DESARROLLO DE LA PRÁCTICA FINAL DIPLOMADO Y PROFUNDIZACIÓN – CISCO DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN

ROGER GARIBELLO MARTÍNEZ

EFRAÍN ALEJANDRO PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ – CUNDINAMARCA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 27 de enero de 2020

DEDICATORIA

De ante mano agradezco a toda la parte educativa y operacional de la Universidad Nacional Abierta y a Distancia “UNAD”, por haber brindado las herramientas tecnológicas y haber brindado el acompañamiento en todos los contenidos programáticos y así poder brindar el servicio estudiantil en aras de la superación personal de muchos aspirantes a ser profesionales.

AGRADECIMIENTOS

De ante mano agradezco a toda la parte educativa y operacional de la Universidad Nacional Abierta y a Distancia “UNAD”, por haber brindado las herramientas tecnológicas y haber brindado el acompañamiento en todos los contenidos programáticos y así poder brindar el servicio estudiantil en aras de la superación personal de muchos aspirantes a ser profesionales.

TABLA DE CONTENIDO

Pág.

INTRODUCCIÓN 8
JUSTIFICACIÓN 9
OBJETIVOS 10
PROPUESTA ESCENARIO 1 11
SOLUCIÓN DE LOS ESCENARIOS 13
ESCENARIO 1 13
ESCENARIO 2 53
CONCLUSIONES 70
BIBLIOGRAFIA 70

LISTA DE FIGURAS

Figura 1. Escenario numero 1 16
Figura 2. Escenario simulado numero 1 17
Figura 3. Tabla de enrutamiento 28
Figura 4. Tabla de enrutamiento R2 29
Figura 5. Diagnóstico de vecinos R1 32
Figura 6. Diagnóstico de vecinos R2 33
Figura 7. Diagnóstico de vecinos R3 34
Figura 8. Evidencia ping desde R1 Medellín 36
Figura 9. Evidencia ping desde R2 Bogotá 37
Figura 10. Evidencia ping desde R3 Cali 39
Figura 11. Evidencia que tiene como vecino a R2 Bogotá 42
Figura 12. Evidencia que tiene como vecino a R1 y a R3 43
Figura 13. Evidencia que tiene como vecino a R2 Bogotá 44
Figura 14. Tablas de enrutamiento 44
Figura 15. Tablas de enrutamiento Medellín hacia Bogotá 45
Figura 16. Tablas de enrutamiento Bogotá hacia Medellín y la red de Cali 46
Figura 17. Evidencia ping 47
Figura 18. Evidencia ping 48
Figura 19. Direccionamiento topología 51
Figura 20. Evidencia ping 53
Figura 21. Evidencia ping 54
Figura 22. Configuración tarjeta de red 55
Figura 23. Evidencia ping 57
Figura 24. Topología escenario 2 58
Figura 25. Simulación Topología escenario 2
Figura 26. Configuración seguridad 60
Figura 27. Configuración seguridad 61
Figura 28. Evidencia de guardo en el equipo 63
Figura 29. Gateway dinámico 64
Figura 30. Prueba de conectividad DHCP Bucaramanga 64
Figura 31. Direccionamiento 65
Figura 32. Evidencia ping 66
Figura 33. Interfaces virtuales. 66
Figura 34. Rutas aprendidas… 68
Figura 35. Evidencia DHCP 69
Figura 36. NAT estático 70
Figura 37. DHCP tomado 72
Figura 38. Tabla de enrutamiento 73
Figura 39. Evidencia ping

GLOSARIO

ARP: (Address Resolution Protocol, protocolo de resolución de direccione) Un protocolo que proporciona asignación dinámica entre las direcciones IP y las direcciones Ethernet. ARP sólo se utiliza con redes IPv4. Las redes IPv6 utilizan el protocolo ND (Neighbor Discovery) para convertir direcciones de protocolo. Para obtener más información, consulte RFC 826.

BYTE: Una unidad de datos que suele ser de ocho bits.

DHCP: Protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor.

DIRECCIÓN IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

DNS: Domain name system, sistema de nombre de dominio Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio y los nombres del equipo para direcciones fuera de la empresa, como las de Internet.

ETHERNET: Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

FIBRA: Medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos.

GATEWAY: Equipos para interconectar redes.

HTTP: Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

MASCARA DE RED: Código de dirección que determina el tamaño de la red.

MULTIFUSIÓN: Envío de datos a un grupo de destinos a la vez.

PING: Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

INTRODUCCIÓN

El presente trabajo contiene la evidencia de la solución del ejercicio de escenarios propuestos en el diplomado de profundización CISCO, donde se plasma el conocimiento teórico y práctico de los módulos estudiados CCNA1 y CCNA2, donde se demuestran las habilidades adquiridas en el diplomado de profundización, desarrollando dos escenarios que plasman un ejercicio real de administración y configuración de redes.

JUSTIFICACIÓN

El diplomado de CISCO - Diseño e Implementación de Soluciones Integradas LAN / WAN, es una de las opciones de grado de la Universidad Nacional Abierta y a Distancia UNAD, ya que logra complementar y brindar herramientas de conocimiento en el área de administración de redes a los ingenieros de sistemas, comunicaciones o de carreras afines.

OBJETIVOS

Durante el desarrollo de los ejercicios solicitados se busca desarrollar habilidades prácticas y teóricos donde se garantice el conocimiento para la administración de Switch, Router y Servidores entre otros componentes que conforma una red computacional. El desarrollo de los escenarios propuestos busca también evidenciar los conocimientos en las técnicas adquiridas de la segmentación y configuración de los dispositivos en aras de garantizar la seguridad y la disponibilidad del servicio que se brindan al usuario final de la red.

PROPUESTA ESCENARIO 1

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

Topología de red
Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.
Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.
Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red. Parte 6: Configuración final.

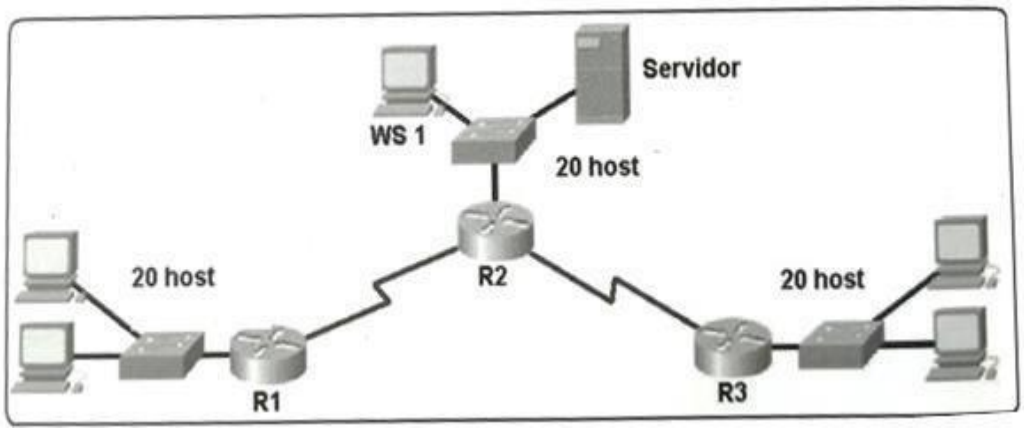

Figura 1. Escenario número 1

Como trabajo inicial se debe realizar lo siguiente.

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

SOLUCIÓN DE LOS ESCENARIOS

ESCENARIO 1

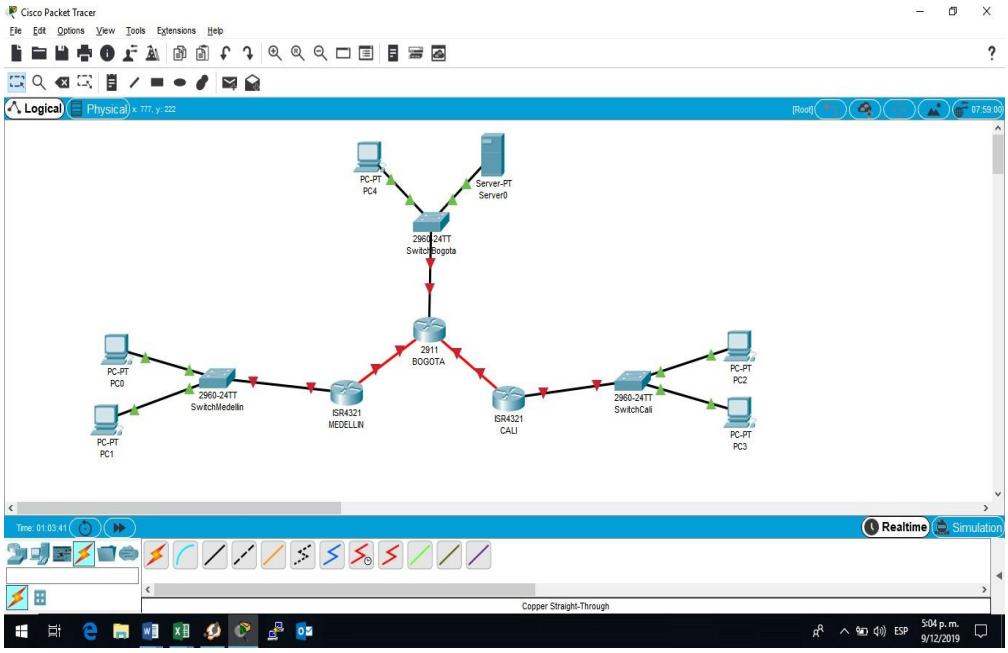

Figura 2. Escenario simulado número 1

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.

Respuesta. Tomará la siguiente mascara /27 = 255.255.255.224

Subneteo de la red 192.168.1.0

	DIRECCIÓN DE RED	**CIDR**	**MASCARA**	**GATEWAY**	**PRIMERA IP DISPONIBLE**	**ULTIMA IP DISPONIBLE**	**BROADCAST**
Red 1	192.168.1.0	27	255.255.255.224	192.168.1.1	192.168.1.2	192.168.1.30	192.168.1.31
Red 2	192.168.1.32	27	255.255.255.224	192.168.1.33	192.168.1.34	192.168.1.62	192.168.1.63

Red 3	192.168.1.64	27	255.255.255.224	192.168.1.65	192.168.1.66	192.168.1.94	192.168.1.95
Red 4	192.168.1.96	27	255.255.255.224	192.168.1.97	192.168.1.98	192.168.1.126	192.168.1.127
Red 5	192.168.1.128	27	255.255.255.224	192.168.1.129	192.168.1.130	192.168.1.158	192.168.1.159
Red 6	192.168.1.160	27	255.255.255.224	192.168.1.161	192.168.1.162	192.168.1.190	192.168.1.191
Red 7	192.168.1.192	27	255.255.255.224	192.168.1.193	192.168.1.194	192.168.1.222	192.168.1.223
Red 8	192.168.1.224	27	255.255.255.224	192.168.1.225	192.168.1.226	192.168.1.254	192.168.1.255

Configuración de seguridad para el Router Bogotá Medellin y Cali, con enable password, enable secret , contraseña al Puerto Auxiliar, Password para la Consola ,Password a Telnet , Banners y encriptación de passwords.

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#

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#

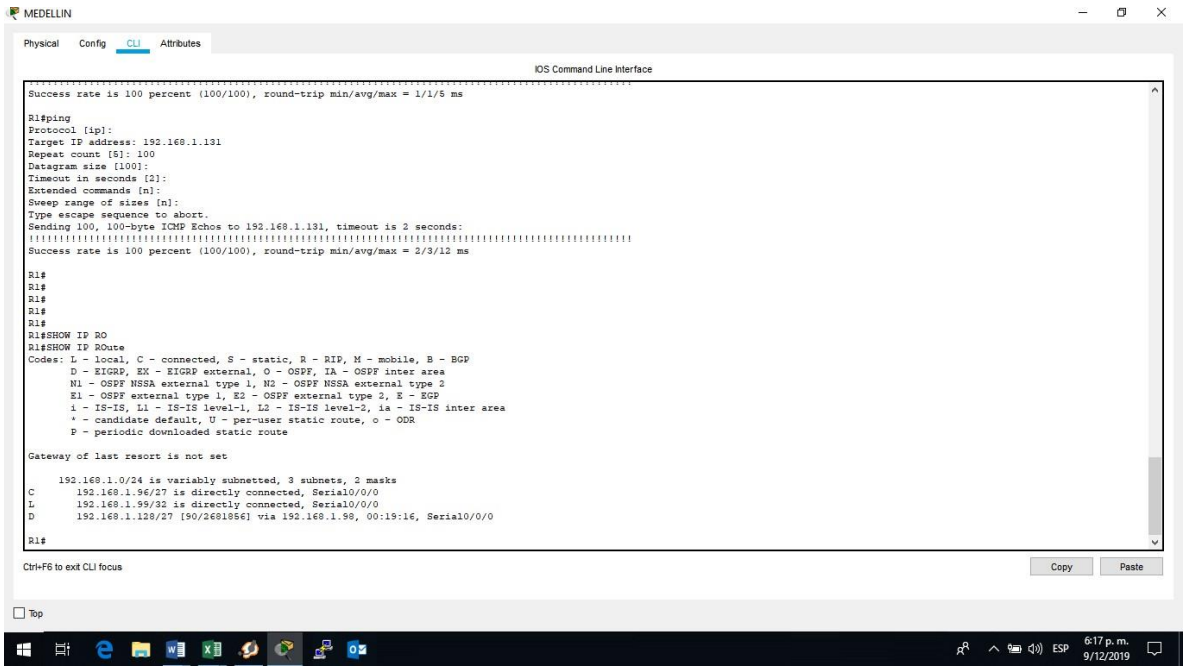

Figura 3. tabla de enrutamiento R1

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#

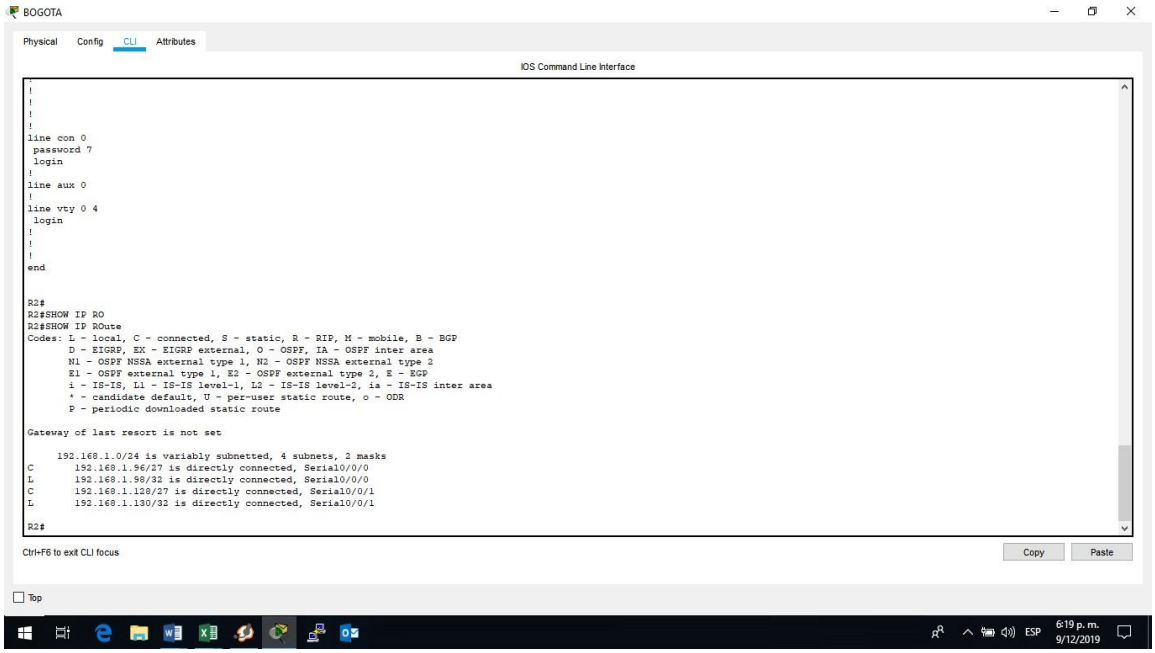

Figura 4. tabla de enrutamiento R2

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#

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#

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#

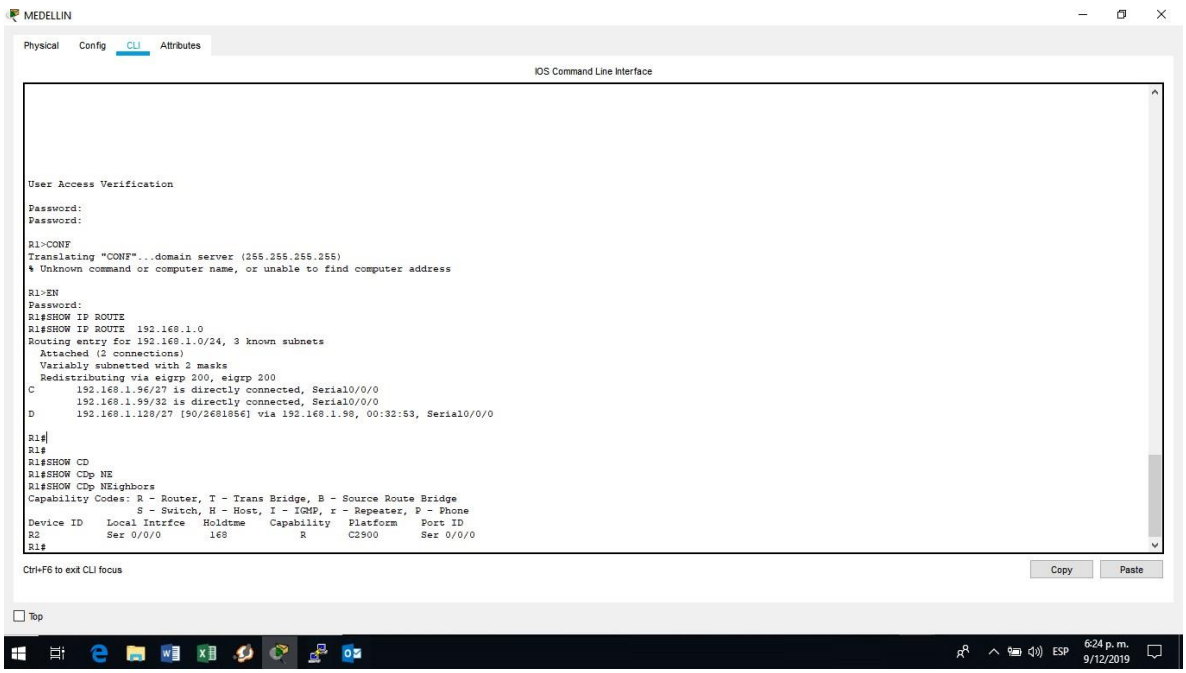

Figura 5. diagnóstico de vecinos R1

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#

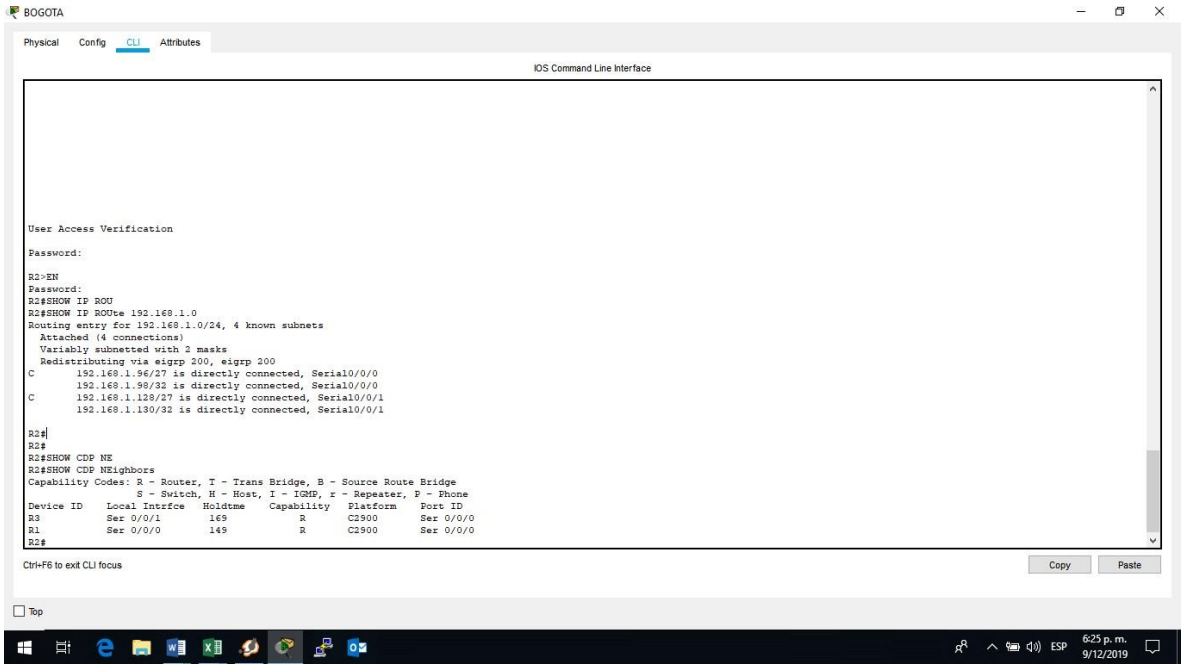

Figura 6. diagnóstico de vecinos R2

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#

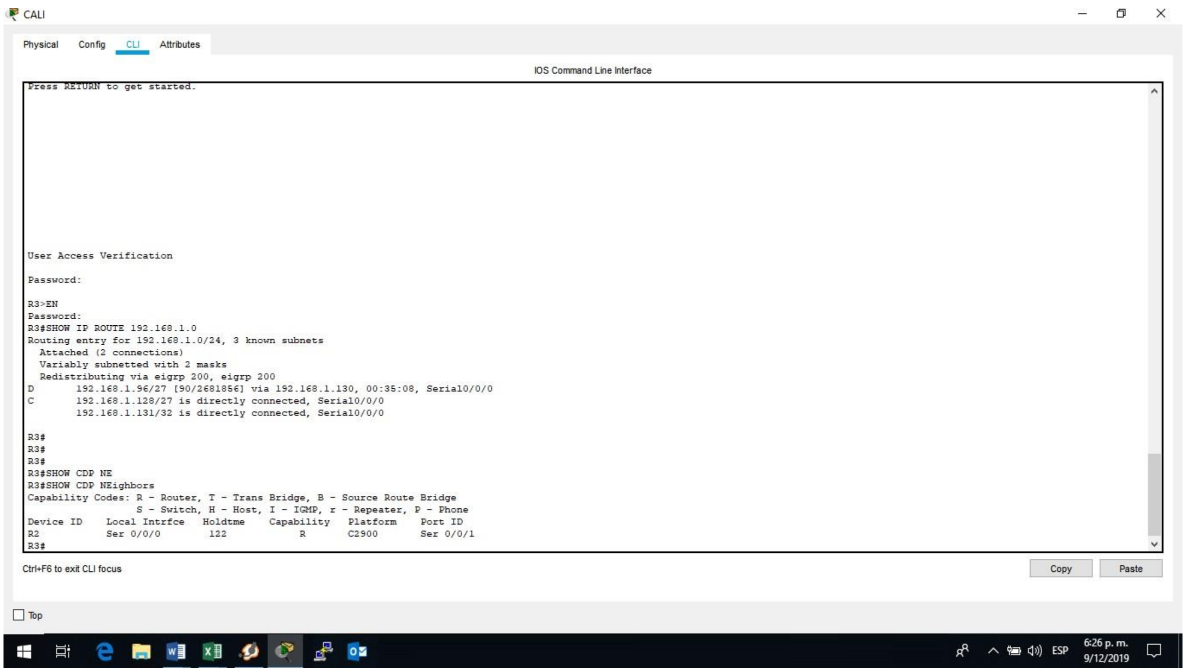

Figura 7. diagnóstico de vecinos R3

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
```

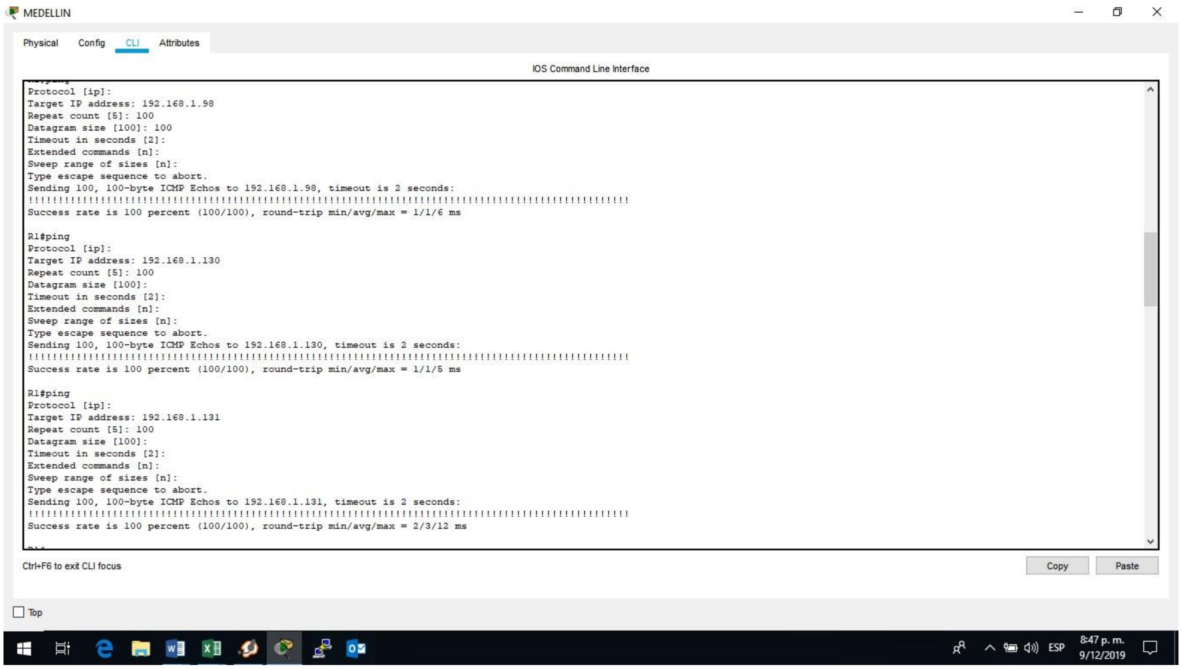

Figura 8. evidencia ping desde R1 Medellín

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

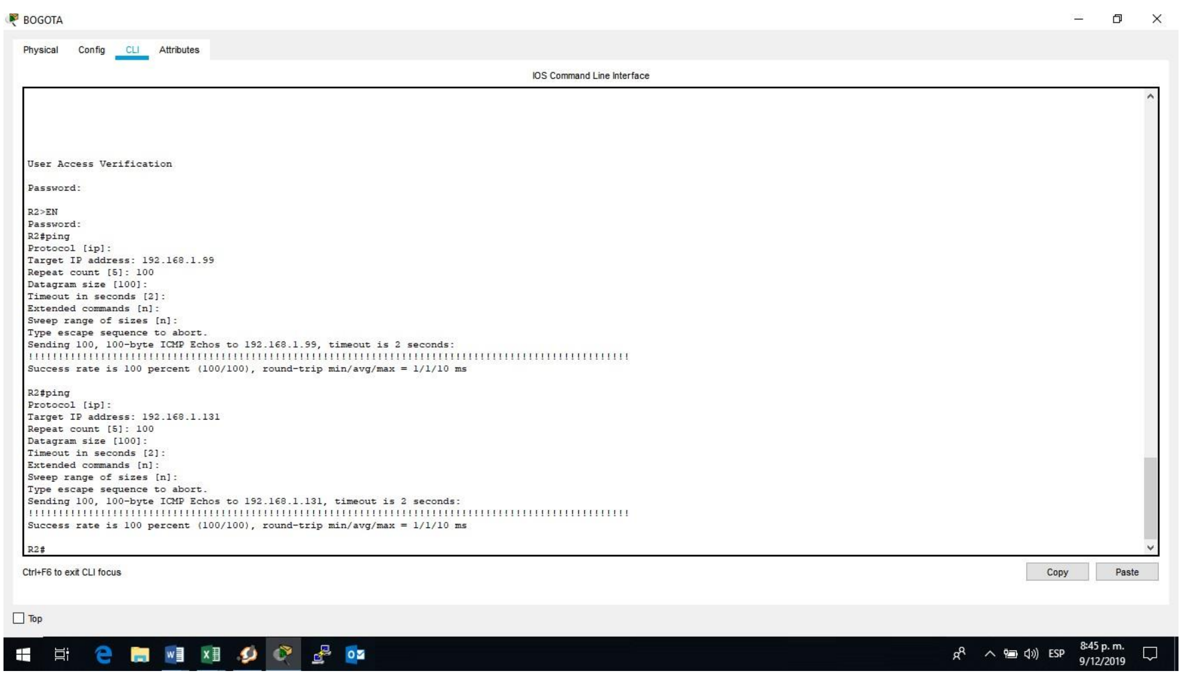

figura 9. *evidencia ping desde R2 Bogotá*

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

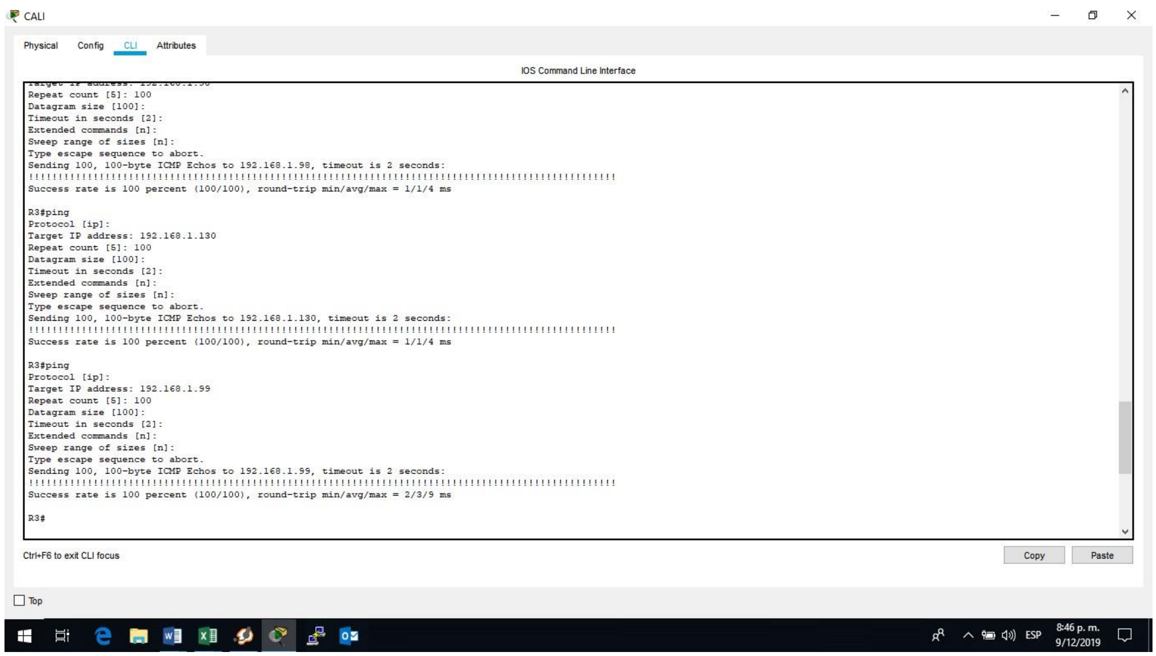

Figura 10. evidencia ping desde R3 Cali

Parte 3: Configuración de Enrutamiento.

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
!
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

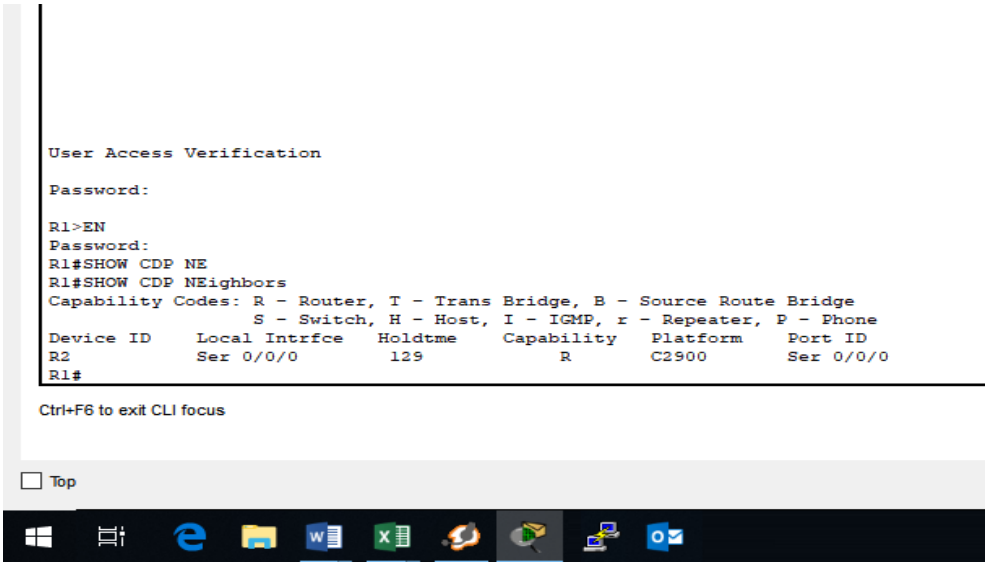

Figura 11. evidencia que tiene como vecino a R2 Bogotá

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

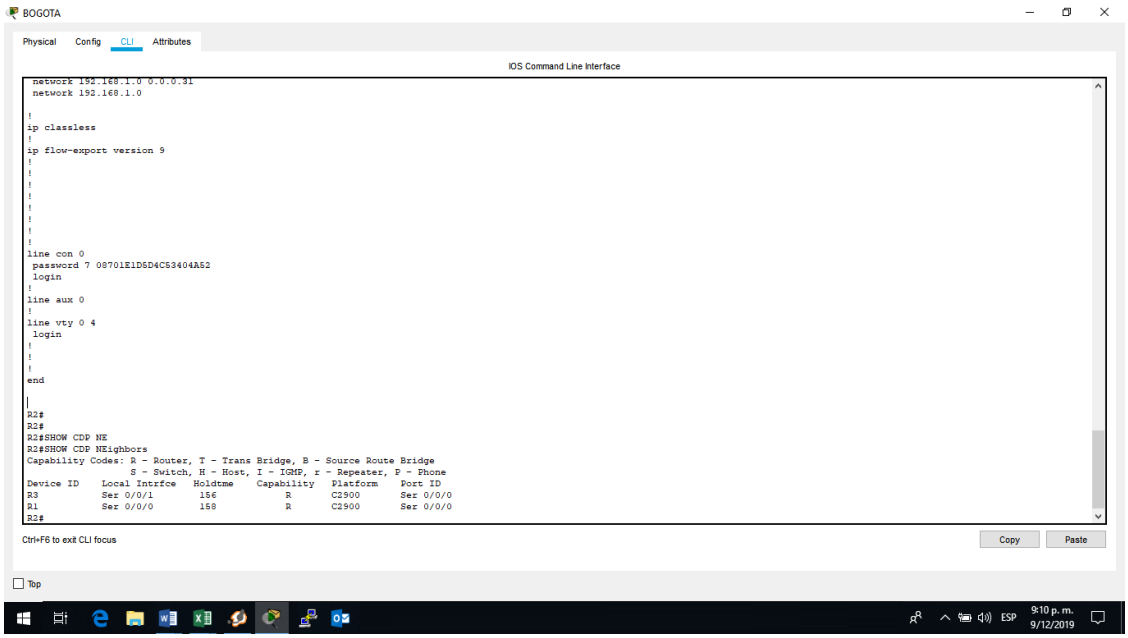

Figura 12. evidencia que tiene como vecino a R1 y a R3

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

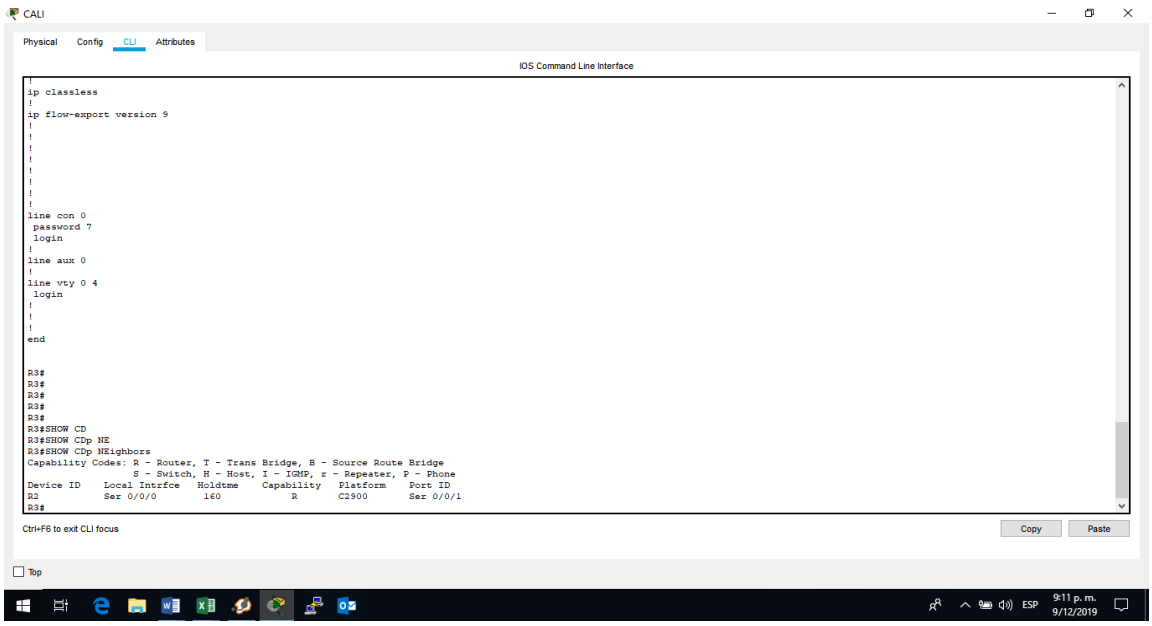

Figura 13. evidencia que tiene como vecino a R2 Bogotá

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

R1MEDELLIN =

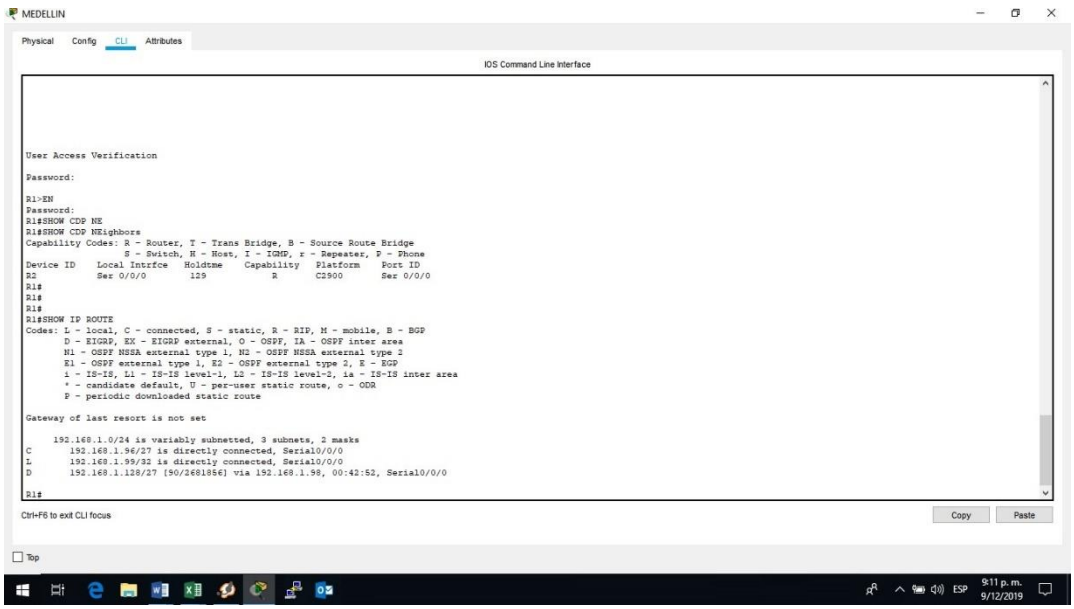

Figura 14. tablas de enrutamiento

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

R2_BOGOTA=

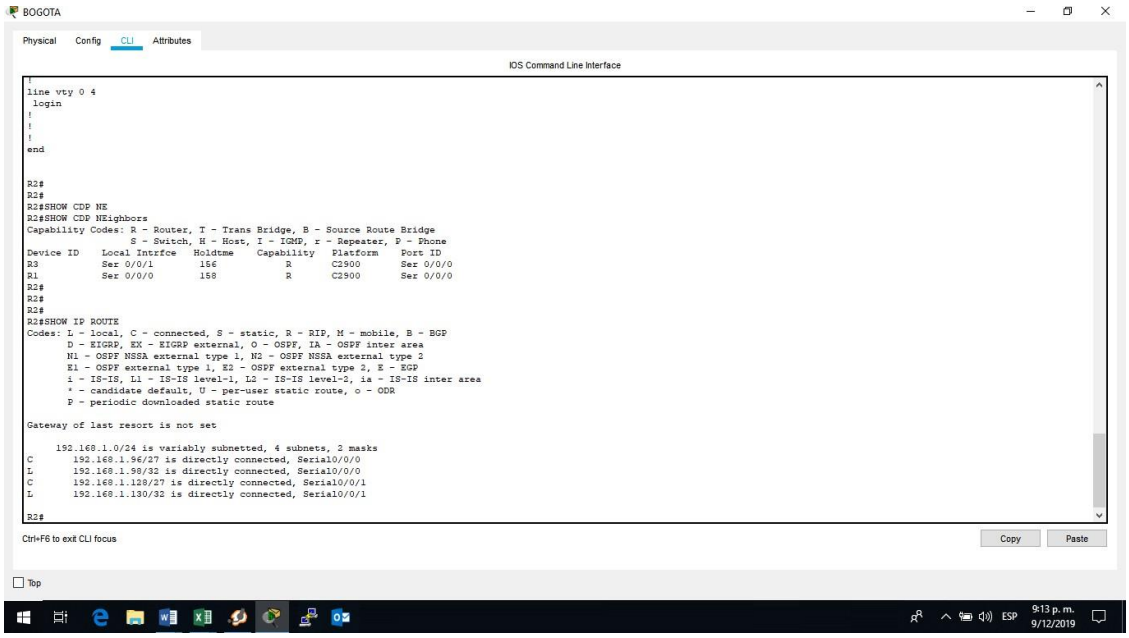

Figura 15. tablas de enrutamiento Medellín hacia Bogotá

RUTAS ESTABLECIDAS EN BOGOTA HACIA MEDELLIN Y LA RED DE CALI.
R3_CALI =

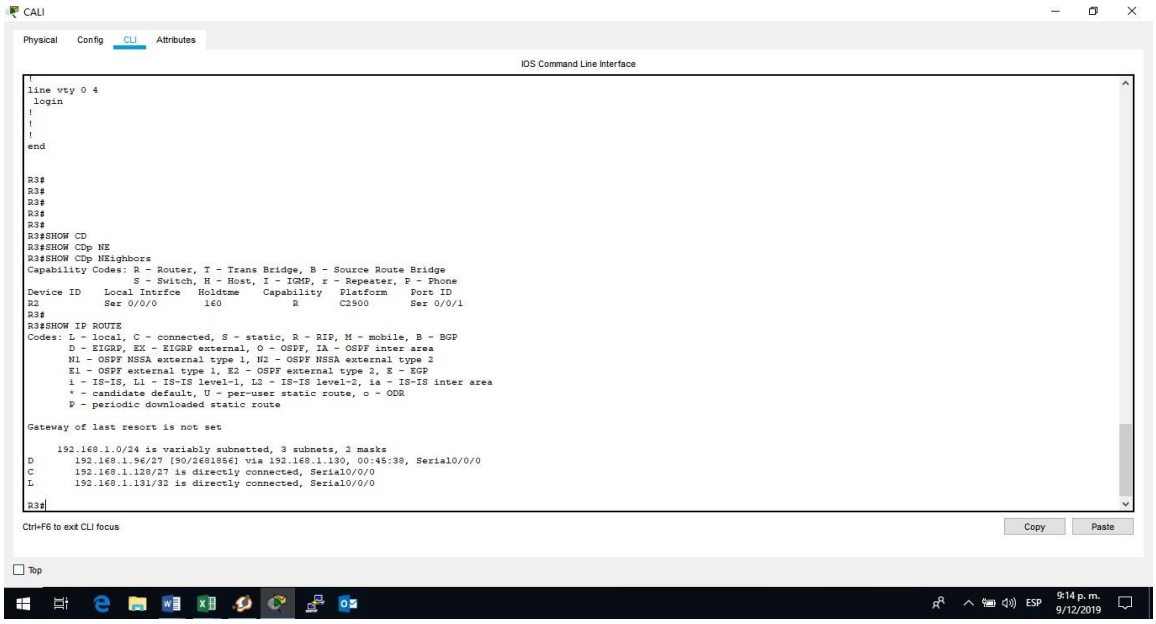

figura 16. tablas de enrutamiento *Bogotá hacia Medellín y la red de Cali*

RUTAS ESTABLECIDAS EN CALI HACIA BOGOTA Y LA RED DE MEDELLIN

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 REALIZA PING A UN ORDENADOR DE LA RED DE MEDELLIN
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:\>

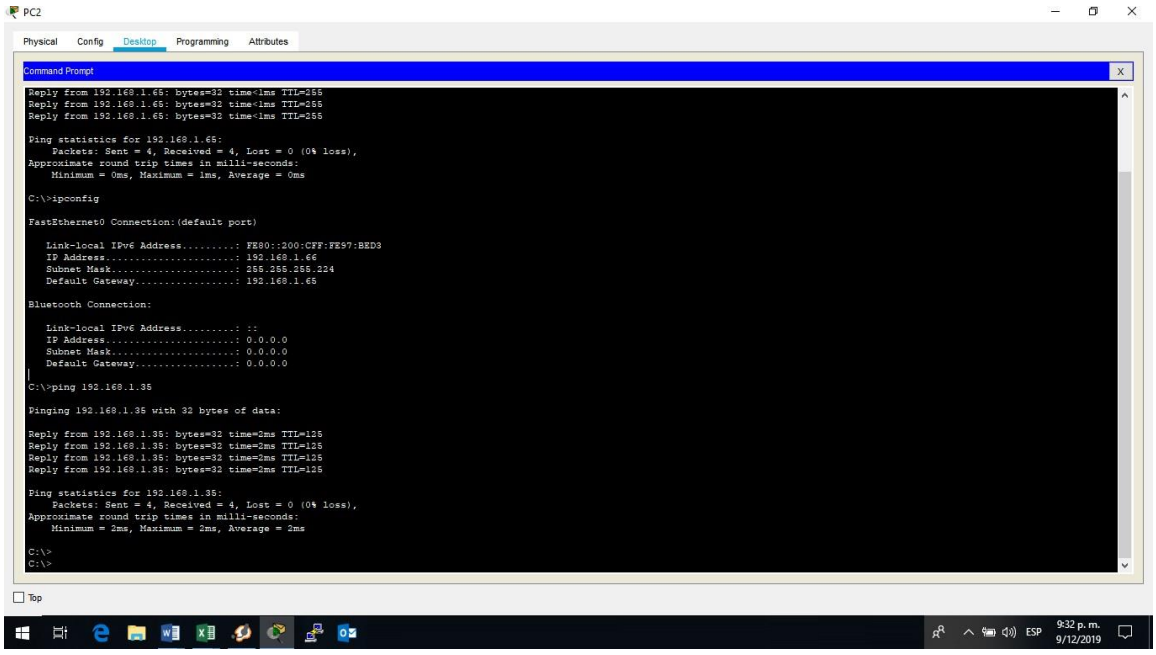

Figura 17. Evidencia ping.

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:\>

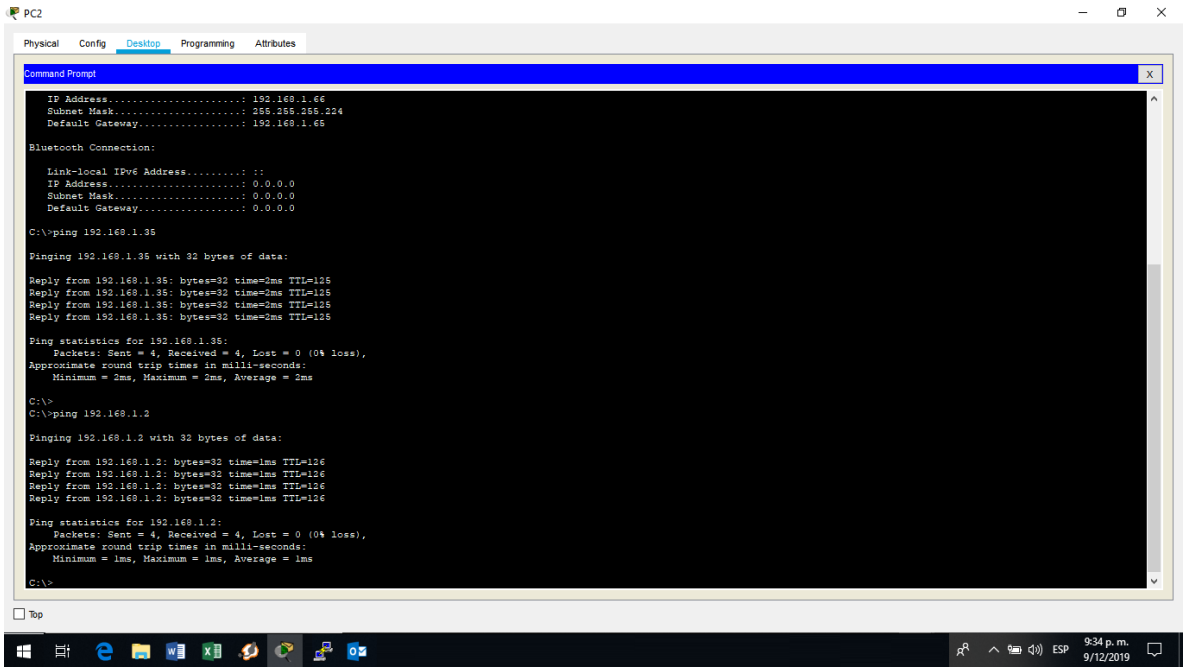

Figura 18. Evidencia ping.

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

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.

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.
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.

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.

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.

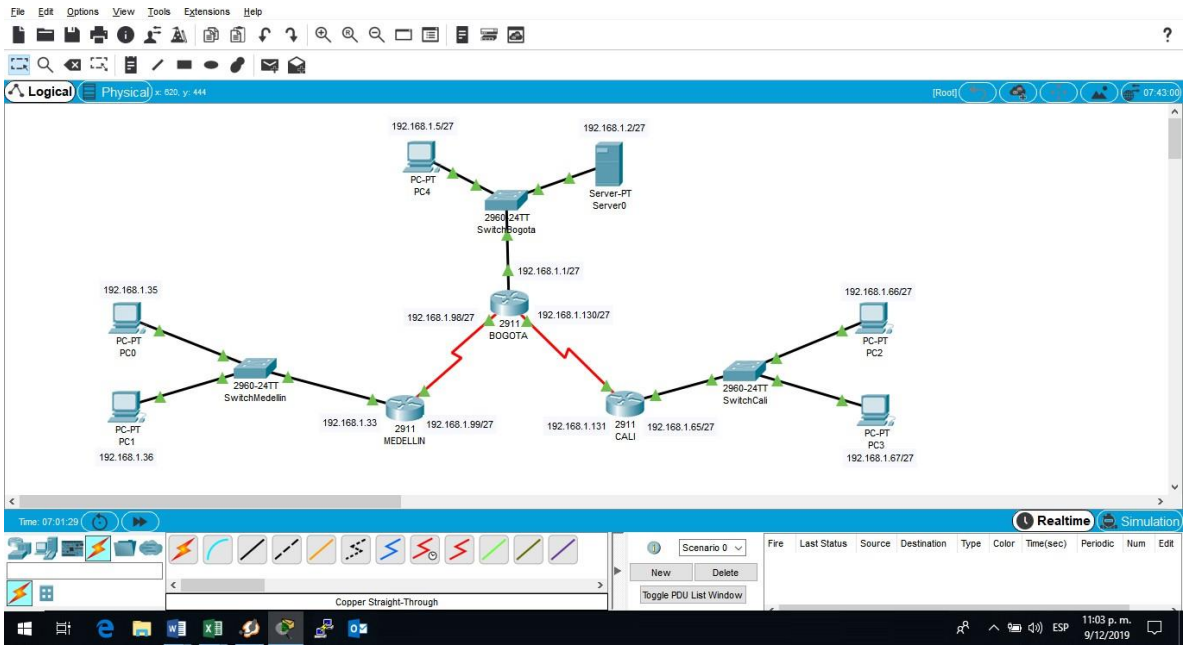

Figura 19. Direccionamiento topología.

Se realiza ping hacia 2 host lan, uno de Cali y otro de Medellín 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

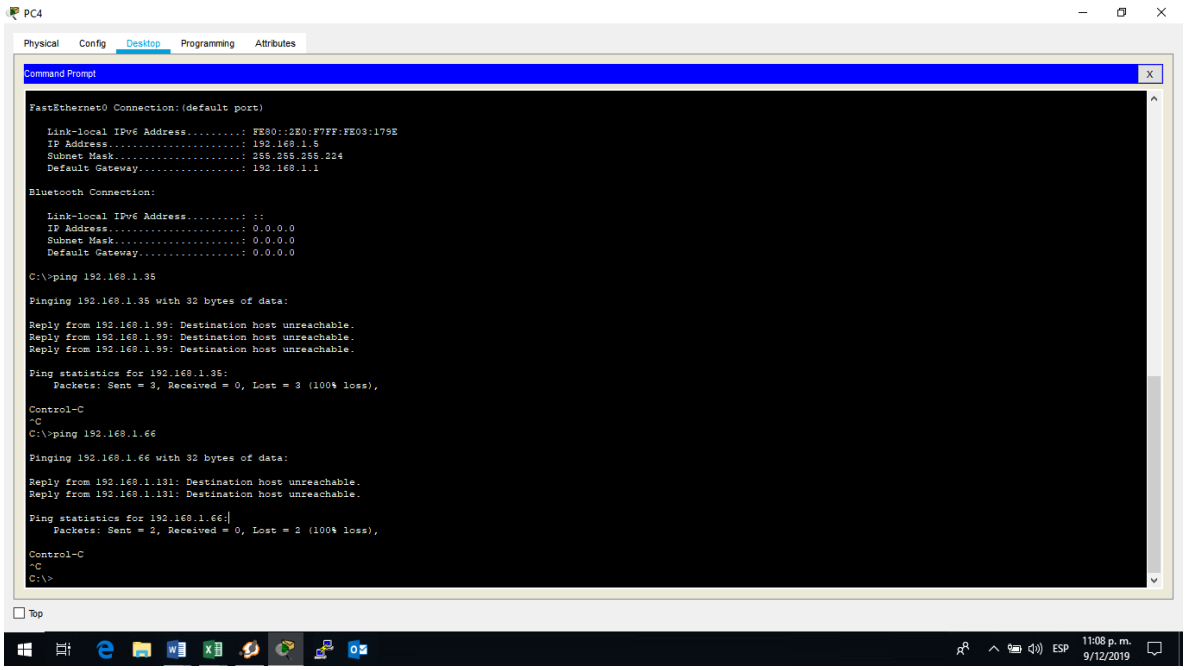

Figura 20. Evidencia ping

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

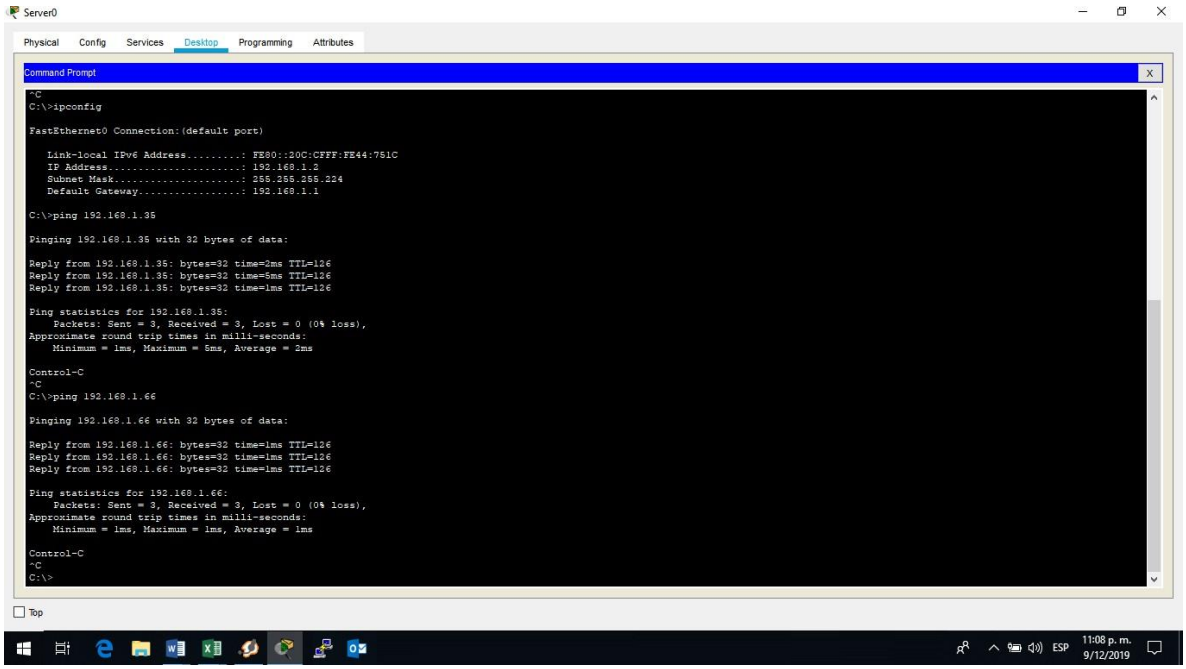

Figura 21. Evidencia ping

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:\>

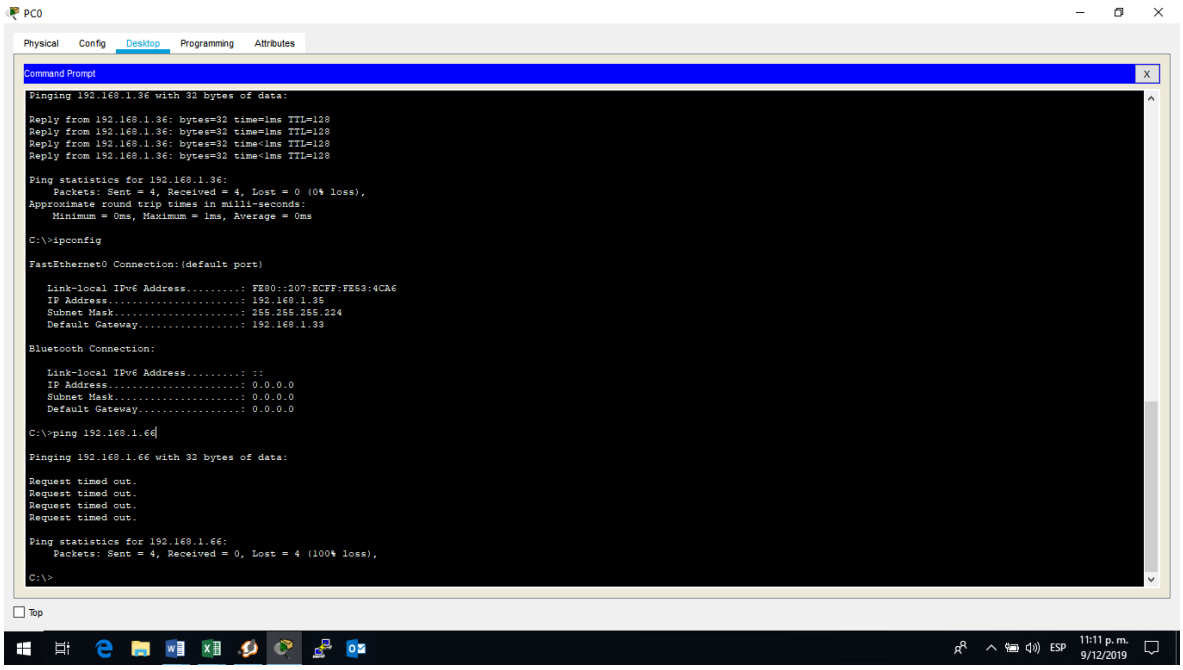

Figura 22. Configuración tarjeta de red.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	ONEXIÓN OK
	WS_1	Router BOGOTA	CONECTA
	Servidor	Router CALI	ONEXIÓN OK
	Servidor	Router MEDELLIN	ONEXIÓN OK
TELNET	AN del Router MEDELLIN	Router CALI	NO CONECTA
	LAN del Router CALI	Router CALI	NO CONECTA
	AN del Router MEDELLIN	Router MEDELLIN	NO CONECTA
	LAN del Router CALI	Router MEDELLIN	NO CONECTA
PING	LAN del Router CALI	WS_1	NO CONECTA
	AN del Router MEDELLIN	WS_1	NO CONECTA
	AN del Router MEDELLIN	LAN del Router CALI	NO CONECTA
PING	LAN del Router CALI	Servidor	ONEXIÓN OK
	AN del Router MEDELLIN	Servidor	ONEXIÓN OK
	Servidor	LAN del Router MEDELLIN	ONEXIÓN OK
	Servidor	LAN del Router CALI	ONEXIÓN OK
	Router CALI	LAN del Router MEDELLIN	ONEXIÓN OK
	Router MEDELLIN	LAN del Router CALI	ONEXIÓN OK

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:\>

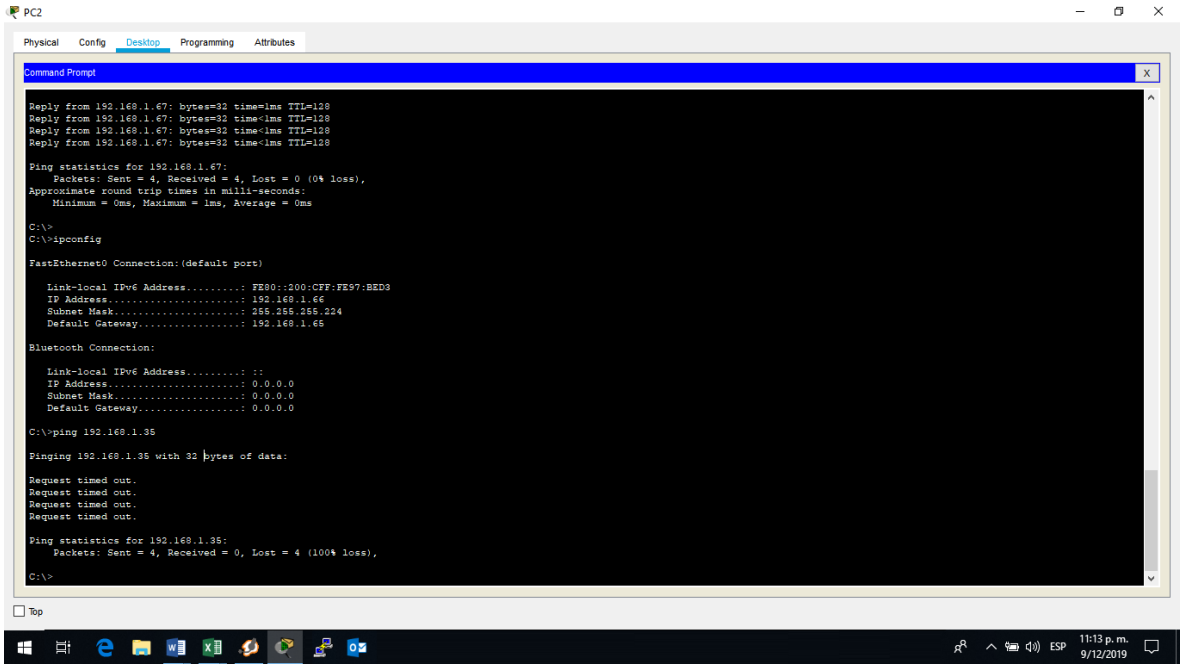

Figura 23. Evidencia ping

ESCENARIO 2

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

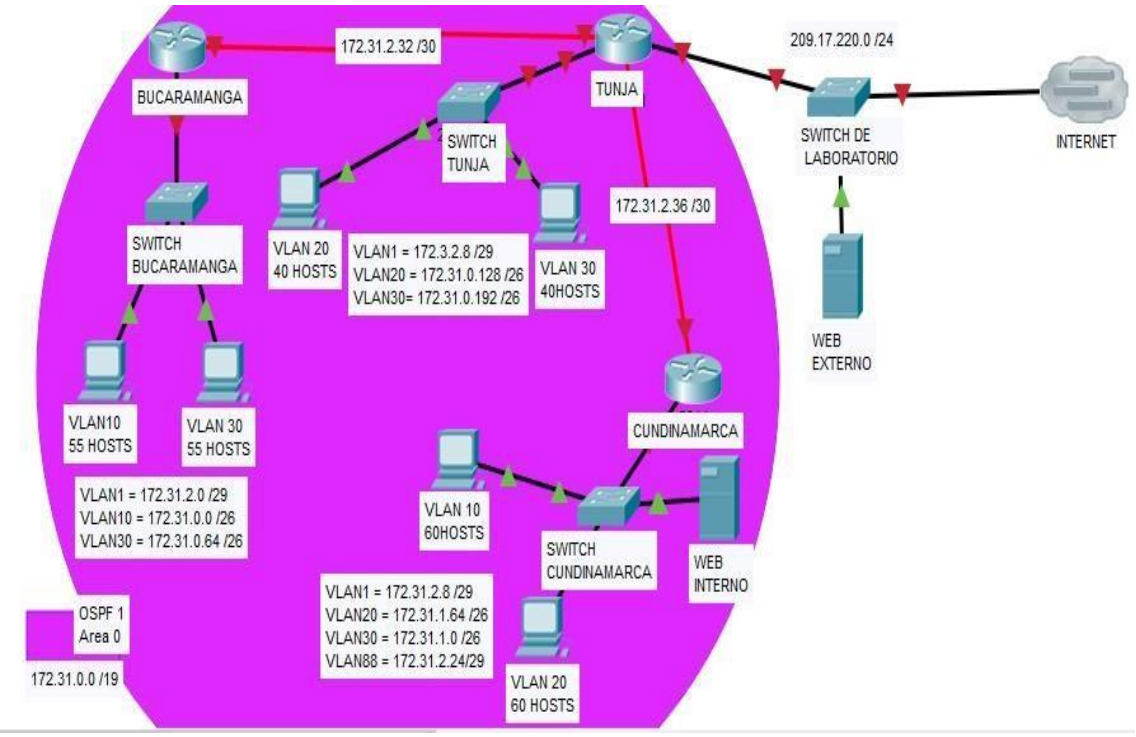

Figura 24. Topología escenario 2.

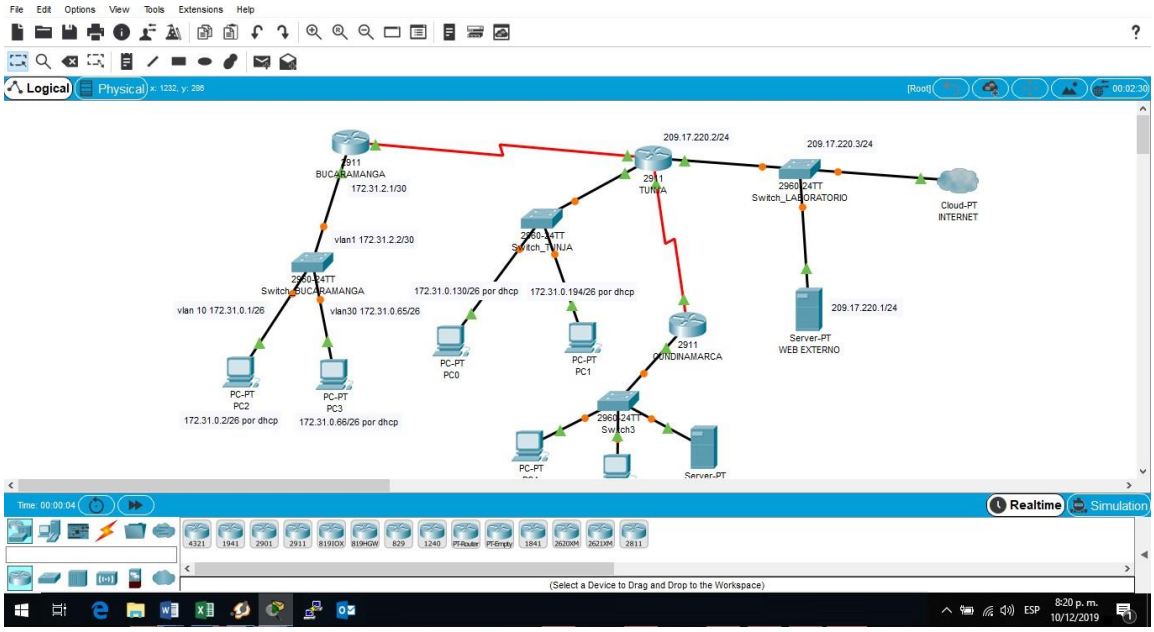

Figura 25. Simulación Topología escenario 2.

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente Configuración:

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

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

Figura 26. Configuración seguridad.

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)#

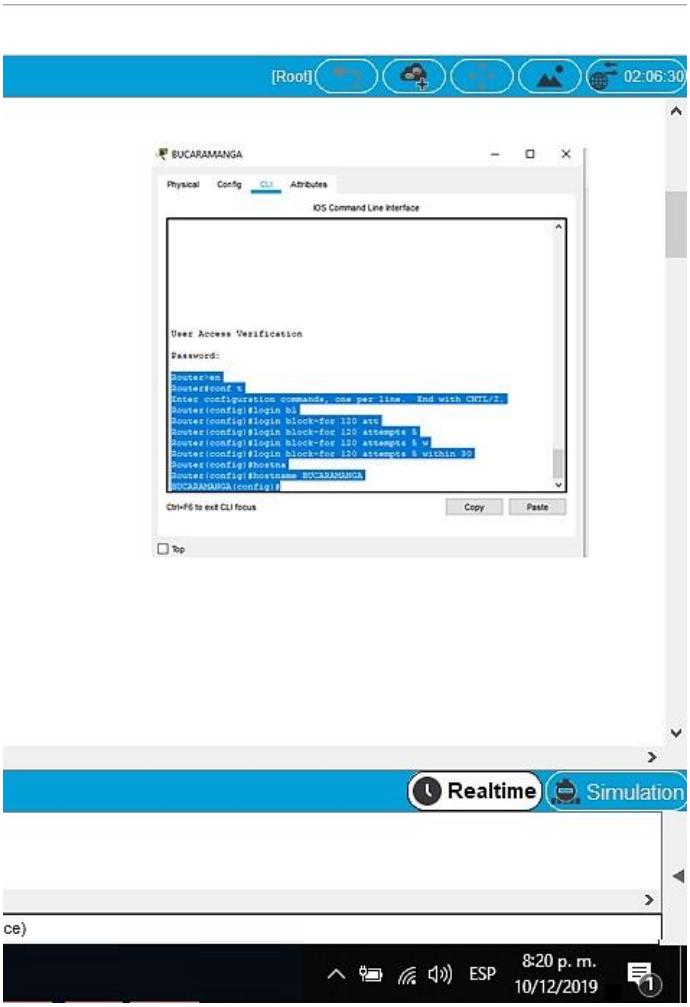

Figura 27. Configuración seguridad.

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#

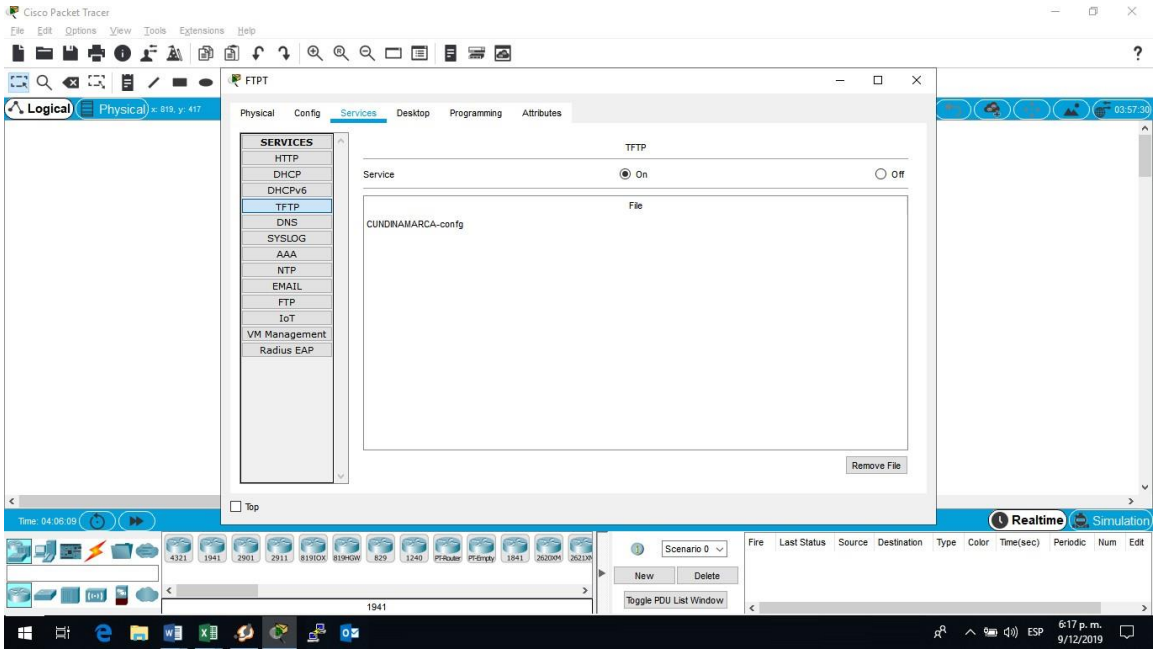

Figura 28. Evidencia de guardo en el equipo.

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:

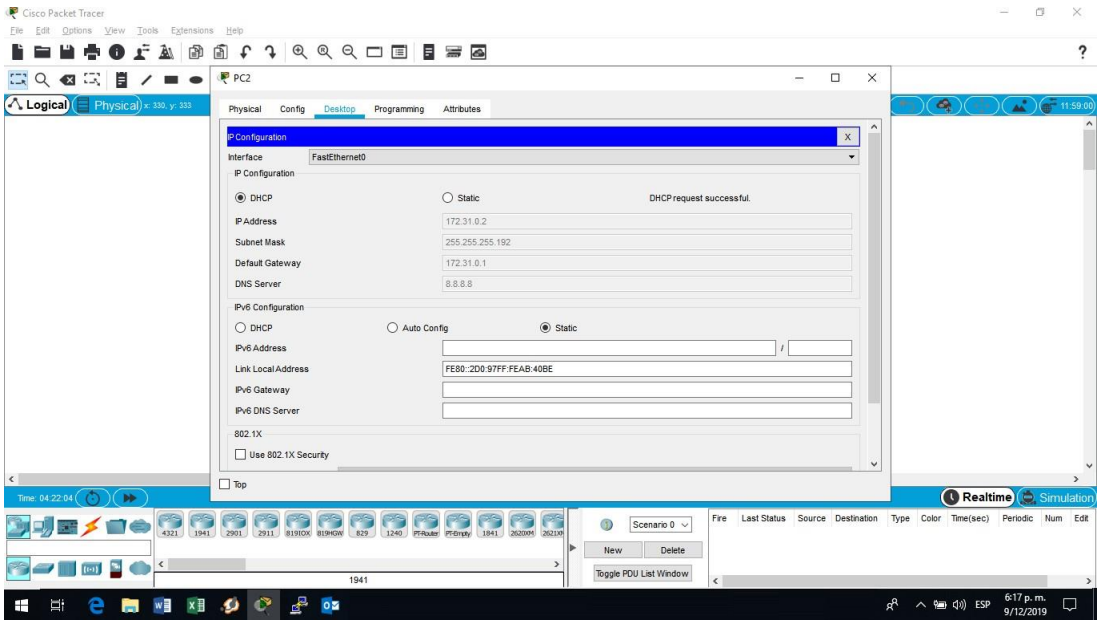

Figura 29. Gateway dinámico.

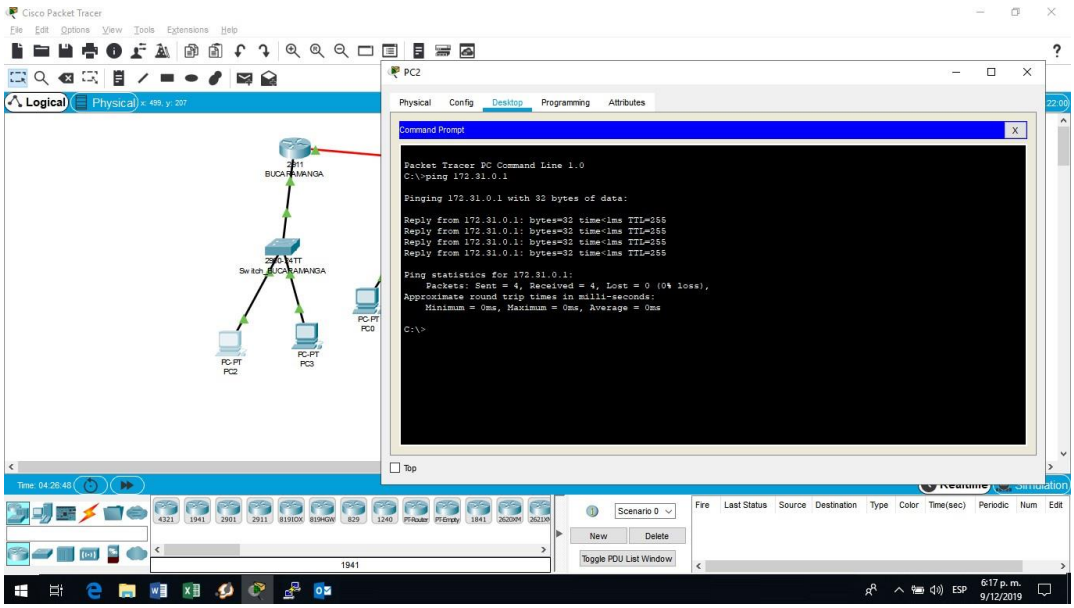

Figura 30. Prueba de conectividad DHCP Bucaramanga.

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#

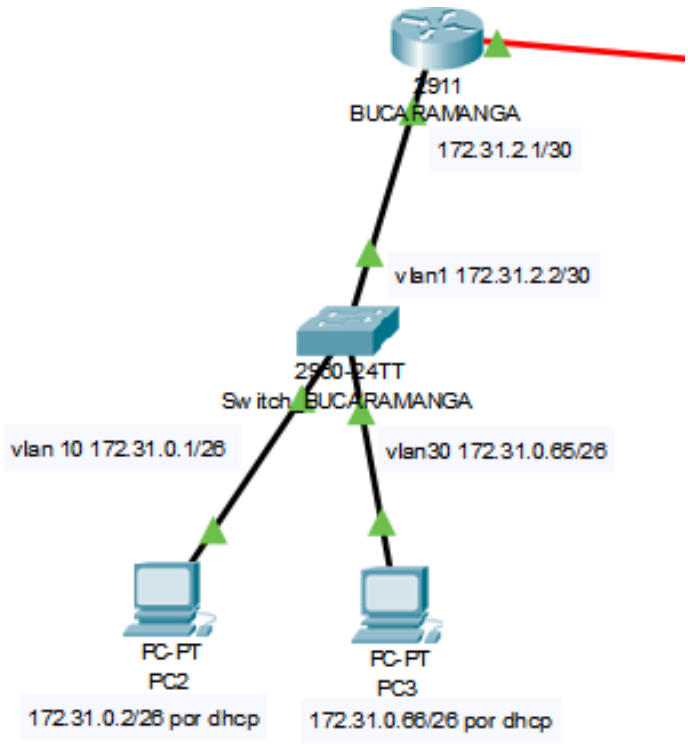

Figura 31. Direccionamiento

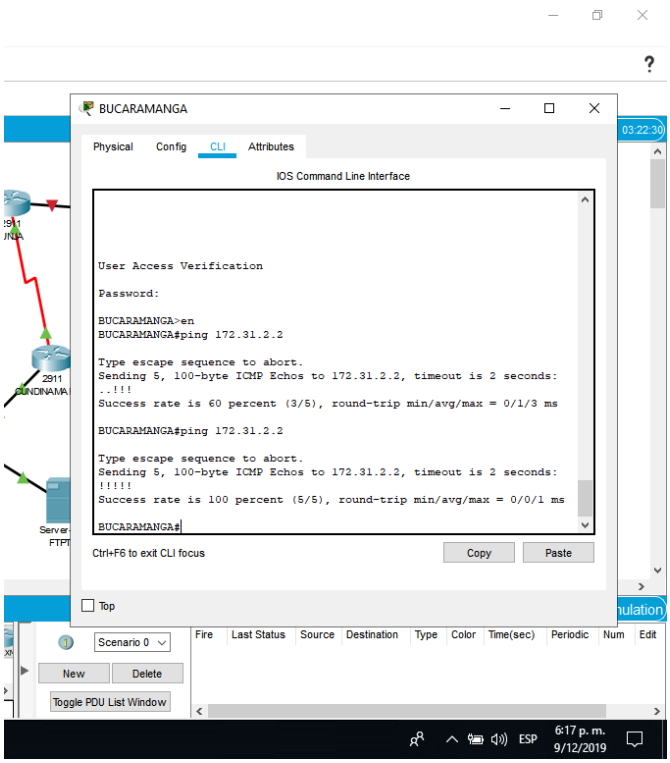

Figura 32. Evidencia ping

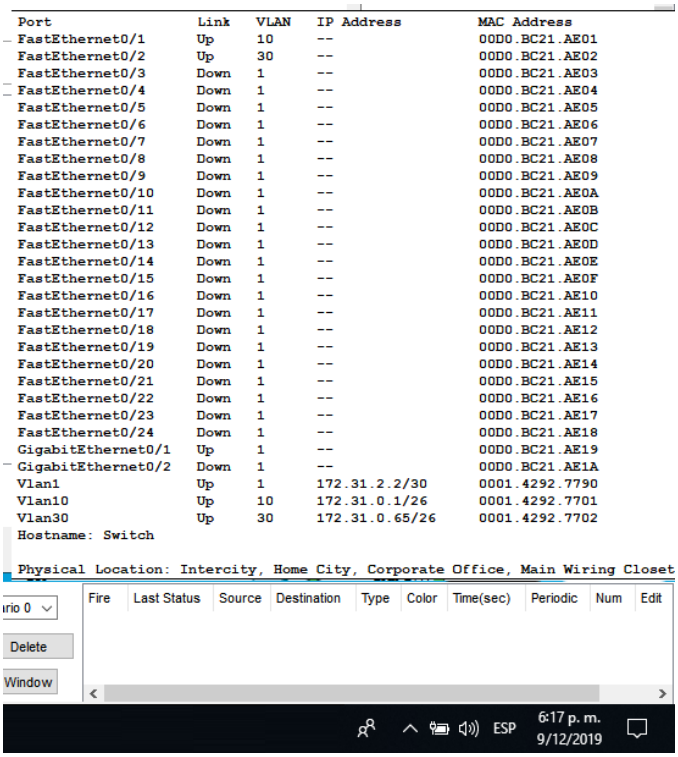

Figura 33. interfaces virtuales

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)#

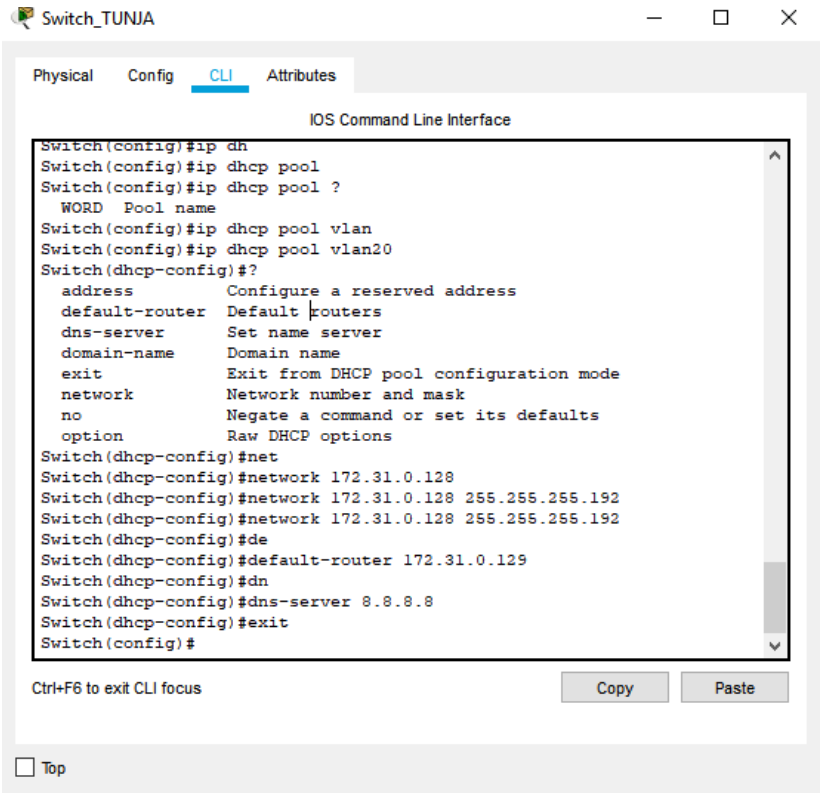

Figura 34. Rutas aprendidas.

Pc en VLAN 20 de Tunja aprendido IP por DHCP:

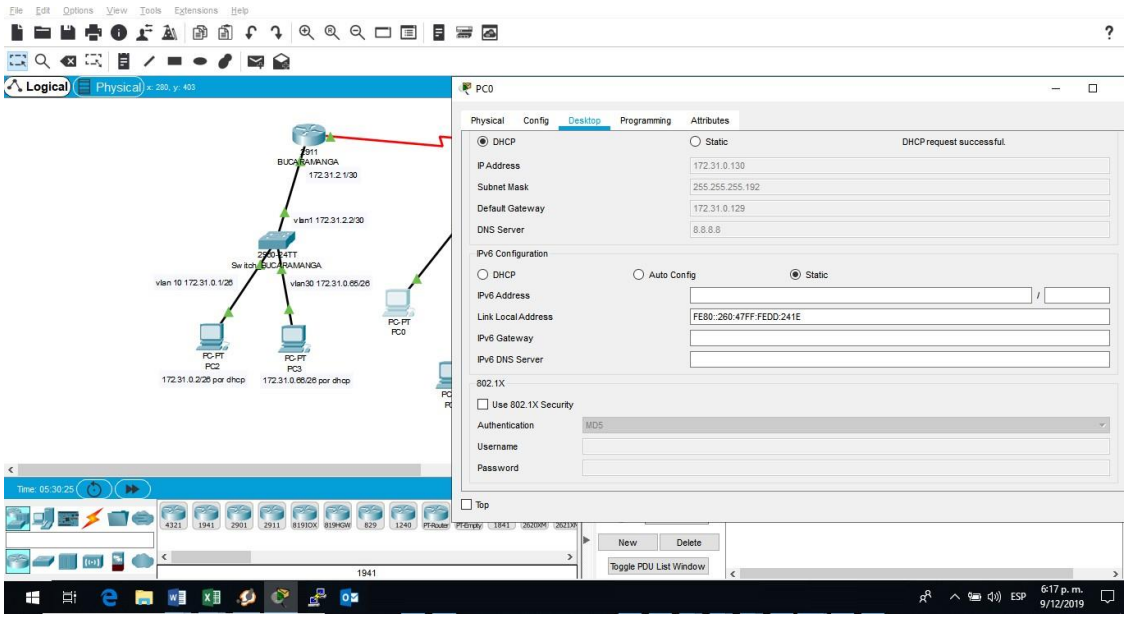

Figura 35. evidencia DHCP.

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

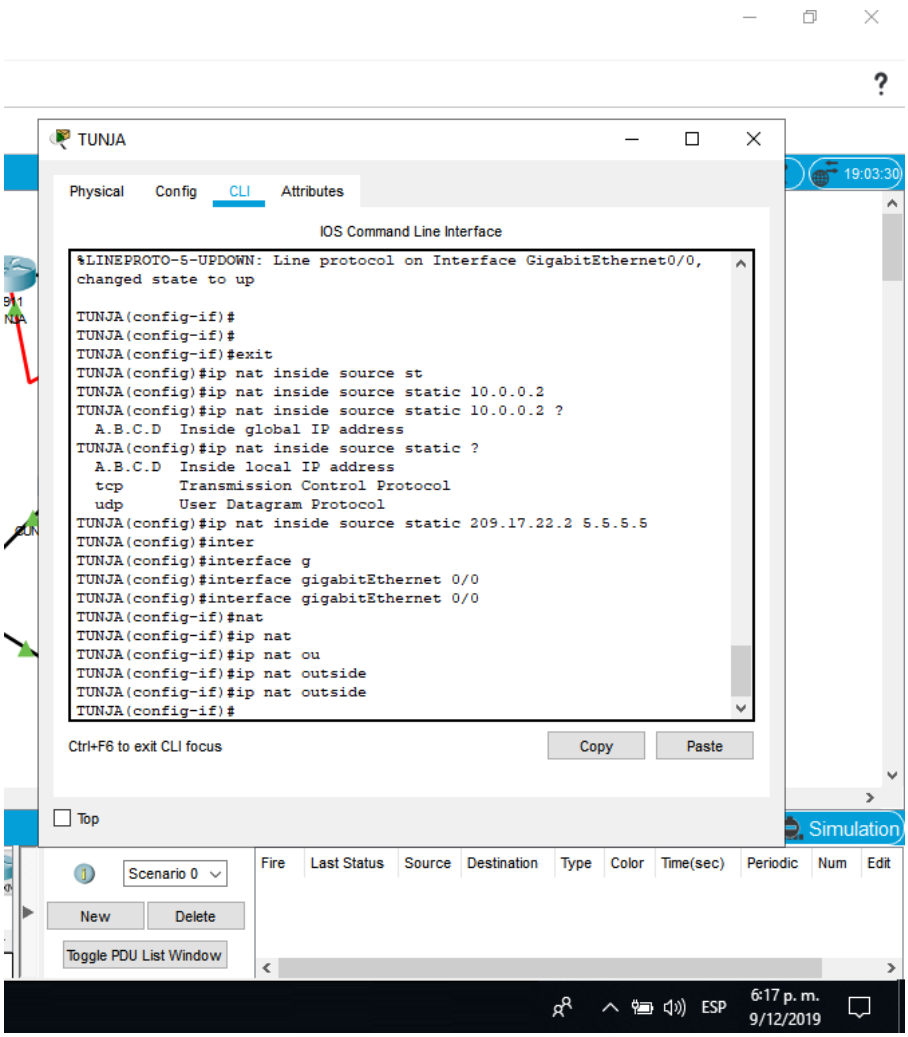

Figura 36. NAT estático.

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)#

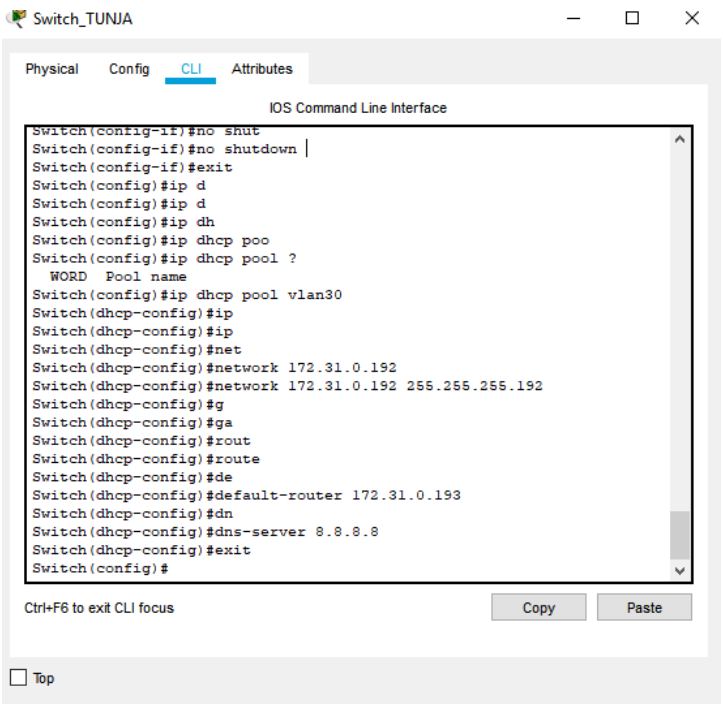

Figura 36. NAT estático

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

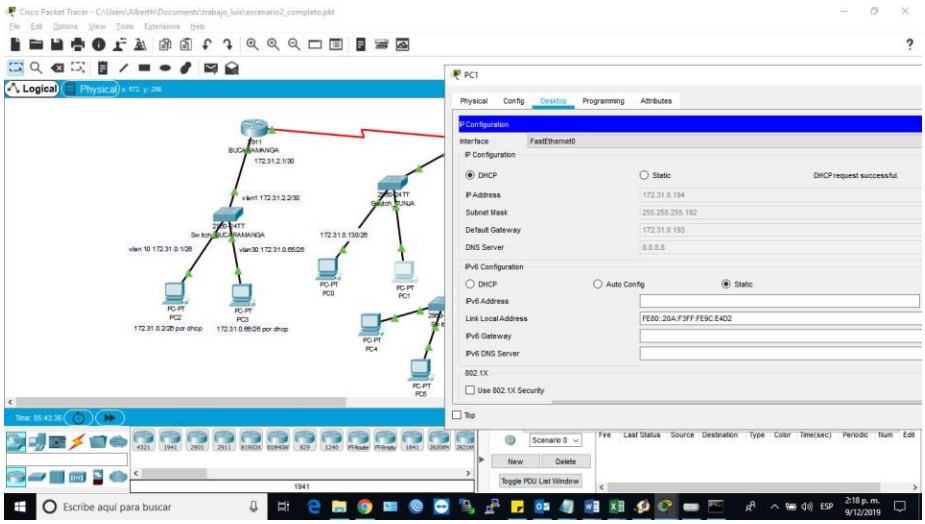

Figura 37. DHCP tomado.

E
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

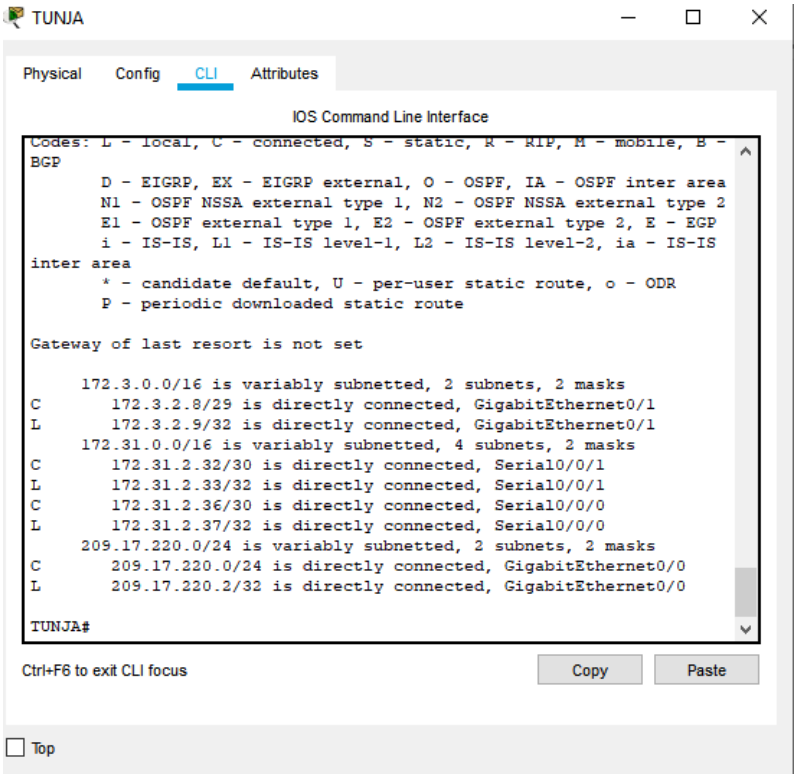

Figura 38. Tabla de enrutamiento.

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 VLAN10.

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

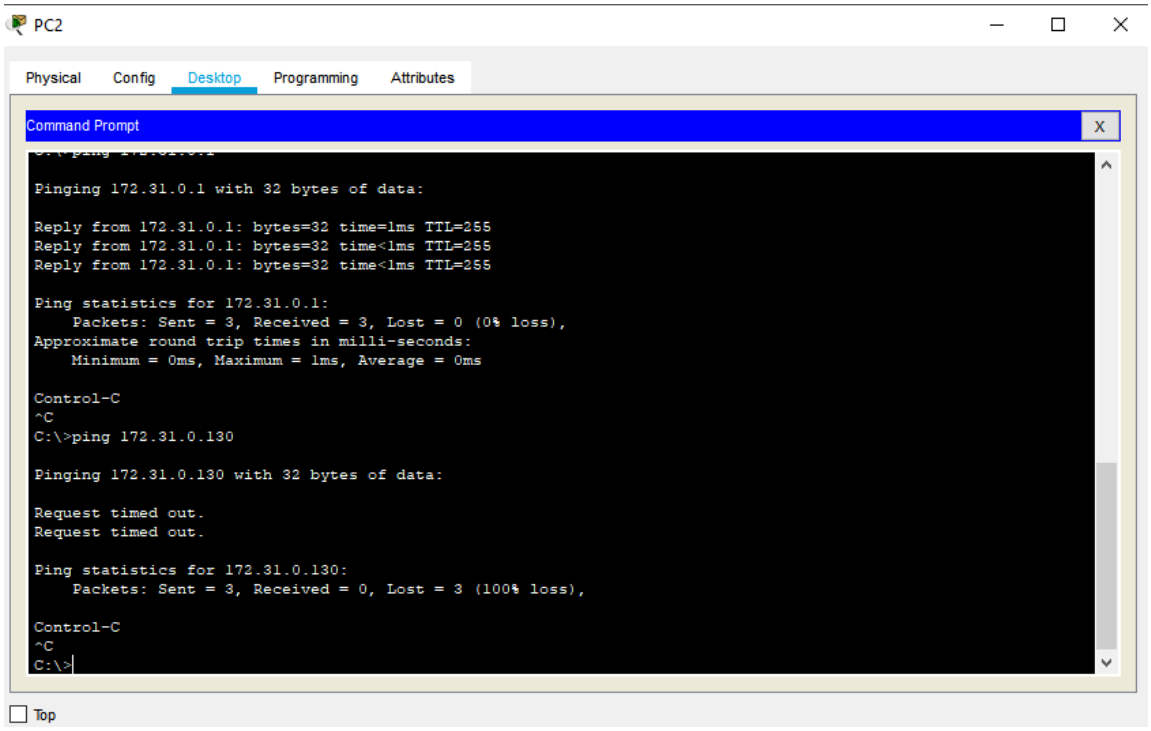

Figura 39. Evidencia ping.

Aspectos validados en la simulación
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

De acuerdo con los contenidos analizados en el diplomado, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat), etc.

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

Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema.

Bibliografía

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

Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software.

Chamorro Serna, L., Montaño Torres, O., Guzmán Pérez, E. H., Daza Navia, M. Y., & Castillo Ortiz, O. F. (2018). Diplomado de Profundización Cisco-Enrutamiento en soluciones de red.

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

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

Es.wikipedia.org. (2018). Open Shortest Path First. [online] disponible en: https://es.wikipedia.org/wiki/Open_Shortest_Path_First [28 May 2018].
Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0

Segui, F. B. (2015). Configuración DHCP en routers CISCO.

Shaughnessy, T., Velte, T., & Sáchez García, J. I. (2000). Manual de CISCO.

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101