DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDISON ALBERTO BETANCUR GALVIS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
MEDELLIN
2020

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDISON ALBERTO BETANCUR GALVIS

Diplomado de opción de grado presentado para
optar el título de INGENIERO EN
TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
MEDELLIN
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Medellín, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco inicialmente, a la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), al tutor y a mis compañeros de curso, quienes con su tiempo, enseñanzas y conocimiento me ayudaron a crecer y fortalecer mi aptitud para culminar con éxito el diplomado de profundización CISCO CCNP.

También agradezco a Dios y a mi familia por brindarme la posibilidad de crecer a nivel profesional, pues sin ellos no podría haber alcanzado esta meta tan anhelada.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

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

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 domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

ENRUTAMIENTO: Se refiere al proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas.

MÉTRICA: Un protocolo de enrutamiento seleccionará como mejor ruta, después de ejecutar su algoritmo, la ruta que tenga la métrica más baja y cada protocolo utiliza su propia métrica.

SISTEMA AUTÓNOMO: Se refiere a una red (o un grupo de redes) que está bajo una sola administración. Podría ser una empresa, un grupo de edificios pertenecientes a la misma empresa, tu propio proveedor de servicios de Internet, o incluso tu red doméstica. La mismísima Internet está formada por sistemas autónomos conectados entre sí.

RESUMEN

En el desarrollo del diplomado de profundización CISCO CCNP se trabajaron temas de Conmutación e implementación de enrutamiento IP, desarrollando la capacidad de configurar y verificar operaciones básicas de enrutamiento Gateway interior mediante el uso de comandos específicos del IOS con el fin identificar y resolver problemas de conectividad y actualización de tablas de enrutamiento, configurar y administrar dispositivos de Networking orientados al diseño de redes escalables.
El objetivo principal de la electrónica es formar un profesional con conocimientos científicos y tecnológicos que lo capaciten para investigar, analizar, diseñar, construir y apropiar tecnologías, principios fundamentales que nos ayudaron a la correcta implementación de la teoría de CCNP ROUTE con base en los módulos CCNP proporcionados por cisco donde se desarrollaron diferentes laboratorios para poner en práctica el funcionamiento de los protocolos implementados en IPv4 e IPv6.
Se realizaron laboratorios en el software GNS3 analizando la operación de la red y de diferentes protocolos, además de construir pequeños ambientes simulados de redes como topologías WAN aplicando los conceptos básicos de enrutamiento dinámico y sus bondades.

ABSTRACT

In the development of the CISCO CCNP in-depth course, we will work on Switching and implementation of IP routing, the ability to configure and verify basic internal gateway routing operations by using specific IOS commands in order to identify and resolve connectivity problems. And updating routing tables, configuration and administration of network devices oriented to the design of scalable networks.
The main objective of electronics is to train a professional with scientific and technological knowledge that enables him to research, analyze, design, build and apply technologies, fundamental principles that help us correct the implementation of the CCNP ROUTE theory based on the modules. CCNP provided by cisco where different laboratories are developed to implement the operation of the protocols implemented in IPv4 and IPv6.
The laboratories were analyzed in the GNS3 software, analyzing the operation of the network and different protocols, in addition to building small simulated network environments as WAN topologies, applying the basic concepts of dynamic routing and its benefits.

INTRODUCCION

En el desarrollo del curso se identificaron situaciones problemáticas asociadas con aspectos de conmutación y enrutamiento, mediante el uso eficiente de estrategias basadas en comandos IOS y estadísticas de tráfico en las interfaces, con el fin de resolver conflictos de configuración y conectividad en contextos de redes LAN y WAN. Adicional, se configuraron plataformas de conmutación basadas en switches, mediante el uso de protocolos como STP y la configuración de VLANs en escenarios de red corporativos, para comprender el modo de operación de las subredes y los beneficios de administrar dominios de broadcast independientes.

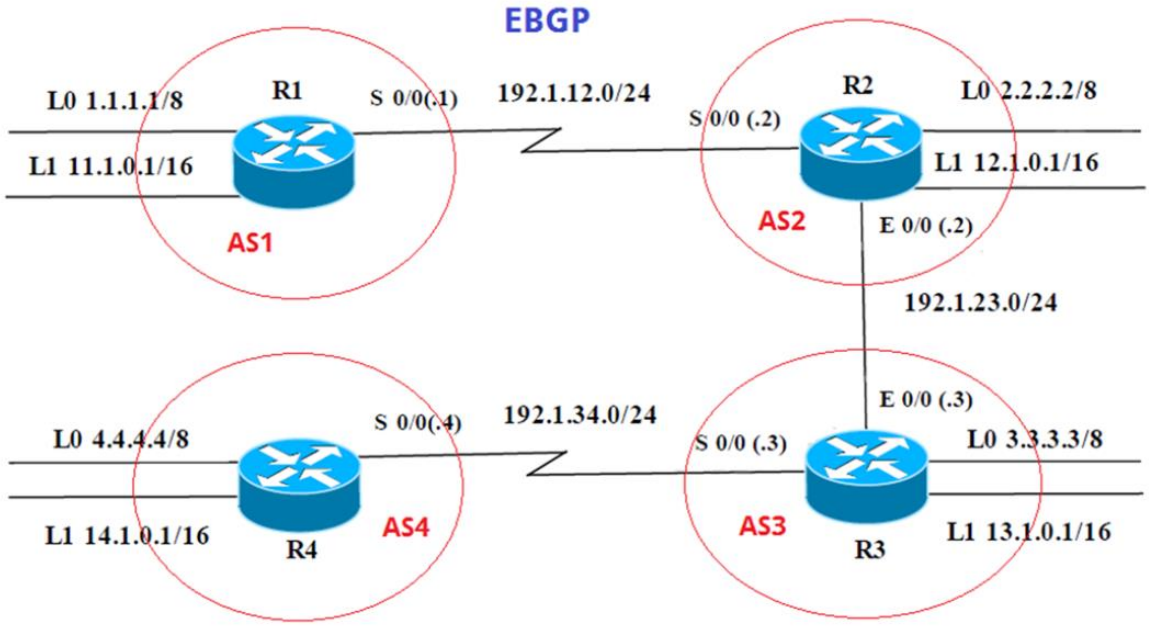
En el desarrollo del escenario 1, se realiza un análisis sobre el comportamiento del protocolo BGP, evaluando el desempeño de los routers, mediante el uso de sistemas AS autónomos y bajo el uso de protocolos de vector distancia y estado enlace.

Para el escenario 2, se implementa el protocolo VTP en una red LAN con el fin de comprender el modo de operación de las VLAN y los beneficios de administrar subredes independientes

DESARROLLO

ESCENARIO 1

Figura 1. Escenario 1



Información para configuración de los router

R1

Tabla 1. Interfaces loopback para crear R1

Interfaz	Dirección IP	Mascara
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

Tabla 2. Interfaces loopback para crear R2

Interfaz	Dirección IP	Mascara
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

Tabla 3. Loopback para crear R3

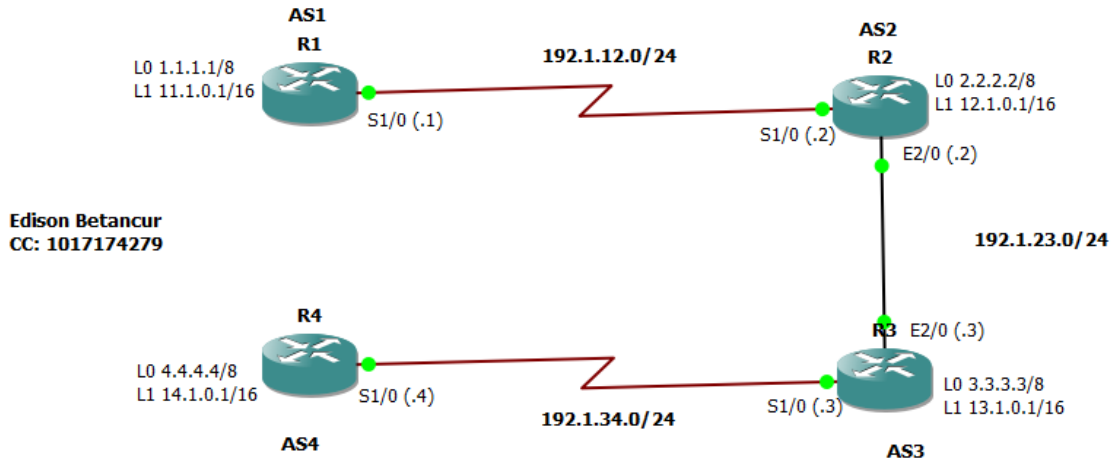
Interfaz	Dirección IP	Mascara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
S 0/0	192.1.34.3	255.255.255.0
E 0/0	192.1.23.3	255.255.255.0

