

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HERNAN DARIO RIVERA MOLINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
ZIPAQUIRA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HERNAN DARIO RIVERA MOLINA

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 BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
ZIPAQUIRA
2020

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

ZIPAQUIRA, 16 de mayo de 2020

AGRADECIMIENTOS

Quiero dar gracias a Dios por la vida y todas las bendiciones recibidas, gracias a todas las personas que me alentaron con su afecto y motivación para no desfallecer en la realización de este proyecto de vida. Pero en especial un gran agradecimiento a mi esposa Olga Janneth, a mis hijos Julián Andrés y Juan Camilo por su paciencia, amor y apoyo incondicional, ellos saben que son la razón que me impulsan para ser cada día mejor persona y profesional.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	9
RESUMEN	10
ABSTRACT.....	10
INTRODUCCION.....	11
DESARROLLO.....	12
1.Escenario 1.....	12
2.Escenario 2.....	26
CONCLUSIONES.....	44
BIBLIOGRAFIA.....	45

LISTA DE TABLAS

Tabla 1. Configuración de los Routers.....	12
Tabla 2. Configuración de direcciones ip de PCs.....	35
Tabla 3. Direcciones ip de PCs.....	35
Tabla 4. Direcciones ip para VLAN 99.....	39

LISTA DE FIGURAS

Figura 1. Escenario 1.....	12
Figura 2. Simulación escenario 1.....	13
Figura 3. Configuración de router R1.....	14
Figura 4. Configuración router R2.....	16
Figura 5. Comando show ip route R1.....	17
Figura 6. Comando show ip route R2.....	18
Figura 7. Configuración de R2 paso 2.....	19
Figura 8. Configuración de router 3.....	20
Figura 9. Verificación de relación vecinos R2-R3.....	21
Figura 10. Verificación de comando Router 3.....	22
Figura 11. Configuración de router R4.....	23
Figura 12. Configuración de adyacencia de vecinos.....	24
Figura 13. Escenario 2.....	25
Figura 14. Simulación escenario 2.....	26
Figura 15. Configuración router SW-AA como cliente.....	27
Figura 16. Configuración router SW-BB//SW-CC como servidor.....	28
Figura 17. Verificaciones configuraciones routers para VTP.....	29
Figura 18. Configuración enlace trunca en SW-BB.....	30
Figura 20. Configuración enlace trunk interfaz F0/3 en SW-AA.....	31
Figura 21. Verificación enlace trunk en SW-AA.....	31
Figura 22. Configuración enlace trunk permanente.....	32
Figura 23. Configuración de VLANs.....	32
Figura 24. Verificación de VLANs.....	34
Figura 25. Configuración mode Access router SW-AA.....	36
Figura 26. Configuración mode Access router SW-BB.....	37

Figura 27. Configuración mode Access router SW-CC.....	38
Figura 28. Configuración mode Access router SW-CC.....	40
Figura 29. Ping de PC0 a PC3.....	41
Figura 30. Ping de PC4 A PC6.....	42
Figura 31. Ping de PC0 a switch SW-AA Y SW-BB.....	43

GLOSARIO

BORDER GATEWAY PROTOCOL (BGP): Es el protocolo de puerta de enlace de frontera, se caracteriza por proporcionar un sistema de enrutamiento Inter dominio que garantice el intercambio de información de enrutamiento sin bucles entre sistemas autónomos. Los enrutadores BGP intercambian información sobre rutas a redes de destino. es el protocolo de enrutamiento utilizado en Internet

DYNAMIC ROUTING PROTOCOL: protocolo de enrutamiento encargado de intercambiar información de accesibilidad de red entre enrutadores y adaptarse dinámicamente a los cambios de red. Estos protocolos utilizan algoritmos de enrutamiento para determinar la ruta óptima entre diferentes segmentos de la red y actualizar las tablas de enrutamiento con las mejores rutas.

ROUTED PORT: una interfaz de capa 3 pura similar a un puerto enrutado en un enrutador Cisco IOS.

SWITCH VIRTUAL INTERFACE (SVI): una interfaz VLAN virtual para el enrutamiento entre VLAN. En otras palabras, las interfaces virtuales de conmutación (SVI) son las interfaces VLAN enrutadas virtuales.

VTP (VLAN TRUNKING PROTOCOL): se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de las VLAN en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un dominio de administración VTP. Un dominio VTP para una red es un conjunto contiguo de *switches* unidos con enlaces *trunk* que tienen el mismo nombre de dominio VTP.

RESUMEN

En el siguiente documento se realizó la prueba de habilidades prácticas CCNP desarrollando el ejercicio del escenario 1 aplicando el protocolo de enrutamiento EBGP que permitió configurar una relación de vecino BGP entre los routers además de codificar los ID para los routers BGP y anunciar las direcciones de Loopback en BGP. Para la realización del escenario 1 se inició con la configuración básica de los routers e interfaces para continuar con la configuración del protocolo bgp y de esta forma establecer las relaciones entre vecinos BGP.

En el escenario 2 se configuraron los switches para VTP, iniciando con la configuración de los switches en modo servidor y cliente, se configuró el enlace troncal dinámico, estático y permanente mediante el comando switchport mode trunk. También se agregaron las VLANs, se asignaron los puertos y dirección ip de los pcs para obtener mediante la verificación del ping los resultados de la conectividad

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

In the following document, the CCNP practical skills test was carried out developing the exercise of scenario 1 applying the EBGP routing protocol that allowed configuring a BGP neighbor relationship between the routers in addition to encoding the IDs for the BGP routers and announcing the Loopback addresses in BGP. For the realization of scenario 1, the basic configuration of the routers and interfaces was started to continue with the configuration of the bgp protocol and thus establish the relationships between BGP neighbors.

In scenario 2 the switches were configured for VTP, starting with the configuration of the switches in server and client mode, the dynamic, static and permanent trunking connection was configured using the switchport mode trunk command. VLANs were also added, the ports and IP addresses of the pcs were assigned to obtain the results of the connectivity through the ping verification

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics

INTRODUCCION

La globalización avanza a través del crecimiento de las diferentes tecnologías adaptadas por diversas industrias y servicios, en el caso de las telecomunicaciones las tecnologías de red también han evolucionado hacia equipos rápidos, escalables y funcionales sin afectar el rendimiento de las redes locales y globales.

La conectividad a nivel empresarial es un tema que abarca grandes retos en cuanto a rendimiento, confiabilidad, seguridad y funcionalidad, por ello las empresas deben adaptar protocolos de redes que brinden todas estas características dentro de sus equipos de trabajo. El protocolo BGP es un protocolo de enrutamiento que se utiliza en internet, las empresas lo utilizan cuando se conectan a sus proveedores de servicios de internet (ISP), además que se caracteriza por ser un protocolo robusto y escalable permitiendo el intercambio de información sobre rutas a redes de destino y ofreciendo soluciones a los problemas que se presenten en la conectividad a internet, evitando consumos de ancho de banda excesivos o consumos de los recursos de la CPU del router.

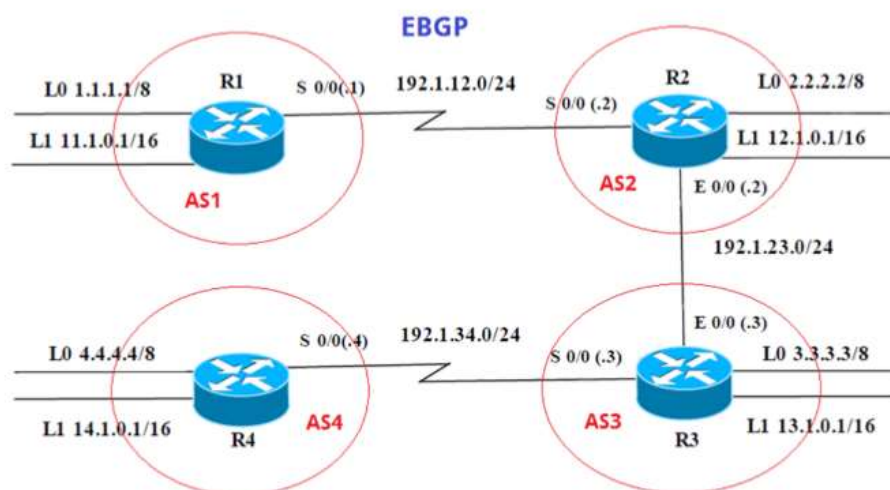
La implementación de las VLANs forma parte de los temas importantes dentro de la conectividad empresarial su llegada ha logrado ciertos beneficios dentro de las redes como por ejemplo disminución en la transmisión del tráfico de la red, mayor flexibilidad en los cambios y administración de la red, mejoras en cuanto a seguridad. las VLANs en equipos cisco pueden ser configuradas mediante el protocolo VTP permitiendo la administración en un dominio de VLANs más simplificado y centralizado.

Por lo tanto, el siguiente documento pretende presentar la aplicación de dos protocolos de red utilizados dentro de las telecomunicaciones como parte del ciclo formativo académico y profesional. De esta manera el estudiante puede apropiarse y afianzar los conocimientos del diplomado CCNP.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1



R1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

R2

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

R3

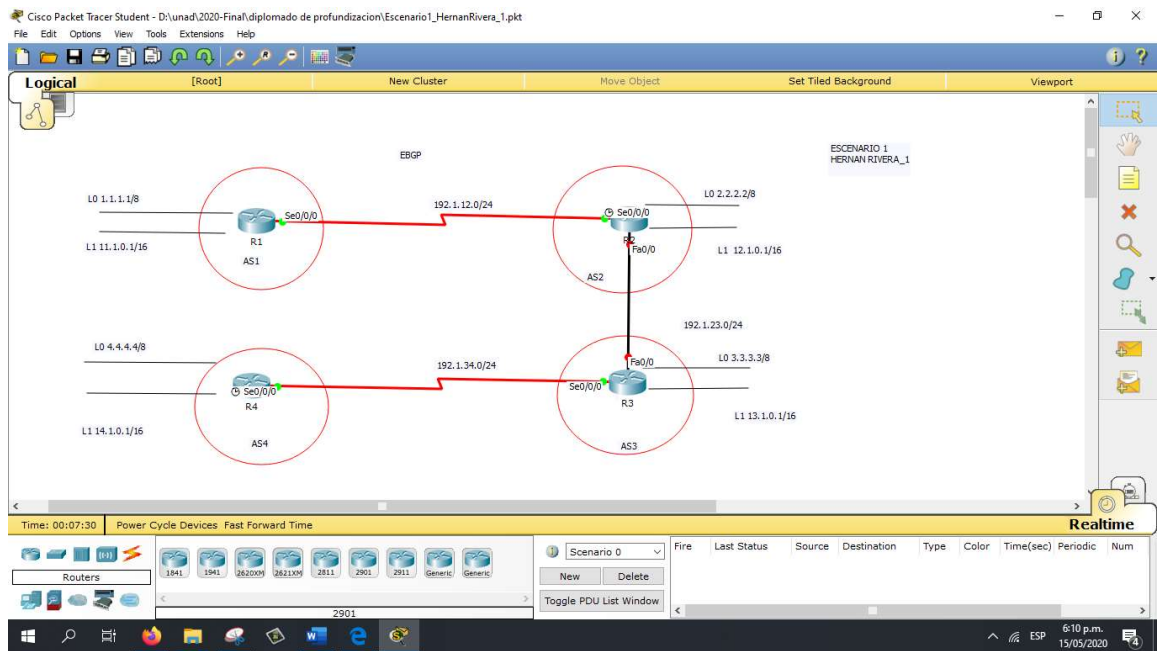
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

R4

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

Tabla 1. Información para configuración de los Routers

. Figura 2. Simulación escenario 1



1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route

```
R1#enable
R1#configure terminal
R1(config)#hostname R1
R1(config)# no ip domain-lookup
R1(config)# line con 0
R1(config-line)# logging synchronous
R1(config-line)# exec-timeout

R1(config)# interface Lo0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config)# interface Lo1
```

```

R1(config-if)# ip address 11.1.0.1 255.255
R1(config)# interface Serial 2/0
R1(config-if)# description R1 -> R2
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-AS 2

```

Figura 3. Configuración de router R1

```

-D:\unad\2020-Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
ols Extensions Help
R1
Physical Config CLI
IOS Command Line Interface
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout
% Incomplete command.
R1(config-line)#exit
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#description R1 -> R2
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
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)#

```

```
R2#enable
R2#configure terminal
R2(config)#hostname R2
R2(config)# no ip domain-lookup
R2(config)# line con 0
R2(config-line)# logging synchronous
R2(config-line)# exec-timeout

R2(config)# interface Lo0
R2(config-if)# ip address 2.2.2.2 255.0.0.0
R2(config)# interface Lo1
R2(config-if)# ip address 12.1.0.1 255.255.0.0

R2(config)# interface Serial 0/0/0
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)# interface f 0/0
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
```

Figura 4. Configuración router R2

```
si\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
R2
Physical Config CLI
IOS Command Line Interface
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exec-timeout
% Incomplete command.
R2(config-line)#exit
R2(config)#interface Lo0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Lol

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface Serial 0/0/0
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)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface f 0/0
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)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

Figura 5. Comando show ip route R1

```
D:\unad\2020-Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
ols  Extensiones  Help
R1
Physical  Config  CLI
IOS Command Line Interface
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 11.1.0.0 mask 255.255.0.0
R1(config-router)#neighbor 192.1.12.2 remote-AS 2
R1(config-router)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R1(config-router)##BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:56:39
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 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, 00:56:39
C    192.1.12.0/24 is directly connected, Serial0/0/0
R1#
```

Figura 6. Comando show ip route R2

```
id\2020-Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
xtensions Help
R2
[Root] Physical Config CLI
IOS Command Line Interface
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:57:42
C    2.0.0.0/8 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, 00:57:42
     12.0.0.0/16 is subnetted, 1 subnets
C    12.1.0.0 is directly connected, Loopback1
C    192.1.12.0/24 is directly connected, Serial0/0/0
R2#
```

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

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

Figura 7. Configuración de R2 paso 2

```

unad\2020-Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
Extensions H
R2
Physical Config CLI
[Root]
IOS Command Line Interface
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

B 1.0.0.0/8 [20/0] via 192.1.12.1, 00:57:42
C 2.0.0.0/8 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, 00:57:42
12.0.0.0/16 is subnetted, 1 subnets
C 12.1.0.0 is directly connected, Loopback1
C 192.1.12.0/24 is directly connected, Serial0/0/0
R2#configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
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)#
  
```

```

R3#enable
R3#configure terminal
R3(config)#hostname R3
R3(config)# no ip domain-lookup
R3(config)# line con 0
R3(config-line)# logging synchronous
R3(config-line)# exit

R3(config)# interface Lo0
R3(config-if)# ip address 3.3.3.3 255.0.0.0
R3(config)# interface Lo1
R3(config-if)# ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface f 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)# interface Serial 0/0/0
R3(config-if)# description R3 -> R4
R3(config-if)# ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-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

```

Figura 8. Configuración de router 3

```

>Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
R3
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#line con 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface Lo0

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Lol

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface f 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
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

```

Figura 9. Verificación de relación vecinos R2-R3

```
na\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
R2
Physical Config CLI
IOS Command Line Interface
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 01:12:14
C    2.0.0.0/8 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, 01:12:14
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
C    192.1.12.0/24 is directly connected, Serial0/0/0
R2#

?0-Final\diplomado de profundizacion\Escenario1_HernanRivera_1.pkt
R3
Physical Config CLI
IOS Command Line Interface
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
R3(config-router)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

C    3.0.0.0/8 is directly connected, Loopback0
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como **66.66.66.66**. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a paso con los comandos utilizados y la salida del comando **show ip route**

```
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
```

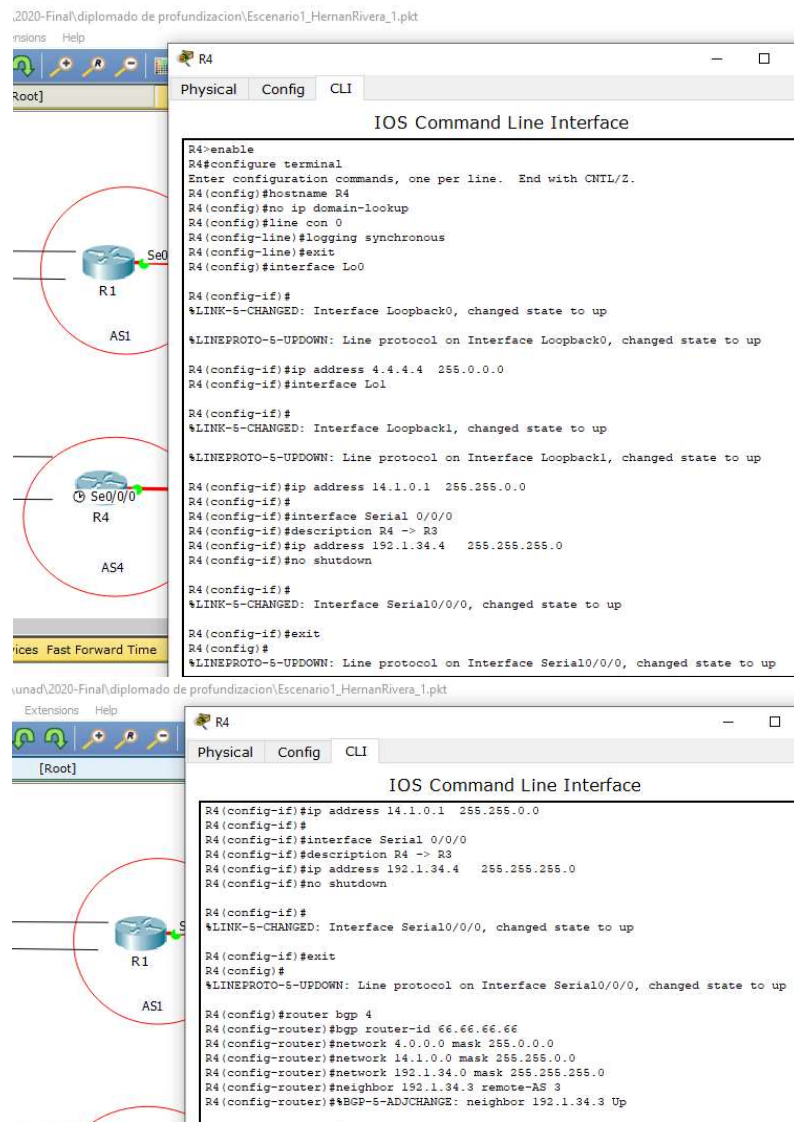
Figura 10. Verificación de comando Router 3

```
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
R3(config-router)#
```

```
R4#enable
R4#configure terminal
R4(config)#hostname R4
R4(config)# no ip domain-lookup
R4(config)# line con 0
R4(config-line)# logging synchronous
R4(config-line)# exit
R4(config)# interface Lo0
R4(config-if)# ip address 4.4.4.4 255.0.0.0
R4(config)# interface Lo1
R4(config-if)# ip address 14.1.0.1 255.255.0.0
R4(config)# interface Serial 0/0/0
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

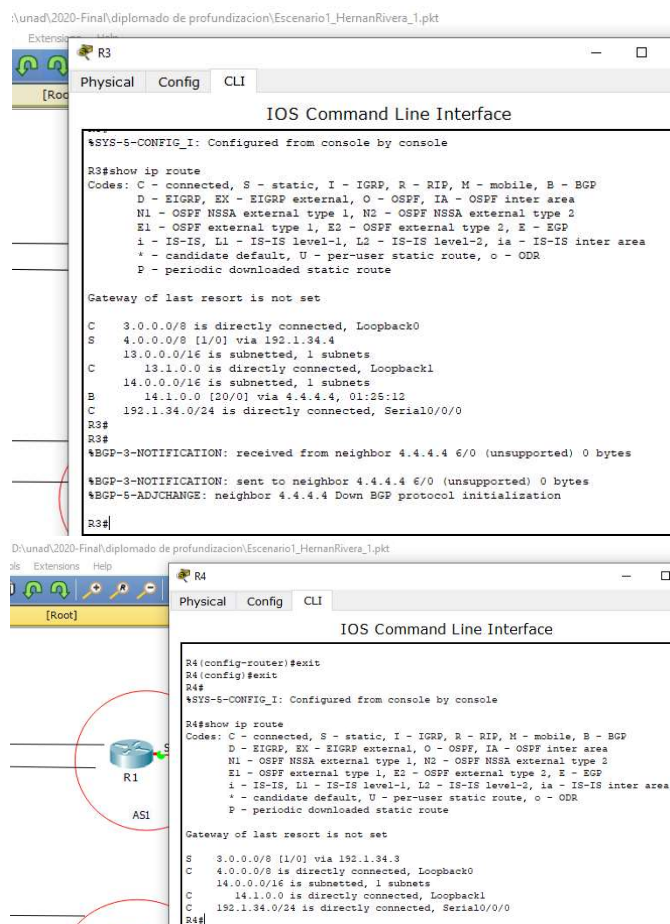
Figura 11. Configuración de router R4



El router vecino necesita informar sobre el uso de esta interfaz en lugar de una interfaz física y, por tanto, se requiere una configuración adicional para establecer los vecinos por ello se establecen las relaciones de adyacencia mediante las direcciones de Loopback

```
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
```

Figura 12. Configuración de adyacencia de vecinos



2. ESCENARIO 2

Figura 13. Escenario 2

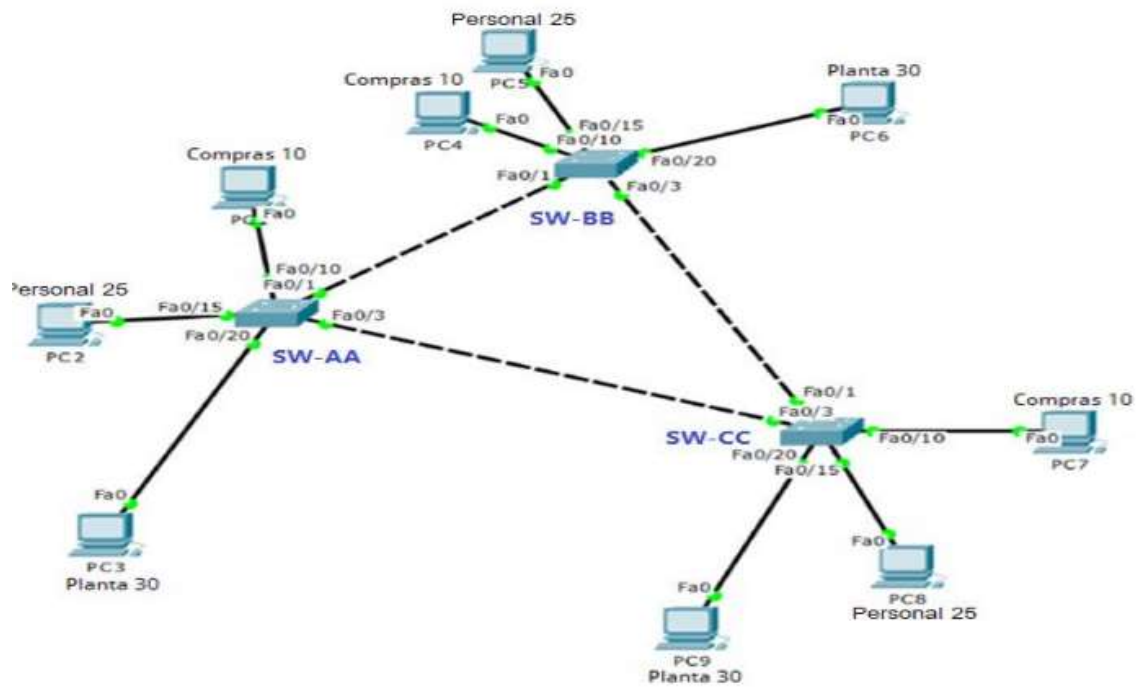
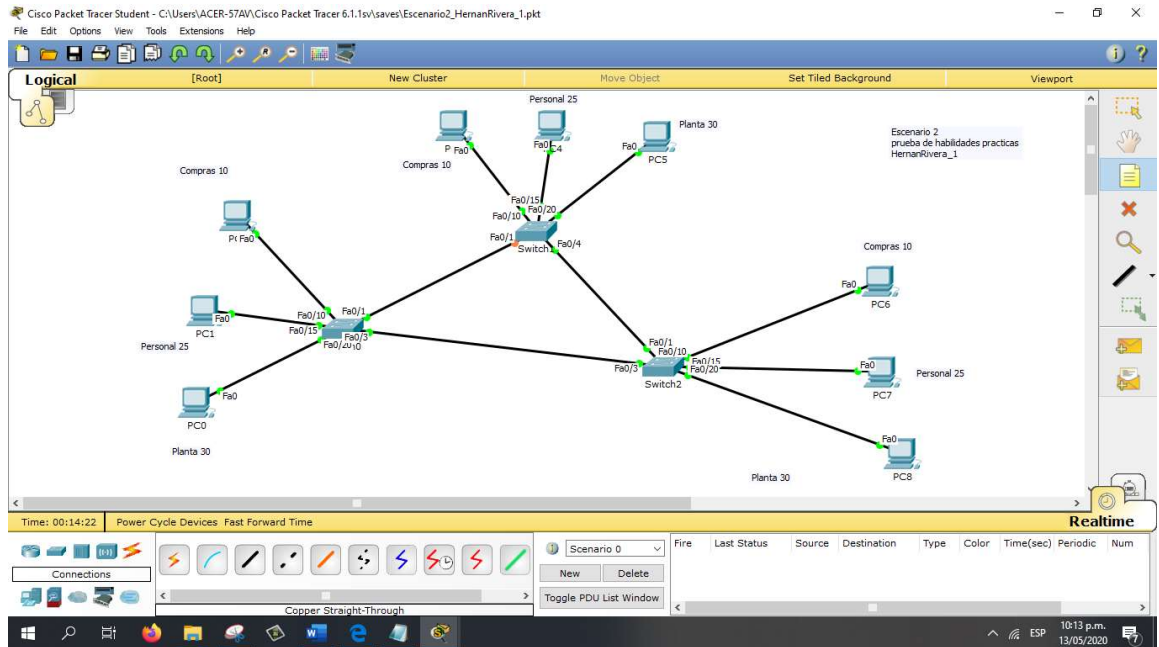


Figura 14. Simulación escenario 2

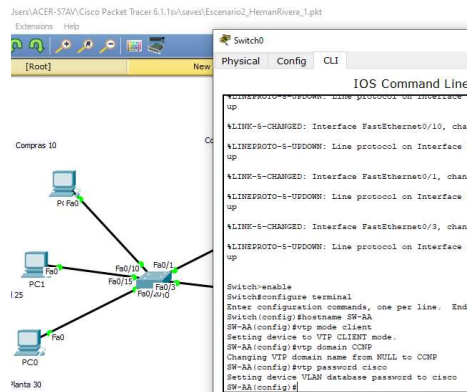


A. Configurar VTP

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

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

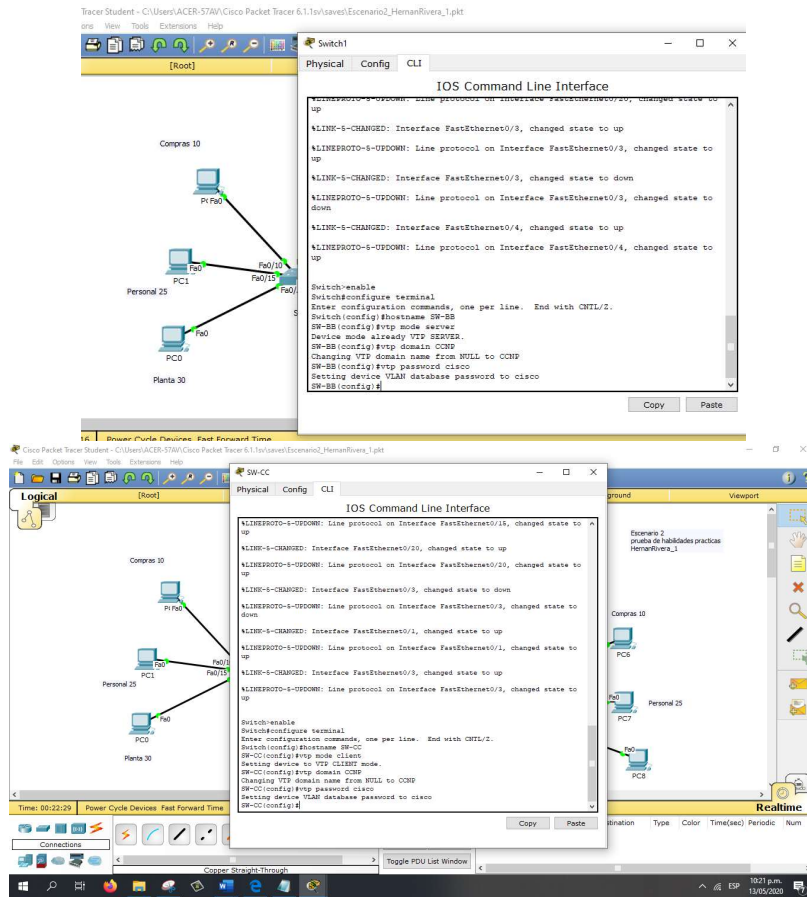
Figura 15. Configuración router SW-AA como cliente



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

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

Figura 16. Configuración router SW-BB//SW-CC como servidor



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

Figura 17. Verificaciones configuraciones routers para VTP

The screenshot shows two windows from Cisco Packet Tracer. The left window is for SW-AA and the right window is for SW-BB. Both windows show the CLI interface with configuration commands and the output of the 'show vtp status' command.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
SW-AA(config)#interface FastEthernet0/5
SW-AA(config-if)#EXIT
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

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 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#
```

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
SW-BB(config)#
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

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 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#
```

The screenshot shows the CLI interface for SW-CC in Cisco Packet Tracer. It displays the configuration commands and the output of the 'show vtp status' command.

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

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
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

B. Configurar DTP (Dynamic Trunking Protocol)

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

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

Figura 18. Configuración enlace troncal en SW-BB

```
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable

SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

%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
```

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

Figura 19. Verificación enlace troncal entre SW-BB y SW-AA

The screenshot shows two terminal windows in Packet Tracer. The left window is for SW-AA and the right window is for SW-BB.

SW-AA CLI Output:

```
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-BB CLI Output:

```
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

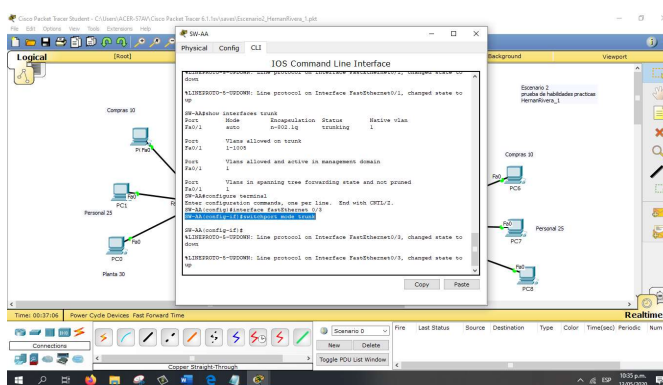
Port      Vlans allowed and active in management domain
Fa0/1     1

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

- Entre SW-AA y SW-CC configure un enlace “trunk” estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW-AA

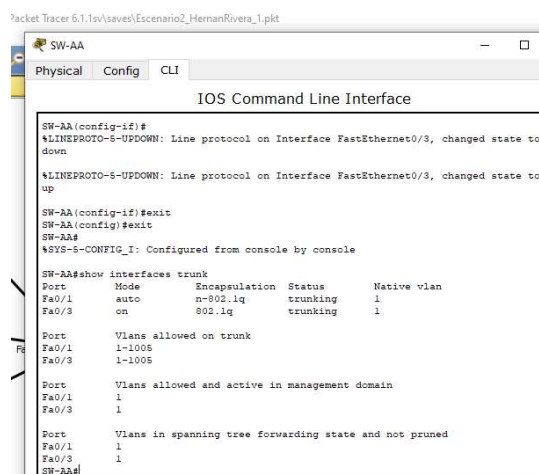
```
SW-AA#configure terminal
SW-AA(config)#interface fa 0/3
SW-AA(config-if)#switchport mode trunk
```

Figura 20. Configuración enlace trunk interfaz F0/3 en SW-AA



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

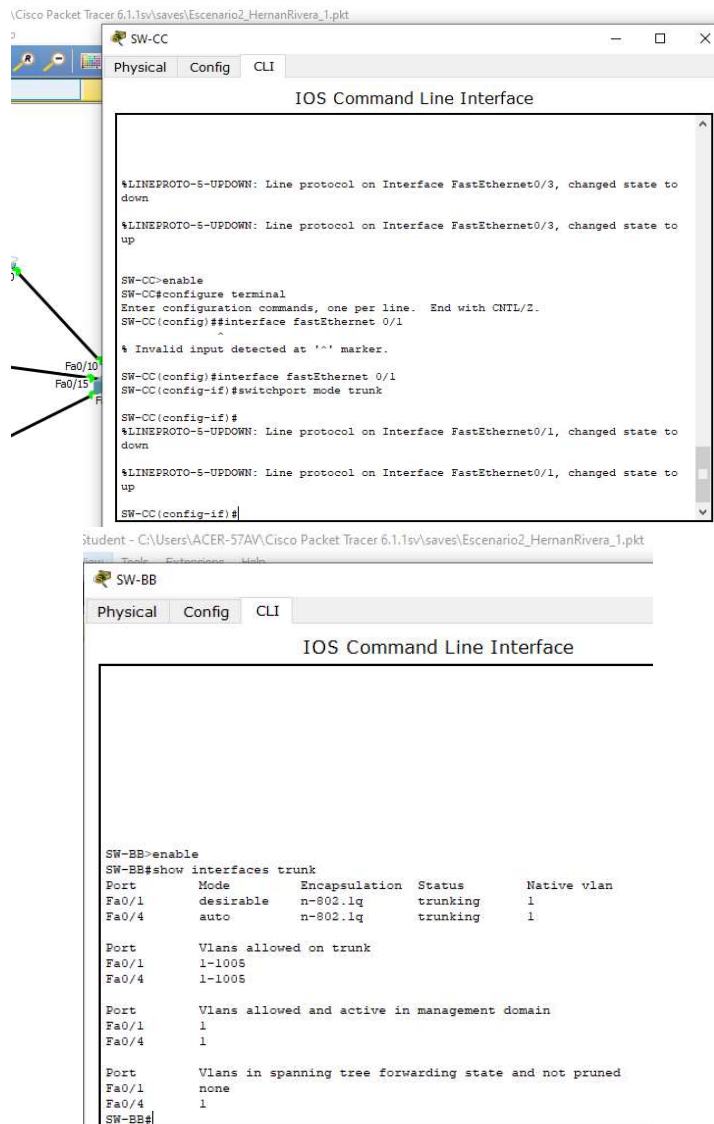
Figura 21. Verificación enlace trunk en SW-AA



7. 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
```

Figura 22. Configuración enlace trunk permanente

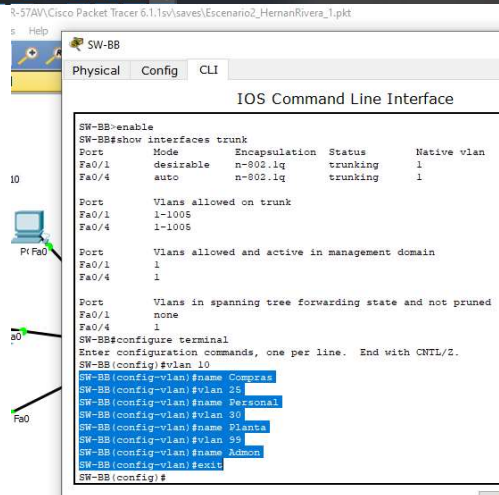
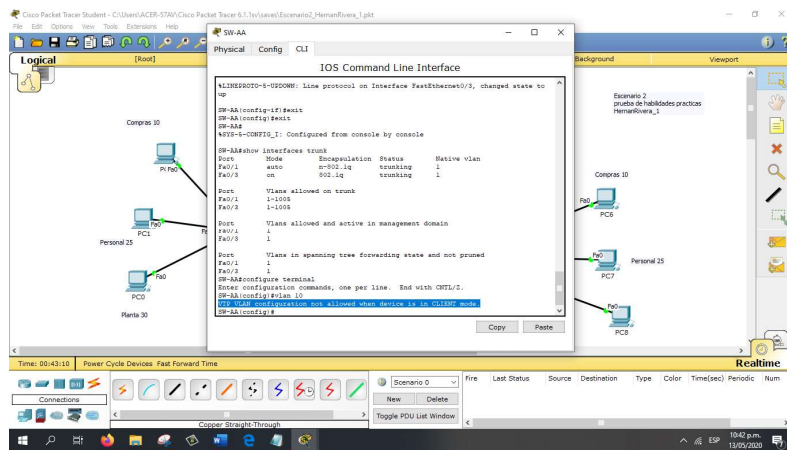


C. Agregar VLANs y asignar puertos.

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

SW-AA#configure terminal
SW-AA(config)#vlan 10

Figura 23. Configuración de VLANs



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

```

9. Verifique que las VLANs han sido agregadas correctamente.

Figura 24. Verificación de VLANs

The image shows two screenshots of network device consoles. The left screenshot shows the configuration of VLANs on SW-BB, and the right screenshot shows the verification of these VLANs on SW-CC.

SW-BB Configuration:

```

SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB#
*SYS-5-CONFIG_I: Configured from console by console
SW-BB#show vlan brief

```

SW-CC Verification:

```

SW-CC#enable
SW-CC#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
SW-CC(config)#exit
SW-CC#
*SYS-5-CONFIG_I: Configured from console by console
SW-CC#show vlan brief

```

SW-AA Verification:

```

SW-AA#show vlan brief

```

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

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

X = número de cada PC particular

Tabla 2. Información para configuración de direcciones ip de PCs

VLAN	PCs	IP	Mascara
VLAN 10	PC0	190.108.10.2	255.225.255.0
VLAN 25	PC1	190.108.20.3	255.225.255.0
VLAN 30	PC2	190.108.30.4	255.225.255.0
VLAN 10	PC3	190.108.10.5	255.225.255.0
VLAN 25	PC4	190.108.20.6	255.225.255.0
VLAN 30	PC5	190.108.30.7	255.225.255.0
VLAN 10	PC6	190.108.10.8	255.225.255.0
VLAN 25	PC7	190.108.20.9	255.225.255.0
VLAN 30	PC8	190.108.30.10	255.225.255.0

Tabla 3. Direcciones ip de PCs

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 F0/25 y F0/30 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```

SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode 36ccess
SW-AA(config-if)#switchport 36ccess vlan 10
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode 36ccess
SW-AA(config-if)#switchport 36ccess vlan 25
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode 36ccess
SW-AA(config-if)#switchport 36ccess vlan 30

```

Figura 25. Configuración mode Access router SW-AA

```

77AV\Cisco Packet Tracer 6.1.1s\save\Escenario2_HernanRivera_1.pkt
SW-AA
Physical Config CLI
IOS Command Line Interface
%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>enable
SW-AA#interface fastEthernet 0/10
% Invalid input detected at '^' marker.
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
SW-AA(config)#

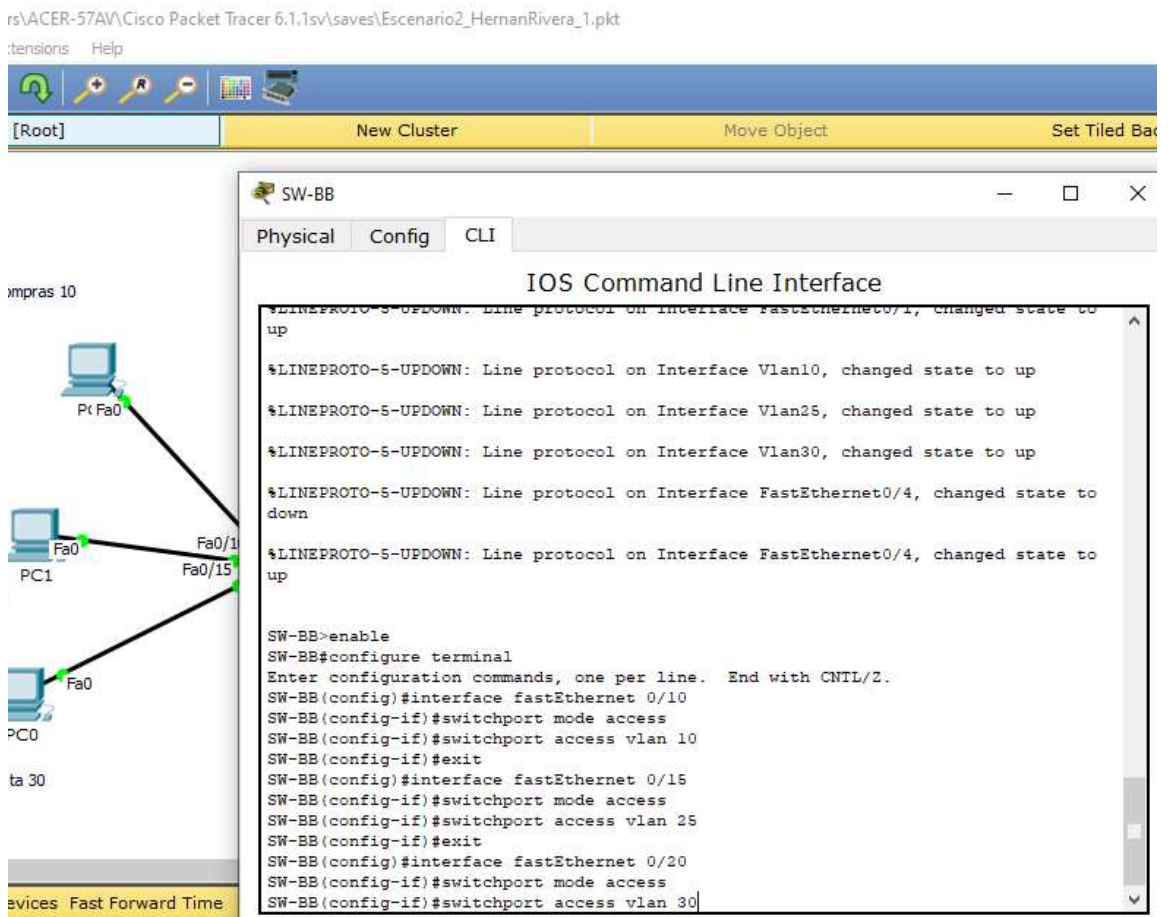
```

```

SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode 37ccess
SW-BB(config-if)#switchport 37ccess vlan 10
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode 37ccess
SW-BB(config-if)#switchport 37ccess vlan 25
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode 37ccess

```

Figura 26. Configuración mode Access router SW-BB

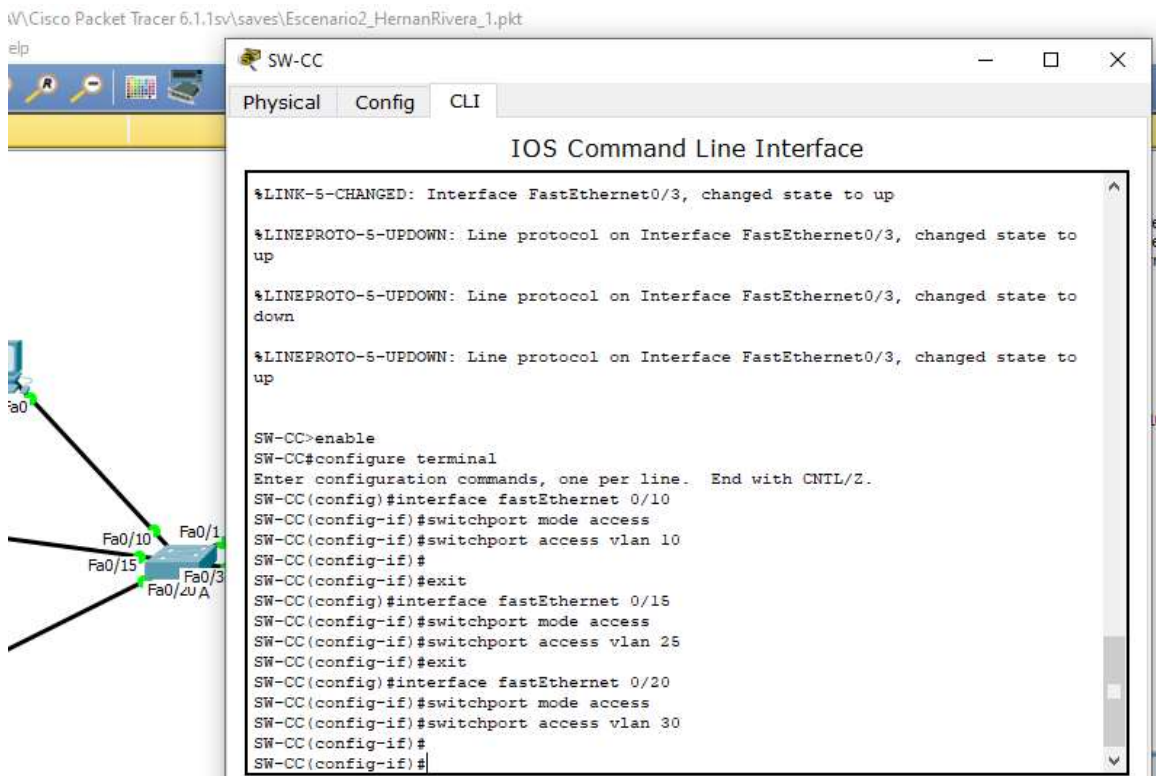


```

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode 38ccess
SW-CC(config-if)#switchport 38ccess vlan 10
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode 38ccess
SW-CC(config-if)#switchport 38ccess vlan 25
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode 38ccess
SW-CC(config-if)#switchport 38ccess vlan 30

```

Figura 27. Configuración mode Access router SW-CC



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 4. Direcciones ip para VLAN 99

```
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-BB#configure terminal  
SW-BB(config)#interface vlan 99  
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

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

Figura 28. Configuración mode Access router SW-CC

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#
```

```
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#
```

```
SW-CC(config)#interface vlan 99
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

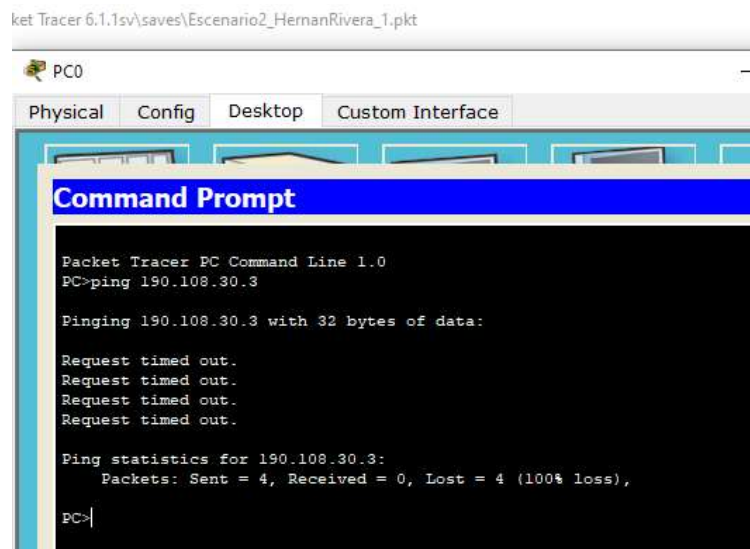
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#
```

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.

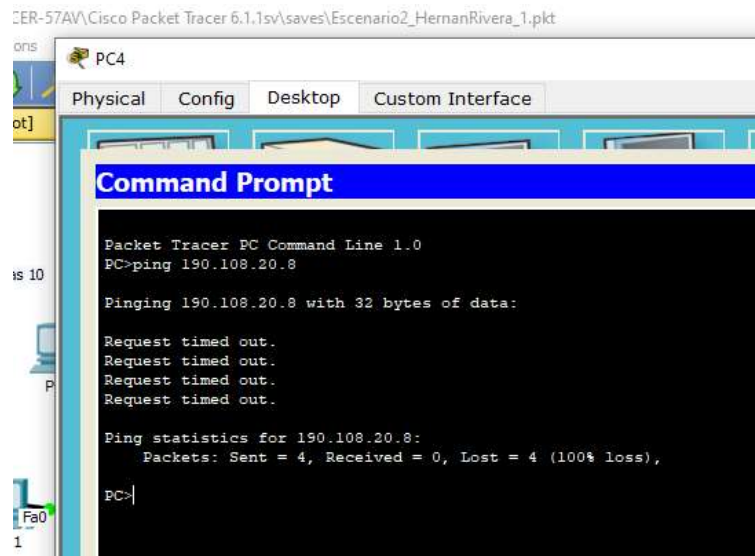
Figura 29. Ping de PC0 a PC3



El ping realizado entre los PCs pertenecientes a diferentes VLANs no tuvo éxito, sin embargo, los pings realizados a PCs que perteneces a la misma Vlan, si tuvieron éxito. El error en los PCs pertenecientes a diferentes VLANs se presenta ya que cada PC pertenece a un segmento de red diferente. Por tanto, para lograr establecer comunicación entre estos PCs, sería necesario incluir en la topología de la red un enrutador o un Switch de capa 3 (Switch Multicapa), los cuales tienen la funcionalidad intrínseca de enrutamiento entre VLANs, para así lograr comunicar el tráfico ICMP entre las diferentes redes propuestas en la tabla de enrutamiento para estos dispositivos.

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

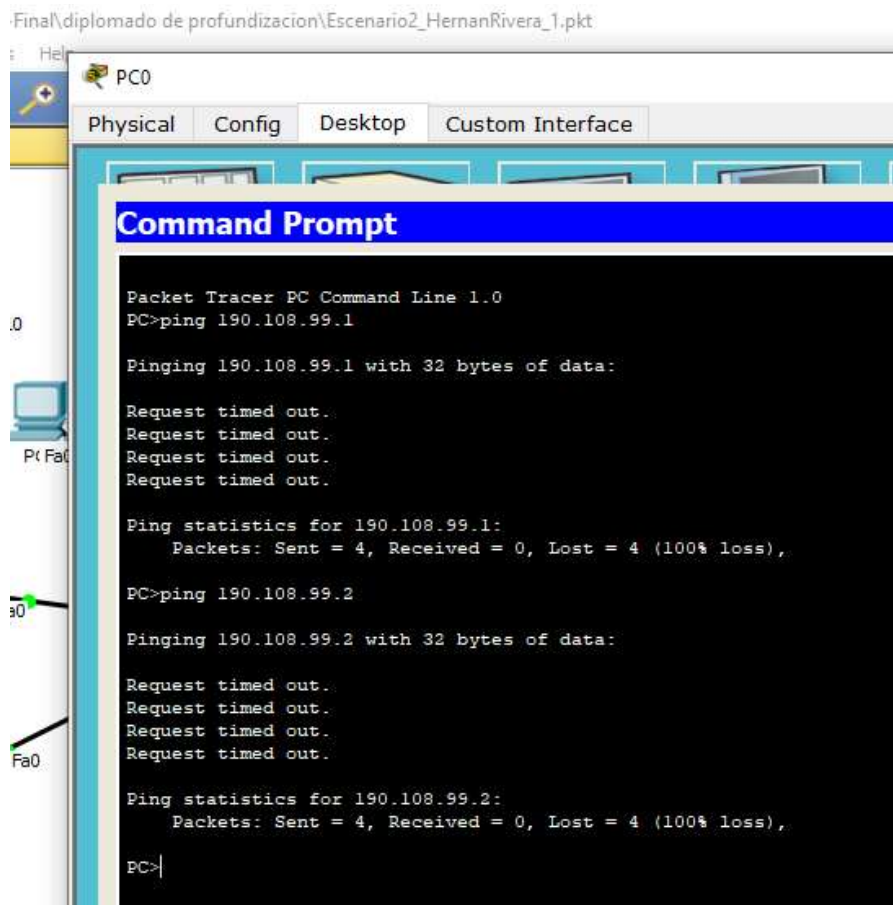
Figura 30. Ping de PC4 A PC6



El ping realizado entre los Switches fue exitoso, dado que las interfaces físicas que enrutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal, y según se verificó mediante el comando *show interfaces trunk*, comparten el mismo tipo de encapsulamiento, así como se encuentran en un modo compatible. Pese a esto, es necesario implementar en las interfaces que conectan los Switches el comando *switchport trunk allowed vlan except "vlan id"*, para establecer el permiso a las VLANs creadas en este escenario, además, se debe determinar la VLAN nativa para dichas interfaces.

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

Figura 31. Ping de PC0 a switch SW-AA Y SW-BB



El ping realizado entre los Switches y los PCs no tuvo éxito. Ya que, si bien se tienen habilitadas las VLANs en cada uno de los Switches a través del protocolo VTP, y se configuro cada una de las interfaces que conectan los switches a los PCs en modo de acceso según la respectiva VLAN a la cual pertenecen, aun no se configura un enrutamiento IP en las VLANs creadas (10-Compras / 25-Personal / 30-Planta). Para solucionar esto, es necesario configurar una dirección IP y una máscara de subred en cada una de las interfaces VLAN de los Switches, la cual pertenezca al mismo segmento de red al cual pertenece el PC que se conecta a cada VLAN. Además, se debe determinar la VLAN nativa para dichas interfaces.

CONCLUSIONES

Se utilizaron los comandos de configuración de routers para la aplicación del protocolo BGP en el escenario 1.

Se establecieron las relaciones de vecinos BGP entre los routers con el fin de evidenciar el funcionamiento del protocolo BGP

Se utilizaron las herramientas de simulación para el análisis y comportamiento de los protocolos de enrutamiento aplicando los principios de conmutación en redes LAN.

Se comprende el funcionamiento de la configuración de las VLANs para redes empresariales mediante la configuración de switches.

Se comprende la importancia del diplomado dentro del desarrollo profesional y laboral, entendiendo su valor agregado dentro de las redes empresariales, la globalización y competitividad para la gestión de servicios y las aplicaciones en telecomunicaciones.

BIBLIOGRAFIA

- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. 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). Switching Features and Technologies. 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). High Availability. 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). Campus Network Security. 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>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Enterprise Internet Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

