DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

SANTIAGO ARNALDO AMAYA MONTOYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA ELECTRONICA
SOGAMOSO-BOYACÁ
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

SANTIAGO ARNALDO AMAYA MONTOYA

Diplomado de opción de grado presentado para optar el título de INGENIERO ELECTRONICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA ELECTRONICA
SOGAMOSO-BOYACÁ
2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

Sogamoso, 15 de mayo de 2020

AGRADECIMIENTOS

Quiero dar gracias a Dios, por el privilegio de realizar este proyecto de investigación, para lograr el título de profesional, el me otorgo la motivación y perseverancia, para alcanzar este proyecto de vida; De esta manera me siento agradecido con él, mi esposa e hijo por brindarme todo su amor, cariño y apoyo en este proceso, a mi madre y hermanos por brindarme todo su apoyo, a todos los tutores de la UNAD que siempre estuvieron hay brindándome sus conocimientos y apoyo, el cual me ha respaldado en todos aspectos de la vida, coloco a unos compañeros y siempre recuerdo, que alrededor de nosotros tenemos personas que verdaderamente nos animan para no desfallecer, por eso no me voy a quedar ahí, solo como profesional, soy constante en el proceso de formación académica, seguiré luchando por la superación personal buscando siempre la excelencia y no el conformismo.

A la ingeniera Sandra Isabel Vargas Docente UNAD Sogamoso; quien asume con vocación la labor de enseñanza con responsabilidad y dedicación para formar jóvenes de calidad para nuestra sociedad.

CONTENIDO

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pag

GLOSARIO

BGP: es un protocolo el cual permite intercambiar información de enrutamiento en sistemas autónomos.

Enrutamiento: es el proceso que el router utiliza para decidir donde enviar un paquete.

Router: es un dispositivo el cual permite interconectar redes de datos.

Switch: es un dispositivo que sirve par conectar varios dispositivos dentro de un red.

VTP: es un protocolo de mensajes de nivel dos que se usa para configurar y administrar las Vlans.

VLAN: Es un método que permite crear redes que lógicamente son independientes dentro de una red física.

RESUMEN

Con el desarrollo de las pruebas de habilidades practicas CCNP permitirá medir los conocimientos desarrollados durante el curso, por medio de dos escenarios propuestos los cuales se configurarán según las indicaciones del documento, en el primer escenario se colocara en práctica el intercambio de información de enrutamiento por medio del protocolo BGP en el segundo escenario se colocara en práctica la configuración las redes de área local y la administración de las Vlan por medio de del protocolo VTP.

Palabras Claves**:** CCNP, BGP, CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica Redes de área local, Vlan, Protocolo VTP.

ABSTRACT

With the development of the practical skills tests CCNP will allow to measure the knowledge developed during the course, by means of two proposed stage which will be configured according to the indications of the document, in the first scenario the exchange of routing information by By means of the BGP protocol, in the second stage, the configuration of the local area networks and the administration of the VLANs through the VTP protocol will be put into practice.

Key Words: CCNP, BGP, CISCO, CCNP, Routing, Swicthing, Networking, Electronics. Local Area Networks, Vlan, VTP Protocol.

INTRODUCCIÓN

En este documento se encontrarán dos escenarios propuestos por la prueba de habilidades practicas del diplomado de profundización CCNP, donde se busca identificar el grado de desarrollo de competencias y habilidades que se adquirieron a lo largo del diplomado, lo principal de este desarrollo es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Durante esta actividad se realizarán dos escenarios propuestos los cuales se configurarán según sus respectivos procesos, en estos procesos se encontrarán protocolos de enrutamiento como BGP, configuraciones de área local, administración de las Vlan por medio de protocolos como VTP.

En el desarrollo del escenario se realiza configuración de rauters con una ip especifica para adoptar una relación vecina BGP entre los rauters en los cuales se desarrolla comando para la solución de esta relación entre rauters. Se realiza ping extremo-extremo para evidenciar la ruta y tener garantía de lo realizado.

Se obtiene del segundo escenario el desarrollo configurando switches para usar VTP y así obtener las actualizaciones de VLAN para clientes en los cuales se asignan ip ya dadas por el escenario y siguiendo todas sus especificaciones en las cuales finalizamos realizando ping desde todos los puntos para verificar si se obtuvo lo deseado.

