INFORME FINAL DE HABILIDADES PRÁCTICAS DIPLOMADO CISCO CCNP

HECTOR ANDRES RAMIREZ CANOLES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD FACULTAD DE INGENIERÍA

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP

NEIVA - HUILA

2020

INFORME FINAL DE HABILIDADES PRÁCTICAS DIPLOMADO CISCO CCNP

HECTOR ANDRES RAMIREZ CANOLES

Presentado al Tutor:

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD FACULTAD DE INGENIERÍA

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP

NEIVA - HUILA

2019

TABLA DE CONTENIDO

Contenido

INTRODUCCION

Cisco es una empresa de comunicaciones líder en el mundo de las redes de datos y TI, es una compañía muy importante que fabrica componentes de red, como routers, firewalls de hardware, productos de telefonía IP, entre otros, estos dispositivos son bastantes robustos y conocidos en todo el mundo. En la actualidad las telecomunicaciones y sistemas han evolucionado a tan altos estándares de seguridad, especificaciones técnicas y complejidad tanto de protocolos de seguridad como de especificaciones técnicas en los diferentes equipos que conforman las redes a nivel mundial por lo cual, se ha creado la necesidad de generar cada día más protocolos, estándares y configuraciones que nos permitan brindar servicios oportunos, adecuados, seguros, confiables y de fácil configuración y administración es por esto que el presente informe se realizará la solución de 2 escenarios con diferentes tipos de configuraciones que se realizan en los entornos reales de las redes de comunicación a diario esto con el fin de evaluar y poner en práctica los conocimientos aprendidos a lo largo del diplomado

RESUMEN

El certificado de Cisco, Certified Network Associate (CCNA**).** Valida la capacidad de instalar, configurar, operar y solucionar problemas de rutas de tamaño medio y redes conmutadas, incluida la implementación y verificación de conexiones a sitios remotos en una WAN**.** El plan de estudios de CCNA incluye la mitigación básica de las amenazas de seguridad, la introducción a conceptos y terminología de redes inalámbricas y las habilidades basadas en el rendimiento. Este nuevo plan de estudios también incluye el uso de los siguientes protocolos: IP, protocolo de enrutamiento de puerta interior mejorada (EIGRP), protocolo de interfaz de línea serie Frame Relay, protocolo de información de enrutamiento versión 2 (RIPv2), VLANs, Ethernet y acceso a listas de control (ACL). Durante el desarrollo de la evaluación denominada “Prueba de habilidades prácticas”, del Diplomado de Profundización CCNP, busca identificar, implementar, desarrollar las competencias y habilidades que se aprendieron durante todo el desarrollo del diplomado, permitiendo así poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos del Networking con los que nos enfrentaremos en la práctica real de nuestra labor como ingenieros o trabajadores en instalación, estructuración e implementación de redes.

ABSTRACT

The Cisco Certificate, Certified Network Associate (CCNA). Validates the ability to install, configure, operate and troubleshoot medium-sized routes and switched networks, including the implementation and verification of connections to remote sites on a WAN. The CCNA curriculum includes basic mitigation of security threats, introduction to wireless network concepts and terminology, and performance-based skills. This new curriculum also includes the use of the following protocols: IP, Enhanced Internal Door Routing Protocol (EIGRP), Frame Relay Serial Line Interface Protocol, Version 2 Routing Information Protocol (RIPv2), VLANs, Ethernet and access to checklists (ACL). During the development of the evaluation called “Test of practical skills”, of the CCNP Deepening Diploma, seeks to identify, implement, develop the skills and abilities that were learned throughout the development of the diploma, thus allowing to test the levels of understanding and solution of problems related to various aspects of Networking with which we will face in the real practice of our work as engineers or workers in installation, structuring and implementation of networks.

OBJETIVOS

OBJETIVO GENERAL:

Repasar y estudiar de manera satisfactoria el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), para aprender y poner en marcha el estudio de la Configuración de Sistemas de Red soportados en VLANs, Configuración y control de ACL para IPv4 e IPv6, Implementación de DHCP y NAT para IPv4 y IPv6 incluye su propio espacio de direcciones IPv6 privadas y NAT, configuración OSPFv2.

OBJETIVOS ESPECÍFICOS

- Realizar las prácticas en Packet Tracer para simular los ambientes reales de trabajo en campo.

- Configurar routers y switches, y resolver problemas relacionados, así como solucionar problemas frecuentes de OSPF de área única y OSPF multiárea, de LAN virtuales y de routing entre VLAN en redes IPv4

- Describir, controlar y configurar ACL para IPv4 y descubrir los tipos de medios utilizados para transportar datos a través de la red.

- Describir las tecnologías de switching mejoradas, como las VLAN, el protocolo de enlace troncal de VLAN (VTP), el protocolo de árbol de expansión rápido (RSTP), el protocolo de árbol de expansión por VLAN (PVSTP) y 802.1q

TABLA DE CONTENIDO DE GRAFICAS

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.

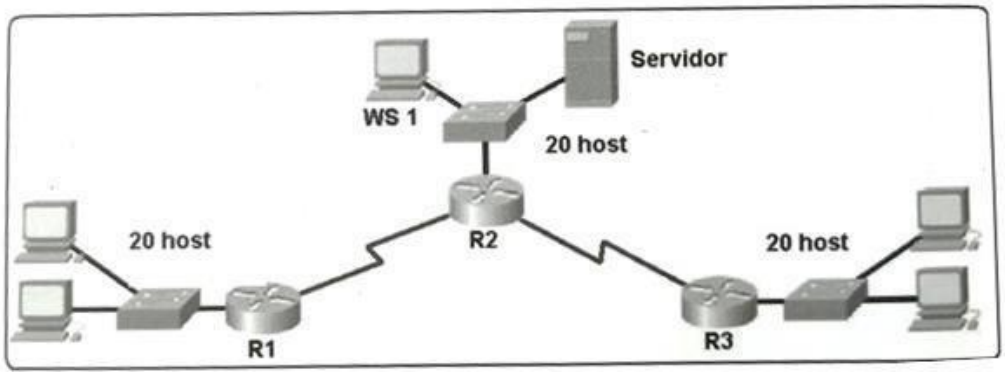
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

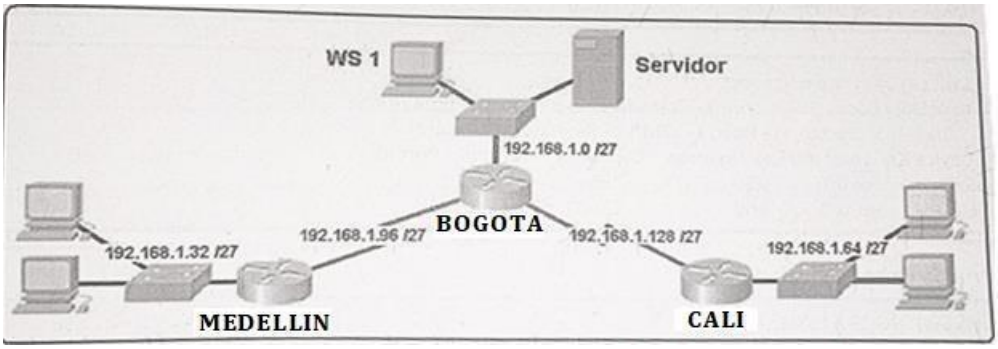
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.





DESARROLLO

NOTA: TODAS LAS CONTRASEÑAS DE ACCESO PARA LOS ESCENARIOS EN CONSOLA TELNET, SON:

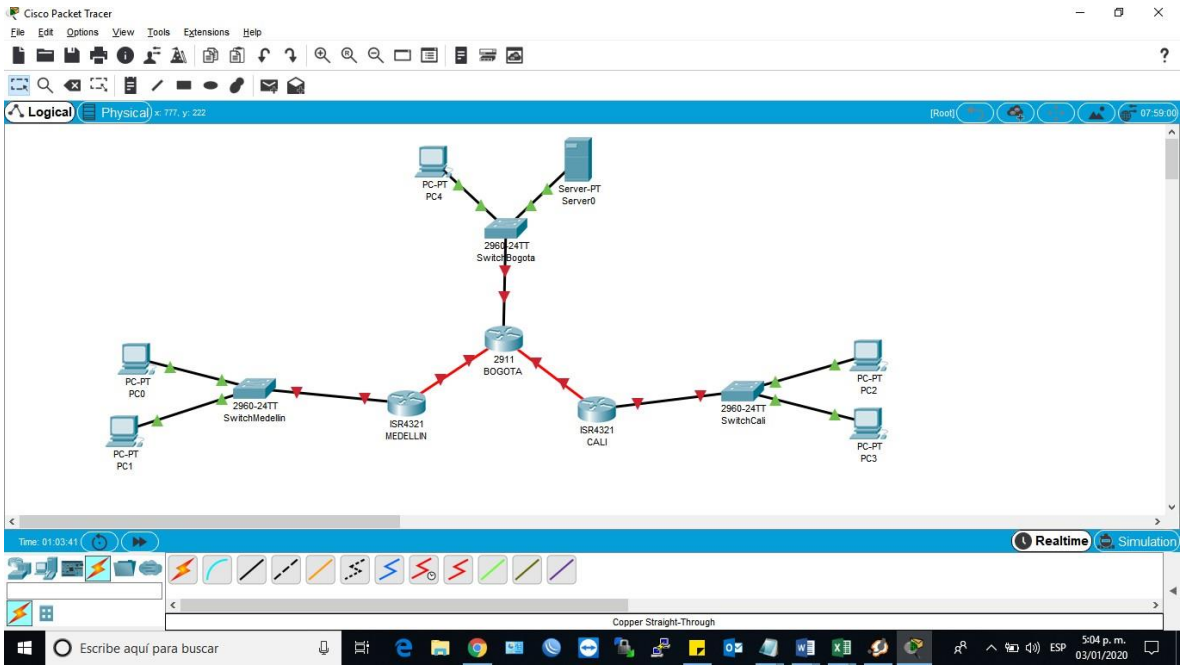
123456789

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico ydejar 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 Configurar la topología de

red, de acuerdo con las siguientes especificaciones.



Parte 1: Asignación de direcciones IP:

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

R/ Se toman 3 bits para crear las 8 subredes. $2^3 = 8$ *Subredes*
Estas tomaran la siguiente mascara $/27 = 255.255.255.224$

			BINARIO		
RED 0	RED	192.168.1.**000**	0	0000	192.168.1.0
	PRIMERA IP	192.168.1.**000**	0	0001	192.168.1.1
	ULTIMA IP	192.168.1.**000**	1	1110	192.168.1.30
	BROADCAST	192.168.1.**000**	1	1111	192.168.1.31

			BINARIO		
RED 1	RED	192.168.1.**001**	0	0000	192.168.1.32
	PRIMERA IP	192.168.1.**001**	0	0001	192.168.1.33
	ULTIMA IP	192.168.1.**001**	1	1110	192.168.1.62
	BROADCAST	192.168.1.**001**	1	1111	192.168.1.63

	BINARIO

RED 2	RED	192.168.1.**010**	0	0000	192.168.1.64
	PRIMERA IP	192.168.1.**010**	0	0001	192.168.1.65
	ULTIMA IP	192.168.1.**010**	1	1110	192.168.1.94
	BROADCAST	192.168.1.**010**	1	1111	192.168.1.95

			BINARIO		
RED 3	RED	192.168.1.**011**	0	0000	192.168.1.96
	PRIMERA IP	192.168.1.**011**	0	0001	192.168.1.97
	ULTIMA IP	192.168.1.**011**	1	1110	192.168.1.126
	BROADCAST	192.168.1.**011**	1	1111	192.168.1.127

			BINARIO		
RED 4	RED	192.168.1.**100**	0	0000	192.168.1.128
	PRIMERA IP	192.168.1.**100**	0	0001	192.168.1.129
	ULTIMA IP	192.168.1.**100**	1	1110	192.168.1.158
	BROADCAST	192.168.1.**100**	1	1111	192.168.1.159

			BINARIO		
RED 5	RED	192.168.1.**101**	0	0000	192.168.1.160
	PRIMERA IP	192.168.1.**101**	0	0001	192.168.1.161
	ULTIMA IP	192.168.1.**101**	1	1110	192.168.1.190
	BROADCAST	192.168.1.**101**	1	1111	192.168.1.191

			BINARIO		
RED 6	RED	192.168.1.**110**	0	0000	192.168.1.192
	PRIMERA IP	192.168.1.**110**	0	0001	192.168.1.193
	ULTIMA IP	192.168.1.**110**	1	1110	192.168.1.222
	BROADCAST	192.168.1.**110**	1	1111	192.168.1.223

			BINARIO		
RED 7	RED	192.168.1.**111**	0	0000	192.168.1.224
	PRIMERA IP	192.168.1.**111**	0	0001	192.168.1.225
	ULTIMA IP	192.168.1.**111**	1	1110	192.168.1.254
	BROADCAST	192.168.1.**111**	1	1111	192.168.1.255

b. Asignar una dirección IP a la red.

R/ 192.168.1.0

Parte 2: Configuración Básica.

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

	R 1	R 2	R 3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ipeninterfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

R1 MEDELLIN =

```
R1#show running-config
Building configuration...

Current configuration : 994 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!enable password 7 08701E1D5D4C53404A52
!
!
!no ip cef
no ipv6 cef
!
!
license udi pid CISCO2911/K9 sn FTX1524S663-
!
!
!
spanning-tree mode pvst
```

```
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed  auto
shutdown
!
interface Serial0/0/0
ip address 192.168.1.99 255.255.255.224
clock rate 2000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!!
line con 0
password 7 08701E1D5D4C53404A52
login
```

```
!
line aux 0
!
line vty 0 4
login
!
!
end
```

R2BOGOTA =

```
R2#SHOW RUNning-config
Building configuration...

Current configuration : 1504 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
enable password 7 08701E1D5D4C53404A52
!
!
no ip cef
no ipv6 cef
!
!
username cisco password 7 08701E1D5D4C53
!
!
license udi pid CISCO2911/K9 sn FTX152490H2-
!
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
no ip address
```

```
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed  auto
shutdown
!
interface Serial0/0/0
ip address 192.168.1.98 255.255.255.224
!
interface Serial0/0/1
ip address 192.168.1.130 255.255.255.224
!
interface GigabitEthernet0/1/0
no ip address
shutdown
!
interface FastEthernet0/2/0
switchport mode access
!
interface FastEthernet0/2/1
switchport mode access
!
interface FastEthernet0/2/2
switchport mode access
!
interface FastEthernet0/2/3
switchport mode access
!
interface FastEthernet0/3/0
switchport mode access
!
interface FastEthernet0/3/1
switchport mode access
!
interface FastEthernet0/3/2
```

```
switchport mode access
!
interface FastEthernet0/3/3
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!
line con 0
password 7 08701E1D5D4C53404A52
login
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

R3CALI =

```
R3#SHOW RUNning-config
Building configuration...

Current configuration : 995 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```

```
hostname R3
!
!
enable password 7 08701E1D5D4C53404A52
!
!
no ip cef
no ipv6 cef
!
!
license udi pid CISCO2911/K9 sn FTX1524RH8Q-
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed  auto
shutdown
!
interface Serial0/0/0
ip address 192.168.1.131 255.255.255.224
clock rate 2000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
```

```
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
!
ip classless
!
ip flow-export version 9
!
!
!
line con 0
password 7 08701E1D5D4C53404A52
login
!
line aux 0
!
line vty 0 4
login
!
!
!end
```

R3#

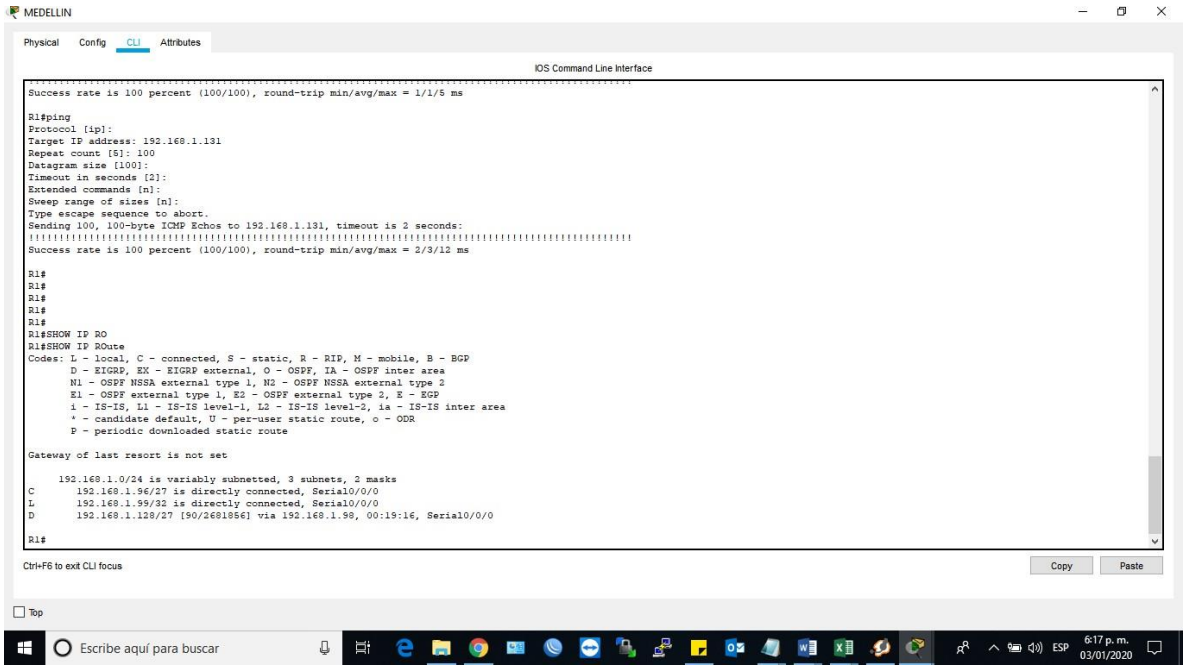
b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

R1MEDELLIN =

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.1.96/27 is directly connected, Serial0/0/0
```

L 192.168.1.99/32 is directly connected, Serial0/0/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:19:16, Serial0/0/0

R1#

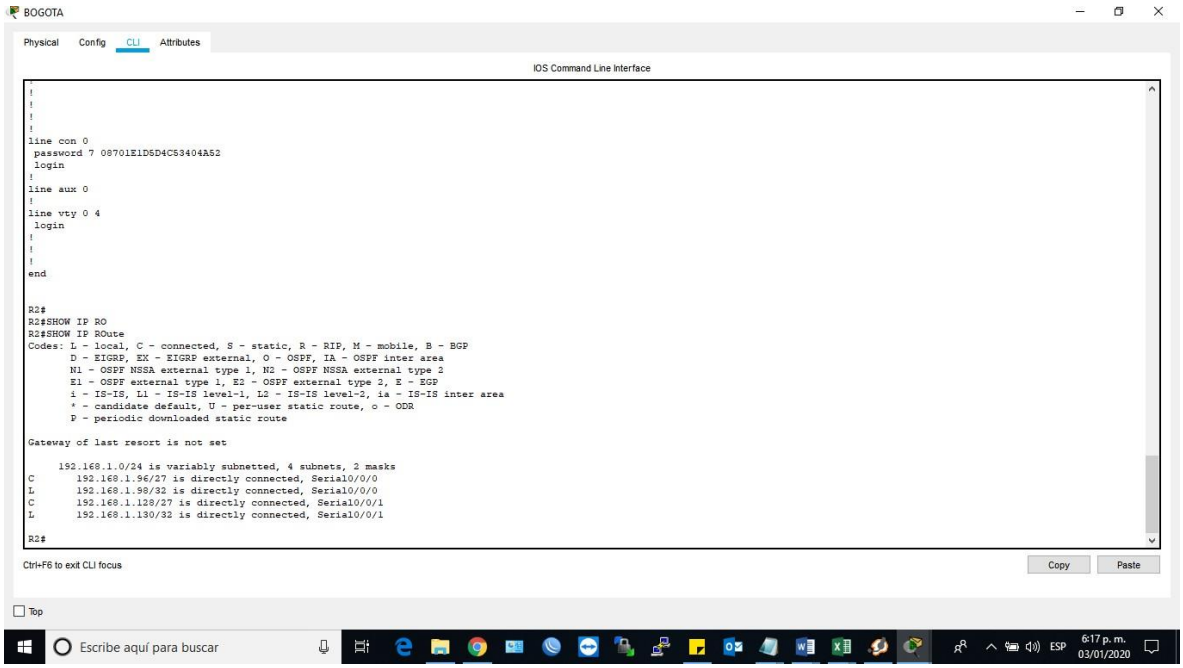


R2BOGOTA =
R2#SHOW IP ROute
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.130/32 is directly connected, Serial0/0/1

R2#

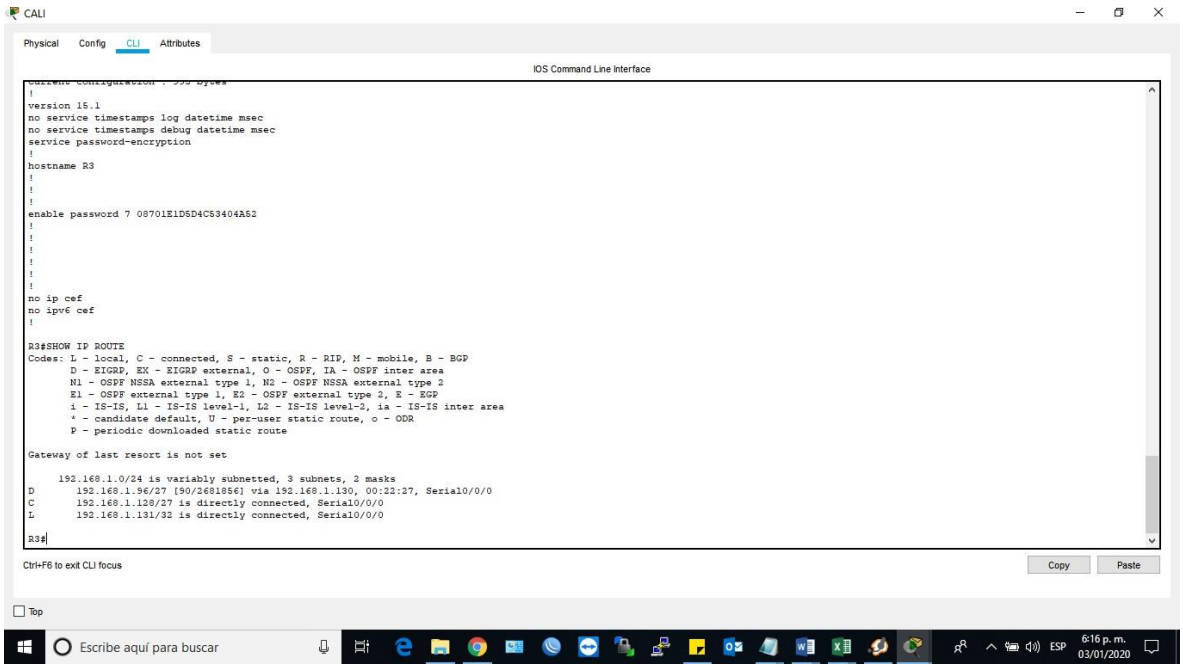


R3CALI =
R3#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:22:27, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/0
L 192.168.1.131/32 is directly connected, Serial0/0/0

R3#



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

R1MEDELLIN =
R1#SHOW IP ROUTE 192.168.1.0
Routing entry for 192.168.1.0/24, 3 known subnets
Attached (2 connections)
Variably subnetted with 2 masks
Redistributing via eigrp 200, eigrp 200
C 192.168.1.96/27 is directly connected, Serial0/0/0
192.168.1.99/32 is directly connected, Serial0/0/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:32:53, Serial0/0/0

R1#

R2BOGOTA =
R2#SHOW IP ROUte 192.168.1.0
Routing entry for 192.168.1.0/24, 4 known subnets
Attached (4 connections)
Variably subnetted with 2 masks
Redistributing via eigrp 200, eigrp 200
C 192.168.1.96/27 is directly connected, Serial0/0/0
192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1

192.168.1.130/32 is directly connected, Serial0/0/1

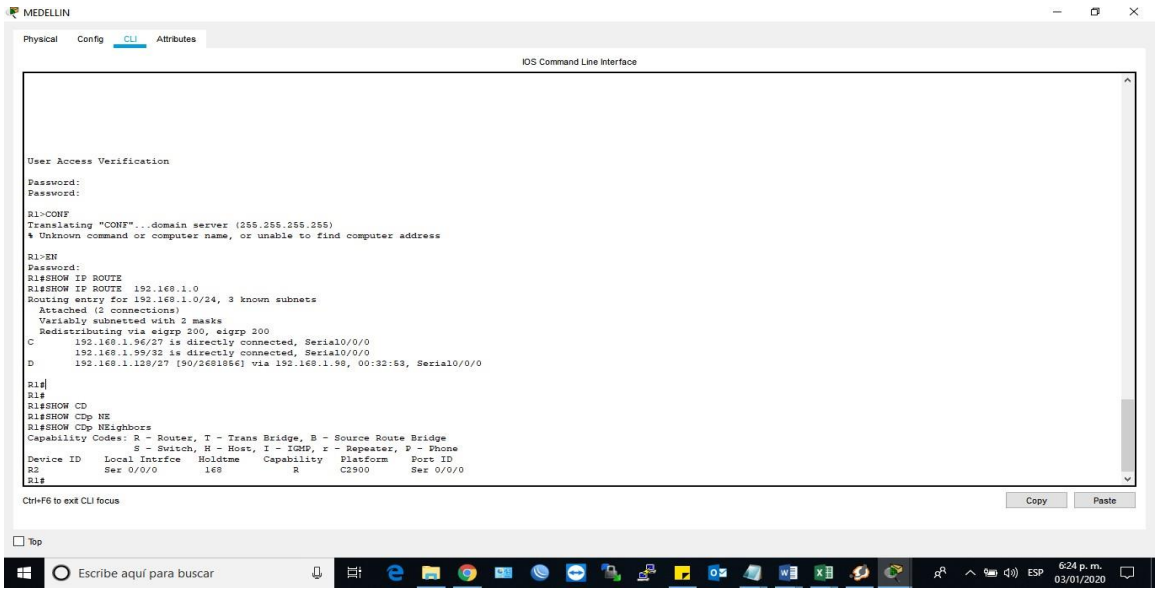
R2#

R3CALI =
R3#SHOW IP ROUTE 192.168.1.0
Routing entry for 192.168.1.0/24, 3 known subnets
Attached (2 connections)
Variably subnetted with 2 masks
Redistributing via eigrp 200, eigrp 200
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:35:08, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/0
192.168.1.131/32 is directly connected, Serial0/0/0

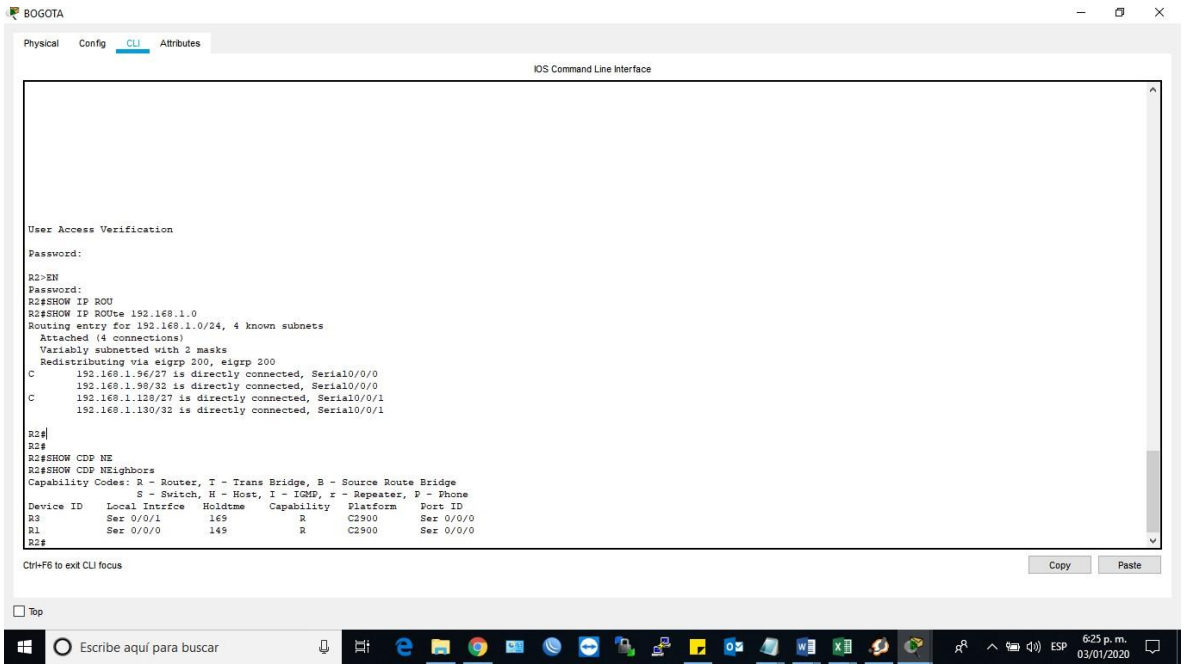
R3#

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

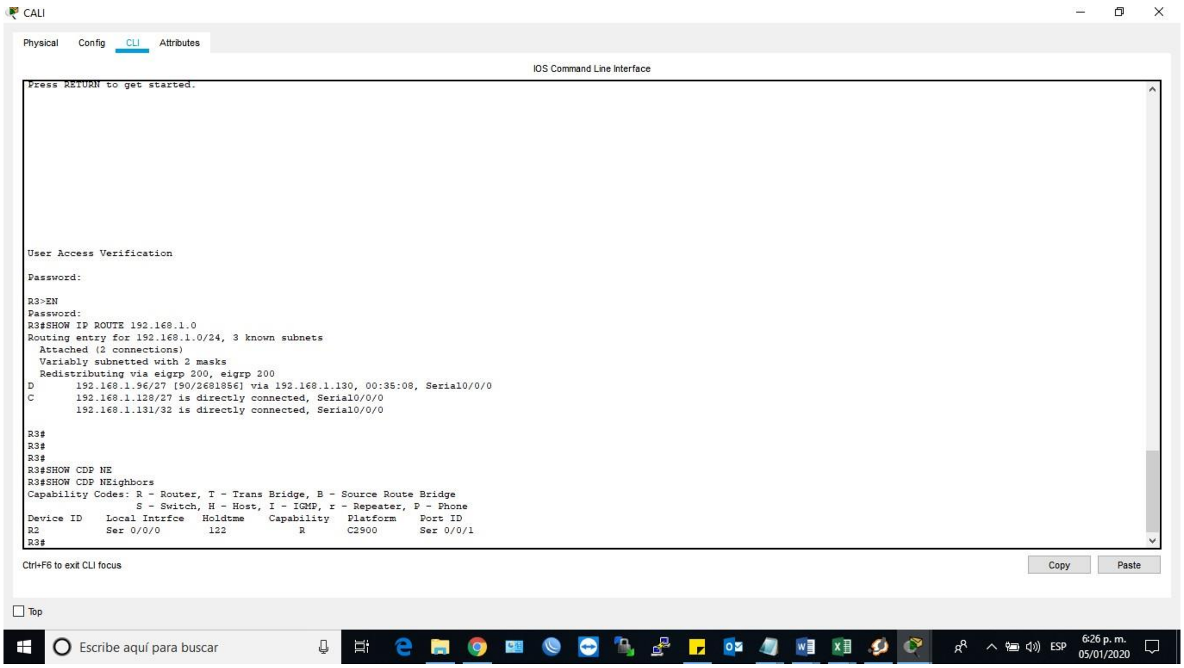
R1MEDELLIN =
R1#SHOW CDp NEighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
R2 Ser 0/0/0 168 R C2900 Ser 0/0/0
R1#



R2BOGOTA =
R2#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
R3 Ser 0/0/1 169 R C2900 Ser 0/0/0
R1 Ser 0/0/0 149 R C2900 Ser 0/0/0
R2#



R3CALI =
R3#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
R2 Ser 0/0/0 122 R C2900 Ser 0/0/1
R3#



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

PRUEBAS R1 HACIA LAS 2 PUNTAS BOGOTA Y MEDELLIN

Prueba de conectividad R1 hacia R2 a la interfaz que tiene 192.168.1.98

R1#ping
Protocol [ip]:
Target IP address: 192.168.1.98
Repeat count [5]: 100
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/6 ms

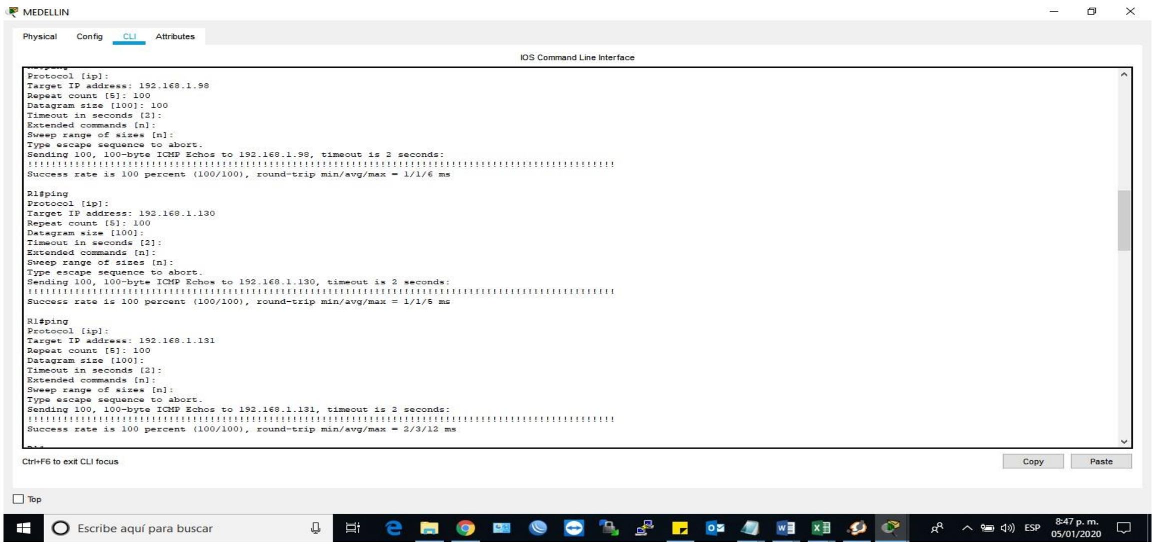
Prueba de conectividad R1 hacia R2 a la interfaz que tiene 192.168.1.130

R1#ping
Protocol [ip]:

Target IP address: 192.168.1.130
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/5 ms

Prueba de conectividad R1 hacia R3 a la interfaz que tiene 192.168.1.131

R1#ping
Protocol [ip]:
Target IP address: 192.168.1.131
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/3/12 ms



EVIDENCIA PING DESDE R1MEDELLIN

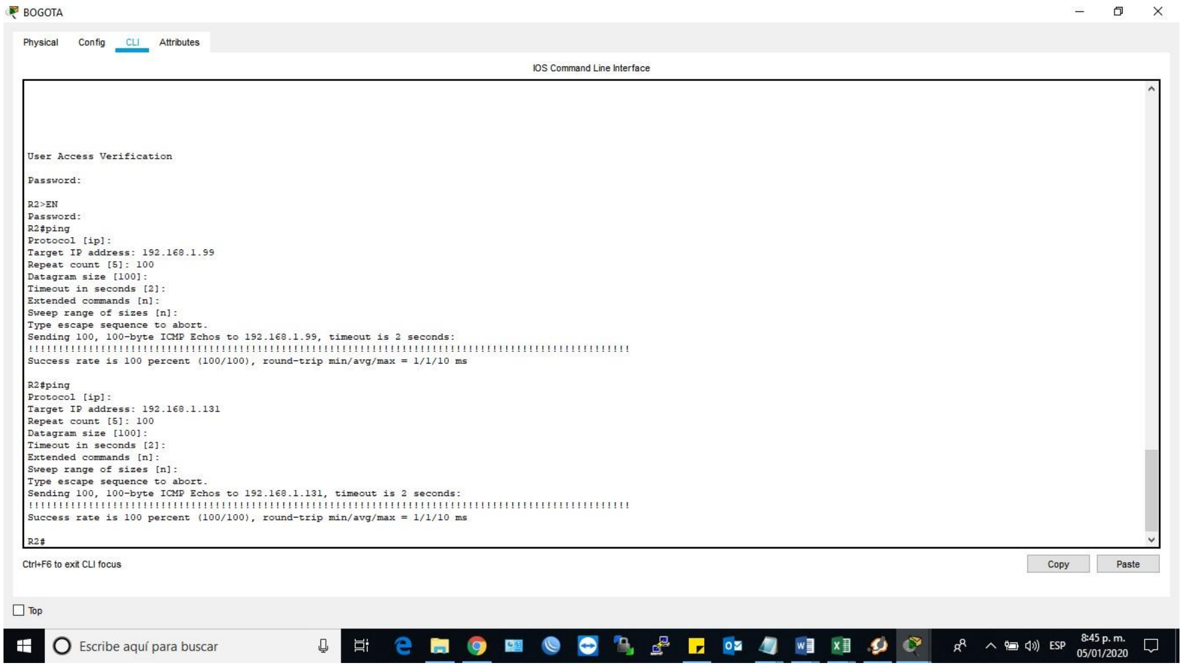
PRUEBAS R2 HACIA LAS 2 PUNTAS CALI Y MEDELLIN

Prueba de conectividad R2 hacia R1 a la interfaz que tiene 192.168.1.99

```
R2>EN
Password:
R2#ping
Protocol [ip]:
Target IP address: 192.168.1.99
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/10 ms
```

Prueba de conectividad R2 hacia R3 a la interfaz que tiene 192.168.1.131

```
R2#ping
Protocol [ip]:
Target IP address: 192.168.1.131
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/10 ms
```



EVIDENCIA PING DESDE R2BOGOTA

PRUEBAS R3 HACIA LAS 2 PUNTAS BOGOTA Y MEDELLIN

Prueba de conectividad R3 hacia R2 a la interfaz que tiene 192.168.1.98

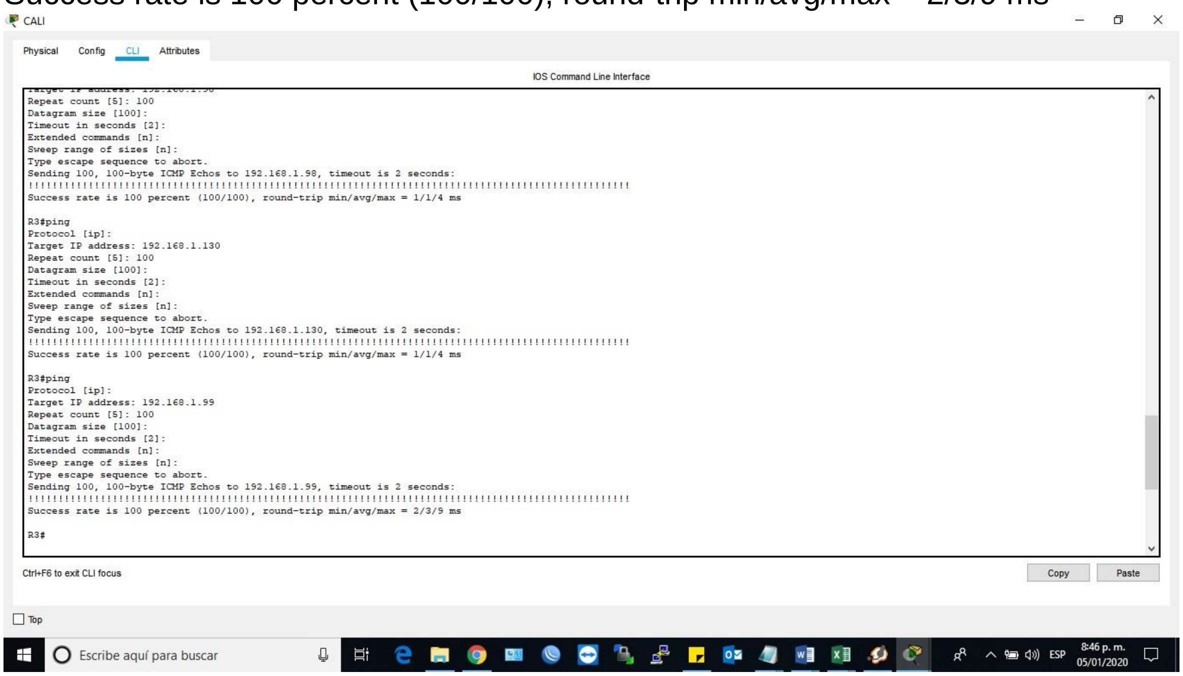
R3#ping
Protocol [ip]:
Target IP address: 192.168.1.98
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

Prueba de conectividad R3 hacia R2 a la interfaz que tiene 192.168.1.130
R3#ping
Protocol [ip]:
Target IP address: 192.168.1.130
Repeat count [5]: 100
Datagram size [100]:

Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

Prueba de conectividad R3 hacia R1 a la interfaz que tiene 192.168.1.99

R3#ping
Protocol [ip]:
Target IP address: 192.168.1.99
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/3/9 ms



Evidencia ping desde R3CALI

Parte 3: Configuración de Enrutamiento.

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

ASIGNACION DEL PROTOCOLO EIGRP A R1 MEDELLIN:

```
R1>EN
Password:
R1#CONFIGURE
R1#CONFIGURE TERMINAl
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ROUTER EIGRP 200
R1(config-router)#NETW
R1(config-router)#NETWORK 192.168.1.0 0.0.0.255
```

RESULTADO DEL RUNNING-CONFIG QUE DEMUESTRA QUE EL PROTOCOLO EIGRP CON EL AS 200 ESTA EN FUNCIONANMIENTO:

```
interface Serial0/0/0
ip address 192.168.1.99 255.255.255.224
clock rate 2000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
    !
```

ASIGNACION DEL PROTOCOLO EIGRP A R2 BOGOTA

```
User Access Verification
Password:
```

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ei
R2(config)#router eigrp 200
R2(config-router)#network 192.168.1.0 0.0.0.255
R2(config-router)#exit
```

RESULTADO DEL RUNNING-CONFIG QUE DEMUESTRA QUE EL PROTOCOLO EIGRP CON EL AS 200 ESTA EN FUNCIONANMIENTO:

```
interface Serial0/0/0
ip address 192.168.1.98 255.255.255.224
!
interface Serial0/0/1
ip address 192.168.1.130 255.255.255.224
!
interface GigabitEthernet0/1/0
no ip address
shutdown
!
interface FastEthernet0/2/0
switchport mode access
!
interface FastEthernet0/2/1
switchport mode access
!
interface FastEthernet0/2/2
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
    !
```

ASIGNACION DEL PROTOCOLO EIGRP A R3 CALI

```
R3>EN
Password:
```

```
R3#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ROUTER EI
R3(config)#ROUTER EIgrp 200
R3(config-router)#NETwork 192.168.1.0 0.0.0.255
R3(config-router)#EXIT
```

RESULTADO DEL RUNNING-CONFIG QUE DEMUESTRA QUE EL PROTOCOLO EIGRP CON EL AS 200 ESTA EN FUNCIONANMIENTO:

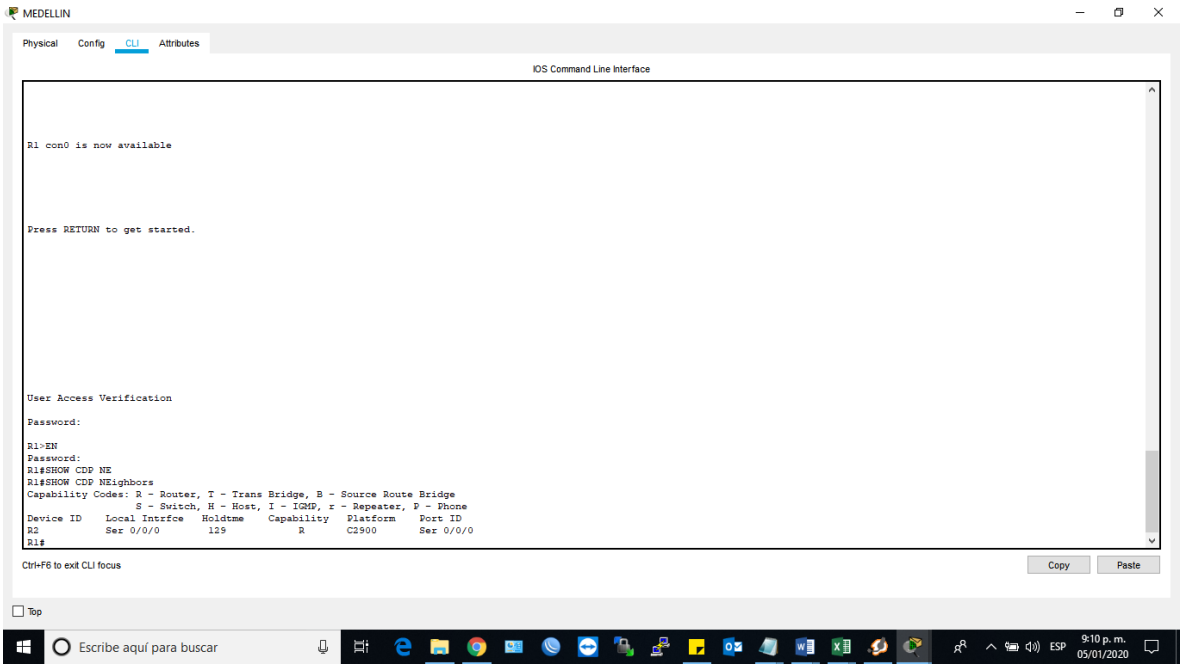
```
!
interface Serial0/0/0
ip address 192.168.1.131 255.255.255.224
clock rate 2000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.0
!
```

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

R1_MEDELLIN

```
R1#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
R2 Ser 0/0/0 129 R C2900 Ser 0/0/0
```