R4

Tabla 4. Loopback para crear R4

Interfaz	Dirección IP	Mascara
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

Figura 2. Simulación de escenario 1



1. 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 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R1(config)#interface Lo0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Lo1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface POS1/0
R1(config-if)#description R1 -> R2
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 22.22.22.22
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

R2(config)#interface Lo0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Lo1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface POS1/0
R2(config-if)#description R2 -> R1
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface E2/0
R2(config-if)#description R2 -> R3
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 33.33.33.33
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
```

A continuación, vemos la salida del comando show ip route donde R1 y R2 contienen en su tabla de enrutamiento las direcciones de Loopback y las direcciones de las redes a las cuales se encuentran conectados de forma directa, además, de las redes configuradas en las interfaces Loopback de su respectivo router vecino.

Figura 3. Tabla de enrutamiento R1

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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, 00:00:36
      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, 00:00:36
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, POS1/0
L        192.1.12.1/32 is directly connected, POS1/0
R1#
```

Figura 4. Tabla de enrutamiento R2

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 00:01:57
      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, 00:01:57
      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, POS1/0
L        192.1.12.2/32 is directly connected, POS1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.2/32 is directly connected, Ethernet2/0
R2#
```

2. 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 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
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
```

```
R3(config)#interface Lo0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface Lo1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface POS1/0
R3(config-if)#description R3 -> R4
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface E2/0
R3(config-if)#description R3 -> R2
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
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
```

A continuación, vemos la salida del comando show ip route, donde R2 ha actualizado su tabla de enrutamiento y ahora contiene las direcciones de Loopback configuradas en el router R3 y R3 ha actualizado su tabla de enrutamiento con las direcciones de red correspondientes a las interfaces Loopback que se configuraron en R2 y R1, rutas que aprendió mediante el protocolo BGP gracias a su relación de adyacencia con R2 y a que dichas redes se anunciaron en cada uno de los routers, así también, R3 contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP y Por último, se identifica que R3 alcanza todas estas redes a través de la interfaz Gi 0/0 que lo conecta con R2 (192.1.23.0/24)

Figura 5. Tabla de enrutamiento R2

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 00:06:24
      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
B     3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:06
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:06:24
      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
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.23.3, 00:00:06
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, POS1/0
L        192.1.12.2/32 is directly connected, POS1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.2/32 is directly connected, Ethernet2/0
R2#
```

Figura 6. Tabla de enrutamiento R3

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:01:21
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:21
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:01:21
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:01:21
      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, 00:01:21
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.3/32 is directly connected, Ethernet2/0
R3#
```

3. 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 66.66.66.66. 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.

```
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

R4(config)#interface Lo0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface Lo1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface POS1/0
R4(config-if)#description R1 -> R2
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 66.66.66.66
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
```

A continuación, vemos la salida del comando show ip route, donde R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este dispositivo con R4 ha cambiado y ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática dado que así se estableció en el paso anterior, sin embargo, pese a que se usa la dirección lógica Loopback 0 para establecer la adyacencia, la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 0/1/0. Así también, se puede identificar que la dirección de red de la interfaz Loopback 1 se siegue aprendiendo mediante el protocolo BGP, pero ahora se alcanza mediante la interfaz Loopback 0 de R4 (4.4.4.4).
En la salida del comando show ip route en R4 se puede evidenciar que la dirección mediante la cual este se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3.

Figura 7. Tabla de enrutamiento R3

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:26:22
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:26:22
      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, 00:26:22
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:26:22
      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
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.34.4, 00:04:23
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:26:22
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.3/32 is directly connected, Ethernet2/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, POS1/0
L        192.1.34.3/32 is directly connected, POS1/0
R3#
```

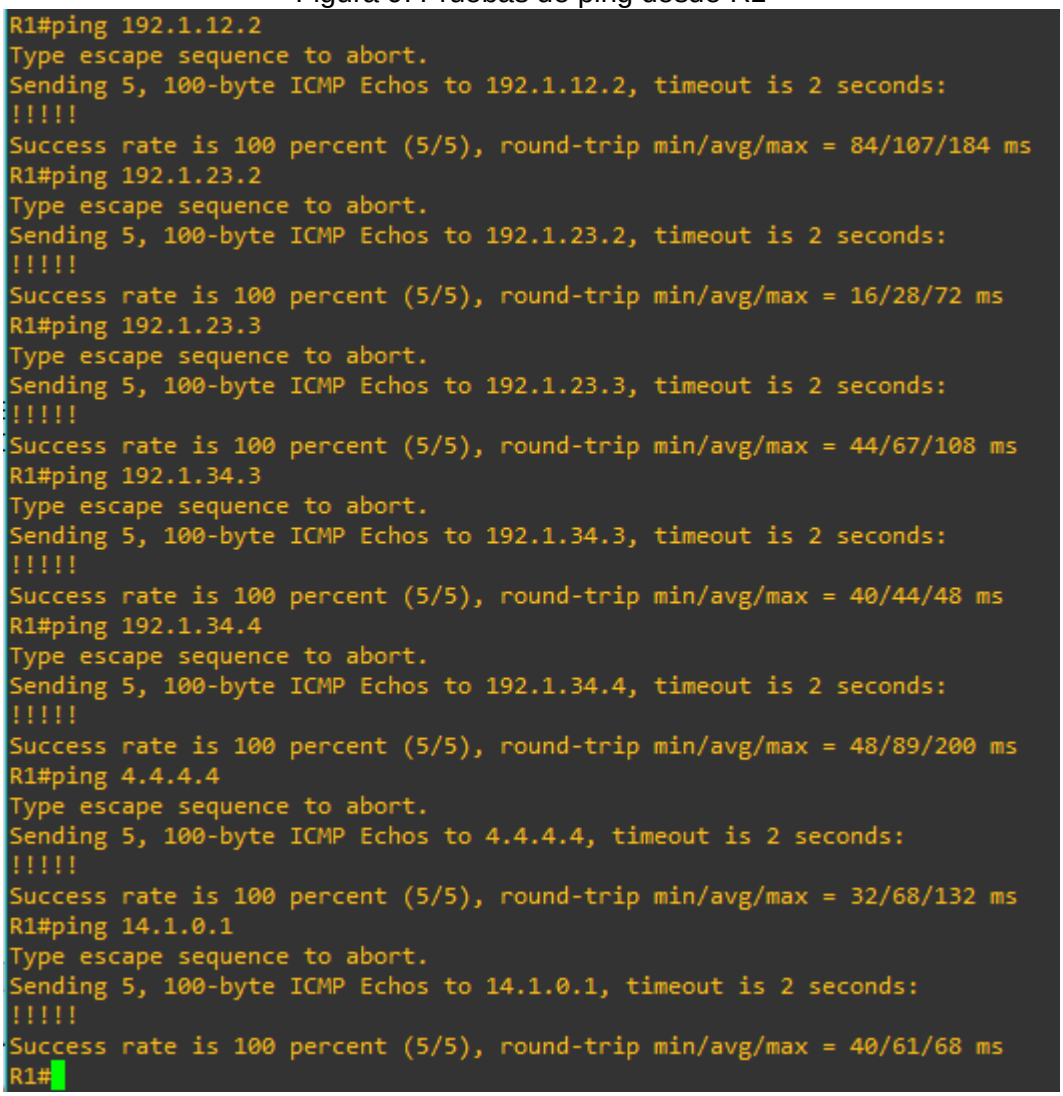
Figura 8. Tabla de enrutamiento R4

```
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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.34.3, 00:05:18
B     2.0.0.0/8 [20/0] via 192.1.34.3, 00:05:18
S     3.0.0.0/8 [1/0] via 192.1.34.3
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.34.3, 00:05:18
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.34.3, 00:05:18
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.34.3, 00:05:18
      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
B     192.1.12.0/24 [20/0] via 192.1.34.3, 00:05:18
B     192.1.23.0/24 [20/0] via 192.1.34.3, 00:05:18
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, POS1/0
L        192.1.34.4/32 is directly connected, POS1/0
R4#
```

Figura 9. Pruebas de ping desde R1



ESCENARIO 2

Figura 10. Escenario 2

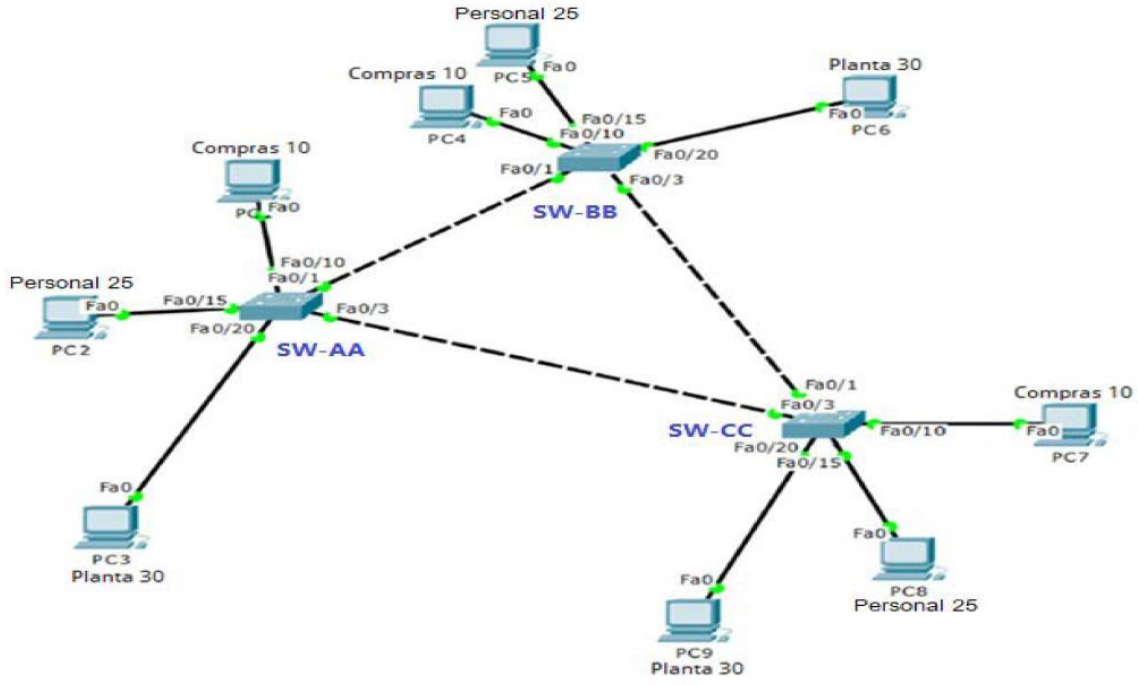
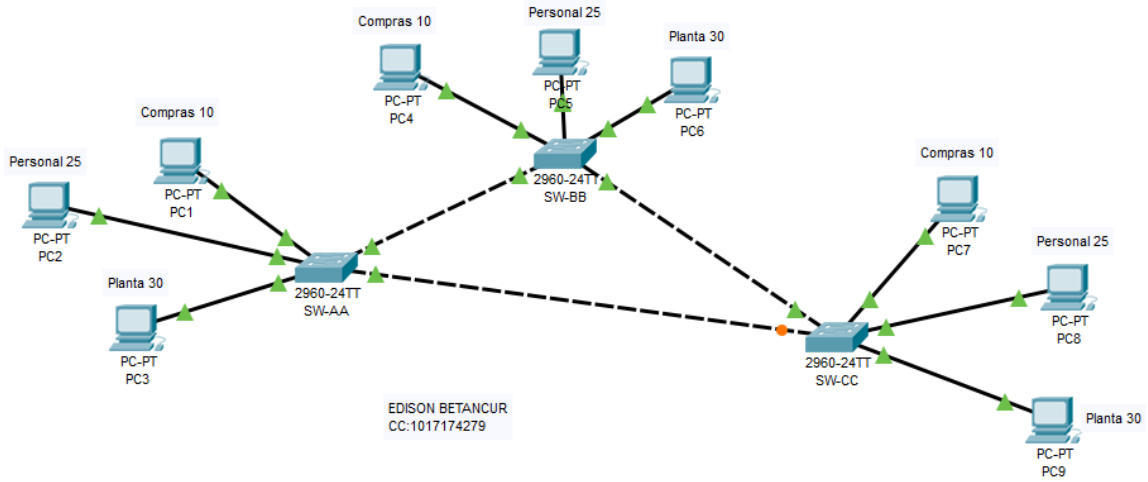


Figura 11. Simulación del escenario 2



A. Configurar VTP

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

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco

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

Figura 12. VTP en SW-AA

```
SW-AA#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
SW-AA#
```

Figura 13. VTP en SW-BB

```
SW-BB#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                 : 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
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 14. VTP en SW-CC

```
SW-CC#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
SW-CC#
```

B. Configurar DTP (Dynamic Trunking Protocol)

3. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable

4. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando show interfaces trunk.

Figura 15. Enlaces trunk SW-AA

```
SW-AA#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
```

Figura 16. Enlaces trunk SW-BB

```
SW-BB#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
```

5. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

6. Verifique el enlace "trunk" el comando show interfaces trunk en SW-AA.

Figura 17. Enlaces trunk SW-AA

```
SW-AA#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       1

SW-AA#
```

7. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk

Figura 18. Enlaces trunk SW-CC

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

C. Agregar VLANs y asignar puertos.

8. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#

9. Verifique que las VLANs han sido agregadas correctamente.

Figura 19. VLANs SW-AA

```
SW-AA#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
25   Personal                          active
30   Planta                            active
99   Admon                             active
1002 fddi-default                      active
```

Figura 20. VLANs SW-BB

```
SW-BB#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
25   Personal                          active
30   Planta                            active
99   Admon                             active
1002 fddi-default                      active
```

Figura 21. VLANs SW-CC

```
SW-CC#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
25   Personal                          active
30   Planta                            active
99   Admon                             active
```

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

Tabla 5. Configuración direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.25.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

11. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

12. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

PC1: ip address 190.108.10.1 255.255.255.0
PC2: ip address 190.108.25.2 255.255.255.0
```

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 190.108.25.5 255.255.255.0
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 190.108.25.8 255.255.255.0
PC9: ip address 190.108.30.9 255.255.255.0

D. Configurar las direcciones IP en los Switches.

13. 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 6. Configurar las direcciones IP en los switch

Equipo	Interfaz	Direcciones IP	Mascara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

E. Verificar la conectividad Extremo a Extremo

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

El ping tiene éxito cuando se realiza entre los PCs de la misma VLAN. Cuando se realiza el ping entre PCs de diferentes VLAN no hay éxito ya que cada PC pertenece a un segmento de red diferente y la única forma de comunicarlos entre sí, sería por medio de un enrutador o un Switch de capa 3 (Switch Multicapa), los cuales tienen la funcionalidad intrínseca de enrutamiento entre VLANs, para así lograr comunicar el tráfico ICMP entre las diferentes redes.

PING DESDE EL PC1 A LOS DEMÁS PCS

C:\>ping 190.108.25.2
Pinging 190.108.25.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.25.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.3
Pinging 190.108.30.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.4
Pinging 190.108.10.4 with 32 bytes of data:
Reply from 190.108.10.4: bytes=32 time=133ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.10.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 133ms, Average = 33ms

C:\>ping 190.108.25.5
Pinging 190.108.25.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.25.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.6
Pinging 190.108.30.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.6:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.7
Pinging 190.108.10.7 with 32 bytes of data:
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=3ms TTL=128
Ping statistics for 190.108.10.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 190.108.25.8
Pinging 190.108.25.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.25.8:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.9:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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

El ping realizado entre Switch es exitoso ya que previamente se había configurado en cada uno de ellos una dirección IP al SVI (Switch Virtual Interface) para VLAN 99

SW-AA#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 = 0/0/2 ms

SW-AA#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 = 0/0/2 ms

SW-BB#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

SW-BB#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

SW-CC#ping 190.108.99.1
ype 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 = 0/1/3 ms

SW-CC#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

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

El ping realizado desde los Switch hacia los PCs no es exitoso ya que no se ha configurado en cada uno de los SW una dirección IP al SVI (Switch Virtual Interface) para las VLAN 10, 25 y 30 donde están trabajando los PCs

PING DESDE EL SW-AA

SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.25.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.25.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.25.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

PING DESDE EL SW-BB

SW-BB#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.25.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.25.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.25.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

PING DESDE EL SW-CC

SW-CC#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.25.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.25.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.25.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```
SW-CC#ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

CONCLUSIONES

Los laboratorios prácticos permitieron afianzar los procedimientos necesarios para emplear herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de múltiples protocolos, evaluando el desempeño de los routers, mediante el uso de comandos de administración avanzados y bajo el uso de protocolos de vector distancia y estado enlace.

El protocolo VTP nos deja como enseñanza que la Versión 3 incorpora muchos cambios de V1 y V2 de VTP como la vlan extendida y VTP V2 introduce el soporte para las VLAN de Token Ring en comparación a VTP V1; también debemos saber que si se configura un switch como servidor VTP sin un nombre de dominio VTP, no será posible configurar una VLAN en el switch.

El protocolo BGP, facilita el intercambio de información de enrutamiento de diferentes sistemas AS autónomos, simplificando en gran medida la configuración entre esos sistemas para el tráfico entre ellos. La propagación de rutas predeterminadas entre sistemas autónomos es más eficiente utilizando BGP omitiendo la información de direccionamiento y utilizando el identificador del AS y el vecino al que se enviará el tráfico.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). High Availability. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg