DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

HELBER GUSTAVO DONCEL BOHORQUEZ

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

HELBER GUSTAVO DONCEL BOHORQUEZ

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Yopal, 20 de Mayo de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

AS (sistema autónomo): es un conjunto de redes IP administradas por uno o más operadores utilizando el protocolo BGP como protocolo de enrutamiento.

BGP (Border Gateway procol): es un protocolo de enrutamiento de tipo vector distancia, también se le conoce como el protocolo de enrutamiento de internet, el protocolo e-BGP (exterior-BGP) se utiliza para la interconexión de diferentes AS mientras que para la comunicación dentro de un AS se utiliza i-BGP (interior-BGP)

DTP (Dynamic Trunking Protocol): es un protocolo desarrollado por CISCO, y trabaja entre switches de la misma marca, y se orienta a la automatización del proceso trunking de las VLAN.

IP (protocolo de internet): es un conjunto de reglas que rigen el formato de envío de datos en una red local y la internet. En esencia se utiliza las direcciones IP para el envío de información través de una red.

VLAN: se le conoce como virtual LAN y es el método utilizado para crear redes lógicas, las cuales funcionan de manera independiente dentro de la misma red física.

VTP: es un protocolo de la marca CISCO, orientado a recibir y entregar información de las VLANs entre switch y asi mantener sincronizada y centralizada la base de datos de VLANs en la red.

RESUMEN

En este informe se desarrolló el procedimiento paso a paso detallado de dos escenarios propuestos como evaluación final del curso, con el fin de aplicar y afianzar los temas como las configuraciones EBGP, VTP, DTP, los protocolos de enrutamiento Avanzado, las VLAN, conmutación, entre otros vistos a lo largo del diplomado de Cisco CCNP, además de identificar las competencias y habilidades que fueron adquiridas poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos en las redes utilizando como herramienta el uso del programa PacketTracer.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this report, the detailed step-by-step procedure of two scenarios proposed as final evaluation of the course was developed, in order to apply and consolidate topics such as EBGP, VTP, DTP configurations, Advanced routing protocols, VLANs, switching, Among others seen throughout the Cisco CCNP diploma, in addition to identifying the competencies and skills that were acquired by testing the levels of understanding and problem solving related to various aspects of the networks using the use of the Packet Tracer program as a tool.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

La información es constantemente transmitida en las organizaciones, debido a la necesidad de mantener informados todos los niveles que constituyen una empresa.Así como también es parte del diario común de todos los seres humanos para mantenerse actualizados en un mundo que cada día avanza más. En el siguiente informe se desarrolla la etapa final del diplomado de profundización en cisco CCNP, mediante la realización de dos escenarios paso a paso detallando los comandos utilizados en el procedimiento de configurar y verificar la conexión de los distintos dispositivos usados por medio del programa Packet Tracer. Este programa tiene un entorno fácil de comprender a la hora de programar y simular lo que permite interactuar de manera más cómoda y aplicar los conocimientos en configuraciones BGP, VTP, DTP, protocolos de enrutamiento Avanzado, VLAN entre otros, donde se aplican y afianzan los temas del curso.

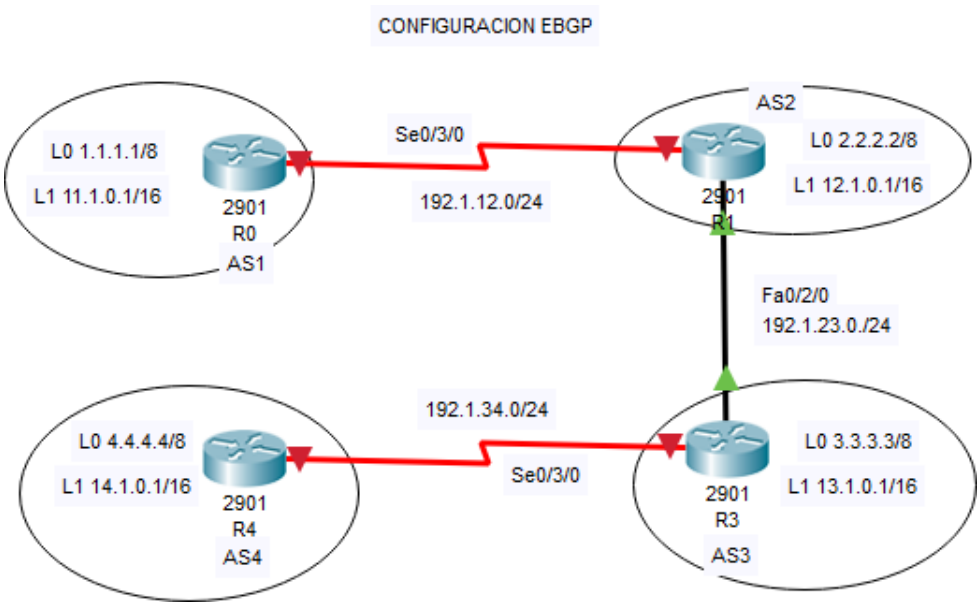
En el escenario 1 se debe realizar la configuración de R1, R2, R3 y R4 asignando sus respectivas direcciones IP y aplicando la configuración para el protocolo BGP entre R1 y R2 y de la misma manera entre R3 y R4.

En el escenario 2 que consta de 3 switches, donde cada uno contiene 3 equipos, y en cada switch se le realizará la configuración mediante protocolo VTP donde el swich SW-BB se definirá como servidor y los switches SW-AA y SW-CC como clientes, seguidamente se aplicara el protocolo DTP, se configuran direcciones IP y demás para luego hacer verificación de comunicación mediante ping desde una terminal hacia los diferentes switches.

DESARROLLO

ESCENARIO 1

Figura 1:Escenario 1



Tablas de Información para la configuración de los Routers:

R1

Tabla: 1 Configuración de R1

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
Se0/3/0	192.1.12.1	255.255.255.0

R2

Tabla: 2 - Configuración de R2

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
Se0/3/0	192.1.12.2	255.255.255.0
Fa0/2/0	192.1.23.2	255.255.255.0

R3

Tabla: 3 - Configuración de R3

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
Fa0/2/0	192.1.23.3	255.255.255.0
Se0/3/0	192.1.34.3	255.255.255.0

R4

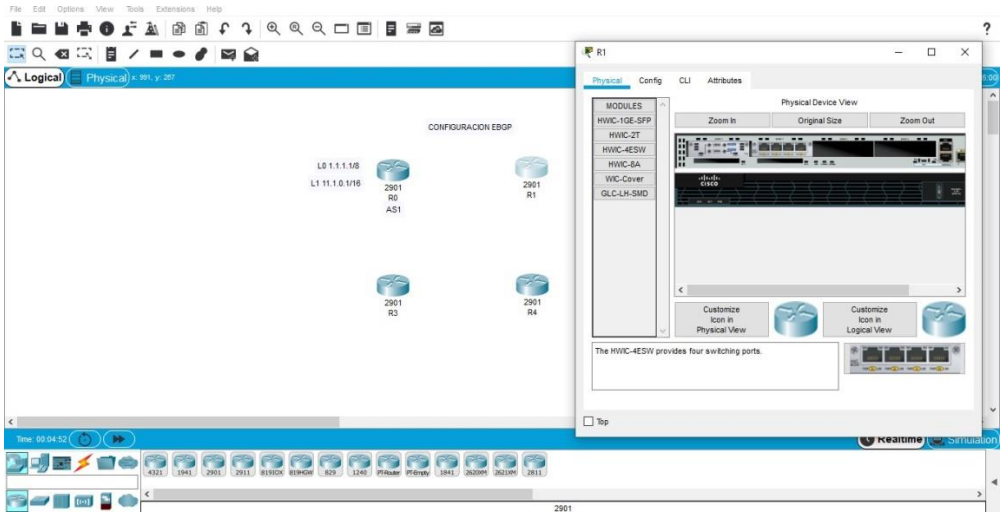
Tabla: 4 - Configuración de R4

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
Se0/3/0	192.1.34.4	255.255.255.0

DESARROLLO DEL ESCENARIO 1

1. Agregar a la pantalla principal del programa Packet Tracer los Routers y realizar la topología que se muestra en la figura1.
2. Agregar los módulos HWIC-2T y HWIC-4ESW al Router. Para ello primero debemos apagar el Router, luego agregar los módulos y volver a encender el Router.

Figura 2: Módulos agregados a cada Route 1



3. Realizar las configuraciones básicas de un Router usando los siguientes comandos.

R1

Router> enable
Router#configure terminal
Router#hostname R1
R1#enable secret cisco.
R1#line console 0
R1#password cisco
R1#login
R1#line vty 0 4
R1#password cisco
R1#login
R1#exit.
R1#service password-encryption
R1#do write

R2

Router> enable
Router#configure terminal
Router#hostname R2
R2#enable secret cisco.
R2#line console 0
R2#password cisco
R2#login
R2#line vty 0 4
R2#password cisco
R2#login
R2#exit.
R2#service password-encryption
R2#do write

R3

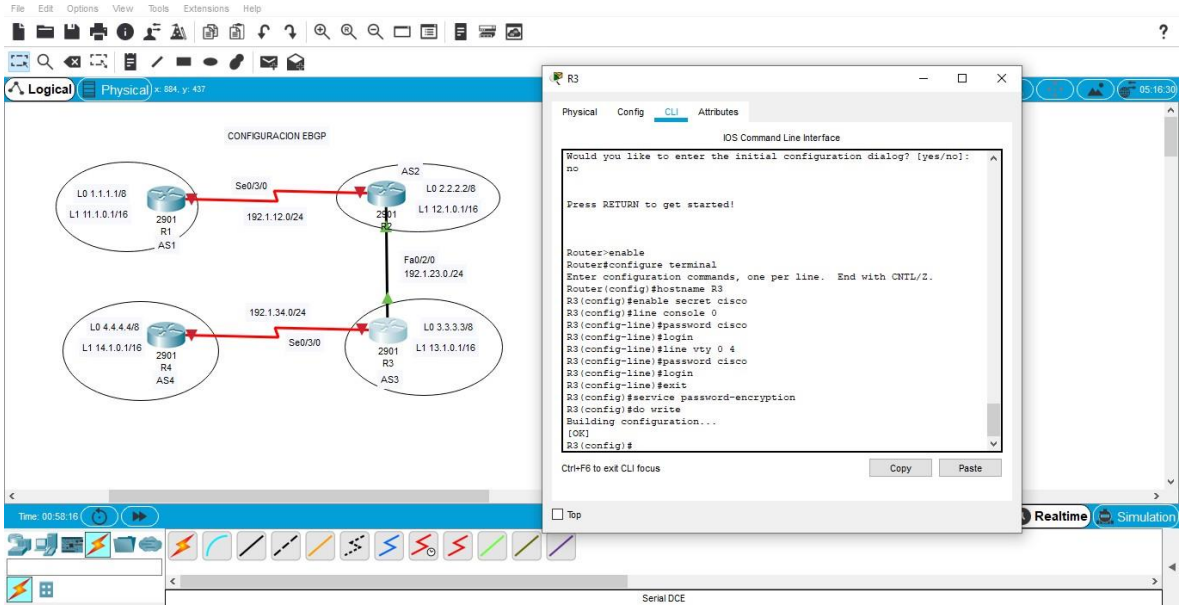
Router> enable
Router#configure terminal
Router#hostname R3
R3#enable secret cisco.
R3#line console 0
R3#password cisco
R3#login

R3#line vty 0 4
R3#password cisco
R3#login
R3#exit.
R3#service password-encryption
R3#do write

Para R4

Router> enable
Router#configure terminal
Router#hostname R4
R4#enable secret cisco.
R4#line console 0
R4#password cisco
R4#login
R4#line vty 0 4
R4#password cisco
R4#login
R4#exit.
R4#service password-encryption
R4#do write

Figura 3: Configuraciones básicas de un Router

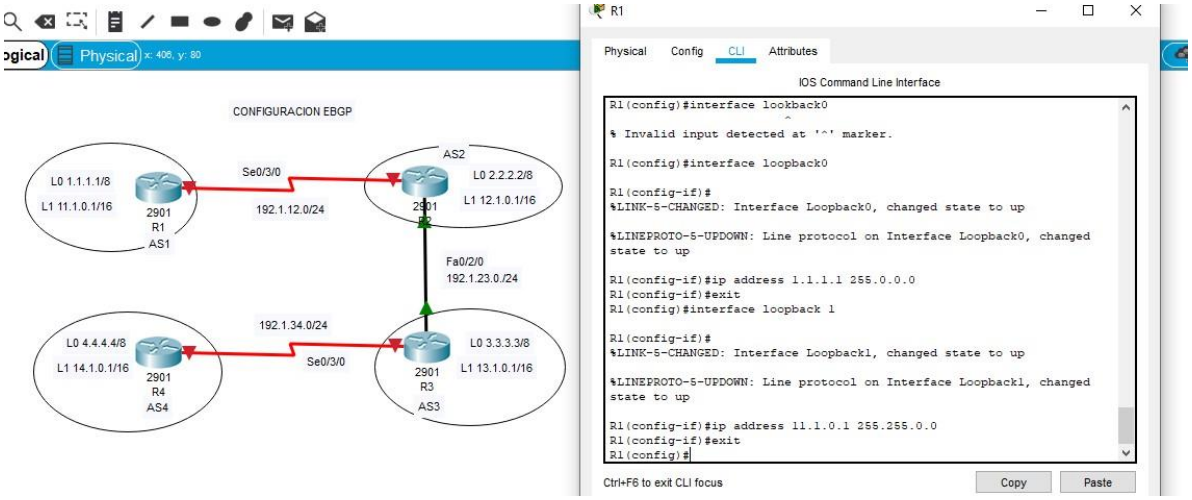


4. Para iniciar con las configuraciones EBGP primero se debe asignar los nombres, las direcciones IP y las direcciones de loopback a cada Router usando los siguientes comandos.

R1

```
R1(config)#interface Se0/3/0
R1(config)#ip address 192.1.12.1 255.255.255.0
R1(config)#no shutdown
R1(config)#exit
R1(config)#interface loopback 0
R1(config)#ip address 1.1.1.1 255.0.0.0
R1(config)#exit
R1(config)#interface loopback 1
R1(config)#ip address 11.1.0.1 255.255.0.0
R1(config)#exit
```

Figura 4: Asignación de direcciones a R1



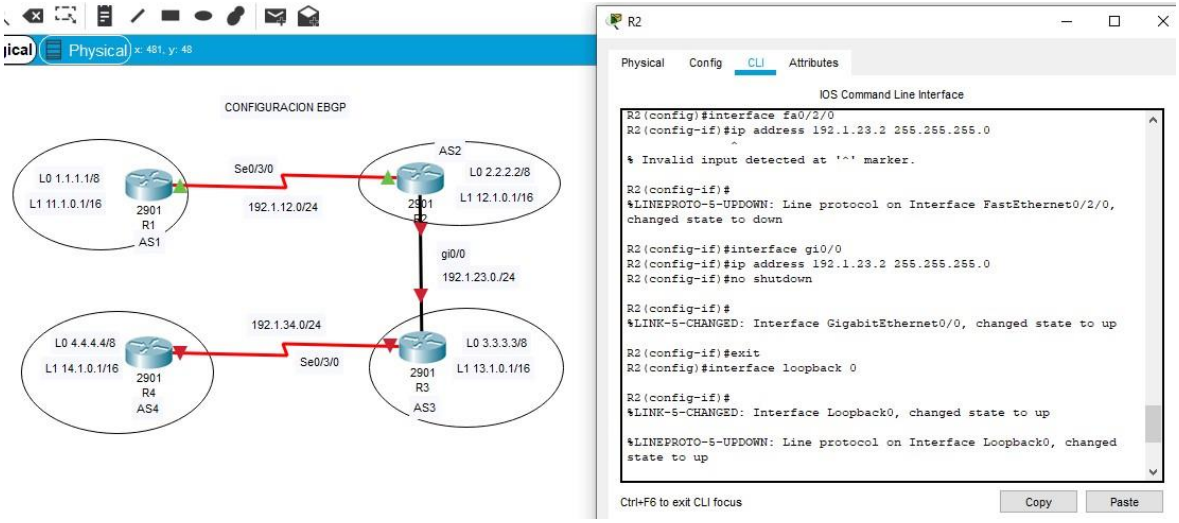
Router R2

```
R2(config)#interface Se0/3/0
R2(config)#ip address 192.1.12.2 255.255.255.0
R2(config)#no shutdown
R2(config)#exit R2(config)#interface gi0/0
R2(config)#ip address 192.1.23.2 255.255.255.0
R2(config)#no shutdown
R2(config)#exit
```

R2(config)#interface loopback 0
R2(config)#ip address 2.2.2.2 255.0.0.0
R2(config)#exit

R2(config)#interface loopback 1
R2(config)#ip address 12.1.0.1 255.255.0.0
R2(config)#exit

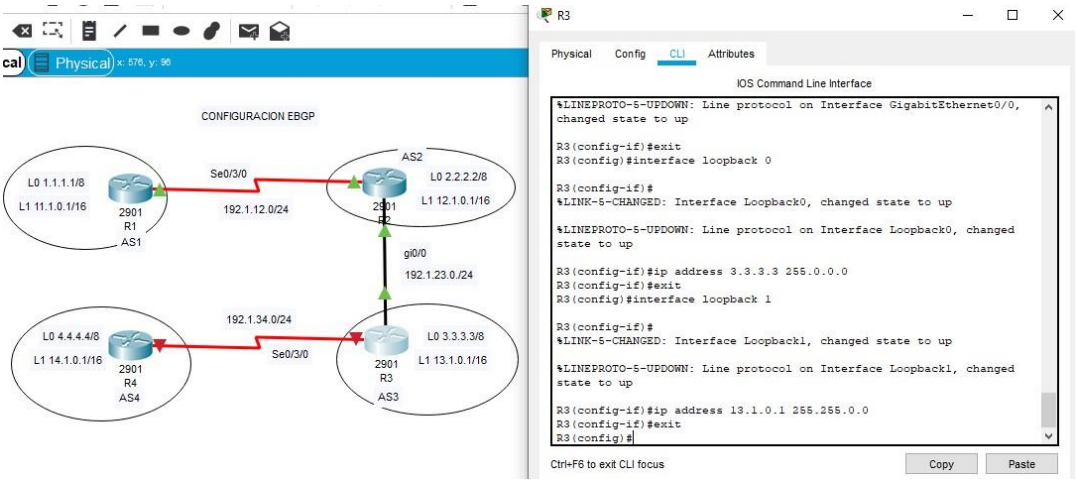
Figura 5: Asignación de direcciones a R2



Router R3

R3(config)#interface Se0/3/0
R3(config)#ip address 192.1.34.3 255.255.255.0
R3(config)#no shutdown
R3(config)#exit R3(config)#interface gi0/0
R3(config)#ip address 192.1.23.3 255.255.255.0
R3(config)#no shutdown
R3(config)#exit
R3(config)#interface loopback 0
R3(config)#ip address 3.3.3.3 255.0.0.0
R3(config)#exit
R3(config)#interface loopback 1
R3(config)#ip address 13.1.0.1 255.255.0.0
R3(config)#exit

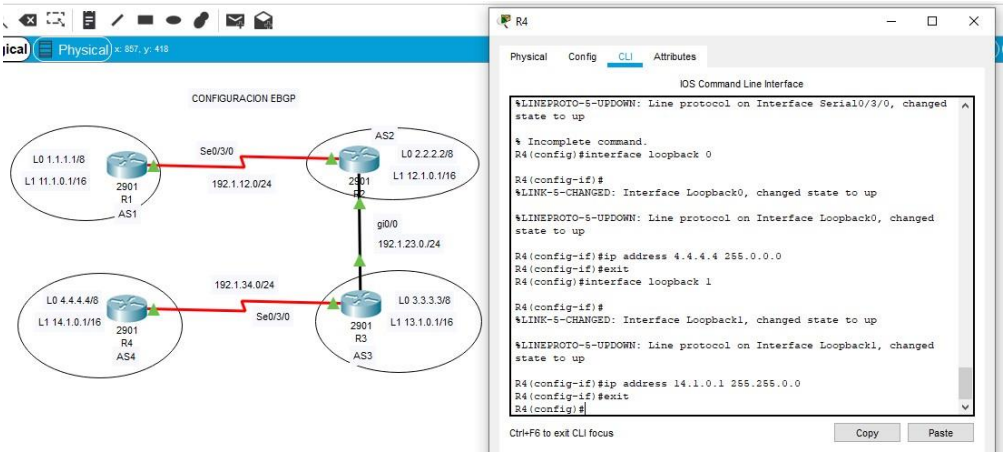
Figura 6: Asignación de direcciones a R3



Router R4

```
R4(config)#interface Se0/3/0
R4(config)#ip address 192.1.34.4 255.255.255.0
R4(config)#no shutdown
R4(config)#exit
R4(config)#interface loopback 0
R4(config)#ip address 4.4.4.4 255.0.0.0
R4(config)#exit
R4(config)#interface loopback 1
R4(config)#ip address 14.1.0.1 255.255.0.0
R4(config)#exit
```

Figura 7: Asignación de direcciones a R4



5. Para continuar con las configuraciones EBGP, debemos realizar una relaciónde 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 Router BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2.

Configurar el vecino BGP para R1 y R2:

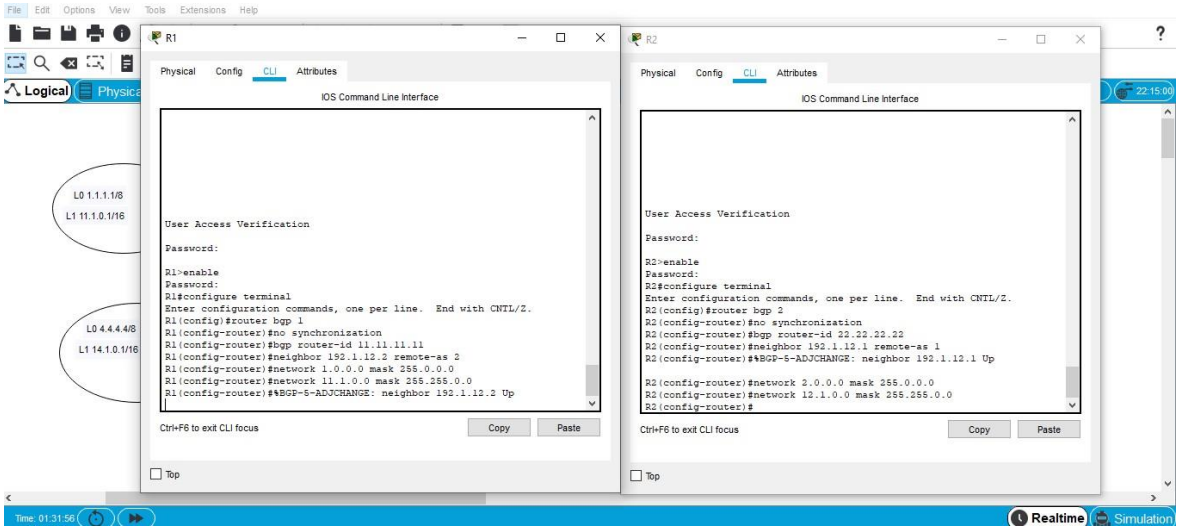
R1

R1(config)#router bgp 1
R1(config-router)#no synchronization
R1(config-router)#bgp router-id 11.11.11.11
R1(config-router)#neighbor 192.1.12.2 remote-as 2
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

R2

R2(config)#router bgp 2
R2(config-router)#no synchronization
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#neighbor 192.1.12.1 remote-as 1
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

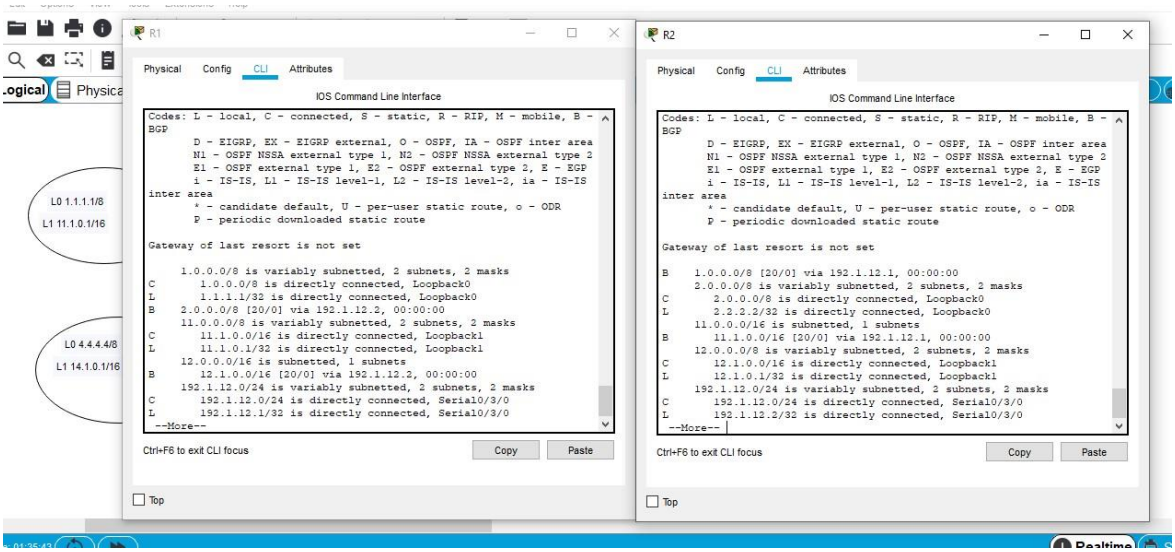
Figura 8: Configuración del vecino BGP para R1 y R2:



6. Verificar los Router R1 y R2

R1# show ip route
R2# show ip route

Figura 9: Verificación en R1y R2 la relación de vecino BGP



7. Ahora hay que configurar una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del Router R3 como 33.33.33.33.

Configurar el vecino BGP para R2 y R3:

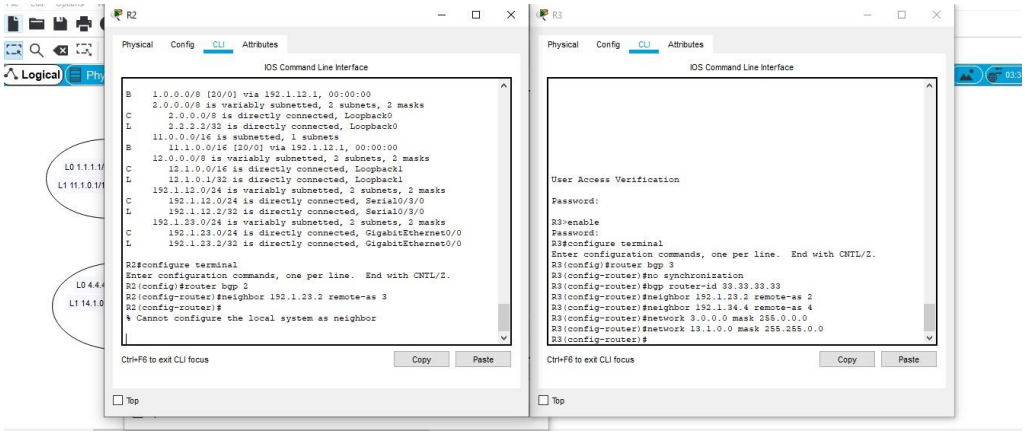
R2

R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.2 remote-as 3

R3

R3(config)#router bgp 3
R3(config-router)#no synchronization
R3(config-router)#bgp router-id 33.33.33.33
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0

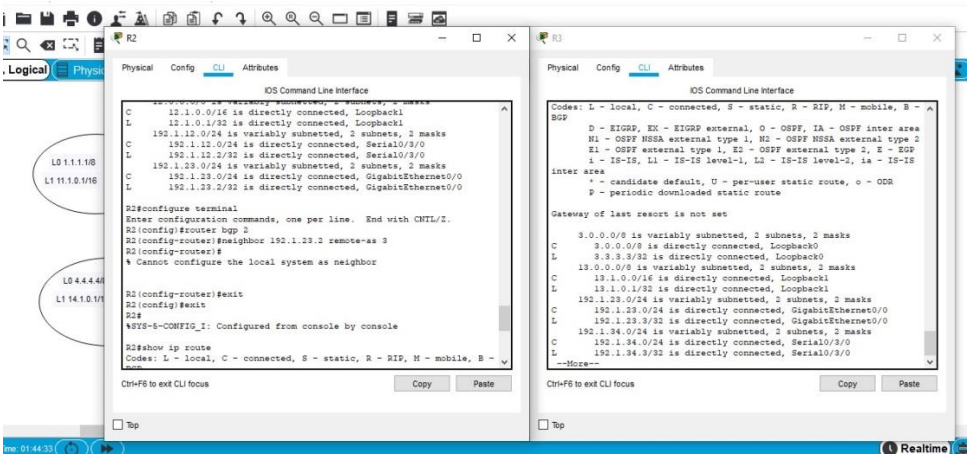
Figura 10: Configuración del vecino BGP para R2 y R3



8. Verificar los Router R2 y R3

R2# show ip route
R3# show ip route

Figura 11: Verificación en R2 y R3 la relación de vecino BGP



9. Luego hay que configurar una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4.
   Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del Router R4 como 44.44.44.44. Establezca las relaciones de vecino con baseen 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.

Configurar el vecino BGP para R3 y R4:

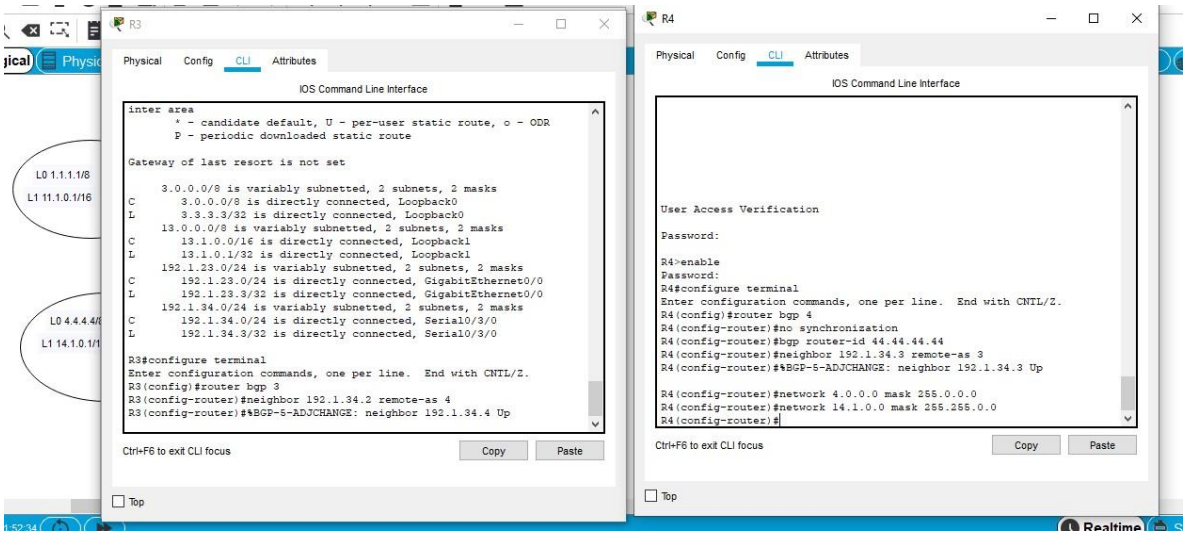
R3

R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.2 remote-as 4

R4

R4(config)#router bgp 4
R4(config-router)#no synchronization
R4(config-router)#bgp router-id 44.44.44.44
R4(config-router)#neighbor 192.1.34.3 remote-as 3
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

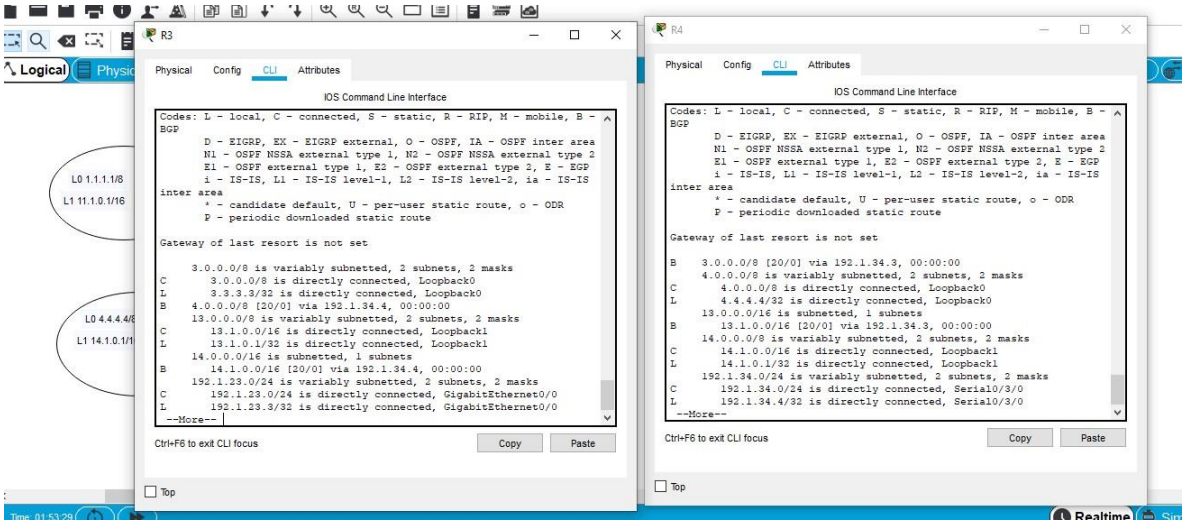
Figura 12: Configuración del vecino BGP para R3 y R4



10. Verificar los Router R3 y R4

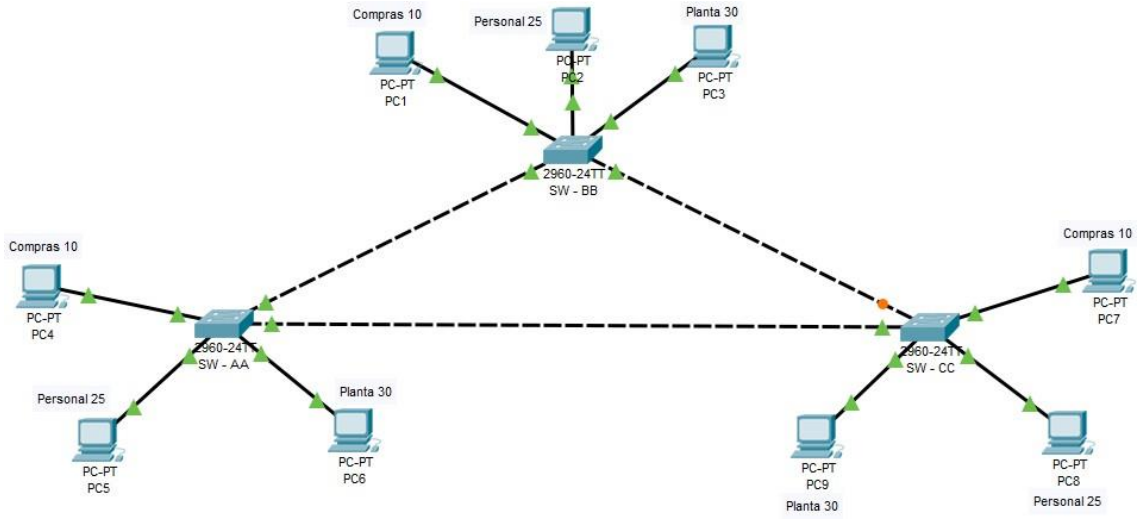
R3# show ip route
R4# show ip route

Figura 13: Verificación en R3 y R4 la relación de vecino BGP



ESCENARIO 2

Figura 14: Escenario 2



DESARROLLO DEL ESCENARIO 1

1. Agregar a la pantalla principal del programa Packet Tracer los switch en la pantalla principal del programa Packet Tracer. Asignándole a cada uno su nombre correspondiente SW-AA, SW-BB y SW-CC además de colocar tres PC's por cada switch y realizar la topologia que se muestra en la figura14.

2. Realizar las configuraciones básicas de un Switch usando los siguientes comandos.

SW-AA

Switch> enable
Switch #configure terminal
Switch #hostname SW-AA SW-AA
#enable secret cisco.
SW-AA #line console 0
SW-AA #password cisco
SW-AA #login

SW-AA #line vty 0 15
SW-AA #password cisco
SW-AA #login
SW-AA #exit.
SW-AA #service password-encryptio
SW-AA #do write

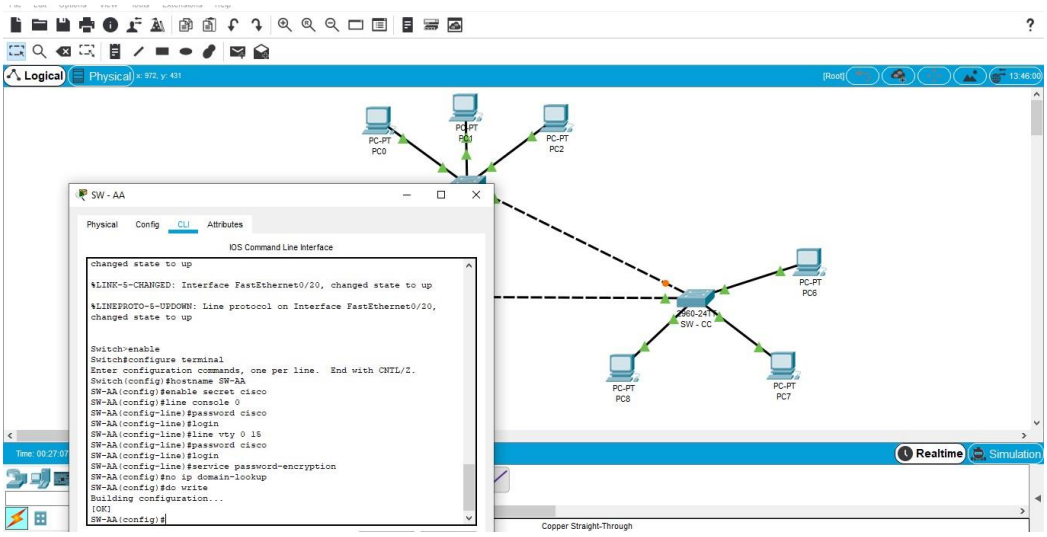
SW-BB

Switch > enable
Switch #configure terminal
Switch #hostname
SW-BB SW-BB #enable secret cisco.
SW-BB #line console 0
SW-BB #password cisco
SW-BB #login
SW-BB #line vty 0 15
SW-BB #password cisco
SW-BB #login
SW-BB #exit.
SW-BB #service password-encryption
SW-BB #do write

SW-CC

Switch > enable
Switch #configure terminal
Switch #hostname R4
SW-CC#enable secret cisco.
SW-CC #line console 0
SW-CC #password cisco
SW-CC #login
SW-CC #line vty 0 15
SW-CC #password cisco
SW-CC #login
SW-CC #exit.
SW-CC #service password-encryption
SW-CC #do write

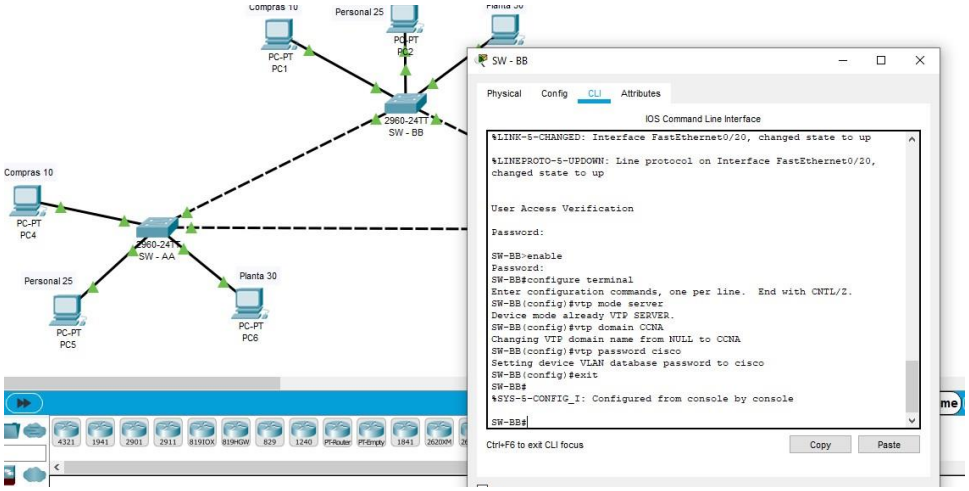
Figura 15: Configuraciones básicas de un Switch



3. Para realizar la configuración VTP, debemos configurar el switch SW-BB como servidor por medio del comando vtp mode server. Luego configurar el nombre del dominio VTP con el comando vtp domain CCNA, donde CCNA es el nombre del dominio y por último configurar la contraseña de dominio VTP usando el comando vtp password cisco, donde cisco es la contraseña.

SW-BB(config)#vtp mode server.
SW-BB(config)#vtp domain CCNA
SW-BB(config)# vtp password cisco
SW-BB(config)# exit

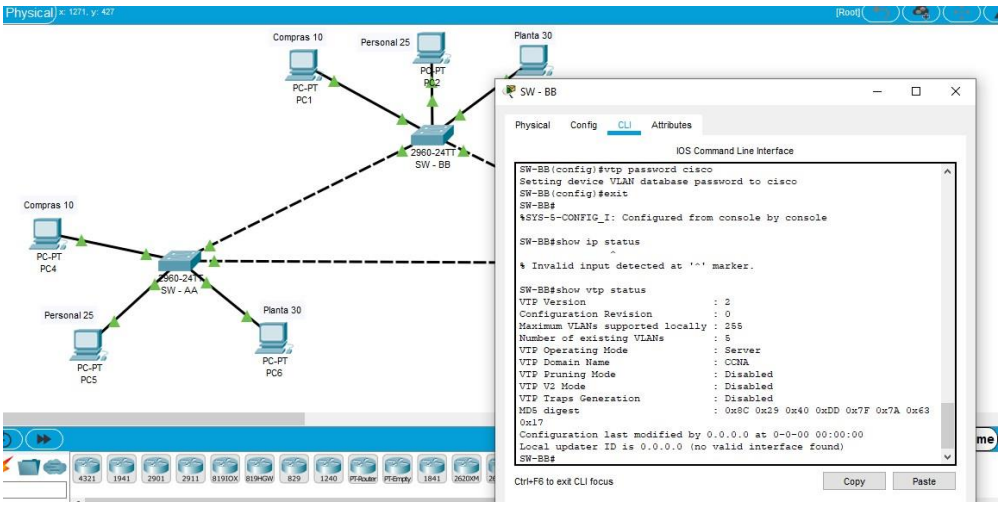
Figura 16: Configuración del switch SW-BB como servidor



4. Verificar por medio del comando show vtp status

SW-BB(config)# show vtp status

Figura 17: Verificación de la configuración del switch SW-BB como servidor

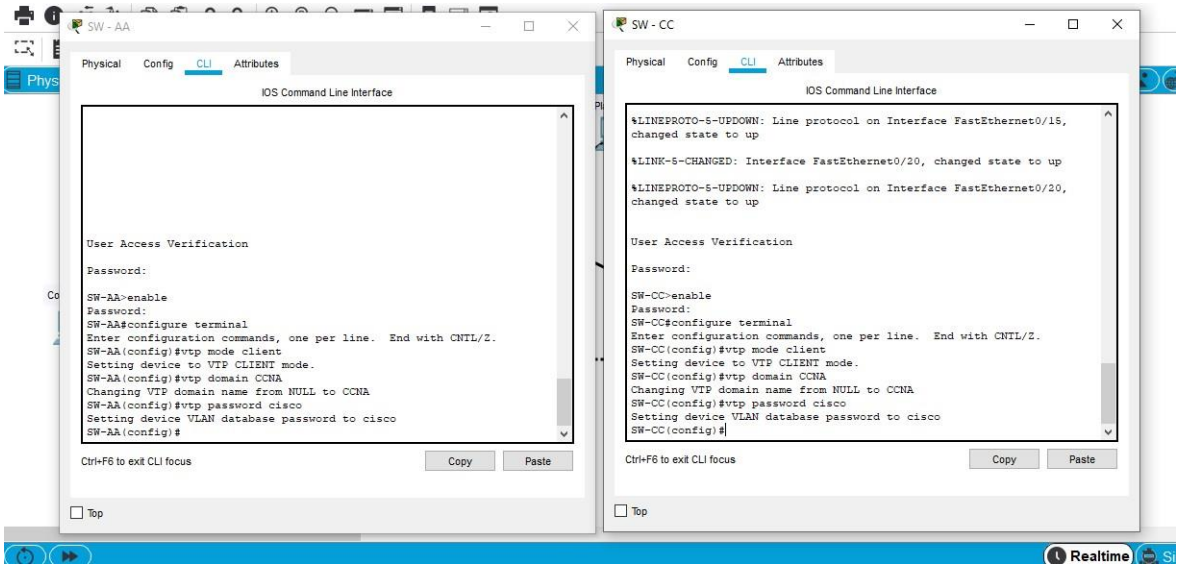


1. Ahora hay que configurar el switch SW-AA y SW-CC como clientes VTP por medio del comando vtp mode client. Seguido hay que configurar el nombredel dominio en estos switch con el comando vtp domain CCNA. Luego configurar la contraseña con el comando vtp password cisco

SW-AA(config)# vtp mode client
SW-AA(config)# vtp domain CCNA
SW-AA(config)# vtp password cisco

SW-CC(config)# vtp mode client
SW-CC(config)# vtp domain CCNA
SW-CC(config)# vtp password cisco

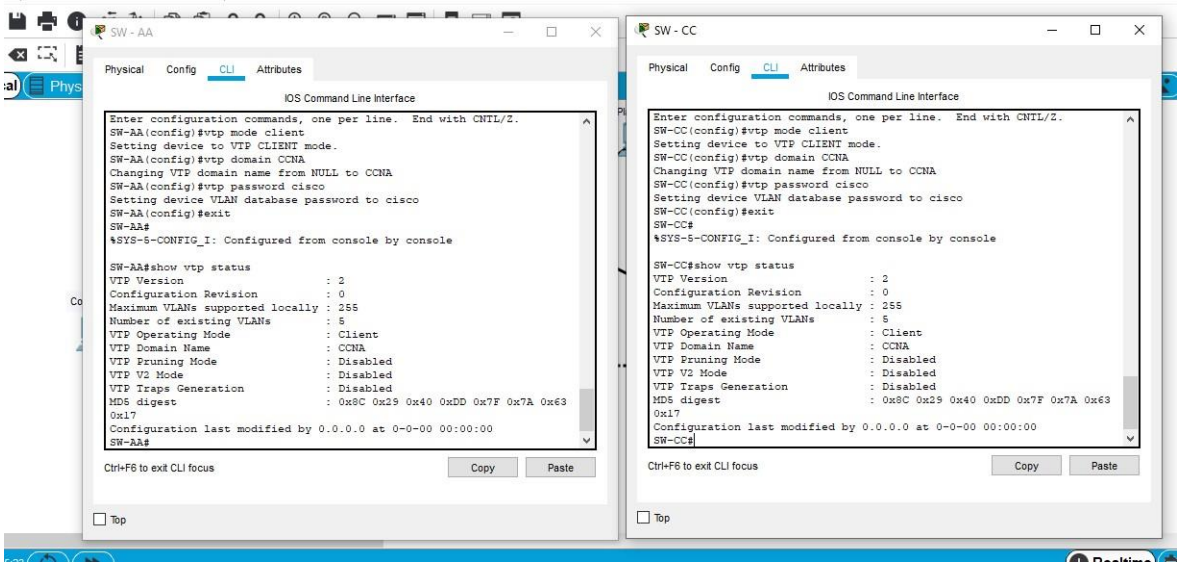
Figura 18: Configuración de los switch SW-AA y SW-CC como cliente



2. Verificar los cambios por medio del comando show vtp status.

SW-AA(config)# show vtp status
SW-CC(config)# show vtp status

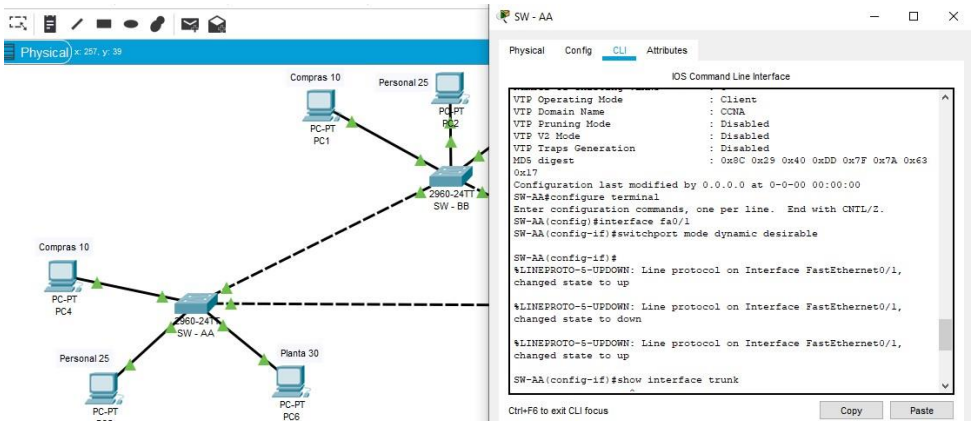
Figura 19: Verificación de la configuración de los switch SW-AA y SW-CC como cliente



3. Para realizar la configuración DTP (Dynamic Trunking Protocol) usamos el comando switchport mode trunk por medio de los siguientes comandos.

SW-AA(config)#interface fa0/1
SW-AA(config)# switchport mode dynamic desirable
SW-AA(config)# exit

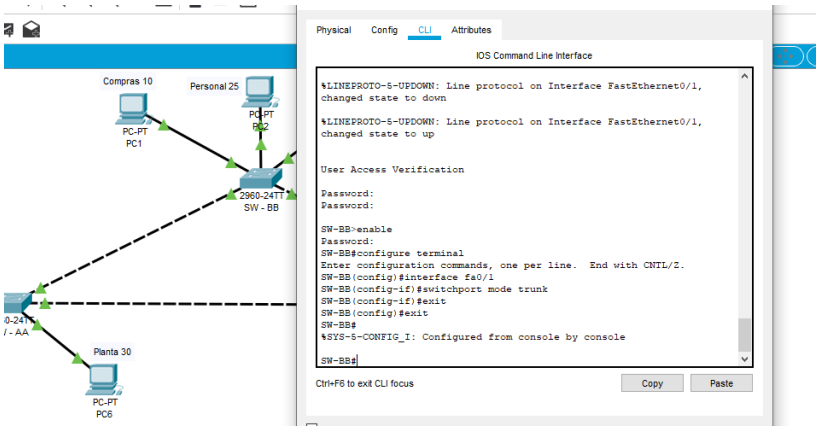
Figura 20: Configuración DTP del SW-AA para la interfaz fa0/1



4. Ahora seguimos configurando en el switch SW-BB el puerto FastEthernet0/1 para enlace trunk.

SW-BB(config)#interface fa0/1
SW-BB(config)# switchport mode trunk
SW-BB(config)# exit

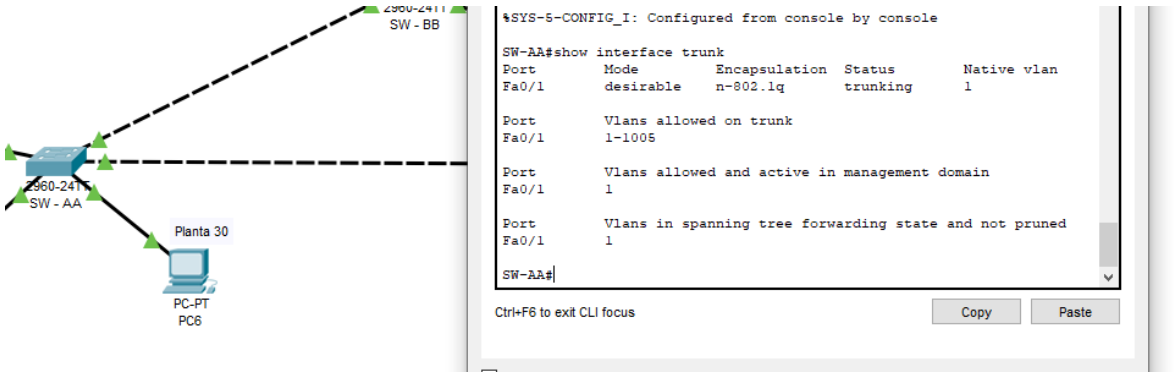
Figura 21: Configuración del switch SW-BB en modo troncal



5. Verificar en el switch SW-AA.

SW-AA#show interface trunk

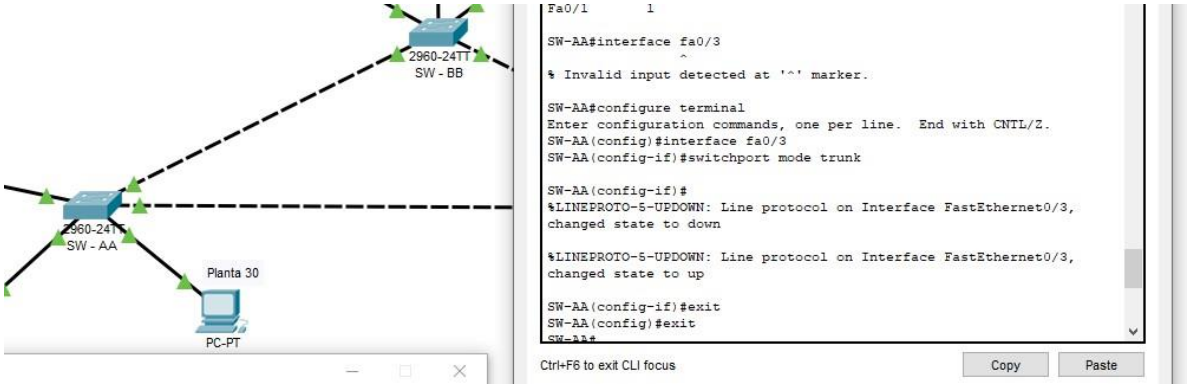
Figura 22: Verificación de enlace trunk fa0/1 en el switch SW-AA



6. Configurar en el switch SW-AA el puerto FastEthernet 0/3 para enlace trunk.

SW-AA(config)#interface fa0/3
SW-AA(config)# switchport mode trunk
SW-AA(config)# exit

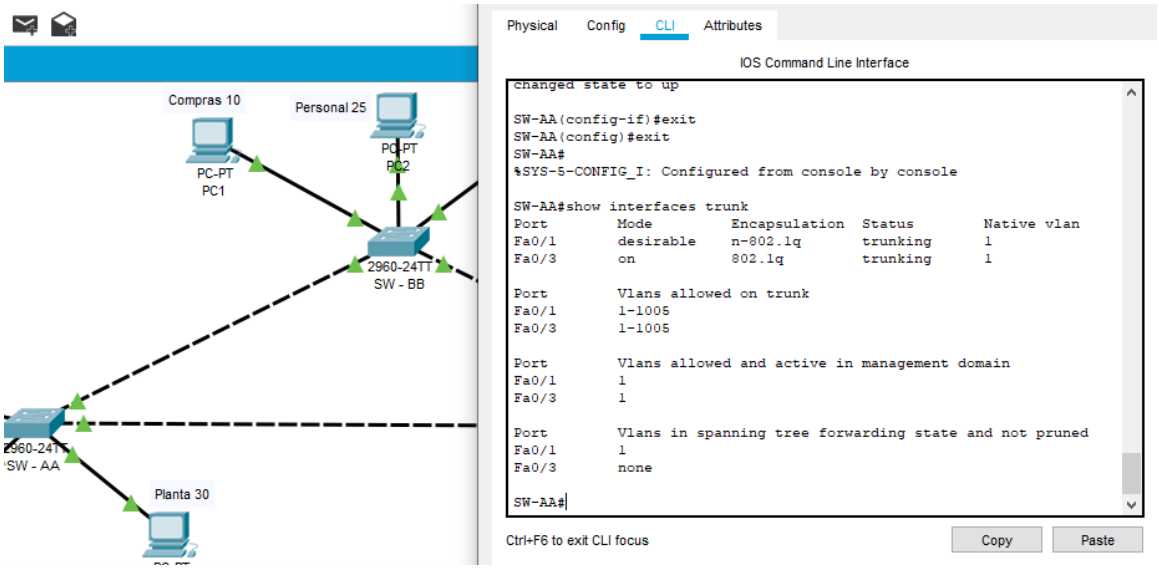
Figura 23: Configuración DTP del SW-AA para la interfaz fa0/3



7. Verificar en el switch SW-AA con el comando show vtp status y show interfaces trunk.

SW-AA# show interfaces trunk.

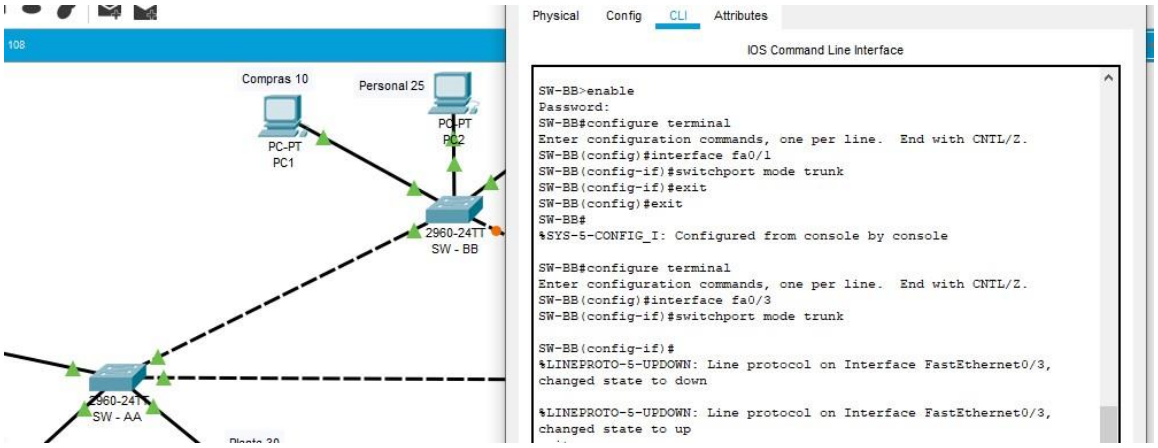
Figura 24: Verificación de enlace trunk fa0/3 en el switch SW-AA



8. Configurar en el switch SW-BB el puerto FastEthernet 0/3 para enlace trunk.

SW-BB(config)#interface fa0/3
SW-BB(config)# switchport mode trunk
SW-BB(config)# exit

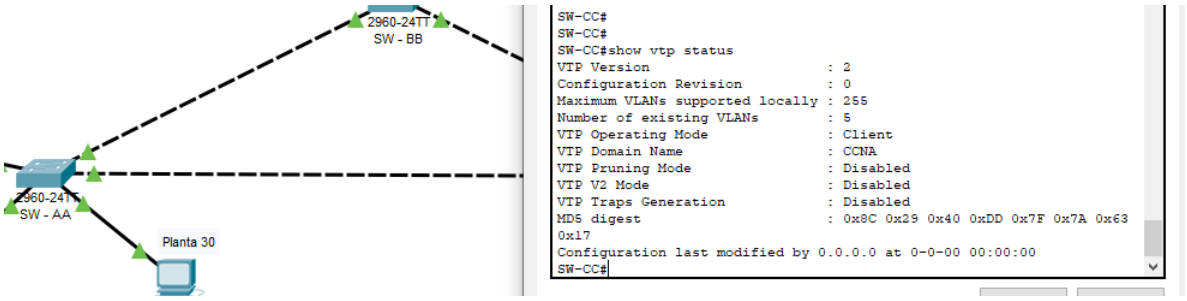
Figura 25: Configuración DTP del SW-BB para la interfaz fa0/3



9. Verificar en el switch SW-CC por medio del comando show interfaces trunk o show vtp status.

SW-CC# show interfaces trunk.

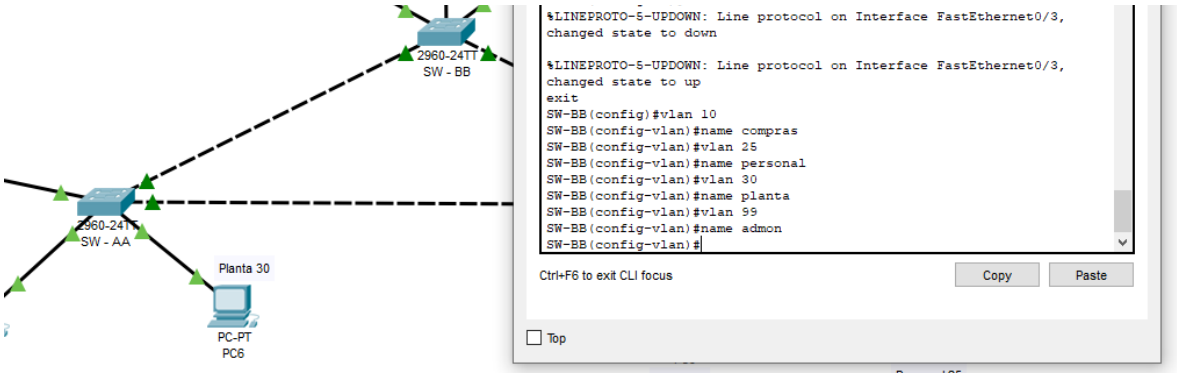
Figura 26: Verificación de enlace trunk fa0/3 en el switch SW-CC



10. Asignar de los puertos y Agregar VLANs. Para crear las vlan usamos los siguientes comandos.

SW-BB(config)# vlan 10
SW-BB(config)# 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

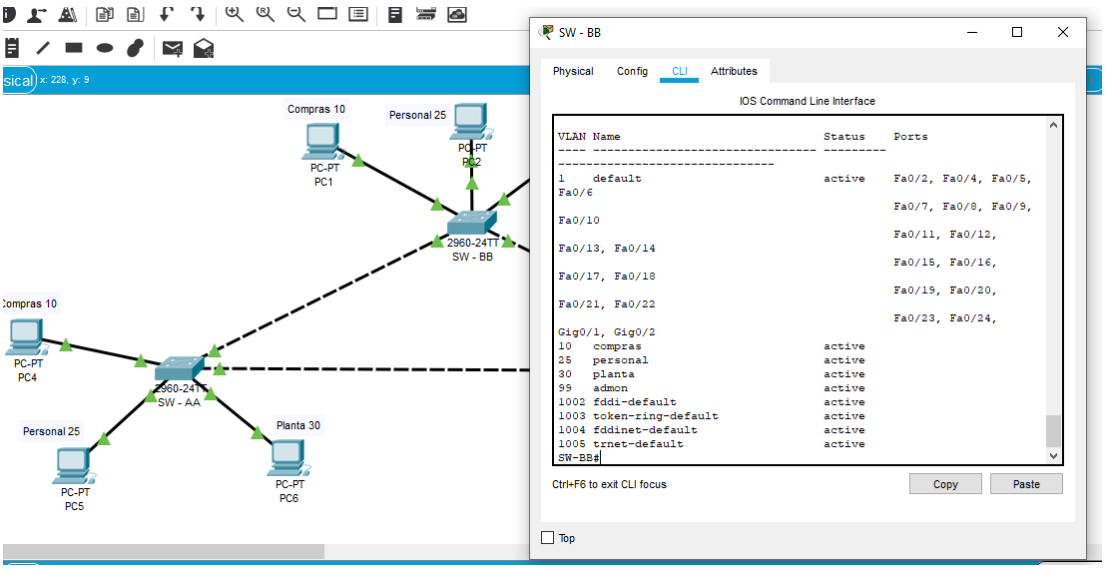
Figura 27: Creación de las vlan en el SW-BB



11. Verificar que las VLANs han sido agregadas correctamente utilizando el comando show vlan brief.

SW-BB# show vlan brief

Figura 28: Verificación de las vlan en el switch SW-BB



12. Asignar a cada PC su dirección IP, mascara de RED y puerta de enlace según corresponda de acuerdo a la siguiente tabla, donde X depende del número de cada PC.

Tabla: 5 Configuración de PC

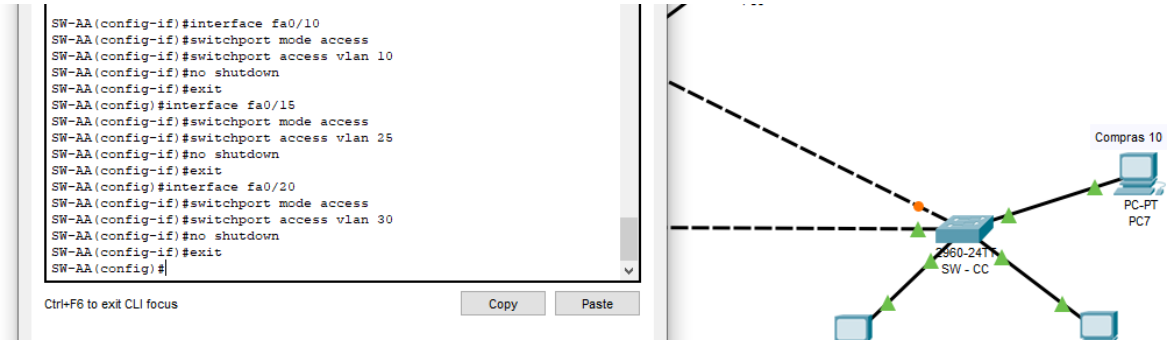
INTERFAZ	VLAN	DIRECCION IP DE LOS PC's
FA0/10	VLAN 10	190.108.10.X
FA0/15	VLAN 25	190.108.20.X
FA0/20	VLAN 30	190.108.30.X

13. Asignar las VLAN a los puertos en los switch por medio de los siguientes comandos.

SW-AA#Configure terminal
SW-AA(Config)#interface fa0/10
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 10

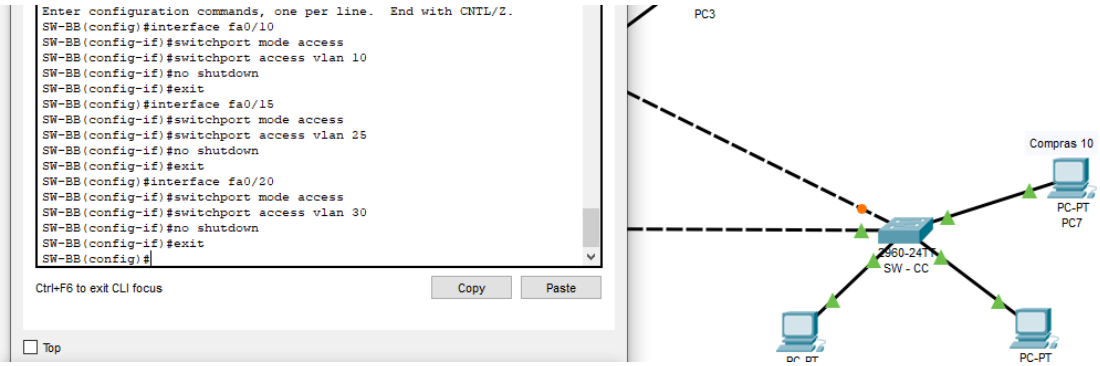
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit
SW-AA(Config)#interface fa0/15
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 25
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit
SW-AA(Config)#interface fa0/20
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 30
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit

Figura 29: Asignación de los puertos en el switch SW-AA



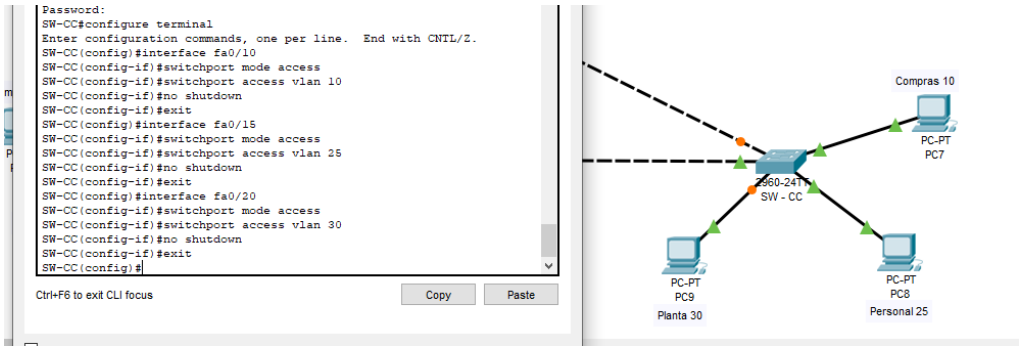
SW-BB#Configure terminal
SW-BB(Config)#interface fa0/10
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport mode Access vlan 10
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit
SW-BB(Config)#interface fa0/15
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport mode Access vlan 25
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit
SW-BB(Config)#interface fa0/20
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport mode Access vlan 30
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit

Figura 30: Asignación de los puertos en el switch SW-BB



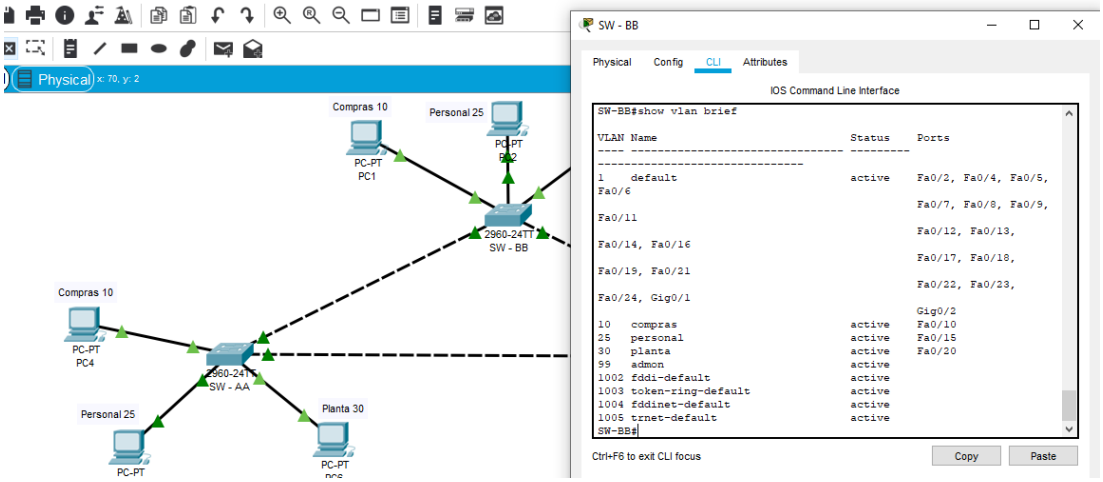
SW-CC#Configure terminal
SW-CC(Config)#interface fa0/10
SW-CC(Config-if)# switchport mode Access
SW-CC(Config-if)# switchport mode vlan 10
SW-CC(Config-if)# no shutdown
SW-CC(Config-if)# exit
SW-CC(Config)#interface fa0/15
SW-CC(Config-if)# switchport mode Access
SW-CC(Config-if)# switchport mode vlan 25
SW-CC(Config-if)# no shutdown
SW-CC(Config-if)# exit
SW-CC(Config)#interface fa0/20
SW-CC(Config-if)# switchport mode Access
SW-CC(Config-if)# switchport mode vlan 30
SW-CC(Config-if)# no shutdown
SW-CC(Config-if)# exit

Figura 31: Asignación de los puertos en el switch SW-CC



14. Verificar la configuración de las VLAN por medio del comando show vlan brief.

Figura 32: Verificación de los puertos en el switch SW-BB



15. Configurar las direcciones IP en los Switch por medio de los siguientes comandos.

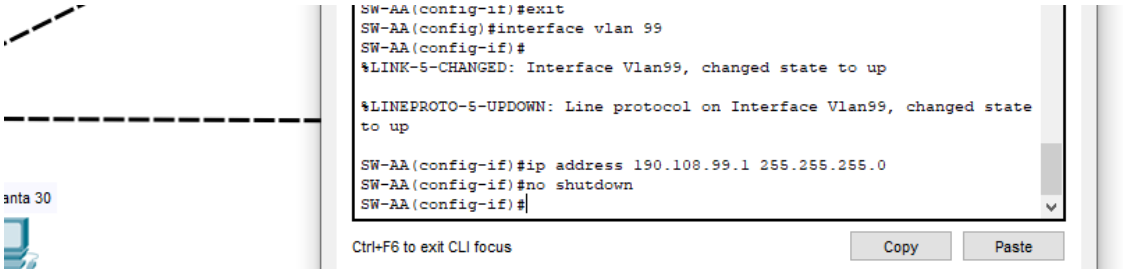
Tabla: 6 Configuración de Switch

EQUIPO	VLAN	DIRECCION IP
SW-AA	VLAN 99	190.108.99.1/24
SW-BB	VLAN 99	190.108.99.2/24
SW-CC	VLAN 99	190.108.99.3/24

SW-AA

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)#no shutdown

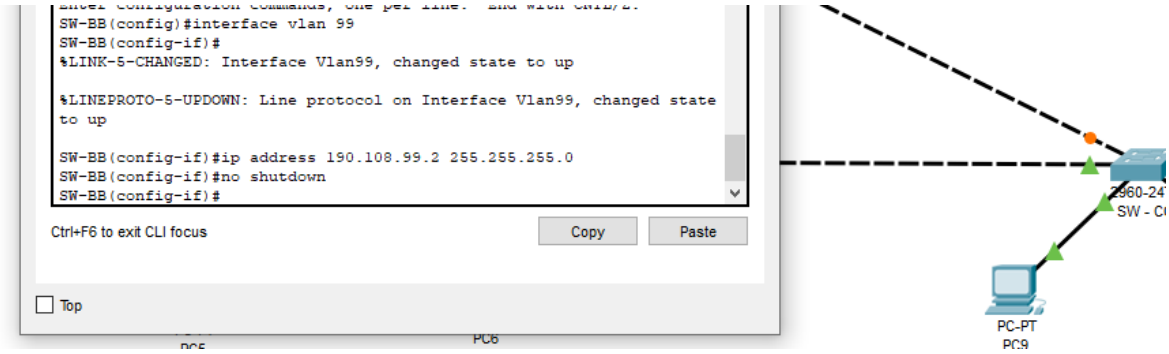
Figura 33: Configuración de las direcciones IP en el switch SW-AA



SW-BB

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)#no shutdown

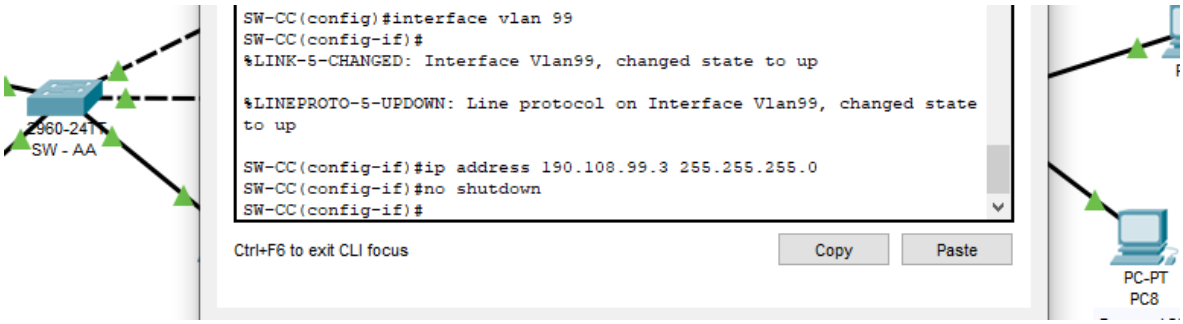
Figura 34: Configuración de las direcciones IP en el switch SW-BB



SW-CC

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)#no shutdown

Figura 35: Configuración de las direcciones IP en el switch SW-CC



16. Verificar la conectividad Extremo a Extremo.

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

Al ejecutar ping desde cada PC a los demás, se pudo observar que al hacer ping entre los PC's que tienen las mismas vlan si hay comunicación, mientras que sí, hacemos ping entre los PC's de diferente vlan, no hay comunicación ya que no se realizó el enrutamiento para que haiga comunicación entre diferentes VLAN.

Figura 36: Comprobación de conexión de PC's con la misma Vlan

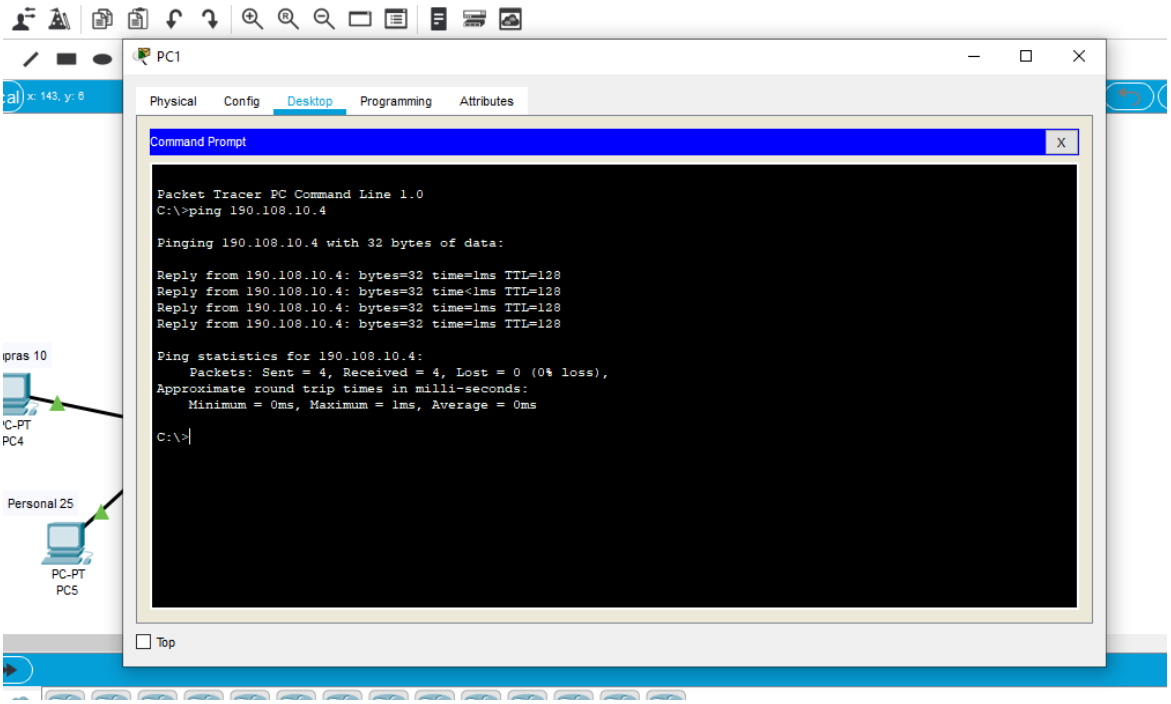
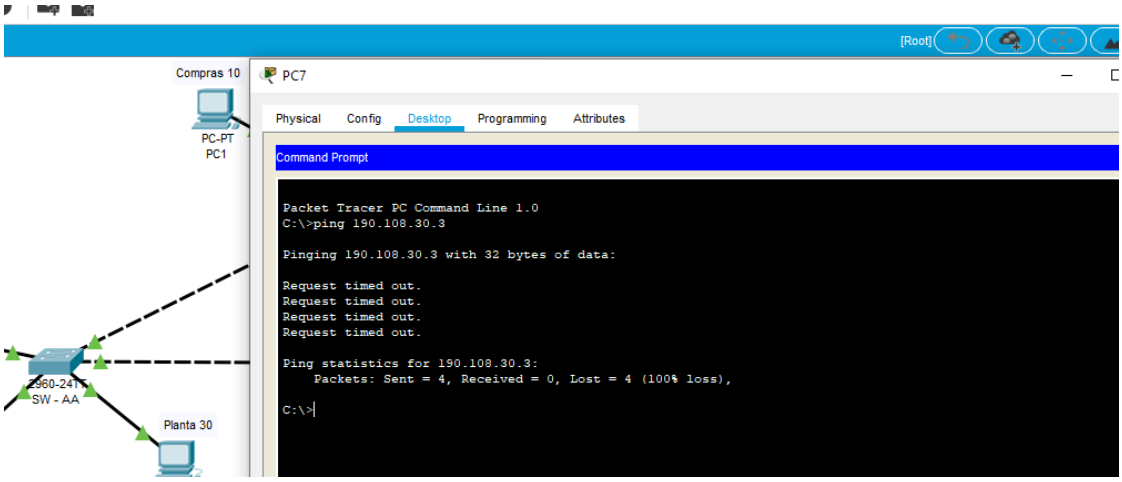


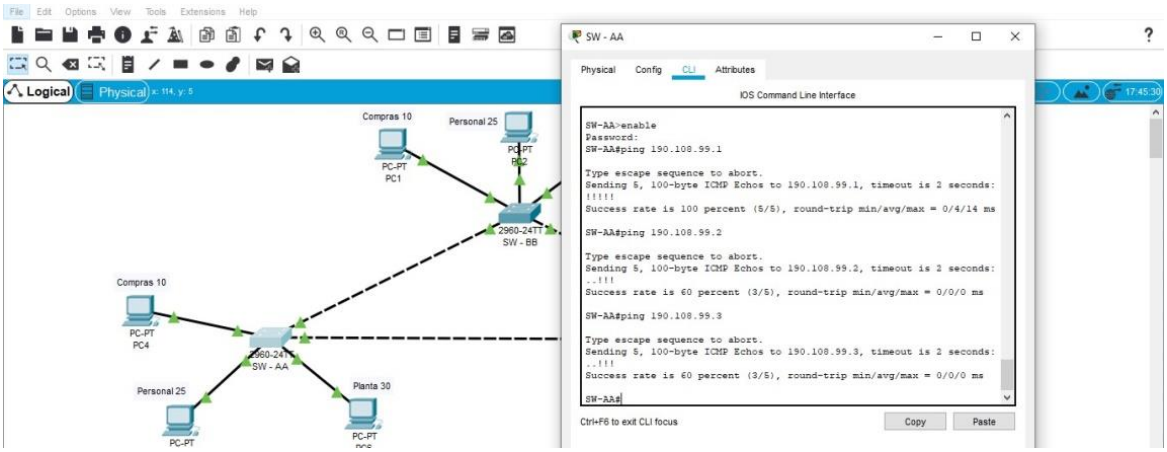
Figura 37: Comprobación de conexión de PC's con distinta Vlan



Ejecute un Ping desde cada Switch a los demás.

Al ejecutar el ping entre los tres switch, es exitoso, pues las direcciones IP que se les configuro están en una misma vlan 99 común para todos y todos cuentan con puertos trunk lo que permite el paso de paquetes y efectivamente comprobamos que si hay comunicación desde este switch a los otros.

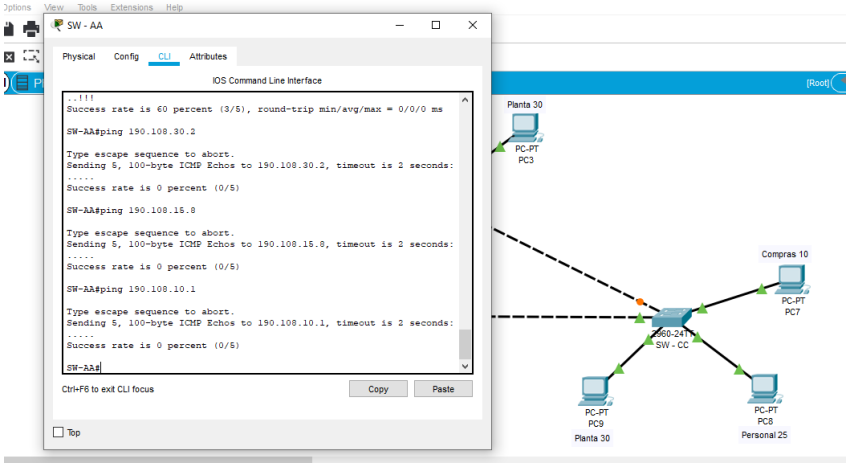
Figura 38: Verificación del ping desde los switch



Ejecute un Ping desde cada Switch a cada PC.

Al ejecutar un ping desde cada switch a cada PC, no se tuvo éxito, no hay comunicación ya que la dirección IP es fundamental permitiendo que cada dispositivo pueda ser reconocido dentro de la misma red y así poder enviar y recibir información y en este caso podemos observar que ni el switch ni el pc tienen configurada una dirección IP, haciendo que los PC's no se encuentren dentro de la red.

Figura 39: Verificación del ping desde los switch a los PC's



CONCLUSIONES

La realización de los escenarios por medio de las simulaciones en el programa packet tracer, tiene muchas ventajas no solo para el aprendizaje en redes y comunicaciones, sino también por la importancia de implementar en una organización estos sistemas e interconectar los distintos dispositivos y transmitir la información de una forma más fácil y segura permitiendo un control más óptimo de los diferentes procesos en una compañía.

Es importante aprender a manejar el programa Packet Tracer, ya que, sin la ejecución y comprensión del mismo no se hubiera logrado cumplir los objetivos y adquirir conocimiento para desarrollar e implementar los escenarios requeridos.

Se desarrollaron distintas habilidades en temas como las configuraciones EBGP, VTP, DTP, los protocolos de enrutamiento Avanzado, las VLAN, entre otros vistos a lo largo del diplomado de cisco CCNP, orientados hacia el mundo profesional y actual, lo cual nos permitirán dar soluciones a los problemas que se presenten y evitar fallas.

Se debe tener en cuenta que en la medida que el mundo de la electrónica evoluciona, también lo hace los diferentes protocolos de comunicación, los cuales cooperan entre sí para mantener la eficiencia y eficacia en el transporte de datos de forma global y local, por lo tanto hay que mantenerse actualizados en su uso y sus diferentes versiones.

BIBLIOGRAFIA

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-NT1IlnMfy2rhPZHwEoWx

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

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db= e000xww&AN=158227&lang=es&site=ehost-live

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

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

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-NT1IlnMfy2rhPZHwEoWx

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

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-NT1IlnWR0hoMxgBNv1CJ

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db= e000xww&AN=158227&lang=es&site=ehost-live

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

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD