EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

SAMUEL RICARDO GARIBELLO VARGAS

DIPLOMADO CISCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERIA DE SISTEMAS
BOGOTA
2019

TABLA DE CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

RESUMEN

Para esta prueba practica de habilidades en CISCO, se implementó el direccionamiento para las topologías de red en cada escenario planteado, así mismo se llevó a cabo la asignación de los parámetros necesarios para cada uno, como también la configuración del enrutamiento, control de acceso, DHCP, NAT, enrutamiento con autenticación, control de acceso de los hosts con VLAN. y demás requerimientos que se plantearon para la solución de los escenarios planteados, todo esto llevando a la práctica todos los conocimientos teóricos y prácticas adelantadas durante el desarrollo del diplomado CCNA1 y CCNA2.

De otra parte, también se contemplaron parámetros de seguridad en los dispositivos, se realizó comprobación de estos y su correcto funcionamiento.

ABSTRACT

For this practical test of skills in CISCO, the addressing for the network topologies was implemented in each scenario proposed, as well as the assignment of the necessary parameters for each one, as well as the routing configuration, access control, DHCP, NAT, routing with authentication, access control of hosts with VLAN. and other requirements that were raised for the solution of the proposed scenarios, all this putting into practice all the theoretical knowledge and practices advanced during the development of the CCNA1 and CCNA2 diploma.

On the other hand, safety parameters were also contemplated in the devices, these were checked and their correct functioning.

INTRODUCCIÓN

Con el fin de dar evidencia de las competencias y habilidades que fueron adquiridas durante el Diplomado de CCNA1 y CCNA2

Para esta actividad, se aplicaron todos los conocimientos adquiridos durante el diplomado con el fin de crear soluciones a los escenarios propuestos, para luego realizar la verificación de conectividad mediante el uso del protocolo ICMP.

El buen uso e implementación de la teoría de redes adquirida fue fundamental para abarcar correctamente la resolución de los escenarios.

OBJETIVOS

- Dar solución a los diferentes escenarios propuestos en la práctica, haciendo uso de los conocimientos adquiridos en el diplomado, para la configuración de las redes en cada caso.

- Definir el direccionamiento en la red de cada escenario.

- Aplicar los parámetros básicos de seguridad y de detección de vecinos directamente conectados.

- Configurar la red y la subred para su interconexión, implementando parámetros de seguridad y de acceso en los diferentes hosts.

- Configurar el enrutamiento y las listas de control de acceso.

1. DESARROLLO DE LOS DOS ESCENARIOS

Descripción de escenarios propuestos para la prueba de habilidades.

1.1. ESCENARIO 1

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

1.1.1 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.

Ilustración 1 Topología de la Red

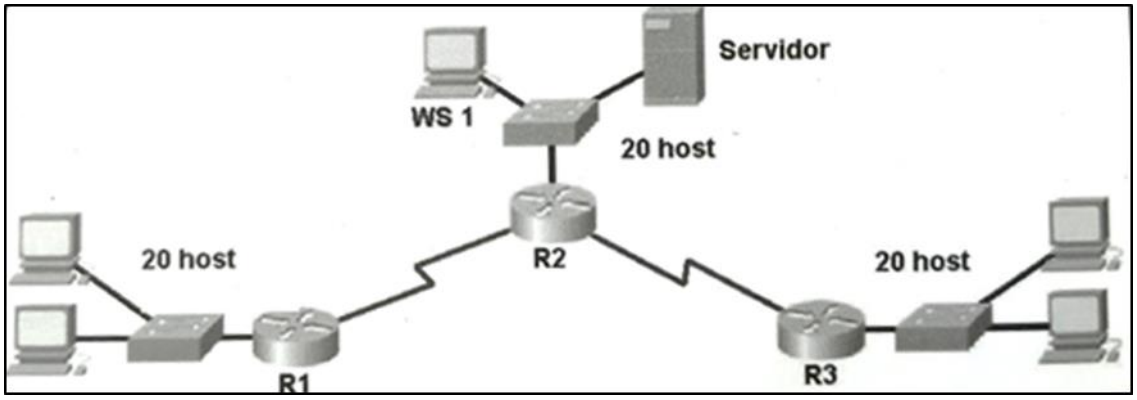
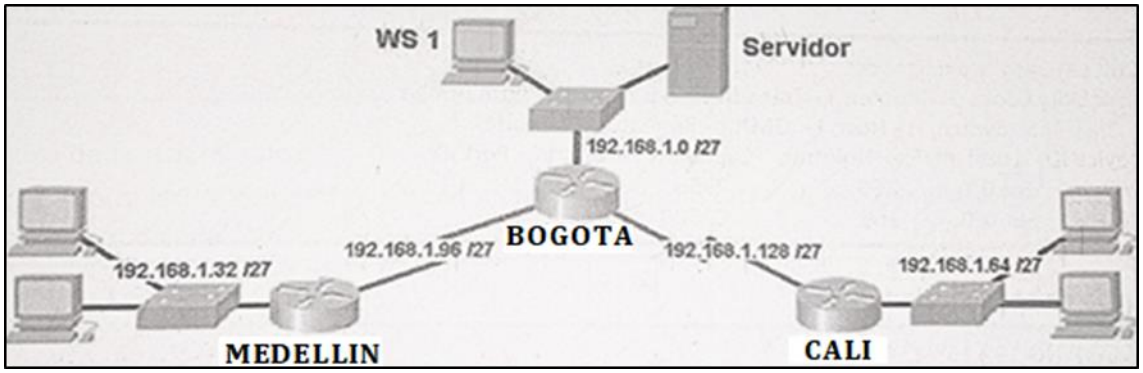


Ilustración 2 Topología de Red direccionamiento IP's

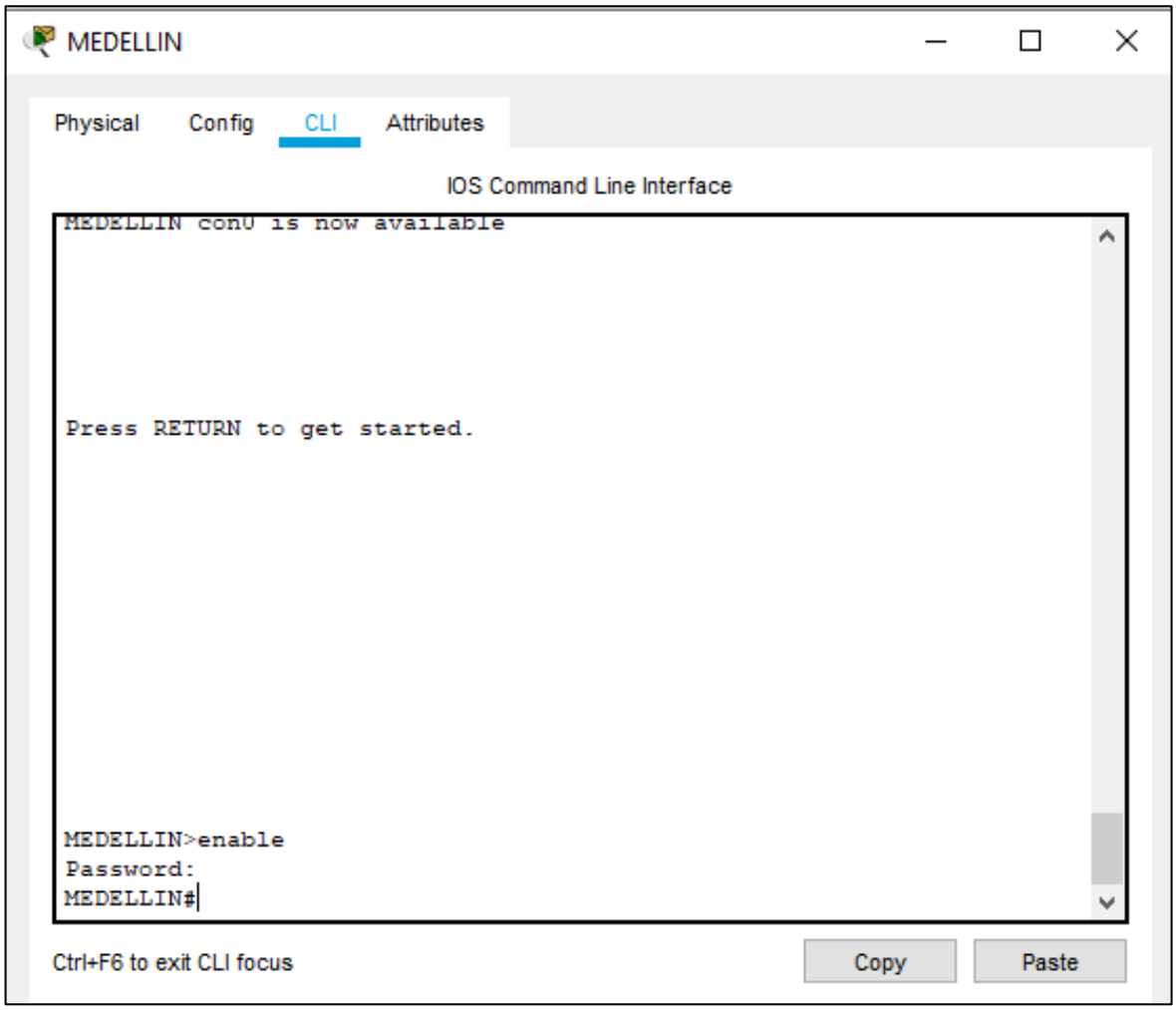


1.2. DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

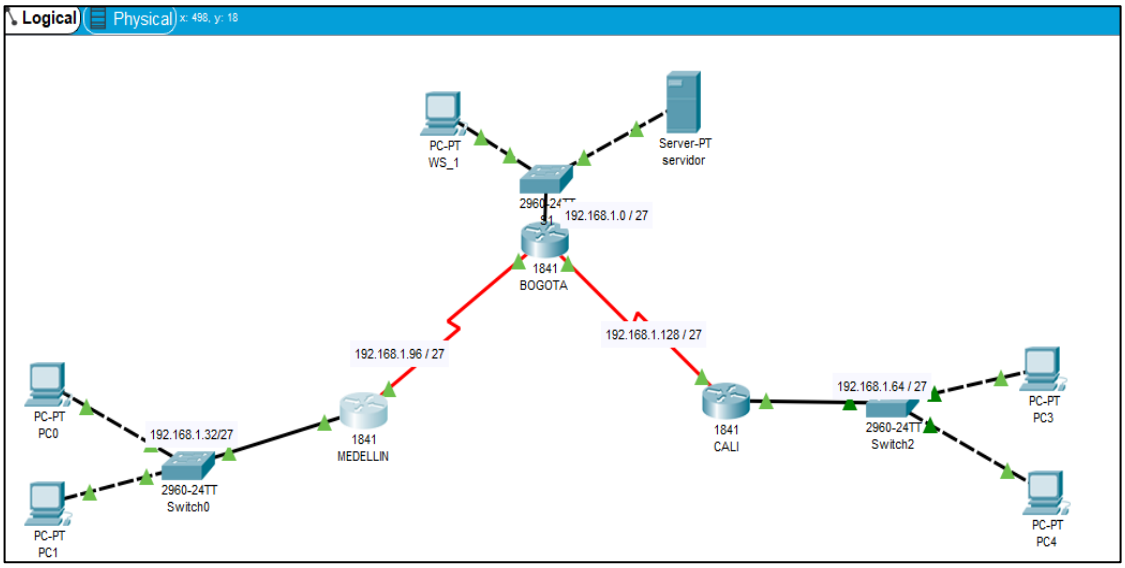
Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Ilustración 3 Ingreso a CLI



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

Ilustración 4 Topología de Red



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

1.2.1 Parte 1: Asignación de direcciones IP:

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

Tabla 1 Asignación direccionamiento IP

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Asignar una dirección IP a la red.

1.2.2 Parte 2: Configuración Básica.

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

Tabla 2 Enrutamiento redes LAN por ciudades

	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	192.168.1.161	192.168.1.130	192.168.1.193
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

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.

Ilustración 5 Tabla de Enrutamiento Bogotá

```
Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/20514560] via 192.168.1.99, 00:46:08, Serial0/0/0
D       192.168.1.64 [90/20514560] via 192.168.1.131, 00:49:13, Serial0/1/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/1/0

BOGOTA#
```

Ilustración 6 Tabla de Enrutamiento Medellín

```
Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.98, 00:55:55, Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/21026560] via 192.168.1.98, 00:50:23, Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/21024000] via 192.168.1.98, 00:55:55, Serial0/0/0

MEDELLIN#
```

Ilustración 7 Tabla de Enrutamiento Cali

```
Gateway of last resort is not set

     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/20514560] via 192.168.1.130, 01:07:34, Serial0/0/0
D       192.168.1.32 [90/21026560] via 192.168.1.130, 00:48:38, Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/21024000] via 192.168.1.130, 00:58:07, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI#
```

- Verificar el balanceo de carga que presentan los routers.
- Realizar un diagnóstico de vecinos uando el comando cdp.

Ilustración 8 Comando CDP Bogotá

```
BOGOTA#show cdp nei
BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
S1           Fas 0/0          120            S       2960        Fas 0/1
CALI         Ser 0/1/0        139            R       C1841       Ser 0/0/0
MEDELLIN     Ser 0/0/0        173            R       C1841       Ser 0/0/0
BOGOTA#
```

Ilustración 9 Comando CDP Cali

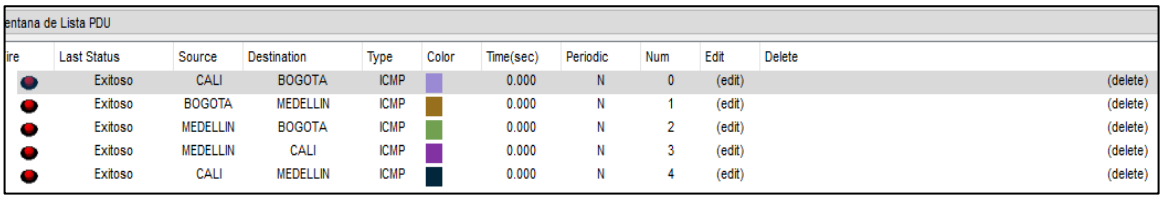
```
CALI>enable
Password:
CALI#showcd
CALI#show c
CALI#show cdp
CALI#show cdp ne
CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          135            S       2960        Fas 0/1
BOGOTA       Ser 0/0/0        154            R       C1841       Ser 0/1/0
CALI#
```

Ilustración 10 Comando CDP Medellín

```
MEDELLIN>enable
Password:
MEDELLIN#show cdp ne
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          167            S       2960        Fas 0/1
BOGOTA       Ser 0/0/0        160            R       C1841       Ser 0/0/0
MEDELLIN#
```

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

Ilustración 11 Prueba Conectividad Ping



entana de Lista PDU

ire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Exitoso	CALI	BOGOTA	ICMP		0.000	N	0	(edit)	(delete)
	Exitoso	BOGOTA	MEDELLIN	ICMP		0.000	N	1	(edit)	(delete)
	Exitoso	MEDELLIN	BOGOTA	ICMP		0.000	N	2	(edit)	(delete)
	Exitoso	MEDELLIN	CALI	ICMP		0.000	N	3	(edit)	(delete)
	Exitoso	CALI	MEDELLIN	ICMP		0.000	N	4	(edit)	(delete)

1.2.3 Parte 3: Configuración de Enrutamiento.

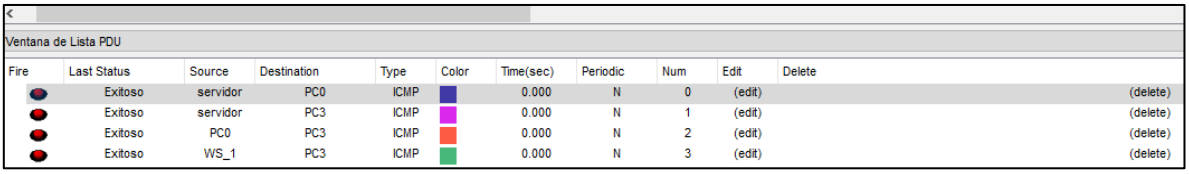
Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Verificar si existe vecindad con los routers configurados con EIGRP.

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

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.

Ilustración 12 Prueba Conectividad Ping Equipos Cliente



Ventana de Lista PDU

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Exitoso	servidor	PC0	ICMP		0.000	N	0	(edit)	(delete)
	Exitoso	servidor	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Exitoso	PC0	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Exitoso	WS_1	PC3	ICMP		0.000	N	3	(edit)	(delete)

1.2.4 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:

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

Ilustración 13 Verificación Telnet Habilitado Cali

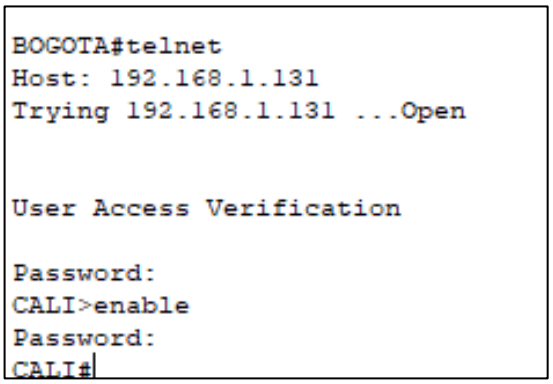


Ilustración 14 Verificación Telnet Habilitado Bogotá

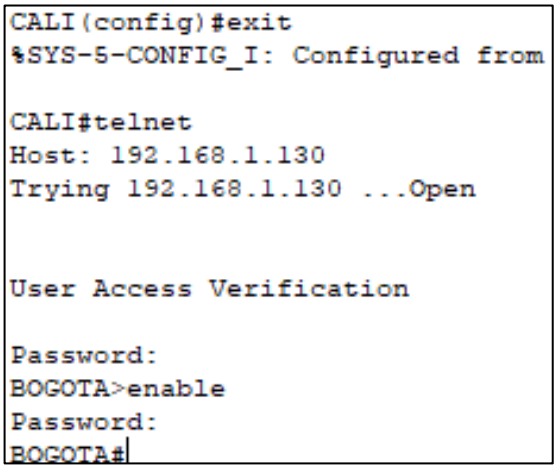
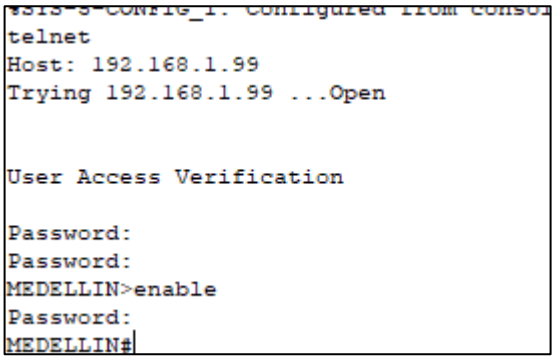


Ilustración 15 Verificación Telnet Habilitado Medellín



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.

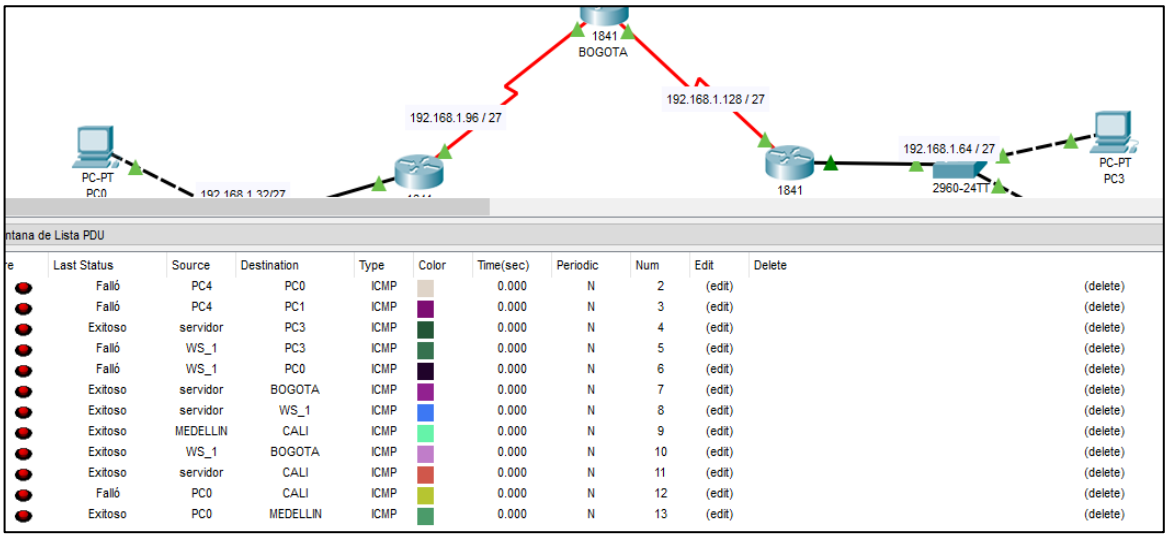
Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

1.2.5 Parte 5: Comprobación de la red instalada.

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

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

Ilustración 16 Comprobación de Conectividad por ICMP



ntana de Lista PDU

te	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Falló	PC4	PC0	ICMP		0.000	N	2	(edit)	(delete)
	Falló	PC4	PC1	ICMP		0.000	N	3	(edit)	(delete)
	Exitoso	servidor	PC3	ICMP		0.000	N	4	(edit)	(delete)
	Falló	WS_1	PC3	ICMP		0.000	N	5	(edit)	(delete)
	Falló	WS_1	PC0	ICMP		0.000	N	6	(edit)	(delete)
	Exitoso	servidor	BOGOTA	ICMP		0.000	N	7	(edit)	(delete)
	Exitoso	servidor	WS_1	ICMP		0.000	N	8	(edit)	(delete)
	Exitoso	MEDELLIN	CALI	ICMP		0.000	N	9	(edit)	(delete)
	Exitoso	WS_1	BOGOTA	ICMP		0.000	N	10	(edit)	(delete)
	Exitoso	servidor	CALI	ICMP		0.000	N	11	(edit)	(delete)
	Falló	PC0	CALI	ICMP		0.000	N	12	(edit)	(delete)
	Exitoso	PC0	MEDELLIN	ICMP		0.000	N	13	(edit)	(delete)

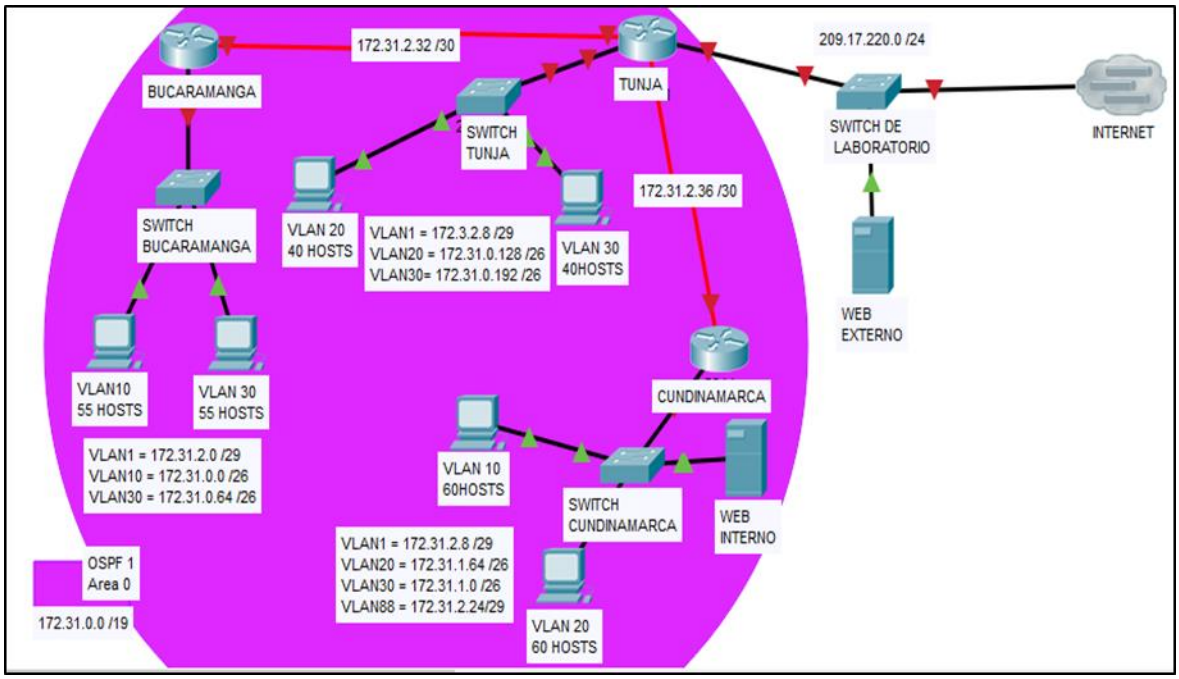
Tabla 3 Pruebas ICMP rutas LAN

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

1.3. 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.

Ilustración 17 Topología de la Red



1.4. DESARROLLO

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente:

1.4.1 Configuración básica.

Router>

en Router#conf term

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname BUCARAMANGA

BUCARAMANGA(config)#no ip domain-lookup

BUCARAMANGA(config)#banner motd #Cuidado Acceso Restringido#
BUCARAMANGA(config)#enable secret class123

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#password cisco123

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#logging synchronous

BUCARAMANGA(config-line)#line vty 0 15

BUCARAMANGA(config-line)#password cisco123

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#logging synchronous

BUCARAMANGA(config)#int g0/0.1

BUCARAMANGA(config-subif)#encapsulation dot1q 1

BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248

BUCARAMANGA(config-subif)#int g0/0.10

BUCARAMANGA(config-subif)#encapsulation dot1q 10

BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192

BUCARAMANGA(config-subif)#int g0/0.30

BUCARAMANGA(config-subif)#encapsulation dot1q 30

BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192

BUCARAMANGA(config-subif)#int g0/0

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#int s0/0/0

BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#router ospf 1

BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0

BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0

BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0

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

TUNJA(config)#no ip domain-lookup

TUNJA(config)#banner motd #Cuidado Acceso Restringido#

TUNJA(config)#enable secret class123

TUNJA(config)#line console 0

TUNJA(config-line)#password cisco123

TUNJA(config-line)#login

TUNJA(config-line)#logging synchronous

TUNJA(config-line)#line vty 0 15

TUNJA(config-line)#password cisco123

TUNJA(config-line)#login

TUNJA(config-line)#logging synchronous

TUNJA(config)#int g0/0.1

TUNJA(config-subif)#encapsulation dot1q 1

TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248

TUNJA(config-subif)#int g0/0.20

TUNJA(config-subif)#encapsulation dot1q 20

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#int g0/0.30

TUNJA(config-subif)#encapsulation dot1q 30

TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config-subif)#int g0/0

TUNJA(config-if)#no shutdown

TUNJA(config-if)#int s0/0/0

TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252

```
TUNJA(config-if)#no shutdown
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#int g0/1
TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#router ospf 1
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0

CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#banner motd #Cuidado Acceso Restringido#
CUNDINAMARCA(config)#enable secret class123
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config)#int g0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
```

CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248

CUNDINAMARCA(config-subif)#int g0/0.20

CUNDINAMARCA(config-subif)#encapsulation dot1q 20

CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192

CUNDINAMARCA(config-subif)#int g0/0.30

CUNDINAMARCA(config-subif)#encapsulation dot1q 30

CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192

CUNDINAMARCA(config-subif)#int g0/0.88

CUNDINAMARCA(config-subif)#encapsulation dot1q 88

CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248

CUNDINAMARCA(config-subif)#int g0/0

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#int s0/0/0

CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#router ospf 1

CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0

CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0

CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0

CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config- router)#end

BUCARAMANGASW(config)#vlan 1

BUCARAMANGASW(config-vlan)#vlan 10

BUCARAMANGASW(config-vlan)#vlan 30

BUCARAMANGASW(config-vlan)#int f0/20

BUCARAMANGASW(config-if)#switchport mode access

```
BUCARAMANGASW(config-if)#switchport access vlan 10
BUCARAMANGASW(config-if)#int f0/24
BUCARAMANGASW(config-if)#switchport mode access
BUCARAMANGASW(config-if)#switchport access vlan 30
BUCARAMANGASW(config-if)#int f0/1
BUCARAMANGASW(config-if)#switchport mode trunk
BUCARAMANGASW(config-if)#int vlan 1
BUCARAMANGASW(config-if)#ip address 172.31.2.3 255.255.255.248
BUCARAMANGASW(config-if)#no shutdown
BUCARAMANGASW(config-if)#ip default-gateway 172.31.2.1

TUNJASW(config)#vlan 1
TUNJASW(config-vlan)#vlan 20
TUNJASW(config-vlan)#vlan 30
TUNJASW(config-vlan)#int f0/20
TUNJASW(config-if)#switchport mode access
TUNJASW(config-if)#switchport access vlan 20
TUNJASW(config-if)#int f0/24
TUNJASW(config-if)#switchport mode access
TUNJASW(config-if)#switchport access vlan 30
TUNJASW(config-if)#int f0/1
TUNJASW(config-if)#switchport mode trunk
TUNJASW(config-if)#
TUNJASW(config-if)#int vlan 1
TUNJASW(config-if)#ip address 172.3.2.11 255.255.255.248
TUNJASW(config-if)#no shutdown
TUNJASW(config-if)#
```

TUNJASW(config-if)#ip default-gateway 172.3.2.9

CUNDINAMARCASW(config)#vlan 1
CUNDINAMARCASW(config-vlan)#vlan 20
CUNDINAMARCASW(config-vlan)#vlan 30
CUNDINAMARCASW(config-vlan)#vlan 88
CUNDINAMARCASW(config-vlan)#exit
CUNDINAMARCASW(config)#int f0/20
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 20
CUNDINAMARCASW(config-if)#int f0/24
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 30
CUNDINAMARCASW(config-if)#int f0/10
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 88
CUNDINAMARCASW(config-if)#int f0/1
CUNDINAMARCASW(config-if)#switchport mode trunk
CUNDINAMARCASW(config-if)#
CUNDINAMARCASW(config-if)#int vlan 1
CUNDINAMARCASW(config-if)#ip address 172.31.2.11 255.255.255.248
CUNDINAMARCASW(config-if)#no shutdown
CUNDINAMARCASW(config-if)#
CUNDINAMARCASW(config-if)#ip default-gateway 172.31.2.9

1.4.2 Autenticación local con AAA

BUCARAMANGA(config-line)#username administrador secret cisco12345
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH

TUNJA(config-line)#username administrador secret cisco12345
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH

CUNDINAMARCA(config-line)#username administrador secret cisco12345
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH

1.4.3 Cifrado contraseñas

BUCARAMANGA(config)#service password-encryption

TUNJA(config)#service password-encryption

CUNDINAMARCA(config)#service password-encryption

1.4.4 Intentos para acceder al router

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60

TUNJA(config-line)#login block-for 5 attempts 4 within 60

CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

1.4.5 Máximo tiempo de acceso al detectar ataques

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60

TUNJA(config-line)#login block-for 5 attempts 4 within 60

CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

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

Ilustración 18 Direccionamiento IP servidor TFTP

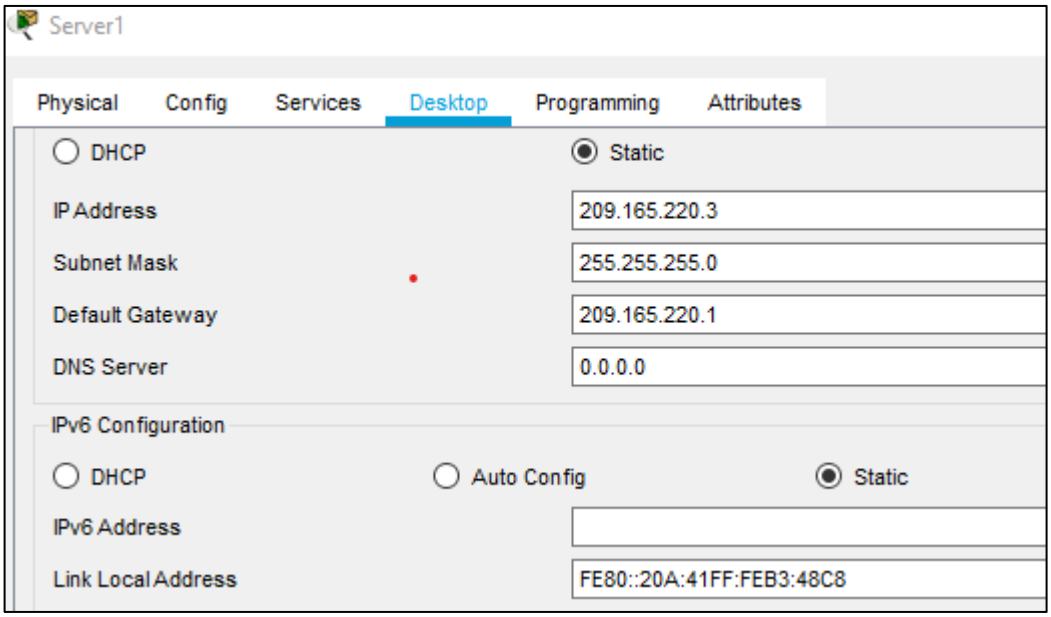
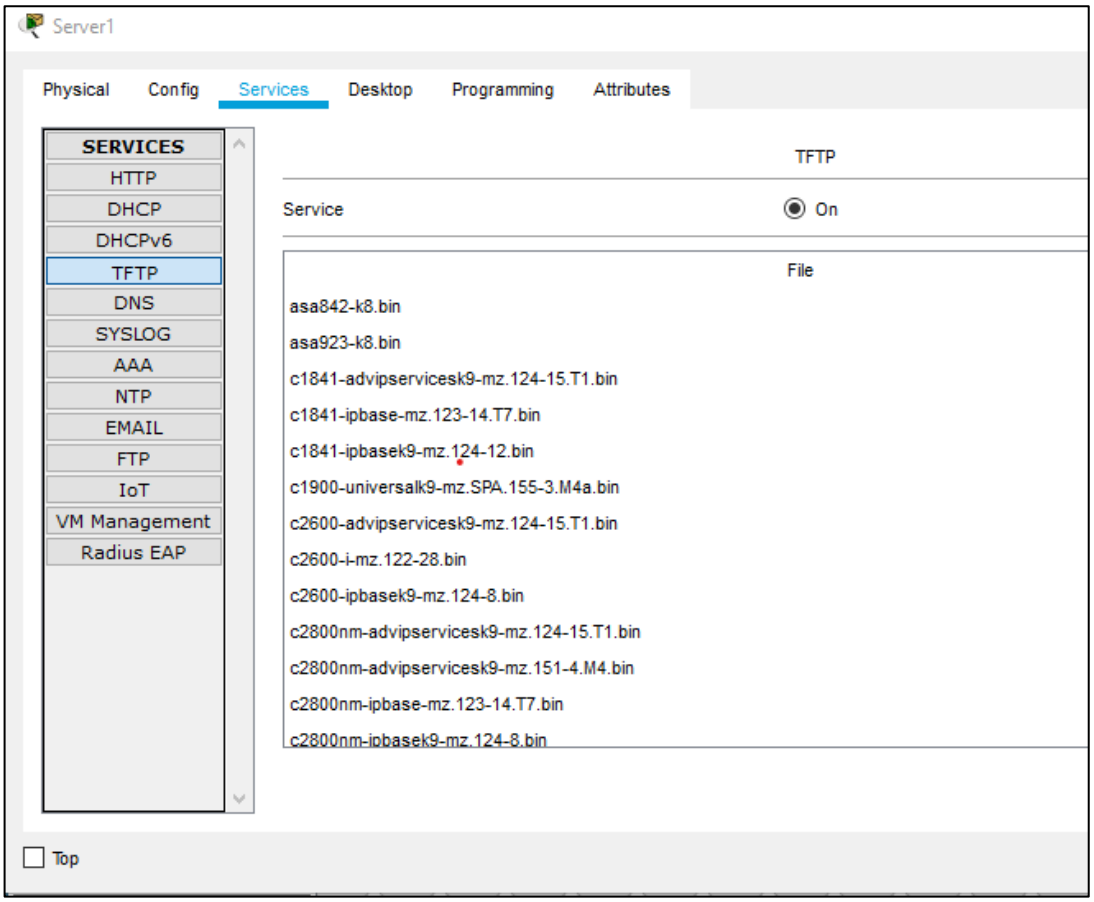


Ilustración 19 Servicio TFTP activo.



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

TUNJA(config)#ip dhcp excluded-address 172.31.0.1

TUNJA(config)#ip dhcp excluded-address 172.31.0.65

TUNJA(config)#ip dhcp excluded-address 172.31.1.65

TUNJA(config)#ip dhcp excluded-address 172.31.1.1

TUNJA(config)#ip dhcp pool V10B

TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192

TUNJA(dhcp-config)#default-router 172.31.0.1

```
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30B
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V20C
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30C
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#

BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end

CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
```

Ilustración 20 Direccionamiento DHCP VLAN 10 Bucaramanga

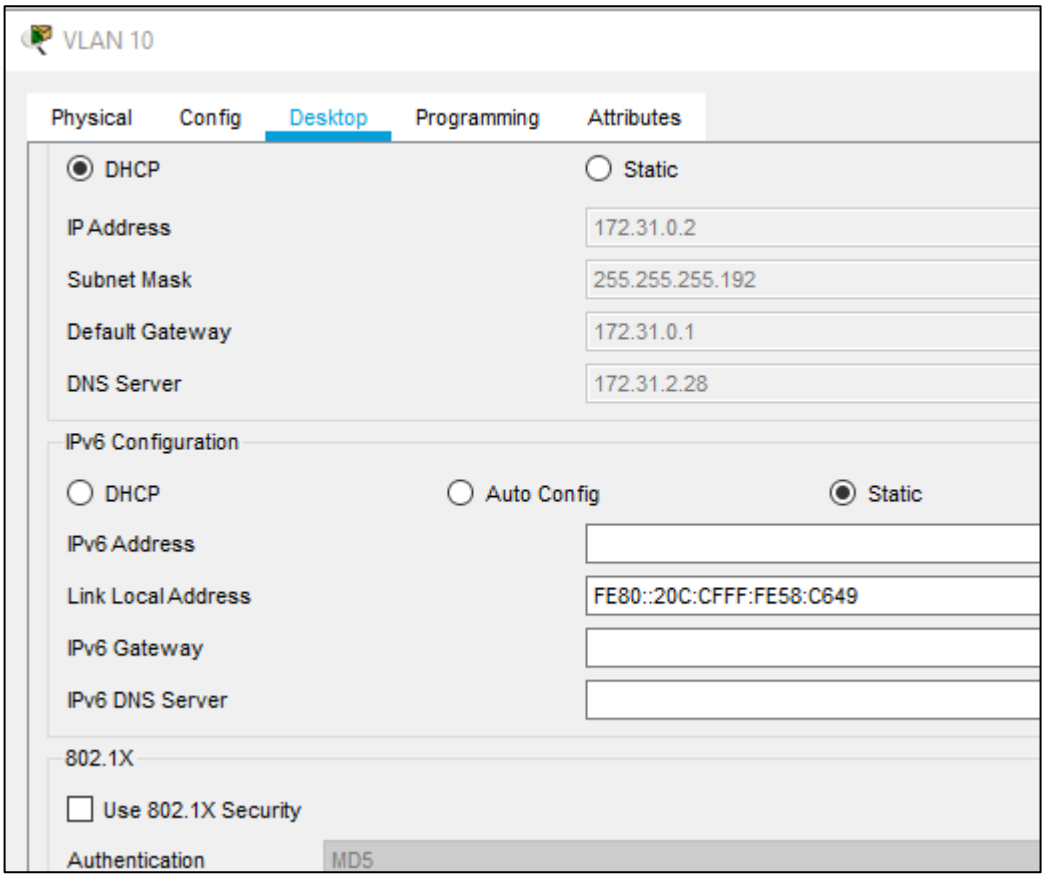


Ilustración 21 Direccionamiento DHCP VLAN 30 Bucaramanga

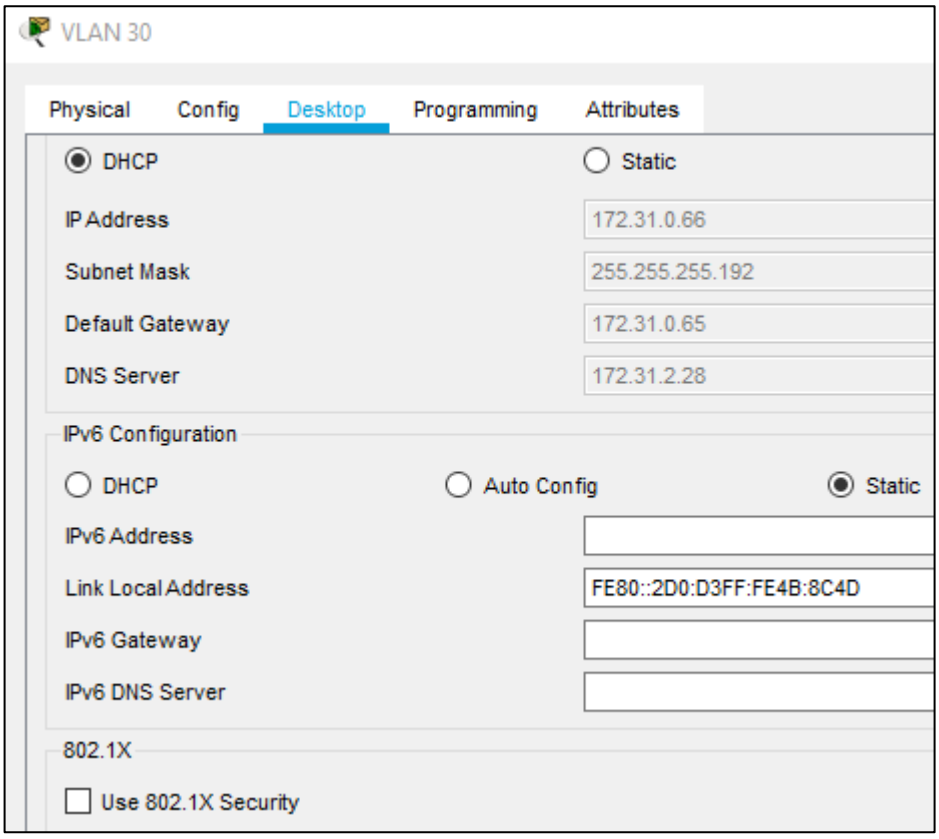


Ilustración 22 Direccionamiento DHCP VLAN 20 Cundinamarca

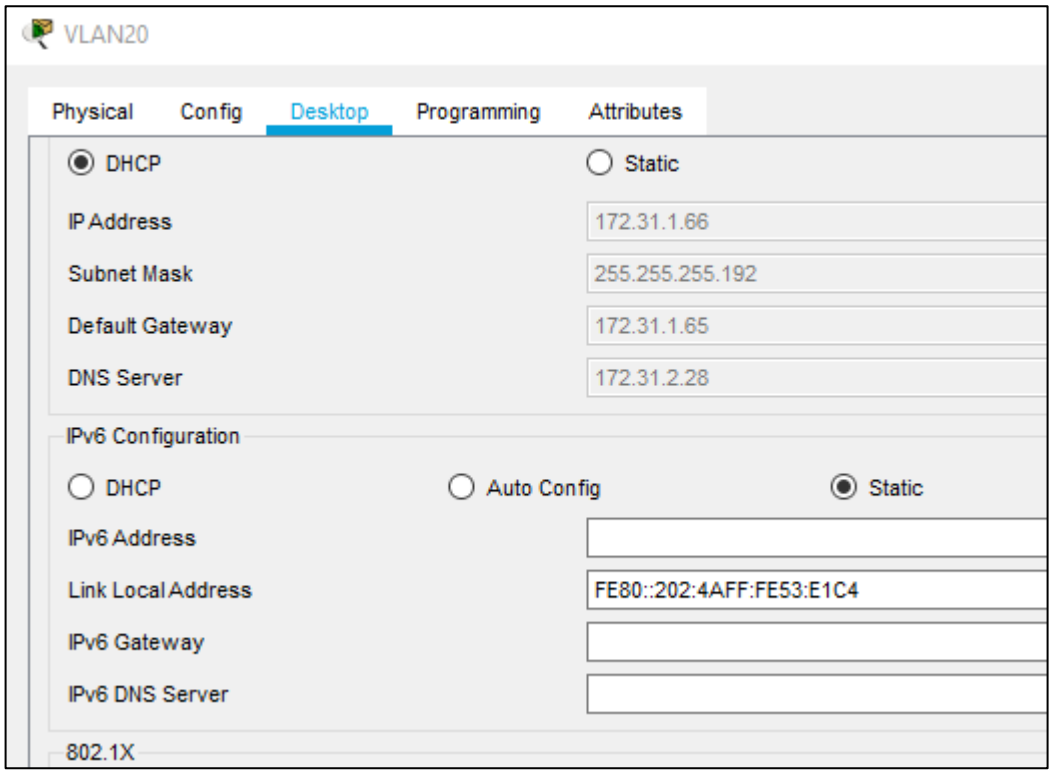
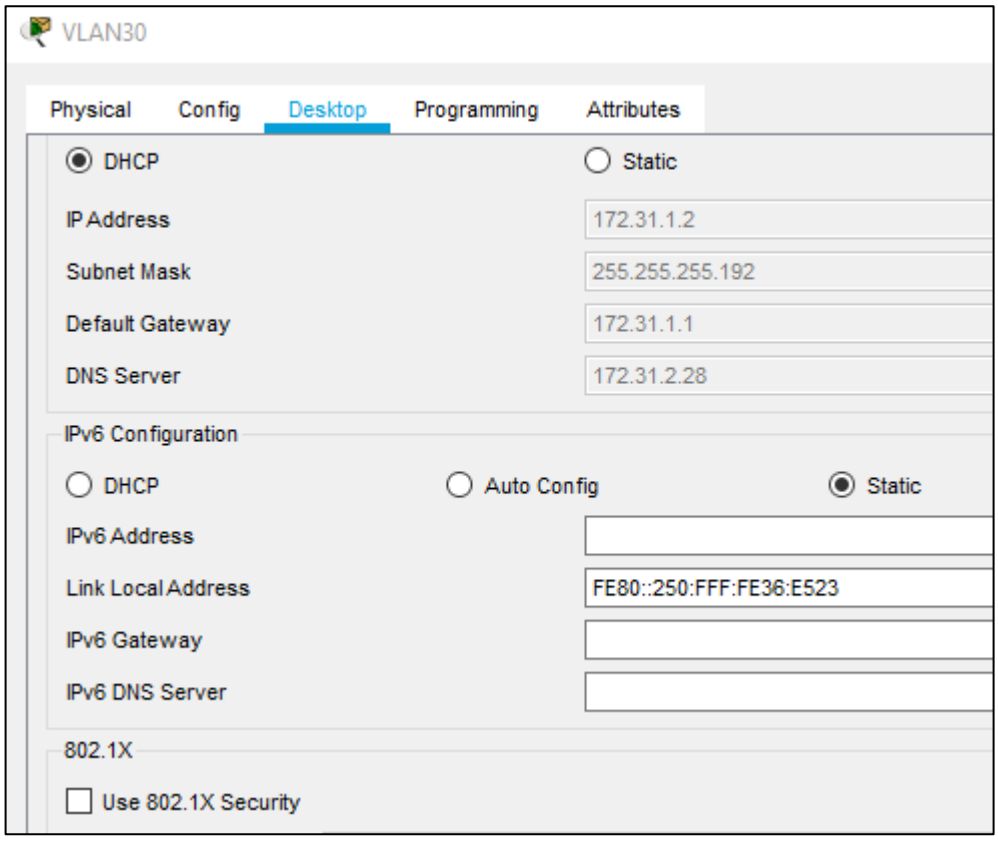


Ilustración 23 Direccionamiento DHCP VLAN 30 Cundinamarca



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

TUNJA(dhcp-config)#ip nat inside source static 172.31.2.28 209.165.220.4

TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255

TUNJA(config)#ip nat inside source list 1 interface g0/1 overload

TUNJA(config)#int g0/1

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#int g0/0.1

TUNJA(config-subif)#ip nat inside

TUNJA(config-subif)#int g0/0.20

```
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/0.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#
TUNJA#show ip route
TUNJA#show ip route

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

Gateway of last resort is 209.165.220.3 to network 0.0.0.0
172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.3.2.8/29 is directly connected, GigabitEthernet0/0.1
L       172.3.2.9/32 is directly connected, GigabitEthernet0/0.1
```

172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks

O 172.31.0.0/26 [110/65] via 172.31.2.34, 01:39:37, Serial0/0/0

O 172.31.0.64/26 [110/65] via 172.31.2.34, 01:39:37, Serial0/0/0

C 172.31.0.128/26 is directly connected, GigabitEthernet0/0.20

L 172.31.0.129/32 is directly connected, GigabitEthernet0/0.20

C 172.31.0.192/26 is directly connected, GigabitEthernet0/0.30

L 172.31.0.193/32 is directly connected, GigabitEthernet0/0.30

O 172.31.1.0/26 [110/65] via 172.31.2.38, 01:06:28, Serial0/0/1

O 172.31.1.64/26 [110/65] via 172.31.2.38, 01:06:28, Serial0/0/1

O 172.31.2.0/29 [110/65] via 172.31.2.34, 02:25:47, Serial0/0/0

O 172.31.2.8/29 [110/65] via 172.31.2.38, 02:05:49, Serial0/0/1

O 172.31.2.24/29 [110/65] via 172.31.2.38, 01:06:28, Serial0/0/1

C 172.31.2.32/30 is directly connected, Serial0/0/0

L 172.31.2.33/32 is directly connected, Serial0/0/0

C 172.31.2.36/30 is directly connected, Serial0/0/1

L 172.31.2.37/32 is directly connected, Serial0/0/1

209.165.220.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.220.0/24 is directly connected, GigabitEthernet0/1

L 209.165.220.1/32 is directly connected, GigabitEthernet0/1

S* 0.0.0.0/0 [1/0] via 209.165.220.3

BUCARAMANGA#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

O 172.3.2.8/29 [110/65] via 172.31.2.33, 02:29:15, Serial0/0/0

172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks

C 172.31.0.0/26 is directly connected, GigabitEthernet0/0.10

L 172.31.0.1/32 is directly connected, GigabitEthernet0/0.10

C 172.31.0.64/26 is directly connected, GigabitEthernet0/0.30

L 172.31.0.65/32 is directly connected, GigabitEthernet0/0.30

O 172.31.0.128/26 [110/65] via 172.31.2.33, 02:29:15, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.33, 02:29:15, Serial0/0/0

O 172.31.1.0/26 [110/129] via 172.31.2.33, 01:09:55, Serial0/0/0

O 172.31.1.64/26 [110/129] via 172.31.2.33, 01:09:55, Serial0/0/0

C 172.31.2.0/29 is directly connected, GigabitEthernet0/0.1

L 172.31.2.1/32 is directly connected, GigabitEthernet0/0.1

O 172.31.2.8/29 [110/129] via 172.31.2.33, 02:09:16, Serial0/0/0

O 172.31.2.24/29 [110/129] via 172.31.2.33, 01:09:55, Serial0/0/0

C 172.31.2.32/30 is directly connected, Serial0/0/0

L 172.31.2.34/32 is directly connected, Serial0/0/0

O 172.31.2.36/30 [110/128] via 172.31.2.33, 02:12:35, Serial0/0/0

O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:04:22, Serial0/0/0

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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O       172.3.2.8/29 [110/65] via 172.31.2.37, 02:13:19, Serial0/0/0

172.31.0.0/16 is variably subnetted, 16 subnets, 4 masks
O       172.31.0.0/26 [110/129] via 172.31.2.37, 01:45:18, Serial0/0/0
O       172.31.0.64/26 [110/129] via 172.31.2.37, 01:45:18, Serial0/0/0
O       172.31.0.128/26 [110/65] via 172.31.2.37, 02:13:19, Serial0/0/0
O       172.31.0.192/26 [110/65] via 172.31.2.37, 02:13:19, Serial0/0/0
C       172.31.1.0/26 is directly connected, GigabitEthernet0/0.30
L       172.31.1.1/32 is directly connected, GigabitEthernet0/0.30
C       172.31.1.64/26 is directly connected, GigabitEthernet0/0.20
L       172.31.1.65/32 is directly connected, GigabitEthernet0/0.20
O       172.31.2.0/29 [110/129] via 172.31.2.37, 02:13:19, Serial0/0/0
C       172.31.2.8/29 is directly connected, GigabitEthernet0/0.1
L       172.31.2.9/32 is directly connected, GigabitEthernet0/0.1
```

C 172.31.2.24/29 is directly connected, GigabitEthernet0/0.88

L 172.31.2.25/32 is directly connected, GigabitEthernet0/0.88

O 172.31.2.32/30 [110/128] via 172.31.2.37, 02:13:19, Serial0/0/0

C 172.31.2.36/30 is directly connected, Serial0/0/0

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

O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:06:36, Serial0/0/0

1.4.9 El enrutamiento deberá tener autenticación

BUCARAMANGA#conf t

BUCARAMANGA(config)#int s0/0/0

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

BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco123

BUCARAMANGA(config-if)#

CUNDINAMARCA(config)#int s0/0/0

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

CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco123

CUNDINAMARCA(config-if)#

TUNJA#conf t

TUNJA(config)#int s0/0/0

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

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco123

TUNJA(config-if)#int s0/0/1

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

TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco123

1.4.10 Listas de control de acceso

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

CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

CUNDINAMARCA(config)#access-list 111 permit ip any

CUNDINAMARCA(config)#int g0/0.20

CUNDINAMARCA(config-subif)#ip access-group 111 in

CUNDINAMARCA(config-subif)#

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

CUNDINAMARCA(config-subif)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

CUNDINAMARCA(config)#access-list 112 deny ip any

CUNDINAMARCA(config)#int g0/0.30

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

CUNDINAMARCA(config-subif)#

1.4.10.3 Los host de la VLAN 30 en Tunja solo acceden a servidores web y FTP de internet

TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80

TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21

TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20

TUNJA(config)#int g0/0.30

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

TUNJA(config-subif)#

1.4.10.4 Los host de la VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca

TUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63

TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

TUNJA(config)#int g0/0.20

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

TUNJA(config-subif)#

1.4.10.5 Los host de la VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de la VLAN 10

BUCARAMANGA(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255

BUCARAMANGA(config)#int g0/0.30

BUCARAMANGA(config-subif)#ip access-group 111 in

BUCARAMANGA(config-subif)#

1.4.10.6 Los host de la VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN20), no internet

BUCARAMANGA(config-subif)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

BUCARAMANGA(config)#int g0/0.10

BUCARAMANGA(config-subif)#ip access-group 112 in

BUCARAMANGA(config-subif)#

1.4.10.7 Los host de una VLAN no pueden acceder a los de otra vlan en una ciudad

BUCARAMANGA(config-subif)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63

BUCARAMANGA(config)#access- list 113 permit ip any

BUCARAMANGA(config)#int g0/0.10

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

BUCARAMANGA(config-subif)#

TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63

TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63

TUNJA(config)#access-list 113 permit ip any

TUNJA(config)#int g0/0.20

TUNJA(config-subif)#ip access-group 113 out

TUNJA(config-subif)#

CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

CUNDINAMARCA(config)#access- list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63

CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

CUNDINAMARCA(config)#access- list 113 permit ip any

CUNDINAMARCA(config)#int g0/0.20

CUNDINAMARCA(config-subif)#ip access-group 113 out

CUNDINAMARCA(config-subif)#

1.4.10.8 Solo los host de las vlan administrativas y de la vlan de servidores tiene acceso a los routers e internet

BUCARAMANGA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7

BUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7

BUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7

BUCARAMANGA(config)#line vty 0 15

BUCARAMANGA(config-line)#access-class 3 in

BUCARAMANGA(config-line)#

TUNJA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7

TUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7

```
TUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 15
TUNJA(config-line)#access-class 3 in

CUNDINAMARCA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
CUNDINAMARCA(config-line)#
```

2. CONCLUSIONES

- Haciendo uso de los comandos ping, traceroute, show ip route del protocolo ICMP, se llevó a cabo la revisión en la configuración de los dispositivos y routers, para cada uno de los escenarios.

- Se definió el direccionamiento para los dispositivos de cada escenario.

- Aplicando los parámetros de enrutamiento, detección de vecinos directamente conectados, los routers lograron intercambiar información de ruteo.

- Se establecen los parámetros de seguridad para la red y las subredes a fin de mantener un entorno seguro.

- Se realizo la configuración de enrutamiento y las listas de control de acceso (ACL) esta permite mejorar la seguridad, haciendo uso de los filtros de tráfico de una lista de redes y acciones correlacionadas, permitiendo el acceso negado a algunos dispositivos de red.

BIBLIOGRAFÍA

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

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

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3