DESARROLLO DE LOS ESCENARIOS

Escenario 1

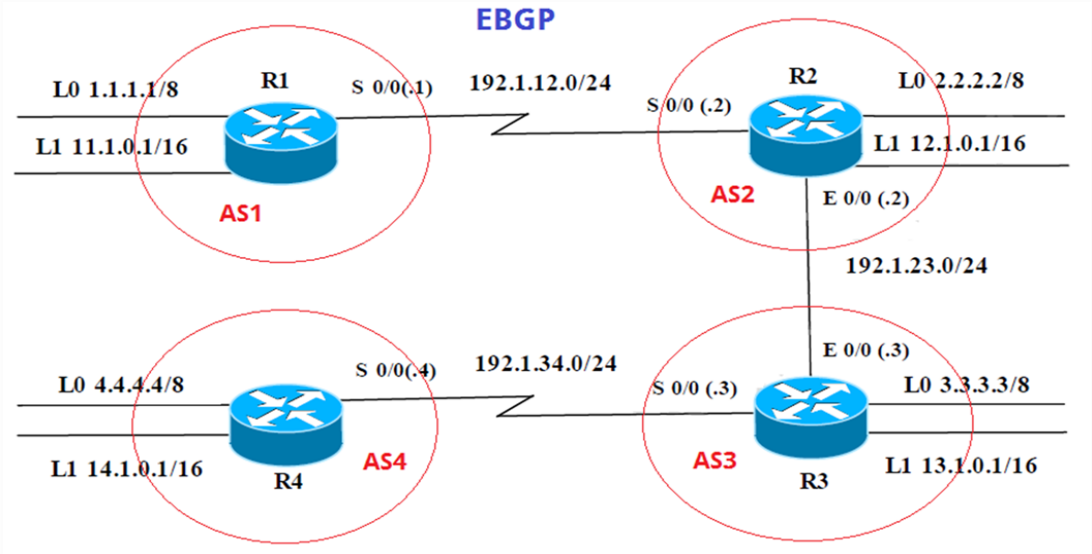

Figura 1. Escenario 1.

Información para configuración de los Routers

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

Tabla 1. Configuración de R1.

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

Tabla 2. Configuración de R2.

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

Tabla 3. Configuración de R3.

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

Tabla 4. Configuración de R4.

Solución escenario 1

Topología

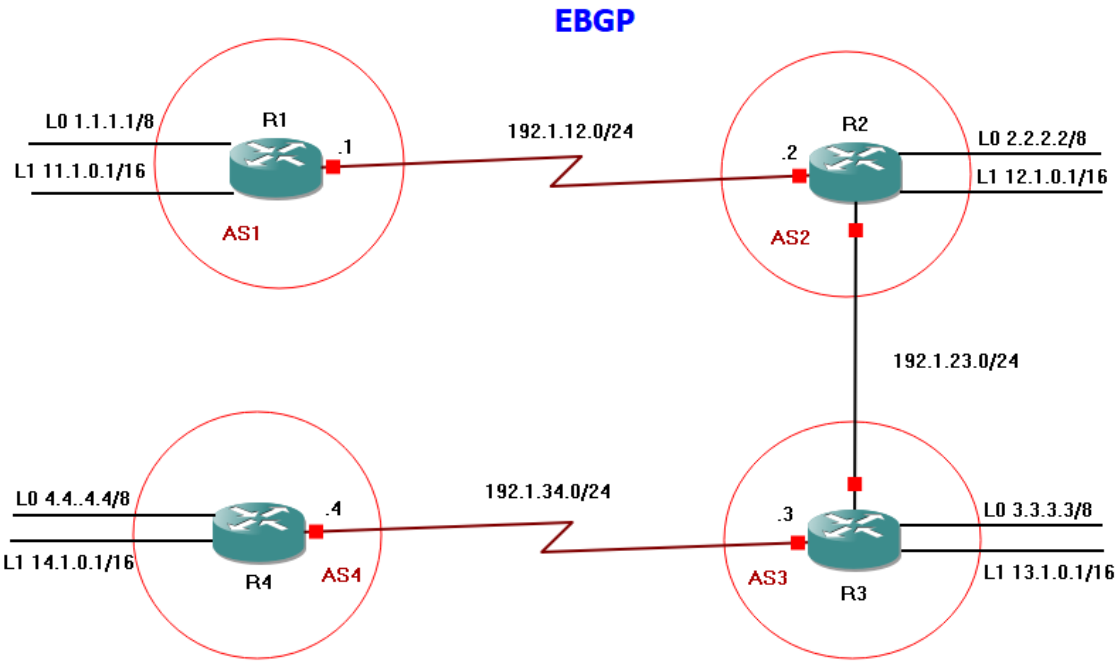

Figura 2. Escenario 1 en GNS3.

Como primer paso se configura el direccionamiento según las tablas de enrutamiento que nos brinda el escenario 1

```
R1#config t
R1(config)#int lo0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#int lo1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#int s1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

```
R2#config t
R2(config)#int lo0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#int lo1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#int s1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R3#config t
R3(config)#int lo0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#int lo1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#int s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#int f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R4#config t
R4(config)#int lo0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#int lo1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
```

```
R4(config-if)#exit
R4(config)#int s1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
```

- Se realiza configuracion de Routers asignado por el escenario ip, ,mascara y loopback en cada uno de los Rauters como lo son R1, R2, R3 Y R4 con los comandos conocidos al transcurso del curso.

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)#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
R1(config-router)#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)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#exit
```

```
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, 00:02:59
      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, 00:02:59
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.1/32 is directly connected, Serial1/0
B     192.1.23.0/24 [20/0] via 192.1.12.2, 00:02:59
```

Figura 3. Enrutamiento de 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, 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, 00:04:58
      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, 00:04:58
      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, Serial1/0
L        192.1.12.2/32 is directly connected, Serial1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, FastEthernet0/0
L        192.1.23.2/32 is directly connected, FastEthernet0/0
```

Figura 4. Enrutamiento R2.

- Se realiza configuracion vecino BGP mediante comandos entre Rauters R1 y R2 como se evidencia validando ip y loopback en BGP a continuacion se realiza comando show ip raute en R1 y 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 fue configurado en el punto anterior, en este punto se procederá a realizar la configuración de R3 y a realizar la relación entre R3 – R2 y R3 – R4, cabe aclarar que la relación en R2 ya está configurada solo falta la relación en R3 para que se conecten.

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)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit

```
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, 00:02:50
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:02:50
      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, 00:02:50
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:02:50
      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, 00:02:50
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, FastEthernet0/0
L        192.1.23.3/32 is directly connected, FastEthernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.3/32 is directly connected, Serial1/0
```

Figura 5. Enrutamiento R3.

- Se realiza configuracion de vesino VGP en R3 no se realiza configuracion R2 por que en el punto anterior del escenario se desarrolla. se realiza comando show ip route para verificar comando como se evidencia en la imagen.

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 fue configurado en el punto anterior, en este punto se procederá a configurar la R4 y a configurar la relación entre R3 – R4.

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

```
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, 00:15:14
B      2.0.0.0/8 [20/0] via 192.1.34.3, 00:15:14
B      3.0.0.0/8 [20/0] via 192.1.34.3, 00:15:14
       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, 00:15:14
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.34.3, 00:15:14
       13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.34.3, 00:15:14
       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, 00:15:14
B      192.1.23.0/24 [20/0] via 192.1.34.3, 00:15:14
       192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.34.0/24 is directly connected, Serial1/0
L         192.1.34.4/32 is directly connected, Serial1/0
```

Figura 6. Enrutamiento de R4.

A continuación, se mostrará la configuración BGP por medio del comando show ip bgp.

```
R1#show ip bgp
BGP table version is 12, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0          0.0.0.0                  0         32768 i
 *>  2.0.0.0          192.1.12.2               0             0 2 i
 *>  3.0.0.0          192.1.12.2                             0 2 3 i
 *>  4.0.0.0          192.1.12.2                             0 2 3 4 i
 *>  11.1.0.0/16      0.0.0.0                  0         32768 i
 *>  12.1.0.0/16      192.1.12.2               0             0 2 i
 *>  13.1.0.0/16      192.1.12.2                             0 2 3 i
 *>  14.1.0.0/16      192.1.12.2                             0 2 3 4 i
 *   192.1.12.0       192.1.12.2               0             0 2 i
 *>                   0.0.0.0                  0         32768 i
 *>  192.1.23.0       192.1.12.2               0             0 2 i
 *>  192.1.34.0       192.1.12.2                             0 2 3 i
R1#
```

Figura 7. Enrutamiento BGP en R1.

```
R2#show ip bgp
BGP table version is 12, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0          192.1.12.1               0             0 1 i
 *>  2.0.0.0          0.0.0.0                  0         32768 i
 *>  3.0.0.0          192.1.23.3               0             0 3 i
 *>  4.0.0.0          192.1.23.3                             0 3 4 i
 *>  11.1.0.0/16      192.1.12.1               0             0 1 i
 *>  12.1.0.0/16      0.0.0.0                  0         32768 i
 *>  13.1.0.0/16      192.1.23.3               0             0 3 i
 *>  14.1.0.0/16      192.1.23.3                             0 3 4 i
 *   192.1.12.0       192.1.12.1               0             0 1 i
 *>                   0.0.0.0                  0         32768 i
 *   192.1.23.0       192.1.23.3               0             0 3 i
 *>                   0.0.0.0                  0         32768 i
 *>  192.1.34.0       192.1.23.3               0             0 3 i
R2#
```

Figura 8. Enrutamiento BGP en R2.

```
R3#show ip bgp
BGP table version is 12, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0          192.1.23.2                             0 2 1 i
 *>  2.0.0.0          192.1.23.2                             0 2 i
 *>  3.0.0.0          0.0.0.0                  0         32768 i
 *>  4.0.0.0          192.1.34.4               0             0 4 i
 *>  11.1.0.0/16      192.1.23.2                             0 2 1 i
 *>  12.1.0.0/16      192.1.23.2               0             0 2 i
 *>  13.1.0.0/16      0.0.0.0                  0         32768 i
 *>  14.1.0.0/16      192.1.34.4               0             0 4 i
 *>  192.1.12.0       192.1.23.2               0             0 2 i
 *   192.1.23.0       192.1.23.2               0             0 2 i
 *>                   0.0.0.0                  0         32768 i
 *   192.1.34.0       192.1.34.4               0             0 4 i
 *>                   0.0.0.0                  0         32768 i
R3#
```

Figura 9. Enrutamiento BGP en R3.

```
R4#show ip bgp
BGP table version is 12, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0          192.1.34.3                             0 3 2 1 i
 *>  2.0.0.0          192.1.34.3                             0 3 2 i
 *>  3.0.0.0          192.1.34.3               0             0 3 i
 *>  4.0.0.0          0.0.0.0                  0         32768 i
 *>  11.1.0.0/16      192.1.34.3                             0 3 2 1 i
 *>  12.1.0.0/16      192.1.34.3                             0 3 2 i
 *>  13.1.0.0/16      192.1.34.3               0             0 3 i
 *>  14.1.0.0/16      0.0.0.0                  0         32768 i
 *>  192.1.12.0       192.1.34.3                             0 3 2 i
 *>  192.1.23.0       192.1.34.3               0             0 3 i
 *   192.1.34.0       192.1.34.3               0             0 3 i
 *>                   0.0.0.0                  0         32768 i
R4#
```

Figura 10. Enrutamiento BGP en R4.

Para rectificar que toda la configuración que se realizó y evidencio se efectuó de la mejor manera se hará ping de extremo a extremo como garantía.

```
R1#ping 192.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/125/168 ms
```

Figura 11. Ping desde R1 a R4.

```
R3#ping 192.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/91/112 ms
R3#
```

Figura 12. Ping desde R3 a R1.

A continuación, se mostrará nuevamente los comandos de show ip route para verificar que todas las nuevas rutas estén aprendidas.

```
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, 01:29:34
B     3.0.0.0/8 [20/0] via 192.1.12.2, 01:16:19
B     4.0.0.0/8 [20/0] via 192.1.12.2, 00:59:11
      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, 01:29:34
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.12.2, 01:16:19
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.12.2, 00:59:11
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.1/32 is directly connected, Serial1/0
B     192.1.23.0/24 [20/0] via 192.1.12.2, 01:29:34
B     192.1.34.0/24 [20/0] via 192.1.12.2, 01:16:19
R1#
```

Figura 13. Enrutamiento actualizada 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, 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, 01:30:58
       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, 01:17:43
B      4.0.0.0/8 [20/0] via 192.1.23.3, 01:00:35
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.12.1, 01:30:58
       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, 01:17:43
       14.0.0.0/16 is subnetted, 1 subnets
B         14.1.0.0 [20/0] via 192.1.23.3, 01:00:35
       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.12.0/24 is directly connected, Serial1/0
L         192.1.12.2/32 is directly connected, Serial1/0
       192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.23.0/24 is directly connected, FastEthernet0/0
L         192.1.23.2/32 is directly connected, FastEthernet0/0
B      192.1.34.0/24 [20/0] via 192.1.23.3, 01:17:43
R2#
```

Figura 14. Enrutamiento actualizada 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, 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, 01:13:12
B      2.0.0.0/8 [20/0] via 192.1.23.2, 01:13:12
       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
B      4.0.0.0/8 [20/0] via 192.1.34.4, 00:56:04
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.23.2, 01:13:12
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.23.2, 01:13:12
       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, 00:56:04
B      192.1.12.0/24 [20/0] via 192.1.23.2, 01:13:12
       192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.23.0/24 is directly connected, FastEthernet0/0
L         192.1.23.3/32 is directly connected, FastEthernet0/0
       192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.34.0/24 is directly connected, Serial1/0
L         192.1.34.3/32 is directly connected, Serial1/0
R3#
```

Figura 15. Enrutamiento actualizada R3.

- Se realiza configuracion de R4 y la relación de R3 y R4 no se realiza configuracion de R3 por que se realiza en el punto anterior. Se procede a realizar comando BGP por medio del comando show ip bgp como se evidencia en la imagen. Para verificar que toda la configuración que se realizó se efectuó de la mejor manera se realiza ping de extremo a extremo como garantía de lo programado se realiza validación de comando show ip route para verificar todas las rutas propuestas.

Escenario 2

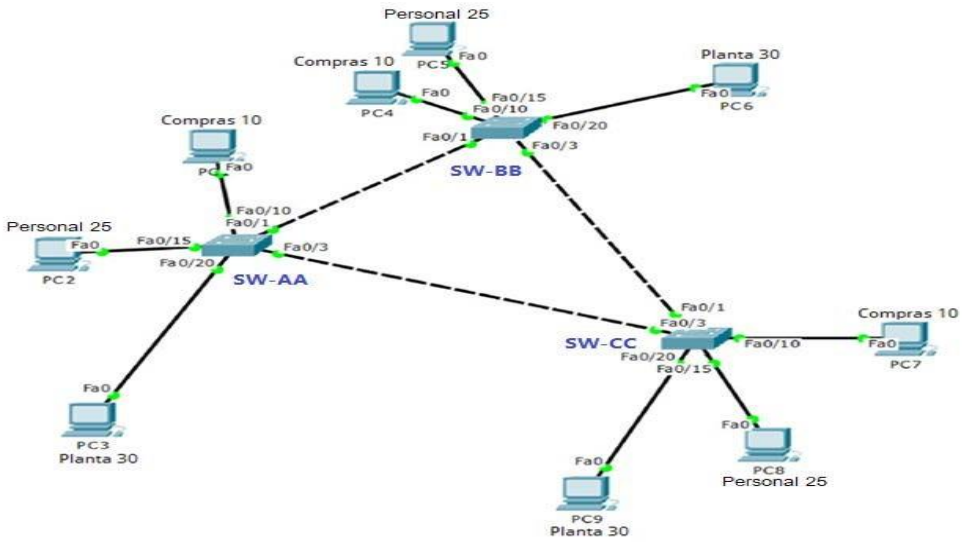

Figura 16. Topología escenario 2.

Solución escenario 2

Topología

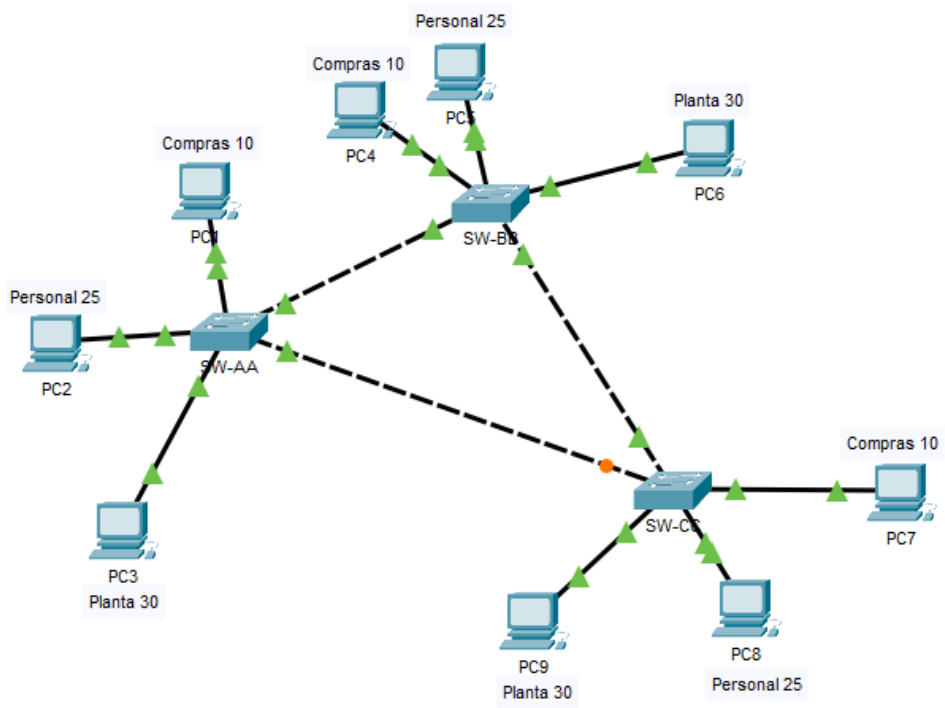

Figura 17. topología escenario 2 en Packet Tracer.

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>enable
Switch#config t
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco

Switch>enable

Switch#config t
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco

Switch>enable
Switch#config t
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco

- Se desarrolla topología en packet tracer se desarrolla programación para switches con configurarán para usar VTP configuramos switch SW-BB como servidor con el siguiente comando (config)#vtp mode server y los switch SW-AA y SW-CC lo configuramos como clientes con el siguiente comando (config)#vtp mode client el dominio lo llamamos CCNP (config)#vtp domain CCNPy su contraseña cisco lo realizamos con el comando (config)#vtp password cisco.

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

```
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 18.Estado de la configuración vtp de SW-AA.

```
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 19. Estado de la configuración vtp de SW-BB.

```
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#
```

Figura 20. Estado de la configuración vtp de SW-CC.

Se realiza ejecución de comando show vtp status en los cuales nos responde al nombre de dominio y modo de operación de cada switches.

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 t
SW-BB(config)#int f0/1
SW-BB(config-if)#switch mode dynamic desirable
SW-BB(config-if)#exit

SW-AA#config t
SW-AA(config)#int f0/1
SW-AA(config-if)# switch mode dynamic auto
SW-AA(config-if)#exit

- se configura sw-bb por defecto dynamic desirable y sw-aa Dynamic auto

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

```
SW-AA#show interface 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 21. Enlace troncal SW-AA.

```
SW-BB#show int 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
```

Figura 22. Enlace troncal SW-BB.

- Se realiza comando show int trunk entre SW-AA y SW-BB los cuales activan el dominio

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

```
SW-AA#config t
SW-AA(config)#interface f0/3
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#exit
```

- Se realiza configuracion de enlace estatico utilizando comando (config-if)#switchport mode trunk en SW-AA

6. Verifique el enlace "trunk" el comando ***show interfaces trunk*** en 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
```

Figura 23. Enlace troncal SW-AA actualizada.

- Se realiza verificación de comando show interfaces trunk en SW-AA el cual nos responde en puertos y vlan

7. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

```
SW-BB#config t
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit

SW-CC#config t
SW-CC(config)#interface f0/1
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#exit
```

```
SW-BB#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    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
```


Figura 24.Enlace troncal SW-BB actualizada.

```
SW-CC#show interface 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
```

Figura 25. Enlace troncal SW-CC actualizada.

- Se realiza enlace trunk permanente en SW-BB y SW-AA se revisa con comando show interface trunk en cada uno de los switches relacionados para verificación de programación dada.

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

SW-BB#config t
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

- Se agrega en SW-AA la vlan 10 y SW-BB se agrega las vlan para compras personal planta y admon con el siguiente comando (config-vlan)#name y (config-vlan)#vlan para numero de vlan

9. Verifique que las VLANs han sido agregadas correctamente.

```
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
```

Figura 26. Verificación de las Vlan creadas.

```
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
```

Figura 27. Verificación de las Vlan creadas.

```
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
```

Figura 28. Verificación de las Vlan creadas.

- Se realiza validación de las vlan anteriormente programadas mediante el comando show vlan brief en SW-AA, SW-BB y SW-CC en cual nos responde con lo programado que se encuentra activo

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

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

Tabla 5. Configuración de puertos a las Vlan y la direcciones IP.

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.

Dirección Ip que se le asigno a los PC:
PC1: 190.108.10.2/24
PC2: 190.108.20.2/24
PC3: 190.108.30.2/24
PC4: 190.108.10.3/24
PC5: 190.108.20.3/24
PC6: 190.108.30.3/24
PC7: 190.108.10.4/24
PC8: 190.108.20.4/24
PC9: 190.108.30.4/24

```
SW-AA#config t
SW-AA(config)#int f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#int f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#int f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
```

```
SW-BB#config t
SW-BB(config)#int f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#int f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#int f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
```

```
SW-CC#config t
SW-CC(config)#int f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#int f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#int f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
```

- Se asocia los puertos a las vlan y se configura ip como lo pide el escenario adicional configuramos el purto f0/10 en modo de acceso para los switches A,B y C y los asignamos a la vlan 10 se realiza programación de los puertos f0/15 y f0/20 en los switches con vlan de la tabla superior con las ip de los pc.

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.

Equipo	Interfaz	Dirección IP	Máscara
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

Tabla 6. Dirección IP para la Vlan 99.

```
SW-AA#config t
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#exit

SW-BB#config t
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#exit

SW-CC#config t
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#exit
```

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.

- Se realiza ping desde el PC1 a todos los otros ochos PC donde se evidencia que solo se hace ping satisfactoriamente a los PC que están en la misma en la misma VLAN, es decir, en el caso del PC1 se realizó ping satisfactoriamente a los PC que están en la VLAN 10, a continuación, se adjuntaran pruebas.

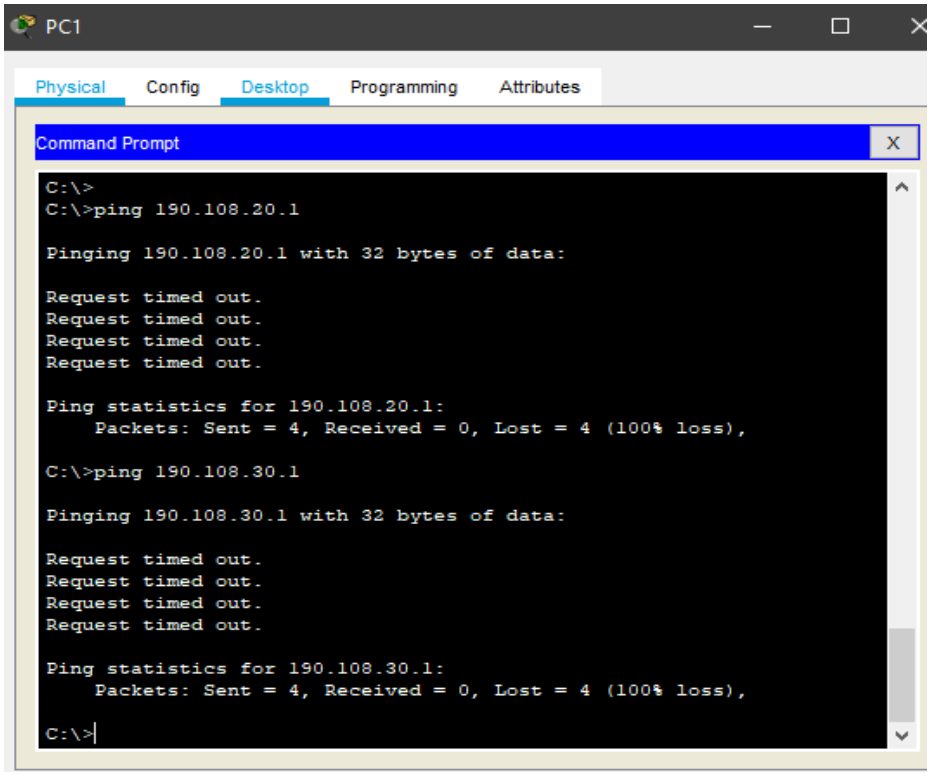

Figura 29. Ping a PC2 y PC3.

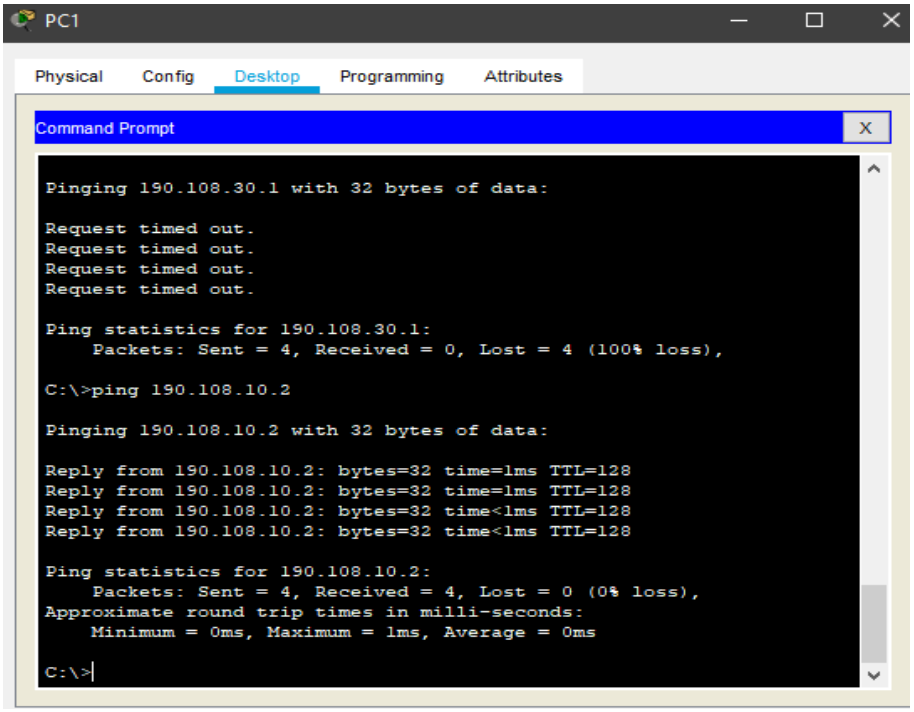

Figura 30. Ping PC4.

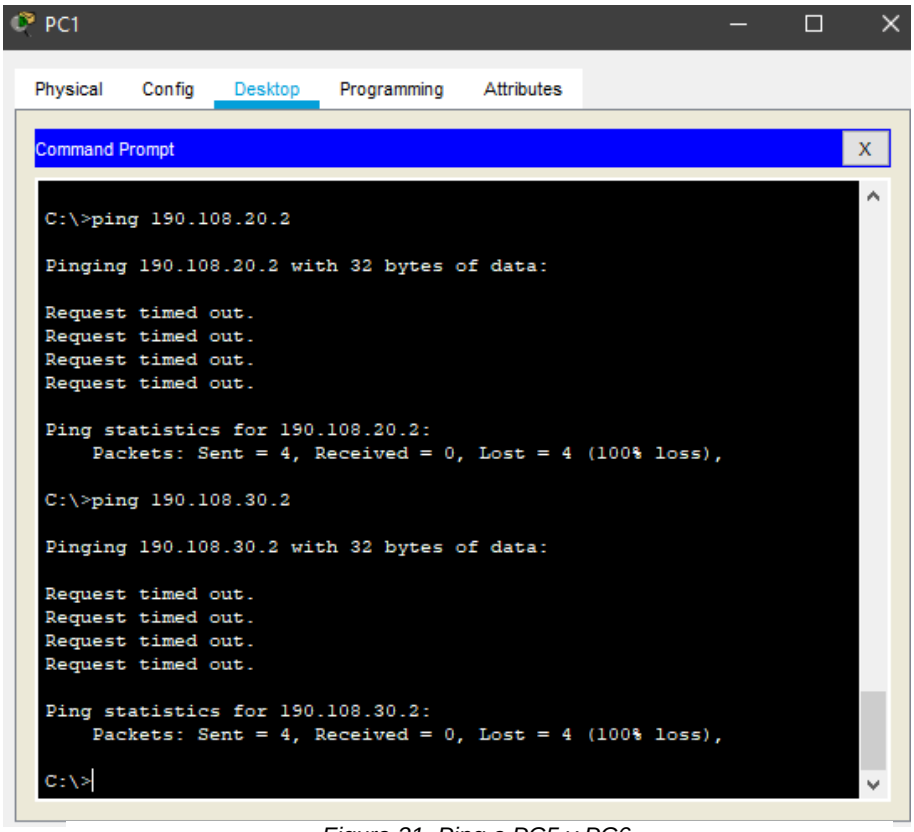

Figura 31. Ping a PC5 y PC6.

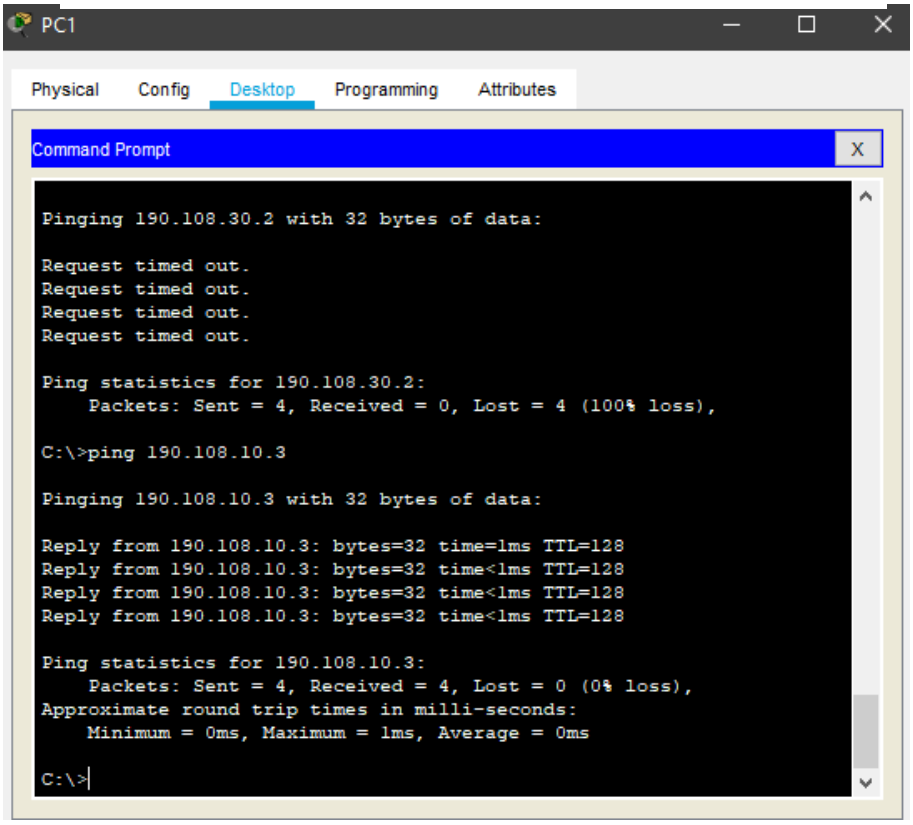

Figura 32. Ping a PC7.

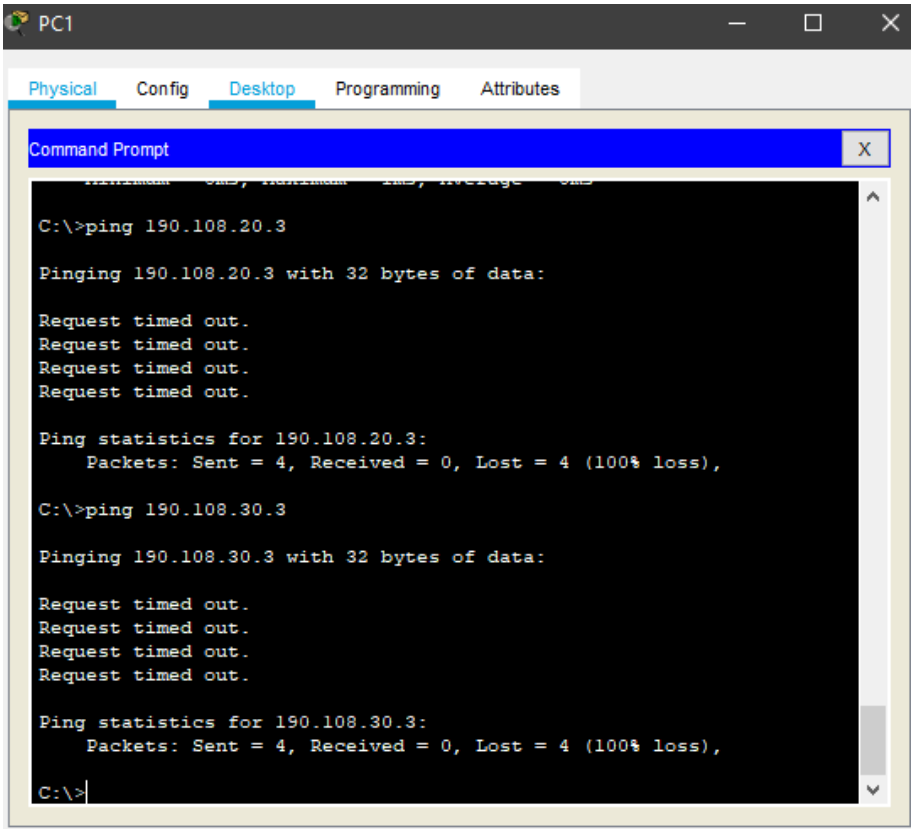

Figura 33. Ping a PC8 y PC9.

- Como se puede evidenciar el PC1 solo realizo ping satisfactoriamente al PC4 y PC7 ya que están conectado a la misma VLAN 10, al momento de realizar ping con los otros PC de diferente VLAN el ping es fallido.

- En esta ocasión se realizó el ejemplo con el PC1 que pertenece a la VLAN10, se aclara que al realizar el mismo procedimiento con los demás PC se obtiene el mismo resultado donde solo se realiza ping satisfactoriamente con los PC de la misma VLAN.

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

```
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 = 0/0/0 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 = 0/0/0 ms
```

Figura 34. Ping desde SW-AA a SW-BB y SW-CC.

```
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 = 0/0/0 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 = 0/1/7 ms
```

Figura 35. Ping desde SW-BB a SW-AA y SW-CC.

```
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 = 0/0/2 ms

SW-CC#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
```

Figura 36. Ping desde SW-CC a SW-BB y SW-AA.

- Se realizo ping entre todos los Switches por medio del direccionamiento de las ip de la VLAN 99, todos los pings fueron satisfactorios.

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

```
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 190.108.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 37. Ping desde SW-BB a PC1 y PC2.

```
SW-BB#ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 38. Ping desde SW-BB a PC3, PC4 y PC5.

```
SW-BB#ping 190.108.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, 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)
```

Figura 39. Ping desde SW-BB a PC6, PC7, PC8 y PC9.

- Para el desarrollo de este punto se tomo como ejemplo el SW-BB donde se realizo ping a cada uno de los PC y como resultado se obtuvo el ping fallido para cada uno de ellos ya que no se configuro el enrutamiento Ip en las Vlan a la cual hacen parte, el resultado del SW-BB es el mismo resultado que se dio en los otros Switches al momento de intentar hacer ping con los PC.

CONCLUSIONES

Con esta prueba de habilidades de CCNP se desarrollo los escenarios propuestos satisfactoriamente donde se logro llevar los conocimientos teóricos a un entorno practico con herramientas como GNS3 y Packet Tracer, lo cual ayuda a comprender y a generar mayor conocimiento en los temas, con el desarrollo de los dos escenarios se logro aplicar protocolos de enrutamientos como BGP con una configuración de direccionamiento de IPv4 en interfaces seriales, FastEthernet y Loopback en dispositivos como Routers, también se logró aplicar una configuración de VTP para las actualizaciones de los Switches en las Vlan que posteriormente se crearan y una conexión por medio de configuración de enlace troncal dinámico, auto y estático.

La aplicación que tiene la implementación de VLANS empleando puertos en modo Access y en modo Trunk.

Las ventajas que tiene usar switches administrables Cisco por medio de VLANS, empleando protocolos para troncales como lo es VTP.

El impacto que genera Cisco en las redes y las telecomunicaciones por su estandarización de protocolos enfocados a Switching y Routing.

Se estableció la funcionalidad de los comandos detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

BIBLIOGRAFIA

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

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

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

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

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv6 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx