DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN

HAROL HERNEY MANRIQUE ARIZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
INIRIDA
2022

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN

HAROL HERNEY MANRIQUE ARIZA

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

TUTORA
PAULITA SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
INIRIDA
2022

CONTENIDO

Resumen 9

Abstract....10

Introducción 11

Objetivos....12

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN....13

Escenario 1....13

Configurar la topología de red....15

Parte 1: Asignación de direcciones IP....19

a) Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa....19

b) Asignar una dirección IP a la red....19

Parte 2: Configuración Básica.....19

a) Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas. 19

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....24

c) Verificar el balanceo de carga que presentan los routers.....26

d) Realizar un diagnóstico de vecinos uando el comando cdp 27

e) Realizar una prueba de conectividad en cada tramo de la ruta usando Ping 29

Parte 3: Configuración de Enrutamiento....31

a) Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado 31

b) Verificar si existe vecindad con los Routers configurados con EIGRP. 32

c) Realizar la comprobación de las tablas de enrutamiento en cada uno de los Routers para verificar cada una de las rutas establecidas. 34

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. 35

Parte 4: Configuración de las listas de Control de Acceso 36

a) Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red 36

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 38

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. 40

Parte 5: Comprobación de la red instalada 42

a) Se debe probar que la configuración de las listas de acceso fue exitosa 42

b) Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red 42

Escenario 2 51

Desarrollo 52

1. Todos los Routers deberán tener lo siguiente 52

- Configuración básica. 52
- Autenticación local con AAA 67
- Cifrado de contraseñas. 72
- Un máximo de internos para acceder al Router. 77
- Máximo tiempo de acceso al detectar ataques. 78

- Establezca un servidor TFTP y almacene todos los archivos necesarios de los Routers. 80

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca 82

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT) 85

4. El enrutamiento deberá tener autenticación 86

5. Listas de control de acceso 89

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja. 89
- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja. 91
- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet. 92
- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga 93
- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10 94
- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet. 95
- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad..... 95
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet. 98

6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento 100

Conclusiones 101

Bibliografía 102

LISTA DE TABLAS

Tabla 1 configuraciones IP de los Routers. 20
Tabla 2 Código de configuraciones IP de los Routers 20
Tabla 3 Configuración básica de Routers. 52
Tabla 4 Configuración de las VLAN de los Routers. 57
Tabla 5 Configuración de los nombres e interfaces de las VLAN. 63
Tabla 6 Autenticación local de los routers con AAA.....67
Tabla 7 Cifrado con contraseña de los Routers. 72
Tabla 8 Cifrado con contraseña de los Switches. 73
Tabla 9 Verificación de acceso a los Routers. 75
Tabla 10 máximo de internos para acceder al Router.....77
Tabla 11 Máximo tiempo de acceso al detectar ataques 78
Tabla 12 Creación de un servidor TFTP que almacene los archivos necesarios de los Routers 80
Tabla 13 Configuración para que el DHCP proporcione solo direcciones a los hosts de Bucaramanga y Cundinamarca. 82
Tabla 14 Configuración de enrutamiento para tener autenticación 86
Tabla 15 configuración de control de acceso de la VLAN 20 89
Tabla 16 configuración de control de acceso a internet de la VLAN 10 91
Tabla 17 configuración de control de acceso a internet, servidor web y ftp de la VLAN 30 92
Tabla 18 Configuración de hosts de VLAN 20 y VLAN 10 de Bucaramanga 93
Tabla 19 configuración de hosts de VLAN 30 94
Tabla 20 configuración de los hosts de la VLAN 10 para acceder a la VLAN 20 de Cundinamarca y Tunja.....95
Tabla 21 configuración de hosts de una VLAN negando el acceso a los de otra VLAN en una ciudad 96
Tabla 22 Configuración de VLAN administrativas y VLAN de servidores. 98

LISTA DE FIGURAS

Figura 1 red establecida por la guía.....14
Figura 2 Equipos de la topología de RED.....15
Figura 3 Configuración Router 1 Medellin.....16
Figura 4 Configuración Switch 1 Med.....16
Figura 5 Configuración Router 2 Bogota.....17
Figura 6 Configuración Switch 2 Bog.....17
Figura 7 Configuración Router 3 Cali.....18
Figura 8 Configuración Switch 3 Cali.....18
Figura 9 Subnetting de red en 8 partes.....19
Figura 10 verificación de enrutamiento en el Router 1 Medellin.....24
Figura 11 verificación de enrutamiento en el Router 2 Bogota.....25
Figura 12 verificación de enrutamiento en el Router 3 Cali.....25
Figura 13 prueba de carga del Router 1 Medellin.....26
Figura 14 prueba de carga del Router 2 Bogotá.....26
Figura 15 prueba de carga del Router 3 Cali.....27
Figura 16 diagnóstico de vecinos Router 1 Medellin.....27
Figura 17 diagnóstico de vecinos Router 2 Bogotá.....28
Figura 18 diagnóstico de vecinos Router 3 Cali.....28
Figura 19 Ping: PC 1 – Servidor.....29
Figura 20 Ping: PC 3 - WS 1.....29
Figura 21 Ping: PC 2 – PC 4.....30
Figura 22 Ping: Servidor – PC 3.....30
Figura 23 protocolo de enrutamiento EIGRP Router Medellin.....31
Figura 24 protocolo de enrutamiento EIGRP Router Bogotá.....31
Figura 25 protocolo de enrutamiento EIGRP Router 3 Cali.....32
Figura 26 Verificar vecindad en el Router Medellín.....32
Figura 27 Verificar vecindad en el Router Bogotá.....33
Figura 28 Verificar vecindad en el Router Cali.....33
Figura 29 comprobación tablas de enrutamiento Router Bogotá.....34

Figura 30 comprobación de las tablas de enrutamiento Router Medellin.....34
Figura 31 comprobación de las tablas de enrutamiento Router Cali.....35
Figura 32 Ping: PC 3 – PC 2.....35
Figura 33 Ping: PC 3 – WS 1.....36
Figura 34 configuración para establecer conexiones telnet Router 1 Medellin. 37
Figura 35 configuración para establecer conexiones telnet Router 2 Bogotá 37
Figura 36 configuración para establecer conexiones telnet Router 3 Cali. 38
Figura 37 Ping del servidor a cualquier Host. 38
Figura 38 HOSTS de la red 192.168.1.32 (Medellin), pueden hacer ping al SERVIDOR 39
Figura 39 HOSTS de la red 192.168.1.64 (Cali), pueden hacer ping al SERVIDOR 39
Figura 40 HOST de la red 192.168.1.5 (WS1), no pueden hacer ping al resto de los equipos de las subredes a excepción del servidor. 40
Figura 41 ROUTER 3 CALI, configuración para negar el acceso a equipos fuera de su subred. 42
Figura 42 Configuración propuesta.....51
Figura 43 Configuración de la topología de red 52
Figura 44 Verificación de servicios AAA de los Routers. 71
Figura 45 Configuración del WEB SERVER. 85

RESUMEN

A continuación, se presentará de manera detallada los pasos y fases para la construcción de redes estructuradas e interconectadas por configuración manual implementando la tecnología CISCO, a través de la formulación de 2 escenarios prácticos en los cuales se abordarán los diferentes comandos empleados para la construcción de estas redes; se abordarán temas como lo son: cableado de red, direccionamiento IP, segmentación de red hasta en 8 partes, configuración de seguridad de los equipos de conexión, solución de registros a los router y acceso de lista en función de la red con sus respectivas restricciones en red.

La estructuración y configuración de la red y de los equipos se llevarán a cabo en el simulador PACKET TRACER.

Palabras Clave: Configuración, Red, Router, Simulador, Packet Tracer.

ABSTRACT

Next, the steps and phases for the construction of structured and interconnected networks by manual configuration will be presented in detail, implementing CISCO technology, through the formulation of 2 practical scenarios in which the different commands used for the construction of networks will be addressed. these networks; Topics such as: network cabling, IP addressing, network segmentation up to 8 parts, security configuration of connection equipment, log solution to routers and list access based on the network with its respective restrictions will be addressed in network.

The structuring and configuration of the network and of the equipment will be carried out in the PACKET TRACER simulator.

Keywords: Configuration, Red, Router, Simulator, Packet Tracer.

INTRODUCCIÓN

El presente trabajo tiene como finalidad la implementación de las diferentes temáticas estudiadas durante el curso de profundización en redes CISCO, a través de soluciones LAN / WAM, las cuales se representarán a través de la formulación y solución de 2 escenarios prácticos en los cuales de abordarán diferentes aspectos de Switching y Routing.

Durante el desarrollo de los escenarios propuestos se aplicarán los siguientes conceptos de Networking:

Configuración e inicialización de dispositivos de red.
Configuración de PC, Routers, Servidores y Switches.
Aplicación de políticas de seguridad en dispositivos de comunicación.
Segmentación de red, configuración de Vlans, DHCP, NAT y sobrecarga.
Configuración de listas de acceso para los dispositivos en las diferentes sub redes.
La estructuración y configuración de la red y de los equipos se llevarán a cabo en el simulador PACKET TRACER.

OBJETIVOS

Objetivos General:

Desarrollar y configurar las topologías de red planteadas a través de 2 escenarios prácticos.

Objetivos Específicos:

Estructuración de topologías de red.

Inicializar dispositivos de red.

Configurar los diferentes dispositivos de comunicación Routers, Switch, servidores.

Aplicar configuración de seguridad para Switches.

Implementar OPSFv2.

Aplicar DHCP Y NAT.

Configurar listas de control de acceso ACL.

Implementar ping entre equipos conectados en red y sub redes.

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN

ESCENARIO 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

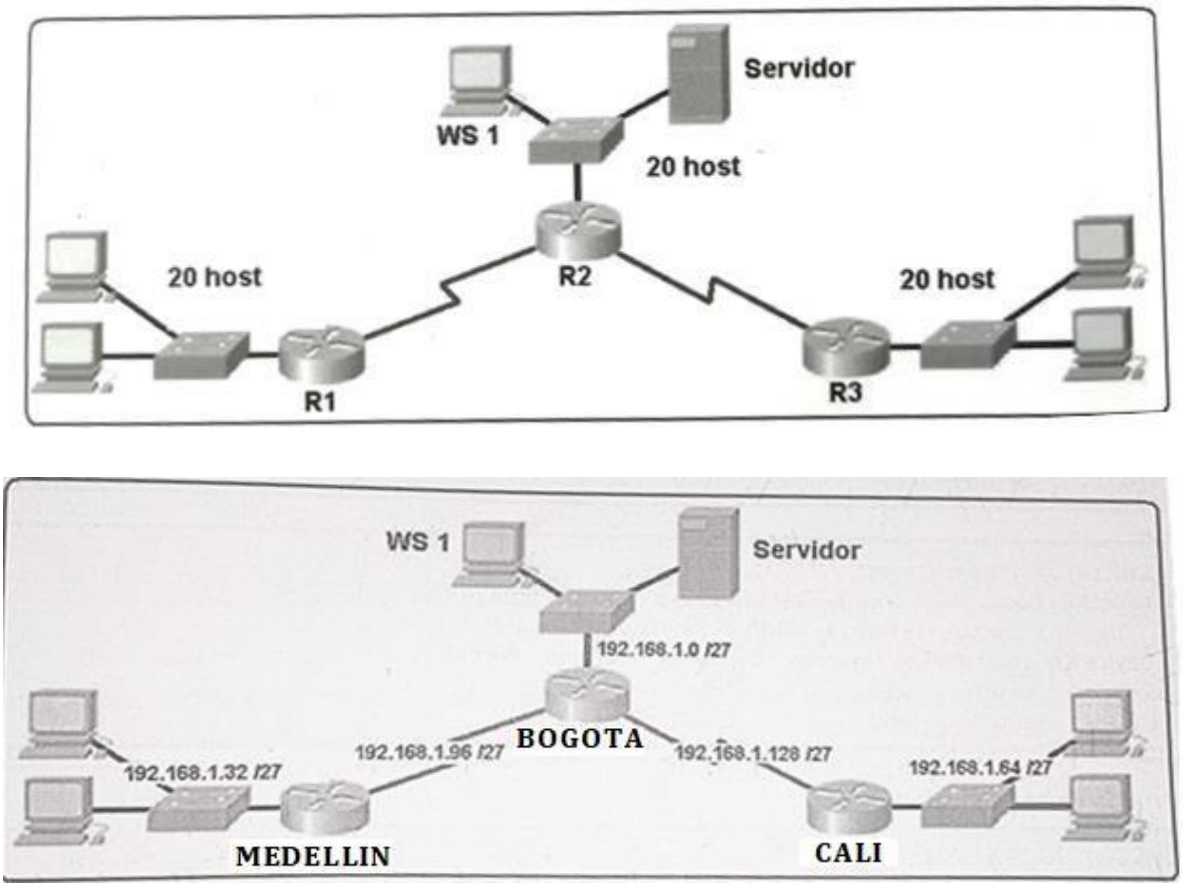
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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

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

Parte 6: Configuración final

Figura 1 red establecida por la guía.



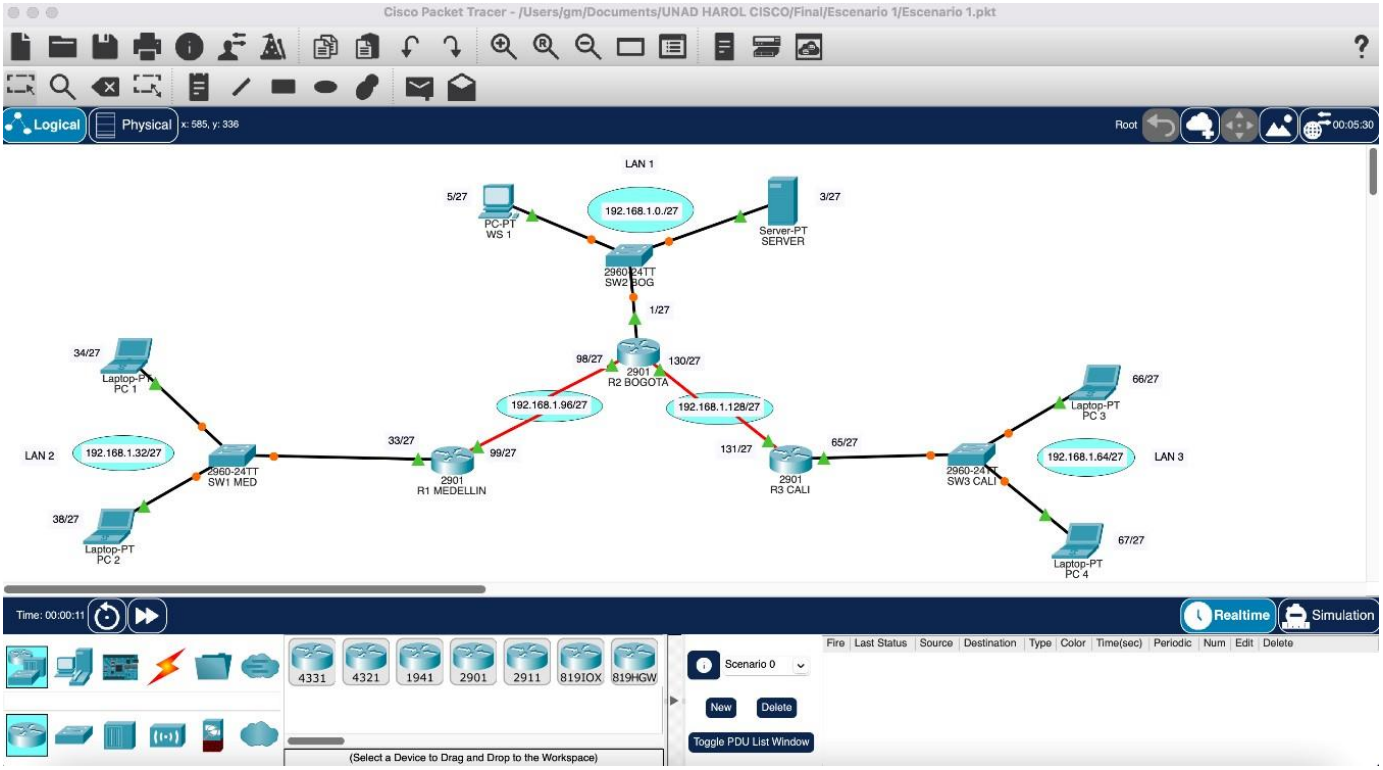
Fuente: (8 de diciembre de 2019). Evaluación – Prueba de habilidades prácticas CCNA.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Figura 2 Equipos de la topología de RED.

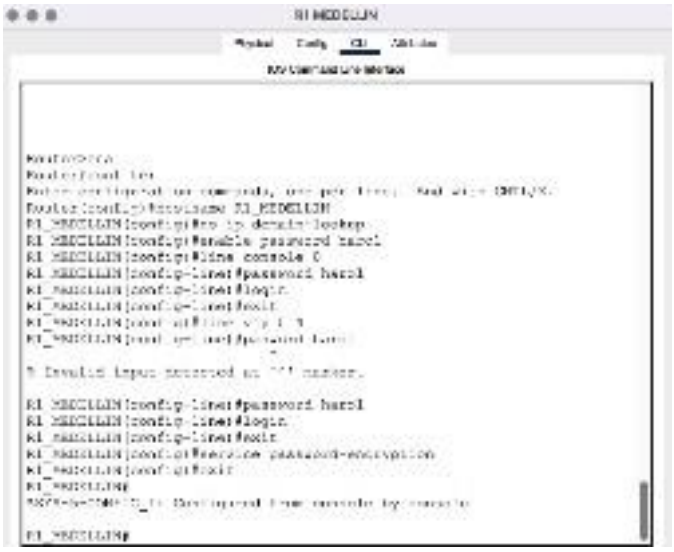


Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Configurar la topología de red

ROUTER 1 MEDELLIN

Figura 3 Configuración Router 1 Medellin



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

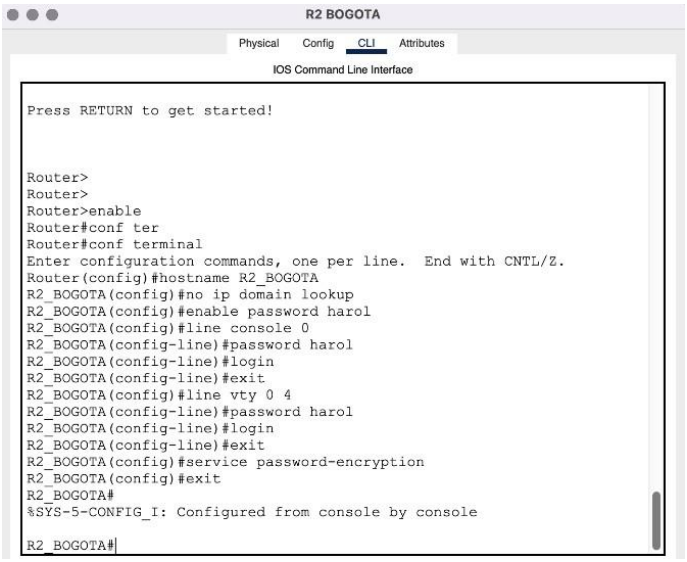
SWITCH 1 MED

Figura 4 Configuración Switch 1 Med

Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 2 BOGOTA

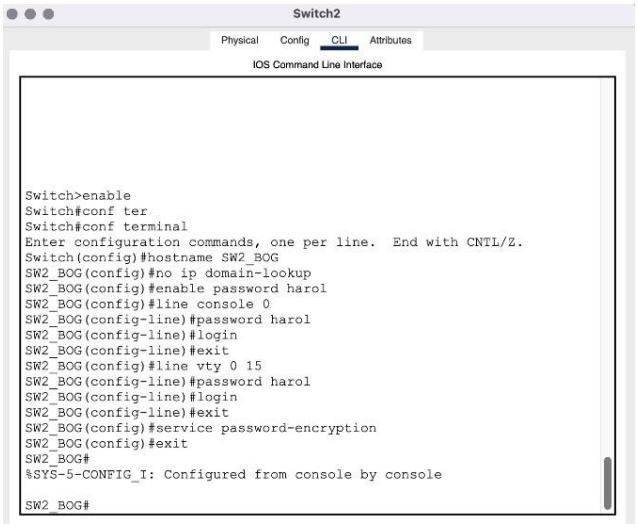
Figura 5 Configuración Router 2 Bogota



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

SWITCH 2 BOG

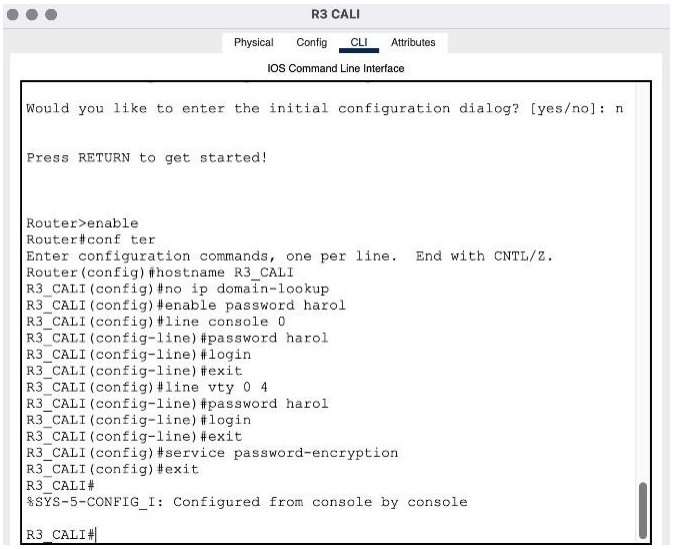
Figura 6 Configuración Switch 2 Bog



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

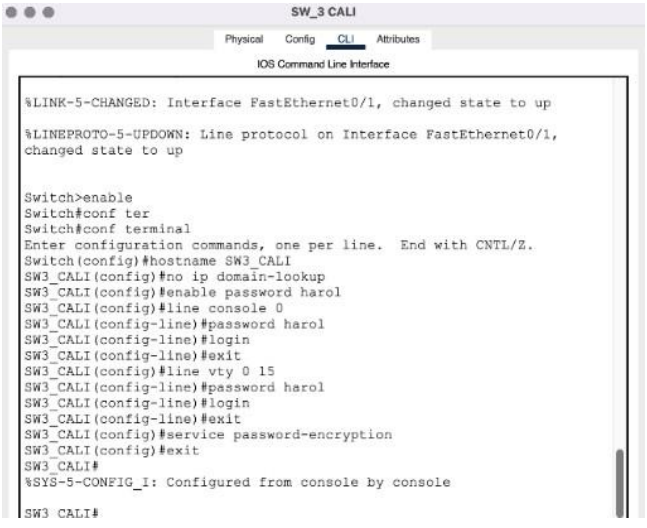
Figura 7 Configuración Router 3 Cali



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

SWITCH 3 CALI

Figura 8 Configuración Switch 3 Cali



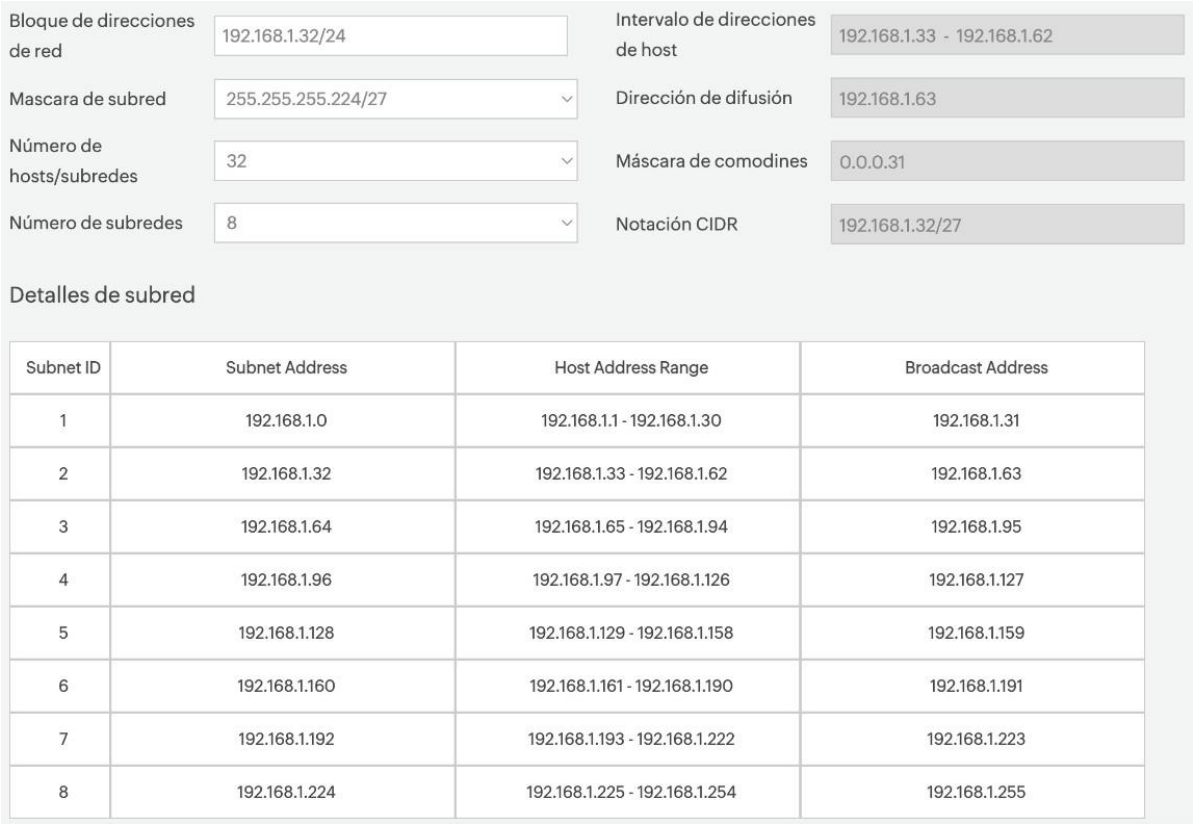
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Parte 1: Asignación de direcciones IP:

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

b) Asignar una dirección IP a la red.

Figura 9 Subnetting de red en 8 partes.



Bloque de direcciones de red	192.168.1.32/24	Intervalo de direcciones de host	192.168.1.33 - 192.168.1.62
Mascara de subred	255.255.255.224/27	Dirección de difusión	192.168.1.63
Número de hosts/subredes	32	Máscara de comodines	0.0.0.31
Número de subredes	8	Notación CIDR	192.168.1.32/27

Detalles de subred

Subnet ID	Subnet Address	Host Address Range	Broadcast Address
1	192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Fuente: Generado y tomado: https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

Parte 2: Configuración Básica.

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

Tabla 1 configuraciones IP de los Routers.

		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
	Host Names	**IP**	**Mask**	**Gateway**
LAN 1	**Server**	**192.168.1.3**	**/27**	**192.168.1.31**
	WS 1	**192.168.1.5**	**/27**	**192.168.1.31**
LAN 2	**PC 1**	**192.168.1.34**	**/27**	**192.168.1.63**
	PC 2	**192.168.1.38**	**/27**	**192.168.1.63**
LAN 3	**PC 3**	**192.168.1.66**	**/27**	**192.168.1.95**
	PC 4	**192.168.1.67**	**/27**	**192.168.1.95**

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Tabla 2 Código de configuraciones IP de los Routers

ROUTER 1 MEDELLIN
Password: R1_MEDELLIN>enable Password: R1_MEDELLIN#confi ter Enter configuration commands, one per line. End with CNTL/Z. R1_MEDELLIN(config)#interface s0/0/0 R1_MEDELLIN(config-if)#ip add 192.168.1.99 255.255.255.224 R1_MEDELLIN(config-if)#no shu R1_MEDELLIN(config-if)#no shutdown

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

R1_MEDELLIN(config-if)#exit

R1_MEDELLIN(config)#exit

R1_MEDELLIN#

R1_MEDELLIN(config)#inter giga0/0

R1_MEDELLIN(config-if)#ip add 192.168.1.33 255.255.255.224

R1_MEDELLIN(config-if)#no shu

R1_MEDELLIN(config-if)#no shutdown

R1_MEDELLIN(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1_MEDELLIN(config-if)#exit

R1_MEDELLIN(config)#

ROUTER 2 BOGOTA

Password:

R2_BOGOTA>ena

Password:

R2_BOGOTA#conf ter

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

R2_BOGOTA(config)#interface s0/0/0

```
R2_BOGOTA(config-if)#ip add 192.168.1.98 255.255.255.224
R2_BOGOTA(config-if)#no shu
R2_BOGOTA(config-if)#no shutdown

R2_BOGOTA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2_BOGOTA(config-if)#exi
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
R2_BOGOTA(config-if)#exit
R2_BOGOTA(config)#interface s0/0/1
R2_BOGOTA(config-if)#ip add 192.168.1.130 255.255.255.224
R2_BOGOTA(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2_BOGOTA(config-if)#exit
R2_BOGOTA(config)#interface giga0/0
R2_BOGOTA(config-if)#ip add 192.168.1.1 255.255.255.224
R2_BOGOTA(config-if)#no shut

R2_BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

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

R2_BOGOTA(config-if)#

ROUTER 3 CALI

Password:

R3_CALI>ena
Password:
R3_CALI#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3_CALI(config)#interface s0/0/0
R3_CALI(config-if)#ip add 192.168.1.131 255.255.255.224
R3_CALI(config-if)#no shut

R3_CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3_CALI(config-if)#exit
R3_CALI(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R3_CALI(config)#interface giga0/0
R3_CALI(config-if)#ip add 192.168.1.65 255.255.255.224
R3_CALI(config-if)#no shut

R3_CALI(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

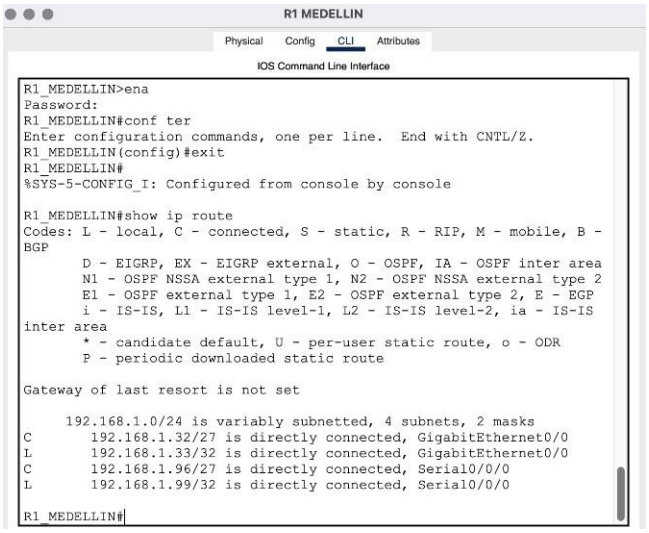
R3_CALI(config-if)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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 1 MEDELLIN

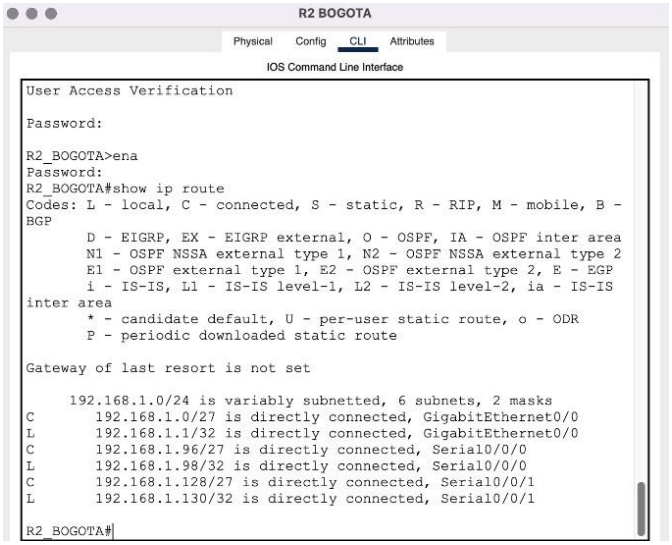
Figura 10 verificación de enrutamiento en el Router 1 Medellin



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 2 BOGOTA

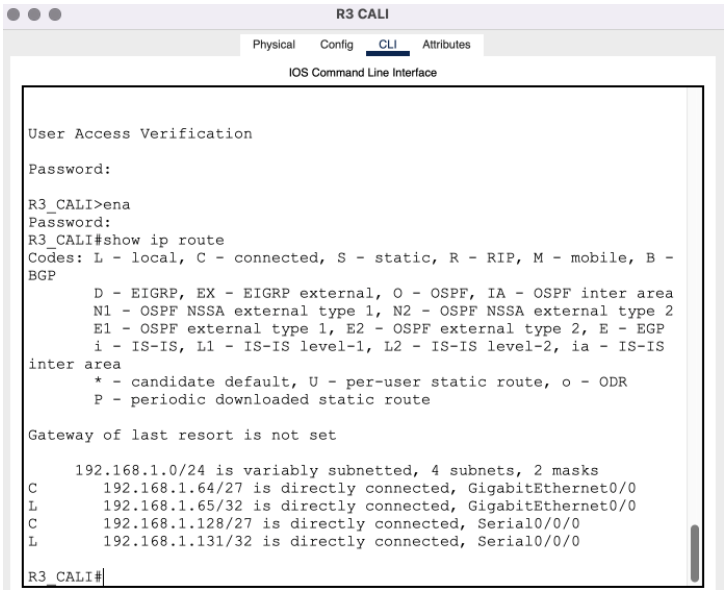
Figura 11 verificación de enrutamiento en el Router 2 Bogota.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

Figura 12 verificación de enrutamiento en el Router 3 Cali.

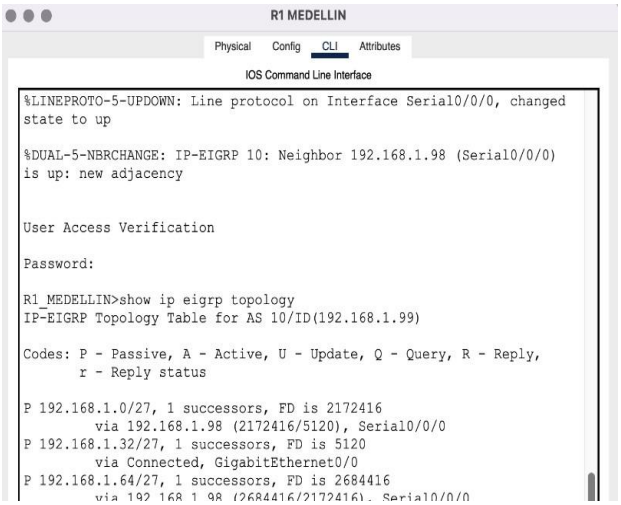


Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

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

ROUTER 1 MEDELLIN

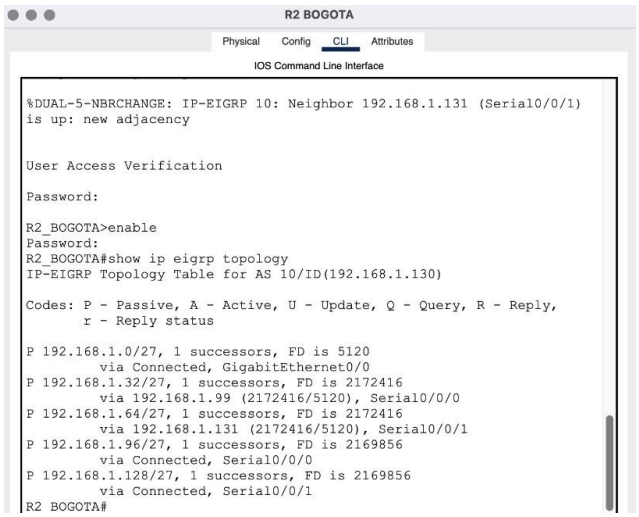
Figura 13 prueba de carga del Router 1 Medellin.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 2 BOGOTA

Figura 14 prueba de carga del Router 2 Bogotá



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

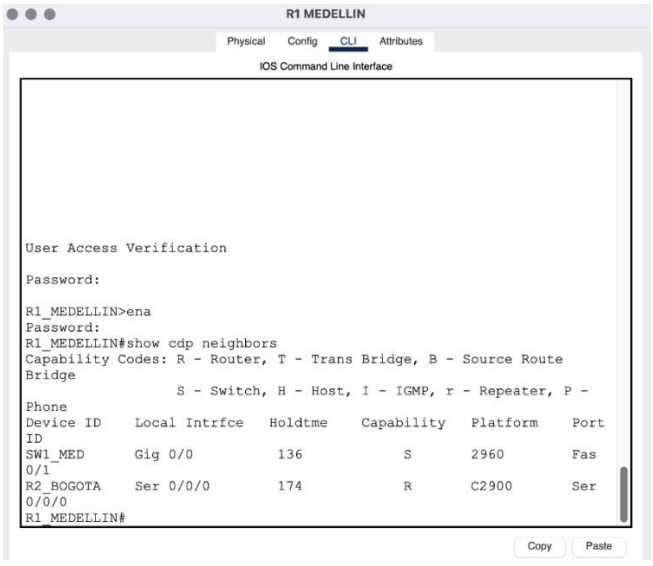
Figura 15 prueba de carga del Router 3 Cali

Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

d) Realizar un diagnóstico de vecinos uando el comando cdp.

ROUTER 1 MEDELLIN

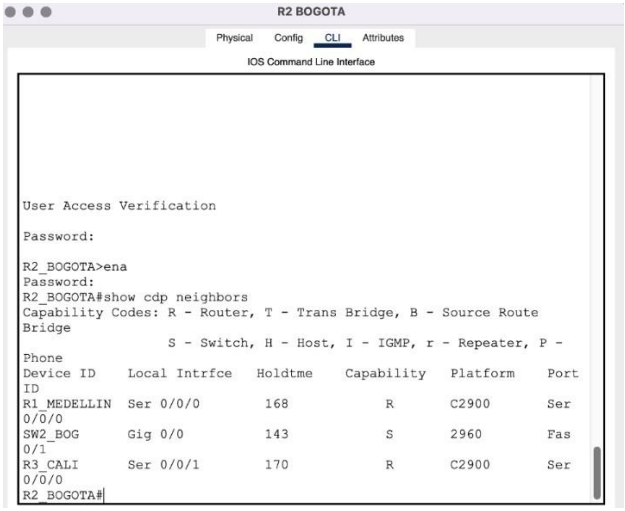
Figura 16 diagnóstico de vecinos Router 1 Medellin.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 2 BOGOTA

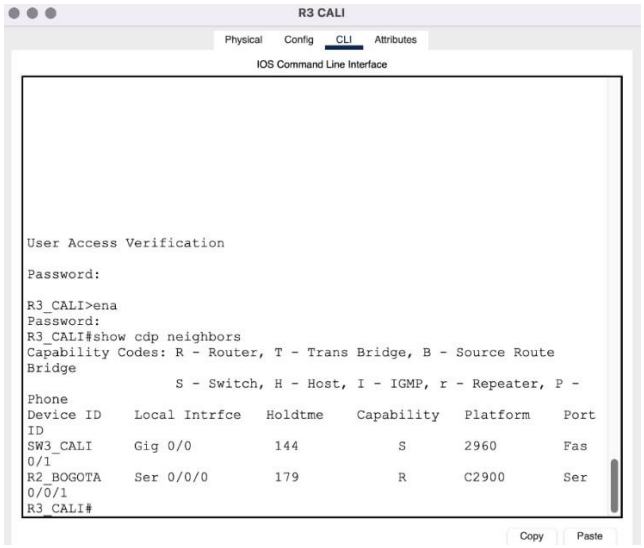
Figura 17 diagnóstico de vecinos Router 2 Bogotá.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

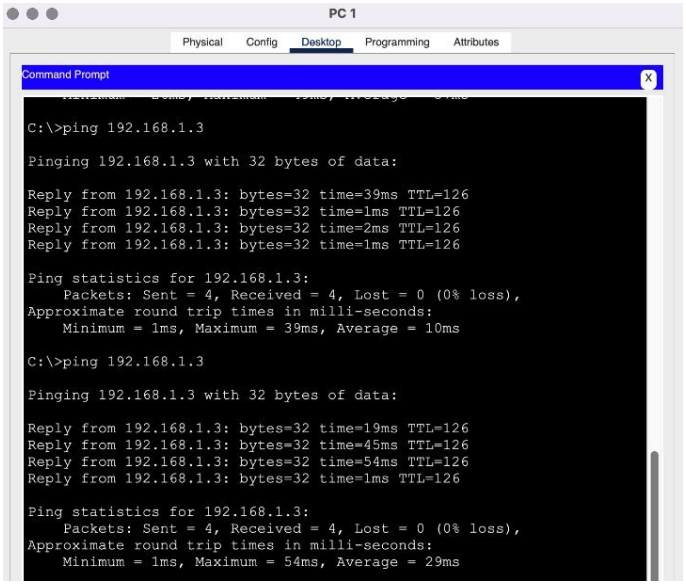
Figura 18 diagnóstico de vecinos Router 3 Cali.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

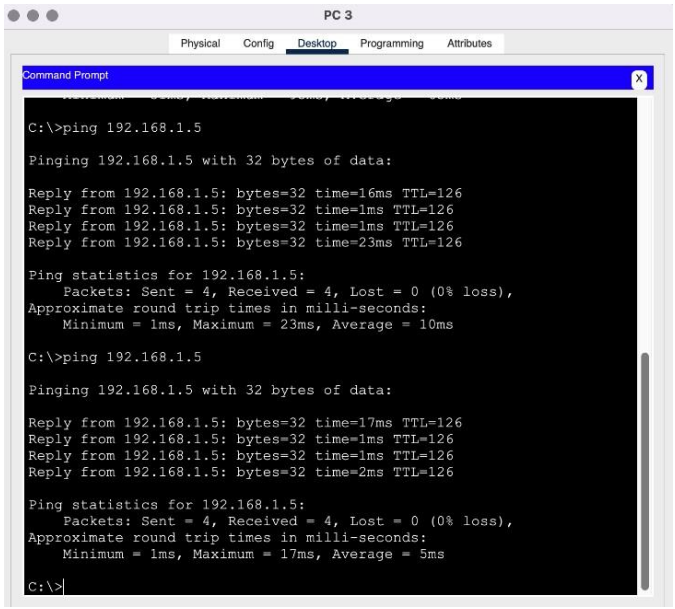
e) Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Figura 19 Ping: PC 1 – Servidor



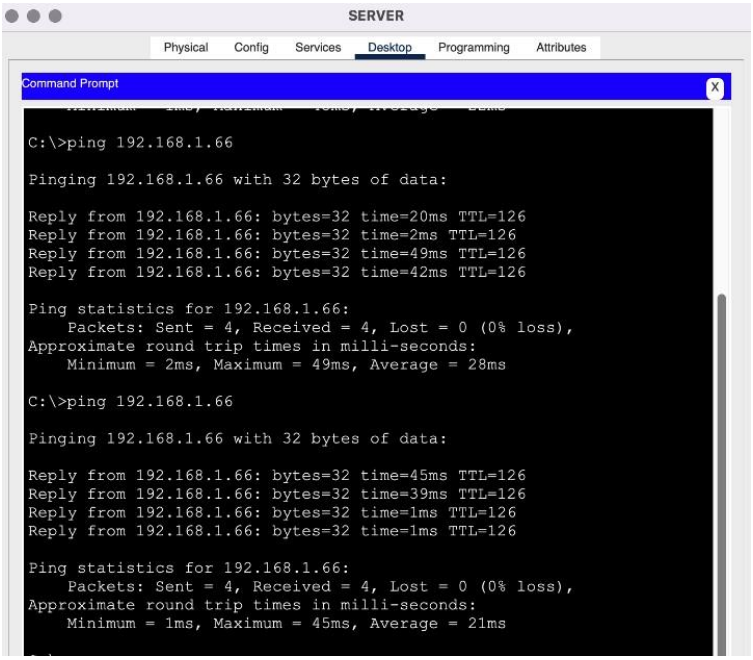
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 20 Ping: PC 3 - WS 1



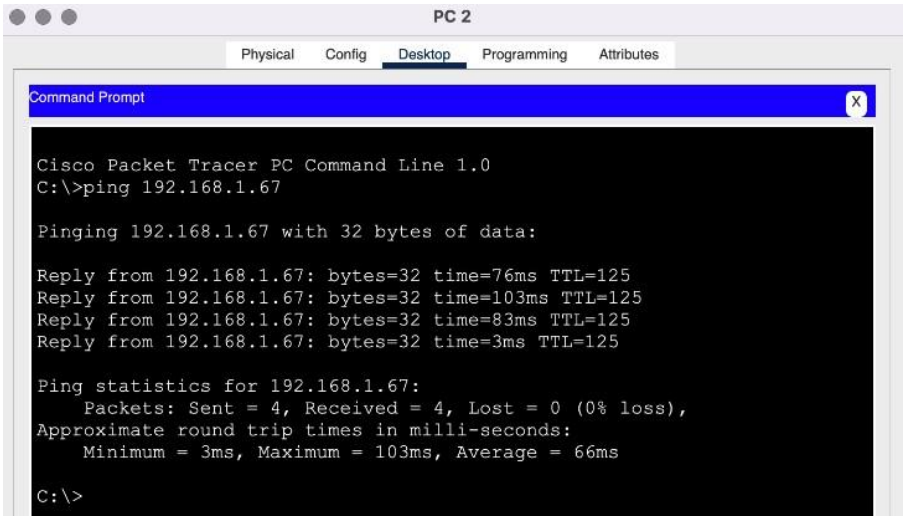
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 21 Ping: PC 2 – PC 4



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 22 Ping: Servidor – PC 3

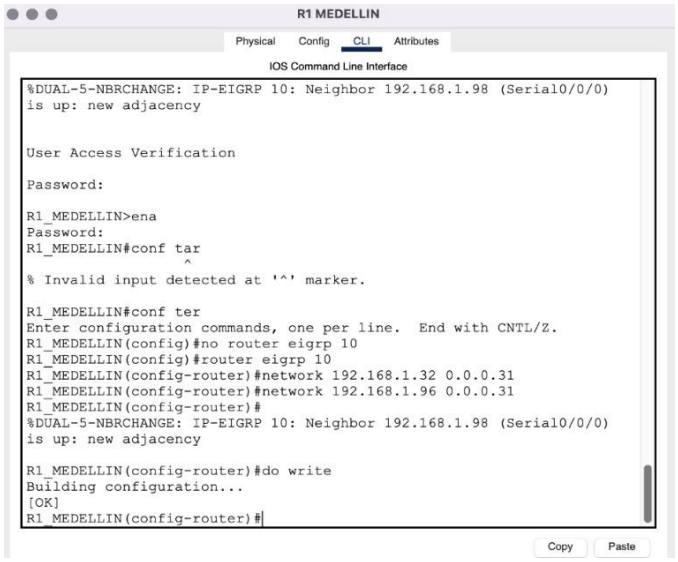


Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Parte 3: Configuración de Enrutamiento.

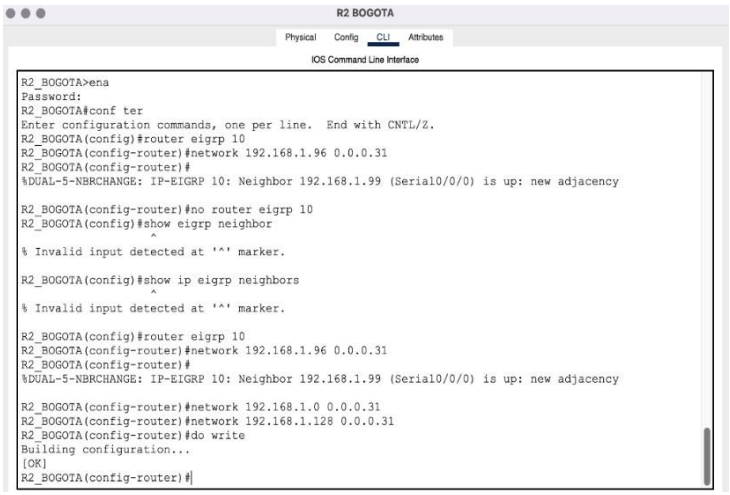
a) Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Figura 23 protocolo de enrutamiento EIGRP Router Medellin.



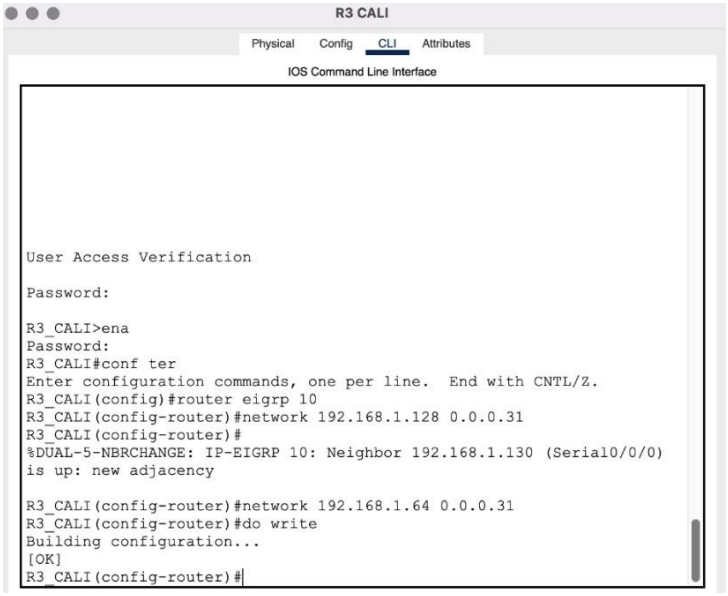
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 24 protocolo de enrutamiento EIGRP Router Bogotá



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

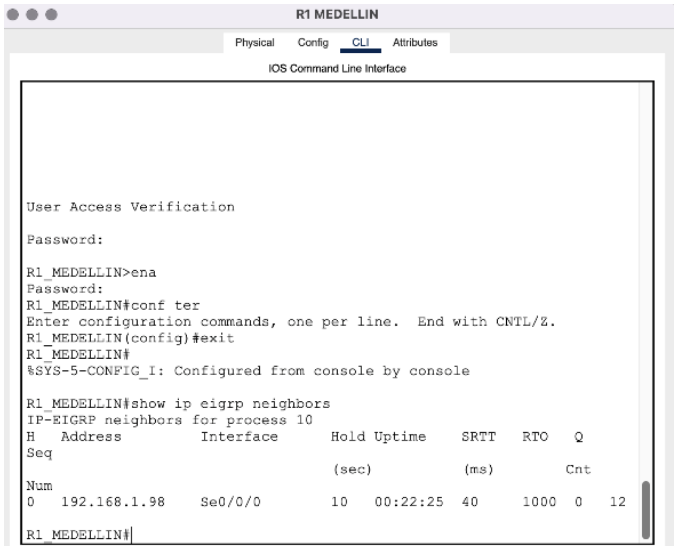
Figura 25 protocolo de enrutamiento EIGRP Router 3 Cali



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

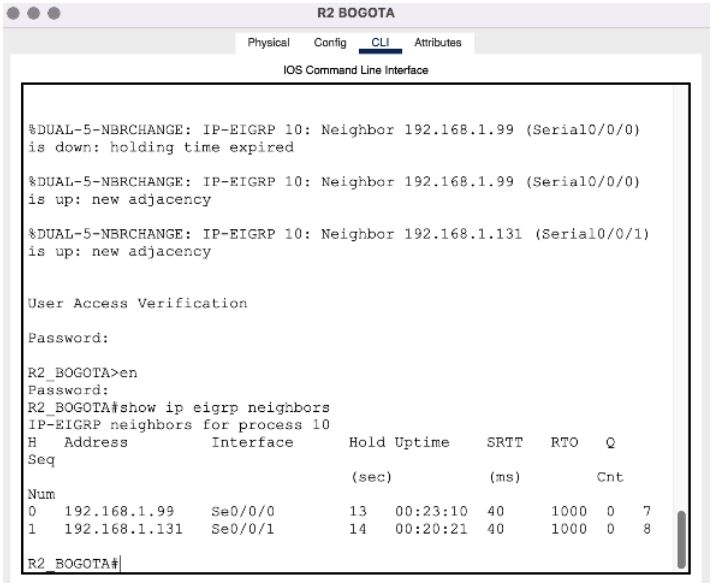
b) Verificar si existe vecindad con los Routers configurados con EIGRP.

Figura 26 Verificar vecindad en el Router Medellín.



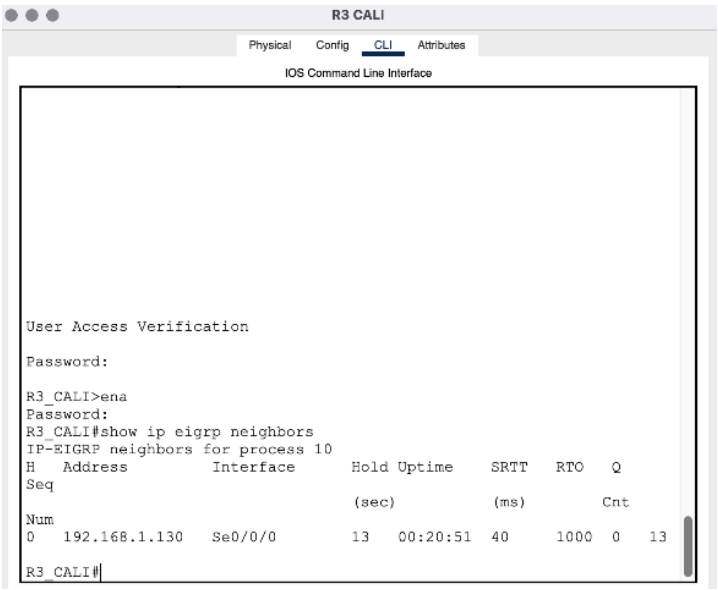
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 27 Verificar vecindad en el Router Bogotá



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

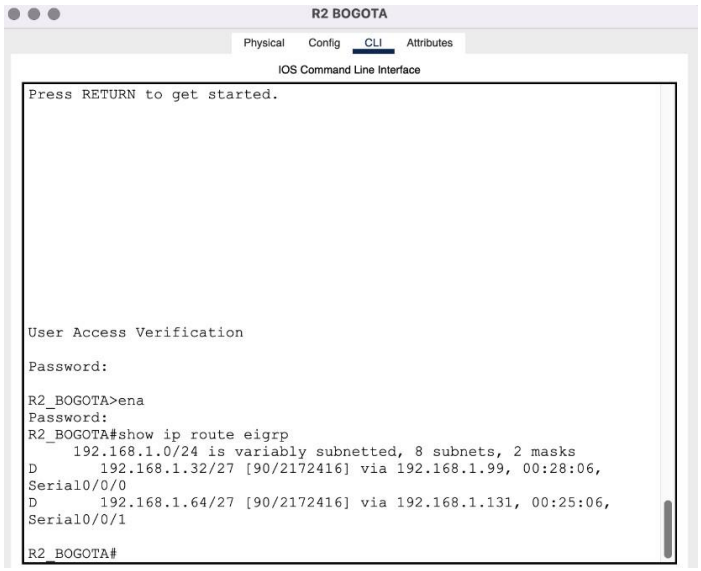
Figura 28 Verificar vecindad en el Router Cali



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

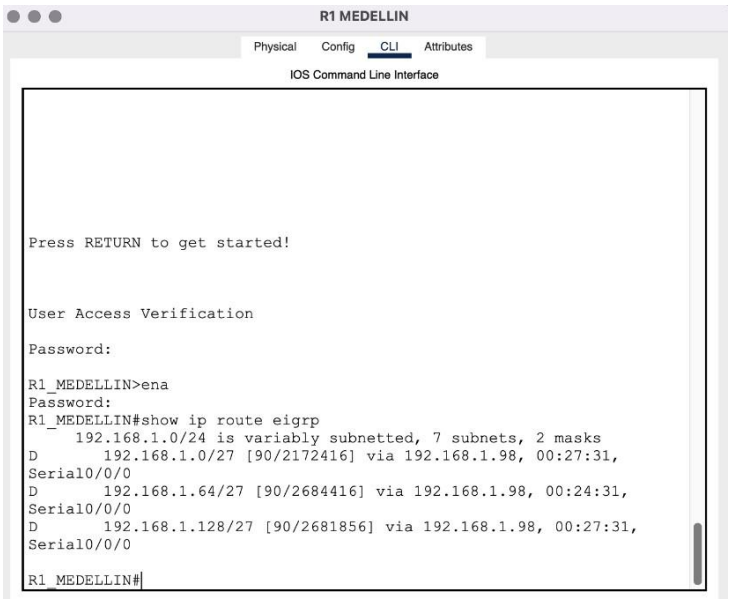
c) Realizar la comprobación de las tablas de enrutamiento en cada uno de los Routers para verificar cada una de las rutas establecidas.

Figura 29 comprobación tablas de enrutamiento Router Bogotá



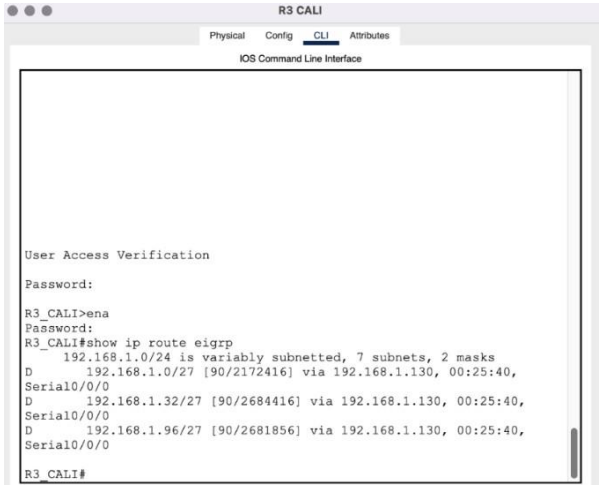
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 30 comprobación de las tablas de enrutamiento Router Medellin.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

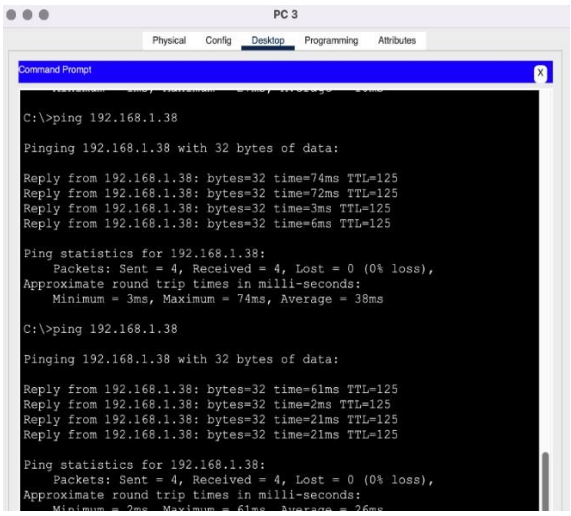
Figura 31 comprobación de las tablas de enrutamiento Router Cali



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

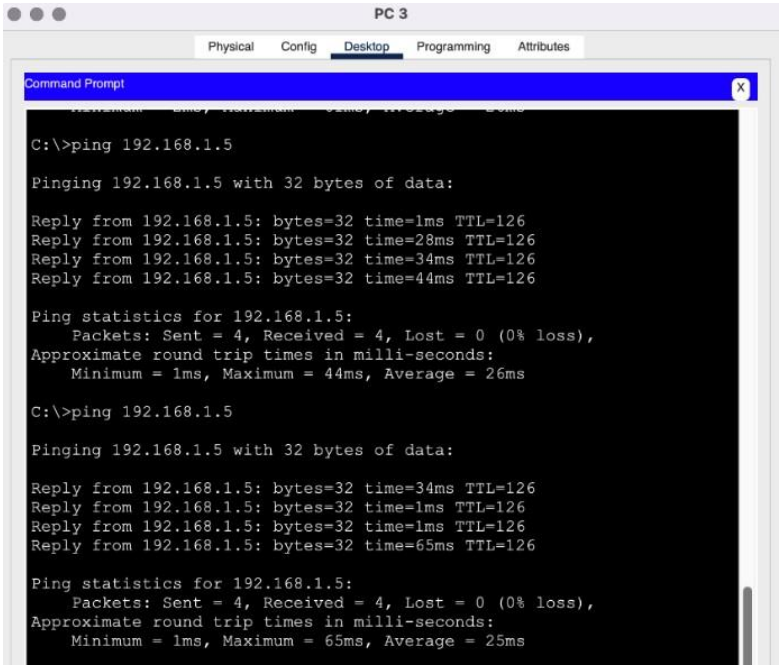
d) Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Figura 32 Ping: PC 3 – PC 2



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

Figura 33 Ping: PC 3 – WS 1



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

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

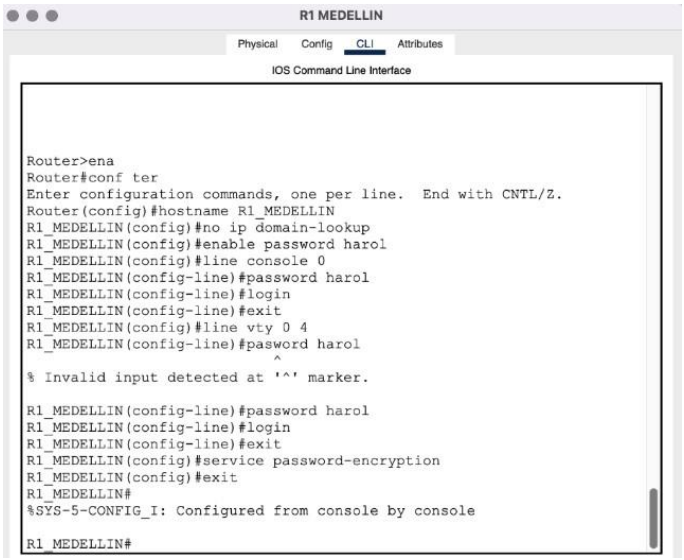
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

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.

ROUTER 1 MEDELLIN

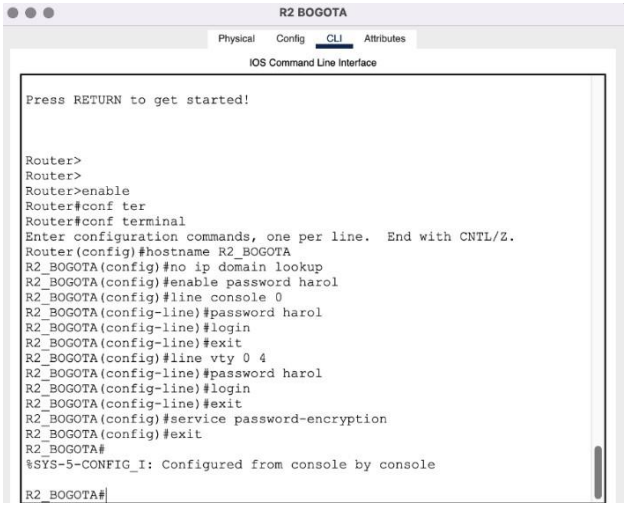
Figura 34 configuración para establecer conexiones telnet Router 1 Medellin.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 2 BOGOTA

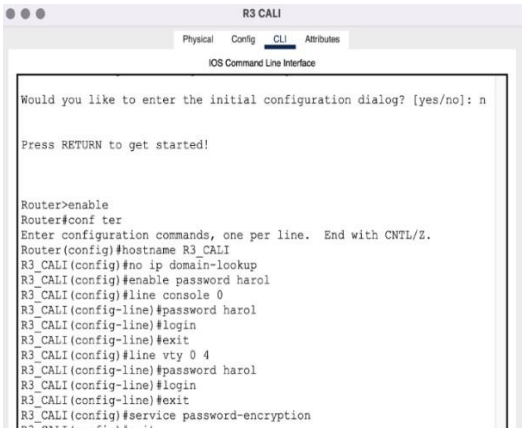
Figura 35 configuración para establecer conexiones telnet Router 2 Bogotá



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

Figura 36 configuración para establecer conexiones telnet Router 3 Cali.



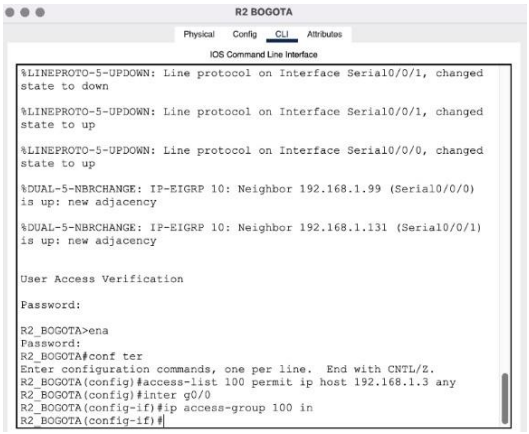
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

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.

ROUTER 2 BOGOTA

El **SERVIDOR** puede hacer ping a cualquier **HOST** de las otras subredes

Figura 37 Ping del servidor a cualquier Host.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 1 MEDELLIN

Los HOSTS de la red 192.168.1.32 (Medellin), pueden hacer ping al **SERVIDOR** (192.168.1.3)

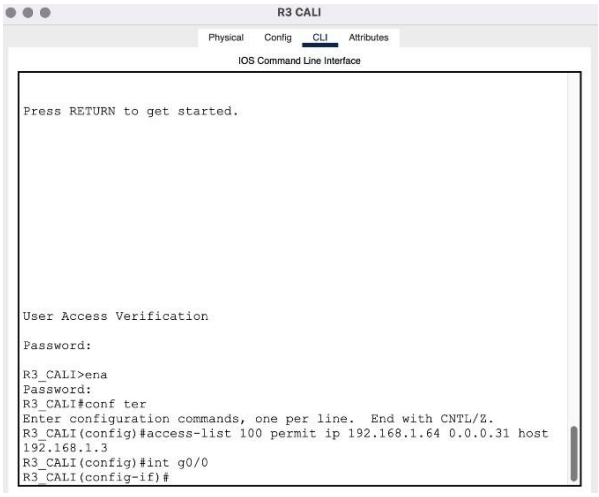
Figura 38 HOSTS de la red 192.168.1.32 (Medellin), pueden hacer ping al SERVIDOR

Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 1 MEDELLIN

Los HOSTS de la red 192.168.1.64 (Cali), pueden hacer ping al SERVIDOR (192.168.1.3)

Figura 39 HOSTS de la red 192.168.1.64 (Cali), pueden hacer ping al SERVIDOR

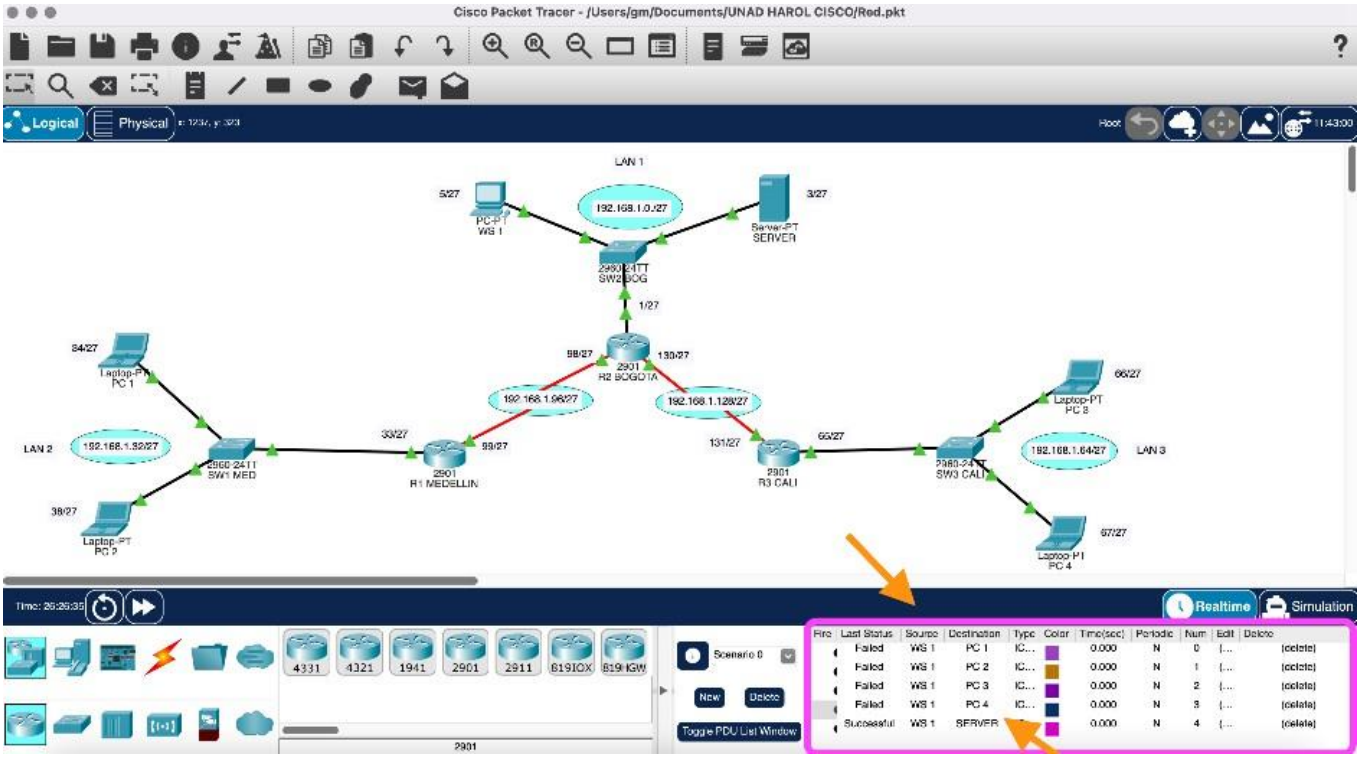


Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

HOST - WS 1 - BOG

El HOST de la red 192.168.1.5 (WS1), no pueden hacer ping al resto de los equipos de las subredes, excepto hacia el SERVIDOR (192.168.1.3)

Figura 40 HOST de la red 192.168.1.5 (WS1), no pueden hacer ping al resto de los equipos de las subredes a excepción del servidor.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

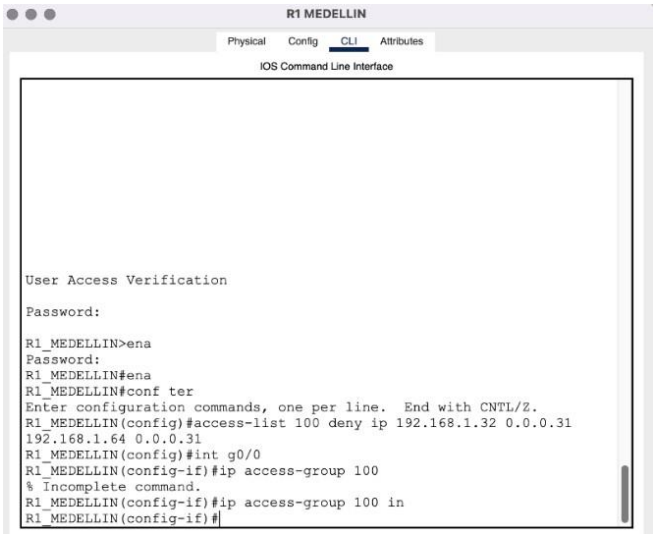
c) Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

ROUTER 1 MEDELLIN

Negando acceso a los equipos de la subred 192.168.1.32 hacia la subred 192.168.1.64.

Los HOSTS 1-2 de la subred 192.168.1.32 (Medellin), no pueden hacer ping hacia los HOSTS 3-4 de la subred 192.168.1.64 (CALI), ni al HOST 192.168.1.5 (WS1), pero si pueden hacer ping al SERVIDOR (192.168.1.3)

Figura 41 ROUTER 1 MEDELLIN, configuración para negar el acceso a equipos fuera de su subred.



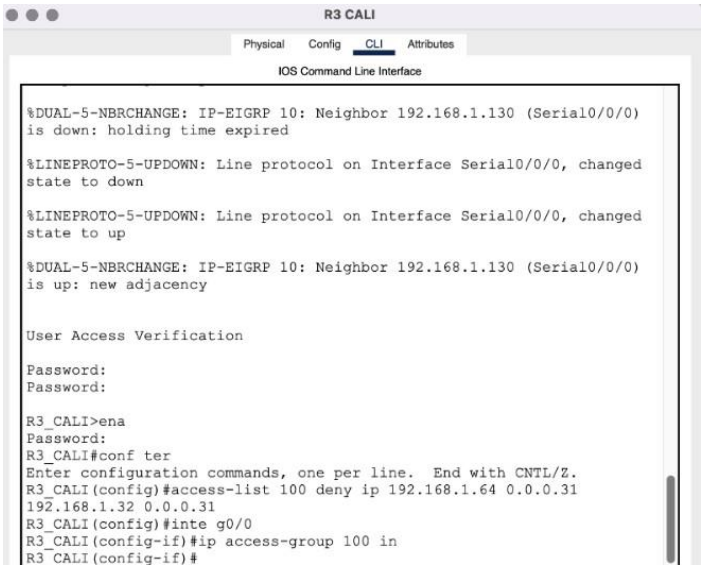
Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

ROUTER 3 CALI

Negando acceso a los equipos de la subred 192.168.1.64 hacia la subred 192.168.1.32.

Los HOSTS 3-4 de la subred 192.168.1.64 (Cali), no pueden hacer ping hacia los HOSTS 1-2 de la subred 192.168.1.32 (CALI), ni al HOST 192.168.1.5 (WS1), pero si pueden hacer ping al SERVIDOR (192.168.1.3)

Figura 41 ROUTER 3 CALI, configuración para negar el acceso a equipos fuera de su subred.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

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.

Tabla 3 condiciones de prueba para confirmar el óptimo funcionamiento de la red

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Password: R1_MEDELLIN>ena Password: Password: R1_MEDELLIN#telnet 192.168.1.131

			Trying 192.168.1.131 ...Open User Access Verification Password: R3_CALI>ena Password: R3_CALI#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3_CALI(config)#exit R3_CALI#exit [Connection to 192.168.1.131 closed by foreign host] R1_MEDELLIN#
	WS_1	**Router BOGOTA**	Cisco Packet Tracer PC Command Line 1.0 C:\>telenet 192.186.1.1 Invalid Command. C:\>telnet 192.186.1.1 Trying 192.186.1.1 ... % Connection timed out; remote host not responding C:\>
	Servidor	**Router CALI**	Cisco Packet Tracer SERVER Command Line 1.0

			C:\>telnet 192.168.1.131 Trying 192.168.1.131 ...Open User Access Verification Password: R3_CALI>ena Password: R3_CALI#config ter Enter configuration commands, one per line. End with CNTL/Z. R3_CALI(config)#exit R3_CALI#exit [Connection to 192.168.1.131 closed by foreign host] C:\>
	Servidor	**Router MEDELLIN**	Cisco Packet Tracer SERVER Command Line 1.0 C:\>telnet 192.168.1.99 Trying 192.168.1.99 ...Open User Access Verification Password: Password: R1_MEDELLIN>ena

			Password: R1_MEDELLIN#confi ter Enter configuration commands, one per line. End with CNTL/Z. R1_MEDELLIN(config)#exit R1_MEDELLIN#exit [Connection to 192.168.1.99 closed by foreign host] C:\>exit
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Cisco Packet Tracer PC Command Line 1.0 C:\>telnet 192.168.1.131 Trying 192.168.1.131 ... % Connection timed out; remote host not responding C:\>
	LAN del Router CALI	**Router CALI**	Cisco Packet Tracer PC Command Line 1.0 C:\>telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding C:\>
	LAN del Router MEDELLIN	**Router MEDELLIN**	:\>telnet 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\>

	LAN del Router CALI	**Router MEDELLIN**	:\>telnet 192.168.1.99 Trying 192.168.1.99 ... % Connection timed out; remote host not responding C:\>
PING	**LAN del Router CALI**	**WS_1**	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.1.5 Pinging 192.168.1.5 with 32 bytes of data: Request timed out. Reply from 192.168.1.65: Destination host unreachable. Reply from 192.168.1.65: Destination host unreachable. Reply from 192.168.1.65: Destination host unreachable. Ping statistics for 192.168.1.5: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>
	LAN del Router MEDELLIN	**WS_1**	C:\>ping 192.168.1.5 Pinging 192.168.1.5 with 32 bytes of data:

			Reply from 192.168.1.33: Destination host unreachable. Reply from 192.168.1.33: Destination host unreachable. Reply from 192.168.1.33: Destination host unreachable. Reply from 192.168.1.33: Destination host unreachable. Ping statistics for 192.168.1.5: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>
	LAN del Router MEDELLIN	**LAN del Router CALI**	Password: R1_MEDELLIN>ena Password: R1_MEDELLIN#ping 192.168.1.131 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 43/65/80 ms R1_MEDELLIN#

PING	**LAN del Router CALI**	**Servidor**	Password: R1_MEDELLIN>ena Password: R1_MEDELLIN#ping 192.168.1.131 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 43/65/80 ms R1_MEDELLIN#
	LAN del Router MEDELLIN	**Servidor**	Password: R1_MEDELLIN>ena Password: R1_MEDELLIN#ping 192.168.1.131 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 43/65/80 ms R1_MEDELLIN#

	Servidor	**LAN del Router MEDELLIN**	Password: R1_MEDELLIN>ena Password: R1_MEDELLIN#ping 192.168.1.131 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 43/65/80 ms R1_MEDELLIN#
	Servidor	**LAN del Router CALI**	Cisco Packet Tracer SERVER Command Line 1.0 C:\>ping 192.168.1.131 Pinging 192.168.1.131 with 32 bytes of data: Reply from 192.168.1.131: bytes=32 time=35ms TTL=254 Reply from 192.168.1.131: bytes=32 time=28ms TTL=254 Reply from 192.168.1.131: bytes=32 time=1ms TTL=254 Reply from 192.168.1.131: bytes=32 time=21ms TTL=254

			Ping statistics for 192.168.1.131: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 35ms, Average = 21ms C:\> Password: R3_CALI>ena Password: R3_CALI#ping 192.168.1.34 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds: ..... Success rate is 0 percent (0/5) R3_CALI#
	Router CALI	**LAN del Router MEDELLIN**	
	Router MEDELLIN	**LAN del Router CALI**	R1_MEDELLIN#ping 192.168.1.66 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds: .....

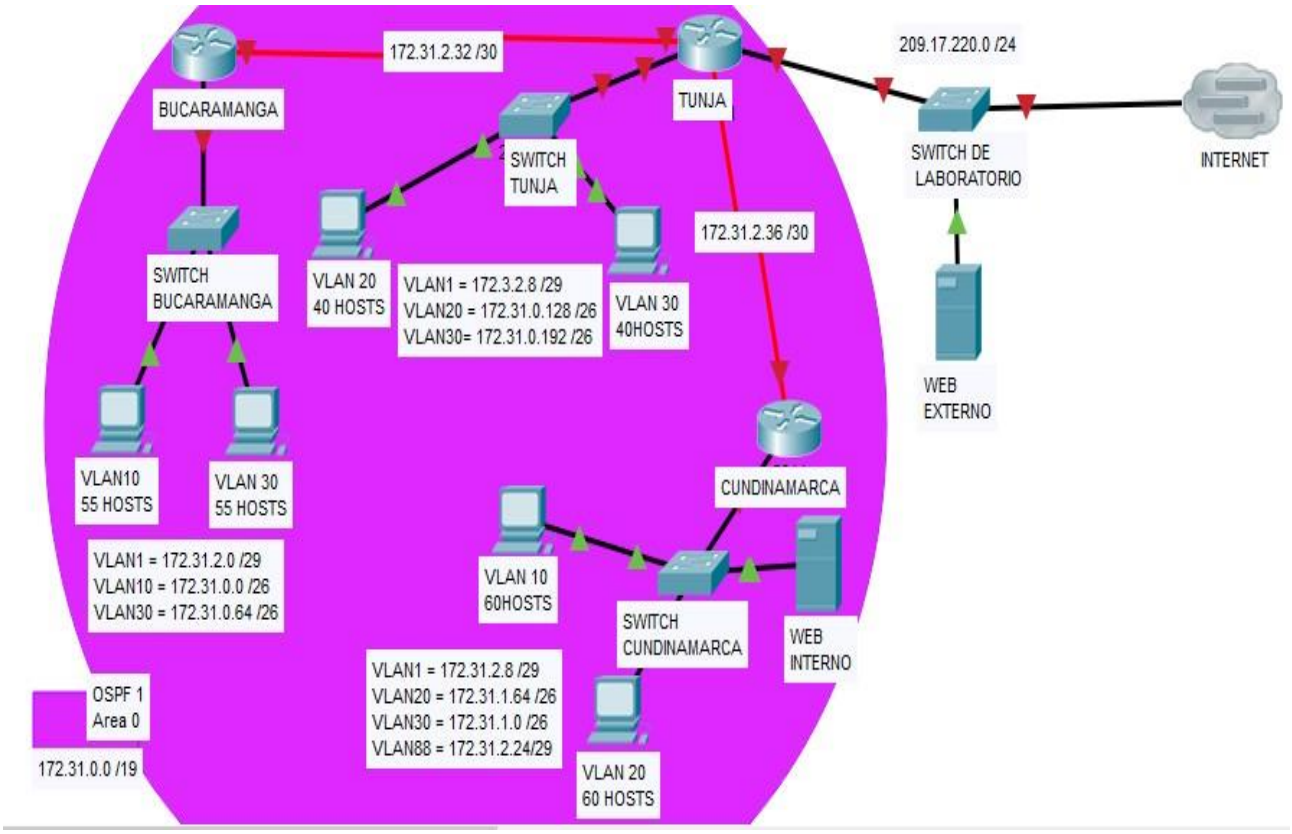
			Success rate is 0 percent (0/5) R1_MEDELLIN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

ESCENARIO 2

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

Figura 42 Configuración propuesta.

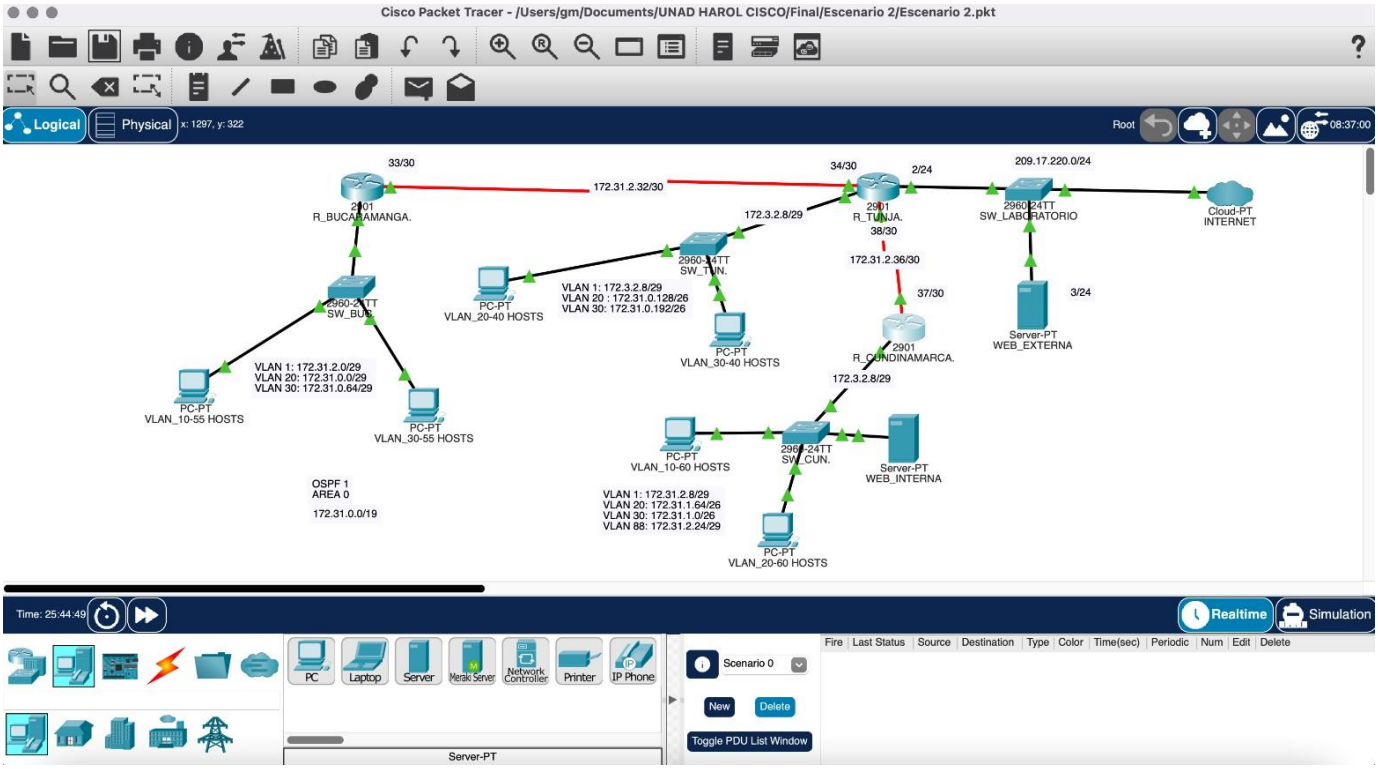


Fuente: (8 de diciembre de 2019). Evaluación – Prueba de habilidades prácticas CCNA.

Desarrollo

Los siguientes son los requerimientos necesarios.

Figura 43 Configuración de la topología de red.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

1. Todos los Routers deberán tener lo siguiente:

- Configuración básica.

Tabla 3 Configuración básica de Routers.

R_BUC Name and IP
Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R_BUC

R_BUC(config)#no ip domain-lookup
R_BUC(config)#interface s0/0/0
R_BUC(config-if)#ip address 172.31.2.33 255.255.255.252
R_BUC(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R_BUC(config-if)#exit
R_BUC(config)#interface g0/0
R_BUC(config-if)#no shutdown

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

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

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

R_BUC#write
Building configuration...
[OK]
R_BUC#

R_TUN
Name and IP

Router>enable
Router#configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R_TUN
R_TUN(config)#no ip domain-lookup
R_TUN(config)#interface s0/0/0
R_TUN(config-if)#ip address 172.31.2.34 255.255.255.252
R_TUN(config-if)#no shutdown

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

R_TUN(config-if)#ex
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R_TUN(config)#interface s0/0/1
R_TUN(config-if)#ip address 172.31.2.38 255.255.255.252
R_TUN(config-if)#clock rate 128000
R_TUN(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R_TUN(config-if)#
R_TUN(config-if)#exit
R_TUN(config)#end
R_TUN#
%SYS-5-CONFIG_I: Configured from console by console

R_TUN#write
Building configuration...
[OK]
```

```
R_TUN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUN(config)#interface g0/1
R_TUN(config-if)#ip add 209.17.220.2 255.255.255.0
R_TUN(config-if)#no shutdown

R_TUN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

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

R_TUN(config-if)#exit
R_TUN(config)#interface g0/0
R_TUN(config-if)#no shutdown

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

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

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

R_TUN#write

Building configuration...

[OK]

R_TUN#

R_CUN
Name and IP

Router>enable

Router#configure terminal

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

Router(config)#hostname R_CUN

R_CUN(config)#no ip domain-lookup

R_CUN(config)#interface s0/0/0

R_CUN(config-if)#ip address 172.31.2.37 255.255.255.252

R_CUN(config-if)#no shutdown

R_CUN(config-if)#

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

R_CUN(config-if)#

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

R_CUN(config-if)#exit

R_CUN(config)#end

R_CUN#

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

R_CUN#write

Building configuration...

[OK]

R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#interface g0/0 R_CUN(config-if)#no shutdown R_CUN(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R_CUN(config-if)#exit R_CUN(config)#end R_CUN# %SYS-5-CONFIG_I: Configured from console by console R_CUN#write Building configuration... [OK] R_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Tabla 4 Configuración de las VLAN de los Routers.

R_BUC VLAN
R_BUC>enable Password: R_BUC#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

```
R_BUC(config)#interface g0/0
R_BUC(config-if)#no shutdown
R_BUC(config-if)#exit
R_BUC(config)#interface g0/0.10
R_BUC(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.10, changed state to up

R_BUC(config-subif)#encap ?
dot1Q IEEE 802.1Q Virtual LAN
R_BUC(config-subif)#encapsulation dot1Q 10
R_BUC(config-subif)#ip address 172.31.0.1 255.255.255.192
R_BUC(config-subif)#exit
R_BUC(config)#exit
R_BUC#
%SYS-5-CONFIG_I: Configured from console by console

R_BUC#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_BUC(config)#interface g0/0.30
R_BUC(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.30, changed state to up
```

R_BUC(config-subif)#encapsulation dot1Q 30
R_BUC(config-subif)#ip add 172.31.0.65 255.255.255.192
R_BUC(config-subif)#exit
R_BUC(config)#interface g0/0.1
R_BUC(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to up

R_BUC(config-subif)#encapsulation dot1Q 1
R_BUC(config-subif)#ip add 172.31.2.1 255.255.255.248
R_BUC(config-subif)#exit
R_BUC(config)#do write
Building configuration...
[OK]
R_BUC(config)#

R_TUN
VLAN

R_TUN>enable
Password:
R_TUN#config term
Enter configuration commands, one per line. End with CNTL/Z.
R_TUN(config)#interface g0/0.20
R_TUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

R_TUN(config-subif)#encapsulation dot1Q 20
R_TUN(config-subif)#ip add 172.31.0.129 255.255.255.192
R_TUN(config-subif)#exit
R_TUN(config)#interface g0/0.30
R_TUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

R_TUN(config-subif)#encapsulation dot1Q 30
R_TUN(config-subif)#ip add 172.31.0.193 255.255.255.192
R_TUN(config-subif)#exit
R_TUN(config)#interface g0/0.1
R_TUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to up

R_TUN(config-subif)#encapsulation dot1Q 1
R_TUN(config-subif)#ip add 172.31.2.9 255.255.255.248
R_TUN(config-subif)#exit
R_TUN(config)#do write
```

Building configuration...

[OK]

R_TUN(config)#no shutdown

^

% Invalid input detected at '^' marker.

R_TUN(config)#interface g0/0

R_TUN(config-if)#no shutdown

R_TUN(config-if)#ip add 172.31.2.9 255.255.255.248

% 172.31.2.8 overlaps with GigabitEthernet0/0.1

R_TUN(config-if)#no shutdown

R_TUN(config-if)#exit

R_TUN(config)#exit

R_TUN#

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

R_TUN#

R_CUN

VLAN

R_CUN>enable

Password:

R_CUN#conf ter

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

R_CUN(config)#interface g0/0.20

R_CUN(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

```
R_CUN(config-subif)#encapsulation dot1Q 20
R_CUN(config-subif)#ip address 172.31.1.65 255.255.255.192
R_CUN(config-subif)#exit
R_CUN(config)#interface g0/0.88
R_CUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.88, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.88, changed state to up

R_CUN(config-subif)#encapsulation dot1Q 88
R_CUN(config-subif)#ip address 172.31.2.25 255.255.255.248
R_CUN(config-subif)#exit
R_CUN(config)#interface g0/0.1
R_CUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.1, changed state to up

R_CUN(config-subif)#encapsulation dot1Q 1
R_CUN(config-subif)#ip add 172.31.2.9 255.255.255.248
R_CUN(config-subif)#exit
R_CUN(config)#do write
Building configuration...
[OK]
R_CUN(config)#
```

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Tabla 5 Configuración de los nombres e interfaces de las VLAN.

SW_BUC Names VLAN
Switch>ena Switch#conf ter Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname SW_BUC SW_BUC(config)#no ip domain-lookup SW_BUC(config)#vlan 10 SW_BUC(config-vlan)#name vlan10 SW_BUC(config-vlan)#exit SW_BUC(config)#vlan 30 SW_BUC(config-vlan)#name vlan30 SW_BUC(config-vlan)#exit SW_BUC(config)#interface range f0/1 - 5 SW_BUC(config-if-range)#switchport mode access SW_BUC(config-if-range)#switchport access vlan 10 SW_BUC(config-if-range)#no shutdown SW_BUC(config-if-range)#exit SW_BUC(config)#interface range f0/6 - 10 SW_BUC(config-if-range)#switchport mode access SW_BUC(config-if-range)#switchport access vlan 30 SW_BUC(config-if-range)#no shutdown SW_BUC(config-if-range)#exit SW_BUC(config)#inter g0/1 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

SW_BUC(config-if)#no shutdown
SW_BUC(config-if)#switchport mode trunk
SW_BUC(config-if)#exit
SW_BUC(config)#do write
Building configuration...
[OK]
SW_BUC(config)#

SW_TUN
Names VLAN

Switch>enable
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_TUN
SW_TUN(config)#no ip domain-lookup
SW_TUN(config)#vlan 20
SW_TUN(config-vlan)#name vlan20
SW_TUN(config-vlan)#exit
SW_TUN(config)#vlan 30
SW_TUN(config-vlan)#name vlan30
SW_TUN(config-vlan)#exit
SW_TUN(config)#interface range f0/1 - 5
SW_TUN(config-if-range)#switchport mode access
SW_TUN(config-if-range)#switchport access vlan 20
SW_TUN(config-if-range)#no shutdown

SW_TUN(config-if-range)#exit
SW_TUN(config)#inter range f0/6 - 10
SW_TUN(config-if-range)#switchport mode access
SW_TUN(config-if-range)#switchport access vlan 30
SW_TUN(config-if-range)#no shutdown
SW_TUN(config-if-range)#exit
SW_TUN(config)#inter g0/1
SW_TUN(config-if)#switchport mode trunk

SW_TUN(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

SW_TUN(config-if)#no shutdown
SW_TUN(config-if)#switchport mode trunk
SW_TUN(config-if)#exit
SW_TUN(config)#do write
Building configuration...
[OK]
SW_TUN(config)#

SW_CUN
Names VLAN

Switch>ena
Switch#conf ter

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_CUN
SW_CUN(config)#no ip domain-lookup
SW_CUN(config)#vlan 88
SW_CUN(config-vlan)#name vlan88
SW_CUN(config-vlan)#exit
SW_CUN(config)#vlan 10
SW_CUN(config-vlan)#name vlan10
SW_CUN(config-vlan)#exit
SW_CUN(config)#vlan 20
SW_CUN(config-vlan)#name vlan20
SW_CUN(config-vlan)#inter f0/1
SW_CUN(config-if)#switchport mode access
SW_CUN(config-if)#switchport access vlan 88
SW_CUN(config-if)#exit
SW_CUN(config)#interface range f0/2 - 10
SW_CUN(config-if-range)#switchport mode access
SW_CUN(config-if-range)#switchport access vlan 10
SW_CUN(config-if-range)#no shutdown
SW_CUN(config-if-range)#exit
SW_CUN(config)#interface range f0/11 - 20
SW_CUN(config-if-range)#switchport mode access
SW_CUN(config-if-range)#switchport access vlan 20
SW_CUN(config-if-range)#no shutdown
SW_CUN(config-if-range)#exit
SW_CUN(config)#inter g0/1
SW_CUN(config-if)#no shutdown
SW_CUN(config-if)#switchport mode trunk
```

SW_CUN(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 SW_CUN(config-if)#no shutdown SW_CUN(config-if)#switchport mode trunk SW_CUN(config-if)#exit SW_CUN(config)#do write Building configuration... [OK] SW_CUN(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

- Autenticación local con AAA.

Tabla 6 Autenticación local de los routers con AAA.

R_BUC
R_BUC>enable R_BUC#configure termina Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#ip domain name harol.org R_BUC(config)#ip ssh version 2 R_BUC(config)#crypto key generate rsa % You already have RSA keys defined named R_BUC.harol.org . % Do you really want to replace them? [yes/no]: y The name for the keys will be: R_BUC.harol.org

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R_BUC(config)#aaa new-model
*Mar 1 1:13:17.583: %SSH-5-ENABLED: SSH 2 has been enabled
R_BUC(config)#aaa authentication login harol group radius local enable
R_BUC(config)#radius-server host 172.31.2.26 key 19002022
R_BUC(config)#line vty 0 4
R_BUC(config-line)#transport input ssh
R_BUC(config-line)#login authentication harol
R_BUC(config-line)#exit
R_BUC(config)#username harol22 secret harol22
R_BUC(config)#username harol secret harol
R_BUC(config)#do write
Building configuration...
[OK]
R_BUC(config)#exit
R_BUC#
%SYS-5-CONFIG_I: Configured from console by console

R_TUN

R_TUN>enable
R_TUN#conf ter

```
Enter configuration commands, one per line. End with CNTL/Z.
R_TUN(config)#ip domain name harol.org
R_TUN(config)#ip ssh version 2
R_TUN(config)#crypto key generate rsa
% You already have RSA keys defined named R_TUN.harol.org .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: R_TUN.harol.org
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512
may take
a few minutes.

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

R_TUN(config)#aaa new-model
*Mar 1 1:18:28.881: %SSH-5-ENABLED: SSH 2 has been enabled
R_TUN(config)#aaa authentication login harol group radius local
enable
R_TUN(config)#radius-server host 172.31.2.26 key 19002022
R_TUN(config)#line vty 0 4
R_TUN(config-line)#transport input ssh
R_TUN(config-line)#login authentication harol
R_TUN(config-line)#exit
R_TUN(config)#username harol22 secret harol22
R_TUN(config)#username harol secret harol
R_TUN(config)#
R_TUN(config)#do write
```

Building configuration...

[OK]

R_TUN(config)#

R_CUN

R_CUN>enable

R_CUN#conf ter

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

R_CUN(config)#ip domain name harol.org

R_CUN(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

R_CUN(config)#crypto key generate rsa

The name for the keys will be: R_CUN.harol.org

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R_CUN(config)#aaa new-model

*Mar 1 1:22:13.76: %SSH-5-ENABLED: SSH 2 has been enabled

R_CUN(config)#aaa authentication login harol group radius local enable

R_CUN(config)#radius-server host 172.31.2.26 key 19002022

R_CUN(config)#line vty 0 4

R_CUN(config-line)#transport input ssh

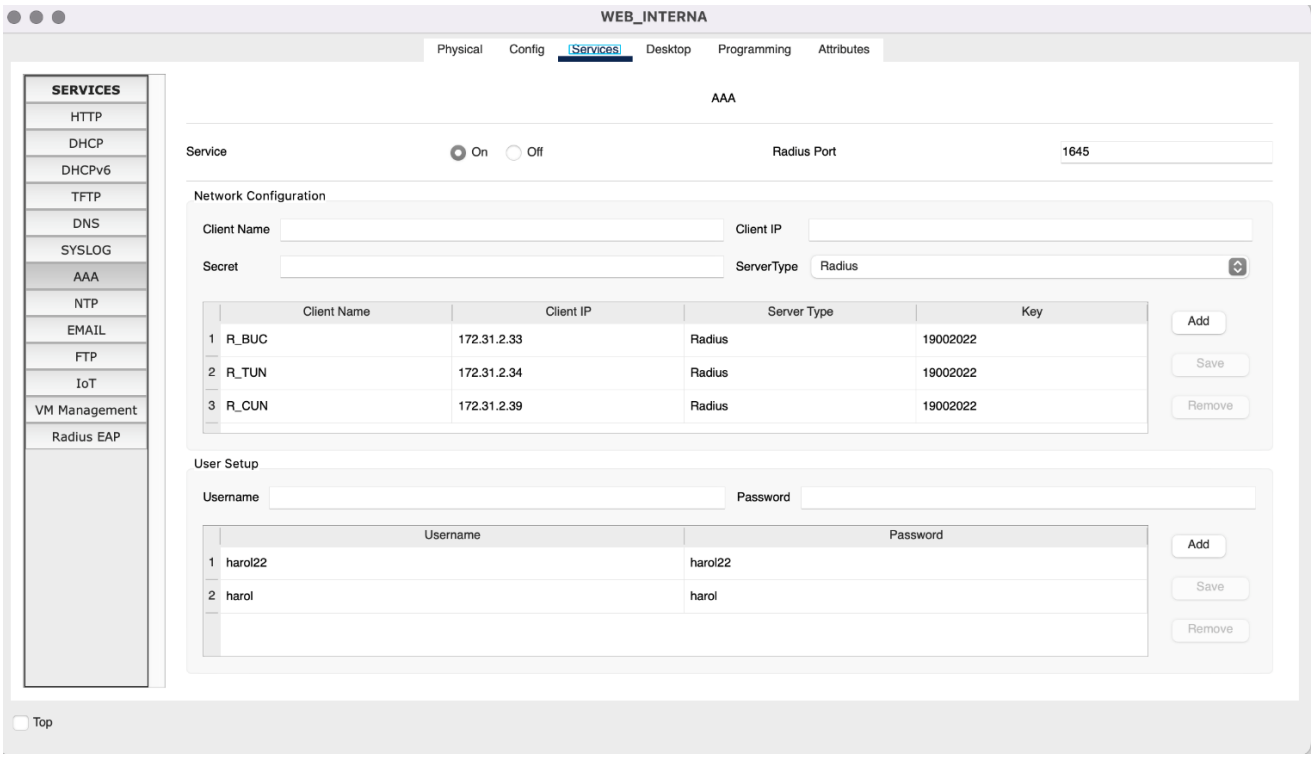
R_CUN(config-line)#login authentication harol

R_CUN(config-line)#exit

```
R_CUN(config)#username harol22 secret harol22
R_CUN(config)#username harol secret harol
R_CUN(config)#do write
Building configuration...
[OK]
R_CUN(config)#
```

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Figura 44 Verificación de servicios AAA de los Routers.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

- Cifrado de contraseñas.

Tabla 7 Cifrado con contraseña de los Routers.

R_BUC
User Access Verification Username: harol Password: R_BUC>enable R_BUC#conf term Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#service password-encryption R_BUC(config)#enable secret harol R_BUC(config)#exit R_BUC# %SYS-5-CONFIG_I: Configured from console by console R_BUC#
R_TUN
R_TUN>ena R_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_TUN(config)#service password-encryption R_TUN(config)#enable secret harol R_TUN(config)#exit R_TUN# %SYS-5-CONFIG_I: Configured from console by console R_TUN#
R_CUN
R_CUN>enable

R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#service password-encryption R_CUN(config)#enable secret harol R_CUN(config)#exit R_CUN# %SYS-5-CONFIG_I: Configured from console by console R_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Tabla 8 Cifrado con contraseña de los Switches.

SW_BUC
SW_BUC>enable SW_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. SW_BUC(config)#line console 0 SW_BUC(config-line)#password harol SW_BUC(config-line)#exit SW_BUC(config)#service password-encryption SW_BUC(config)#enable secret harol SW_BUC(config)#do write Building configuration... [OK] SW_BUC(config)#
SW_TUN
SW_TUN>ena SW_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. SW_TUN(config)#line console 0

SW_TUN(config-line)#password harol
SW_TUN(config-line)#exit
SW_TUN(config)#service password-encryption
SW_TUN(config)#enable secret harol
SW_TUN(config)#do write
Building configuration...
[OK]
SW_TUN(config)#
SW_TUN(config)#exit
SW_TUN#
%SYS-5-CONFIG_I: Configured from console by console
SW_TUN#
SW_CUN
SW_CUN>enable
SW_CUN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW_CUN(config)#line console 0
SW_CUN(config-line)#password harol
SW_CUN(config-line)#exit
SW_CUN(config)#service password-encryption
SW_CUN(config)#enable secret harol
SW_CUN(config)#do write
Building configuration...
[OK]
SW_CUN(config)#exit
SW_CUN#
%SYS-5-CONFIG_I: Configured from console by console
SW_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

Tabla 9 Verificación de acceso a los Routers.

R_BUC
User Access Verification Username: harol Password: R_BUC>enab Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#ip ssh authentication-retries 3 R_BUC(config)#ip ssh time-out 60 R_BUC(config)#do write Building configuration... [OK] R_BUC(config)#
R_TUN
User Access Verification Password: R_TUN>ena Password: R_TUN#ena R_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_TUN(config)#ip ssh authentication-retries 3 R_TUN(config)#ip ssh time-out 60 R_TUN(config)#do write

Building configuration... [OK] R_TUN(config)#exit R_TUN# %SYS-5-CONFIG_I: Configured from console by console R_TUN#
R_CUN
User Access Verification Password: R_CUN>ena Password: R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#ip ssh authentication-retries 3 R_CUN(config)#ip ssh time-out 60 R_CUN(config)#do write Building configuration... [OK] R_CUN(config)#exit R_CUN# %SYS-5-CONFIG_I: Configured from console by console R_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

- Un máximo de internos para acceder al Router.

Tabla 10 máximo de internos para acceder al Router.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#line console 0 R_BUC(config-line)#login block-for 5 attempts 8 within 60 R_BUC(config)#exit R_BUC# %SYS-5-CONFIG_I: Configured from console by console R_BUC#
R_TUN
User Access Verification Password: R_TUN>enable Password: R_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_TUN(config)#line console 0 R_TUN(config-line)#login block-for 5 attempts 8 within 60

R_TUN(config)#exit R_TUN# %SYS-5-CONFIG_I: Configured from console by console R_TUN#exit
R_CUN
User Access Verification Password: R_CUN>ena Password: R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#line console 0 R_CUN(config-line)#login block-for 5 attempts 8 within 60 R_CUN(config)#exit R_CUN# %SYS-5-CONFIG_I: Configured from console by console R_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

- Máximo tiempo de acceso al detectar ataques.

Tabla 11 Máximo tiempo de acceso al detectar ataques.

R_BUC
User Access Verification Username: harol Password:

R_BUC>ena

Password:

R_BUC#conf ter

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

R_BUC(config)#line console 0

R_BUC(config-line)#login block-for 5 attempts 8 within 60

R_BUC(config)#exit

R_BUC#

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

R_BUC#

R_TUN

User Access Verification

Password:

R_TUN>ena

Password:

R_TUN#conf ter

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

R_TUN(config)#line console 0

R_TUN(config-line)#login block-for 5 attempts 8 within 60

R_TUN(config)#exit

R_TUN#

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

R_TUN#

R_CUN

User Access Verification

Password: R_CUN>ena Password: R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#line console 0 R_CUN(config-line)#login block-for 5 attempts 8 within 60 R_CUN(config)#exit R_CUN# %SYS-5-CONFIG_I: Configured from console by console R_CUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 12 Creación de un servidor TFTP que almacene los archivos necesarios de los Routers

R_BUC
Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#exit R_BUC# %SYS-5-CONFIG_I: Configured from console by console R_BUC#copy running-config tftp Address or name of remote host []? 172.31.2.26

Destination filename [R_BUC-confg]? Backup_R_BUC

Writing running-config.....

R_TUN

R_TUN>ena

Password:

R_TUN#conf ter

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

R_TUN(config)#exit

R_TUN#

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

R_TUN#copy running-config tftp

Address or name of remote host []? 172.31.2.26

Destination filename [R_TUN-confg]? Backup_R_TUN

Writing running-config.....

R_CUN

R_CUN>ena

Password:

R_CUN#conf ter

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

R_CUN(config)#exit

R_CUN#

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

R_CUN#copy running-config tftp

Address or name of remote host []? 172.31.2.26 Destination filename [R_CUN-confg]? Backup_R_CUN Writing running-config.....

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 13 Configuración para que el DHCP proporcione solo direcciones a los hosts de Bucaramanga y Cundinamarca.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#ip dhcp pool vlan10 R_BUC(dhcp-config)#network 172.31.0.0 255.255.255.192 R_BUC(dhcp-config)#dns-server 8.8.8.8 R_BUC(dhcp-config)#default-router 172.31.0.1 R_BUC(dhcp-config)#exit R_BUC(config)#ip dhcp excluded-address 172.31.0.1 R_BUC(config)#ip dhcp pool vlan30 R_BUC(dhcp-config)#network 172.31.0.64 255.255.255.192 R_BUC(dhcp-config)#dns-server 8.8.8.8

R_BUC(dhcp-config)#default-router 172.31.0.65

R_BUC(dhcp-config)#exit

R_BUC(config)#ip dhcp excluded-address 172.31.0.65

R_BUC(config)#do write

Building configuration...

[OK]

R_BUC(config)#

R_TUN

User Access Verification

Password:

R_TUN>ena

Password:

R_TUN#conf ter

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

R_TUN(config)#ip dhcp pool vlan20

R_TUN(dhcp-config)#network 172.31.1.64 255.255.255.192

R_TUN(dhcp-config)#dns-server 8.8.8.8

R_TUN(dhcp-config)#default-router 172.31.1.65

R_TUN(dhcp-config)#exit

R_TUN(config)#ip dhcp excluded-address 172.31.1.65

R_TUN(config)#ip dhcp pool vlan30

R_TUN(dhcp-config)#network 172.31.0.192 255.255.255.192

R_TUN(dhcp-config)#dns-server 172.31.0.193

R_TUN(dhcp-config)#exit

R_TUN(config)#ip dhcp excluded-address 172.31.0.193

R_TUN(config)#ip dhcp pool vlan30

R_TUN(dhcp-config)#network 172.31.1.0 255.255.255.192

R_TUN(dhcp-config)#dns-server 8.8.8.8

R_TUN(dhcp-config)#default-router 172.31.1.1

R_TUN(dhcp-config)#exit

R_TUN(config)#ip dhcp excluded-address 172.31.1.1

R_TUN(config)#do write

Building configuration...

[OK]

R_TUN(config)#exit

R_TUN#

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

R_TUN#

R_CUN

User Access Verification

Password:

R_CUN>ena

Password:

R_CUN#conf ter

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

R_CUN(config)#ip dhcp pool vlan20

R_CUN(dhcp-config)#network 172.31.1.64 255.255.255.192

R_CUN(dhcp-config)#dns-server 8.8.8.8

R_CUN(dhcp-config)#default-router 172.31.1.65

R_CUN(dhcp-config)#exit

R_CUN(config)#ip dhcp excluded-address 172.31.1.65

R_CUN(config)#ip dhcp pool vlan30

R_CUN(dhcp-config)#network 172.31.0.192 255.255.255.192

R_CUN(dhcp-config)#dns-server 172.31.0.193

R_CUN(dhcp-config)#exit

R_CUN(config)#ip dhcp excluded-address 172.31.0.193

R_CUN(config)#ip dhcp pool vlan30

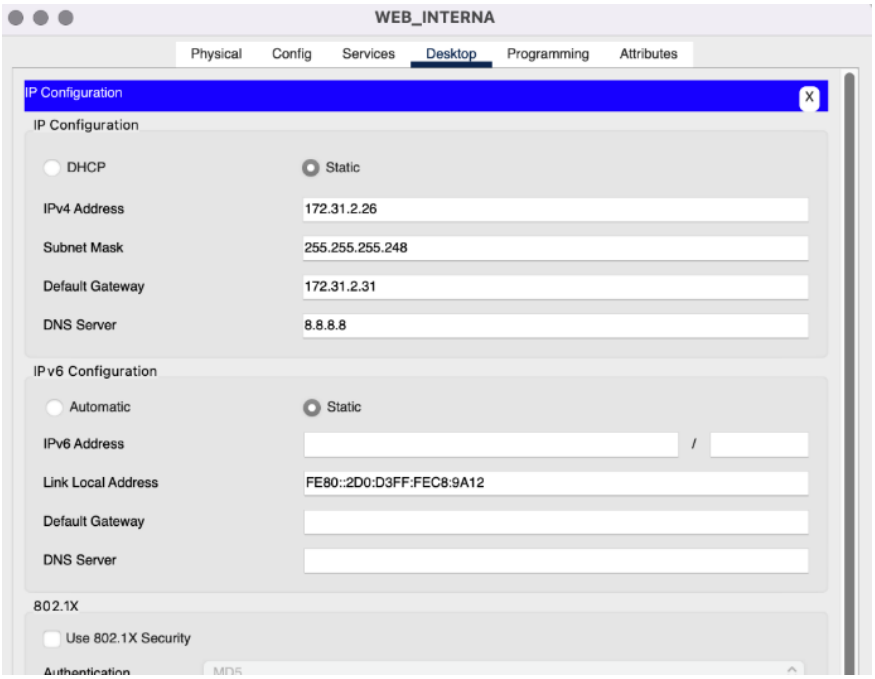
R_CUN(dhcp-config)#network 172.31.1.0 255.255.255.192

```
R_CUN(dhcp-config)#dns-server 8.8.8.8
R_CUN(dhcp-config)#default-router 172.31.1.1
R_CUN(dhcp-config)#exit
R_CUN(config)#ip dhcp excluded-address 172.31.1.1
R_CUN(config)#do write
Building configuration...
[OK]
R_CUN(config)#exit
R_CUN#
%SYS-5-CONFIG_I: Configured from console by console
R_CUN#
```

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Figura 45 Configuración del WEB SERVER.



Fuente: harol, m. (28 de septiembre de 2022). Obtenido de Packet Tracer autoría propia.

4. El enrutamiento deberá tener autenticación.

Tabla 14 Configuración de enrutamiento para tener autenticación.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#router ospf 1 R_BUC(config-router)#network 172.31.0.0 0.0.0.3 area 0 R_BUC(config-router)#network 172.31.2.0 0.0.0.3 area 0 R_BUC(config-router)#network 172.31.2.32 0.0.0.3 area 0 R_BUC(config-router)#network 172.31.2.0 0.0.0.7 area 0 R_BUC(config-router)#network 172.31.0.0 0.0.0.63 area 0 R_BUC(config-router)#network 172.31.0.64 0.0.0.63 area 0 R_BUC(config-router)#exit R_BUC(config)#inter s0/0/0 R_BUC(config-if)#ip ospf message-digest-key 1 md5 cisco R_BUC(config-if)#ip ospf authentication message-digest R_BUC(config-if)#exit R_BUC(config)#do write Building configuration... [OK] R_BUC(config)#exit R_BUC# %SYS-5-CONFIG_I: Configured from console by console

R_BUC#

R_TUN

User Access Verification

Password:

R_TUN>ena
Password:
R_TUN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_TUN(config)#router ospf 1
R_TUN(config-router)#network 172.31.0.0 0.0.0.3 area 0
R_TUN(config-router)#network 172.31.2.0 0.0.0.3 area 0
R_TUN(config-router)#network 172.31.2.32 0.0.0.3 area 0
R_TUN(config-router)#network 172.31.2.36 0.0.0.3 area 0
R_TUN(config-router)#network 209.17.220.5 0.0.0.255 area 0
R_TUN(config-router)#network 172.31.0.128 0.0.0.63 area 0
R_TUN(config-router)#network 172.31.0.192 0.0.0.63 area 0
R_TUN(config-router)#network 172.3.2.8 0.0.0.7 area 0
R_TUN(config-router)#exit
R_TUN(config)#inter s0/0/0
R_TUN(config-if)#ip ospf message-digest-key 1 md5 cisco
R_TUN(config-if)#ip ospf authentication message-digest
R_TUN(config-if)#
01:07:17: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.33 on Serial0/0/0 from LOADING to FULL, Loading Done
exit
R_TUN(config)#inter s0/0/1
R_TUN(config-if)#ip ospf message-digest-key 1 md5 cisco

R_TUN(config-if)#ip ospf authentication message-digest

R_TUN(config-if)#exit

R_TUN(config)#do write

Building configuration...

[OK]

R_TUN(config)#exit

R_TUN#

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

R_TUN#

R_CUN

User Access Verification

Password:

R_CUN>ena

Password:

R_CUN#conf ter

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

R_CUN(config)#router ospf 1

R_CUN(config-router)#network 172.31.0.0 0.0.0.3 area 0

R_CUN(config-router)#network 172.31.2.0 0.0.0.3 area 0

R_CUN(config-router)#network 172.31.2.32 0.0.0.3 area 0

R_CUN(config-router)#network 172.31.2.36 0.0.0.3 area 0

R_CUN(config-router)#network 209.17.220.5 0.0.0.255 area 0

R_CUN(config-router)#network 172.31.0.128 0.0.0.63 area 0

R_CUN(config-router)#network 172.31.0.192 0.0.0.63 area 0

R_CUN(config-router)#network 172.3.2.8 0.0.0.7 area 0

R_CUN(config-router)#exit

R_CUN(config)#inter s0/0/0

R_CUN(config-if)#ip ospf message-digest-key 1 md5 cisco R_CUN(config-if)#ip ospf authentication message-digest R_CUN(config-if)# 01:13:57: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.2 on Serial0/0/0 from LOADING to FULL, Loading Done R_CUN(config-if)#exit R_CUN(config)#exit R_CUN# %SYS-5-CONFIG_I: Configured from console by console exit

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

5. Listas de control de acceso:

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

Tabla 15 configuración de control de acceso de la VLAN 20.

R_CUN
Password: R_CUN>ena Password: Password: R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#access-list 111 deny ip 172.31.1.64 0.0.0.63 % Incomplete command. R_CUN(config)#exit R_CUN#

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

R_CUN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_CUN(config)#access-list 100 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
R_CUN(config)#access-list 100 permit ip any any
R_CUN(config)#int g0/0.20
R_CUN(config-subif)#ip access-group 100 in
R_CUN(config-subif)#

R_CUN

User Access Verification

Password:

R_CUN>ena
Password:
R_CUN#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R_CUN(config)#access-list 101 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
R_CUN(config)#access-list 101 deny ip any any
R_CUN(config)#int g0/0.30
R_CUN(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

R_CUN(config-subif)#ip access-group 101 in R_CUN(config-subif)#exit R_CUN(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 16 configuración de control de acceso a internet de la VLAN 10.

R_CUN
User Access Verification Password: R_CUN>ena Password: R_CUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_CUN(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80 R_CUN(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21 R_CUN(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20 R_CUN(config)#int g0/0.30 R_CUN(config-subif)# R_CUN(config-subif)#ip access-group 100 in R_CUN(config-subif)#exit R_CUN(config)#do wr

Building configuration... [OK] R_CUN(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 17 configuración de control de acceso a internet, servidor web y ftp de la VLAN 30.

R_TUN
User Access Verification Password: R_TUN>ena Password: R_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_TUN(config)#access-list 100 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255 R_TUN(config)#int g0/0.30 R_TUN(config-subif)#ip access-group 100 in R_TUN(config-subif)#exit R_TUN(config)#do wr Building configuration... [OK] R_TUN(config)#exit R_TUN# %SYS-5-CONFIG_I: Configured from console by console R_TUN#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 18 Configuración de hosts de VLAN 20 y VLAN 10 de Bucaramanga.

R_TUN
User Access Verification Password: R_TUN>ena Password: R_TUN#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_TUN(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63 R_TUN(config)#access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63 R_TUN(config)#int g0/0.20 R_TUN(config-subif)#ip access-group 101 in R_TUN(config-subif)#exit R_TUN(config)#do wr Building configuration... [OK] R_TUN(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 19 configuración de hosts de VLAN 30.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#access-list 100 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255 R_BUC(config)#int g0/0.30 R_BUC(config-subif)#ip access-group 100 in R_BUC(config-subif)#exit R_BUC(config)#do wr Building configuration... [OK] R_BUC(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 20 configuración de los hosts de la VLAN 10 para acceder a la VLAN 20 de Cundinamarca y Tunja.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63 R_BUC(config)#access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63 R_BUC(config)#int g0/0.10 R_BUC(config-subif)#ip access-group 101 in R_BUC(config-subif)#exit R_BUC(config)#do write Building configuration... [OK] R_BUC(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 21 configuración de hosts de una VLAN negando el acceso a los de otra VLAN en una ciudad.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#access-list 102 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63 R_BUC(config)#access-list 102 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63 R_BUC(config)#access-list 102 permit ip any any R_BUC(config)#int g0/0.10 R_BUC(config-subif)#ip access-group 102 out R_BUC(config-subif)#exit R_BUC(config)#do wr Building configuration... [OK] R_BUC(config)#
R_TUN
User Access Verification Password: R_TUN>ena Password:

R_TUN#conf ter

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

R_TUN(config)#access-list 102 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63

R_TUN(config)#access-list 102 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63

R_TUN(config)#access-list 102 permit ip any any

R_TUN(config)#int g0/0.20

R_TUN(config-subif)#ip access-group 102 out

R_TUN(config-subif)#

R_CUN

User Access Verification

Password:

R_CUN>ena

Password:

R_CUN#conf ter

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

R_CUN(config)#access-list 102 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

R_CUN(config)#access-list 102 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63

R_CUN(config)#access-list 102 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

R_CUN(config)#access-list 102 permit ip any any

R_CUN(config)#int g0/0.20

R_CUN(config-subif)#ip access-group 102 out

R_CUN(config-subif)#exit

R_CUN(config)#do wr

Building configuration... [OK] R_CUN(config)#

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

Tabla 22 Configuración de VLAN administrativas y VLAN de servidores.

R_BUC
User Access Verification Username: harol Password: R_BUC>ena Password: R_BUC#conf ter Enter configuration commands, one per line. End with CNTL/Z. R_BUC(config)#int g0/0.10 R_BUC(config-subif)#access-list 2 permit 172.31.2.0 0.0.0.7 R_BUC(config)#access-list 2 permit 172.3.2.8 0.0.0.7 R_BUC(config)#access-list 2 permit 172.31.2.8 0.0.0.7 R_BUC(config)#line vty 0 4 R_BUC(config-line)#access-class 2 in R_BUC(config-line)#exit R_BUC(config)#do wr Building configuration... [OK]

R_BUC(config)#

R_TUN

User Access Verification

Password:

R_TUN>ena

Password:

R_TUN#conf ter

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

R_TUN(config)#int g0/0.20

R_TUN(config-subif)#access-list 2 permit 172.31.2.0 0.0.0.7

R_TUN(config)#access-list 2 permit 172.3.2.8 0.0.0.7

R_TUN(config)#access-list 2 permit 172.31.2.8 0.0.0.7

R_TUN(config)#line vty 0 4

R_TUN(config-line)#access-class 2 in

R_TUN(config-line)#exit

R_TUN(config)#do wr

Building configuration...

[OK]

R_TUN(config)#

R_CUN

User Access Verification

Password:

R_CUN>ena

Password:

R_CUN#conf ter

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

```
R_CUN(config)#int g0/0.20
R_CUN(config-subif)#access-list 2 permit 172.31.2.0 0.0.0.7
R_CUN(config)#access-list 2 permit 172.3.2.8 0.0.0.7
R_CUN(config)#access-list 2 permit 172.31.2.8 0.0.0.7
R_CUN(config)#line vty 0 4
R_CUN(config-line)#access-class 2 in
R_CUN(config-line)#exit
R_CUN(config)#do wr
Building configuration...
[OK]
R_CUN(config)#
```

Fuente: harol, m. (28 de septiembre de 2022), autoría propia.

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

CONCLUSIONES

Durante el desarrollo del curso de adquirieron los conocimientos necesarios para aplicabilidad en escenarios prácticos, abordando temas como lo son: topologías de red, segmentación de red, direccionamiento IP, protocolos de enrutamiento como son EIGRP, OSPF Y DCHP, configuración de depósitos de red, configuración de seguridad para dispositivos en red, listas de control para equipos conectados en red y sub redes.

La implementación y prueba de redes estructuradas, así como su configuración inicial y final de redes locales LAN/WAN, puede ser desarrollada a través de software diseñados para la simulación de estos, para este caso el uso de Packet Tracer fue necesario para la simulación de los escenarios prácticos propuestos.

BIBLIOGRAFÍA

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Obtenido de:https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

IP Addressing and Subnetting for New Users Obtenido de: https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

Resolver problemas los entornos del Switching de LAN. (S.F).Obtenido de: https://www.cisco.com/c/es_mx/support/docs/lan-switching/ethernet/12006-chapter22.html