

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**JUAN GABRIEL ALVARADO PEREZ**

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**JUAN GABRIEL ALVARADO PEREZ**

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*  
BOGOTÁ  
2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

BOGOTÁ 22 DE MAYO DE 2020

## AGRADECIMIENTOS

Agradezco a Dios por bendecirme cada día de mi vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y debilidad. A mis padres, esposa y hermanos por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas

## CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN .....	10
DESARROLLO .....	11
1. ESCENARIO 1.....	11
1.1 Configure una relación de vecino BGP entre R1 y R2.....	12
1.2 Configure una relación de vecino BGP entre R2 y R3.....	15
1.3 Configure una relación de vecino BGP entre R3 y R4.....	17
2. ESCENARIO 2.....	21
2.1 Configurar VTP.....	22
2.2 Configurar DTP (Dynamic Trunking Protocol) .....	23
2.3 Agregar VLANs y asignar puertos .....	25
2.4 Configurar las direcciones Ip en los switches .....	29
2.5 Verificar conectividad extremo a extremo.....	29
CONCLUSIONES .....	35
BIBLIOGRAFÍA.....	36

## LISTA DE TABLAS

Tabla 1. Direccionamiento R1.....	12
Tabla 2. Direccionamiento R2.....	12
Tabla 3. Direccionamiento R3.....	12
Tabla 4. Direccionamiento R4.....	12
Tabla 5. Direccionamiento Interfaz .....	27
Tabla 6. Direccionamiento SW-AA.....	27
Tabla 7. Direccionamiento SW-BB.....	27
Tabla 8. Direccionamiento SW-CC .....	27
Tabla 9. Direccionamiento VLAN 99.....	29

## LISTA DE FIGURAS

Figura 1. Escenario 1 .....	11
Figura 2. Simulación Escenario 1 .....	11
Figura 3. R1 Tabla de Enrutamiento .....	14
Figura 4. R2 Tabla de Enrutamiento .....	15
Figura 5. R2 Tabla de Enrutamiento .....	16
Figura 6. R3 Tabla de Enrutamiento .....	17
Figura 7. R4 Tabla de Enrutamiento .....	19
Figura 8. R3 Tabla de Enrutamiento .....	20
Figura 9. R4 Tabla de Enrutamiento .....	20
Figura 10. Escenario 2 .....	21
Figura 11. Simulación Escenario 2 .....	21
Figura 12. Configuración VTP switches .....	22
Figura 13. Configuración enlace troncal .....	23
Figura 14. Configuración enlace troncal SW-AA.....	24
Figura 15. Configuración enlace troncal SW- BB y SW-CC.....	25
Figura 16. VLANs SW-AA.....	26
Figura 17. VLANs SW-BB.....	26
Figura 18. VLANs SW-CC .....	26
Figura 19. Conectividad entre PCs .....	30
Figura 20. Conectividad entre PCs .....	31
Figura 21. Conectividad entre Switch .....	32
Figura 22. Conectividad de SW-AA a PCs.....	33
Figura 23. Conectividad de SW-BB a PCs.....	33
Figura 24. Conectividad de SW-CC a PCs .....	34

## GLOSARIO

**ROUTER:** Dispositivo de hardware que permite la interconexión de redes, es un dispositivo que permite operar en nivel tres, así mismo comparten una misma conexión a internet.

**SWITCH:** Dispositivo o conmutador de interconexión de redes informáticas, el cual se encarga de transmitir frames, puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

**IPV4:** es la cuarta versión del protocolo de internet, es el que identifica los diferentes dispositivos conectados a la red, se representa normalmente en formato decimal separado por puntos, los 32 bits están subdivididos en octetos de 8 bits cada uno.

**INTERFACES DE RED:** TCP/IP define una interfaz abstracta a través de la cual se accede a dicho hardware. Esta interfaz ofrece un conjunto de operaciones que son las mismas para todos los tipos de hardware y básicamente trata con el envío y la recepción de paquetes.

**MSTP:** Protocolo Múltiple Spanning Tree es un protocolo que crea los arboles de expansión múltiple (casos) para cada LAN virtual (Vlan) en una sola red física. Esto permite para que cada Vlan tenga una Topología configurada del root Bridge y de la expedición. Esto reduce el número de unidades a través de la red y reduce la tensión en las unidades de procesamiento central de los dispositivos de red.

**VLAN:** es una red de área local de carácter virtual, permite crear redes que lógicamente son independientes aunque estas se encuentran dentro de una misma red física

**PROTOCOLO DE RED:** conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación y transferencia de datos entre dos puntos finales.

**VPN (Virtual Private Network):** Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante autenticación y cifrado; por ejemplo los datos se pueden transmitir de forma segura entre dos sucursales a través de internet o cifrarse entre un servidor y un cliente en una red de área local (LAN).

## RESUMEN

La realización del trabajo de habilidades hace parte de un proceso por el cual se pretende obtener un conocimiento sobre redes, los cuales se ven evidenciados en este repositorio dirigido a la Universidad Nacional Abierta y a Distancia UNAD, mediante el diplomado de profundización CISCO CCNP, con el fin de lograr una experiencia de gran importancia para el desarrollo profesional en el campo de las comunicaciones, profundizando temas de conmutación y enrutamiento adquiriendo competencias y habilidades que permiten ser aplicadas en el campo de las telecomunicaciones y la electrónica para un óptimo desempeño laboral y personal.

Durante el desarrollo de los escenarios propuestos se configuran equipos activos de red establecidos en topologías, los cuales se aplican protocolos de enrutamiento BGP, propuestos para su desarrollo; así mismo aplicación de administración y soporte de Switch en redes donde se asemejan a escenarios reales, las cuales incluyen la administración de Vlan y configuración de interfaces troncales.

## ABSTRACT

The realization of the skills work is part of a process by which it is intended to obtain knowledge about networks, which are evidenced in this repository addressed to the National Open and Distance University UNAD, through the CISCO CCNP deepening diploma, with the In order to achieve an experience of great importance for professional development in the field of communications, deepening Switching and Routing topics, acquiring competencies and skills that allow them to be applied in the field of telecommunications and electronics for optimal work and personal performance.

During the development of the proposed scenarios, active network equipment is configured in topologies, which apply BGP routing protocols, proposed for their development; Likewise, Switch management and support application in networks where they resemble real scenarios, which include Vlan administration and trunk interface configuration.

## INTRODUCCIÓN

El presente trabajo contiene el desarrollo de dos escenarios prácticos, los cuales hacen parte de las actividades evaluativas para del diplomado de profundización CCNP, donde uno de los objetivos principales es poner a prueba los niveles de comprensión y entendimiento en temas de ROUTING y SWITCHING, adquiridos en los diferentes módulos de la plataforma de CISCO, estableciendo una serie de objetivos y problemas en los cuales los conocimientos previos deben ser utilizados para su desarrollo en temas de redes de datos.

Para desarrollar el escenario número uno, se realizan diferentes configuraciones establecidas en los procesos de enrutamiento, las cuales son establecidas mediante el protocolo BGP y habilitación de redes Loopback en cada uno de los equipos, posterior al desarrollo de la práctica se realizan pruebas de conectividad verificando las posibles fallas en la conexión, así mismo las soluciones correspondientes.

Por otra parte el desarrollo del escenario número dos, se abordan temas de swtiching donde se implementan protocolos de Vlan trunking Protocol (VTP), configuración de enlaces troncales estáticos en los diferentes equipos activos de red (switch).Igualmente se realiza una descripción detallada de los puntos establecidos en cada escenario donde se relacionan los pasos correspondientes a su configuración y la línea de comandos establecida para obtener los resultados esperados.

# DESARROLLO

## 1. ESCENARIO 1

### Topología de Red

Figura 1. Escenario 1

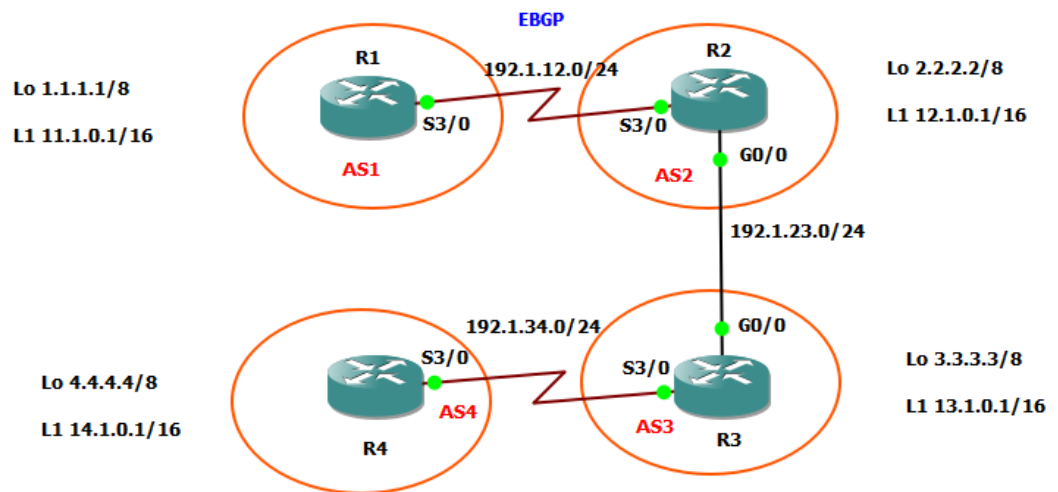


Figura 2. Simulación Escenario 1

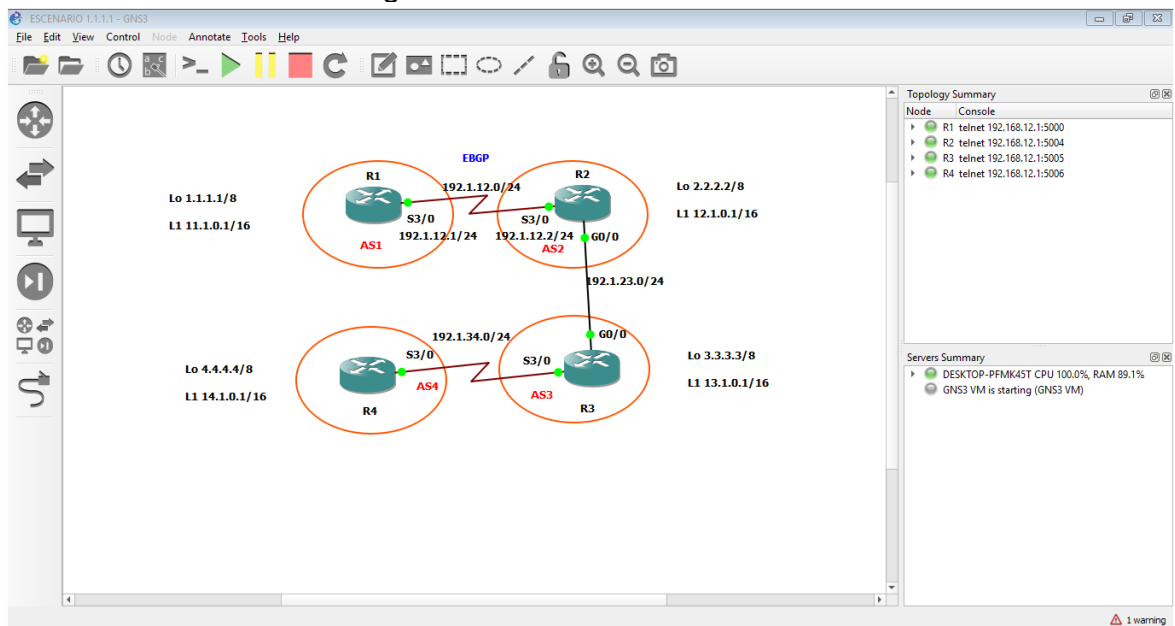


Tabla 1. Direccionamiento R1

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 3/0	192.1.12.1	255.255.255.0

Tabla 2. Direccionamiento R2

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 3/0	192.1.12.2	255.255.255.0
G 0/0	192.1.23.2	255.255.255.0

Tabla 3. Direccionamiento R3

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
S 3/0	192.1.34.3	255.255.255.0
G 0/0	192.1.23.3	255.255.255.0

Tabla 4. Direccionamiento R4

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 3/0	192.1.34.4	255.255.255.0

- 1.1 Configure una relación de vecino BGP entre R1 y R2, R1 debe de estar en AS1 y R2 debe estar en AS2, anuncie las direcciones de Loopback en BGP, codifique los ID para los router paso BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el a paso con los comandos utilizados y la salida del comando **show ip route**.

Como primera medida se realiza la configuración básica del router Luego se procede a realizar la configuración de cada una de las interfaces de los router así:

```
R1#configure terminal
R1 (config) # interface Loopback 0
R1 (config-if) # description Network Link 1
```

```
R1 (config-if) # ip address 1.1.1.1 255.0.0.0
R1 (config-if) # exit
R1 (config) # interface Loopback 1
R1 (config-if) # description Network Link 2
R1 (config-if) # ip address 11.1.0.1 255.255.0.0
R1 (config-if) # exit
R1 (config) # interface Serial 3/0
R1 (config-if) # description R1 -> R2
R1 (config-if) # ip address 192.1.12.1 255.255.255.0
R1 (config-if) # clock rate 128000
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
R1 (config-router) #end
```

```
R2#enable
R2#configure terminal
R2 (config) # interface Loopback 0
R2 (config-if) # description Network Link 3
R2 (config-if) # ip address 2.2.2.2 255.0.0.0
R2 (config-if) # exit
R2 (config) # interface Loopback 1
R2 (config-if) # description Network Link 4
R2 (config-if) # ip address 12.1.0.1 255.255.0.0
R2 (config-if) # exit
R2 (config) # interface Serial 3/0
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) # exit
R2 (config) # interface Gigabit Ethernet 3/0
```

```

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
R2 (config-router) #end

```

Luego de realizar las habilitaciones de las interfaces y la habilitación del protocolo BGP en cada router se procede a ejecutar en comando **show ip route**, el cual va a mostrar en su tabla de enrutamiento cada una de las direcciones y redes loopback que se encuentran conectadas así:

Figura 3. R1 Tabla de Enrutamiento

```

R1
*May 1 13:55:17.363: %BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
R1#
R1#
R1#sh
R1#show ip rou
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, 00:08:56
       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
B       12.0.0.0/16 is subnetted, 1 subnets
       12.1.0.0 [20/0] via 192.1.12.2, 00:08:56
       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial13/0
L       192.1.12.1/32 is directly connected, Serial13/0
R1#

```

Figura 4. R2 Tabla de Enrutamiento

```
R2
[OK]
R2#
R2#
R2#sho
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, 00:13:00
     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
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:13:00
     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
L    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial3/0
L    192.1.12.2/32 is directly connected, Serial3/0
L    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#
```

1.2 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 paso con los comandos utilizados y la salida del comando **show ip route**.

Se procede a realizar la configuración de relación de vecino en R2:

```
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
R2 (config-router) #end
```

Se procede a configurar las interfaces de R3 y BGP así:

```
R3#enable
R3#configure terminal
R3 (config) # interface Loopback 0
R3 (config-if) # description Network Link 5
R3 (config-if) # ip address 3.3.3.3 255.0.0.0
R3 (config-if) # exit
R3 (config) # interface Loopback 1
```

```

R3 (config-if) # description Network Link 6
R3 (config-if) # ip address 13.1.0.1 255.255.0.0
R3 (config-if) # exit

R3 (config) # interface Serial 3/0
R3 (config-if) # description R3 -> R4
R3 (config-if) # ip address 192.1.34.3 255.255.255.0
R3 (config-if) # clock rate 128000
R3 (config-if) # no shutdown
R3 (config-if) # exit

R3 (config) # interface Gigabit Ethernet 3/0
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-if) # exit

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

```

Luego de realizar la configuración en R3, se procede a digitar el comando **show ip route**, en cada uno de los router, donde se observa las tablas de enrutamiento actualizadas. Se observa cuatro rutas a través del protocolo BGP.

Figura 5. R2 Tabla de Enrutamiento

```

R2#show ip rou
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, 03:22:13
C    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, 02:40:34
B    11.0.0.0/16 is subnetted, 1 subnets
     11.1.0.0 [20/0] via 192.1.12.1, 03:22:13
C    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
B    13.0.0.0/16 is subnetted, 1 subnets
     13.1.0.0 [20/0] via 192.1.23.3, 02:40:34
C    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial3/0
L    192.1.12.2/32 is directly connected, Serial3/0
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#

```

Igualmente se digita el comando show ip route en el R3, en el cual se observa la tabla de enrutamiento con las direcciones de red de las interfaces loopback configuradas en el R1 y R2, las cuales se evidencian por el protocolo BGP, es de anotar que la identificación de todas estas redes se realizan por la interfaz Giga Ethernet 0/0, conectado al R2. Demostrado en la siguiente imagen:

Figura 6. R3 Tabla de Enrutamiento

```

R3#
R3#
R3#show ip rou
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, 03:22:01
B    2.0.0.0/8 [20/0] via 192.1.23.2, 03:22:01
    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, 03:22:01
    12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 03:22:01
    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, 03:22:01
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial3/0
L        192.1.34.3/32 is directly connected, Serial3/0
R3#

```

- 1.3 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 paso con los comandos utilizados y la salida del comando **show ip route** inicialmente se configure BGP en R3 y se incluye a la red entre R3 y R4.

```

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

```

Luego se realiza la configuración de las interfaces en R4 su habilitación y configuración de BGP así:

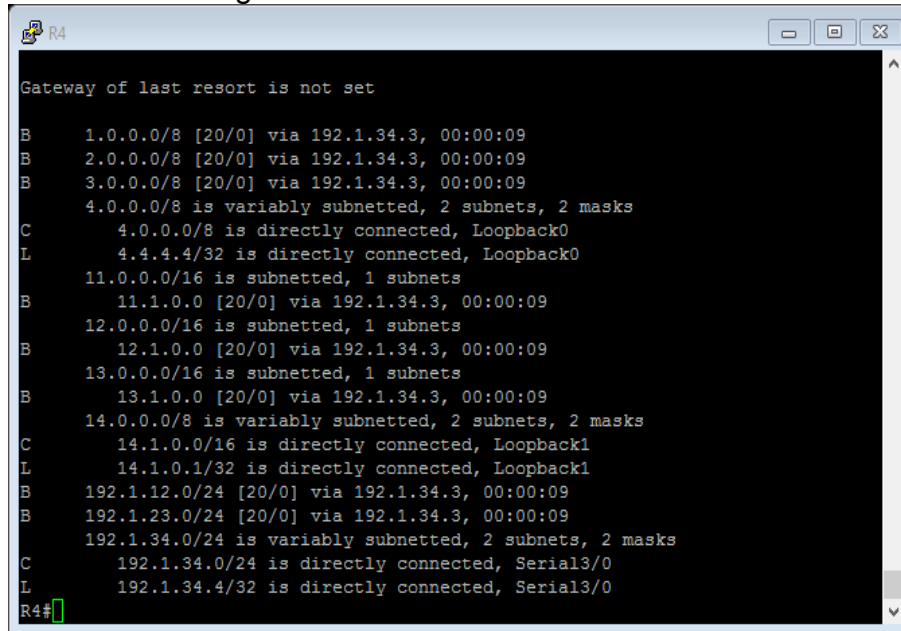
```
R4#enable
R4#configure terminal
R4 (config) # interface Loopback 0
R4 (config-if) # description Network Link 7
R4 (config-if) # ip address 4.4.4.4 255.0.0.0
R4 (config-if) # exit

R4 (config) # interface Loopback 1
R4 (config-if) # description Network Link 8
R4 (config-if) # ip address 14.1.0.1 255.255.0.0
R4 (config-if) # exit

R4 (config) # interface Serial 3/0
R4 (config-if) # description R4 -> R3
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
R4 (config-router) #exit
```

Figura 7. R4 Tabla de Enrutamiento



```
R4
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:09
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:00:09
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:09
    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, 00:00:09
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.34.3, 00:00:09
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.34.3, 00:00:09
    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, 00:00:09
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:09
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial3/0
L    192.1.34.4/32 is directly connected, Serial3/0
R4#
```

Para realizar la relación de vecinos mediante las direcciones loopback, el router vecino requiere realizar la siguiente configuración:

```
R3#configure terminal
```

```
R3 (config) # ip route 4.0.0.0 255.0.0.0 192.1.34.4
```

```
R3 (config) #router bgp 3
```

```
R3 (config-router) # no neighbor 192.1.34.4
```

```
R3 (config-router) # no network 3.0.0.0 mask 255.0.0.0
```

```
R3 (config-router) # neighbor 4.4.4.4 remote-as 4
```

```
R3 (config-router) # neighbor 4.4.4.4 update-source loopback 0
```

```
R3 (config-router) # neighbor 4.4.4.4 ebgp-multihop
```

```
R4#configure terminal
```

```
R4 (config) # ip route 3.0.0.0 255.0.0.0 192.1.34.3
```

```
R4 (config) #router bgp 4
```

```
R4 (config-router) # no neighbor 192.1.34.3
```

```
R4 (config-router) # neighbor 3.3.3.3 remote-as 3
```

```
R4 (config-router) # neighbor 3.3.3.3 update-source loopback 0
```

```
R4 (config-router) # neighbor 3.3.3.3 ebgp-multihop
```

Mediante la ejecución del comando show ip route se puede evidenciar en la tabla de enrutamiento que la dirección que conecta con R4 es la Loopback 0.

Figura 8. R3 Tabla de Enrutamiento

```
R3
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, 00:18:25
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:18:40
    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, 00:18:25
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:18:40
    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 4.4.4.4, 00:01:36
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:18:40
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial13/0
L    192.1.34.3/32 is directly connected, Serial13/0
R3#
```

Igualmente para el R4 se puede evidenciar en su tabla de enrutamiento que la dirección con la que se comunica con sus vecinos BGP ahora es la Loopback 0 de R3.

Figura 9. R4 Tabla de Enrutamiento

```
R4
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:00:10
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:00:10
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 3.3.3.3, 00:00:11
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:00:11
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:00:11
    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 3.3.3.3, 00:00:11
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:00:11
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial13/0
L    192.1.34.4/32 is directly connected, Serial13/0
R4#
```

## 2. ESCENARIO 2

### Topología de Red

Figura 10. Escenario 2

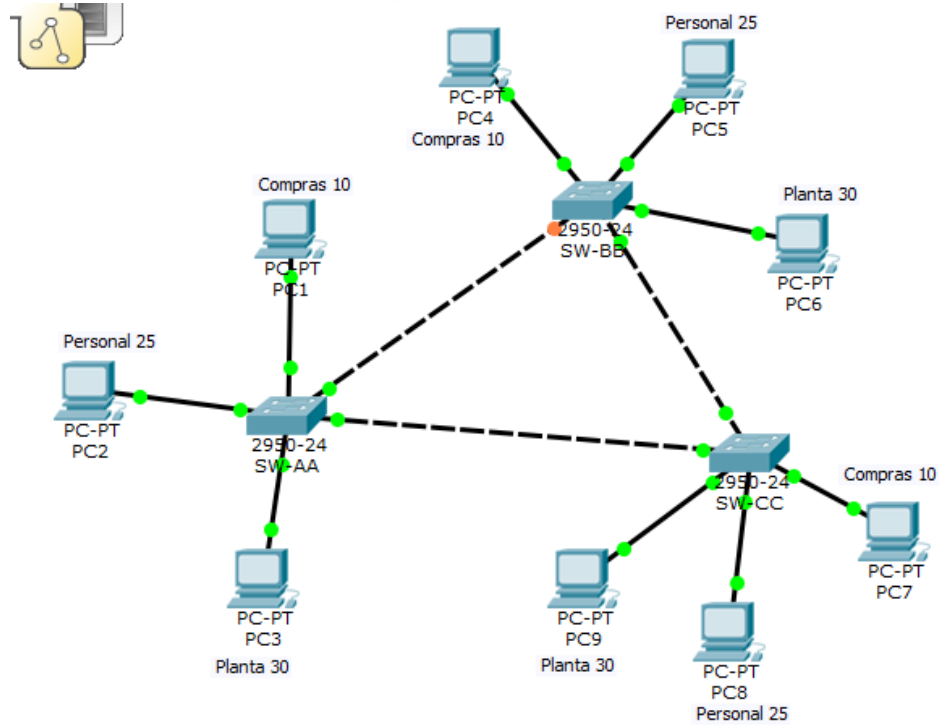
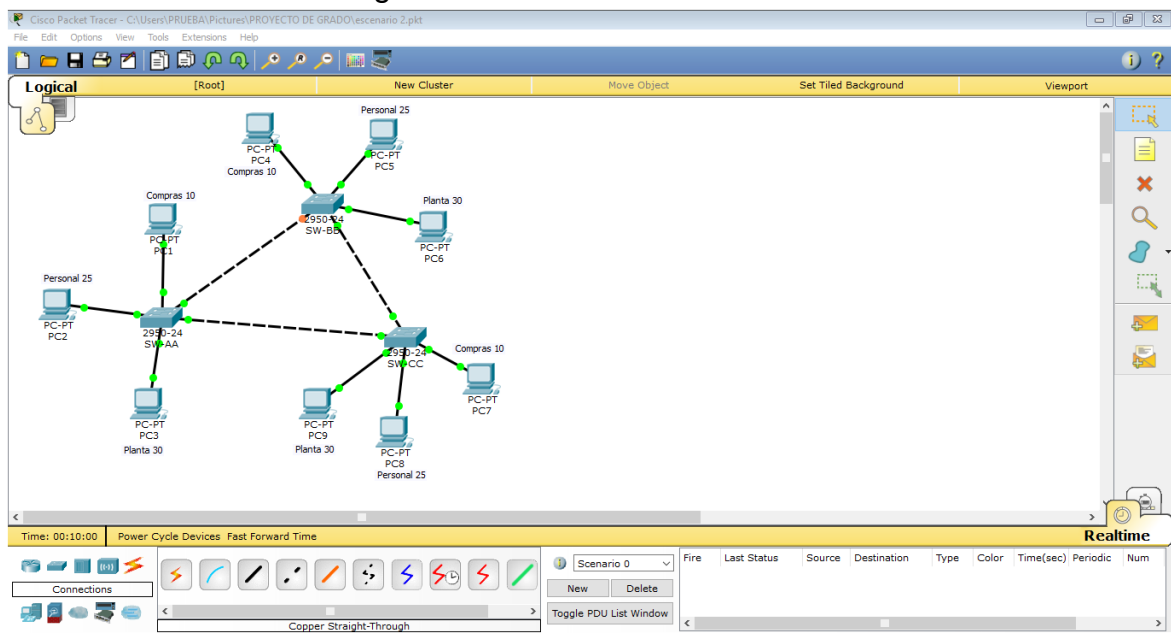


Figura 11. Simulación Escenario 2



## 2.1 Configurar VTP

Todos los switches se configuraran 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 VTP llamado CCNP y usando la contraseña cisco.

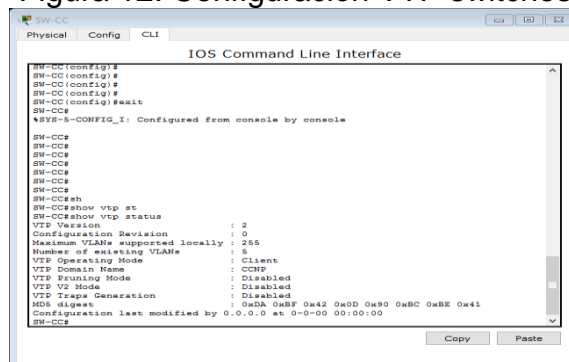
```
Switch #configure terminal
Switch (config) #hostname SW-AA
SW-AA (config) #vtp mode client
SW-AA (config) #vtp domain CCNP
SW-AA (config) #vtp password cisco
SW-AA (config) #exit
```

```
Switch #configure terminal
Switch (config) #hostname SW-BB
SW-BB (config) #vtp mode server
SW-BB (config) #vtp domain CCNP
SW-BB (config) #vtp password cisco
SW-BB (config) #exit
```

```
Switch #configure terminal
Switch (config) #hostname SW-CC
SW-CC (config) #vtp mode client
SW-CC (config) #vtp domain CCNP
SW-CC (config) #vtp password cisco
SW-CC (config) #exit
```

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

Figura 12. Configuración VTP switches



```
SW-CC
Physical Config CLI
IOS Command Line Interface
SW-CC(config)#
SW-CC(config)#
SW-CC(config)#
SW-CC(config)#
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#
SW-CC#show vtp st
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 Trap Generation : Disabled
MD5 digest : 0aDA 0aBF 0a42 0a0D 0a90 0aBC 0aBE 0a41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

```

SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp pass
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#
SW-AA#
SW-AA#
SW-AA#sh
SW-AA#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
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xEE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#

```

```

SW-BB(config)#
SW-BB(config)#vtp pas
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
SW-BB(config)#
SW-BB(config)#
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#
SW-BB#
SW-BB#
SW-BB#sh
SW-BB#show vtp st
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
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xEE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updates ID is 0.0.0.0 (no valid interface found)
SW-BB#

```

## 2.2 Configurar DTP (Dynamic Trunking Protocol)

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

Verifique el enlace troncal “trunk” entre SW-AA y SW-BB usando el comando show interfaces trunk.

Figura 13. Configuración enlace troncal

```

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
SW-AA#
SW-AA#
SW-AA#
SW-AA#sh
SW-AA#show in
SW-AA#show interfaces trun
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
SW-AA#
SW-AA#
SW-AA#

```

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
SW-BB (config-if)#
SW-BB (config-if)#
SW-BB (config-if)#exit
SW-BB (config)#
SW-BB (config)#
SW-BB (config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#
SW-BB#
SW-BB#sh
SW-BB#show inter
SW-BB#show interfaces tr
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    none
SW-BB#

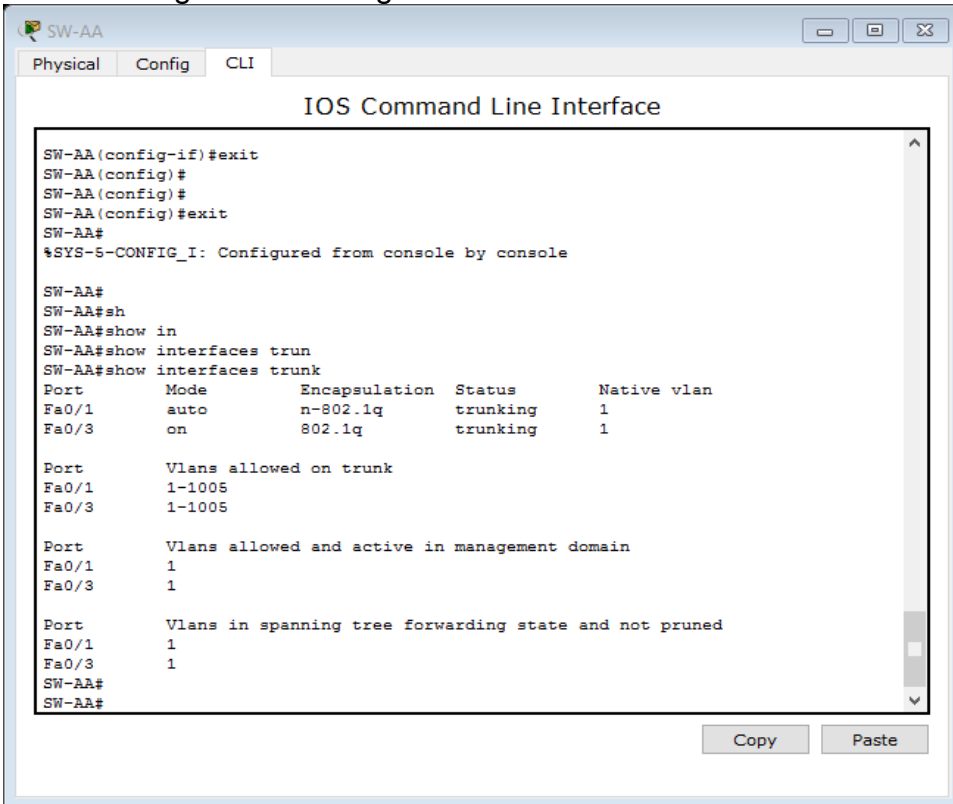
```

Entre SW-AA y SW-CC configure un enlace “trunk” estático utilizando el comando switch port mode trunk en la interfaz E0/1 de SW-AA.

```
SW-AA #configure terminal
SW-AA (config) # interface Ethernet 0/3
SW-AA (config-if) #switchport mode trunk
SW-AA (config-if) #exit
```

Verifique el enlace “trunk” el comando show interfaces trunk en SW-AA

Figura 14. Configuración enlace troncal SW-AA



```
SW-AA
Physical Config CLI
IOS Command Line Interface

SW-AA(config-if)#exit
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#
SW-AA#sh
SW-AA#show in
SW-AA#show interfaces trun
SW-AA#show interfaces trunk
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

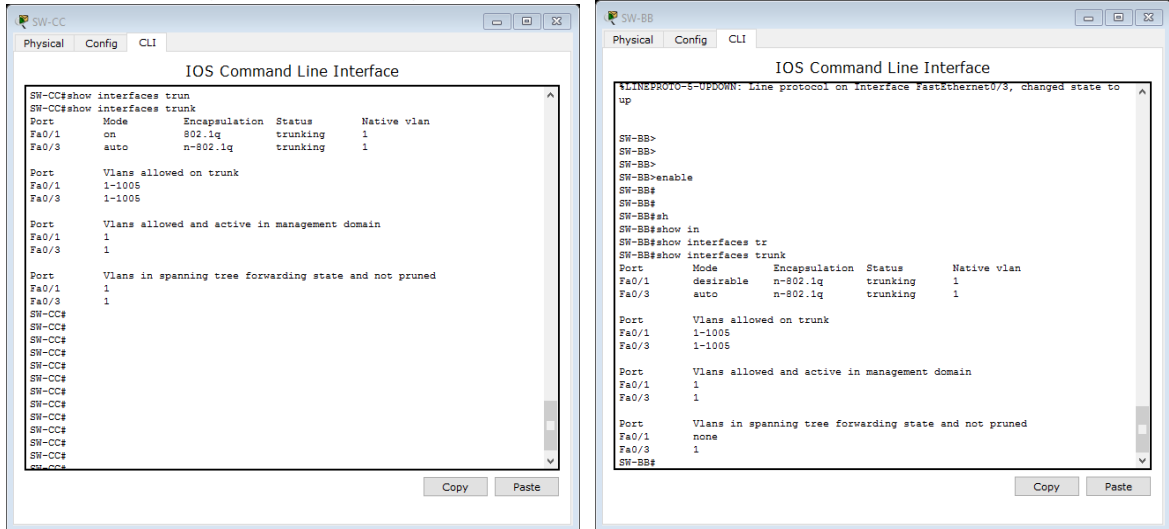
Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1
SW-AA#
SW-AA#
```

Configure un enlace “trunk” permanente entre SW-BB y SW-CC

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

Figura 15. Configuración enlace troncal SW- BB y SW-CC



### 2.3 Agregar VLANs y asignar puertos

En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs compras (10), personal (25), Planta (30) y Admon (99).

```
SW-AA # configure terminal
```

```
SW-AA (config) # vlan 10
```

VTP VLAN configuration not allowed when device is in CLIENT mode.

```
SW-AA (config-vlan) #exit
```

No se puede realizar esta tarea teniendo en cuenta que se encuentra configurado el SW. En modo cliente por lo cual toda la configuración de VLANs deberán configurarse en el SW que se tomó como SERVER el cual es SW-BB.

A continuación se agregan las Vlan mencionadas en SW-BB (server) así:

```
SW-BB # configure terminal
```

```
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

Verifique que las VLANs han sido agregadas correctamente.

Figura 16. VLANs SW-AA

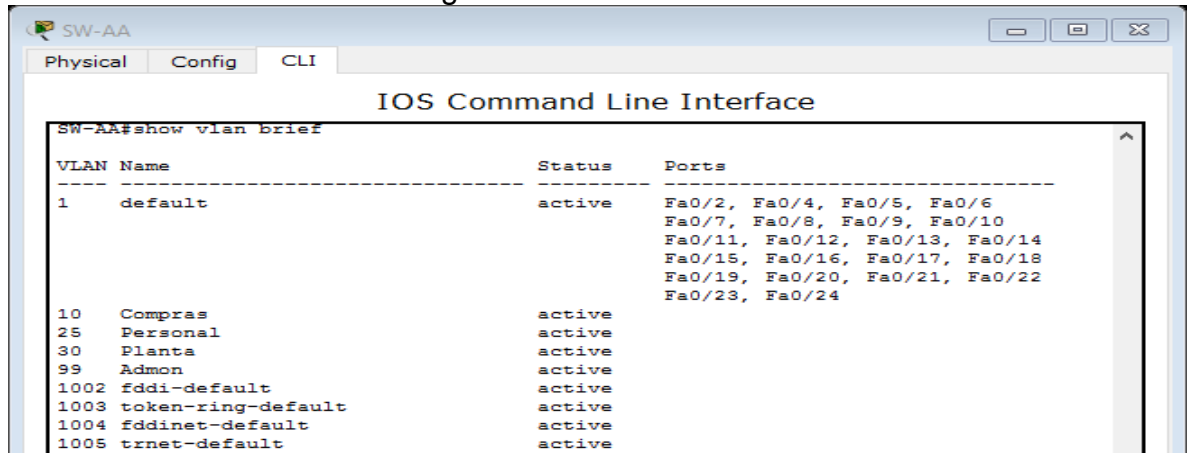


Figura 17. VLANs SW-BB

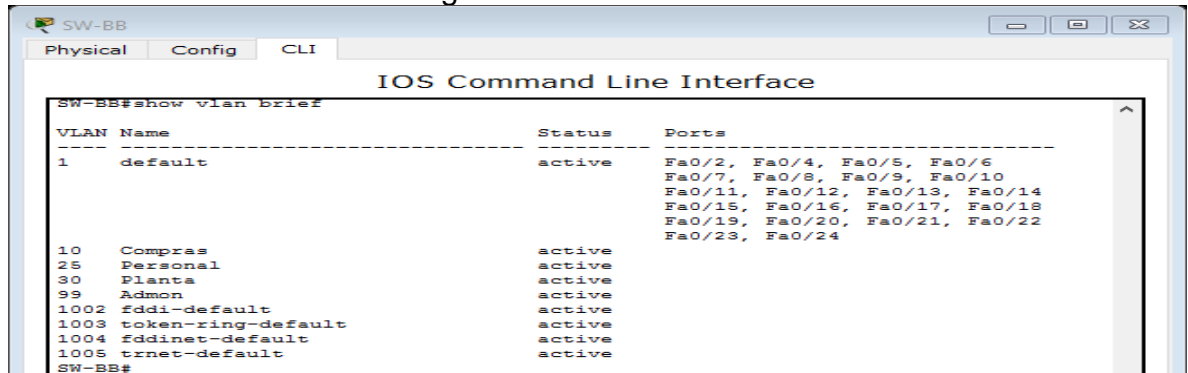
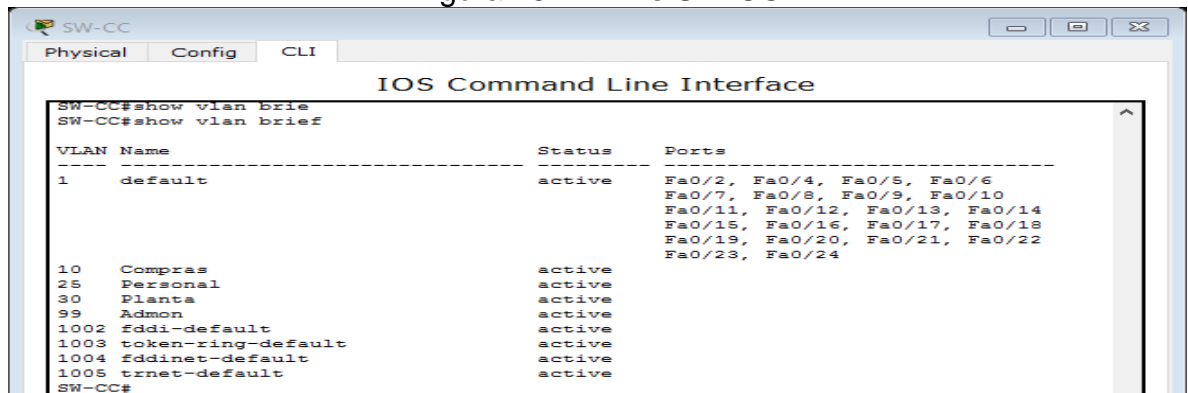


Figura 18. VLANs SW-CC



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

Tabla 5. Direccionamiento Interfaz

Interfaz	VLAN	Direcciones IP 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

X= número de cada PC particular

Se realiza la distribución del direccionamiento IP según tabla anterior:

Tabla 6. Direccionamiento SW-AA

SW-AA		
Interfaz	VLAN	Direcciones IP PCs
F0/10	Vlan 10	190.108.10.10 /24
F0/15	Vlan 25	190.108.20.10 /24
F0/20	Vlan 30	190.108.30.10 /24

Tabla 7. Direccionamiento SW-BB

SW-BB		
Interfaz	VLAN	Direcciones IP PCs
F0/10	Vlan 10	190.108.10.20 /24
F0/15	Vlan 25	190.108.20.20 /24
F0/20	Vlan 30	190.108.30.20 /24

Tabla 8. Direccionamiento SW-CC

SW-CC		
Interfaz	VLAN	Direcciones IP PCs
F0/10	Vlan 10	190.108.10.30 /24
F0/15	Vlan 25	190.108.20.30 /24
F0/20	Vlan 30	190.108.30.30 /24

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

Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB, 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 Ethernet 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) # interface Ethernet 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) # interface Ethernet F0/20
SW-AA (config-if) # switchport mode access
SW-AA (config-if) # switchport access vlan 30
SW-AA (config-if) # exit
```

```
SW-BB # configure terminal
SW- BB (config) # interface Ethernet 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) # interface Ethernet 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) # interface Ethernet F0/20
SW- BB (config-if) # switchport mode access
SW- BB (config-if) # switchport access vlan 30
SW- BB (config-if) # exit
```

```
SW-CC # configure terminal
SW- CC (config) # interface Ethernet 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) # interface Ethernet 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) # interface Ethernet F0/20
SW- CC (config-if) # switchport mode access
SW- CC (config-if) # switchport access vlan 30
SW- CC (config-if) # exit

```

## 2.4 Configurar las direcciones Ip en los switches

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 9. Direccionamiento VLAN 99

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 # configure terminal
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 # configure terminal
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 # configure terminal
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

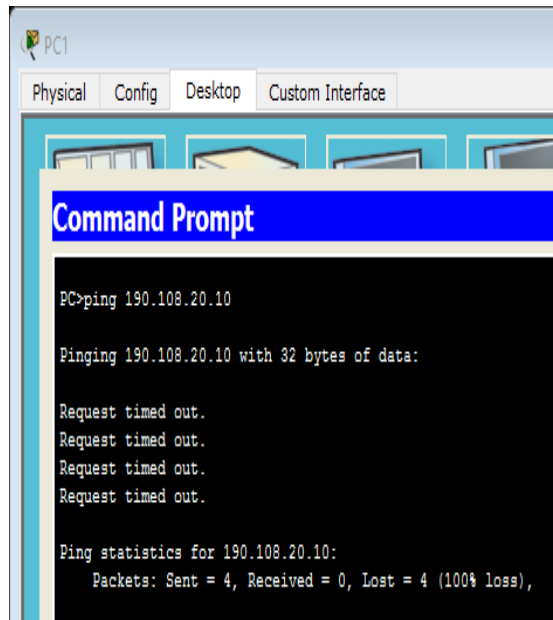
```

## 2.5 Verificar conectividad extremo a extremo

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

Figura 19. Conectividad entre PCs

Ping PC1 A PC2



```
PC1
Physical Config Desktop Custom Interface

Command Prompt

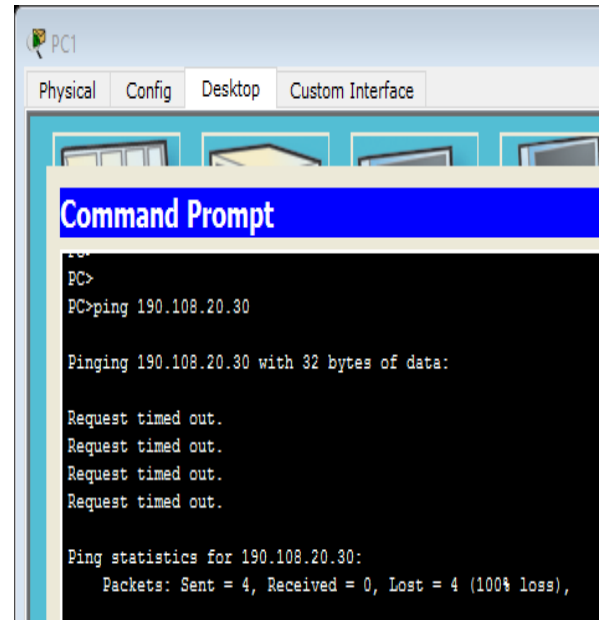
PC>ping 190.108.20.10

Pinging 190.108.20.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping PC1 A PC8



```
PC1
Physical Config Desktop Custom Interface

Command Prompt

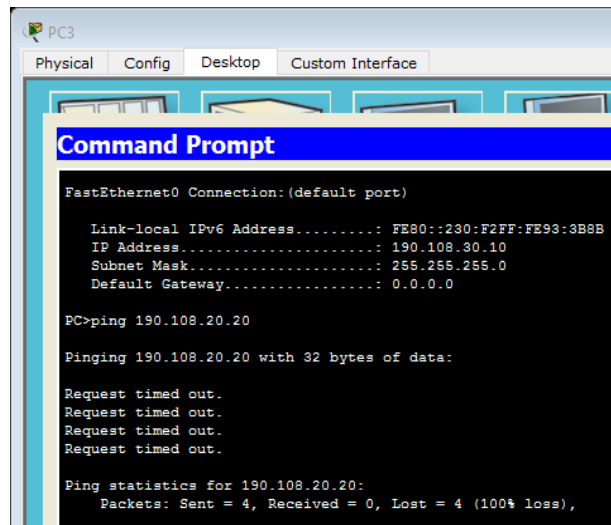
PC>
PC>ping 190.108.20.30

Pinging 190.108.20.30 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping PC3 A PC5



```
PC3
Physical Config Desktop Custom Interface

Command Prompt

FastEthernet0 Connection: (default port)

Link-local IPv6 Address . . . . . : FE80::230:F2FF:FE93:3B8B
IP Address . . . . . : 190.108.30.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0

PC>ping 190.108.20.20

Pinging 190.108.20.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Al ejecutar el comando ping en cada uno de los equipos se logró observar que no hay comunicación entre PCs que están en diferente segmento, es decir no se pueden comunicar teniendo en cuenta el protocolo de Vlan las cuales están configuradas en tres segmentos diferentes, por lo cual equipos con diferente Vlan no tienen comunicación alguna.

Figura 20. Conectividad entre PCs

Ping PC2 A PC5

```
PC2
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>IPCONFIG

FastEthernet0 Connection: (default port)

Link-local IPv6 Address . . . . . : FE80::201:96FF:FE29:D0B5
IP Address . . . . . : 190.108.20.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0

PC>ping 190.108.20.20

Pinging 190.108.20.20 with 32 bytes of data:

Reply from 190.108.20.20: bytes=32 time=0ms TTL=128
Reply from 190.108.20.20: bytes=32 time=0ms TTL=128
Reply from 190.108.20.20: bytes=32 time=0ms TTL=128
Reply from 190.108.20.20: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.20.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping PC9 A PC3

```
PC9
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address . . . . . : FE80::2E0:B0FF:FE82:CD8B
IP Address . . . . . : 190.108.30.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0

PC>ping 190.108.30.10

Pinging 190.108.30.10 with 32 bytes of data:

Reply from 190.108.30.10: bytes=32 time=0ms TTL=128
Reply from 190.108.30.10: bytes=32 time=0ms TTL=128
Reply from 190.108.30.10: bytes=32 time=0ms TTL=128
Reply from 190.108.30.10: bytes=32 time=0ms TTL=128

Ping statistics for 190.108.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping PC7 A PC1

```
PC7
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address . . . . . : FE80::201:96FF:FE7C:E1ED
IP Address . . . . . : 190.108.10.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 0.0.0.0

PC>ping 190.108.10.10

Pinging 190.108.10.10 with 32 bytes of data:

Reply from 190.108.10.10: bytes=32 time=1ms TTL=128
Reply from 190.108.10.10: bytes=32 time=0ms TTL=128
Reply from 190.108.10.10: bytes=32 time=0ms TTL=128
Reply from 190.108.10.10: bytes=32 time=0ms TTL=128

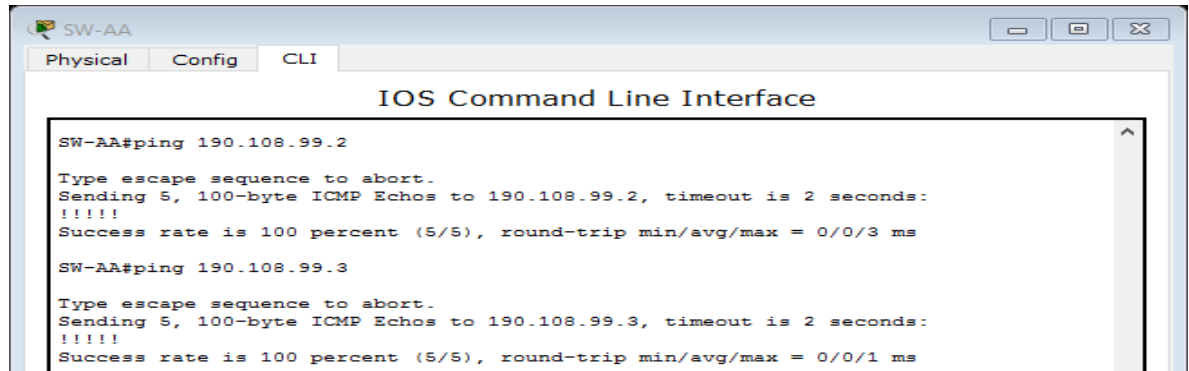
Ping statistics for 190.108.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Al ejecutar el comando ping en cada equipo se logra observar el envío de paquetes de manera satisfactoria entre equipos de la misma Vlan ya que de acuerdo a su configuración se logran comunicar satisfactoriamente.

Ejecute el ping desde cada switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Figura 21. Conectividad entre Switch

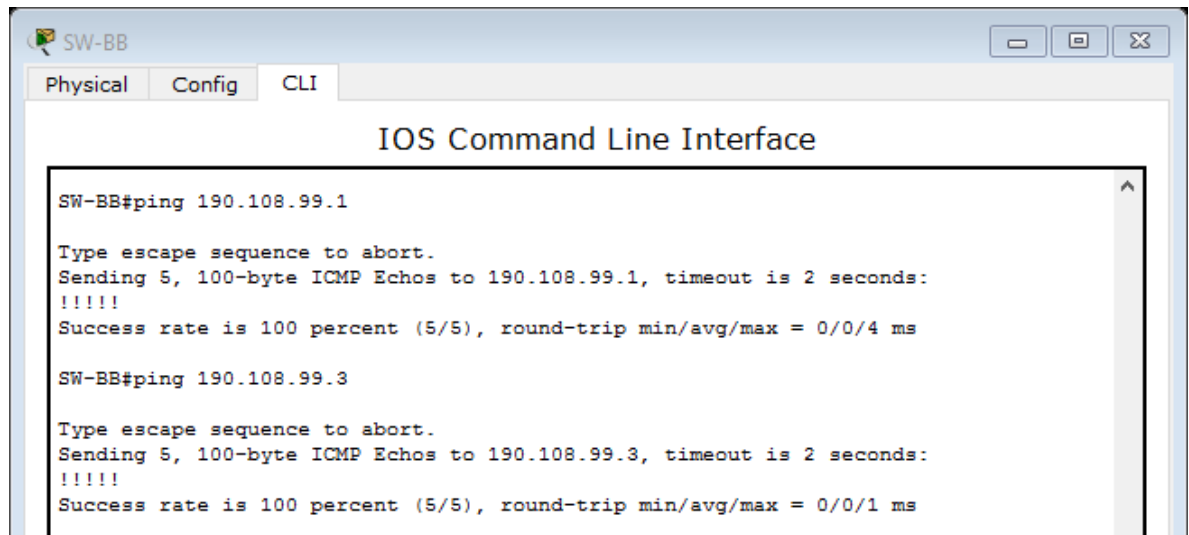
Ping SW-AA a SW-BB, SW-CC



```
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 = 0/0/3 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 = 0/0/1 ms
```

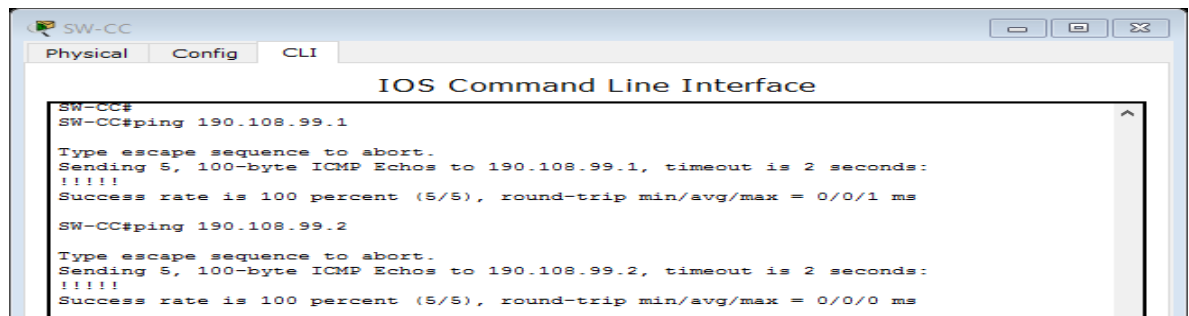
Ping SW-BB a SW-AA, SW-CC



```
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 = 0/0/4 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
```

Ping SW-CC a SW-AA, SW-BB



```
SW-CC#
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

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
```

Al ejecutar el comando ping en cada uno de los SW, se evidencia el envío de paquetes de manera satisfactoria, teniendo en cuenta su configuración en modo troncal realizada en cada una de las interfaces, así mismo el tipo de encapsulamiento lo cual es compatible para su comunicación entre SW.

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

Figura 22. Conectividad de SW-AA a PCs



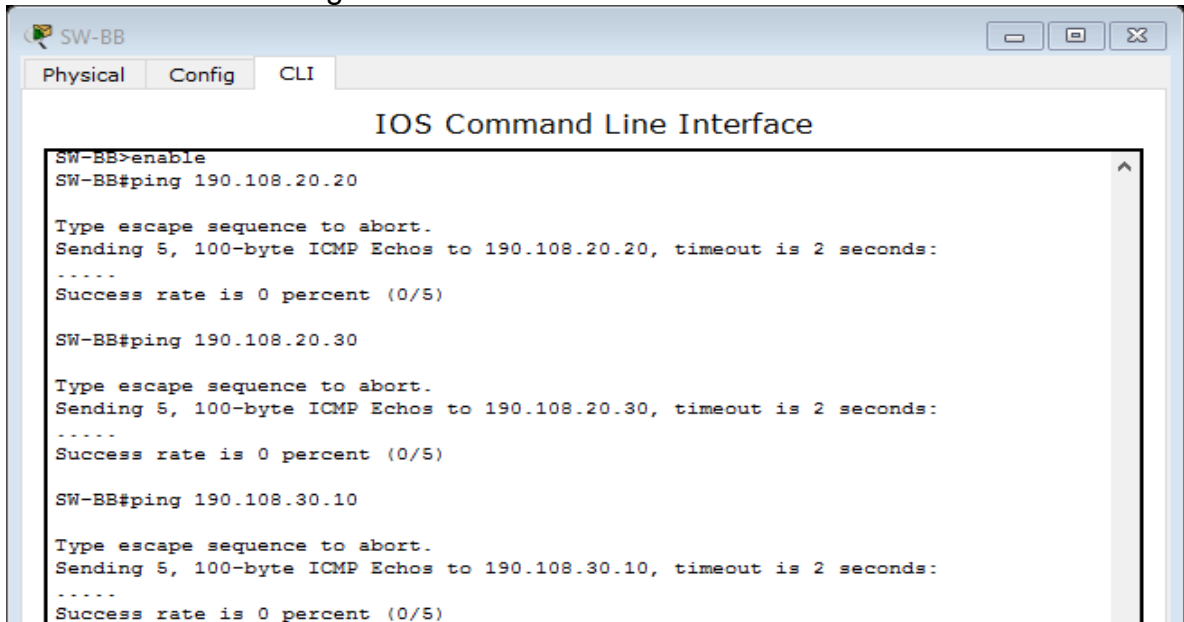
```
SW-AA#
SW-AA#ping 190.108.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.30, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 23. Conectividad de SW-BB a PCs

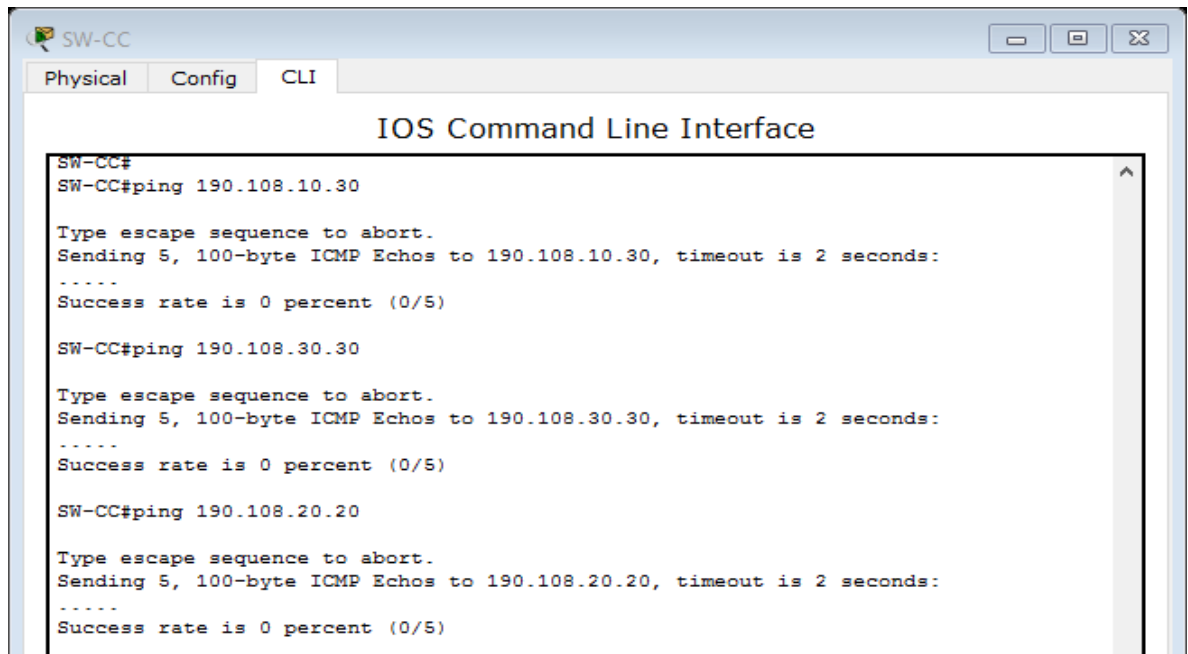


```
SW-BB>enable
SW-BB#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.30, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 24. Conectividad de SW-CC a PCs



```
SW-CC#
SW-CC#ping 190.108.10.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.30, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.30, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.20.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Al ejecutar el comando ping desde cada SW a los PC, no se logró comunicación alguna, debido a su configuración realizada ya que las interfaces deberían de tener un direccionamiento IP dentro de los segmentos de red configurados, así mismo tenga un protocolo de enrutamiento para su conexión.

## CONCLUSIONES

Mediante la realización del trabajo se logró comprender aspectos importantes en switching y routing a través de cada uno de los protocolos establecidos y la temática comprendida en los diferentes capítulos propuestos en la plataforma, donde se abordaron temas como protocolos de enrutamiento BGP; de igual manera protocolos como VTP, DTP, configuración de VLANs y enlaces troncales en equipos activos de red.

Con el desarrollo de las actividades del presente trabajo, se logra entender conceptos vistos en el diplomado de CCNP, así mismo el uso de herramientas de simulación como Packet Tracer y GNS3, los cuales permitieron el desarrollo óptimo en los escenarios propuestos, aplicando los protocolos y configuraciones aprendidas en cada uno de los módulos del diplomado.

Se adquieren habilidades prácticas en el desarrollo de cada uno de los escenarios, donde se aplican protocolos de enrutamiento como BTP y configuración de puertos troncales, así mismo la creación de VLAN y su distribución entre equipos activos de red.

Los escenarios propuestos para este trabajo lograron adquirir habilidades y destrezas en la ejecución de línea de comandos en los cuales se realizan las configuraciones en los equipos activos (router, switch), igualmente la visualización de los comandos utilizados en cada una de las interfaces.

La conectividad en cada escenario es de vital importancia y sus pruebas realizadas entre equipos permitieron el entendimiento del ejercicio, igualmente los fallos presentados, ya que se requiere una revisión minuciosa de cada procedimiento adelantado, verificando las configuraciones faltantes y realizando la solución más viable para la correcta configuración de los equipos propuestos en el escenario.

## BIBLIOGRAFÍA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). V. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>.

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>.

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

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl>.