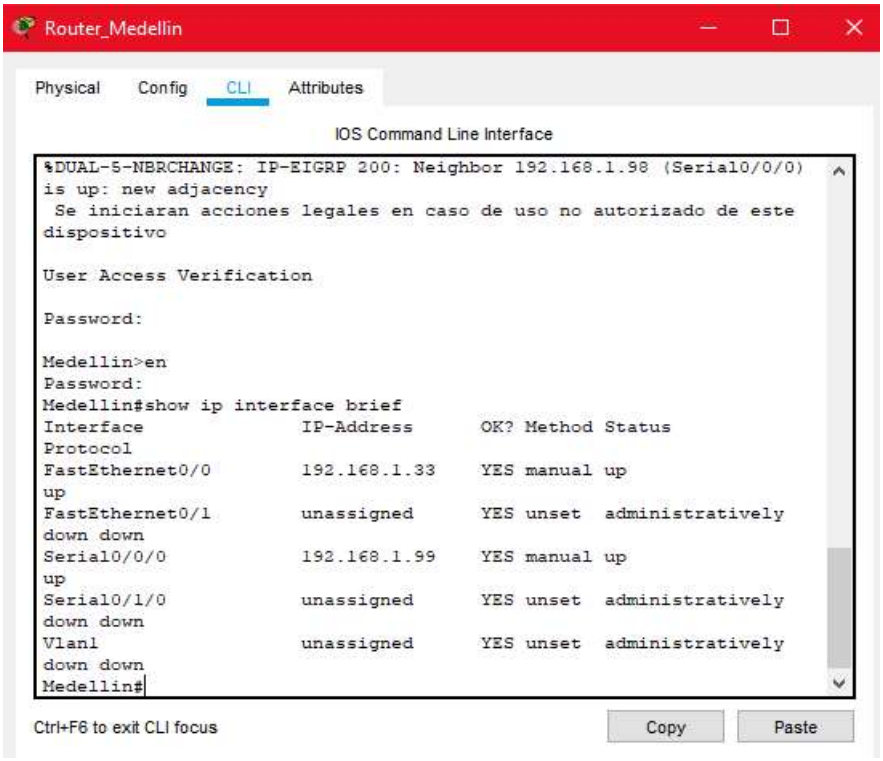


Ilustración 7: Interfaces configuradas en router Medellín

Router Bogotá

Bogota(config)#

Bogota(config)#interface Serial 0/0/0

Bogota(config-if)#ip ad

Bogota(config-if)#ip address 192.168.1.98 255.255.255.224

Bogota(config-if)#no sh

Bogota(config-if)#no shutdown

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

Bogota(config-if)#exit

Bogota(config)#interface Serial 0/1/0

Bogota(config-if)#ip ad

Bogota(config-if)#ip address 192.168.1.130 255.255.255.224

Bogota(config-if)#no sh

Bogota(config-if)#no shutdown

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

Bogota(config-if)#exit

Bogota(config)#interface fa

Bogota(config)#interface fastEthernet 0/0

Bogota(config-if)#ip ad

Bogota(config-if)#ip address 192.168.1.1 255.255.255.224

Bogota(config-if)#no sh

Bogota(config-if)#no shutdown

Bogota(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

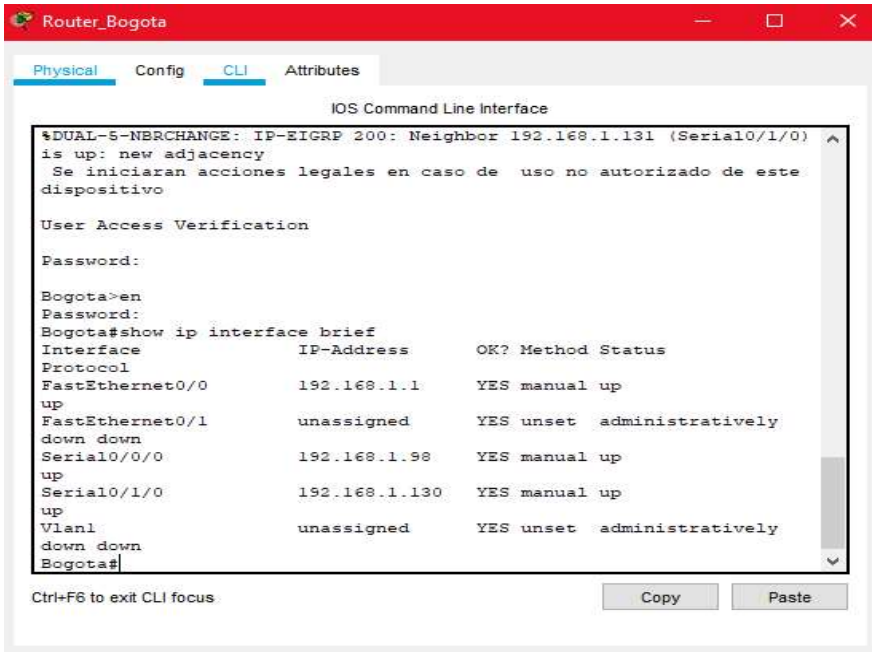


Ilustración 8: Interfaces configuradas en router Bogotá

Router Cali

Cali(config)#

Cali(config)#interface Serial 0/0/0

Cali(config-if)#ip ad

Cali(config-if)#ip address 192.168.1.131 255.255.255.224

Cali(config-if)#no sh

Cali(config-if)#no shutdown

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

Cali(config-if)#exit

Cali(config)#interface fa

Cali(config)#interface fastEthernet 0/0

Cali(config-if)#ip ad

Cali(config-if)#ip address 192.168.1.65 255.255.255.224

Cali(config-if)#no sh

Cali(config-if)#no shutdown

Cali(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

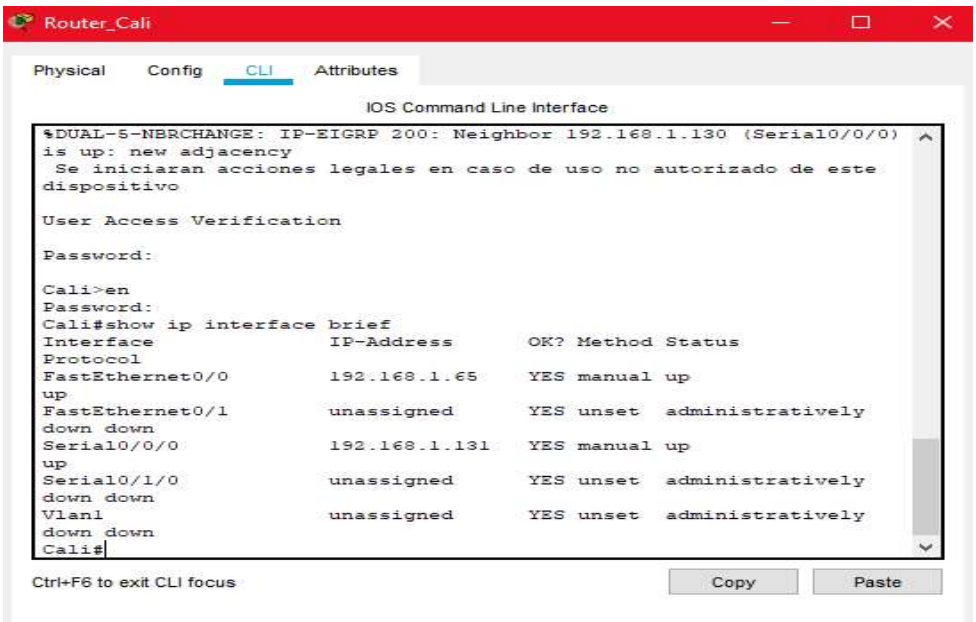


Ilustración 9: Interfaces configuradas router Cali

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.

Router Medellín

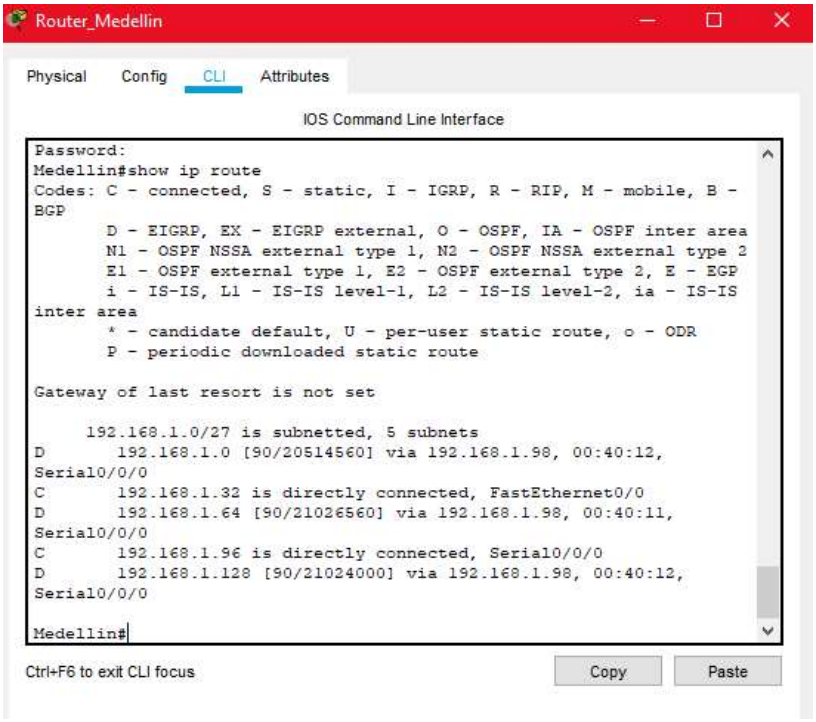


Ilustración 10: Tabla de enrutamiento Router Medellín

Router Bogotá

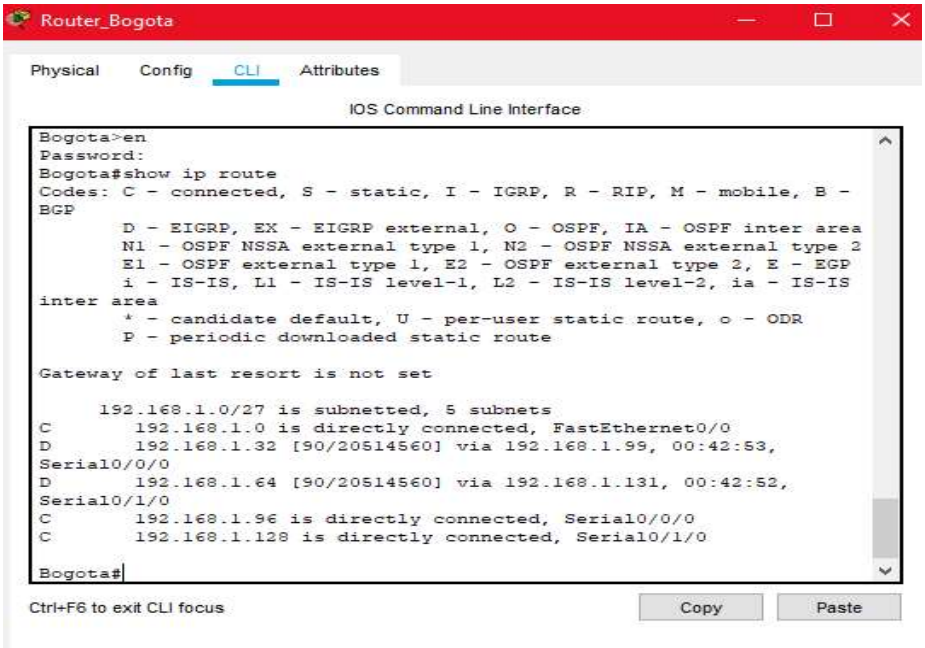


Ilustración 11: Tabla de enrutamiento Router Bogotá

Router Cali

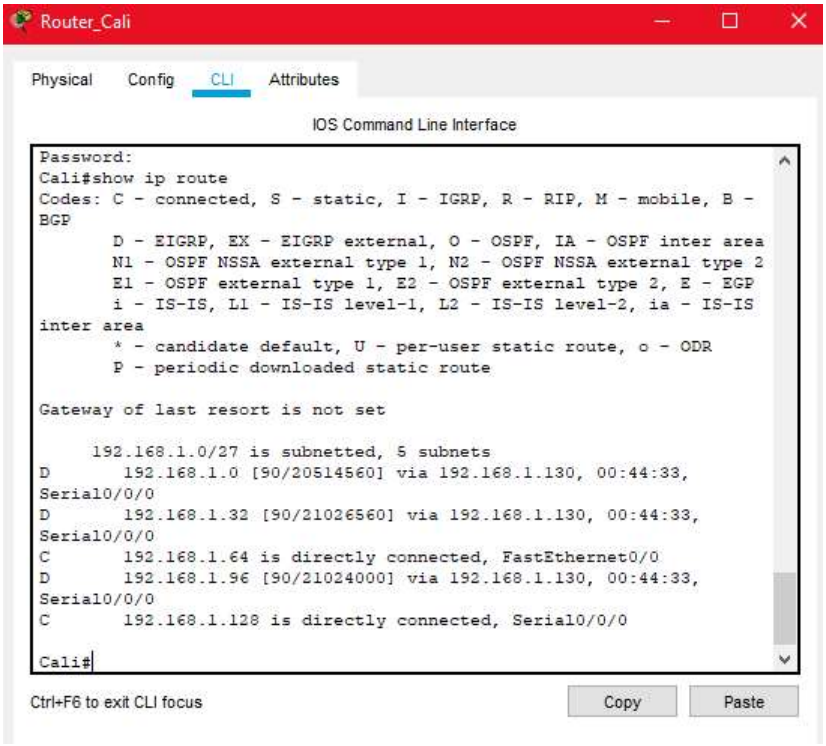


Ilustración 12: Tabla de enrutamiento Router Cali

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

Como podemos apreciar en la siguiente imagen, por medio del comando **show ip eigrp topology** vemos el óptimo balanceo de carga que tienen los 3 routers y el sistema autónomo asignado por la tabla dada que es **200.**

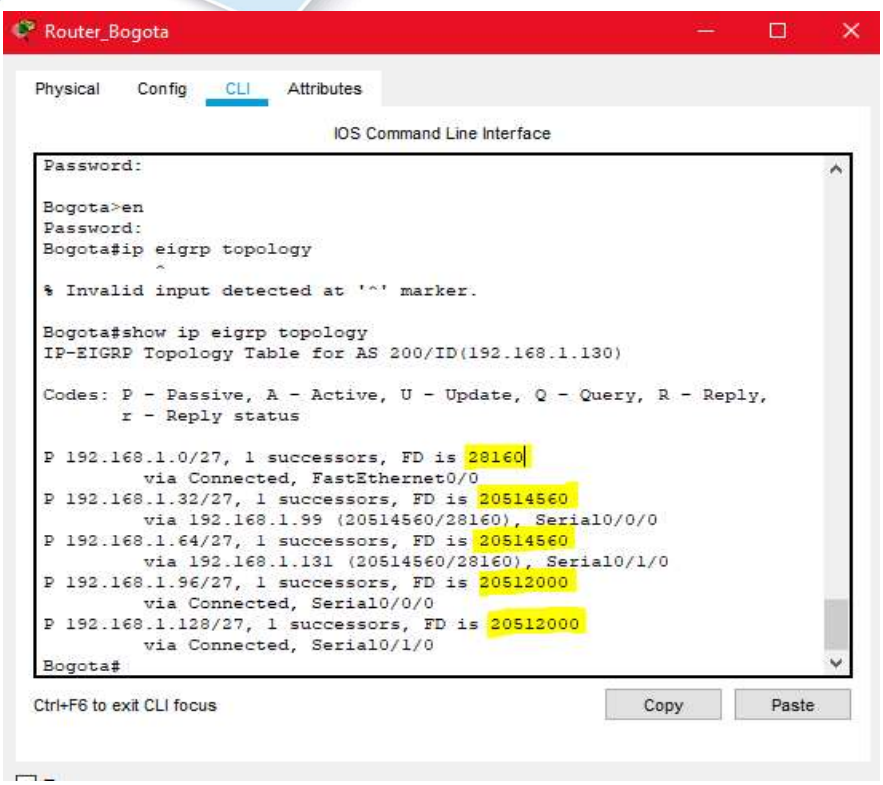


Ilustración 13: Tabla de balanceo de cargas de los routers

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

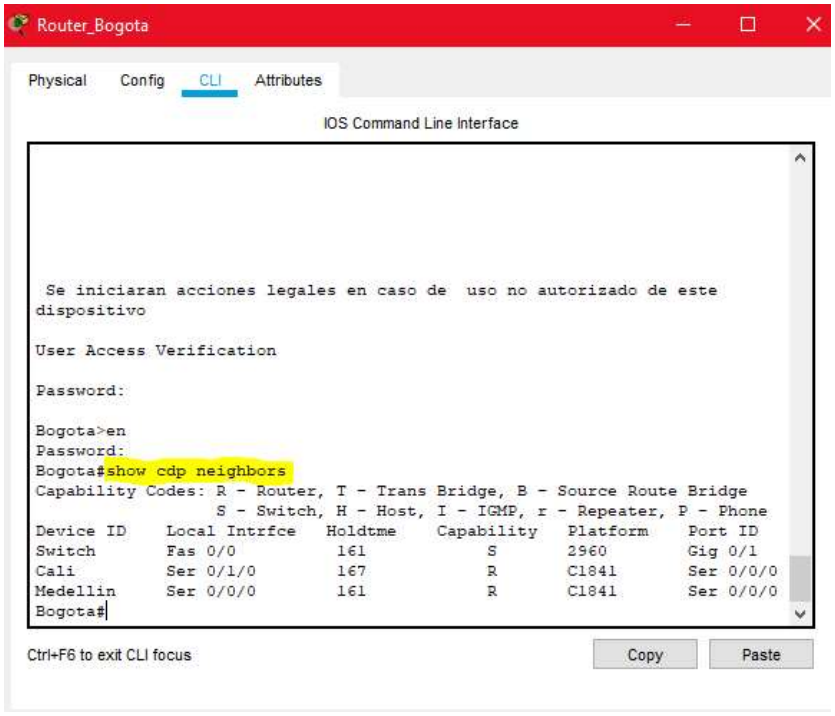


Ilustración 14: Diagnostico de vecinos desde el router Bogotá

Como podemos apreciar ejecutando el comando **Show cdp neighbors** podemos ver los routers de Cali y Medellín, si ejecutamos este mismo comando en los otros routers también nos mostrara los otros dos routers de la red.

Esta es la descripción de cada uno de los ítems presentados al ejecutar este comando.

- **Device ID:** Hostname del dispositivo vecino. Si no hay un hostname disponible se indica la dirección MAC o el número de serie del dispositivo.
- **Local Intrfce:** Interface del dispositivo en el cual se ejecuta el comando, a través de la cual se recibe la información CDP del dispositivo vecino.
- **Holdtime**: Tiempo remanente en segundos por el cual este dispositivo aguardará una nueva actualización del dispositivo vecino, antes de descartar la entrada.
- **Capability:** Tipo de dispositivo que ha generado la información CDP que se ha recibido. Puede ser un router (R), bridge transparente (B), switch (S), host (H), dispositivo IGMP (I) o repetidor (r)
- **Platform:** ID de producto o modelo de dispositivo vecino del cual se ha recibido la información.
- **Port ID:** ID de puerto del dispositivo vecino que generó el paquete de información que se ha recibido.

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

Ping desde PC_Med1 a Router Medellin

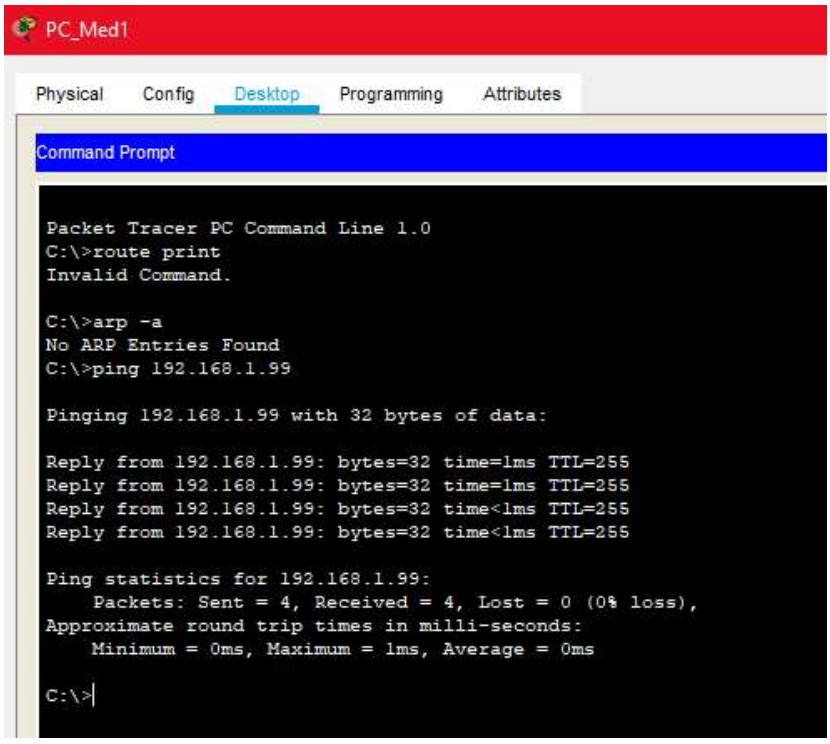


Ilustración 15: Prueba ping desde pc_Med1 a Router Medellín

Ping desde Router Medellin a Router Bogotá

Ilustración 16: Prueba ping desde Router Medellín a Router Bogotá

Ping desde Router Bogotá a WS1

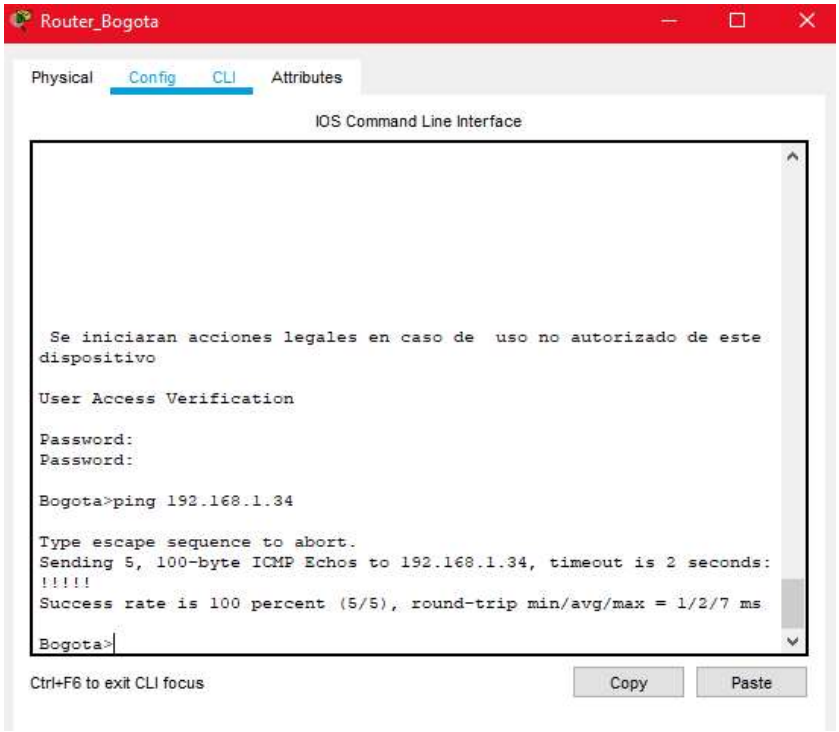


Ilustración 17: Prueba ping desde Router Bogotá a WS1

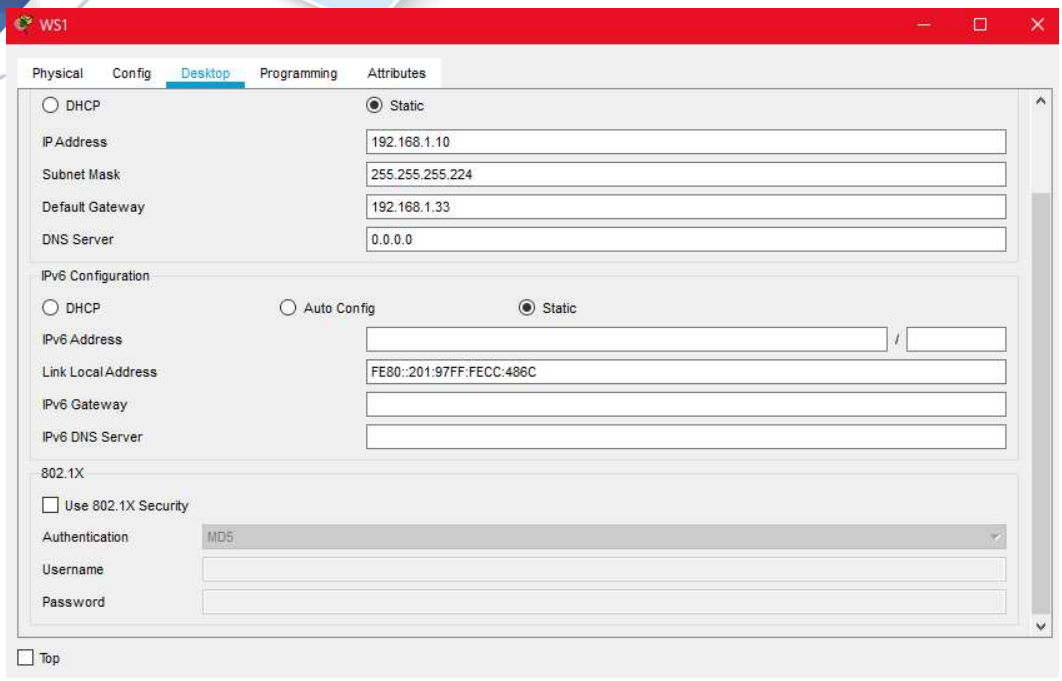


Ilustración 18: IP configurada en WS1

Ping desde Router Bogotá a Router Cali

Ilustración 19: Prueba ping desde router Bogotá a router Cali

Ping desde Router Cali a PC_Cali2

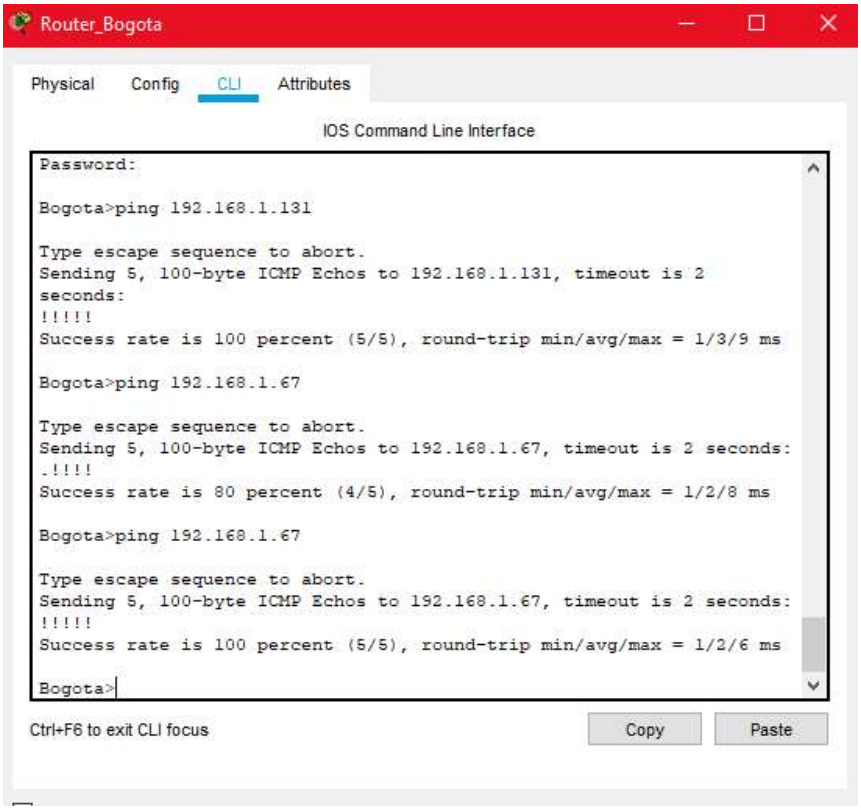


Ilustración 20: Prueba ping desde router Cali a PC_Cali2

Parte 3: Configuración de Enrutamiento.

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

Para cada uno de los routers se ejecuta el siguiente comando, se asigna el **ID 200** porque ese es el sistema autónomo que solicitan en la tabla.

Medellin#conf

Medellin#configure t

Medellin#configure terminal

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

Medellin(config)#router eigrp 200

Medellin(config-router)#net

Medellin(config-router)#network 192.168.1.0

Medellin(config-router)#

%LINK-5-CHANGED: IP-EIGRP 200: Neighbor 192.168.1.90 (Serial0/0/0) is up: new adjacency

Medellin(config-router)#do wr
Building configuration...
[OK]
Medellin(config-router)#

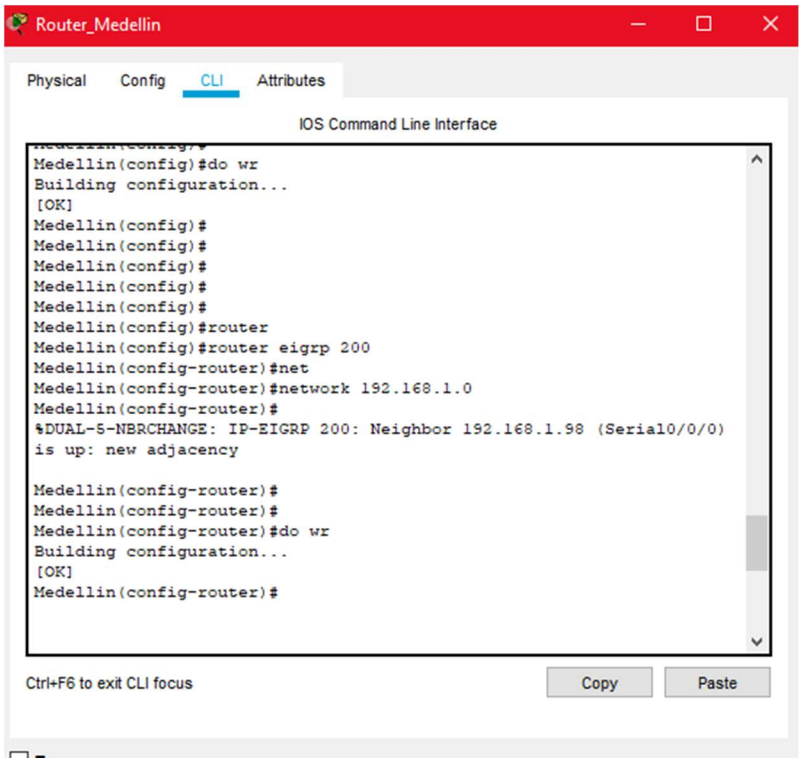


Ilustración 21: Ejecución comando router eigrp 200

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

Para verificar dicha vecindad lo verificamos desde el router de Bogotá que esta enlazado a los otros dos routers (Medellín- Cali), por ende desde aquí podemos certificar que dicho protocolo entre vecinos se está aplicando correctamente.

EIGRP incrementa el crecimiento potencial de la red reduciendo el tiempo de convergencia. Esto se consigue con las siguientes características:

- DUAL
- Redes libres de bucles.
- Actualizaciones incrementales
- Direccionamiento de multicast para actualizaciones.
- Protocolo vector distancia avanzado.
- Tabla de routing libres de bucles.
- Soporte para diferentes tecnologías.
- Convergencia rápida.
- Utilización de ancho de banda reducido.
- Configuración sencilla.
- Utilización de métrica compuesta.
- Balanceo de carga entre enlaces de coste diferente.

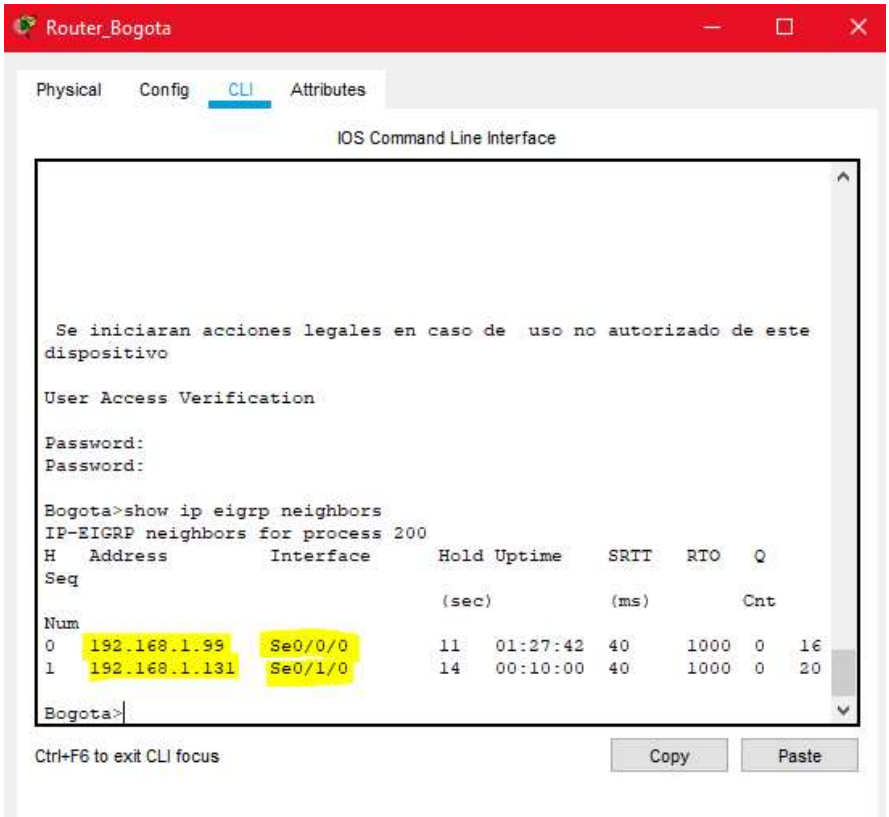


Ilustración 22: Vecindad entre routers

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

Tabla de routing Router_Bogota

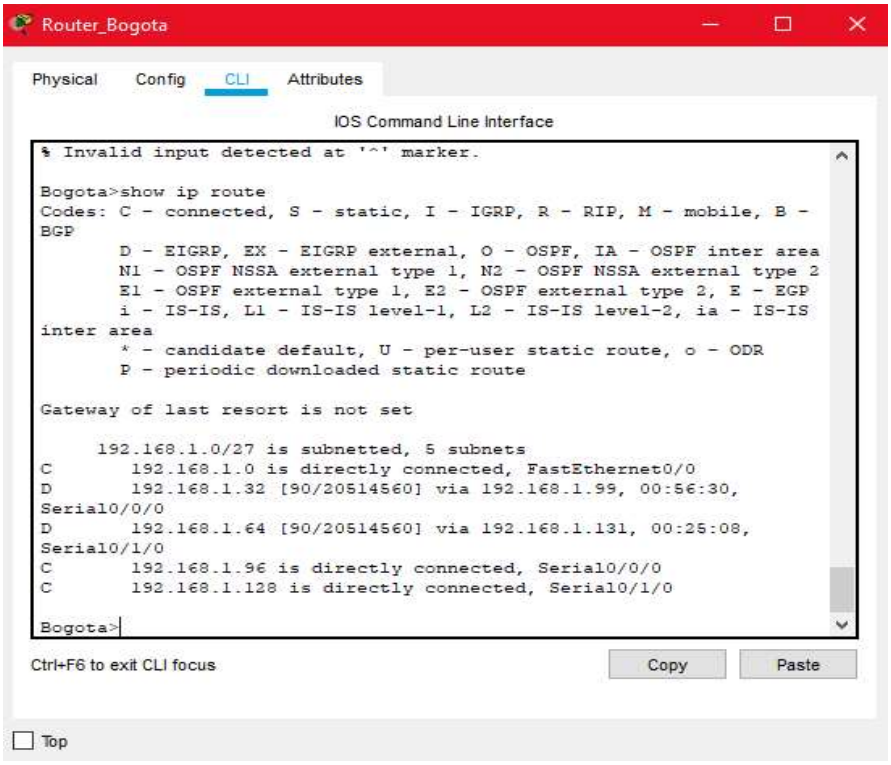


Ilustración 23: Tabla routing en Bogotá

Tabla de routing Router_Medellin

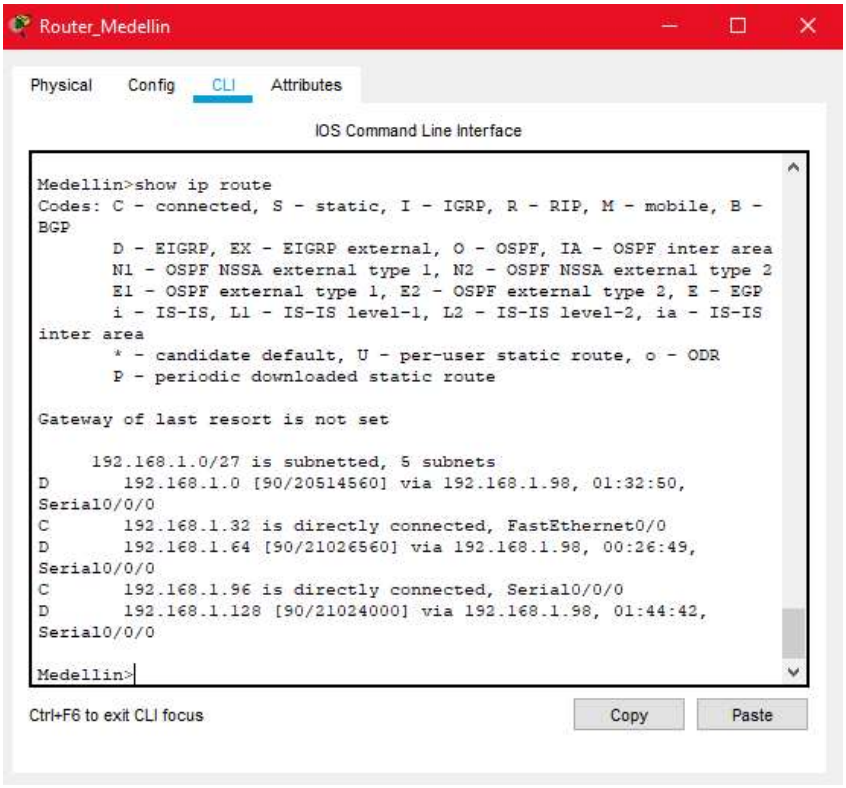


Ilustración 24: Tabla routing en Medellin

Tabla de routing Router_Cali

Ilustración 25: Tabla routing en 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.

Ping desde PC_Cali1 a PC_Med1

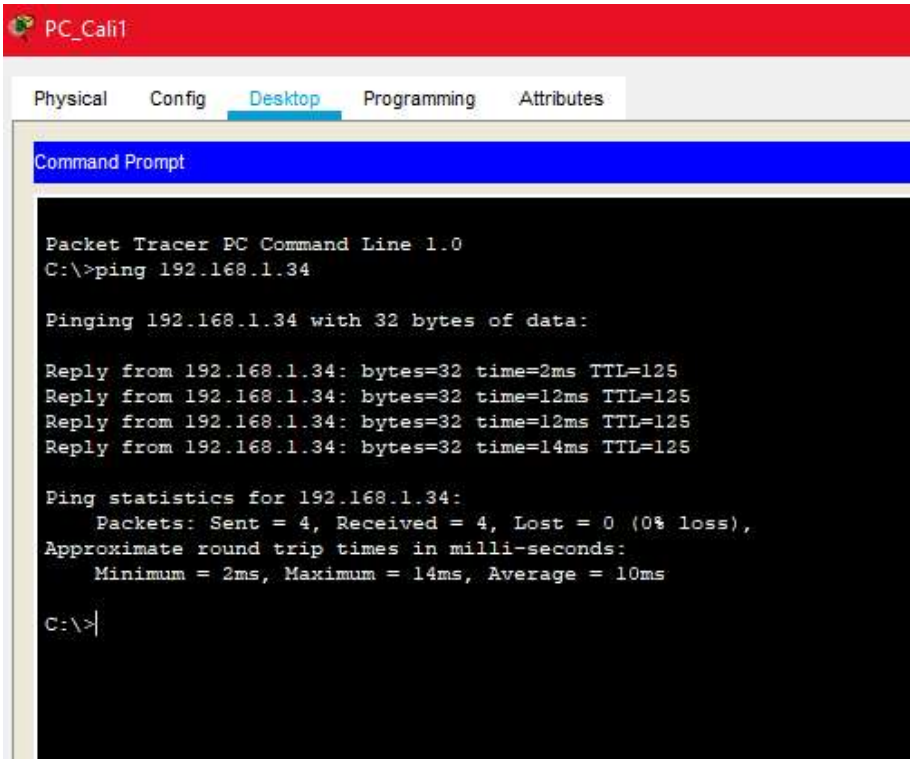


Ilustración 26: Ping entre equipos de diferentes sedes

Ping PC_Cali1 al Servidor

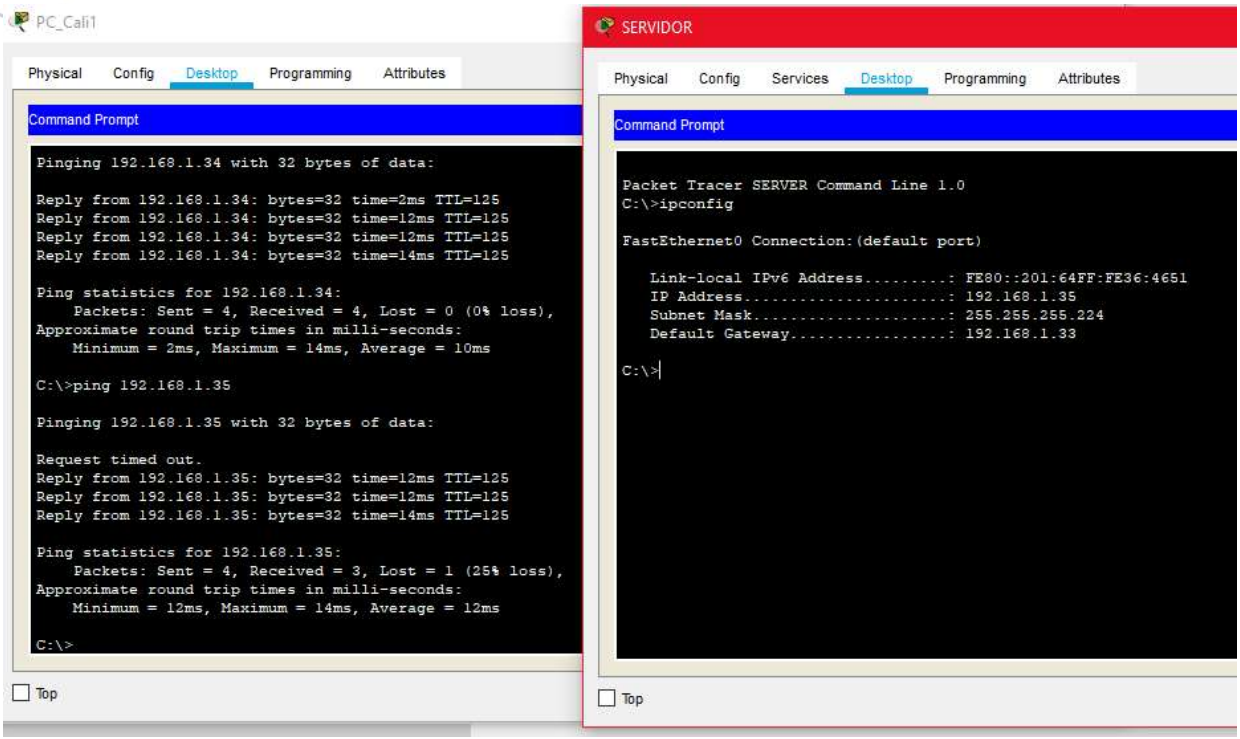


Ilustración 27: Ping desde pc Cali al servidor

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.

Telnet de Router Medellin a Router Bogotá

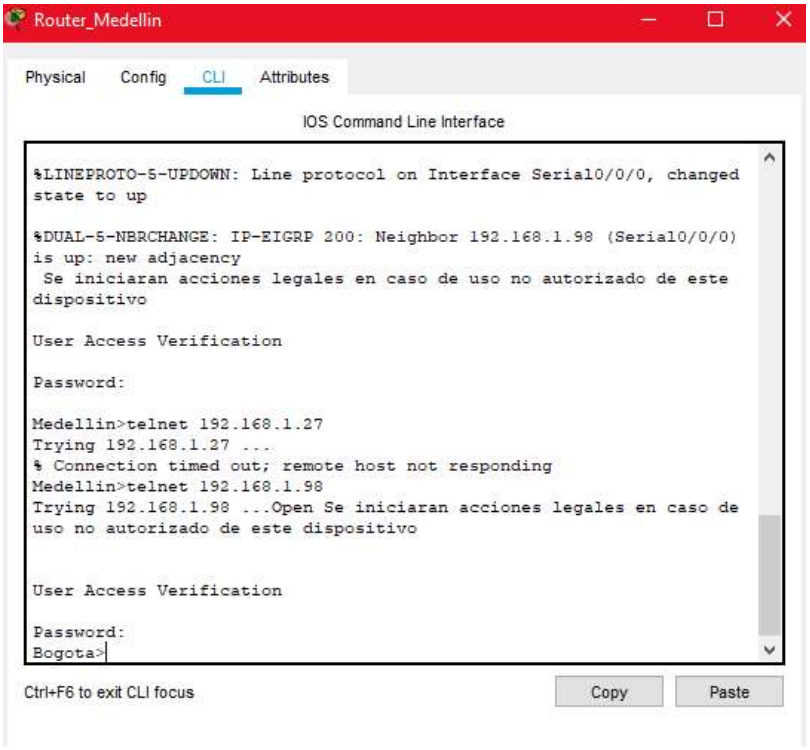


Ilustración 28: Telnet entre routers

Telnet de Router Cali a Router Bogotá

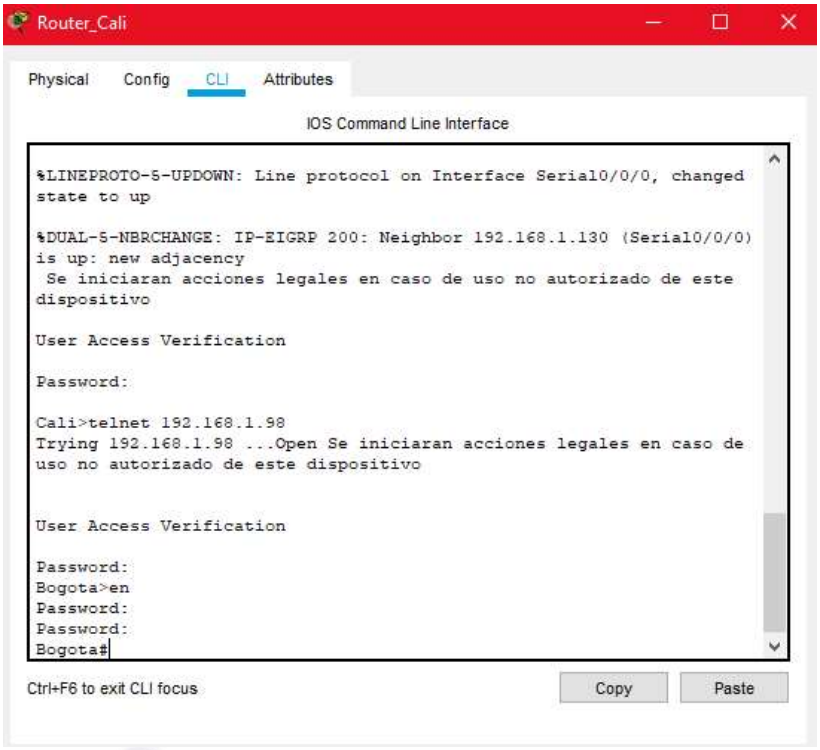


Ilustración 29: Telnet entre routers 2

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

Para verificar dicha propuesta realizamos un **Tracert** que nos muestra los saltos que hará desde el servidor hasta los equipos de otras redes.

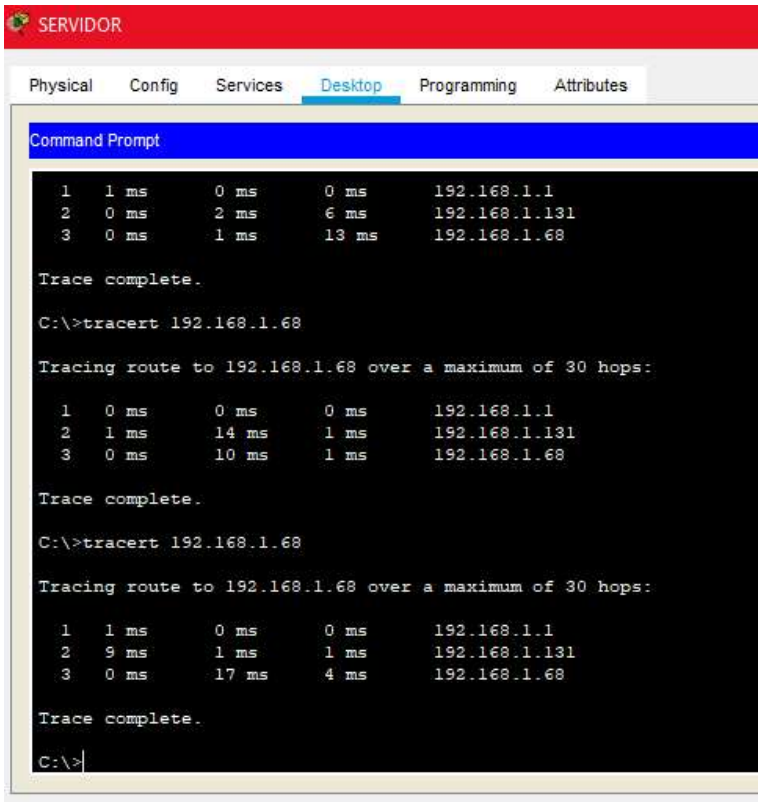


Ilustración 30: Tracert de Servidor a PC_Cali1

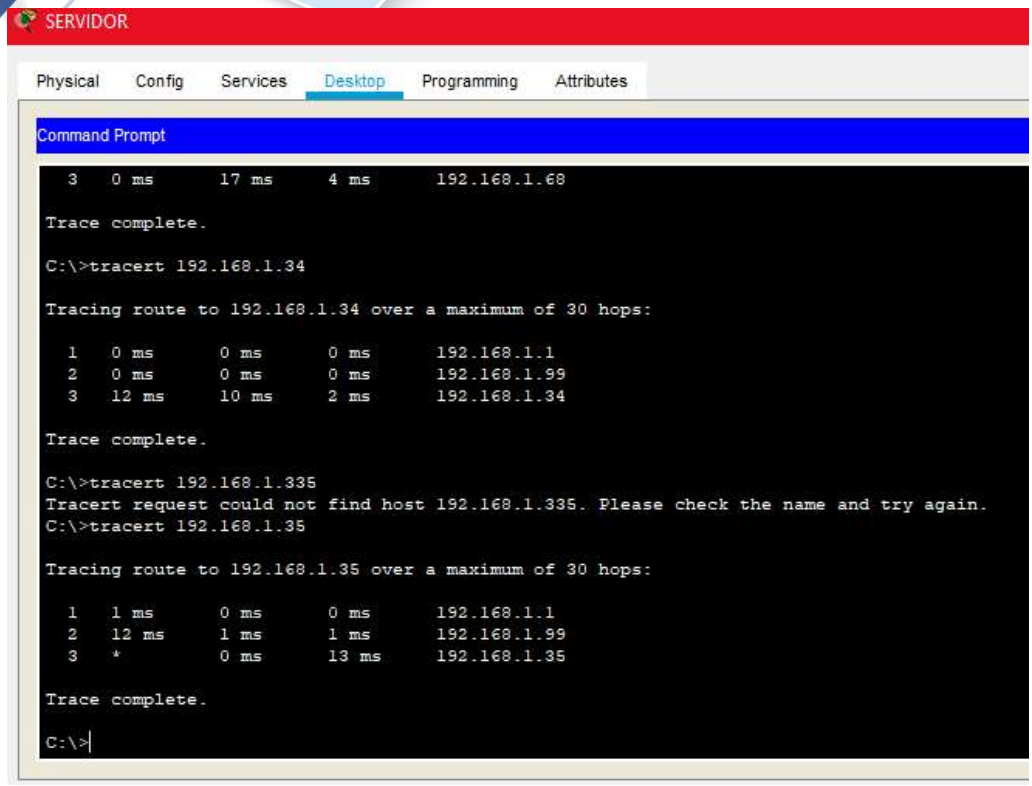


Ilustración 31: Tracert de Servidor a PC_Med1

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.

Primero dejo pruebas de ping desde **PC_Med1** al **WS1** y al **servidor**

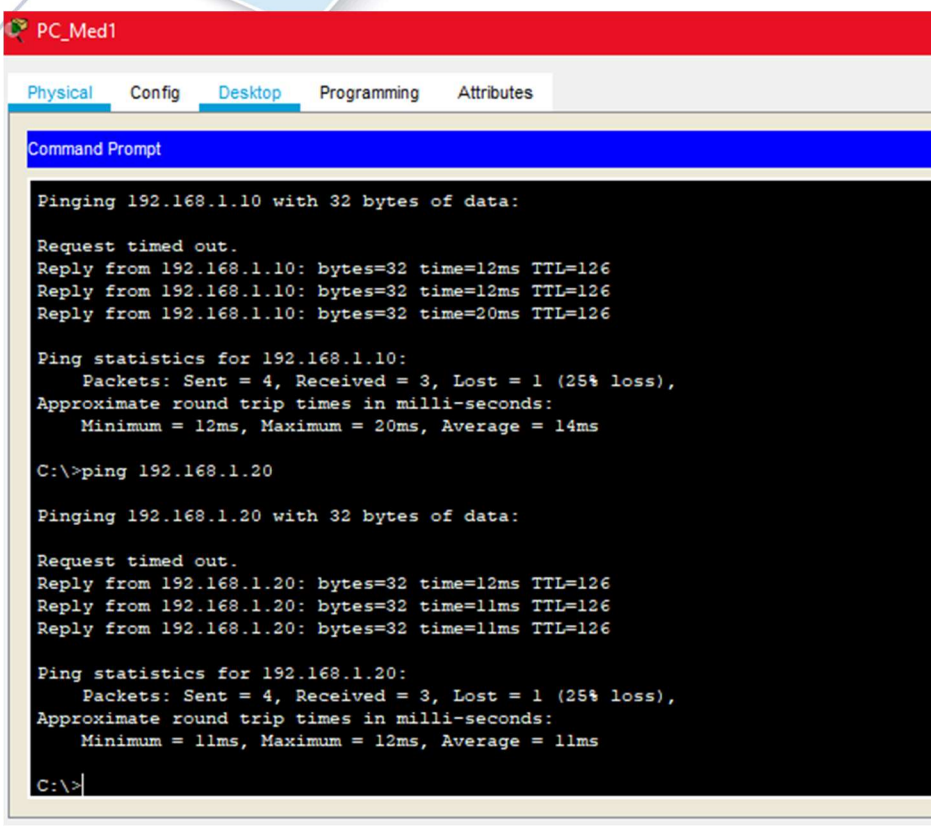


Ilustración 32: Pruebas de ping hacia red administrativa

Ahora configuramos el router de Bogotá con las CPL o listas de acceso para que ninguno de los equipos de Medellín y Cali pueda acceder a la red de Bogotá, esto lo verificamos por medio de prueba PING.

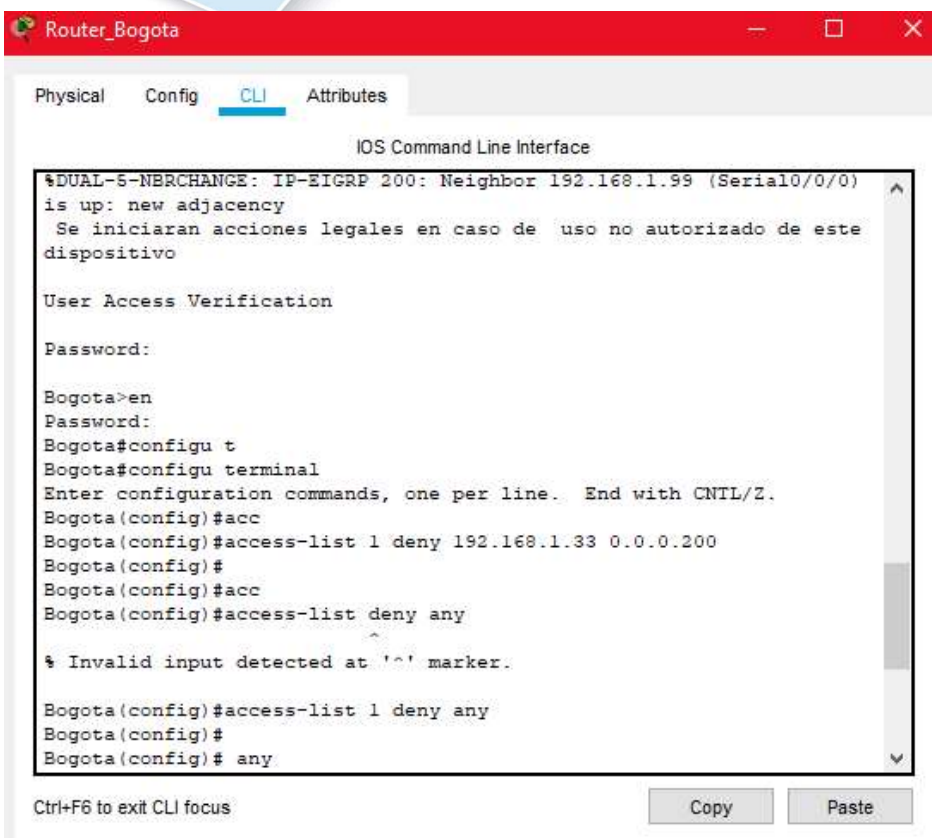


Ilustración 33: Configuración listas de acceso

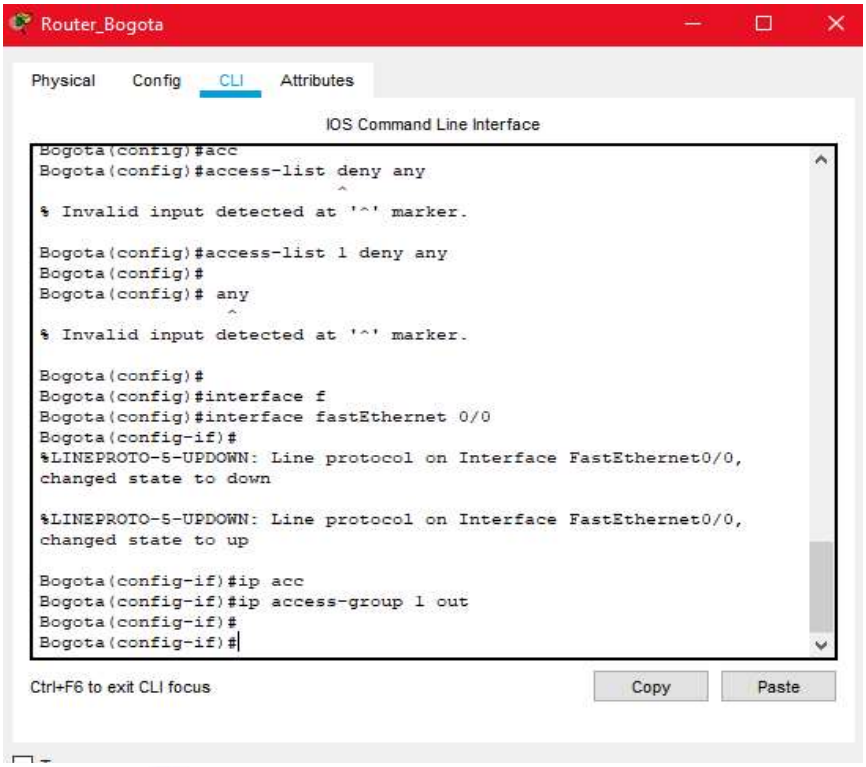


Ilustración 34: Configuración listas de acceso 2

Ahora realizamos la prueba de **PING** que hicimos al comienzo y cómo podemos apreciar dice: **Destination Host Unreacheable**

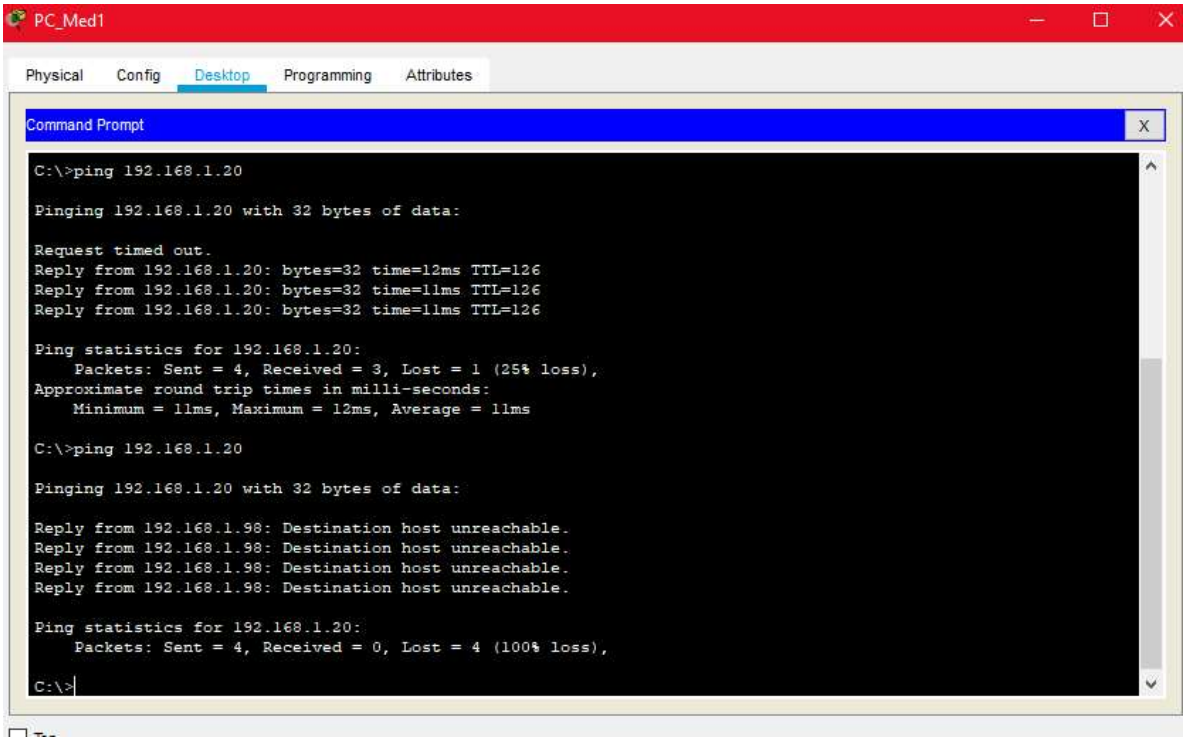


Ilustración 35: verificación de CPL configuradas

Realizamos la misma prueba de ping desde un equipo de la red de Cali y este es el resultado.

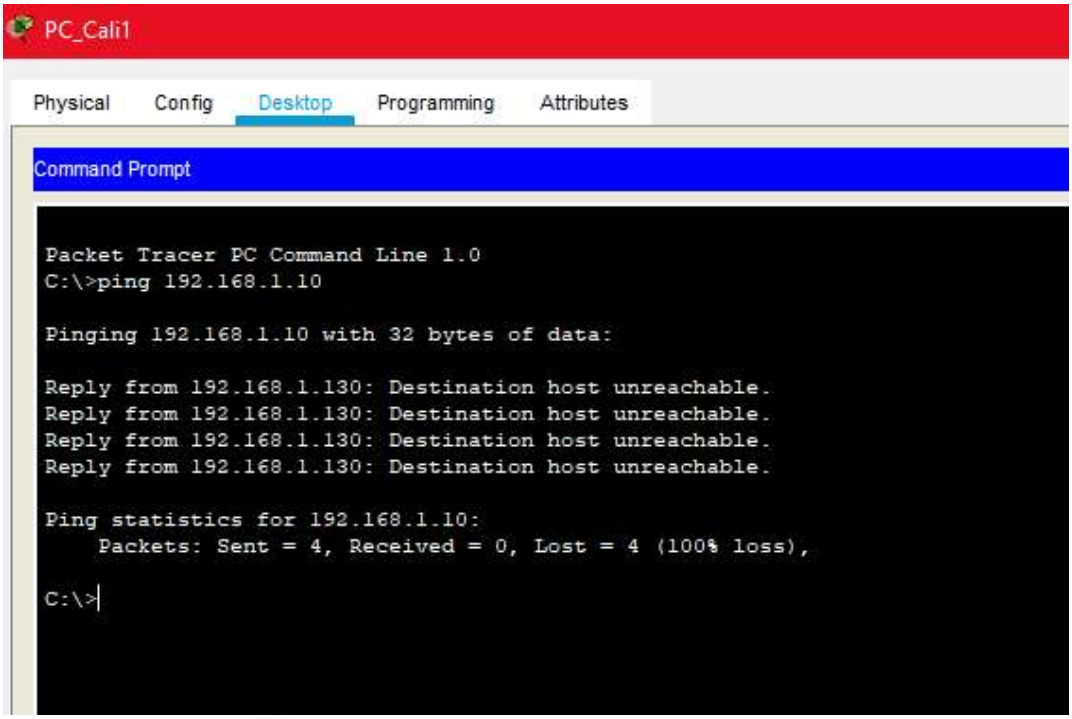


Ilustración 36: verificación de CPL configuradas 2

Parte 5: Comprobación de la red instalada.

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

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

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	OPEN
	WS 1	Router BOGOTA	OPEN
	Servidor	Router CALI	OPEN
	Servidor	Router MEDELLIN	OPEN
TELNET	LAN del router MEDELLIN	Router CALI	CLOSED
	LAN del router CALI	Router CALI	OPEN
	LAN del router MEDELLIN	Router MEDELLIN	OPEN
	LAN del Router CALI	Router MEDELLIN	CLOSED
PING	LAN del Router CALI	WS1	HOST UNREACHEABLE
	LAN del Router MEDELLIN	WS1	HOST UNREACHEABLE
	LAN del Router MEDELLIN	LAN del Router CALI	HOST UNREACHEABLE
PING	LAN del Router CALI	Servidor	HOST UNREACHEABLE
	LAN del Router MEDELLIN	Servidor	HOST UNREACHEABLE
	Servidor	LAN del Router MEDELLIN	PING COMPLETE 5/5
	Servidor	LAN del Router CALI	PING COMPLETE 5/5
	Router CALI	LAN del Router MEDELLIN	PING COMPLETE 5/5
	Router MEDELLIN	LAN del Router CALI	PING COMPLETE 5/5

Ilustración 37: Tabla de verificación de TELNET y PING

Para finalizar con este escenario dejo la ilustración de como quedo la implementación final de la red en el Packet Tracer.

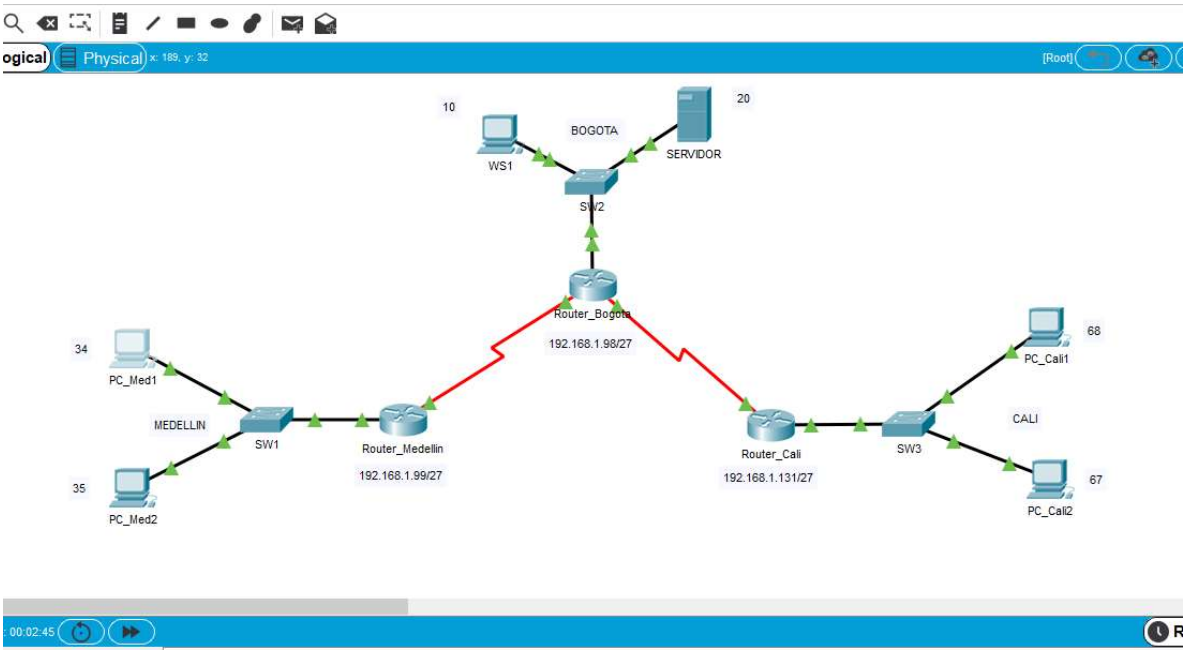
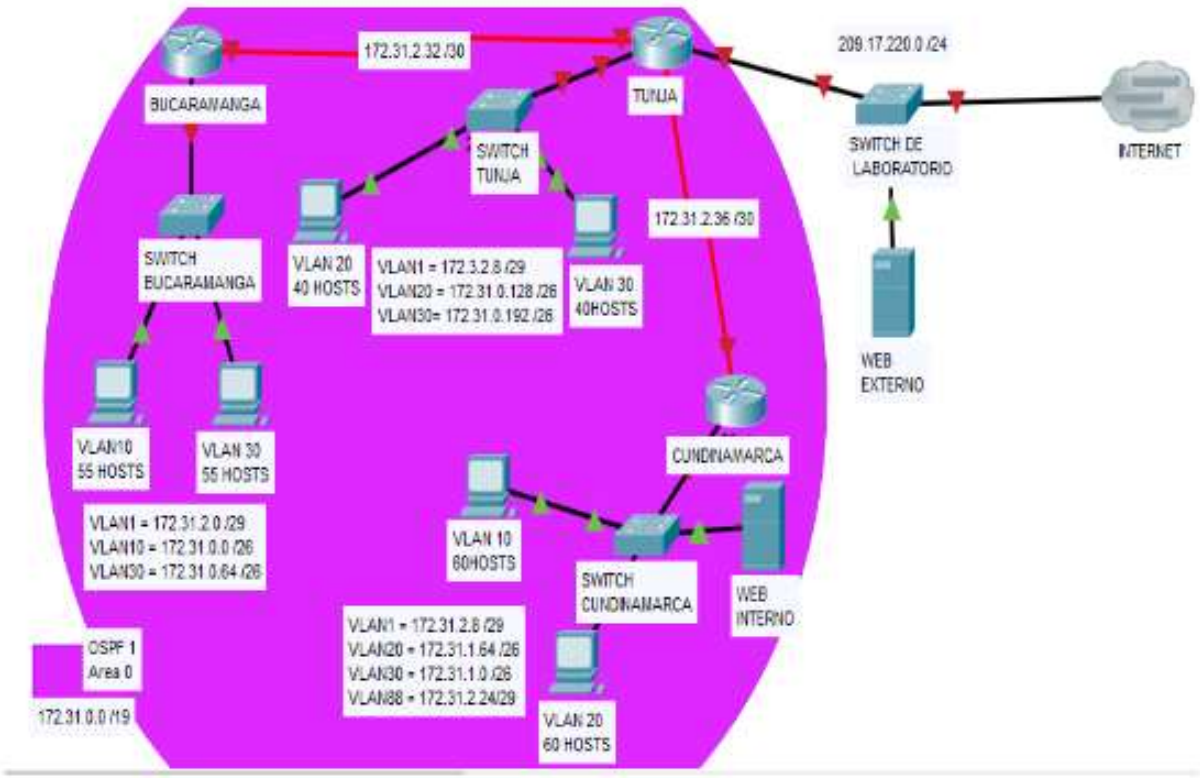


Ilustración 38: Red completa y configurada

Escenario 2

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



Desarrollo

Los siguientes son los requerimientos necesarios:

Parte 1. Todos los routers deberán tener lo 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.

Comenzamos a implementar la red con los dispositivos pertinentes para la correcta configuración en Packet Tracert, dichos dispositivos son:

- 3 Routers 1841 para conexión WAN
- 4 Switches Catalyst 2960 series de 24 puertos
- 6 PC'S
- 2 Servidores (Uno interno y otro externo)

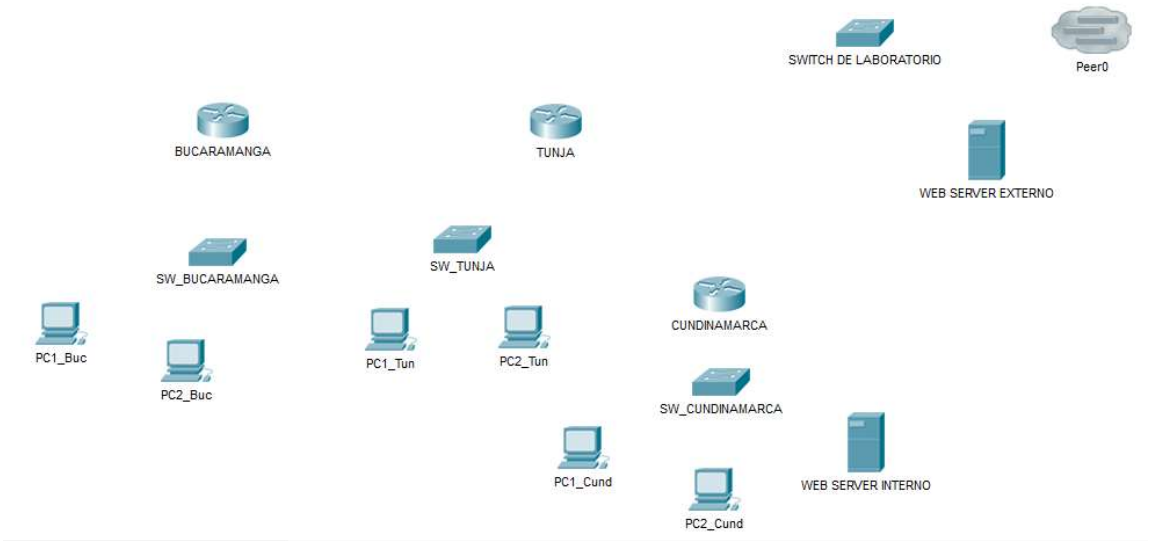


Ilustración 39: Implementando la red escenario 2

Para cada uno de los routers se debe apagar el dispositivo en la pestaña Physical y dar clic como se muestra en la siguiente ilustración.

Ilustración 40: Apagado de router cisco 1841

Seguido de esto damos clic en la pestaña llamada **MODULES** que está dentro de la pestaña Physical y seleccionamos **WIC-1T** esto para permitir la conectividad **WAN** entre los demás routers.

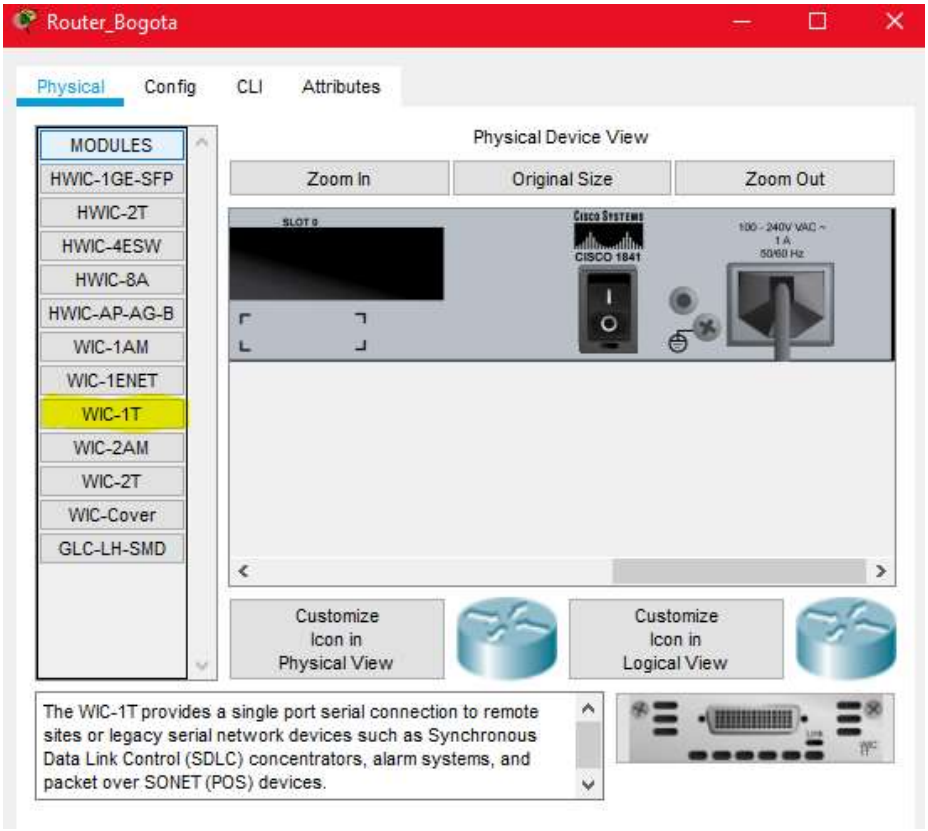


Ilustración 41: Selección WIC-1T

Una vez seleccionado el módulo **WIC-1T** lo arrastramos al Slot 0 y Slot 1 del router y debe quedar como en la siguiente ilustración.

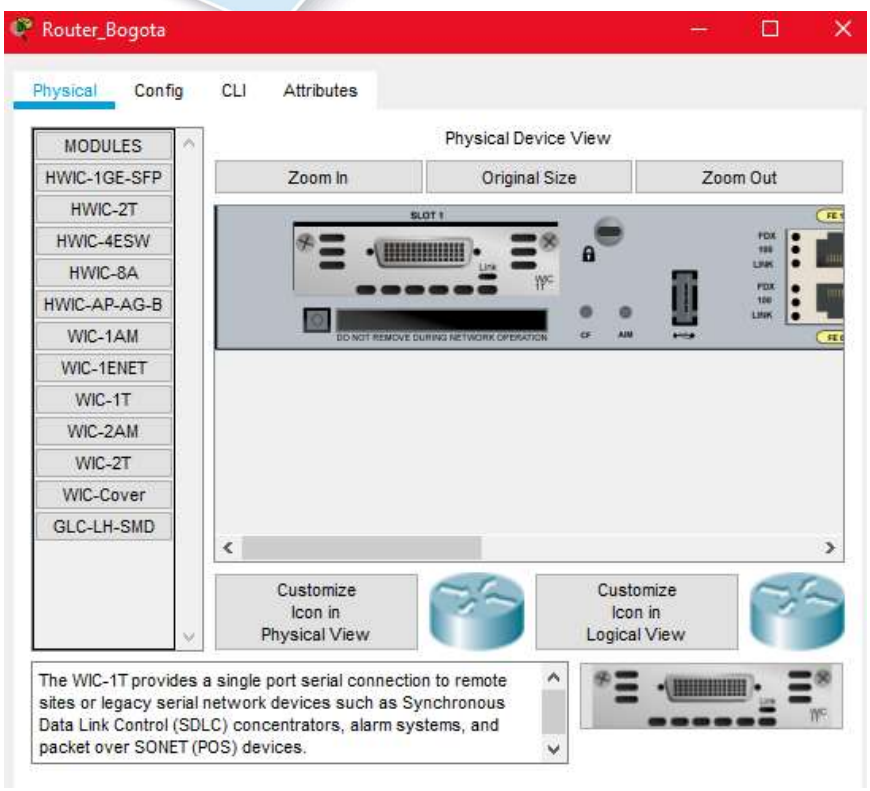


Ilustración 42: Modulo WIC-1T en Slot 1

Una vez instaladas las tarjetas en los routers, encendemos los routers y comenzamos con la configuración inicial de cada uno de los mismos. En dicha configuración se le asigna un nombre al router, contraseñas de seguridad y mensaje de seguridad de conexión no autorizada a los mismos.

Configuración Router Tunja

Router>en

Router#configure t

Router#configure terminal

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

Router(config)#hostname TUNJA

TUNJA(config)#enable secret tunja

TUNJA(config)#

TUNJA(config)#username admin secret UNAD

TUNJA(config)#

TUNJA(config)#

TUNJA(config)#aaa new

TUNJA(config)#aaa new-model

TUNJA(config)#aaa au

TUNJA(config)#aaa auth

TUNJA(config)#aaa authentication login default local

TUNJA(config)#

TUNJA(config)#

TUNJA(config)#aaa authenti

TUNJA(config)#aaa authentication login TELNET-LOGIN local

TUNJA(config)#

TUNJA(config)#line con 0

TUNJA(config-line)#login a

TUNJA(config-line)#login authentication d

TUNJA(config-line)#login authentication default

TUNJA(config-line)#

TUNJA(config-line)#exit

TUNJA(config)#line vty 0 4

TUNJA(config-line)#lo

TUNJA(config-line)#login ath

TUNJA(config-line)#login authentication TELNET-LOGIN

TUNJA(config-line)#exit

TUNJA(config)#

Configuración Router Bucaramanga

Router>en

Router#configure t

Router#configure terminal

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

Router(config)#hostname BUCARAMANGA

BUCARAMANGA(config)#enable secret bucaramanga

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#username admin secret UNAD

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#aaa new

BUCARAMANGA(config)#aaa new-model

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#aaa authentication login defa

BUCARAMANGA(config)#aaa authentication login default local

BUCARAMANGA(config)#aaa authentication login default local

BUCARAMANGA(config)#

BUCARAMANGA(config)#

BUCARAMANGA(config)#aaa authenti

BUCARAMANGA(config)#aaa authentication login TELNET-LOGIN local

BUCARAMANGA(config)#

BUCARAMANGA(config)#line con 0

BUCARAMANGA(config-line)#

BUCARAMANGA(config-line)#login authe

BUCARAMANGA(config-line)#login authentication def

BUCARAMANGA(config-line)#login authentication default

BUCARAMANGA(config-line)#

BUCARAMANGA(config-line)#exit

BUCARAMANGA(config)#line vty 0 4

BUCARAMANGA(config-line)#

BUCARAMANGA(config-line)#login auth

BUCARAMANGA(config-line)#login authentication TELNET-LOGIN

BUCARAMANGA(config-line)#exit

BUCARAMANGA(config)#

Configuración router Cundinamarca

Router>en

Router#configure t

Router#configure terminal

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

Router(config)#hostname CUNDINAMARCA

CUNDINAMARCA(config)#enable secret cundinamarca

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#username admin secret UNAD

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#aaa new

CUNDINAMARCA(config)#aaa new-model

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#aaa authentication login default local

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#aaa auth

CUNDINAMARCA(config)#aaa authentication login TELNET-LOGIN local

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#line con 0

CUNDINAMARCA(config-line)#login authentication default

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#line con 0 4

^

% Invalid input detected at '^' marker.

CUNDINAMARCA(config)#line vty 0 4

CUNDINAMARCA(config-line)#login authentication TELNET-LOGIN

CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#

Una vez configurados cada uno de los routers, se procede a cablear la red teniendo en cuenta la topología manejada en el ejemplo dado y la red queda estructurada de la siguiente manera.

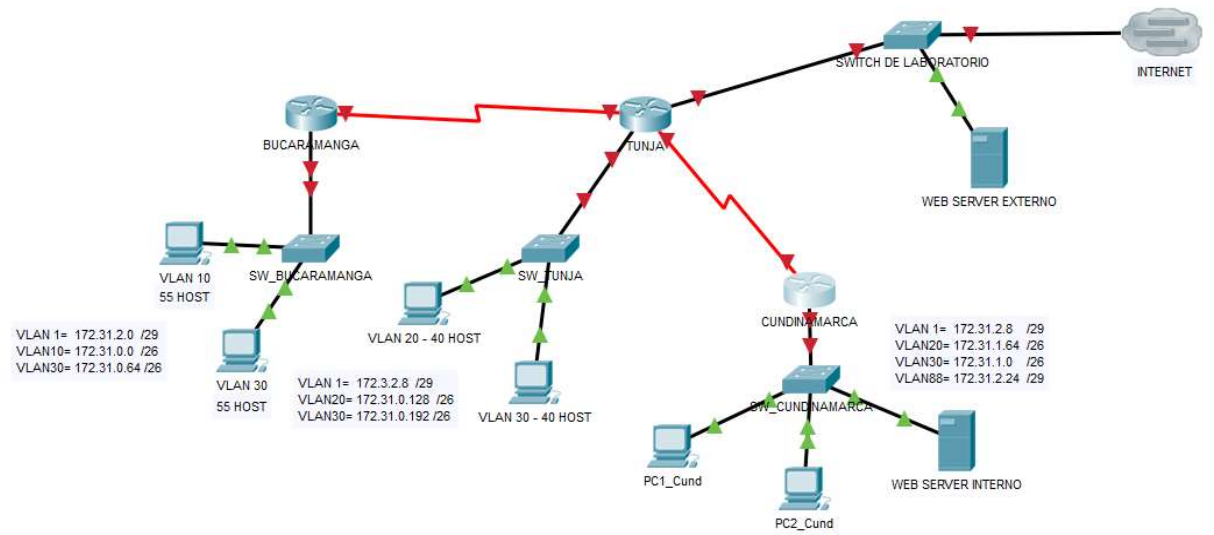


Ilustración 43: Red cableada

Como podemos apreciar todos los puertos están down, la única conectividad existente es la de los computadores a los puertos de los switches; Basándonos en la tabla de direccionamiento y en los segmentos dados por el escenario dos, estructuramos la tabla de direccionamiento entre los routers que es la siguiente.

		ENLACES ROUTERS				
ID. DE RED	#HOST	PREFIJO	IP INICIAL	IP FINAL	BROADCAST	MASCARA DE RED
172.31.2.32	2	30	172..31.2.33	172.31.2.34	172.31.2.35	255.255.255.255
172.31.2.36	2	30	172.31.2.37	172.31.2.38	172.31.2.39	255.255.255.255

Ilustración 44: Tabla de direccionamiento entre routers

Como podemos apreciar los segmentos de red son de mascara 30 por ende solo tienen disponibles dos host, cada una de estos host se les asignara a cada puerto serial del router según corresponda de la siguiente manera.

Configuración puertos Serial Tunja

TUNJA#configure ter

TUNJA#configure terminal

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

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252

TUNJA(config-if)#no sh

TUNJA(config-if)#no shutdown

TUNJA(config-if)#exit

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

TUNJA(config)#interface serial 0/1/0

TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252

TUNJA(config-if)#no sh

TUNJA(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Configuración puertos Serial Bucaramanga

BUCARAMANGA#configur t

BUCARAMANGA#configur terminal

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

BUCARAMANGA config-if)#ip address 172.31.2.33 255.255.255.252

BUCARAMANGA(config-if)#no shut

 (config)#interface serial 0/1/0

BUCARAMANGA(

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Configuración puertos Serial Cundinamarca

CUNDINAMARCA#configure t

CUNDINAMARCA#configure terminal

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

CUNDINAMARCA(config)#interface serial 0/1/0

CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252

CUNDINAMARCA(config-if)#no shu

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#

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

CUNDINAMARCA(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Una vez configurados los puertos seriales de los tres routers, podemos apreciar que ya existe conectividad entre ellos, ahora vamos a configurar cada uno de los puertos **FastEthernet 0/0** en cada uno de los routers teniendo en cuenta la tabla de direccionamiento para cada una de las ciudades.

Configuración puertos Fast Ethernet Tunja

Se le asigna esta IP al **Fast Ethernet 0/0** porque es la IP que viene del identificador de red desde afuera.

TUNJA#configu t

TUNJA#configu terminal

Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface FastE
TUNJA(config)#interface FastEthernet 0/0
TUNJA(config-if)#ip address 209.17.220.20 255.255.255.0
TUNJA(config-if)#no shut
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Ahora configuramos el puerto Fast Ethernet 0/1 con la dirección IP del segmento de la red de Tunja basándonos en la tabla de direccionamiento que nos entregan en el escenario, así mismo se realizara con los demás routers.

TUNJA#configure t
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface faste
TUNJA(config)#interface fastethernet 0/1
TUNJA(config-if)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-if)#no shut
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Configuración puertos Fast Ethernet Bucaramanga

BUCARAMANGA#configure t

BUCARAMANGA#configure terminal

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

BUCARAMANGA(config)#inter

BUCARAMANGA(config)#interface FastE

BUCARAMANGA(config)#interface FastEthernet 0/0

BUCARAMANGA(config-if)#ip address 172.31.2.1 255.255.255.248

BUCARAMANGA(config-if)#no shu

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

Configuración puertos Fast Ethernet Cundinamarca

CUNDINAMARCA#configu t

CUNDINAMARCA#configu terminal

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

CUNDINAMARCA(config)#interface fast e

CUNDINAMARCA(config)#interface faste

CUNDINAMARCA(config)#interface fastethernet

% Incomplete command.

CUNDINAMARCA(config)#interface fastethernet 0/0

CUNDINAMARCA(config-if)#ip address 172.31.2.10 255.255.255.248

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#no shut

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

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

Como primera instancia debemos configurar las VLANS en cada uno de los switches por donde se configurara el direccionamiento DHCP que se solicitara al router de TUNJA por medio del comando helper-address.

Configuración VLANS Bucaramanga

VLAN 1

```
SW_Buc(config)#vlan 1
SW_Buc(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
SW_Buc(config-vlan)#exit
SW_Buc(config)#int vlan1
SW_Buc(config-if)#ip ad
SW_Buc(config-if)#ip address 172.31.2.1 255.255.255.248
SW_Buc(config-if)#no shut
SW_Buc(config-if)#no shutdown
SW_Buc(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

VLAN 10

```
Switch>
Switch>en
Switch#confi t
Switch#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_Buc
SW_Buc(config)#vlan 10
SW_Buc(config-vlan)#name VLAN10
SW_Buc(config-vlan)#EXIT
SW_Buc(config)#int vlan10
SW_Buc(config-if)#ip ad
SW_Buc(config-if)#ip address 172.31.0.1 255.255.255.192
SW_Buc(config-if)#no shut
SW_Buc(config-if)#no shutdown
SW_Buc(config-if)#do wr
SW_Buc(config-if)#do wr
Building configuration...
```

[OK]

VLAN 30

```
SW_Buc(config)#vlan 30
SW_Buc(config-vlan)#name VLAN30
SW_Buc(config-vlan)#exit
SW_Buc(config)#int vlan 30
SW_Buc(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SW_Buc(config-if)#ip ad
SW_Buc(config-if)#ip address 172.31.0.65 255.255.255.192
SW_Buc(config-if)#no shut
SW_Buc(config-if)#no shutdown
SW_Buc(config-if)#do wr
SW_Buc(config-if)#do wr
Building configuration...
[OK]
SW_Buc(config-if)#
```

Configuración VLANS Tunja

VLAN 1

```
Switch>en
Switch#confi t
Switch#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_Tun
SW_Tun(config)#vlan1
^
% Invalid input detected at '^' marker.
SW_Tun(config)#vlan 1
SW_Tun(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
SW_Tun(config-vlan)#exit
SW_Tun(config)#int vlan 1
SW_Tun(config-if)#ip ad
SW_Tun(config-if)#ip address 172.31.2.8 255.255.255.248
Bad mask /29 for address 172.31.2.8
SW_Tun(config-if)#ip address 172.31.2.9 255.255.255.248
SW_Tun(config-if)#no shut
SW_Tun(config-if)#no shutdown
```

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

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

VLAN 20

SW_Tun(config)#vlan 20
SW_Tun(config-vlan)#name VLAN20
SW_Tun(config-vlan)#exit
SW_Tun(config)#int vlan 20
SW_Tun(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW_Tun(config-if)#ip ad
SW_Tun(config-if)#ip address 172.31.0.129 255.255.255.192
SW_Tun(config-if)#no shut
SW_Tun(config-if)#no shutdown
SW_Tun(config-if)#
SW_Tun(config-if)#do wr
Building configuration...
[OK]
SW_Tun(config-if)#exit
SW_Tun(config)#

VLAN 30

SW_Tun(config)#vlan 30
SW_Tun(config-vlan)#name VLAN30
SW_Tun(config-vlan)#exit
SW_Tun(config)#int vlan 30
SW_Tun(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SW_Tun(config-if)#ip ad
SW_Tun(config-if)#ip address 172.31.0.193 255.255.255.192
SW_Tun(config-if)#no shut
SW_Tun(config-if)#no shutdown
SW_Tun(config-if)#do wr
Building configuration...
[OK]
SW_Tun(config-if)#exit
SW_Tun(config)#

Configuración VLANS Cundinamarca

VLAN 1

```
Switch#configure t
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_Cund
SW_Cund(config)#vlan 1
SW_Cund(config-vlan)#name VLAN 1
^
% Invalid input detected at '^' marker.
SW_Cund(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
SW_Cund(config-vlan)#exit
SW_Cund(config)#int vlan 1
SW_Cund(config-if)#ip add
SW_Cund(config-if)#ip address 172.31.2.9 255.255.255.248
SW_Cund(config-if)#no shut
SW_Cund(config-if)#no shutdown

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

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

VLAN 20

```
SW_Cund(config)#vlan 20
SW_Cund(config-vlan)#name VLAN20
SW_Cund(config-vlan)#exit
SW_Cund(config)#int vlan 20
SW_Cund(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW_Cund(config-if)#ip ad
SW_Cund(config-if)#ip address 1172.31.1.65 255.255.255.192
^
% Invalid input detected at '^' marker.
SW_Cund(config-if)#ip ad
SW_Cund(config-if)#ip address 172.31.1.65 255.255.255.192
SW_Cund(config-if)#no shut
SW_Cund(config-if)#no shutdown
SW_Cund(config-if)#do wr
SW_Cund(config-if)#do wr
Building configuration...
```

[OK]
SW_Cund(config-if)#

VLAN 30

SW_Cund(config)#vlan 30
SW_Cund(config-vlan)#name VLAN30
SW_Cund(config-vlan)#exit
SW_Cund(config)#int vlan 30
SW_Cund(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SW_Cund(config-if)#ip ad
SW_Cund(config-if)#ip address 172.31.1.1 255.255.255.192
SW_Cund(config-if)#n shut
SW_Cund(config-if)#n shutdown
SW_Cund(config-if)#do wr
SW_Cund(config-if)#do wr
Building configuration...
[OK]
SW_Cund(config-if)#
SW_Cund(config-if)#exit
SW_Cund(config)#

VLAN 88

SW_Cund(config)#vlan 88
SW_Cund(config-vlan)#name VLAN88
SW_Cund(config-vlan)#exit
SW_Cund(config)#int vla 88
SW_Cund(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

SW_Cund(config-if)#ip ad
SW_Cund(config-if)#ip address 172.31.2.25 255.255.255.248
SW_Cund(config-if)#no shut
SW_Cund(config-if)#no shutdown
SW_Cund(config-if)#do wr
SW_Cund(config-if)#do wr
Building configuration...
[OK]
SW_Cund(config-if)#

Una vez configuradas las VLANS procedemos a configurar el router de tunja para el direccionamiento DHCP de la siguiente manera.

Configuración DHCP router Tunja

Configuramos un pool de dhcp para cada VLAN existente en la red

POOL 1

TUNJA>en

Password:

TUNJA#confi t

TUNJA#confi terminal

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

TUNJA(config)#ip dhcp pool tunja

TUNJA(dhcp-config)#net

TUNJA(dhcp-config)#network 172.31.0

TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192

TUNJA(dhcp-config)#def

TUNJA(dhcp-config)#default-router 172.31.0.1

TUNJA(dhcp-config)#dn

TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#exit

TUNJA(config)#exit

TUNJA#

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

POOL 2

TUNJA(config)#ip dhcp pool tunja2

TUNJA(dhcp-config)#net

TUNJA(dhcp-config)#network 172.31.2.0 255.255.255.248

TUNJA(dhcp-config)#defa

TUNJA(dhcp-config)#default-router 172.31.2.7

TUNJA(dhcp-config)#dns

TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#do wr

TUNJA(dhcp-config)#

TUNJA(dhcp-config)#exit

POOL 3

TUNJA(config)#ip dhcp pool tunja3

TUNJA(dhcp-config)#net

TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192

TUNJA(dhcp-config)#defa

TUNJA(dhcp-config)#default-router 172.31.0.127

TUNJA(dhcp-config)#dns

TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#do wr

TUNJA(dhcp-config)#

Seguido de esto implementamos el comando ip helper-address desde el router de Bucaramanga, este comando le pide permiso al router de Tunja para que deje pasar las peticiones que van hacia ese router.

Configuración router Bucaramanga para solicitar helper-address al puerto Serial 0/0/0 del router de Tunja

BUCARAMANGA(config)#INT FA
BUCARAMANGA(config)#INT FAstEthernet 0/0
BUCARAMANGA(config-if)#ip he
BUCARAMANGA(config-if)#ip helper-address 172.31.2.34
BUCARAMANGA(config-if)#int fa 0/0.2
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int fa 0/0.3
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

BUCARAMANGA(config-subif)#do wr
Building configuration...
[OK]
BUCARAMANGA(config-subif)#

Ahora debemos configurar el switch de Bucaramanga en el puerto Gig 0/1 en modo truncal para que puedan pasar las VLAN que configuramos en dicho switch.

Configuración Switch Bucaramanga a modo TRUNK

SW_Buc>
SW_Buc>en
SW_Buc#conf t
SW_Buc#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW_Buc(config)#int gig
SW_Buc(config)#int gigabitEthernet 0/1
SW_Buc(config-if)#switch
SW_Buc(config-if)#switchport mode tr
SW_Buc(config-if)#switchport mode trunk

SW_Buc(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

Como podemos apreciar las VLAN que se habían configurado quedan arriba (up).

Ahora debemos crear el direccionamiento en el router de Tunja para mostrarle la ruta hacia donde debe enviar el direccionamiento por medio del comando ip route.

TUNJA(config)#ip route 172.31.2.0 255.255.255.248 172.31.2.33
TUNJA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.33
TUNJA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.33
TUNJA(config)#
TUNJA(config)#do wr
Building configuration...
[OK]
TUNJA(config)#

Ahora nos dirigimos al equipo VLAN10 de la red de Bucaramanga y cómo podemos apreciar el direccionamiento DHCP fue exitoso.

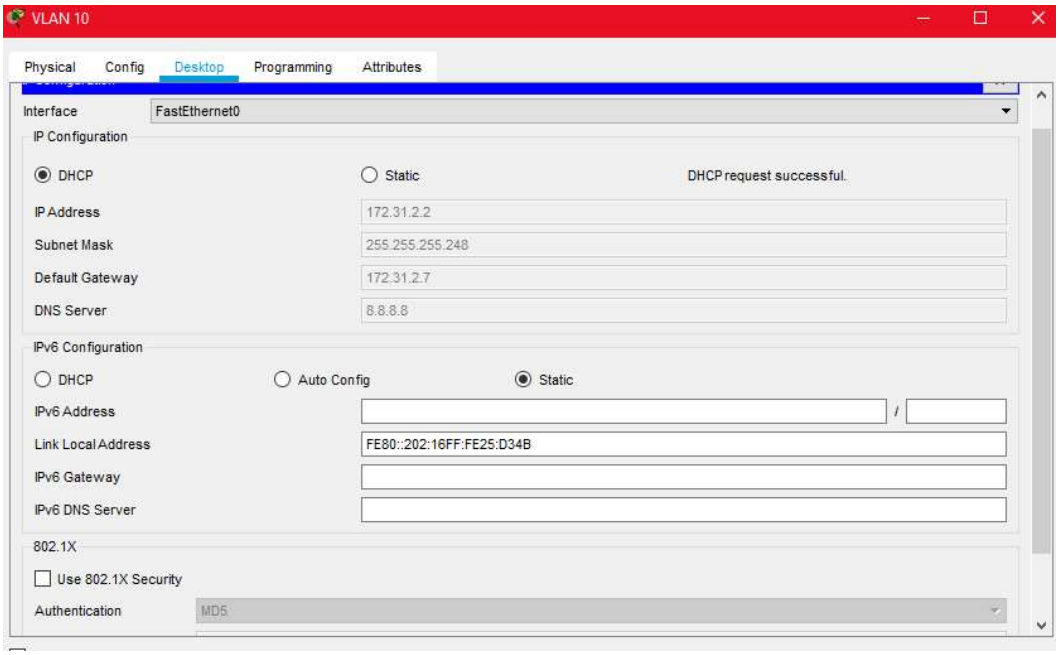


Ilustración 45: DHCP completado en red Bucaramanga

Seguido de esto realizamos el mismo procedimiento para la red de Cundinamarca para que el router de esta ciudad solicite al router de Tunja el direccionamiento DHCP.
Como podemos apreciar el direccionamiento DHCP en el WEB SERVER INTERNO en la red de Cundinamarca fue exitoso.

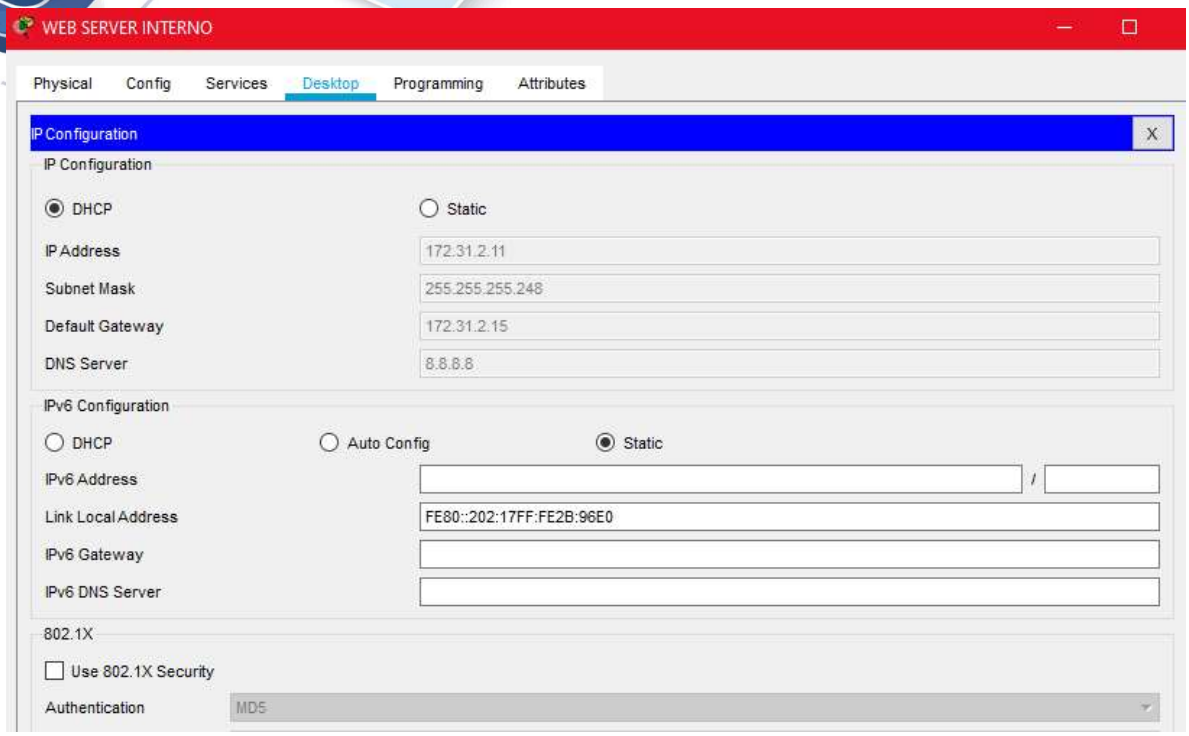


Ilustración 46: DHCP completado en red Cundinamarca

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

NAT estático en WEB Server externo

Se configura una IP pública en el Web Server Externo, teniendo en cuenta el identificador de red dada en el trabajo.

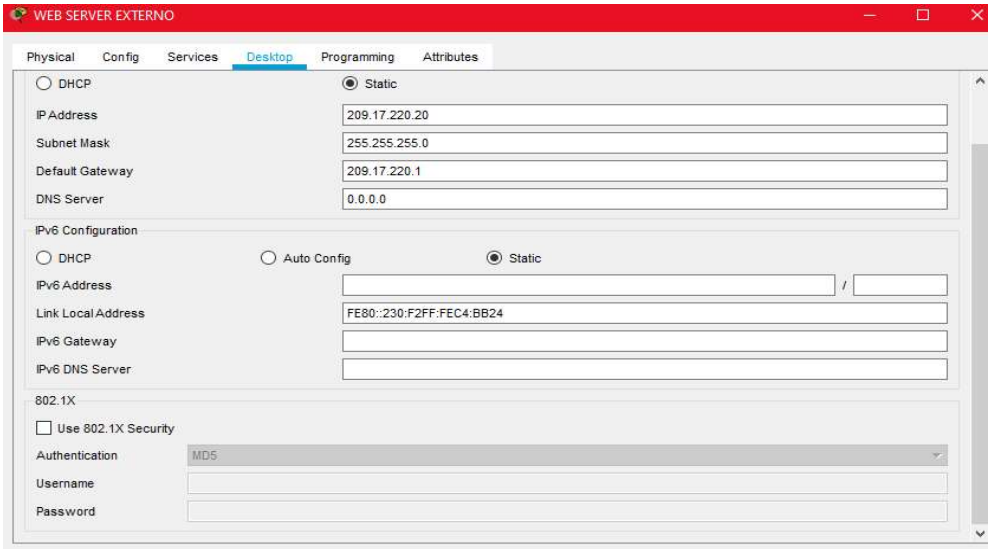


Ilustración 47: NAT estático en Web Server

NAT sobrecarga en router Tunja

```
TUNJA>en
Password:
TUNJA#configur t
TUNJA#configur terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access
TUNJA(config)#access-list 1 permit 172.31.0.0 255.255.192.0
TUNJA(config)#ip nat inside source list 1 interface serial 0/0 overload
%Invalid interface number (Slot is empty)
TUNJA(config)#ip nat inside source list 1 interface serial 0/0/0 overload
TUNJA(config)#interface fa
TUNJA(config)#interface fastEthernet 0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#
```

NAT sobrecarga en router Bucaramanga

```
BUCARAMANGA>en
Password:
BUCARAMANGA#config t
BUCARAMANGA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 255.255.255.192
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 0.0.0.192
BUCARAMANGA(config)#ip nat inside so
BUCARAMANGA(config)#ip nat inside source list 1 interface fa 0/0 overload
BUCARAMANGA(config)#interface fa 0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface se 0/1(0
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config)#interface se
BUCARAMANGA(config)#interface serial 0/1/0
BUCARAMANGA(config-if)#ip nat outside
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

NAT sobrecarga en router Cundinamarca

CUNDINAMARCA>en
Password:
CUNDINAMARCA#configu t
CUNDINAMARCA#configu terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#acc
CUNDINAMARCA(config)#access-list 1 permit 172.31.1.0 0.0.0.192
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#ip nat inside source list 1 in
CUNDINAMARCA(config)#ip nat inside source list 1 interface fa 0/0 overload
CUNDINAMARCA(config)#interfac fa
CUNDINAMARCA(config)#interfac fastEthernet 0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface se
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit

Parte 4. El enrutamiento deberá tener autenticación.

Para implementar el OSPF – AREA 0 tomamos como referencia la IP dada en el trabajo (**172.31.0.0 con mascara de red 19**) y la implementamos en cada uno de los routers, utilizamos la Wildcard (Sombreada en amarillo) de la IP para que abarque toda la red, sin tener que poner IP por IP en la configuración de router OSPF.

Ilustración 48: OSPF en AREA 0

Configuración OSPF en router Bucaramanga

BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#router-id 1.1.1.1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.31.255 area 0
BUCARAMANGA(config-router)#
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#

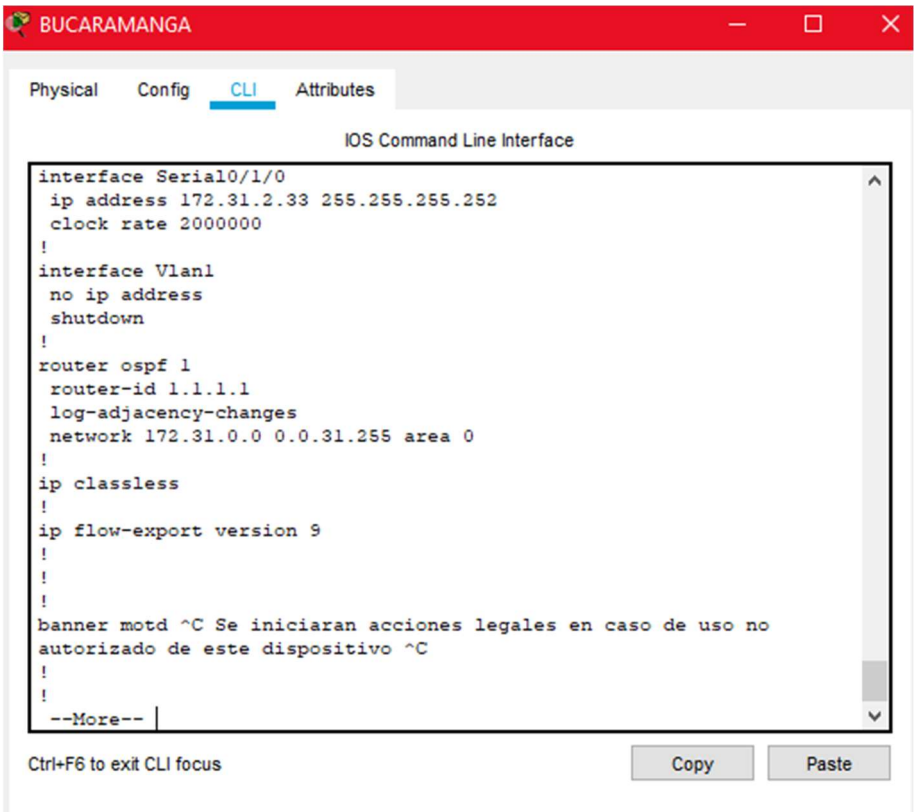


Ilustración 49: Comando Show Running Config Bucaramanga

Configuración OSPF en router Tunja

```
TUNJA>en
Password:
TUNJA#confi
TUNJA#configure t
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#router ospf 1
TUNJA(config-router)#ro
TUNJA(config-router)#router-id 2.2.2.2
TUNJA(config-router)#network 172.31.0.0 0.0.31.255 area 0
TUNJA(config-router)#exit
TUNJA(config)#
00:36:44: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
```

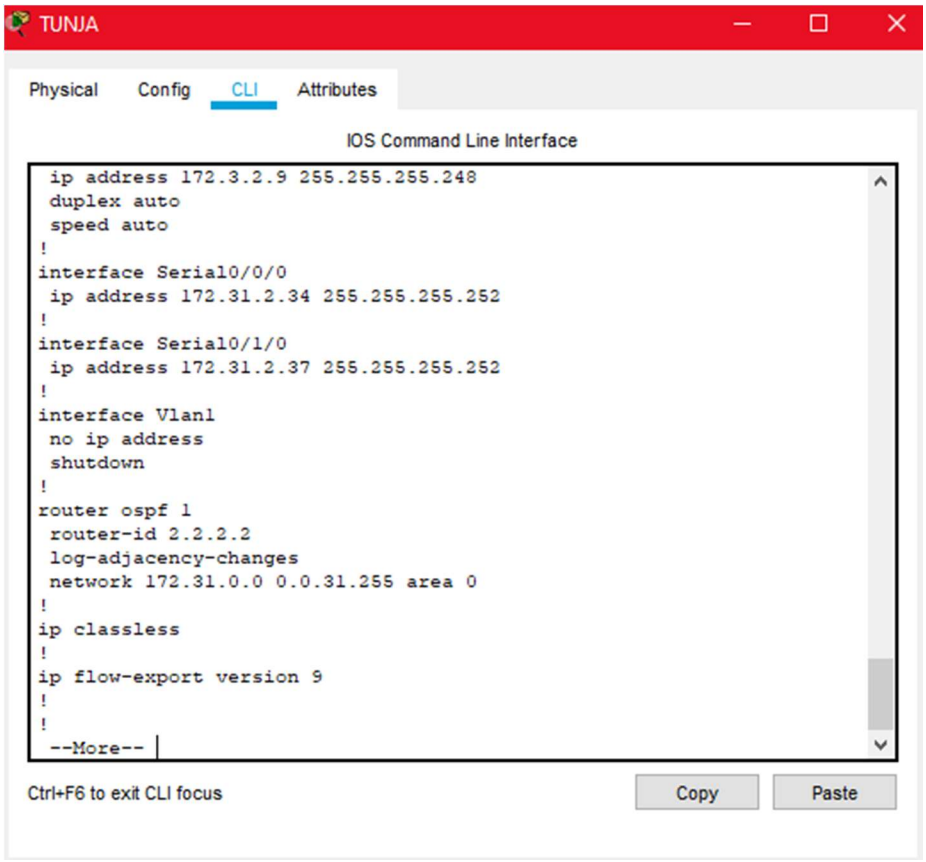


Ilustración 50: Comando Show Running Config Tunja

Configuración OSPF en router Cundinamarca

CUNDINAMARCA#configure t
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#rout
CUNDINAMARCA(config-router)#router-id 3.3.3.3
CUNDINAMARCA(config-router)#network 172.31.0.0 0.0.31.255 area 0
CUNDINAMARCA(config-router)#
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#
01:11:08: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/1/0 from LOADING to FULL, Loading Done

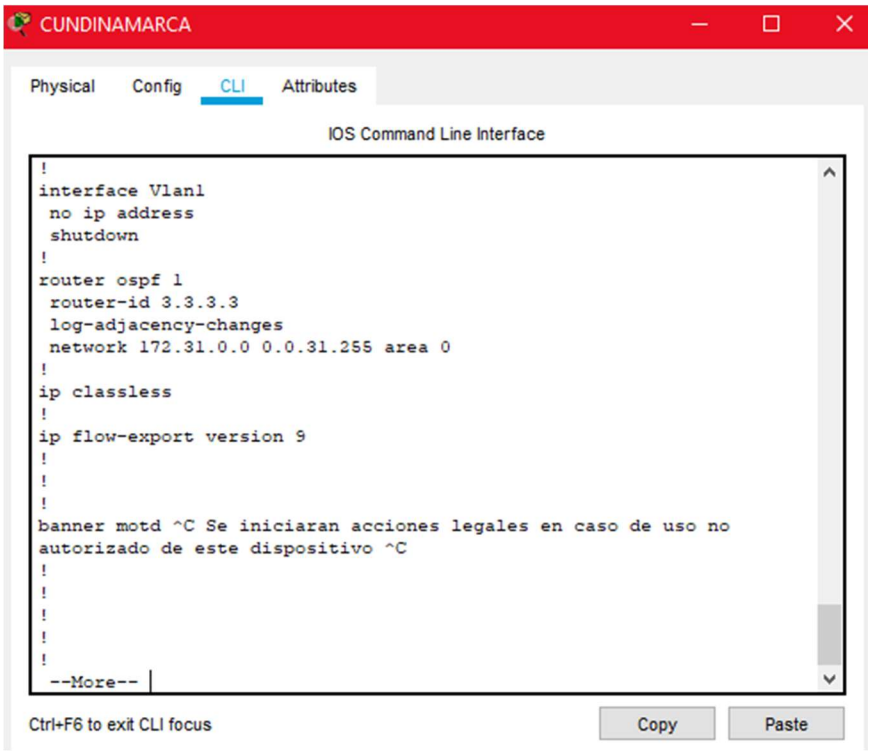


Ilustración 51: Comando Show Running Config Cundinamarca

Ahora cómo podemos apreciar en la siguiente ilustración por medio del comando **Show ip ospf neighbor** podemos ver los routers vecinos configurados con **OSPF**.

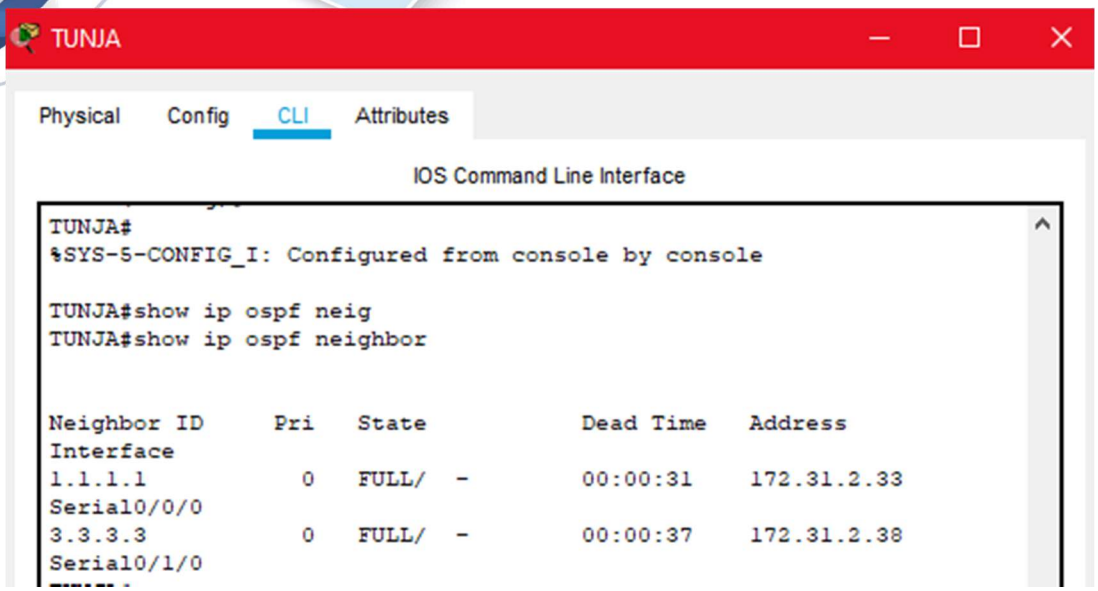


Ilustración 52: Comando Show Ip ospf neighbor en router de Tunja

Parte 5. Listas de control de acceso:

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

Configuramos el bloqueo de la VLAN 20 hacia afuera, con una Access list extendida, el punto más cercano de salida es el puerto serial 0/1/0 del router de Cundinamarca el cual configuramos con la lista de acceso creada en out.

CUNDINAMARCA(config)#access-list 101 deny icmp host 172.31.1.64 host 172.31.2.37
CUNDINAMARCA(config)#interfac
CUNDINAMARCA(config)#interface se
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip acc
CUNDINAMARCA(config-if)#ip access-group 101 out
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

Y configuramos el router de Tunja en el puerto serial 0/1/0 con la lista de acceso en deny IN para todo lo que entre de direccionamiento.

```
TUNJA#conf t
TUNJA#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface 0/1/0
^
% Invalid input detected at '^' marker.
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip acc
TUNJA(config-if)#ip access-group 101 in
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Permitir salida de paquetes hacia el router de tunja y de tunja hacia el ISP

```
CUNDINAMARCA(config)#acc
CUNDINAMARCA(config)#access-list 102 permit icmp host 172.31.2.8 host 172.31.2.37
CUNDINAMARCA(config)#interfe
CUNDINAMARCA(config)#interf
CUNDINAMARCA(config)#interface seri
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip acc
CUNDINAMARCA(config-if)#ip access-group out
% Incomplete command.
CUNDINAMARCA(config-if)#ip ac
CUNDINAMARCA(config-if)#ip access-group 102 out
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
```

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

Configuración router de tunja con la access list creada

TUNJA#confi t
TUNJA#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#acc
TUNJA(config)#interf
TUNJA(config)#interface se
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip acc
TUNJA(config-if)#ip access-group 102 in
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

Ahora bloqueamos todas las conexiones hacia las demás VLANS en el mismo router

De VLAN 10 a VLAN 20

CUNDINAMARCA(config)#access
CUNDINAMARCA(config)#access-list 103 deny icmp host 172.31.2.8 host 172.31.1.64
CUNDINAMARCA(config)#
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#interface seri
CUNDINAMARCA#confi t
CUNDINAMARCA#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#inter
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip acc
CUNDINAMARCA(config-if)#ip access-group 103 in

CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

De VLAN 10 a VLAN 30

CUNDINAMARCA(config)#access-list 104 deny icmp host 172.31.2.8 host 172.31.1.0
CUNDINAMARCA(config)#inter
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip acc
CUNDINAMARCA(config-if)#ip access-group 104 in
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

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

TUNJA(config)#access-list 105 permit icmp host 172.31.1.0 host 209.17.220.20
TUNJA(config)#
TUNJA(config)#inter
TUNJA(config)#interface fa
TUNJA(config)#interface fa fast
TUNJA(config)#interface fastethernet 0/0
TUNJA(config-if)#
TUNJA(config-if)#ip acc
TUNJA(config-if)#ip access-group 105 out
TUNJA(config-if)#exit
TUNJA(config)#interface fast
TUNJA(config)#interface fastEthernet 0/1

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 105 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

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

VLAN 20 Tunja a VLAN 20 Cundinamarca

TUNJA(config)#acces

TUNJA(config)#access-list 106 permit icmp host 172.31.0.128 host 172.31.1.64

TUNJA(config)#

TUNJA(config)#

TUNJA(config)#interf

TUNJA(config)#interface fast

TUNJA(config)#interface fastEthernet 0/1

TUNJA(config-if)#

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 106 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interfa

TUNJA(config)#interface seri

TUNJA(config)#interface serial 0/1/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 106 out

TUNJA(config-if)#

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#exit

TUNJA#

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

02:31:03: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from LOADING to FULL, Loading Done

Configuración Puerto serial en router Cundinamarca

CUNDINAMARCA#confi t

CUNDINAMARCA#confi terminal

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

CUNDINAMARCA(config)#interface 0/1/0

^

% Invalid input detected at '^' marker.

CUNDINAMARCA(config)#interface serial 0/1/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip ac

CUNDINAMARCA(config-if)#ip access-group 106 in

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#

02:31:03: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/1/0 from LOADING to FULL, Loading Done

Exit

VLAN 20 Tunja a VLAN 10 Bucaramanga

TUNJA#confi t

TUNJA#confi terminal

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

TUNJA(config)#

TUNJA(config)#acc

TUNJA(config)#access-list 107 permit icmp host 172.31.0.128 host 172.31.2.0

TUNJA(config)#

TUNJA(config)#interf

TUNJA(config)#interface fas

TUNJA(config)#interface fastEthernet 0/1

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 107 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interf

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 107 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

TUNJA(config)#

Configuración Puerto serial en router Bucaramanga

BUCARAMANGA#confi t

BUCARAMANGA#confi terminal

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

BUCARAMANGA(config)#interface seri

BUCARAMANGA(config)#interface serial 0/1/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc
BUCARAMANGA(config-if)#ip access-group 107 in
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface fast
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#ip ac
BUCARAMANGA(config-if)#ip access-group 107 out
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#

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

VLAN 30 a INTERNET

BUCARAMANGA(config)#ACC
BUCARAMANGA(config)#ACCess-list 108 permit icmp host 172.31.0.64 host 209.17.220.20
BUCARAMANGA(config)#
BUCARAMANGA(config)#interface fast
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#ip acc
BUCARAMANGA(config-if)#ip access-group 108 in
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#

BUCARAMANGA(config)#interfa se

BUCARAMANGA(config)#interfa serial 0/1/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 108 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#

BUCARAMANGA(config)#

Configuración de puerto de entrada y salida en router de Tunja

TUNJA#conf t

TUNJA#conf terminal

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

TUNJA(config)#interface se

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 108 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#inetr

TUNJA(config)#inetr fa

TUNJA(config)#interf

TUNJA(config)#interface fast

TUNJA(config)#interface fastEthernet 0/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 108 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#exit

TUNJA#

VLAN 30 Bucaramanga a VLAN 10 Tunja

BUCARAMANGA(config)#acc

BUCARAMANGA(config)#access-list 109 permit icmp host 172.31.0.64 host 172.31.2.8

BUCARAMANGA(config)#inter

BUCARAMANGA(config)#interface fast

BUCARAMANGA(config)#interface fastEthernet 0/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 109 in

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#interf

BUCARAMANGA(config)#interface ser

BUCARAMANGA(config)#interface serial 0/1/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 109 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#

Configuración router Tunja para la Access- list 109.

TUNJA#configure t

TUNJA#configure terminal

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

TUNJA(config)#interf

TUNJA(config)#interface ser

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 109 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interf

TUNJA(config)#interface fast

TUNJA(config)#interface fastEthernet 0/1

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 109 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

VLAN 30 Bucaramanga a VLAN 10 Cundinamarca

BUCARAMANGA(config)#acc

BUCARAMANGA(config)#access-list 110 permit icmp host 172.31.0.64 host 172.31.2.8

BUCARAMANGA(config)#inter

BUCARAMANGA(config)#interface fast

BUCARAMANGA(config)#interface fastEthernet 0/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip ac

BUCARAMANGA(config-if)#ip access-group 110 in

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#interface se

BUCARAMANGA(config)#interface serial 0/1/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip ac

BUCARAMANGA(config-if)#ip access-group 110 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#

Configuración router Tunja para la Access- list 110

TUNJA#confi t

TUNJA#confi terminal

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

TUNJA(config)#interface se

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#

TUNJA(config-if)#ip a

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 110 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interfa fast

TUNJA(config)#interfa fastEthernet 0/1

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 110 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

Dejamos abierto el puerto serial 0/1=/0 para que pase al router de Cundinamarca

TUNJA(config-if)#exit

TUNJA(config)#interfa

TUNJA(config)#interface se

TUNJA(config)#interface serial 0/1/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 110 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

Configuración router Cundinamarca para la Access- list 110

CUNDINAMARCA#confi t

CUNDINAMARCA#confi terminal

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

CUNDINAMARCA(config)#inter

CUNDINAMARCA(config)#interface se

CUNDINAMARCA(config)#interface serial 0/1/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip acc

CUNDINAMARCA(config-if)#ip access-group 110 in

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interf

CUNDINAMARCA(config)#interface fast

CUNDINAMARCA(config)#interface fastEthernet 0/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip acc

CUNDINAMARCA(config-if)#ip access-group 110 out

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#exit

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

Para dicho ejercicio implementamos dos Access-list extendidas la 111 y la 112 las cuales se configuran en los routers de la siguiente manera:

Configuración router Bucaramanga para las Access- list 111 y 112

BUCARAMANGA#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#
BUCARAMANGA(config)#acc
BUCARAMANGA(config)#access-list 111 permit icmp host 172.31.2.0 host 172.31.0.128
BUCARAMANGA(config)#access-list 112 permit icmp host 172.31.2.0 host 172.31.1.64
BUCARAMANGA(config)#inter
BUCARAMANGA(config)#interface fast
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#ip ac
BUCARAMANGA(config-if)#ip access-group
BUCARAMANGA(config-if)#ip access-group 111 in
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#ip access-group 112 in
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interfa
BUCARAMANGA(config)#interface s
BUCARAMANGA(config)#interface serial 0/1/0
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 111 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 112 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#exit

BUCARAMANGA#

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

Configuración router Tunja para las Access- list 111 y 112

TUNJA#confi

TUNJA#confi terminal

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

TUNJA(config)#interface seri

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 111 in

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 112 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interface fa

TUNJA(config)#interface fastEthernet 0/1

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 111

% Incomplete command.

TUNJA(config-if)#ip access-group 111 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#interface ser

TUNJA(config)#interface serial 0/1/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 112 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

Configuración router Cundinamarca para la Access- list 112

CUNDINAMARCA#confi t

CUNDINAMARCA#confi terminal

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

CUNDINAMARCA(config)#interface se

CUNDINAMARCA(config)#interface serial 0/1/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip acc

CUNDINAMARCA(config-if)#ip access-group 112 in

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interfac

CUNDINAMARCA(config)#interface fast

CUNDINAMARCA(config)#interface fastEthernet 0/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip acc

CUNDINAMARCA(config-if)#ip access-group 112 out

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

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

Configuración router Bucaramanga

BUCARAMANGA(config)#access-list 113 deny icmp host 172.31.2.0 host 172.31.0.0

BUCARAMANGA(config)#access-list 114 deny icmp host 172.31.2.0 host 172.31.0.64

BUCARAMANGA(config)#access-list 115 deny icmp host 172.31.0.0 host 172.31.2.0

BUCARAMANGA(config)#access-list 116 deny icmp host 172.31.0.0 host 172.31.0.64

BUCARAMANGA(config)#access-list 117 deny icmp host 172.31.0.64 host 172.31.2.0

BUCARAMANGA(config)#access-list 118 deny icmp host 172.31.0.64 host 172.31.0.0

BUCARAMANGA(config)#interface fast

BUCARAMANGA(config)#interface fastEthernet 0/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip acc

BUCARAMANGA(config-if)#ip access-group 113 out

BUCARAMANGA(config-if)#ip access-group 114 out

BUCARAMANGA(config-if)#ip access-group 115 out

BUCARAMANGA(config-if)#ip access-group 116 out

BUCARAMANGA(config-if)#ip access-group 117 out

BUCARAMANGA(config-if)#ip access-group 118 out

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#

BUCARAMANGA(config)#

Configuración router Tunja

TUNJA#conf t

TUNJA#conf terminal

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

TUNJA(config)#acc

TUNJA(config)#access-list 119 deny icmp host 172.31.2.8 host 172.31.0.128

TUNJA(config)#access-list 120 deny icmp host 172.31.2.8 host 172.31.0.192

TUNJA(config)#access-list 121 deny icmp host 172.31.0.128 host 172.31.2.8

TUNJA(config)#access-list 122 deny icmp host 172.31.0.128 host 172.31.0.192

TUNJA(config)#access-list 123 deny icmp host 172.31.0.192 host 172.31.2.8

TUNJA(config)#access-list 124 deny icmp host 172.31.0.192 host 172.31.0.128

TUNJA(config)#

TUNJA(config)#inter

TUNJA(config)#interface fast 0/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 119 out

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 120 out

TUNJA(config-if)#ip access-group 121 out

TUNJA(config-if)#ip access-group 122 out

TUNJA(config-if)#ip access-group 123 out

TUNJA(config-if)#ip access-group 124 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

Configuración router Cundinamarca

CUNDINAMARCA#confi t

CUNDINAMARCA#confi terminal

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

CUNDINAMARCA(config)#acc

CUNDINAMARCA(config)#access-list 125 deny icmp host 172.31.2.8 host 172.31.1.64

CUNDINAMARCA(config)#access-list 126 deny icmp host 172.31.2.8 host 172.31.1.0

CUNDINAMARCA(config)#access-list 127 deny icmp host 172.31.1.64 host 172.31.2.8

CUNDINAMARCA(config)#access-list 128 deny icmp host 172.31.1.64 host 172.31.1.0

CUNDINAMARCA(config)#access-list 129 deny icmp host 172.31.1.0 host 172.31.2.8

CUNDINAMARCA(config)#access-list 130 deny icmp host 172.31.1.0 host 172.31.1.64
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#interf
CUNDINAMARCA(config)#interface fast
CUNDINAMARCA(config)#interface fastEthernet 0/0
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#ip acc
CUNDINAMARCA(config-if)#ip access-group 125 out
CUNDINAMARCA(config-if)#ip access-group 126 out
CUNDINAMARCA(config-if)#ip access-group 127 out
CUNDINAMARCA(config-if)#ip access-group 128 out
CUNDINAMARCA(config-if)#ip access-group 129 out
CUNDINAMARCA(config-if)#ip access-group 130 out
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by consol

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

Configuramos 3 access list, una que va hacia internet y las otras dos que van a cada uno de los routers y las implementamos de la siguiente manera:

Configuración router Cundinamarca

CUNDINAMARCA(config)#access-list 131 permit icmp host 172.31.2.24 host 209.17.220.0
CUNDINAMARCA(config)#access-list 132 permit icmp host 172.31.2.24 host 172.31.2.37
CUNDINAMARCA(config)#access-list 133 permit icmp host 172.31.2.24 host 172.31.2.33
CUNDINAMARCA(config)#

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#interfa

CUNDINAMARCA(config)#interface fast

CUNDINAMARCA(config)#interface fastEthernet 0/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip ac

CUNDINAMARCA(config-if)#ip access-group 131 in

CUNDINAMARCA(config-if)#ip access-group 132 in

CUNDINAMARCA(config-if)#ip access-group 133 in

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#interfac

CUNDINAMARCA(config)#interface ser

CUNDINAMARCA(config)#interface serial 0/1/0

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#ip acc

CUNDINAMARCA(config-if)#ip access-group 131 out

CUNDINAMARCA(config-if)#ip access-group 132 out

CUNDINAMARCA(config-if)#ip access-group 133 out

CUNDINAMARCA(config-if)#

CUNDINAMARCA(config-if)#exit

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#

Configuración router Tunja

TUNJA#confi terminal

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

TUNJA(config)#interface se

TUNJA(config)#interface serial 0/1/0

TUNJA(config-if)#

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 131 in

TUNJA(config-if)#ip access-group 132 in

TUNJA(config-if)#ip access-group 133 in

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

TUNJA(config)#interface fast

TUNJA(config)#interface fast 0/0

TUNJA(config-if)#

TUNJA(config-if)#ip ac

TUNJA(config-if)#ip access-group 131 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#

TUNJA(config)#interface ser

TUNJA(config)#interface serial 0/0/0

TUNJA(config-if)#ip acc

TUNJA(config-if)#ip access-group 132 out

TUNJA(config-if)#ip access-group 133 out

TUNJA(config-if)#

TUNJA(config-if)#exit

TUNJA(config)#exit

Configuración router Bucaramanga

BUCARAMANGA#conf t

BUCARAMANGA#conf terminal

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

BUCARAMANGA(config)#interfa

BUCARAMANGA(config)#interface se

BUCARAMANGA(config)#interface serial 0/1/0

BUCARAMANGA(config-if)#

BUCARAMANGA(config-if)#ip ac
BUCARAMANGA(config-if)#ip access-group 132 in
BUCARAMANGA(config-if)#ip access-group 133 in
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#

Listas de control de acceso extendidas creadas:

access-list 101 deny icmp host 172.31.1.64 host 172.31.2.37
access-list 102 permit icmp host 172.31.2.8 host 172.31.2.37
access-list 103 deny icmp host 172.31.2.8 host 172.31.1.64
access-list 104 deny icmp host 172.31.2.8 host 172.31.1.0
access-list 105 permit icmp host 172.31.1.0 host 209.17.220.20
access-list 106 permit icmp host 172.31.0.128 host 172.31.1.64
access-list 107 permit icmp host 172.31.0.128 host 172.31.2.0
access-list 108 permit icmp host 172.31.0.64 host 209.17.220.20
access-list 109 permit icmp host 172.31.0.64 host 172.31.2.8
access-list 110 permit icmp host 172.31.0.64 host 172.31.2.8
access-list 111 permit icmp host 172.31.2.0 host 172.31.0.128
access-list 112 permit icmp host 172.31.2.0 host 172.31.1.64
access-list 113 deny icmp host 172.31.2.0 host 172.31.0.0
access-list 114 deny icmp host 172.31.2.0 host 172.31.0.64
access-list 115 deny icmp host 172.31.0.0 host 172.31.2.0
access-list 116 deny icmp host 172.31.0.0 host 172.31.0.64
access-list 117 deny icmp host 172.31.0.64 host 172.31.2.0
access-list 118 deny icmp host 172.31.0.64 host 172.31.0.0
access-list 119 deny icmp host 172.31.2.8 host 172.31.0.128
access-list 120 deny icmp host 172.31.2.8 host 172.31.0.192
access-list 121 deny icmp host 172.31.0.128 host 172.31.2.8
access-list 122 deny icmp host 172.31.0.128 host 172.31.0.192

access-list 123 deny icmp host 172.31.0.192 host 172.31.2.8

access-list 124 deny icmp host 172.31.0.192 host 172.31.0.128

access-list 125 deny icmp host 172.31.2.8 host 172.31.1.64

access-list 126 deny icmp host 172.31.2.8 host 172.31.1.0

access-list 127 deny icmp host 172.31.1.64 host 172.31.2.8

access-list 128 deny icmp host 172.31.1.64 host 172.31.1.0

access-list 129 deny icmp host 172.31.1.0 host 172.31.2.8

access-list 130 deny icmp host 172.31.1.0 host 172.31.1.64

access-list 131 permit icmp host 172.31.2.24 host 209.17.220.0

access-list 132 permit icmp host 172.31.2.24 host 172.31.2.37

access-list 133 permit icmp host 172.31.2.24 host 172.31.2.33

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

Las tablas de direccionamiento serían las siguientes:

		RANGO DE DIRECCIONES						
VLAN	CIUDAD	ID. DE RED	# HOST	PREFIJO	IP INICIAL	IP FINAL	BROADCAST	MASCARA DE RED
VLAN1	Bucaramanga	172.31.2.0	6	29	172.31.2.1	172.31.2.6	172.31.2.7	255.255.255.248
VLAN 10	Bucaramanga	172.31.0.0	55	26	172.31.0.1	172.31.0.62	172.31.0.63	255.255.255.192
VLAN 30	Bucaramanga	172.31.0.64	55	26	172.31.0.65	172.31.0.126	172.31.0.127	255.255.255.192
VLAN 20	Tunja	172.31.0.128	40	26	172.31.0.129	172.31.0.190	172.31.0.191	255.255.255.192
VLAN 30	Tunja	172.31.0.192	40	26	172.31.0.193	172.31.0.254	172.31.0.255	255.255.255.192
VLAN1	Cundinamarca	172.31.2.8	6	29	172.31.2.9	172.31.2.14	172.31.2.15	255.255.255.248
VLAN 20	Cundinamarca	172.31.1.64	60	26	72.31.1.2	172.31.1.126	172.31.1.127	255.255.255.192
VLAN 30	Cundinamarca	172.31.1.0	60	26	172.31.1.1	172.31.1.62	172.31.1.63	255.255.255.192
VLAN 88	Cundinamarca	172.31.2.24	6	29	172.31.2.25	172.31.2.30	172.31.2.31	255.255.255.248

Ilustración 53: Tabla de direccionamiento de la Red

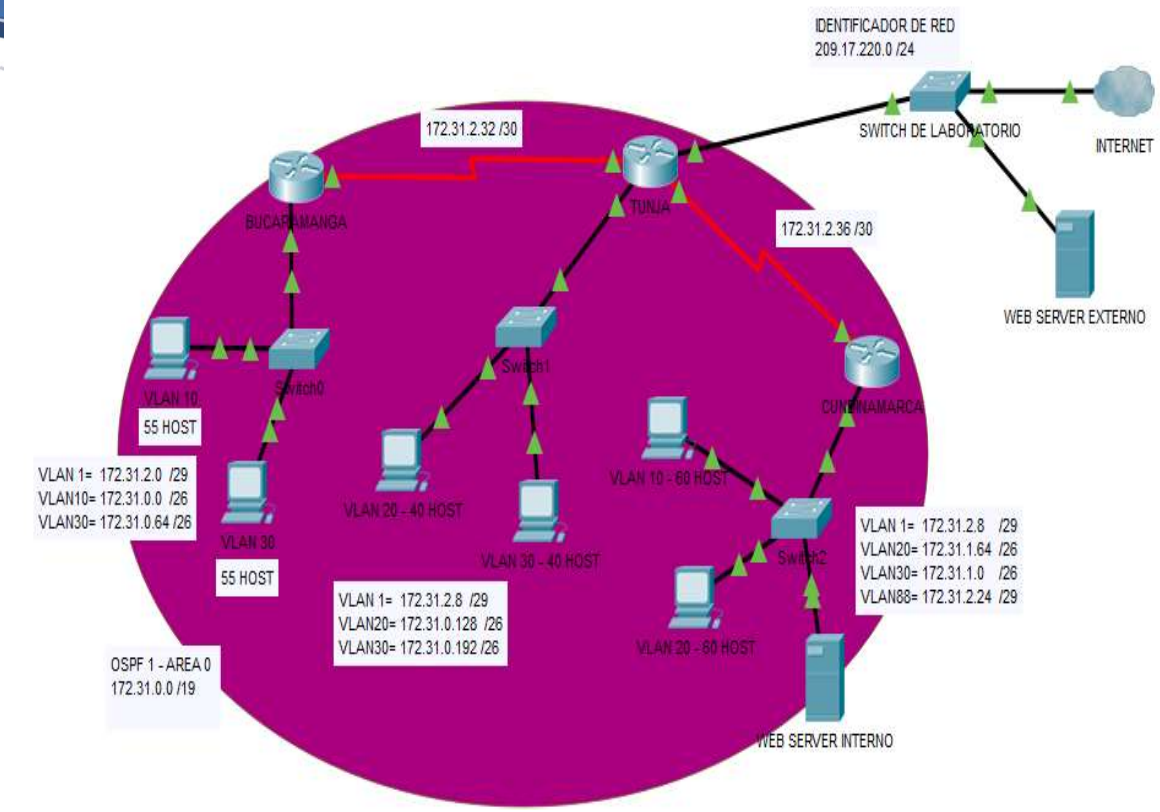


Ilustración 54: Red cableada y configurada a totalidad

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.

CONCLUSIONES

Por medio de los dos escenarios planteados como trabajo final del diplomado de profundización diseño e implementación de redes LAN/WAN, se realizaron las configuraciones de topología física, cumpliendo con el direccionamiento adecuado que satisficiera las especificaciones de las problemáticas planteadas. Todo lo anterior utilizando el software de simulación Packet Tracer versión 7.2.1.0218, para el modelamiento y la conectividad LAN/WAN, comprobada y verificada con los comandos Ping y TracerT.

Lo anterior haciendo énfasis en los conocimientos adquiridos a lo largo de este diplomado de profundización, correspondientes a los aspectos básicos y elementos de las redes de telecomunicaciones y técnicas de conmutación. Entre algunos de esos temas se encuentran los protocolos, servicios de seguridad de redes, modelos capa OSI y TCP/IP, configuración de dispositivos y enrutamientos.

- El protocolo DHCP está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la administración de las direcciones IP de la red.

- OSPF es un protocolo que gestiona un sistema autónomo (AS) en áreas. Dichas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

- ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en una terminal u otro dispositivo de capa de red. Las listas de acceso de control pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a unos cortafuegos.

BIBLIOGRAFIA

- Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0

- Cisco Ccna – Configuración DHCP. (S.F.). Http://Blog.Capacityacademy.Com/2014/01/09/Cisco-Ccna-Como- Configurar-Dhcp-En-Cisco-Router/.

- CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Acceso. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1

- Como Configurar Opsf En Router. (S.F.). Http://Blog.Capacityacademy.Com/2014/06/23/Cisco-Ccna-Como-Configurar-Ospf-En-Cisco-Router/

- CISCO SYSTEM. (2017). Capítulo 6. Enrutamiento estático. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6.0.1.1

- CISCO SYSTEM. (2017). Capítulo 7. Routing Dinámico. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7.0.1.1

- CISCO SYSTEM. (2017). Capítulo 6. Enrutamiento estático. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6.0.1.1

- CISCO SYSTEM. (2017). Capítulo 7. Routing Dinámico. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7.0.1.1

- Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).