

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON EDILBERTO RODRÍGUEZ BALANTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA ELECTRÓNICA
VILLAVICENCIO
2019.

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON EDILBERTO RODRÍGUEZ BALANTA

Diplomado de opción de grado presentado para optar al título
de Ingeniero electrónico.

Gerardo Granados Acuña
Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA ELECTRÓNICA
VILLAVICENCIO
2019.

Nota de aceptación:

Presidente del jurado

Jurado

Jurado

Villavicencio 17 de julio de 2019.

CONTENIDO

	pág.
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	10
RESUMEN	12
ABSTRACT	12
INTRODUCCIÓN	14
1. ESCENARIO 1.	15
1.1. CONFIGURACIONES INICIALES Y PROTOCOLOS DE ENRUTAMIENTO.....	15
1.2. CREACIÓN DE INTERFACES LOOPBACK EN R1	18
1.3. CREACIÓN DE INTERFACES LOOPBACK EN R5	20
1.4. ANÁLISIS DE LA TABLA DE ENRUTAMIENTO DE R3	21
1.5. CONFIGURACIÓN R3 PARA REDISTRIBUIR LAS RUTAS EIGRP EN OSPF ...	22
1.6. VERIFICACIÓN DE EXISTENCIA EN R1 Y R5 DE LAS RUTAS DEL SISTEMA AUTÓNOMO OPUESTO.....	23
2. ESCENARIO 2	28
2.1. RELACIÓN DE VECINO BGP ENTRE R1 Y R2.....	29
2.2. RELACIÓN DE VECINO BGP ENTRE R2 Y R3.....	31

2.3.	RELACIÓN DE VECINO BGP ENTRE R3 Y R4.....	34
3.	ESCENARIO 3	37
A.	CONFIGURAR VTP	37
B.	CONFIGURAR DTP (DYNAMIC TRUNKING PROTOCOL)	39
C.	AGREGAR VLANS Y ASIGNAR PUERTOS.	42
D.	CONFIGURAR LAS DIRECCIONES IP EN LOS SWITCHES	46
D.	VERIFICAR LA CONECTIVIDAD EXTREMO A EXTREMO	46
4.	CONCLUSIONES.....	54
	BIBLIOGRAFÍA.....	55

LISTA DE TABLAS

Tabla 1. Direcciones de red para Loopback requeridas en el router R1	18
Tabla 2. Direcciones de red para Loopback requeridas en el router R5	20
Tabla 3. Configuración de los router. Escenario 2.....	28
Tabla 4. Interfaz y direcciones IP para los PCs según las VLAN.....	44
Tabla 5. Direccionamiento de IP para SWT 1, 2 y 3.....	46

LISTA DE FIGURAS

Figura 1. Topología propuesta para el escenario 1. Imagen tomada del programa GNS3	15
Figura 2. Captura de pantalla de Ping entre R1 y R4	17
Figura 3. Captura de pantalla de ping entre R4 y R5.....	17
Figura 4. Captura de pantalla, comprobación de creación de interfaces Loopback en R1, mediante el comando show ip route. Tomada del programa GNS3.....	19
Figura 5. Captura de pantalla, comprobación de creación de interfaces Loopback en R5, mediante el comando show ip route. Tomada del programa GNS3.....	21
Figura 6. Captura de pantalla, aprendizaje de interfaces Loopback en R3, mediante el comando show ip route. Tomada del programa GNS3.....	21
Figura 7. Captura de pantalla configuración de R3. Tomada del programa GNS3	22
Figura 8. Captura de pantalla, verificación de existencia en R1 de las rutas del sistema autónomo opuesto, mediante el comando show ip route y show ip ospf database. Tomada del programa GNS3	23
Figura 9. Captura de pantalla, verificación de existencia en R5 de las rutas del sistema autónomo opuesto, mediante el comando show ip route y show ip eigrp topology. Tomada del programa GNS3	25
Figura 10. Verificación de comunicación desde R1 hasta R5. Imagen tomada del programa GNS3.....	26
Figura 11. Topología de red propuesta para el escenario 2. Captura tomada del programa GNS3.....	28
Figura 12. Verificación de relación de vecino BGP entre R1 y R2, mediante el uso del comando show ip route.....	30
Figura 13. Verificación de relación de vecino BGP entre R2 y R3, mediante el uso del comando show ip route.....	33

Figura 14. Verificación de relación de vecino BGP entre R3 y R4, mediante el uso del comando show ip route.	35
Figura 15. Topología de red propuesta para el escenario 3. Captura tomada del programa Packet Tracer.....	37
Figura 16. Verificación de configuraciones en SWT1, SWT2 y SWT3. Captura de pantalla tomada del programa Packet Tracer	38
Figura 17. Verificación de enlace “trunk” entre SWT1 y SWT2. Captura tomada del programa Packet Tracer	40
Figura 18. Verificación de enlace “trunk” en SWT1. Captura tomada del programa Packet Tracer	41
Figura 19. Enlace permanente entre SWT2 y SWT3. Captura de pantalla tomada del programa Packet Tracer.	42
Figura 20. Emisión del comando show vlan brief en SWT 1, 2 y 3. Captura de pantalla tomada del programa Packet Tracer.	43
Figura 21. Ping desde PC1 a PC4 y PC7. Captura tomada del programa Packet Tracer.	47
Figura 22. Ping desde PC1 a PC3, PC5, PC6, PC7, PC8 y PC9. Captura tomada del programa Packet Tracer.	47
Figura 23. Ping desde PC2 a PC5 y PC8. Captura tomada del programa Packet Tracer.	48
Figura 24. Ping desde PC3 a PC6 y PC9. Captura tomada del programa Packet Tracer.	49
Figura 25. Ping desde SWT1 a SWT2 Y SWT3. Captura tomada del programa Packet Tracer.	50
Figura 26. Ping desde SWT2 a SWT1 Y SWT3. Captura tomada del programa Packet Tracer.	51
Figura 27. Ping desde SWT3 a SWT1 Y SWT2. Captura tomada del programa Packet Tracer.	51

Figura 28. Ping entre SWT1 y las PC1, PC2 y PC3. Imagen tomada del programa Packet Tracer.52

GLOSARIO

BGP: es un protocolo de gateway exterior (EGP), usado para realizar el ruteo entre dominios en las redes TCP/IP. Un router BGP debe establecer una conexión (en el puerto TCP 179) con cada uno de sus peers BGP para poder intercambiar las actualizaciones de BGP. La sesión de BGP entre dos peers BGP se dice que es una sesión de BGP externo (eBGP) si los peers BGP se encuentran en sistemas autónomos diferentes (AS). Una sesión de BGP entre dos peers BGP se dice que es una sesión de BGP interno (iBGP) si los peers BGP se encuentran en los mismos sistemas autónomos.

CCNP: (Cisco Certified Network Professional) curso de nivel intermedio programado por CISCO. Las personas que se desean certificar, deben superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

EIGRP: protocolo de Enrutamiento de Puerta de enlace Interior Mejorado, es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

FIREWALL: software especializado que examina los datos entrantes y protege la red de su negocio de posibles ataques.

INTERFAZ: en informática, se utiliza para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporcionan una comunicación de distintos niveles permitiendo el intercambio de información. Su plural es interfaces.

IPV6: el protocolo de internet versión 6, en inglés, Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

LOOPBACK: el dispositivo de red loopback es una interfaz de red virtual. Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers.

OSPF: el protocolo Open Shortest Path First (OSPF), definido en RFC 2328, es un Internal Gateway Protocol (IGP) que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo. El protocolo OSPF está basado en tecnología de estado de link, la cual es una desviación del algoritmo basado en el vector Bellman-Ford usado en los protocolos de ruteo de Internet tradicionales, como el RIP. OSPF ha introducido

conceptos nuevos, como la autenticación de actualizaciones de ruteo, Máscaras de subred de longitud variable (VLSM), resumen de ruta, etc

PROCOLO: es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

RED: una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información.

ROUTER: los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y de esta forma, compartir una conexión de Internet entre varios usuarios.

STP: spanning tree protocol es un protocolo de capa 2 que se ejecuta en bridges y switches. La especificación para STP es IEEE 802.1D. El propósito principal de STP es garantizar que usted no cree loops cuando tenga trayectorias redundantes en su red.

SWITCH: los switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar varias computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí.

TRUNK: es una configuración de canal para puertos de switch que estén en una red Ethernet, que posibilita que se pueda pasar varias VLAN por un único link, o sea, un link de troncal es un canal que puede ser switch-switch o switch-router, por donde se pasan información originada y con destino a más de una VLAN.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

VTP: son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

RESUMEN

La imperiosa necesidad que tienen los seres humanos por comunicarse, hace que cada día se desarrollen procesos más tecnificados y satisfactorios para los usuarios, por tanto, el presente informe evidencia el desarrollo de habilidades en el manejo y configuración de topologías con routers, estableciendo los protocolos de enrutamiento, configurando las distintas interfaces según el escenario propuesto, y creando interfaces de tipo Loopback de acuerdo a las direcciones asignadas.

La propuesta se basa en tres escenarios con topologías, configuraciones y tareas distintas.

En el escenario 1 se configuran los routers según lo planteado en cada actividad y se verifican estas configuraciones mediante el uso de los comandos show ip route. Igualmente se crean rutas mediante EIGRP en OSPF.

De otra parte, se propone un escenario 2, en donde se configuran los routers para una relación vecino usando el protocolo BGP y las tablas de direcciones definidas.

Finalmente se hace la implementación del escenario 3 en donde se hace la configuración de los Switches para VTP con actualizaciones de VLAN, DTP (Dynamic Trunking Protocol) enlace troncal ("trunk") dinámico, se Agregan VLANs y se asignan puertos, se configuran las direcciones IP en cada switch y se verifican la conectividad en la topología propuesta.

Para el desarrollo e implementación de los escenarios 1 y 2 se trabaja en el entorno de simulación GNS3 usando routers C7200; mientras que para el escenario 3 la implementación de la topología y la configuración de los distintos dispositivos se trabaja en el programa Packet Tracer con Switches 2960.

Palabras claves: Cisco, CNNP, electrónica, router, switch, Networking.

ABSTRACT

The imperative need that human beings have to communicate makes every day more technologically advanced and satisfactory processes for users, therefore, this report demonstrates the development of skills in the management and configuration of topologies with routers, establishing protocols of routing, configuring the different interfaces according to the proposed scenario, and creating interfaces of type Loopback according to the assigned addresses.

The proposal is based on three scenarios with different topologies, configurations and tasks.

In scenario 1, the routers are configured according to what is proposed in each activity and these configurations are verified by using the show ip route commands. Likewise, routes are created through EIGRP in OSPF.

On the other hand, a scenario 2 is proposed, where the routers for a neighbor relation are configured using the BGP protocol and the defined address tables.

Finally, the scenario 3 is implemented, where the configuration of the switches for VTP with VLAN updates, DTP (Dynamic Trunking Protocol) dynamic link (trunk), VLANs are added and ports are assigned. IP addresses in each switch and the connectivity in the proposed topology is verified.

For the development and implementation of scenarios 1 and 2, we work in the GNS3 simulation environment using C7200 routers; while for scenario 3 the implementation of the topology and the configuration of the different devices is worked in the Packet Tracer program with 2960 switches.

Keywords: Cisco, CNNP, electronics, router, switch, Networking.

INTRODUCCIÓN

El mundo de las telecomunicaciones ha evolucionado bastante y esto ha hecho que las formas tradicionales de comunicación hayan sido reemplazadas, por ejemplo, los chats, las video llamadas, las videoconferencias, las compras, ventas por internet, la transmisión de eventos en vivo, entre otras actividades. Todo esto junto ha permitido el desarrollo de nuevos conocimientos y de paso la necesidad de contar con profesionales capacitados en el diseño, implementación y mantenimiento de redes en las distintas empresas, con el fin de salvaguardar la información y la seguridad en la transmisión y recepción de los mensajes; para lograrlo es necesario desarrollar habilidades en la conexión y configuración de dispositivos como routers, switches y equipos de cómputo configurados con los protocolos de velocidad de transmisión, comunicación y seguridad apropiados.

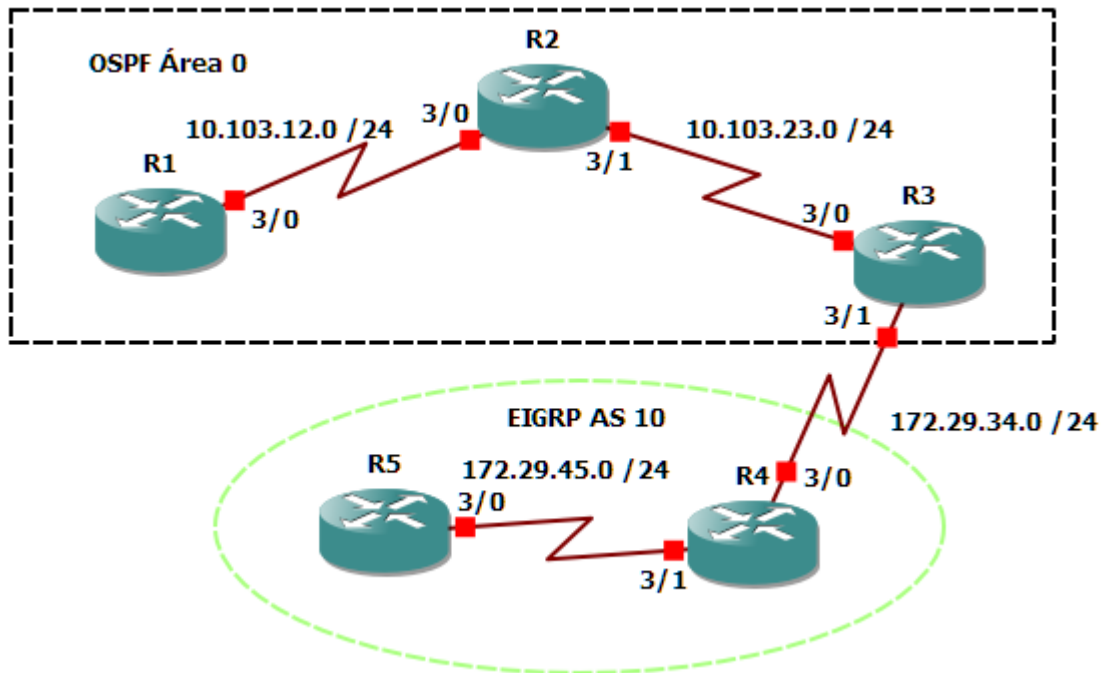
En la actualidad existen varias empresas en el mercado de las telecomunicaciones; pero de una u otra forma cada una de ellas termina implementando protocolos de comunicaciones y redes configuradas con dispositivos CISCO, lo que ha propiciado que cualquier profesional interesado en este fascinante mundo, deba adelantar los cursos que ofrece la empresa CISCO, ya que éstos permiten obtener las certificaciones que verifican que se tiene la competencia para implementar redes de comunicación.

En el presente informe se evidencia el desarrollo de habilidades de configuración de redes, que pueden ser implementadas en empresas de cualquier sector, ya sea a través de redes de Área local (LAN) cuyo propósito es el manejo de la información de forma privada, redes de Área metropolitana (MAN) aunque en la actualidad está en desuso o en redes de Área amplia (WAN) que abarcan comunicación en grandes superficies y requieren de la configuración de varios dispositivos. La metodología empleada para evidenciar el desarrollo de estas habilidades se basa en el trabajo de tres situaciones planteadas bajo igual número de escenarios, en donde cada uno presenta actividades-problema, las cuales guardan bastante relación con el quehacer diario y las dificultades a las que se debe enfrentar un profesional del manejo de las redes de comunicación.

1. ESCENARIO 1.

Topología de la red propuesta para el escenario 1.

Figura 1. Topología propuesta para el escenario 1. Imagen tomada del programa GNS3



Para el desarrollo de esta actividad se trabaja con el programa GNS 3 en el que hace el montaje de la red propuesta y se configuran los dispositivos, en la práctica se usan routers C7200.

1.1. CONFIGURACIONES INICIALES Y PROTOCOLOS DE ENRUTAMIENTO

Aplice las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Configuración R1.

```
R1# configure terminal
R1(config)# interface serial 3/0
R1(config-if)# ip address 10.103.12.1 255.255.255.0
R1(config-if)# clock rate 56000
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 10.103.12.0 0.0.0.255 area 0
```

Configuración R2.

```
R2# configure terminal
R2(config)# interface serial 3/0
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config)# interface serial 3/1
R2(config-if)# ip address 10.103.23.1 255.255.255.0
R2(config-if)# no shutdown
R1(config-if)# exit
R2(config)# router ospf 1
R2(config-router)# network 10.103.12.0 0.0.0.255 area 0
R2(config-router)# network 10.103.23.0 0.0.0.255 area 0
```

Configuración R3.

```
R3# configure terminal
R3(config)# interface serial 3/0
R3(config-if)# ip address 10.103.23.2 255.255.255.0
R3(config-if)# clock rate 56000
R3(config-if)# no shutdown
R3(config-if)# interface serial 3/1
R3(config-if)# ip address 172.29.34.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# router ospf 1
R3(config-router)# network 10.103.23.0 0.0.0.255 area 0
R3(config-router)# network 172.29.34.0 0.0.0.255 area 0
R3(config-if)# exit
R3(config)# router eigrp 10
R3(config-router)# network 172.29.34.0 0.0.0.255
R3(config-router)# no auto-summary
```

Configuración R4.

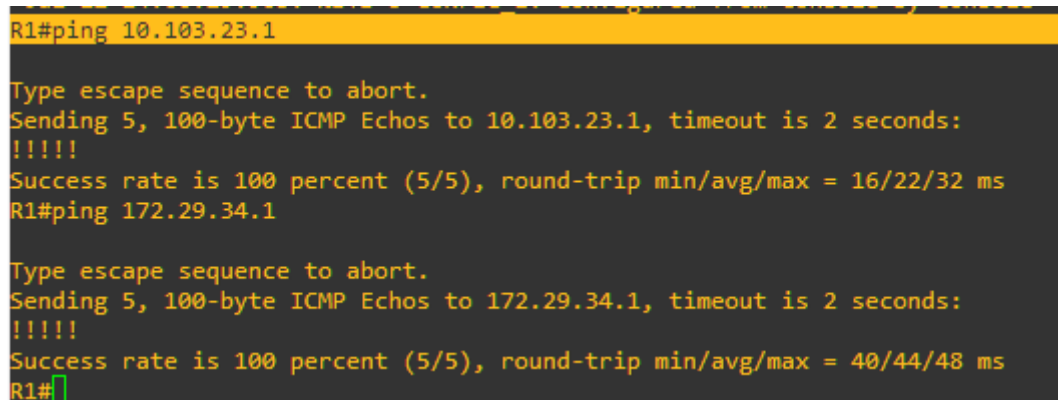
```
R4# configure terminal
R4(config-if)# interface serial 3/0
R4(config-if)# ip address 172.29.34.2 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# interface serial 3/1
R4(config-if)# ip address 172.29.45.1 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# exit
R4(config)# router eigrp 10
R4(config-router)# network 172.29.34.0 0.0.0.255
R4(config-router)# network 172.29.45.0 0.0.0.255
R4(config-router)# no auto-summary
```


Configuración R5.

```
R5# configure terminal
R5(config-if)# interface serial 3/0
R5(config-if)# ip address 172.29.45.5 255.255.255.0
R5(config-if)# clock rate 56000
R5(config-if)# no shutdown
R5(config-if)# exit
R5(config)# router eigrp 10
R5(config-router)# network 172.29.45.0 0.0.0.255
R4(config-router)# no auto-summary
```

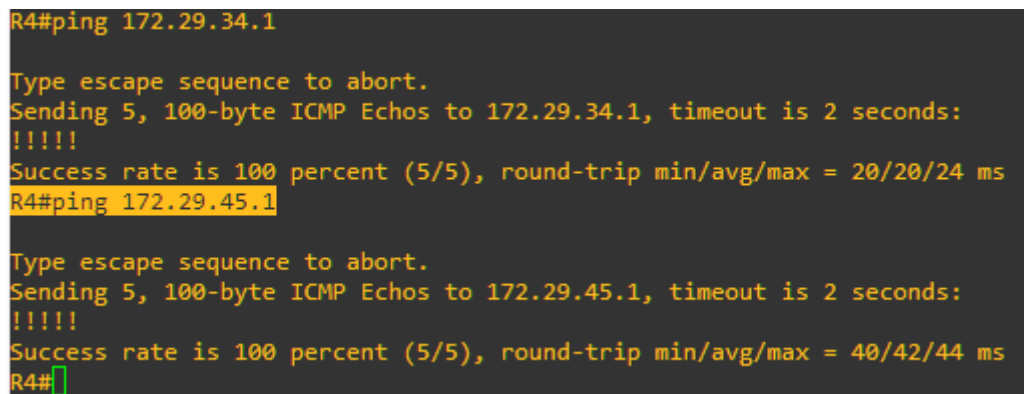
Una vez configurados los routers se procede a verificar la comunicación entre los router R1 a R4 y sus vecinos mediante el uso OSPF, de la misma forma entre R4 y R5 usando EIGRP.

Figura 2. Captura de pantalla de Ping entre R1 y R4



```
R1#ping 10.103.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/22/32 ms
R1#ping 172.29.34.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.34.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/44/48 ms
R1#
```

Figura 3. Captura de pantalla de ping entre R4 y R5



```
R4#ping 172.29.34.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.34.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
R4#ping 172.29.45.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.45.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/44 ms
R4#
```

1.2. CREACIÓN DE INTERFACES LOOPBACK EN R1

Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Para crear las 4 interfaces Loopback es necesario que cada una de ellas tenga su propia dirección de red, a continuación, se describe el procedimiento para su creación:

Se hace la conversión a binario de la dirección IP de la red y la máscara de subred.

$$\begin{aligned} 10.1.0.0 &= 00001010.00000001.00000000.00000000 \\ 255.255.252.0 &= 11111111.11111111.11111100.00000000 \end{aligned}$$

Luego se ponen en ceros los bits de la porción de host para obtener el valor binario de la red:

$$10.1.0.0/22 = 00001010.00000001.00000000.00000000$$

Para obtener la dirección de broadcast de la red se ponen en uno todos los bits de la porción de host de la red.

$$10.1.3.255 = 00001010.00000001.00000011.11111111$$

Esto quiere decir que el rango de hosts de la red se encuentra entre todos aquellos valores que existen entre la red y la dirección broadcast:

$$\begin{aligned} 10.1.0.1 &= 00001010.00000001.00000000.00000001 \\ 10.1.3.254 &= 00001010.00000001.00000011.11111110 \end{aligned}$$

Con base en lo anterior se determinan las siguientes direcciones de red:

Tabla 1. Direcciones de red para Loopback requeridas en el router R1

Dirección	Binario
10.1.0. 0/24	00001010.00000001.00000000.00000000
10.1. 1. 0/24	00001010.00000001.00000001.00000000
10.1. 2. 0/24	00001010.00000001.00000010.00000000
10.1. 3. 0/24	00001010.00000001.00000011.00000000

Con estas direcciones se procede a configurar el Loopback para R1 así:

```
R1# configure terminal
R1(config)# interface Loopback 1
R1(config-if)# ip address 10.1.0.1 255.255.255.0
R1(config)# interface Loopback 2
```

```

R1(config-if)# ip address 10.1.1.2 255.255.255.0
R1(config)# interface Loopback 3
R1(config-if)# ip address 10.1.2.3 255.255.255.0
R1(config)# interface Loopback 4
R1(config-if)# ip address 10.1.3.4 255.255.255.0
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# network 10.1.0.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.2.0 0.0.0.255 area 0
R1(config-router)# network 10.1.3.0 0.0.0.255 area 0

```

Finalmente, en la siguiente captura de pantalla se evidencia la creación de las interfaces Loopback en el R1, mediante el uso del comando **show ip route**, él demuestra la configuración explicada anteriormente.

Figura 4. Captura de pantalla, comprobación de creación de interfaces Loopback en R1, mediante el comando show ip route. Tomada del programa GNS3

```

R1#
*Jul 12 14:38:27.291: %SYS-5-CONFIG_I: Configured from console by console
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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
C       10.1.0.0/24 is directly connected, Loopback1
L       10.1.0.1/32 is directly connected, Loopback1
C       10.1.1.0/24 is directly connected, Loopback2
L       10.1.1.2/32 is directly connected, Loopback2
C       10.1.2.0/24 is directly connected, Loopback3
L       10.1.2.3/32 is directly connected, Loopback3
C       10.1.3.0/24 is directly connected, Loopback4
L       10.1.3.4/32 is directly connected, Loopback4
C       10.103.12.0/24 is directly connected, Serial3/0
L       10.103.12.1/32 is directly connected, Serial3/0
O       10.103.23.0/24 [110/128] via 10.103.12.2, 00:47:11, Serial3/0
172.29.0.0/24 is subnetted, 1 subnets
O       172.29.34.0 [110/192] via 10.103.12.2, 00:45:23, Serial3/0
R1#

```

1.3. CREACIÓN DE INTERFACES LOOPBACK EN R5

Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

Teniendo en cuenta el procedimiento explicado anteriormente se configuran las siguientes 4 direcciones de Loopback para el router 5.

Tabla 2. Direcciones de red para Loopback requeridas en el router R5

Dirección	Binario
172.5.0.0/24	10101100.00000101.00000000.00000000
172.5.1.0/24	10101100.00000101.00000001.00000000
172.5.2.0/24	10101100.00000101.00000010.00000000
172.5.3.0/24	10101100.00000101.00000011.00000000

Con estas direcciones se procede a configurar el Loopback para R1 así:

```
R5# configure terminal
R5(config)# interface Loopback 1
R5(config-if)# ip address 172.5.0.1 255.255.255.0
R5(config)# interface Loopback 2
R5(config-if)# ip address 172.5.1.2 255.255.255.0
R5(config)# interface Loopback 3
R5(config-if)# ip address 172.5.2.3 255.255.255.0
R5(config)# interface Loopback 4
R5(config-if)# ip address 172.5.3.4 255.255.255.0
R5(config-if)# exit
```

```
R5(config)# router eigrp 10
R5(config-router)# network 172.5.0.0 0.0.0.255
R5(config-router)# network 172.5.1.0 0.0.0.255
R5(config-router)# network 172.5.2.0 0.0.0.255
R5(config-router)# network 172.5.3.0 0.0.0.255
```

Finalmente, en la siguiente captura de pantalla se evidencia la creación de las interfaces Loopback en el R1, mediante el uso del comando **show ip route**, él demuestra la configuración explicada anteriormente.

Figura 5. Captura de pantalla, comprobación de creación de interfaces Loopback en R5, mediante el comando show ip route. Tomada del programa GNS3

```
*Jul 12 16:22:45.335: %SYS-5-CONFIG_I: Configured from console by console
R5#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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

    172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.5.0.0/24 is directly connected, Loopback1
L       172.5.0.1/32 is directly connected, Loopback1
C       172.5.1.0/24 is directly connected, Loopback2
L       172.5.1.2/32 is directly connected, Loopback2
C       172.5.2.0/24 is directly connected, Loopback3
L       172.5.2.3/32 is directly connected, Loopback3
C       172.5.3.0/24 is directly connected, Loopback4
L       172.5.3.4/32 is directly connected, Loopback4
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.29.34.0/24 [90/2681856] via 172.29.45.1, 02:27:03, Serial3/0
C       172.29.45.0/24 is directly connected, Serial3/0
L       172.29.45.5/32 is directly connected, Serial3/0
R5#
```

1.4. ANÁLISIS DE LA TABLA DE ENRUTAMIENTO DE R3

Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

En la figura 6, se puede apreciar que al emitir el comando show ip route en el router 3, se muestran las direcciones de red correspondientes a las interfaces de Loopback creadas en R1, lo que evidencia que estas direcciones de red fueron aprendidas a través del protocolo de enrutamiento dinámico OSPF, de otra parte, es posible verificar que R3 alcanza estas redes a través del router 2, lo que indica que usa la red 10.103.23.0 que se encuentra conectada a la interfaz serial 3/0 del dispositivo.

Figura 6. Captura de pantalla, aprendizaje de interfaces Loopback en R3, mediante el comando show ip route. Tomada del programa GNS3

```

*Jul 12 16:32:56.451: %SYS-5-CONFIG_I: Configured from console by console
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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.1.0.1/32 [110/129] via 10.103.23.1, 01:54:52, Serial3/0
O       10.1.1.2/32 [110/129] via 10.103.23.1, 01:54:42, Serial3/0
O       10.1.2.3/32 [110/129] via 10.103.23.1, 01:54:42, Serial3/0
O       10.1.3.4/32 [110/129] via 10.103.23.1, 01:54:32, Serial3/0
O       10.103.12.0/24 [110/128] via 10.103.23.1, 02:40:55, Serial3/0
C       10.103.23.0/24 is directly connected, Serial3/0
L       10.103.23.2/32 is directly connected, Serial3/0

```

1.5. CONFIGURACIÓN R3 PARA REDISTRIBUIR LAS RUTAS EIGRP EN OSPF

Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

Para realizar este procedimiento se configura el router 3 de la siguiente forma:

```
R3# configure terminal
```

```
R3(config)# router ospf 1
```

```
R3(config-router)# redistribute eigrp 10 metric 50000 subnets
```

```
R3(config-if)# exit
```

```
R3(config)# router eigrp 10
```

```
R3(config-router)# redistribute ospf 1 metric 1544 20000 255 1 1500
```

Figura 7. Captura de pantalla configuración de R3. Tomada del programa GNS3

```

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 10 metric 50000 subnets
R3(config-router)#exit
R3(config)#router eigrp 10
R3(config-router)#redistribute ospf 1 metric 1544 20000 255 1500
^
% Invalid input detected at '^' marker.

R3(config-router)#redistribute ospf 1 metric 1544 20000 2551500
^
% Invalid input detected at '^' marker.

R3(config-router)#redistribute ospf 1 metric 1544 20000 255 1 1500
R3(config-router)#

```

1.6. VERIFICACIÓN DE EXISTENCIA EN R1 Y R5 DE LAS RUTAS DEL SISTEMA AUTÓNOMO OPUESTO

Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.

En la figura 8 se puede apreciar que la tabla de enrutamiento del router R1 presenta:

- Las 2 subredes asignadas a los routers R4 y R5 (172.29.0.0/24).
- Las 4 subredes configuradas en las interfaces de Loopback (172.5.0.0/24) creadas en el router R5. Mediante EIGRP (AS 10).
- Se muestra que R1 aprendió estas nuevas rutas mediante enlaces externos del protocolo OSPF. Gracias a la redistribución de las rutas EIGRP configurada en R3
- Se aprecia que, que R1 identifica como próximo salto para alcanzar estas rutas a la interfaz serial 3/0, la cual lo conecta directamente a R2 a través de la IP 10.103.12.1
- Finalmente, la red 10.103.23.0/24, ruta que conecta a R2 y R3, también ha sido aprendida mediante OSPF.

Figura 8. Captura de pantalla, verificación de existencia en R1 de las rutas del sistema autónomo opuesto, mediante el comando show ip route y show ip ospf database. Tomada del programa GNS3

```
R1#show ip ospf database
      OSPF Router with ID (10.103.12.1) (Process ID 1)

      Router Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum Link count
10.103.12.1    10.103.12.1  312          0x80000000    0x007223 6
10.103.23.1    10.103.23.1  1206        0x80000008    0x002051 4
172.29.34.1    172.29.34.1  946         0x80000008    0x007F69 3

      Type-5 AS External Link States

Link ID        ADV Router    Age           Seq#           Checksum Tag
172.5.0.0      172.29.34.1  946          0x80000001    0x0033CE 0
172.5.1.0      172.29.34.1  946          0x80000001    0x0028D8 0
172.5.2.0      172.29.34.1  946          0x80000001    0x001DE2 0
172.5.3.0      172.29.34.1  946          0x80000001    0x0012EC 0
172.29.45.0    172.29.34.1  946          0x80000001    0x00219B 0
```

```

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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
C       10.1.0.0/24 is directly connected, Loopback1
L       10.1.0.1/32 is directly connected, Loopback1
C       10.1.1.0/24 is directly connected, Loopback2
L       10.1.1.2/32 is directly connected, Loopback2
C       10.1.2.0/24 is directly connected, Loopback3
L       10.1.2.3/32 is directly connected, Loopback3
C       10.1.3.0/24 is directly connected, Loopback4
L       10.1.3.4/32 is directly connected, Loopback4
C       10.103.12.0/24 is directly connected, Serial3/0
L       10.103.12.1/32 is directly connected, Serial3/0
O       10.103.23.0/24 [110/128] via 10.103.12.2, 03:00:46, Serial3/0
    172.5.0.0/24 is subnetted, 4 subnets
O E2    172.5.0.0 [110/50000] via 10.103.12.2, 00:10:58, Serial3/0
O E2    172.5.1.0 [110/50000] via 10.103.12.2, 00:10:59, Serial3/0
O E2    172.5.2.0 [110/50000] via 10.103.12.2, 00:11:00, Serial3/0
O E2    172.5.3.0 [110/50000] via 10.103.12.2, 00:11:00, Serial3/0
    172.29.0.0/24 is subnetted, 2 subnets
O       172.29.34.0 [110/192] via 10.103.12.2, 02:58:59, Serial3/0
O E2    172.29.45.0 [110/50000] via 10.103.12.2, 00:11:02, Serial3/0
R1#

```

En la tabla del router 5 se puede apreciar:

- Las 2 redes que conectan los routers: R1 a R2 y R2 a R3 (10.103.12.0/24 y 10.103.23.0/24 respectivamente).
- Las 4 subredes correspondientes a las interfaces Loopback (172.5.0.0/24) configuradas en el router R1 y enrutadas mediante el protocolo OSPF (Área 0).
- Muestra que R5 aprendió estas nuevas rutas mediante enlaces externos del protocolo EIGRP, gracias a la redistribución de las rutas OSPF configurada en R3.
- Contiene la red que conecta los routers R3 y R4 la cual se identifica como vecina mediante el protocolo EIGRP.
- R5 designa como próximo salto para alcanzarlas todas estas rutas, a la interfaz serial 3/0 que lo conecta de forma directa con el router R3 a través de la dirección IP 172.29.45.1.

Figura 9. Captura de pantalla, verificación de existencia en R5 de las rutas del sistema autónomo opuesto, mediante el comando show ip route y show ip eigrp topology. Tomada del programa GNS3

```
R5#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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D EX  10.1.0.1/32 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
D EX  10.1.1.2/32 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
D EX  10.1.2.3/32 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
D EX  10.1.3.4/32 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
D EX  10.103.12.0/24 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
D EX  10.103.23.0/24 [170/7801856] via 172.29.45.1, 00:20:43, Serial3/0
172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C     172.5.0.0/24 is directly connected, Loopback1
L     172.5.0.1/32 is directly connected, Loopback1
C     172.5.1.0/24 is directly connected, Loopback2
L     172.5.1.2/32 is directly connected, Loopback2
C     172.5.2.0/24 is directly connected, Loopback3
L     172.5.2.3/32 is directly connected, Loopback3
C     172.5.3.0/24 is directly connected, Loopback4
L     172.5.3.4/32 is directly connected, Loopback4
172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D     172.29.34.0/24 [90/2681856] via 172.29.45.1, 03:08:19, Serial3/0
C     172.29.45.0/24 is directly connected, Serial3/0
L     172.29.45.5/32 is directly connected, Serial3/0
R5#
```

```

R5#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(172.29.45.5)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.1.0.1/32, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 10.1.2.3/32, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 10.103.23.0/24, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 172.29.34.0/24, 1 successors, FD is 2681856
   via 172.29.45.1 (2681856/2169856), Serial3/0
P 10.1.3.4/32, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 172.29.45.0/24, 1 successors, FD is 2169856
   via Connected, Serial3/0
P 10.103.12.0/24, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 10.1.1.2/32, 1 successors, FD is 7801856
   via 172.29.45.1 (7801856/7289856), Serial3/0
P 172.5.0.0/24, 1 successors, FD is 128256
   via Connected, Loopback1
P 172.5.2.0/24, 1 successors, FD is 128256
   via Connected, Loopback3
P 172.5.3.0/24, 1 successors, FD is 128256
   via Connected, Loopback4
P 172.5.1.0/24, 1 successors, FD is 128256
   via Connected, Loopback2

```

Figura 10. Verificación de comunicación desde R1 hasta R5. Imagen tomada del programa GNS3.

```

R1#ping 172.5.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/86/88 ms
R1#ping 172.5.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.2.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/85/88 ms
R1#ping 172.5.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.3.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/84/88 ms
R1#ping 172.29.45.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.45.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
R1#

```

```
R5#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
R5#ping 10.1.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/62/68 ms
R5#ping 10.1.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/84/88 ms
R5#ping 10.103.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.12.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/53/56 ms
R5#
```

Las anteriores imágenes demuestran que se logró la comunicación en toda la red configurada desde R1 hacia las interfaces Loopback y serial de R5 así como desde R5 hacia las interfaces Loopback y serial de R1, que se implementaron exitosamente los protocolos de enrutamiento dinámico OSPF y EIGRP; de acuerdo al planteamiento del escenario 1.

2. ESCENARIO 2

Topología

Para el desarrollo de esta actividad se utilizan router C7200 configurados y simulados en el programa GNS3.

Figura 11. Topología de red propuesta para el escenario 2. Captura tomada del programa GNS3.

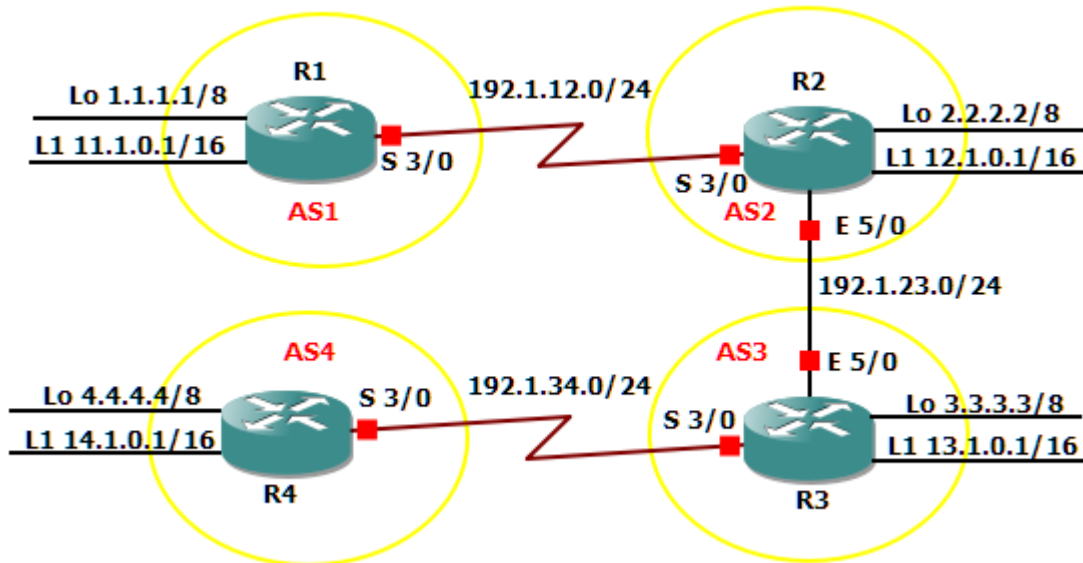


Tabla 3. Configuración de los router. Escenario 2

R1		
Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0
R2		
Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0
R3		
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

R4		
Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

2.1. RELACIÓN DE VECINO BGP ENTRE R1 Y R2

Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

De acuerdo a lo solicitado se configura R1 de la siguiente forma:

```
R1# configure terminal
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# interface Loopback 1
R1(config-if)# ip address 11.1.0.1 255.255.0.0
R1(config-if)# interface serial 3/0
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# router bgp 1
R1(config-router)# bgp router-id 11.11.11.11
R1(config-router)# network 1.0.0.0 mask 255.0.0.0
R1(config-router)# network 11.1.0.0 mask 255.255.0.0
R1(config-router)# network 192.1.12.0 mask 255.255.255.0
R1(config-router)# neighbor 192.1.12.2 remote-as 2
```

Ahora se procede a configurar R2 así:

```
R2# configure terminal
R2(config)# interface Loopback 0
R2(config-if)# ip address 2.2.2.2 255.0.0.0
R2(config-if)# interface Loopback 1
R2(config-if)# ip address 12.1.0.1 255.255.0.0
R2(config-if)# interface serial 3/0
R2(config-if)# ip address 192.1.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface fastEthernet 5/0
R2(config-if)# ip address 192.1.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# router bgp 2
```

```

R2(config-router)# bgp router-id 22.22.22.22
R2(config-router)# network 2.0.0.0 mask 255.0.0.0
R2(config-router)# network 12.1.0.0 mask 255.255.0.0
R2(config-router)# network 192.1.12.0 mask 255.255.255.0
R2(config-router)# neighbor 192.1.12.1 remote-as 1

```

En las siguientes capturas de pantalla del programa GNS3 se puede apreciar la tabla de direccionamiento de acuerdo a las especificaciones solicitadas para el escenario 2, de la misma forma se aprecian las interfaces Loopback las cuales se identifican mediante el código B, lo que hace suponer que fueron aprendidas mediante el protocolo BGP. Finalmente se verifica que la ruta de direccionamiento 192.1.12.0/24 es la que utilizan los dos router para comunicarse ya que es la que se encuentra físicamente conectada a los dos dispositivos.

Figura 12. Verificación de relación de vecino BGP entre R1 y R2, mediante el uso del comando show ip route.

```

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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

 1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    1.0.0.0/8 is directly connected, Loopback0
L    1.1.1.1/32 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:01:51
 11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    11.1.0.0/16 is directly connected, Loopback1
L    11.1.0.1/32 is directly connected, Loopback1
 12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.12.2, 00:01:51
 192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial3/0
L    192.1.12.1/32 is directly connected, Serial3/0
R1#

```

```

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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:03:01
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     2.0.0.0/8 is directly connected, Loopback0
L     2.2.2.2/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B     11.1.0.0 [20/0] via 192.1.12.1, 00:03:01
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     12.1.0.0/16 is directly connected, Loopback1
L     12.1.0.1/32 is directly connected, Loopback1
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.1.12.0/24 is directly connected, Serial3/0
L     192.1.12.2/32 is directly connected, Serial3/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.1.23.0/24 is directly connected, FastEthernet5/0
L     192.1.23.2/32 is directly connected, FastEthernet5/0
R2#

```

2.2. RELACIÓN DE VECINO BGP ENTRE R2 Y R3

Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33. Presente el paso a) con los comandos utilizados y la salida del comando show ip route.

Para configurar el R2 se utilizan los siguientes comandos:

```

R2# configure terminal
R2(config)# router bgp 2
R2(config-router)# network 192.1.23.0 mask 255.255.255.0
R2(config-router)# neighbor 192.1.23.3 remote-as 3

```

En el R3 se utiliza la siguiente configuración:

```

R3# configure terminal
R3(config)# interface Loopback 0
R3(config-if)# ip address 3.3.3.3 255.0.0.0
R3(config-if)# interface Loopback 1
R3(config-if)# ip address 13.1.0.1 255.255.0.0
R3(config-if)# interface fastEthernet 5/0
R3(config-if)# ip address 192.1.23.3 255.255.255.0

```

```
R3(config-if)# no shutdown
R3(config-if)# interface serial 3/0
R3(config-if)# ip address 192.1.34.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# router bgp 3
R3(config-router)# bgp router-id 33.33.33.33
R3(config-router)# network 3.0.0.0 mask 255.0.0.0
R3(config-router)# network 13.1.0.0 mask 255.255.0.0
R3(config-router)# network 192.1.23.0 mask 255.255.255.0
R3(config-router)# neighbor 192.1.23.2 remote-as 2
```

En la figura 13 gracias a la emisión del comando **show ip route** se puede apreciar la actualización de la tabla de enrutamiento para el router 2, en donde se muestran las direcciones de Loopback configuradas para el router 3, lo que indica que ha aprendido 4 direcciones o rutas mediante el uso del protocolo BGP; éstas se pueden identificar con la letra B.

También es posible ver las redes que están conectadas a R3, bien sea en los interfaces Loopback o las que comunican los routers R3 y R4, en los puertos fastEthernet 5/0 y serial 3/0; de la misma manera se evidencia la actualización de las direcciones en las interfaces Loopback que fueron configuradas en R2 y R1, luego esto quiere decir que las aprendió gracias al protocolo BGP, debido a la adyacencia con R2 ya que estas redes fueron anunciadas en cada uno de los routers. Otro aspecto importante que se puede apreciar es que R3 muestra la dirección de red que conecta los routers R1 y R2, esto gracias nuevamente al protocolo BGP.

Finalmente es posible verificar que R3 detecta todas estas redes mediante la interfaz fastEthernet 5/0 conectada con R2 (192.1.23.0/24)

Figura 13. Verificación de relación de vecino BGP entre R2 y R3, mediante el uso del comando show ip route.

```
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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:10:04
C    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:01:05
C    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:10:04
C    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
C    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:01:05
C    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.12.0/24 is directly connected, Serial3/0
L    192.1.12.2/32 is directly connected, Serial3/0
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.23.0/24 is directly connected, FastEthernet5/0
L    192.1.23.2/32 is directly connected, FastEthernet5/0
R2#
```

```
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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:02:13
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:02:13
C    3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    3.0.0.0/8 is directly connected, Loopback0
L    3.3.3.3/32 is directly connected, Loopback0
C    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:02:13
C    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:02:13
C    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:02:13
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.23.0/24 is directly connected, FastEthernet5/0
L    192.1.23.3/32 is directly connected, FastEthernet5/0
R3#
```

2.3. RELACIÓN DE VECINO BGP ENTRE R3 Y R4

Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 44.44.44.44. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

En la configuración del router 3 se agregan los siguientes parámetros:

```
R3# configure terminal
R3(config)# router bgp 3
R3(config-router)# network 192.1.34.0 mask 255.255.255.0
R3(config-router)# neighbor 192.1.34.4 remote-as 4
```

Para el router 4 se realiza la siguiente configuración:

```
R4# configure terminal
R4(config)# interface Loopback 0
R4(config-if)# ip address 4.4.4.4 255.0.0.0
R4(config-if)# interface Loopback 1
R4(config-if)# ip address 14.1.0.1 255.255.0.0
R4(config-if)# interface serial 3/0
R4(config-if)# ip address 192.1.34.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# exit
R4(config)# router bgp 4
R4(config-router)# bgp router-id 44.44.44.44
R4(config-router)# network 4.0.0.0 mask 255.0.0.0
R4(config-router)# network 14.1.0.0 mask 255.255.0.0
R4(config-router)# network 192.1.34.0 mask 255.255.255.0
R4(config-router)# neighbor 192.1.34.3 remote-as 3
```

Es necesario que router vecino informe del uso de la interfaz, en vez de una interfaz física, para poder establecer las relaciones de adyacencia mediante las direcciones de Loopback, lo que implica una configuración adicional a cada router así:

```
R3# configure terminal
R3(config)# ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)# router bgp 3
R3(config-router)# no neighbor 192.1.34.4
R3(config-router)# no network 3.0.0.0 mask 255.0.0.0
R3(config-router)# neighbor 4.4.4.4 remote-as 4
R3(config-router)# neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
```

```

R4(config)# ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)# router bgp 4
R4(config-router)# no neighbor 192.1.34.3
R4(config-router)# neighbor 3.3.3.3 remote-as 4
R4(config-router)# neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop

```

En la figura 14 se puede apreciar la actualización de la tabla de direcciones en el router 3 y el cambio de dirección de red de conexión con R4, por lo que ahora corresponde al Loopback 0. Fenómeno que se da gracias a la configuración establecida; sin embargo, es importante recordar que la conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 5/0.

De otra parte, se evidencia el aprendizaje mediante el protocolo BGP de la interfaz Loopback 1, la diferencia radica en que esta vez lo hace a través la interfaz Loopback 0 de R4 (4.4.4.4). los otros routers vecinos no fueron alterados y esto se verifica en la tabla de enrutamiento.

En el router 4 ha cambiado la dirección de comunicación con sus vecinos, por lo que ahora lo hace usando la interfaz Loopback 0 de R3. Igualmente aparece la ruta estática creada en el router 3.

Figura 14. Verificación de relación de vecino BGP entre R3 y R4, mediante el uso del comando show ip route.

```

R4#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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
L    14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
L    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial3/0
L    192.1.34.4/32 is directly connected, Serial3/0

```

```

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
       i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:11:18
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:11:18
     3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      3.0.0.0/8 is directly connected, Loopback0
L      3.3.3.3/32 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
     11.0.0.0/16 is subnetted, 1 subnets
B      11.1.0.0 [20/0] via 192.1.23.2, 00:11:18
     12.0.0.0/16 is subnetted, 1 subnets
B      12.1.0.0 [20/0] via 192.1.23.2, 00:11:18
     13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      13.1.0.0/16 is directly connected, Loopback1
L      13.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:10:48
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.1.23.0/24 is directly connected, FastEthernet5/0
L      192.1.23.3/32 is directly connected, FastEthernet5/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.1.34.0/24 is directly connected, Serial3/0
L      192.1.34.3/32 is directly connected, Serial3/0
R3#

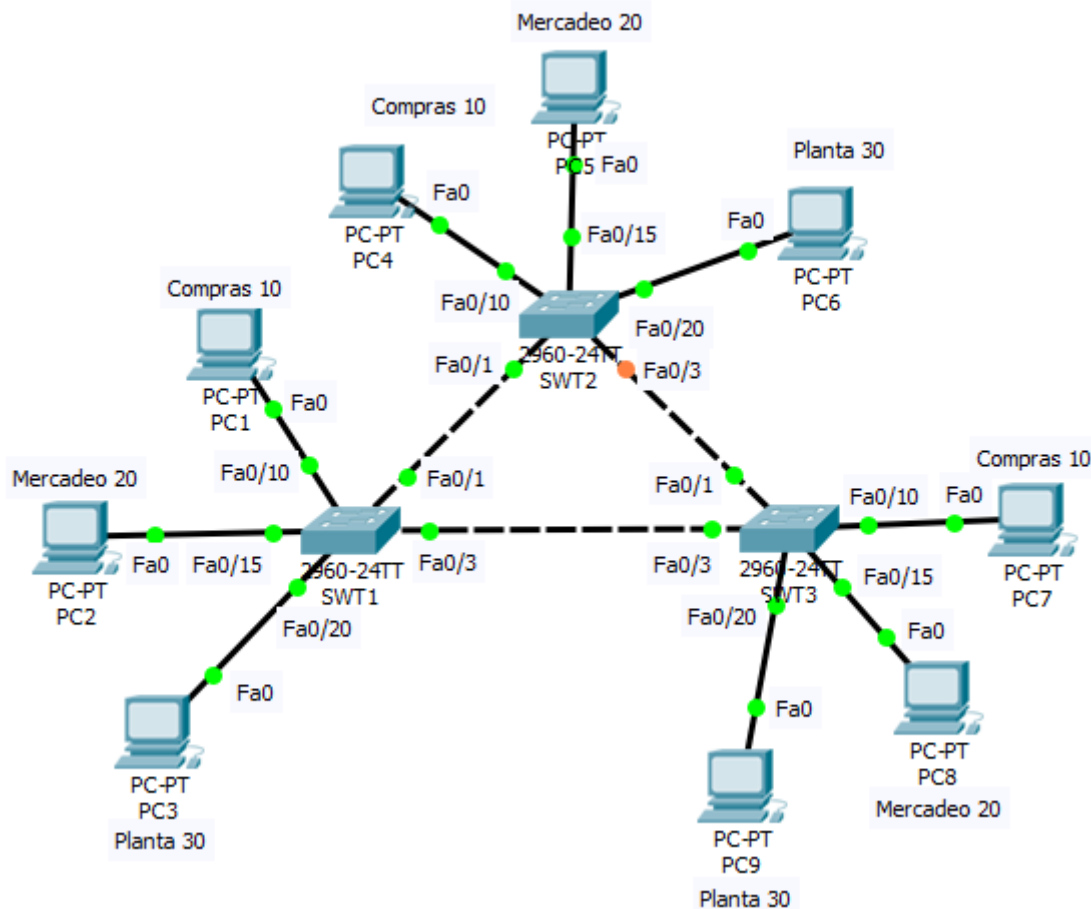
```

3. ESCENARIO 3

Topología.

Para el desarrollo de esta actividad se trabaja en el simulador Packet Tracer, utilizando swiches 2960.

Figura 15. Topología de red propuesta para el escenario 3. Captura tomada del programa Packet Tracer.



A. CONFIGURAR VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

De acuerdo a lo anterior se parametriza cada switch con las siguientes instrucciones:

SWT1.

```
SWT1# configure terminal
SWT1(config)# vtp mode client
Setting device to VTP CLIENT mode.
```

```
SWT1(config)# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT1(config)# vtp password cisco
Setting device VLAN database password to cisco
```

SWT2.

```
SWT2# configure terminal
SWT2(config)# vtp mode server
Setting device to VTP SERVER mode.
SWT2(config)# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT2(config)# vtp password cisco
Setting device VLAN database password to cisco
```

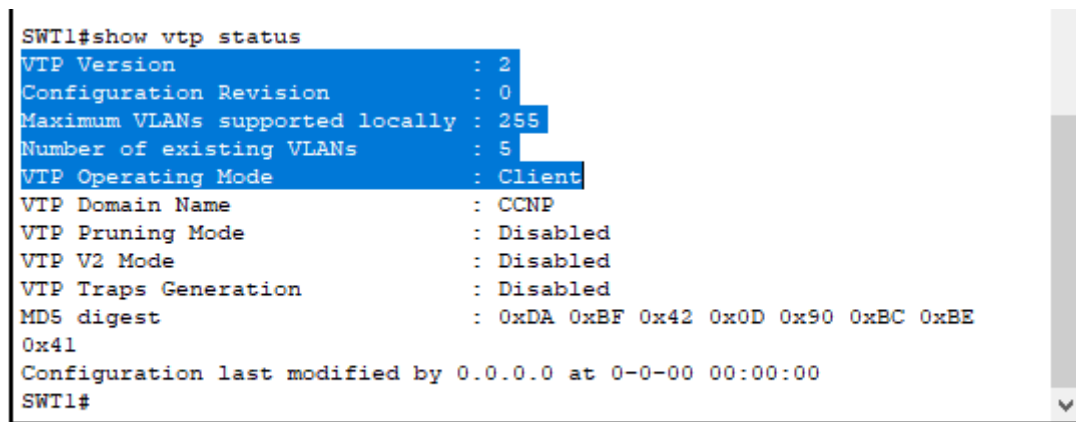
SWT3.

```
SWT3# configure terminal
SWT3(config)# vtp mode client
Setting device to VTP CLIENT mode.
SWT3(config)# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT13(config)# vtp password cisco
Setting device VLAN database password to cisco
```

2. Verifique las configuraciones mediante el comando show vtp status.

La figura 16 muestra las capturas de pantalla de cada uno de los switch según los parámetros solicitados.

Figura 16. Verificación de configuraciones en SWT1, SWT2 y SWT3. Captura de pantalla tomada del programa Packet Tracer



```
SWT1#show vtp status
VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Client
VTP Domain Name       : CCNP
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MD5 digest             : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWT1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
SWT2#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name : CCNE
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SWT2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

```
SWT3#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name : CCNE
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWT3#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

B. CONFIGURAR DTP (DYNAMIC TRUNKING PROTOCOL)

1. Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Para realizar la configuración se parametriza el SWT2 de la siguiente forma:

```
SWT2# configure terminal
SWT2(config)# interface fastEthernet 0/1
SWT2(config-if)# switchport mode dynamic desirable
```

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

La figura 17 muestra la configuración solicitada para SWT1 y SWT2

Figura 17. Verificación de enlace "trunk" entre SWT1 y SWT2. Captura tomada del programa Packet Tracer

```
SWT1#show interfaces trunk
Port      Mode           Encapsulation  Status        Native vlan
Fa0/1     auto           n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

SWT1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
SWT2(config-if)#do show interfaces trunk
Port      Mode           Encapsulation  Status        Native vlan
Fa0/1     desirable      n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

SWT2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

- Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SWT1.

Para lograr lo solicitado se procede a parametrizar el STW1 de la siguiente forma:

```
SWT1# configure terminal
SWT1(config)# interface fastEthernet 0/3
SWT1(config-if)# switchport mode trunk
```

- Verifique el enlace "trunk" con el comando show interfaces trunk en SWT1. La figura 18 muestra la captura de pantalla con el procedimiento solicitado.

Figura 18. Verificación de enlace "trunk" en SWT1. Captura tomada del programa Packet Tracer

```
SWT1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto     n-802.1q      trunking    1
Fa0/3     on       802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     none

SWT1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

5. Configure un enlace "trunk" permanente entre SWT2 y SWT3.

Para lograr este procedimiento se requiere configurar SWT3 de la siguiente forma:

```
SWT3# configure terminal
SWT3(config)# interface fastEthernet 0/1
SWT3(config-if)# switchport mode trunk
```

La figura 19 evidencia el enlace permanente solicitado entre SWT2 y SWT3.

Figura 19. Enlace permanente entre SWT2 y SWT3. Captura de pantalla tomada del programa Packet Tracer.

```

SWT2>en
SWT2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.lq       trunking    1
Fa0/3     auto      n-802.lq       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     none

SWT2#

```

Ctrl+F6 to exit CLI focus

Copy Paste

```

SWT3#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.lq         trunking    1
Fa0/3     auto      n-802.lq       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1

SWT3#

```

Ctrl+F6 to exit CLI focus

Copy Paste

C. AGREGAR VLANS Y ASIGNAR PUERTOS.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99). Para agregar las Vlan se procede a parametrizar los switch de la siguiente forma:

```

SWT1# configure terminal
SWT1(config)# vlan 10

```

```

SWT2# configure terminal
SWT2(config)# vlan 10
SWT2(config-vlan)# name Compras
SWT2(config-vlan)# vlan 20
SWT2(config-vlan)# name Mercadeo
SWT2(config-vlan)# vlan 30
SWT2(config-vlan)# name Planta
SWT2(config-vlan)# vlan 99
SWT2(config-vlan)# name Admon
SWT2(config-vlan)# exit

```

2. Verifique que las VLANs han sido agregadas correctamente.

La figura 20 muestra una captura de pantalla con la emisión del comando show vlan brief y la creación de las Vlan solicitadas.

Figura 20. Emisión del comando show vlan brief en SWT 1, 2 y 3. Captura de pantalla tomada del programa Packet Tracer.

```

SWT1#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trnet-default	active	

```

SWT1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

```
SWT2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWT2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
SWT3>en
SWT3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWT3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Tabla 4. Interfaz y direcciones IP para los PCs según las VLAN.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 20	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

Para cada pc la configuración sería la siguiente:

```
PC1: ip address 190.108.10.1 255.255.255.0
PC2: ip address 190.108.20.2 255.255.255.0
PC3: ip address 190.108.30.3 255.255.255.0
PC4: ip address 190.108.10.4 255.255.255.0
PC5: ip address 190.108.20.5 255.255.255.0
PC6: ip address 190.108.30.6 255.255.255.0
PC7: ip address 190.108.10.7 255.255.255.0
PC8: ip address 190.108.20.8 255.255.255.0
PC9: ip address 190.108.30.9 255.255.255.0
```

4. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.
5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba. De acuerdo con lo solicitado en el punto 4 y 5 se procede a configurar los switch 1, 2 y 3 de la siguiente forma:

```
SWT1# configure terminal
SWT1(config)# interface fastEthernet 0/10
SWT1(config-if)# switchport mode access
SWT1(config-if)# switchport access vlan 10
SWT1(config)# interface fastEthernet 0/15
SWT1(config-if)# switchport mode access
SWT1(config-if)# switchport access vlan 20
SWT1(config)# interface fastEthernet 0/20
SWT1(config-if)# switchport mode access
SWT1(config-if)# switchport access vlan 30
```

```
SWT2# configure terminal
SWT2(config)# interface fastEthernet 0/10
SWT2(config-if)# switchport mode access
SWT2(config-if)# switchport access vlan 10
SWT2(config)# interface fastEthernet 0/15
SWT2(config-if)# switchport mode access
SWT2(config-if)# switchport access vlan 20
SWT2(config)# interface fastEthernet 0/20
SWT2(config-if)# switchport mode access
SWT2(config-if)# switchport access vlan 30
```

```
SWT3#configure terminal
SWT3(config)# interface fastEthernet 0/10
SWT3(config-if)# switchport mode access
```

```

SWT3(config-if)# switchport access vlan 10
SWT3(config)# interface fastEthernet 0/15
SWT3(config-if)# switchport mode access
SWT3(config-if)# switchport access vlan 20
SWT3(config)# interface fastEthernet 0/20
SWT3(config-if)# switchport mode access
SWT3(config-if)# switchport access vlan 30

```

D. CONFIGURAR LAS DIRECCIONES IP EN LOS SWITCHES.

1. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 5. Direccionamiento de IP para SWT 1, 2 y 3.

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

Para configurar las direcciones ip se procede la siguiente forma:

```

SWT1# configure terminal
SWT1(config)# interface vlan 99
SWT1(config-if)# ip address 190.108.99.1 255.255.255.0

```

```

SWT2# configure terminal
SWT2(config)# interface vlan 99
SWT2(config-if)# ip address 190.108.99.2 255.255.255.0

```

```

SWT3# configure terminal
SWT3(config)# interface vlan 99
SWT3(config-if)# ip address 190.108.99.3 255.255.255.0

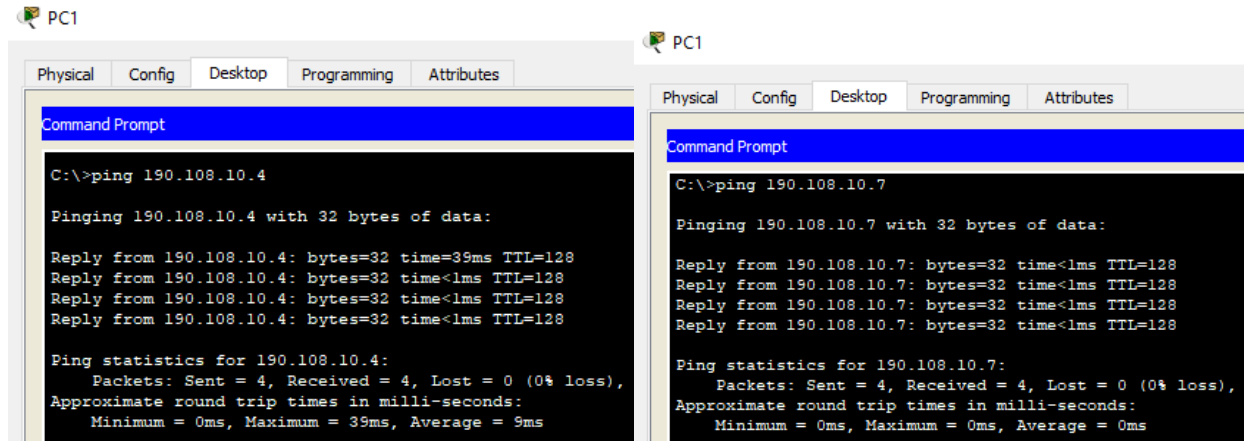
```

D. VERIFICAR LA CONECTIVIDAD EXTREMO A EXTREMO

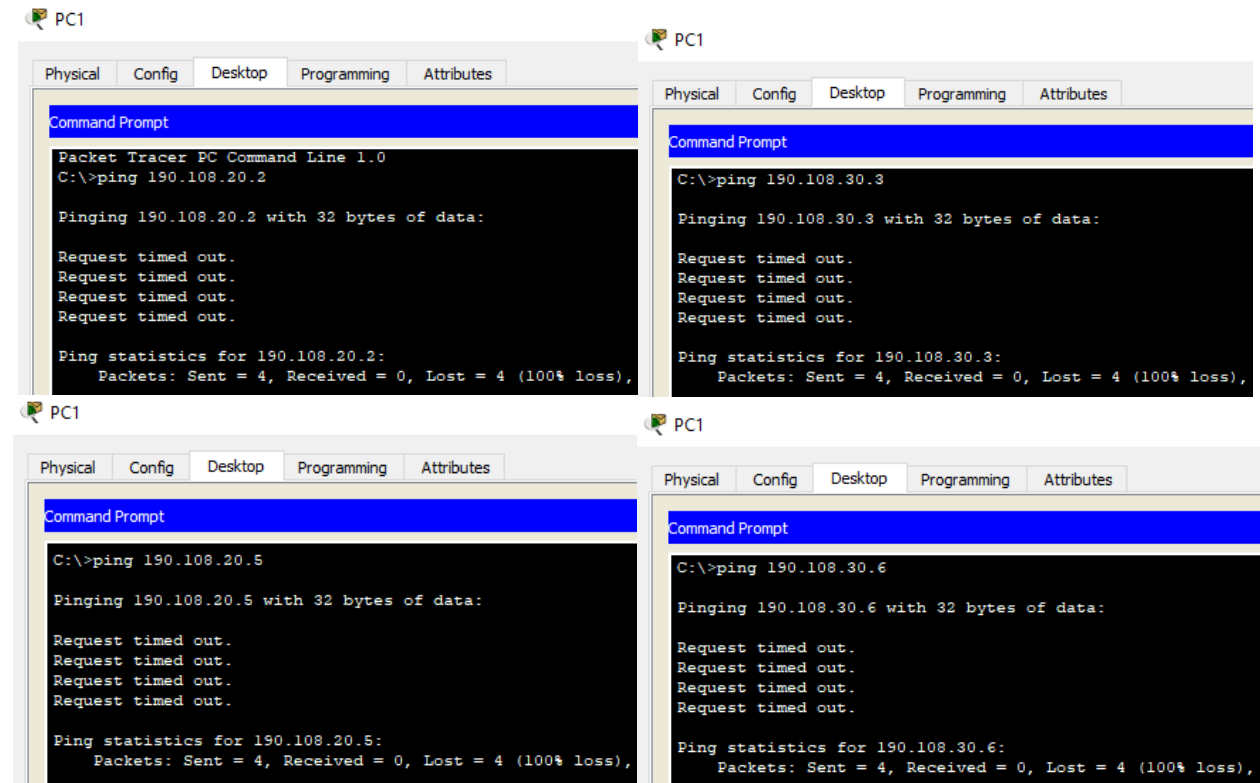
1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

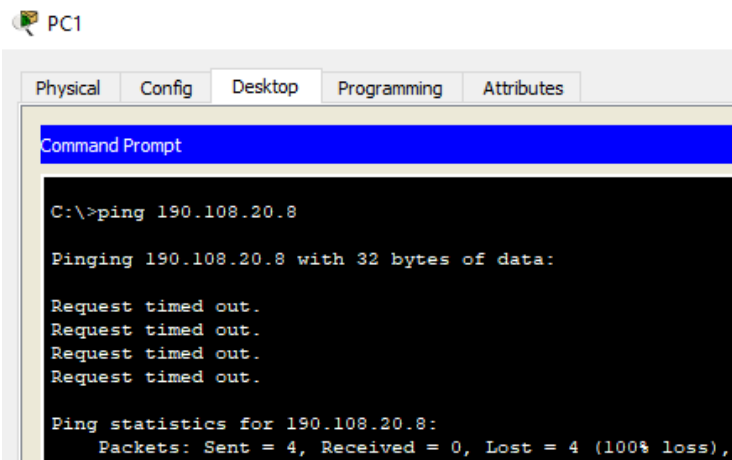
Desde PC1 se tuvo éxito con PC4 y PC7. Como se aprecia en la siguiente figura.

Figura 21. Ping desde PC1 a PC4 y PC7. Captura tomada del programa Packet Tracer.



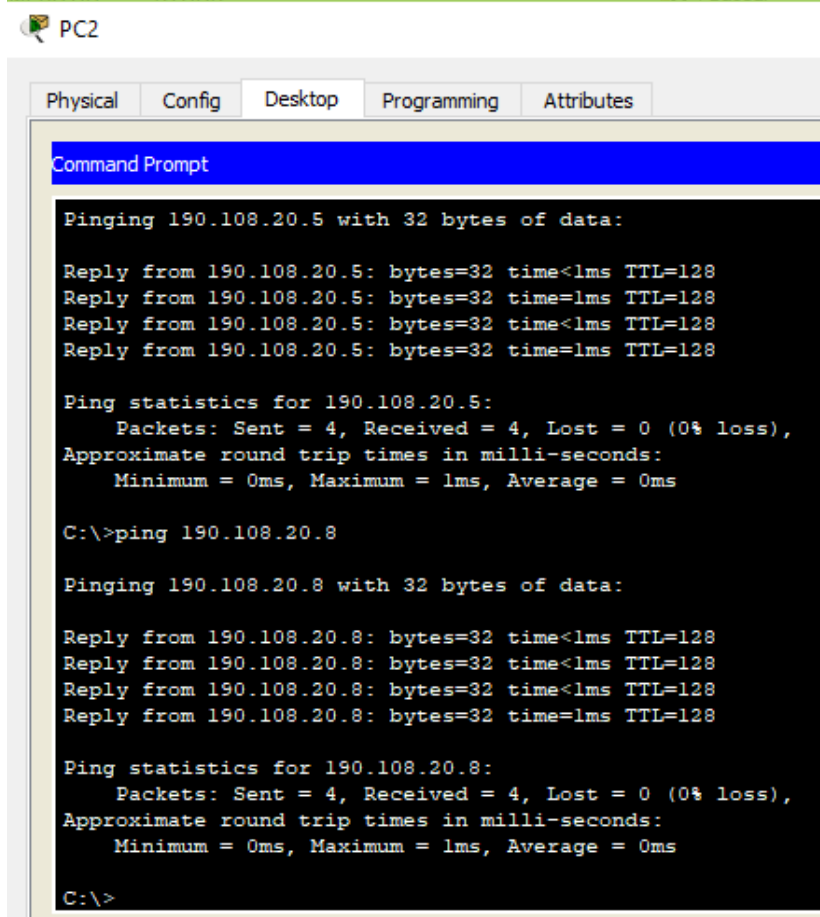
En las demás direcciones no hubo comunicación, como se evidencia en la figura 22. Figura 22. Ping desde PC1 a PC3, PC5, PC6, PC7, PC8 y PC9. Captura tomada del programa Packet Tracer.





Desde el PC2 se tuvo éxito con el PC5 y PC8, como se aprecia en la figura 23.

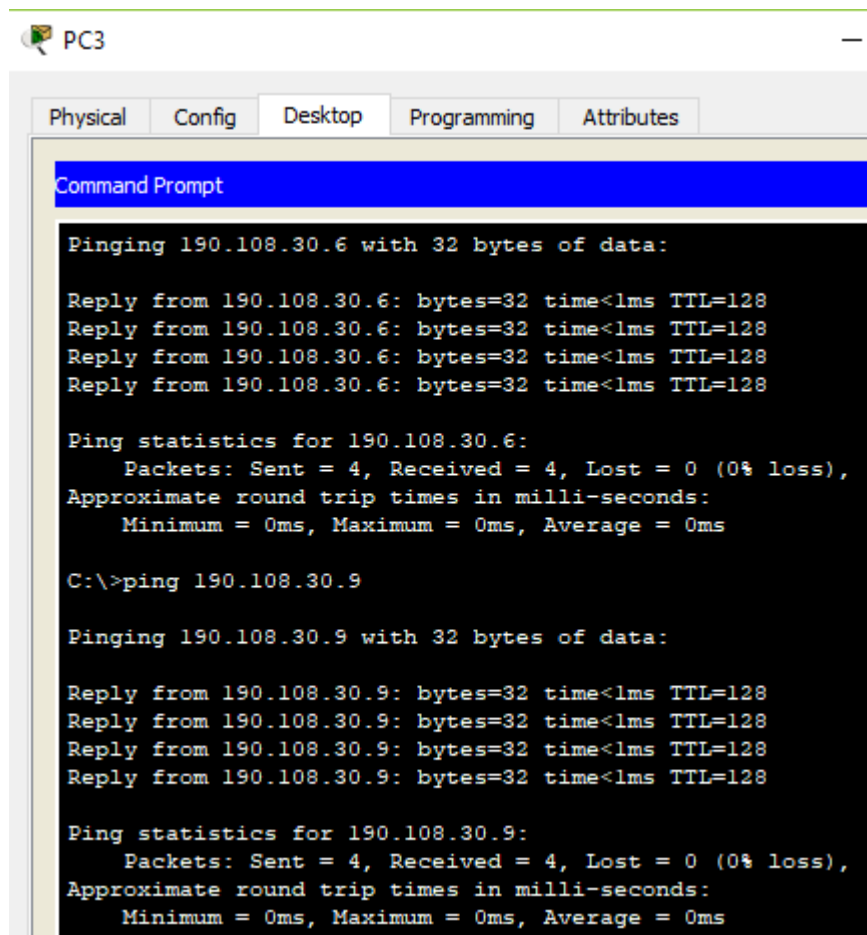
Figura 23. Ping desde PC2 a PC5 y PC8. Captura tomada del programa Packet Tracer.



Con las demás no hubo comunicación.

Desde el PC3 se tuvo éxito con los PCs 6 y 9, como se evidencia en la figura 24.

Figura 24. Ping desde PC3 a PC6 y PC9. Captura tomada del programa Packet Tracer.



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.30.6 with 32 bytes of data:
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Reply from 190.108.30.9: bytes=32 time<lms TTL=128
Reply from 190.108.30.9: bytes=32 time<lms TTL=128
Reply from 190.108.30.9: bytes=32 time<lms TTL=128
Reply from 190.108.30.9: bytes=32 time<lms TTL=128
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En las demás no hubo comunicación.

De lo anterior se puede inferir que el ping realizado entre los PCs interconectados a distintas Vlans no tuvo éxito, de otra parte, al hacer ping entre PCs que pertenecen a la misma Vlan, si tuvieron éxito.

La falta de comunicación o error en los PCs de diferentes Vlans se da porque cada computador ésta asociado a un segmento de red diferente. Es decir que, si se quiere establecer comunicación entre estos PCs, habría que incorporar en la red un Switch de capa 3 (Switch Multicapa), ya que éstos poseen la capacidad intrínseca de enrutamiento entre VLANs, con esto se logra comunicar el tráfico ICMP entre las diversas topologías planteadas de acuerdo con las tablas de enrutamiento para estos dispositivos.

2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

En la figura 25, 26 y 27 se puede apreciar que existe comunicación entre los distintos switches, debido a configuración en modo troncal de las interfaces físicas para el envío de datos mediante el protocolo ICPM, esto de acuerdo a lo comprobado mediante el comando show interfaces trunk, ya que intercambian el encapsulamiento.

Figura 25. Ping desde SWT1 a SWT2 Y SWT3. Captura tomada del programa Packet Tracer.

```
SWT1#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms

SWT1#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms

SWT1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 26. Ping desde SWT2 a SWT1 Y SWT3. Captura tomada del programa Packet Tracer.

```
SWT2#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms

SWT2#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
ms

SWT2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 27. Ping desde SWT3 a SWT1 Y SWT2. Captura tomada del programa Packet Tracer.

```
SWT3>en
SWT3#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms

SWT3#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5
ms

SWT3#
```

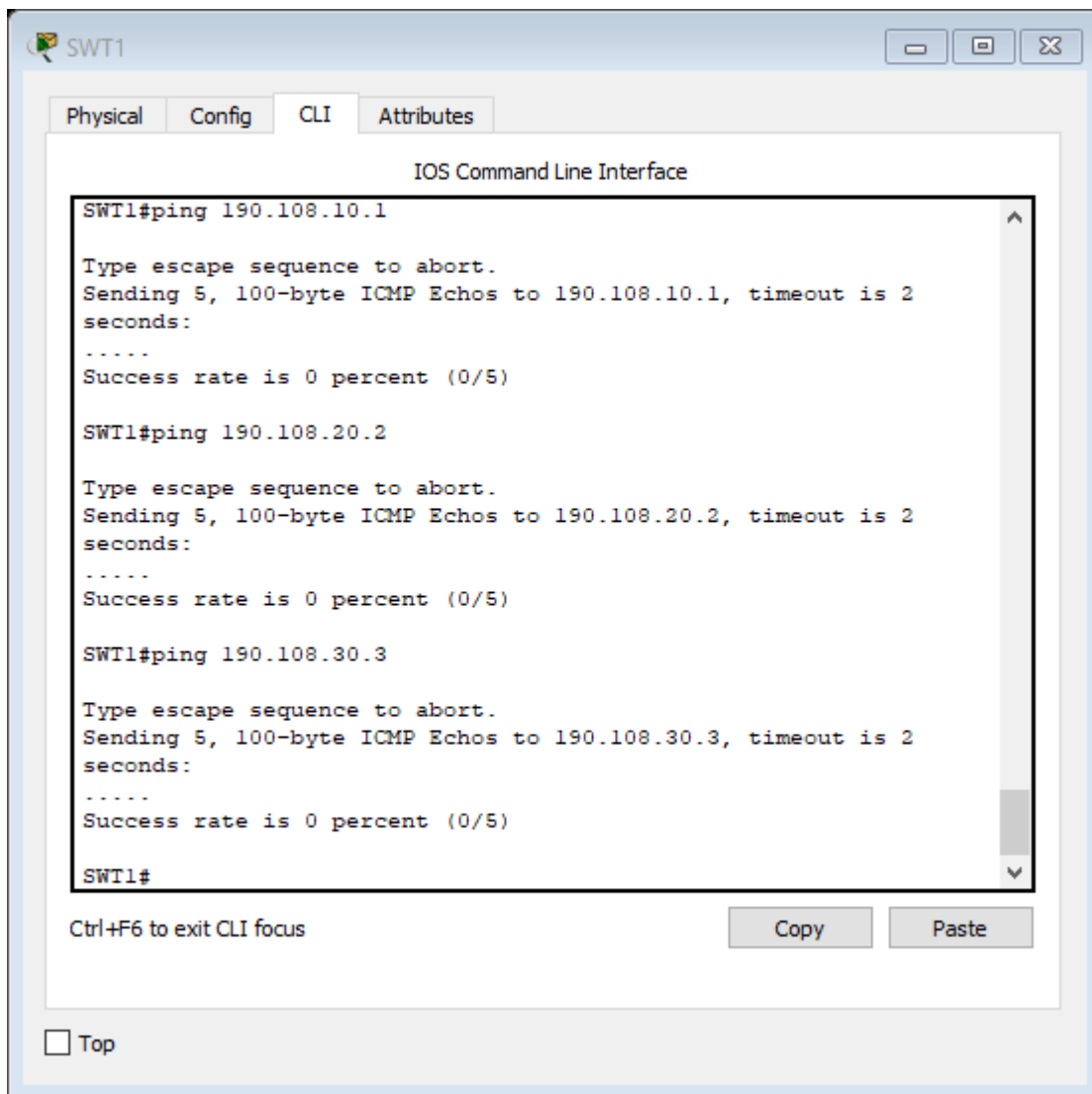
Ctrl+F6 to exit CLI focus

Copy Paste

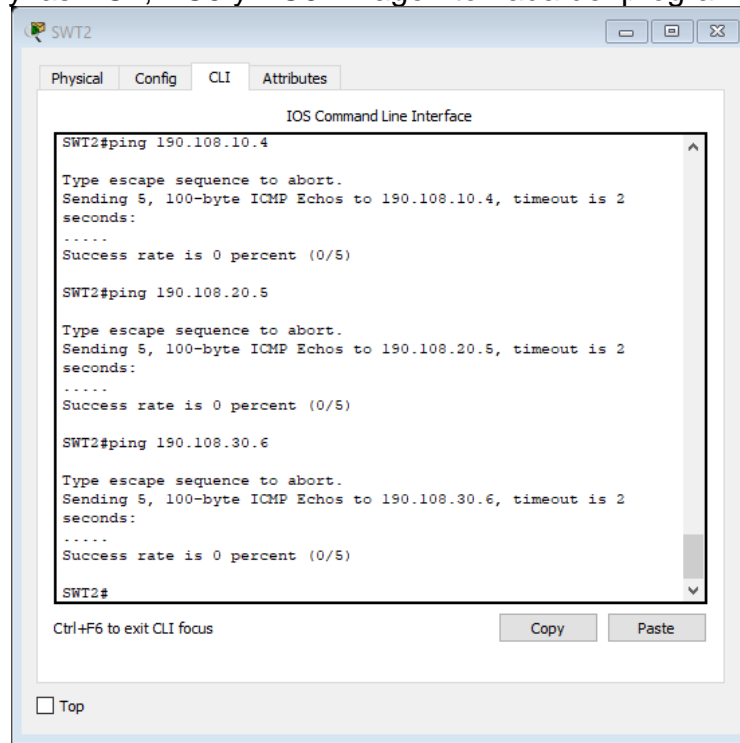
3. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

Al intentar hacer ping entre los Switch y las PCs, no se estableció la comunicación, esto es debido a que en la configuración de la red aún no se ha configurado un enrutamiento IP entre las VLAN Compras 10, Mercadeo 20 y planta 30, esto se logra al establecer una dirección IP, junto con la máscara subred en interfaz de VLAN de cada Switch y ésta debe pertenecer al mismo segmento de red del computador a comunicar con su respectiva VLAN, determinando la VLAN nativa en cada interfaz.

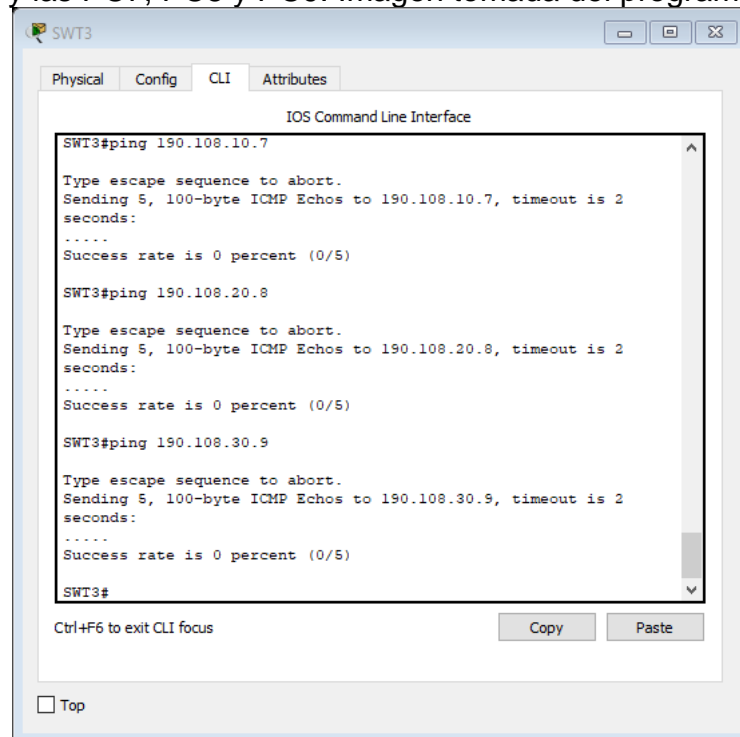
Figura 28. Ping entre SWT1 y las PC1, PC2 y PC3. Imagen tomada del programa Packet Tracer.



Ping entre SWT2 y las PC4, PC5 y PC6. Imagen tomada del programa Packet Tracer.



Ping entre SWT3 y las PC7, PC8 y PC9. Imagen tomada del programa Packet Tracer.



4. CONCLUSIONES

El desarrollo de las actividades permitió configurar el uso de una interfaz Loopback para definir vecinos, y esto es común con IBGP, pero no con eBGP. generalmente, se usa la interfaz Loopback para lograr que la dirección IP del vecino permanezca activa y sea independiente del hardware para que funcione correctamente.

En los escenarios 1 y 2 se puede hacer una interpretación de los mapas de ruta con BGP. En este protocolo, el mapa de ruta es un método para controlar y modificar la información de ruteo. El control y la modificación de la información de ruteo ocurre a través de la definición de condiciones para la redistribución de rutas de un protocolo de ruteo a otro. O bien, el control de la información de ruteo puede ocurrir en la inserción dentro y fuera de BGP.

Al establecer comunicaciones mediante BGP en los escenarios propuestos, se pudo verificar que después de que BGP recibe actualizaciones sobre diferentes destinos de distintos sistemas autónomos, el protocolo deberá elegir las trayectorias para alcanzar un destino específico. BGP elige solo una única trayectoria para alcanzar un destino específico, de otra parte, este protocolo basa su decisión en diferentes atributos, como salto siguiente, pesos administrativos, preferencia local, origen de ruta, longitud de trayectoria, código de origen, métrica y otros atributos.

Con base en lo planteado para el escenario 3, se verificó que Las VLAN ayudan a los administradores a tener el nodo final o el grupo de estaciones de trabajo que están segmentados lógicamente por funciones, equipos de proyecto y aplicaciones, sin importar la ubicación física de los usuarios. Además, las VLAN le permiten implementar políticas de acceso y seguridad para grupos particulares de usuarios y limitar el dominio de difusión.

BIBLIOGRAFÍA

Teare, D., Vachon, B., & Graziani, R. (2015). *Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide*. Indianapolis, IN 46240 USA: Cisco Systems, Inc. Recuperado el Abril de 2019

CISCO. (30 de octubre de 2008). *cisco.com*. Recuperado el 5 de Julio de 2019, de Estudios de caso BGP: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Cisco. (10 de 09 de 2018). *Principios básicos de routing y switching*. Obtenido de Capítulo 1 Introducción a redes conmutadas: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#1.0.1.1>

Cisco. (15 de 09 de 2018). *Principios básicos de routing y switching*. Obtenido de Capítulo 2 Configuración y conceptos básicos de switching: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#2.0.1.1>

Cisco. (15 de 09 de 2018). *Principios básicos de routing y switching*. Obtenido de Capítulo 3 VLAN: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#3.0.1.1>

Cisco. (22 de 09 de 2018). *Principios básicos de routing y switching*. Obtenido de Capítulo 5 Enrutamiento entre VLAN: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#5.0.1.1>

Froom, R., & Frahim, E. (2015). *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide*. Indianapolis, IN 46240: Cisco Press. Recuperado el 20 de 05 de 2019, de https://onedrive.live.com/?authkey=%21AJHSGgzGAE2_Ulk&cid=483D35BEE8610962&id=483D35BEE8610962%212933&parId=483D35BEE8610962%212932&o=OneUp

GuilleSQL. (17 de 03 de 2008). *GuilleSQL*. Recuperado el 5 de 04 de 2019, de Cap 2. Protocolos de Enrutamiento: http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

ICONTEC. (2008). *NTC 5613, Referencias bibliográficas. Contenido, forma y estructura*. Bogotá D.C: ICONTEC. Recuperado el 4 de julio de 2019

ICONTEC. (2018). *NTC 1486 Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación* (Séptima actualización ed.). Bogotá D.C: ICONTEC. Recuperado el 4 de Julio de 2019