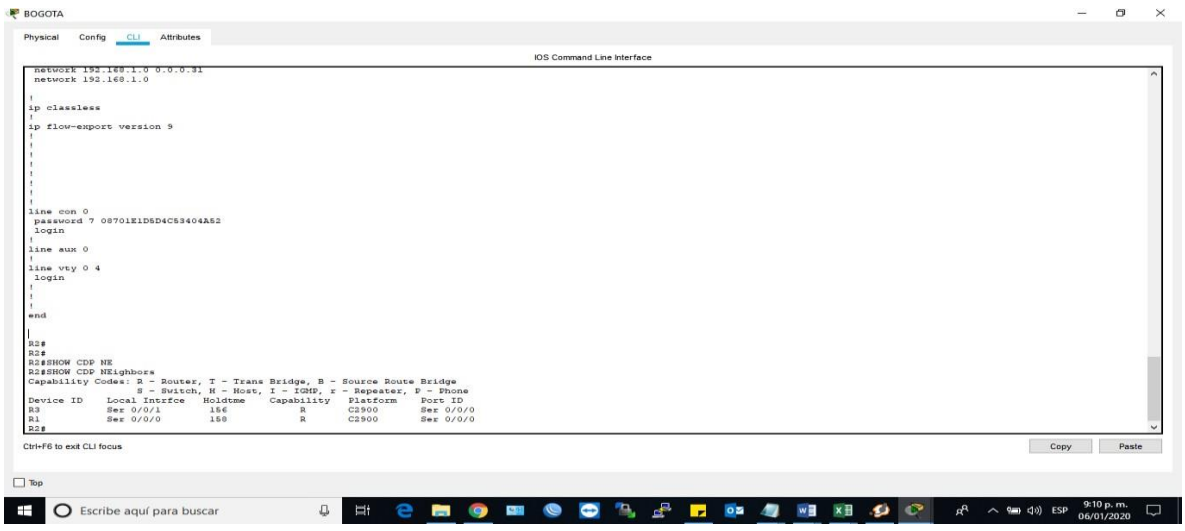
SE EVIDENCIA QUE TIENE COMO VECINO A R2 BOGOTA Y ESTE ES EL QUE REDIRECCIONA HACIA CALI



R2_BOGOTA

R2#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
R3 Ser 0/0/1 156 R C2900 Ser 0/0/0
R1 Ser 0/0/0 158 R C2900 Ser 0/0/0

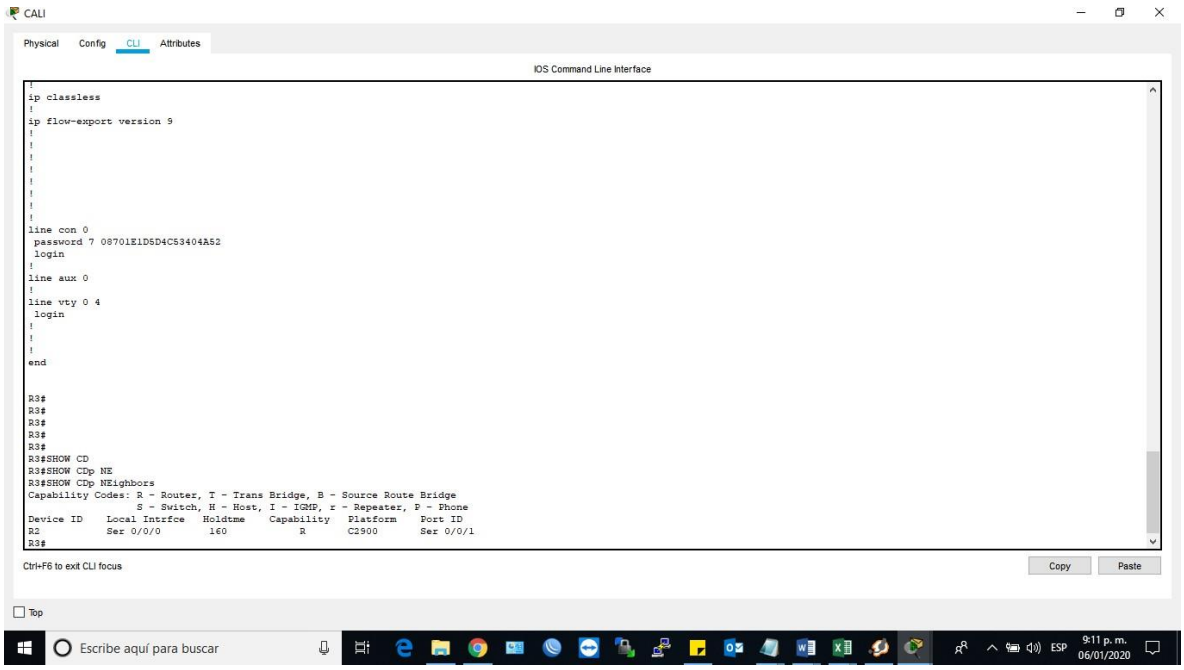
SE EVIDENCIA QUE TIENE COMO VECINO A R1 Y A R3



R3_CALI

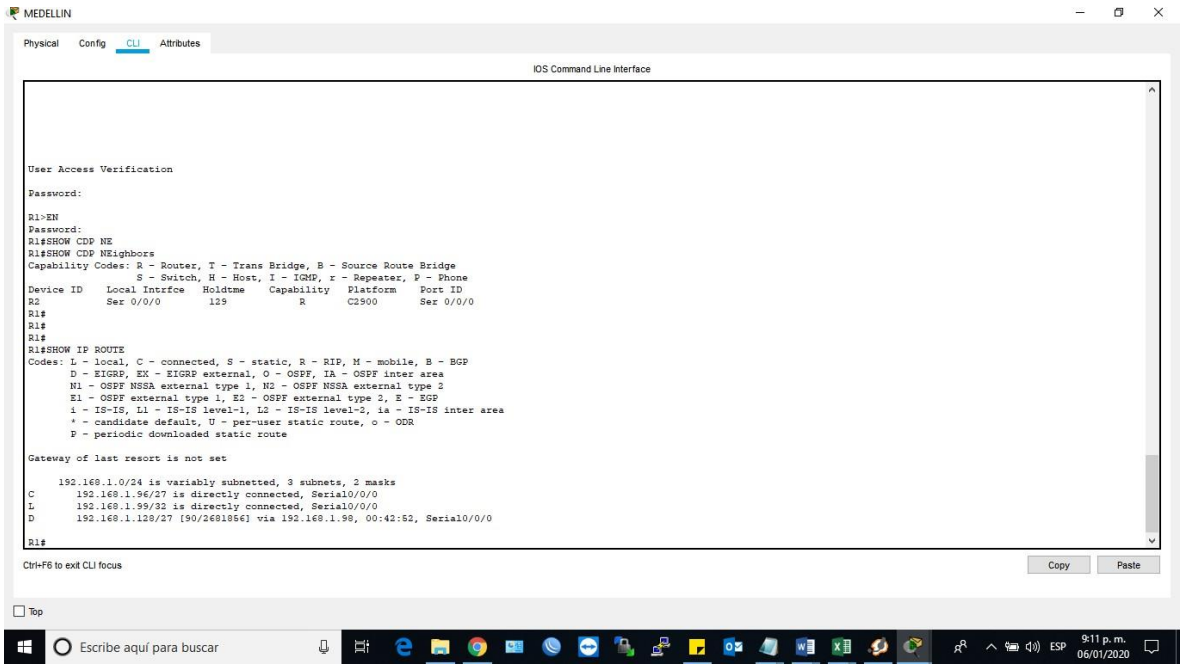
R3#SHOW CDp NEighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
R2 Ser 0/0/0 160 R C2900 Ser 0/0/1

SE EVIDENCIA QUE TIENE COMO VECINO A R2 BOGOTA Y ESTE ES EL QUE REDIRECCIONA HACIA MEDELLIN



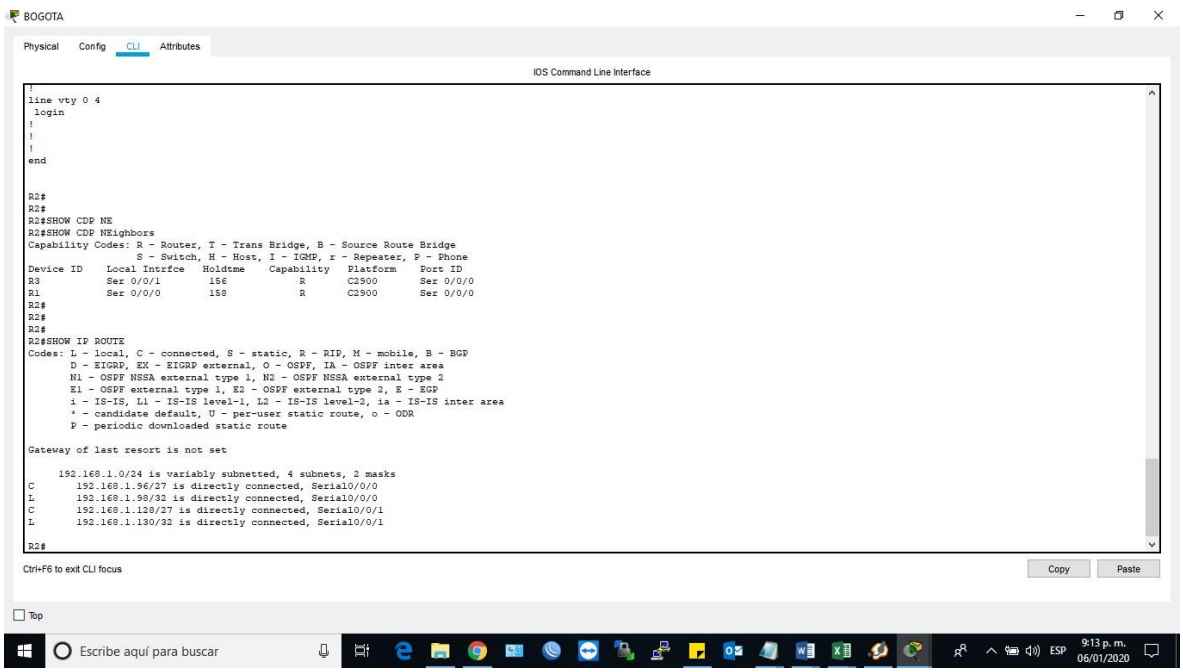
c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

R1MEDELLIN =



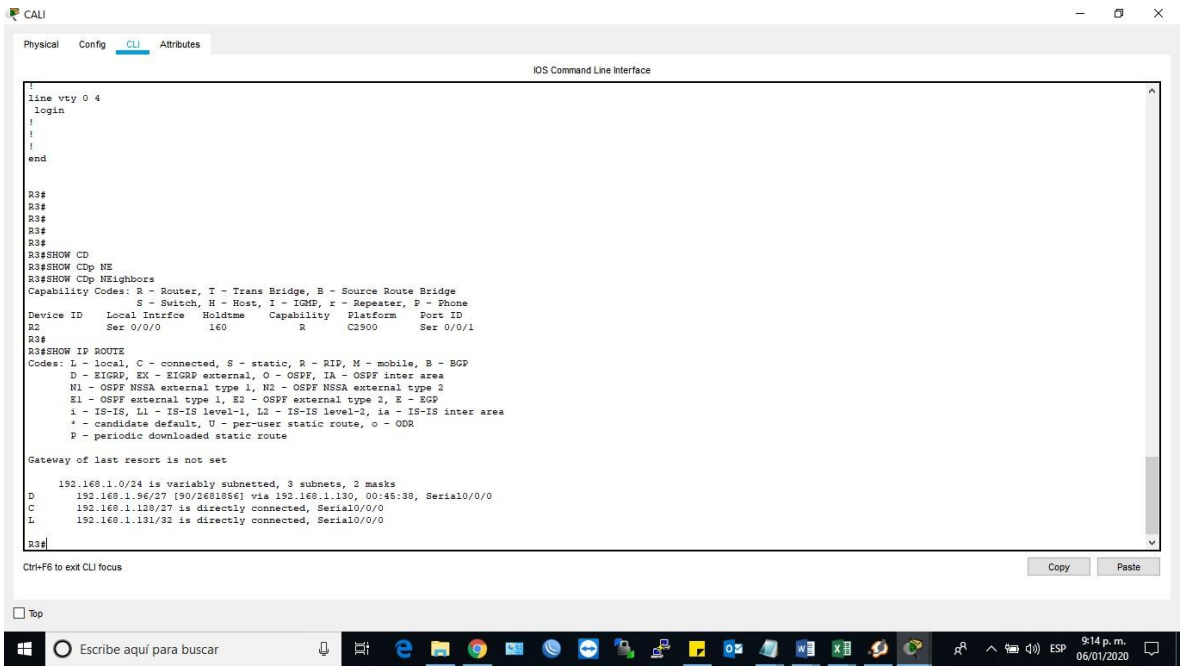
RUTAS ESTABLECIDAS EN MEDELLIN HACIA BOGOTA Y LA RED DE CALI.

R2_BOGOTA=



RUTAS ESTABLECIDAS EN BOGOTA HACIA MEDELLIN Y LA RED DE CALI.

R3_CALI =



RUTAS ESTABLECIDAS EN CALI HACIA BOGOTA Y LA RED DE MEDELLIN

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.

PRUEBAS DESDE UN EQUIPO DE LA RED DE CALI EL CUAL TIENE LA IP 192.168.1.66 REALIZA PING A UN ORDENADOR DE LA RED DE MEDELLIN EL CUAL TIENE LA IP 192.168.1.35.
PRUEBA EXITOSA.

C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::200:CFF:FE97:BED3
IP Address. .....: 192.168.1.66
Subnet Mask.....: 255.255.255.224
Default Gateway ..... : 192.168.1.65

Bluetooth Connection:
Link-local IPv6 Address.....: ::

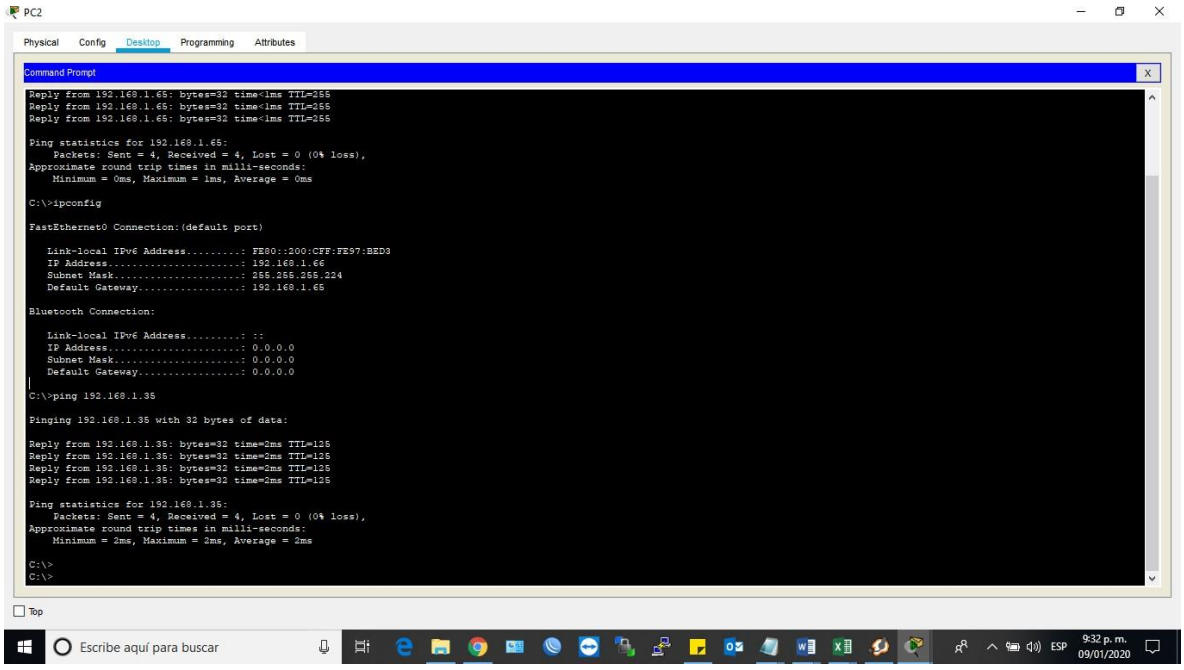
IP Address. .....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway ..... : 0.0.0.0

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168 1.35: bytes=32 time=2ms TTL=125
Reply from 192.168 1.35: bytes=32 time=2ms TTL=125
Reply from 192.168 1.35: bytes=32 time=2ms TTL=125
Reply from 192.168 1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>



EL SERVIDOR DE LA RED DE BOGOTA TIENE LA SIGUIENTE IP = 192.168 1.2/27

SE REALIZA PING DESDE EL MISMO ORDENADOR CON LA IP

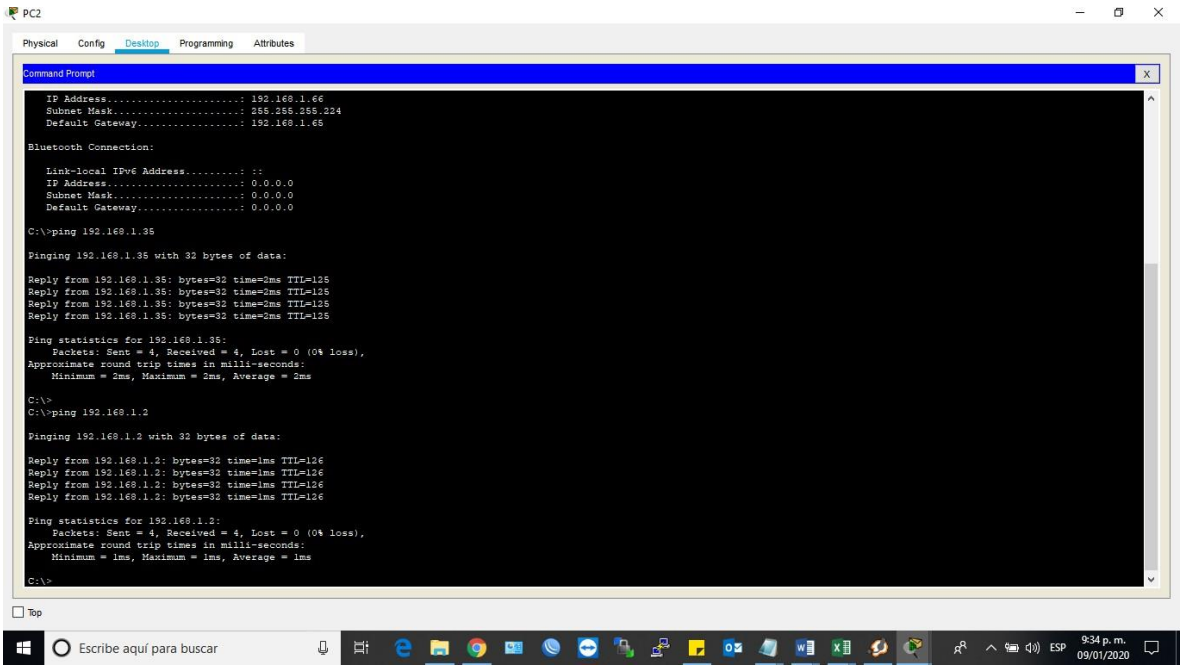
192.168.1.66/27(ordenador en Cali) HACIA 192.168.1.2/27(servidor en Bogotá)

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>



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.

Se configura en acceso a telnet con hasta 16 sesiones en simultaneo R1_MEDELLIN:

```
R1_medellin=
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 15
R1(config-line)#password 123456789
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Se configura en acceso a telnet con hasta 16 sesiones en simultaneo R2_BOGOTA:

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty
R2(config)#line vty 0 15
R2(config)#line vty 0 15
R2(config-line)#pass
R2(config-line)#password 123456789
R2(config-line)#login
R2(config-line)#exit
R2(config)#exit
```

Se configura en acceso a telnet con hasta 16 sesiones en simultaneo R3_CALI:

```
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line vt
R3(config)#line vty 0 15
R3(config-line)#password 123456789
R3(config-line)#login
R3(config-line)#exit
R3(config)#exit
```

Se configura el acl en r1_medellin=

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#acce
R1(config)#access-list 10 de
R1(config)#access-list 10 deny 192.168.1.64 0.0.0.31
R1(config)#inter gigabitEthernet 0/0
R1(config-if)#ip access-group 10 out
R1(config-if)#exit
R1(config)#access-list 11 permit host 192.168.1.2
R1(config)#interface g0/0
R1(config-if)#ip access-group 11 out
R1(config-if)#exit
R1(config)#
```

Se crea el Access list 10 donde se restringe la salida hacia cualquier equipo que no esté en su red.
Luego se crea el Access list 11 donde se indica que tiene acceso al host 192.168.1.2 el cual es el servidor de Bogotá.
Nota: los ACL se asocian a la interfaz g0/0 debido a que no se cuenta con fat 0/0 en este router, desde luego tambie porque ya están quedando obsoletas.

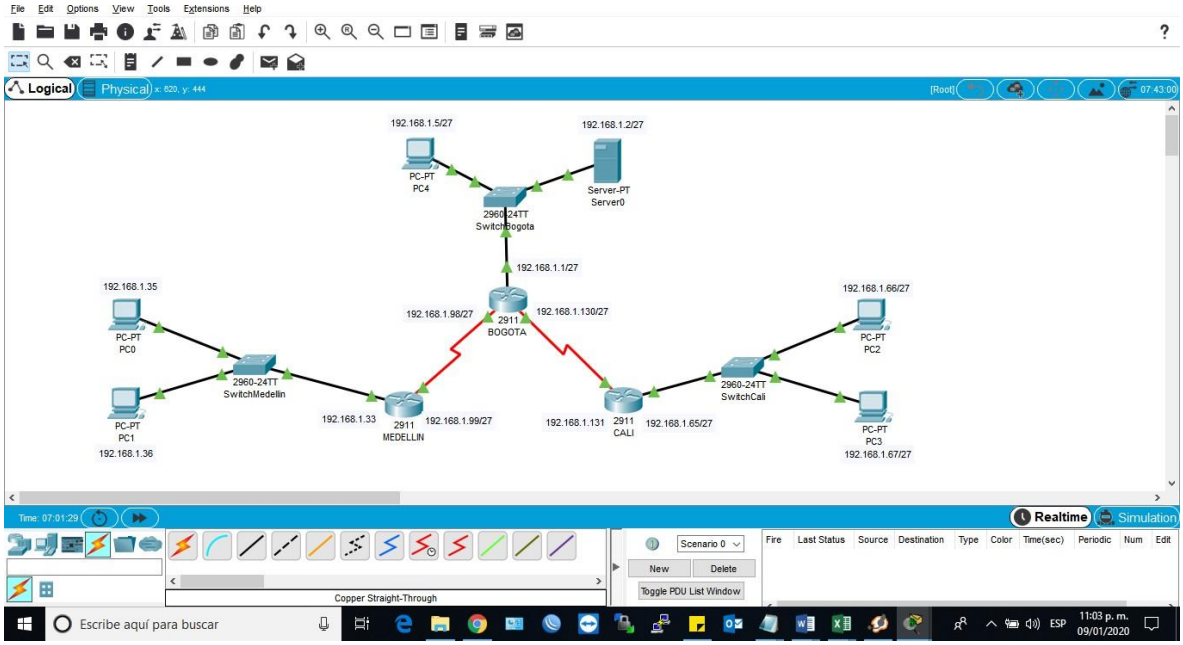
Se configura el acl en R3_cali=

```
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 12 deny 192.168.1.32 0.0.0.31
R3(config)#access-list 13 permit host 192.168.1.2
R3(config)#inter g0/0
R3(config-if)#ip access-group 12 out
R3(config-if)#ip access-group 13 out
R3(config-if)#exit
R3(config)#
```

Se crea el Access list 12 donde se restringe la salida hacia cualquier equipo que no esté en su red.
Luego se crea el Access list 13 donde se indica que tiene acceso al host 192.168.1.2 el cual es el servidor de Bogotá.
Nota: los ACL se asocian a la interfaz g0/0 debido a que no se cuenta con fat 0/0 en este router, desde luego tambie porque ya están quedando obsoletas.

De la siguiente manera solo el host 192.168.1.2 del que pertenece al segmento de red 192.168.0.0/27 puede accesar a todos los equipos de la red siendo este el server de administración.

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



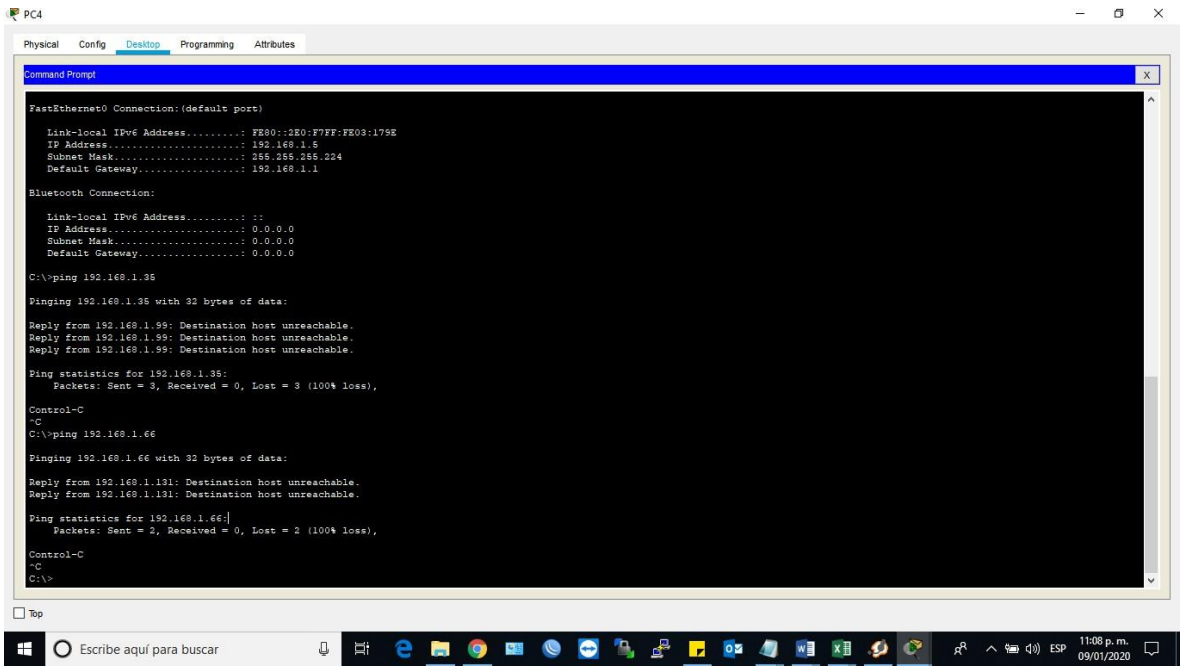
Se realiza ping hacia 2 host lan, uno de cali y otro de medellin y no se tiene respuesta desde el ws1 que pertenece a la subred de administración:

C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::2E0:F7FF:FE03:179E
IP Address. .....: 192.168.1.5
Subnet Mask.....: 255.255.255.224
Default Gateway ..... : 192.168.1.1
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address. .....: 0.0.0.0

Subnet Mask.....: 0.0.0.0
Default Gateway ..... : 0.0.0.0

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.99: Destination host unreachable.
Reply from 192.168.1.99: Destination host unreachable.
Reply from 192.168.1.99: Destination host unreachable.
Ping statistics for 192.168.1.35:
Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.
Ping statistics for 192.168.1.66:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C



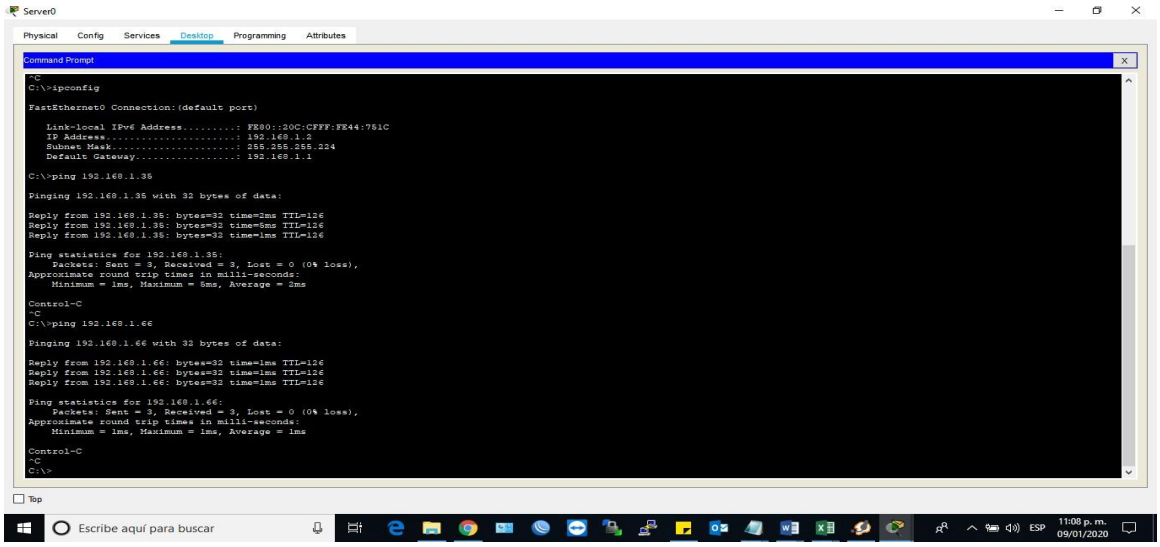
Pero si se realiza desde el servidor si se tiene una respuesta hacia los mismos equipos=

C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::20C:CFFF:FE44:751C
IP Address. .....: 192.168.1.2
Subnet Mask.....: 255.255.255.224
Default Gateway ..... : 192.168.1.1

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168 1.35: bytes=32 time=2ms TTL=126
Reply from 192.168 1.35: bytes=32 time=5ms TTL=126
Reply from 192.168 1.35: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.35:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms

Control-C

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168 1.66: bytes=32 time=1ms TTL=126
Reply from 192.168 1.66: bytes=32 time=1ms TTL=126
Reply from 192.168 1.66: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.66:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C



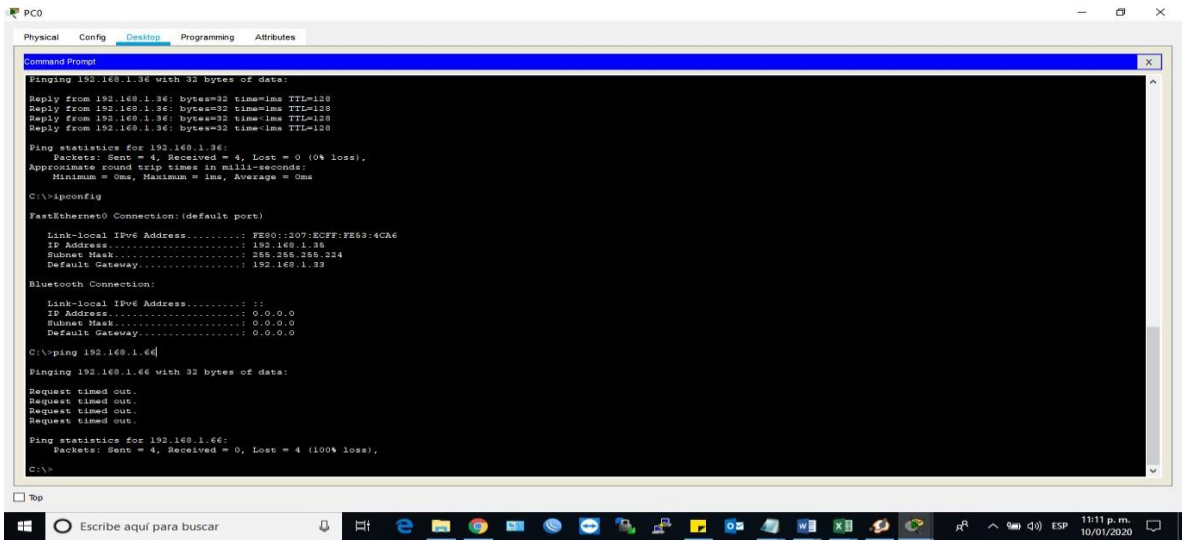
c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Desde la lan medellin no se tiene acceso a la lan de cali

C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::207:ECFF:FE53:4CA6
IP Address. .....: 192.168.1.35
Subnet Mask.....: 255.255.255.224
Default Gateway ..... : 192.168.1.33
Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address. .....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway ..... : 0.0.0.0

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

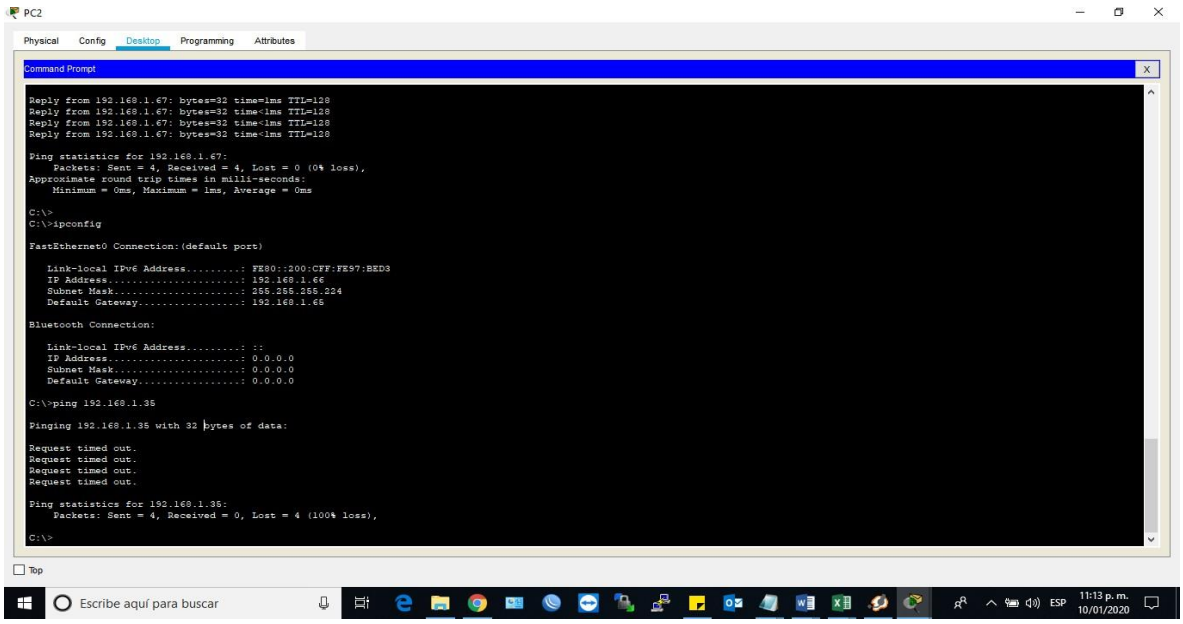


Desde la lan Cali no se tiene acceso a la lan de Medellín

C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::200:CFF:FE97:BED3
IP Address. .....: 192.168.1.66
Subnet Mask.....: 255.255.255.224
Default Gateway .....: 192.168.1.65
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address. .....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway ..... : 0.0.0.0

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>



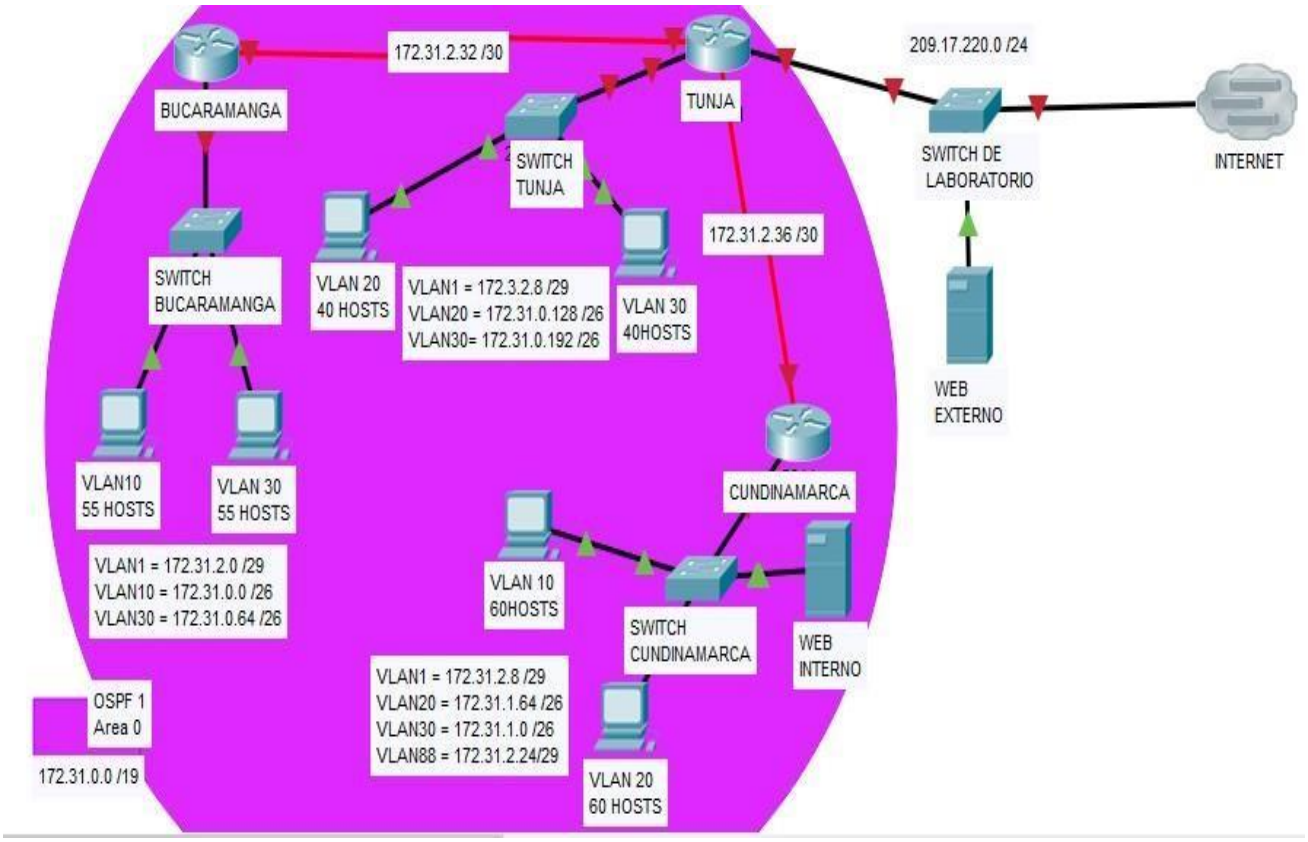
Parte 5: Comprobación de la red instalada.

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 e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Conexión correcta
	WS_1	Router BOGOTA	Conexión correcta
TELNET	Servidor	Router CALI	Conexión correcta
	Servidor	Router MEDELLIN	Conexión correcta
	LAN del Router MEDELLIN	Router CALI	TIEMPO AGOTADO
	LAN del Router CALI	Router CALI	Conexión correcta
PING	LAN del Router MEDELLIN	Router MEDELLIN	Conexión correcta
	LAN del Router CALI	Router MEDELLIN	TIEMPO AGOTADO
	LAN del Router CALI	WS_1	TIEMPO AGOTADO
	LAN del Router MEDELLIN	WS_1	TIEMPO AGOTADO
	LAN del Router MEDELLIN	LAN del Router CALI	TIEMPO AGOTADO
PING	LAN del Router CALI	Servidor	Conexión correcta
	LAN del Router MEDELLIN	Servidor	Conexión correcta
	Servidor	LAN del Router MEDELLIN	Conexión correcta
	Servidor	LAN del Router CALI	Conexión correcta
	Router CALI	LAN del Router MEDELLIN	TIEMPO AGOTADO
	Router MEDELLIN	LAN del Router CALI	TIEMPO AGOTADO

1.2. ESCENARIO 2

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



172.31.2.36

Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.

     Nombre a los host password las direcciónes a las interfaces seriales y los not-shutdown a las interfaces que conectan con los switches en capa 2. A RTUNJA – RBUCARAMANGA – RCUNDINAMARCA.

   - Autenticación local con AAA.

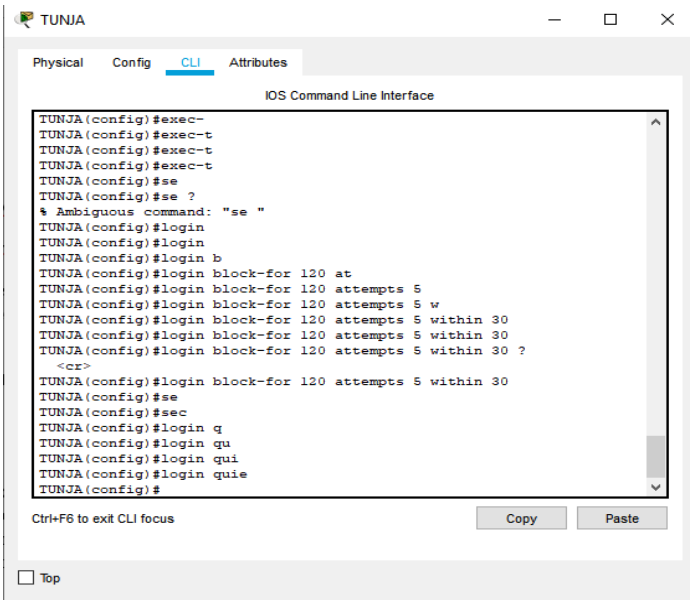
```
TUNJA(config)#aaa new-model
TUNJA(config)#username cisco password 123456789
TUNJA(config)#
    TUNJA#

  BUCARAMANGA(config)#aaa new-model
  BUCARAMANGA(config)#username cisco password 123456789
    BUCARAMANGA(config)#


  CUNDINAMARCA(config)#aaa new-model
  CUNDINAMARCA(config)#username cisco password 123456789
    CUNDINAMARCA(config)#
```

   - Cifrado de contraseñas.

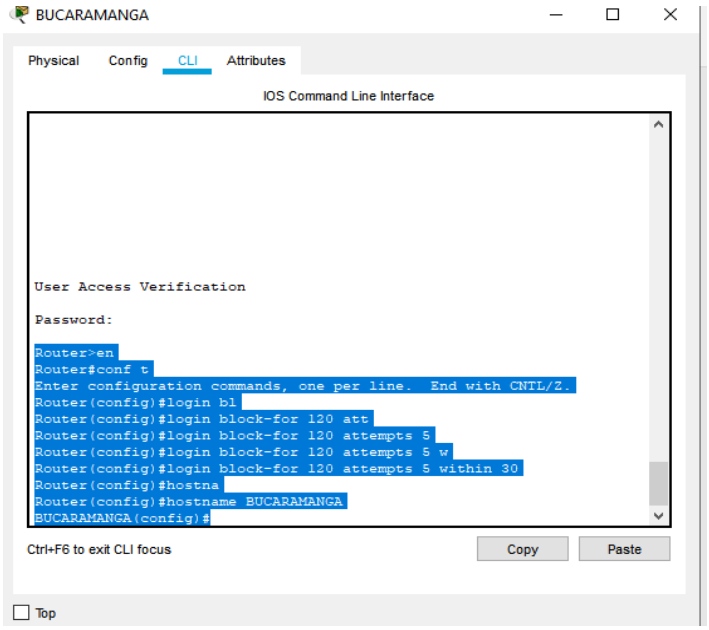
```
TUNJA(config)#service password-encryption
BUCARAMANGA(config)#SERVICE PAssword-encryption
CUNDINAMARCA(config)#service password-encryption
```

   - Un máximo de internos para acceder al router.

     TUNJA(config)#login block-for 120 attempts 5 within 30



Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#login block-for 120 attempts 5 within 30
Router(config)#hostna
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#



- Máximo tiempo de acceso al detectar ataques.

  TUNJA# configure terminal
  TUNJA(config)# line vty
  TUNJA(config-line)# no exec-timeout

CUNDINAMARCA# configure terminal
CUNDINAMARCA(config)# line vty
CUNDINAMARCA(config-line)# no exec-timeout

BUCARAMANGA# configure terminal
BUCARAMANGA(config)# line vty
BUCARAMANGA(config-line)# no exec-timeout

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

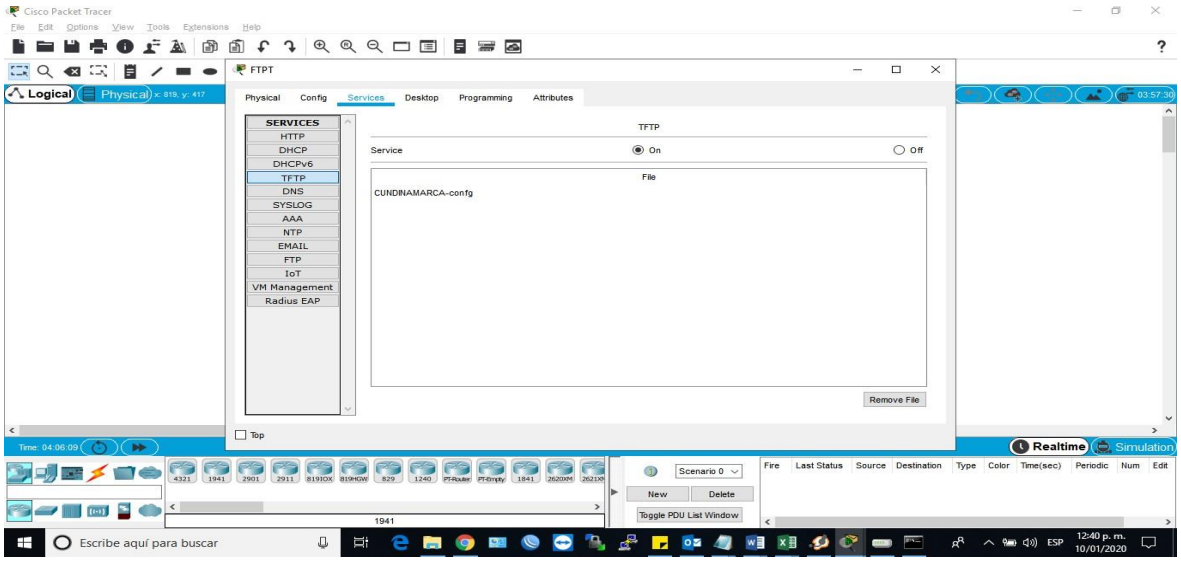
  Guardando archivo de configuración en servidor tftp configurado para la red de Cundinamarca.

  CUNDINAMARCA#copy running-config tftp: ?
  <cr>
  CUNDINAMARCA#copy running-config tftp:
  Address or name of remote host []? 172.31.2.10
  Destination filename [CUNDINAMARCA-confg]?

  Writing running-config...!!
  [OK - 1185 bytes]

  1185 bytes copied in 0.018 secs (65833 bytes/sec)
  CUNDINAMARCA#

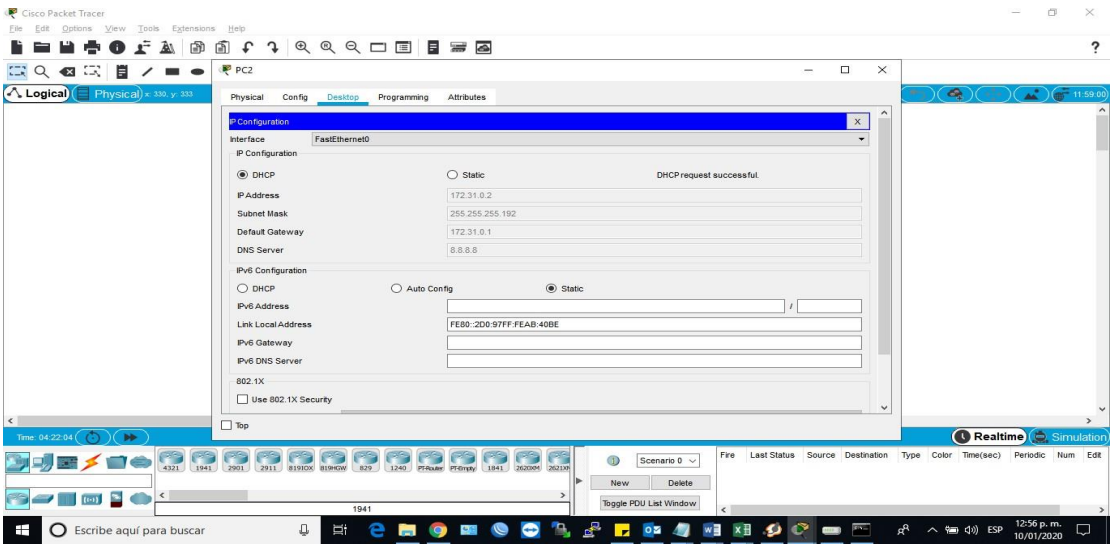
Evidencia de guardo en el equipo:



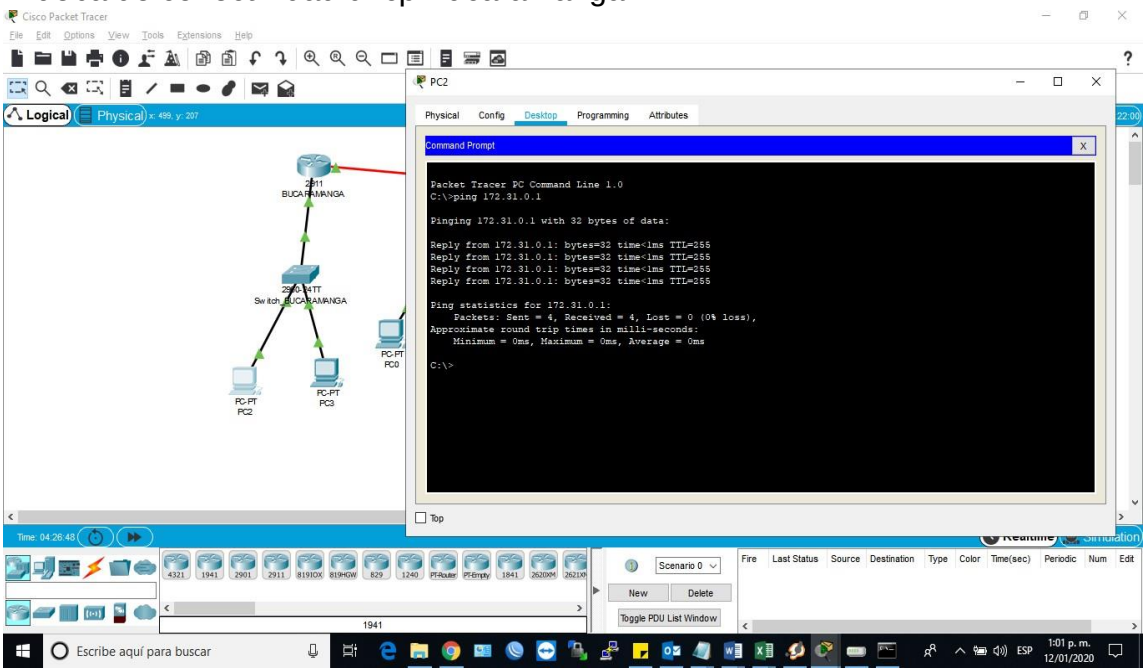
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

Switch_BUCARAMANGA(config)#IP DHcp POol VLAN10
Switch_BUCARAMANGA (dhcp-config)#NEtwork 172.31.0.0 255.255.255.192
Switch_BUCARAMANGA (dhcp-config)#DEFAult-router 172.31.0.1
Switch_BUCARAMANGA (dhcp-config)#DNS-server 8.8.8.8
Switch_BUCARAMANGA (dhcp-config)#EXIT

APRENDIENDO IP POR DHCP EVIDENCIA Y APRENDIENDO DINAMICAMENTE EL GATEWAY VLAN 10 SEGÚN TOPOLOGIA:



Prueba de conectividad dhcp Bucaramanga:

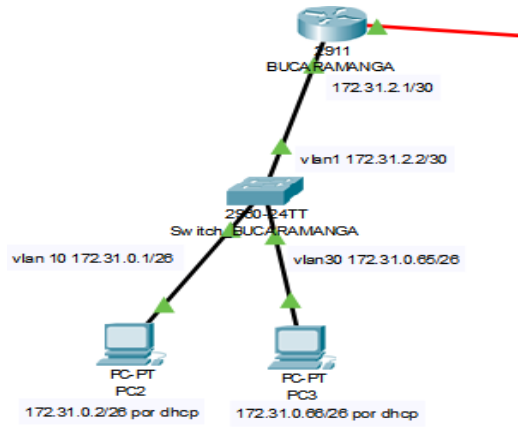


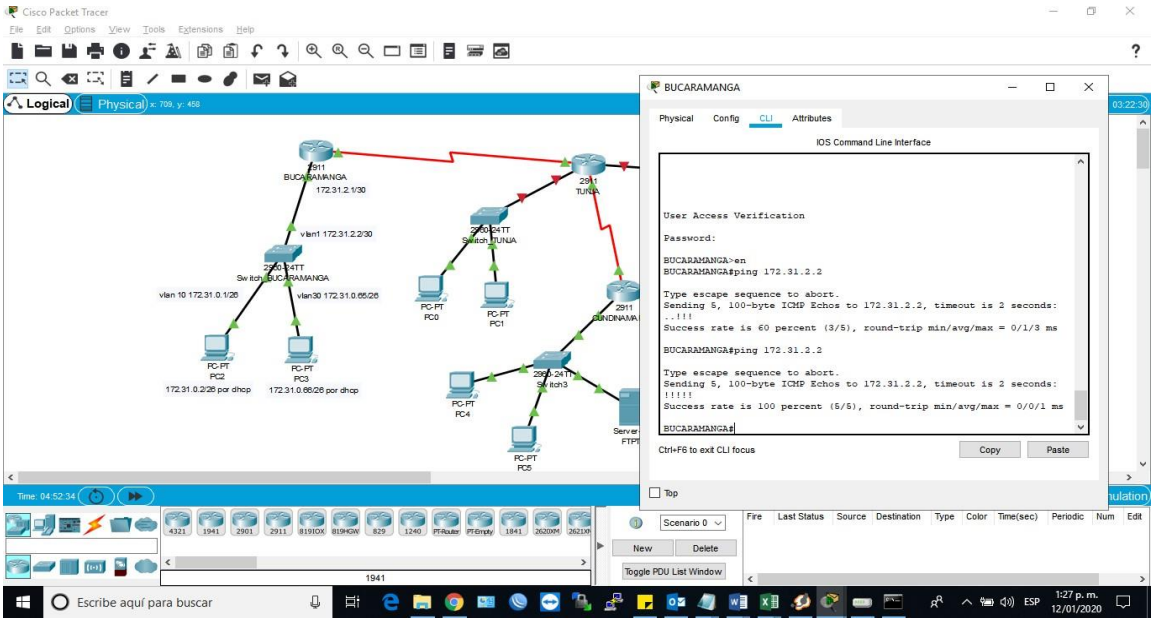
Tiempo de respuestas excelente 1 ms.

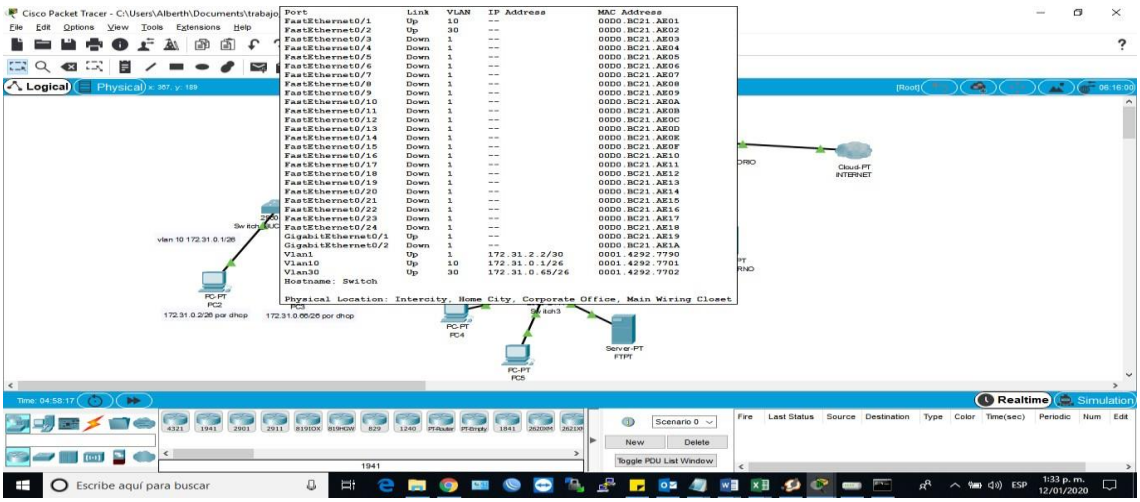
Pruebas desde router Bucaramanga hacia el switch Bucaramanga con la ip que tiene asociada en la vlan 1 de gestión:

BUCARAMANGA#ping 172.31.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
BUCARAMANGA#


2911
BUCARAMANGA
172.31.2.1/30
vlan1 172.31.2.2/30
2960-24TT
Switch BUCARAMANGA
vlan 10 172.31.0.1/26
vlan30 172.31.0.65/26
PC-PT
PC2
172.31.0.2/26 por dhcp
PC-PT
PC3
172.31.0.66/26 por dhcp

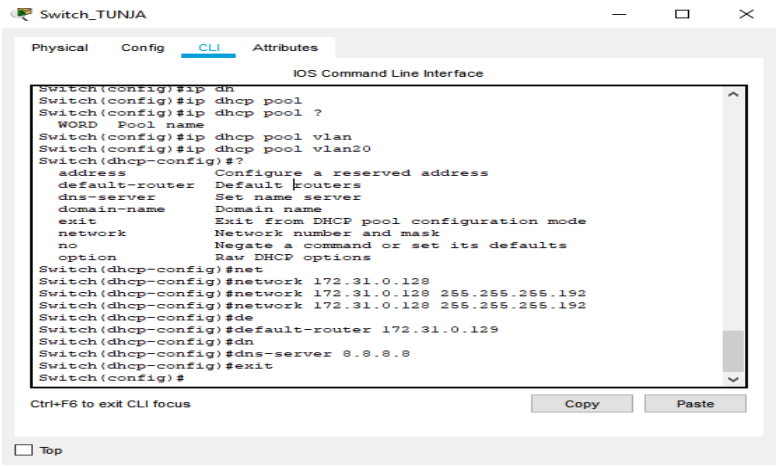

Cisco Packet Tracer
BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Password:
BUCARAMANGA>en
BUCARAMANGA#ping 172.31.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/1/3 ms
BUCARAMANGA#ping 172.31.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
BUCARAMANGA#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Logical
Physical
Escribe aquí para buscar


Cisco Packet Tracer - C:\Users\Alberth\Documents\trabajo
Port Link VLAN IP Address MAC Address
FastEthernet0/1 Up 10 -- 00D0.BC21.AE01
FastEthernet0/2 Up 30 -- 00D0.BC21.AE02
FastEthernet0/3 Down 1 -- 00D0.BC21.AE03
FastEthernet0/4 Down 1 -- 00D0.BC21.AE04
FastEthernet0/5 Down 1 -- 00D0.BC21.AE05
FastEthernet0/6 Down 1 -- 00D0.BC21.AE06
FastEthernet0/7 Down 1 -- 00D0.BC21.AE07
FastEthernet0/8 Down 1 -- 00D0.BC21.AE08
FastEthernet0/9 Down 1 -- 00D0.BC21.AE09
FastEthernet0/10 Down 1 -- 00D0.BC21.AE0A
FastEthernet0/11 Down 1 -- 00D0.BC21.AE0B
FastEthernet0/12 Down 1 -- 00D0.BC21.AE0C
FastEthernet0/13 Down 1 -- 00D0.BC21.AE0D
FastEthernet0/14 Down 1 -- 00D0.BC21.AE0E
FastEthernet0/15 Down 1 -- 00D0.BC21.AE0F
FastEthernet0/16 Down 1 -- 00D0.BC21.AE10
FastEthernet0/17 Down 1 -- 00D0.BC21.AE11
FastEthernet0/18 Down 1 -- 00D0.BC21.AE12
FastEthernet0/19 Down 1 -- 00D0.BC21.AE13
FastEthernet0/20 Down 1 -- 00D0.BC21.AE14
FastEthernet0/21 Down 1 -- 00D0.BC21.AE15
FastEthernet0/22 Down 1 -- 00D0.BC21.AE16
FastEthernet0/23 Down 1 -- 00D0.BC21.AE17
FastEthernet0/24 Down 1 -- 00D0.BC21.AE18
GigabitEthernet0/1 Up 1 -- 00D0.BC21.AE19
GigabitEthernet0/2 Down 1 -- 00D0.BC21.AE1A
Vlan1 Up 1 172.31.2.2/30 0001.4292.7790
Vlan10 Up 10 172.31.0.1/26 0001.4292.7701
Vlan30 Up 30 172.31.0.65/26 0001.4292.7702
Hostname: Switch
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Cloud-PT
INTERNET
Server-PT
FTPT
Realtime
Simulation
Escribe aquí para buscar

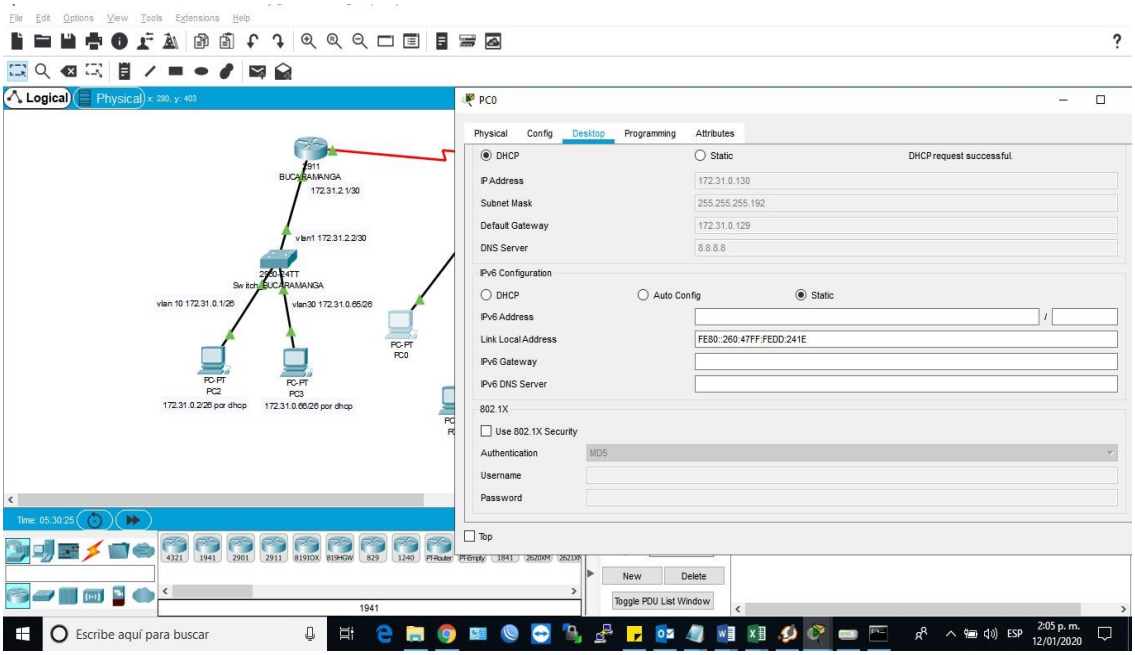
Visualización de las interfaces virtuales asociadas a los direccionamientos correspondientes según topología.

Vlan_20 tunja

```
Switch(config-if)#ip add
Switch(config-if)#ip address 172.31.0.128 255.255.255.192
Bad mask /26 for address 172.31.0.128
Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#dhc
Switch(config)#ip dh
Switch(config)#ip dhcp pool
Switch(config)#ip dhcp pool ?
WORD Pool name
Switch(config)#ip dhcp pool vlan
Switch(config)#ip dhcp pool vlan20
Switch(dhcp-config)#?
address Configure a reserved address
default-router Default routers
dns-server Set name server
domain-name Domain name
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
option Raw DHCP options
Switch(dhcp-config)#net
Switch(dhcp-config)#network 172.31.0.128
Switch(dhcp-config)#network 172.31.0.128 255.255.255.192
Switch(dhcp-config)#network 172.31.0.128 255.255.255.192
Switch(dhcp-config)#de
Switch(dhcp-config)#default-router 172.31.0.129
Switch(dhcp-config)#dn
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#exit
Switch(config)#
```



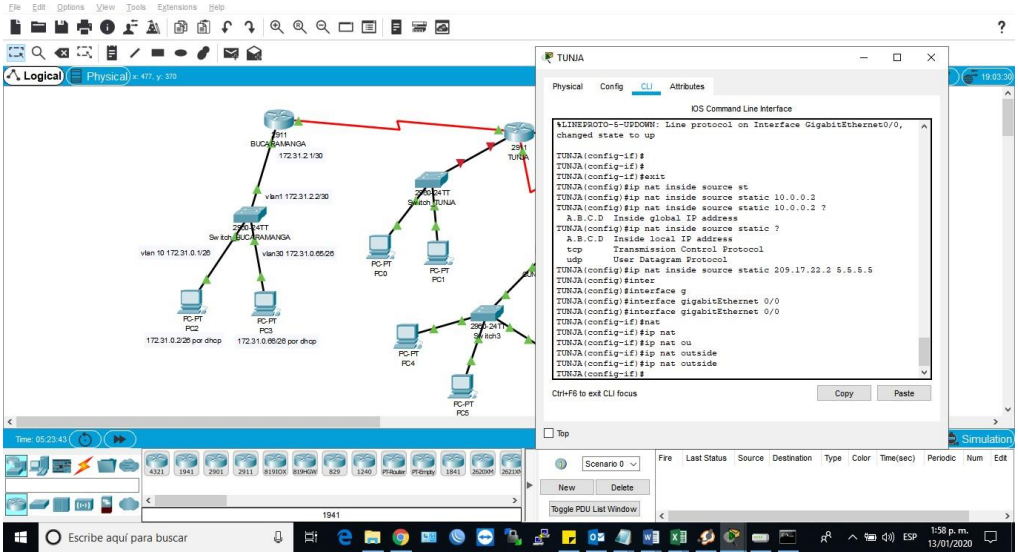
Pc en vlan 20 de tunja aprendido ip por dhcp:



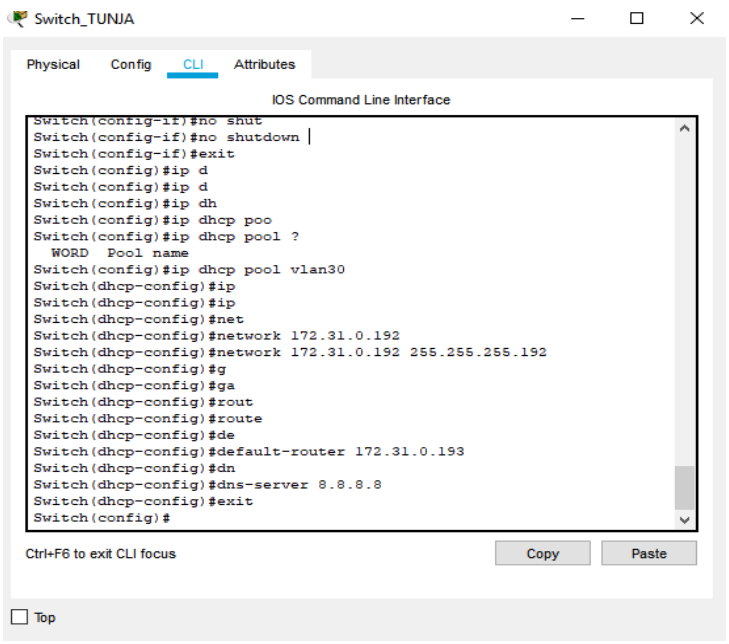
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

TUNJA(config)#ip nat inside source static 209.17.22.2 5.5.5.5
TUNJA(config)#inter
TUNJA(config)#interface g
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config-if)#nat
TUNJA(config-if)#ip nat

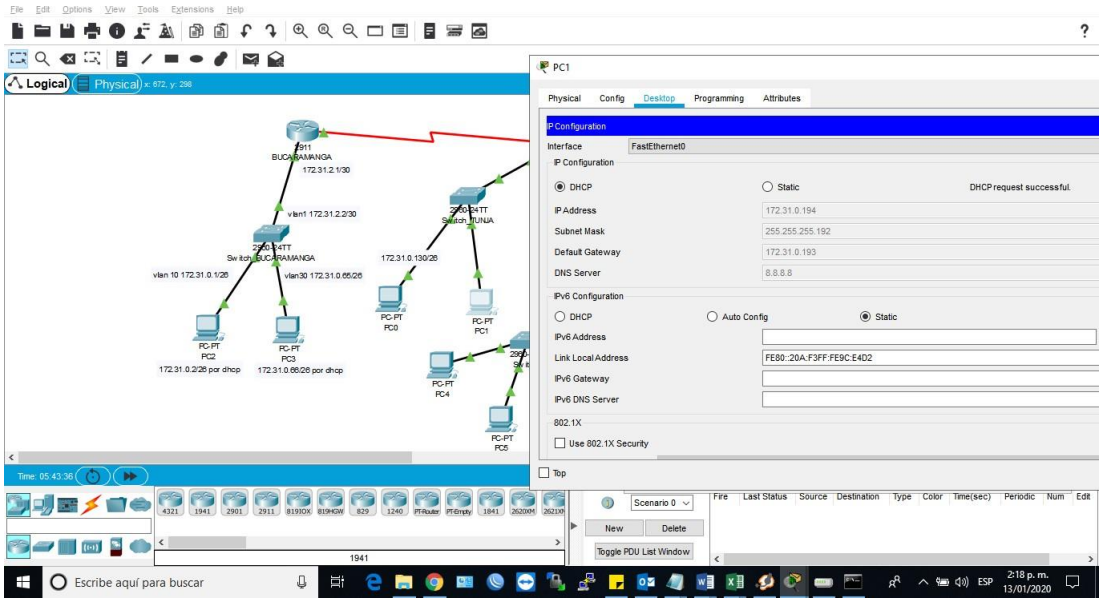
```
TUNJA(config-if)#ip nat ou
TUNJA(config-if)#ip nat outside
    TUNJA(config-if)#ip nat outside
```




```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface vlan 30
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to
up

Switch(config-if)#ip address 172.31.0.193 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip dhcp pool ?
WORD Pool name
Switch(config)#ip dhcp pool vlan30
Switch(dhcp-config)#network 172.31.0.192
Switch(dhcp-config)#network 172.31.0.192 255.255.255.192
Switch(dhcp-config)#default-router 172.31.0.193
Switch(dhcp-config)#dn
Switch(dhcp-config)#dns-server 8.8.8.8
Switch(dhcp-config)#exit
Switch(config)#
```

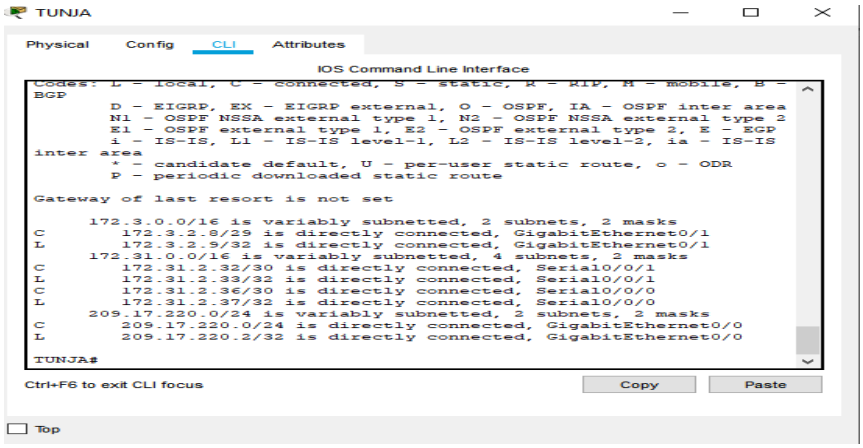


Equipo que está en la interfaz asociada a la vlan 30 aprende ip por dhcp.



4. El enrutamiento deberá tener autenticación.

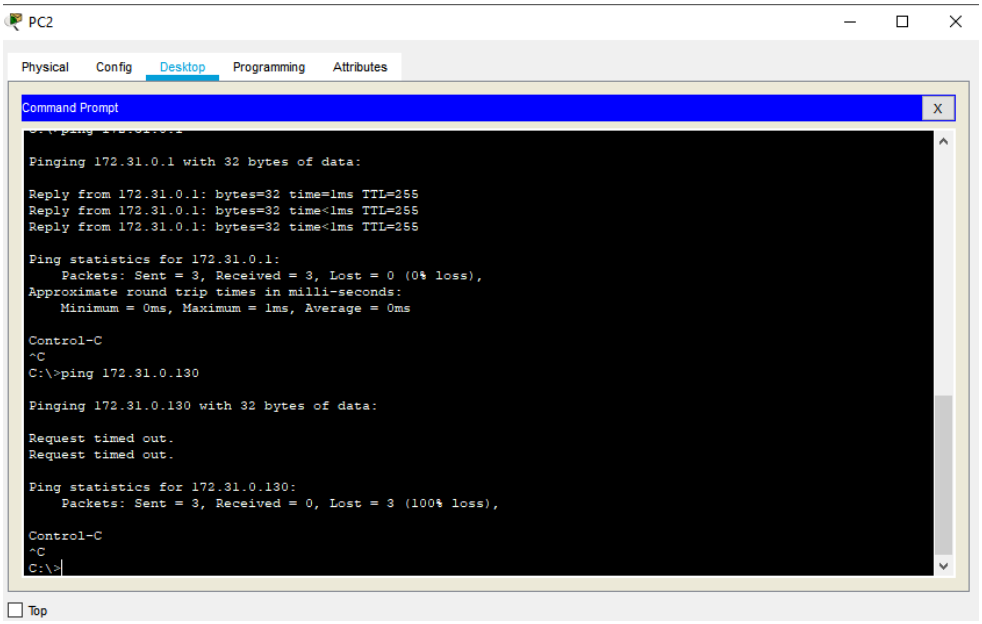
```
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
Gateway of last resort is not set
172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.3.2.8/29 is directly connected, GigabitEthernet0/1
L 172.3.2.9/32 is directly connected, GigabitEthernet0/1
172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.31.2.32/30 is directly connected, Serial0/0/1
L 172.31.2.33/32 is directly connected, Serial0/0/1
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.37/32 is directly connected, Serial0/0/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/24 is directly connected, GigabitEthernet0/0
L 209.17.220.2/32 is directly connected, GigabitEthernet0/0
```



5. Listas de control de acceso:
   - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
   - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja
   - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
   - Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
   - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

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



RECOMENDACIONES

- **NOTA**: el primer ping es fallido, porque apenas el router ingresa a la mac y el direccionamiento en capa 3 de la tabla art, luego de esto ya no hay ninguna perdida, todo llega correctamente en cada uno de los escenarios simulados en packet tracer.

- **NOTA:** todas las contraseñas de acceso para los escenarios en consola telnet, son:

123456789

  - Habilitar VLAN en cada switch y permitir su enrutamiento. =ok
  - Enrutamiento OSPF con autenticación en cada router. = ok
  - Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca. = ok
  - Configuración de NAT estático y de sobrecarga. = ok
  - Establecer una lista de control de acceso de acuerdo con los criterios señalados. =ok
  - Habilitar las opciones en puerto consola y terminal virtual= ok

CONCLUSIONES

El objetivo final de esta actividad fue apropiar y alcanzar los conceptos y tecnologías básicos de red. El material me ayudo a desarrollar aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones. Las habilidades específicas desarrolladas en mi conocimiento para la actividad se describían en la solución dada a cada uno de las Topologías y todas las tareas propuestas. Como finalidad a la realización de los Principios Básicos de Routing y Switching de CCNA. Tal como indicó el desarrollo de la Prueba de habilidades prácticas CCNA, esta Práctica se centró en el aprendizaje de la arquitectura, los componentes y el funcionamiento de los routers y switches en una red. En esta actividad, aprendimos las habilidades prácticas y conceptuales que constituyen la base para entender lo básico de las redes en relación a routers y switches. Para lo cual se utilizó el Packet Tracer simulando los ambientes prácticos del día a día. Además:

Configuré las operaciones básicas de una red conmutada pequeña y resolví problemas relacionados. Describí las tecnologías de switching mejoradas, como las VLAN, el protocolo de enlace troncal de VLAN (VTP), se configuró y verifico el routing estático y el routing predeterminado. También se configuró VLAN y el routing entre VLAN, y se resolvieron problemas relacionados. Así como la configuración y control de ACL para IPv4 e IPv6.

BIBLIOGRAFIA

- **Temática: Exploración de la red,** CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1
- **Temática: Configuración de un sistema operativo de red,** CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1
- **Temática: Protocolos y comunicaciones de red,** CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1
- Todaa la información virtual del curso CISCO. netacad, VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1
- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live
- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU

- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf

- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU