DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO ALEJANDRO CASTELLANOS PINEDA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO ALEJANDRO CASTELLANOS PINEDA

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
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C, 22 de mayo de 2020

AGRADECIMIENTOS

Al culminar una nueva etapa, llena de dificultades en el desarrollo del Diplomado De Profundización CISCO CCNP, es para mí un verdadero placer poder dedicar este espacio, al poder expresar mi más sincero agradecimiento al profesor Alejandro Pérez y al director de grado Gerardo Granados. Por su apoyo, orientación y confianza durante el trascurso de aprendizaje del Diplomado De Profundización CISCO CCNP.

Finalmente agradezco a mis compañeros de curso. A José Cándelo, Johana Parada, Cesar Correa y Orlando Linares. Por su comunicación contantes en cada una de las actividades y el apoyo incondicional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CONFIGURACIÓN EBGP E IBGP: Es el que permite crear un dominio en el ruteo libre de loops en un sistema de autónomo. Es el protocolo de BGP utilizado para el transporte de mensajes para abrir y se encarga de la conexión de los parámetros.

NETLAB: Son las topologías de redes en datos, en particular las empresas que trabajan con redes de datos controlados remotamente con fines únicamente educativos.

PROTOCOLO HSRP: Es un protocolo de propiedad de Cisco, Es de capa tres encargado de proporcionar redundancia al Gateway. Se utiliza para cuando se produce una falla de red en un sistema multicast.

HOT STANDBY: Es un protocolo de Cisco que se encarga del despliegue de los routes en caso de que se produzca una falla de red. Lo que evita las inconsistencias de puntos de fallo únicos en el sistema.

REDUNDANCY PROTOCOL (VRRP): Este tipo de protocolo permite la comunicación de un propietario definido y puede estar diseñado con el fin de aumentar los enlaces de puerta dados a una misma máquina de subred.

PLANTILLAS SDM: Son las que permiten a los routes la configuración con el fin de sacar el mayor rendimiento de los routes de centro de red para poder maximizar los recursos del sistema mediante unicast.

RESUMEN

En este estudio de Diplomado CISCO CCNP, es un curso de profundización. Se examinó los aspectos más relevantes de enrutamiento y conmutación, donde se busca una manara de equipar a nuevos profesionales en el ámbito laboral y se puedan adquirir métodos de diseño de redes, para el enrutamiento de redes avanzadas, la implementación de diversos mecanismos en la actualización de enrutamiento en el tráfico de redes empresariales.

Se desarrolla el módulo CCNP ROUTE, donde se utiliza el método de tareas, con esta estrategia se promueve el aprendizaje de cada una de las competencias, las cuales cumple con un orden lógico, facilitando el aprendizaje de cad uno de los temas con los simuladores de Packet Tracer / GNS3 y el acceso a la plataforma de laboratorios remotos SMARTLAB.

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

ABSTRACT

In this CISCO CCNP Diploma study, it is an in-depth course. The most relevant aspects of routing and switching are examined, where team management is sought for new professionals in the workplace and network design methods can be obtained, for routing advanced networks, the implementation of various mechanisms in updating routing in business network traffic.

The CCNP ROUTE module is developed, where the task method is used, with this strategy the learning of each of the competences is promoted, which complies with a logical order, facilitating the learning of each of the topics with the simulators of Packet Tracer / GNS3 and access to the SMARTLAB remote laboratory platform.

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

INTRODUCCIÓN

Con el siguiente trabajo, se debe dar cumplimiento al desarrollo de los dos escenarios planteados en el Diplomado de profundización CNNP, con el fin de realizar un proceso de documentación y solución a cada una de las actividades propuestas con su respectiva configuración de los dispositivos.

Durante el desarrollo del escenario uno, se emplea el software GNS3, con el fin de crear una topología donde por medio de 4 Router se busca dar la configuración BGP y la codificación de los ID para los routers. Por medio del comando show ip route, se debe verificar la información utilizada en el enrutamiento. Se debe elaborar un paso a paso del escenario plantado.

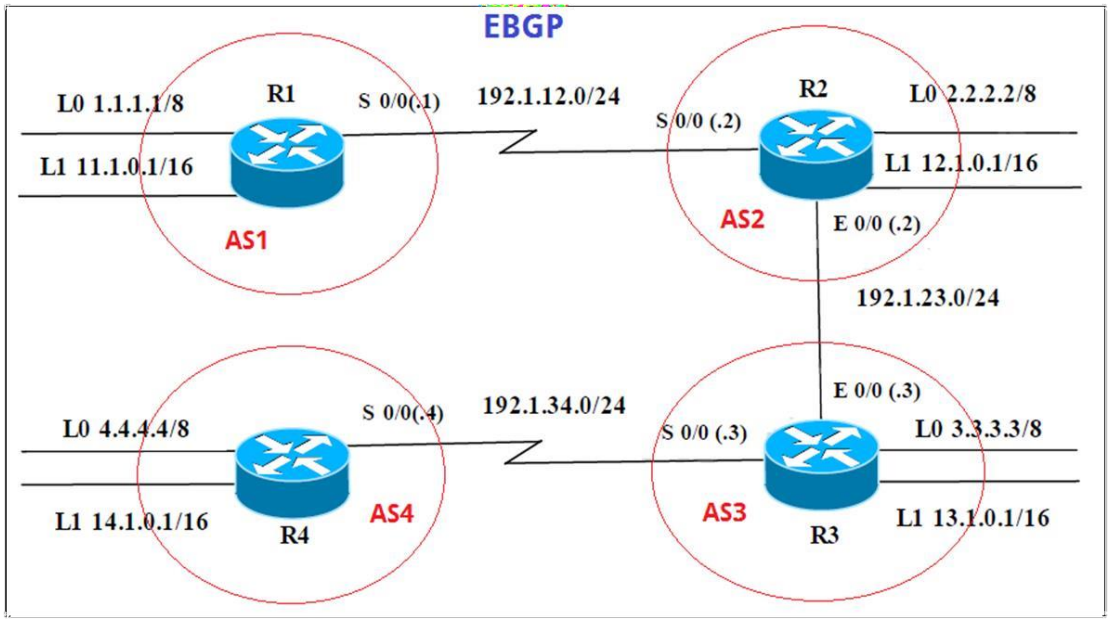
En el escenario dos, se emplea el software Packet Tracer, a partir de una topología donde se deben emplear switches y computadores de escritorio. Se debe crear un protocolo dinámico con la configuración del VTP y la actualización de las VLAN en los switch. En los PC se deben asociar los puertos VLAN y configurar las direcciones IP. Por medio de un ping entre los PC y los Switch se debe comprobar su conexión.

DESARROLLO

ESCENARIO 1

1. Para este escenario se utilizó el software GNS3

Figura 1. Escenario 1



Información para configuración de los Routers

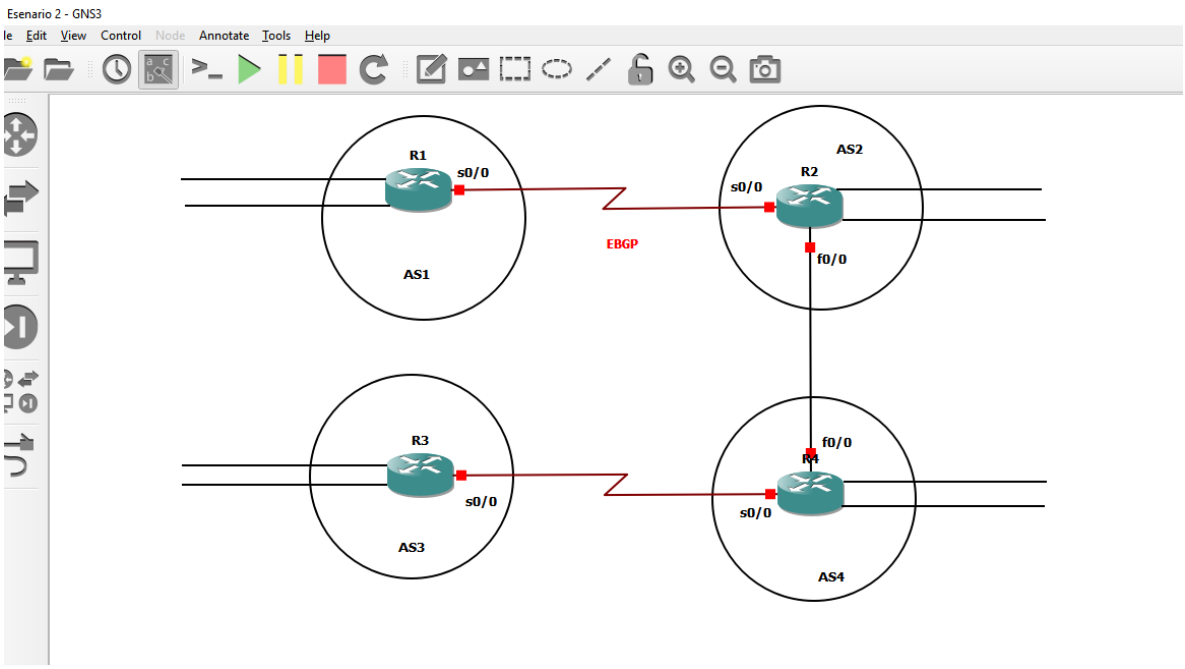
Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

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

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

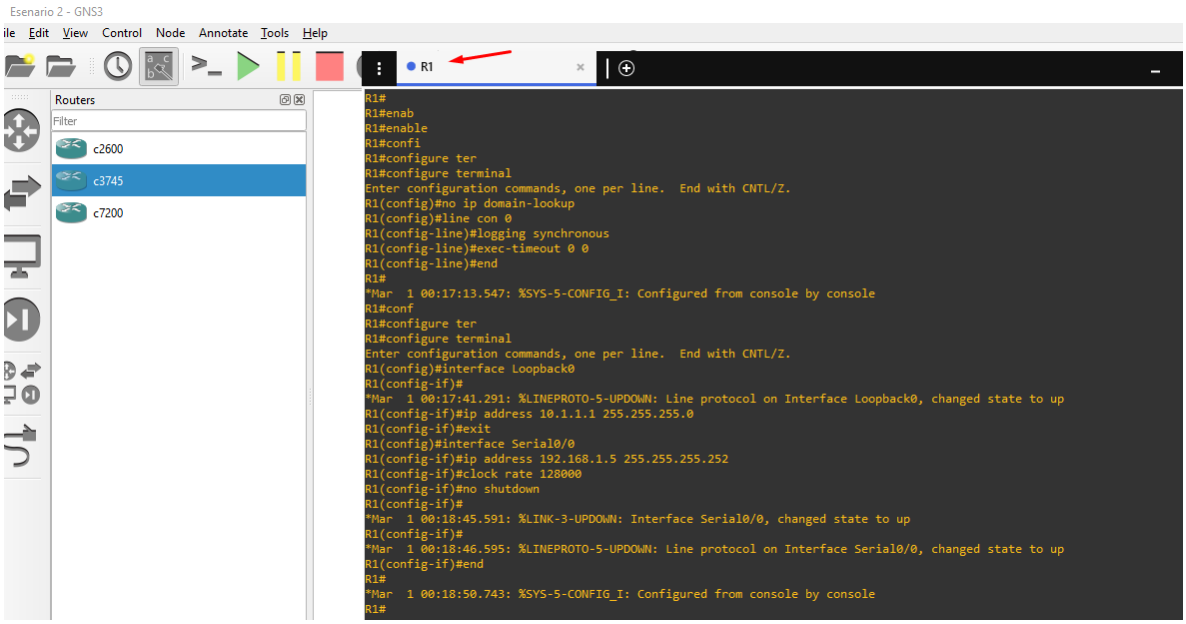
Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

Figura 2. Simulación de escenario 1



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.

Figura 3. Aplicando código R1



Se configura los routrs con el BGP y las dirreciones de loopback, se utiliza el comando show ip route.

Router R1

R1 #configure terminal

R1 (config)#int Loopback 0

R1(config-if)#ip addre

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)#interface s1/0

R1(config-if)#ip address 192.1.12.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#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

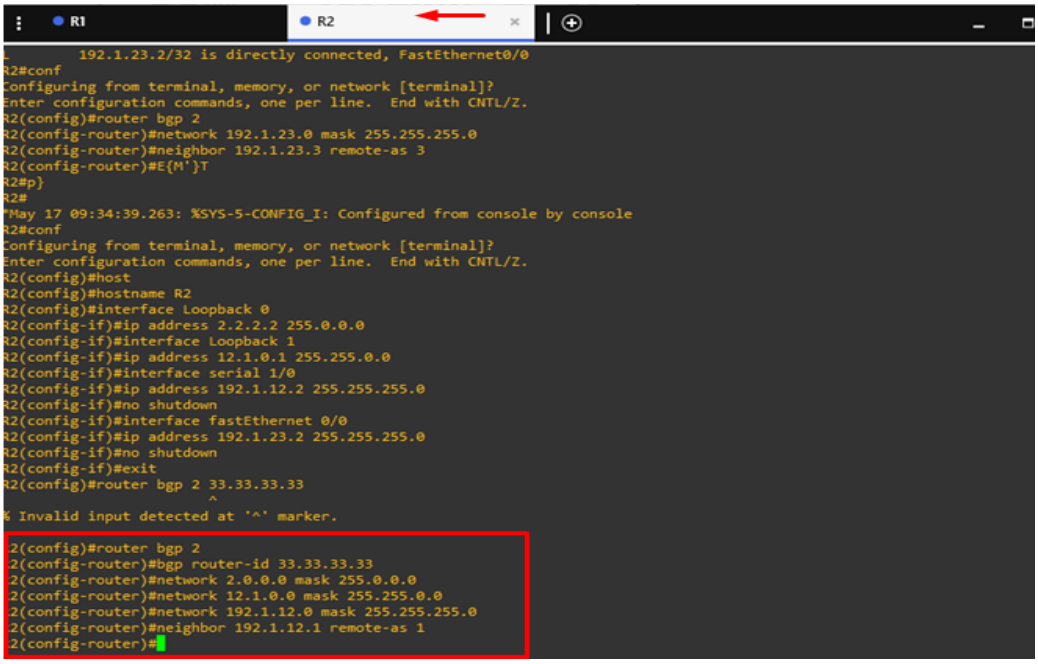
R1(config-router)#netw

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 4. Aplicando código R2

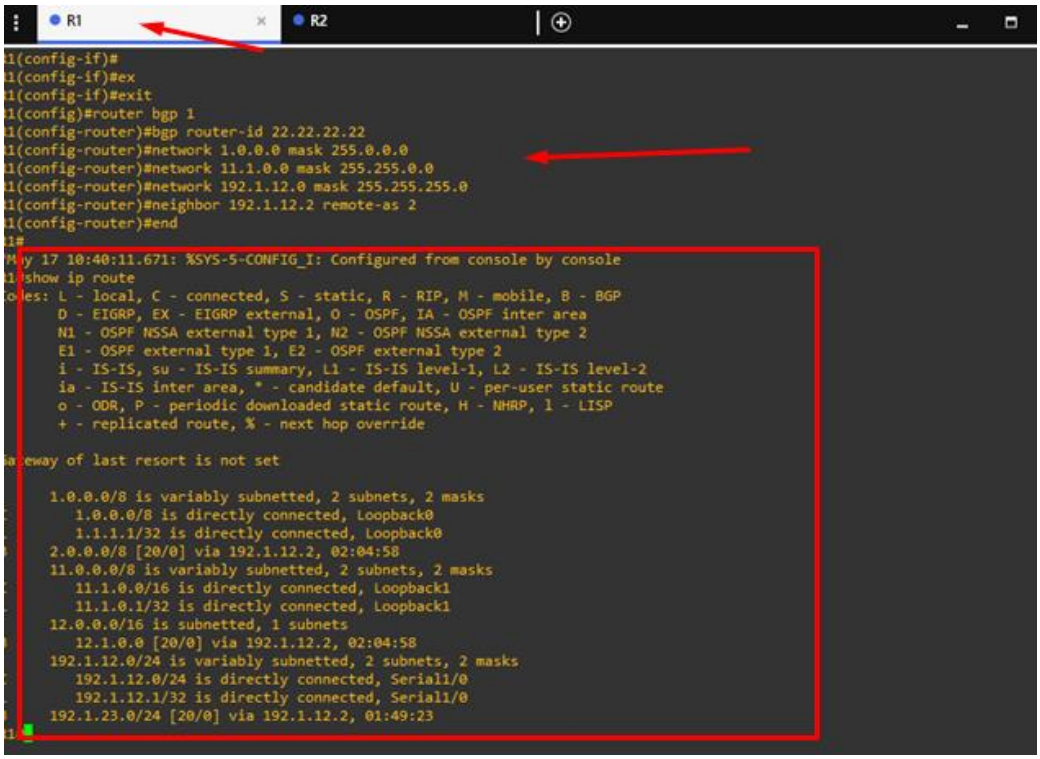


Se configura los routrs con el BGP y las dirreciones de loopback, se utiliza el comando show ip route y se evidencia tanto como el router 1 y 2 contienen un enrutamiento Loopback y reconoce las rutas del 192.1.12.0/24 por medio de la interfaz 1/0.

Router R2

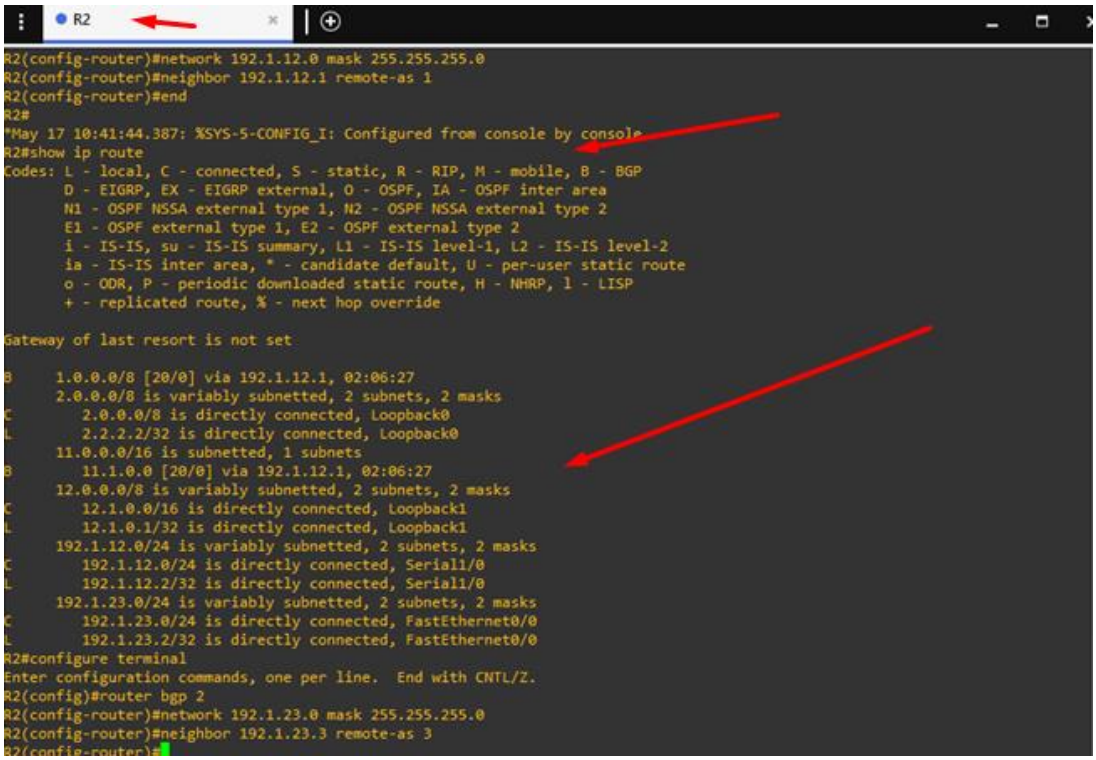
```
R R2#configure terminal
R2(config)#int Loopback 0
R2(config-if)#ip address  2.2.2.2  255.0.0.0
R2(config-if)#interface  Loopback 1
R2(config-if)#ip address 12.1.0.1  255.255.0.0
R2(config-if)#interface s1/0
R2(config-if)#ip addre
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface f 0/0
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 5. Comprobación del código R1



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 con los comandos utilizados y la salida del comando show ip route

Figura 6. Aplicando código R2



Se configuro el BGP

Router R2

R2#configure

R2#configure term

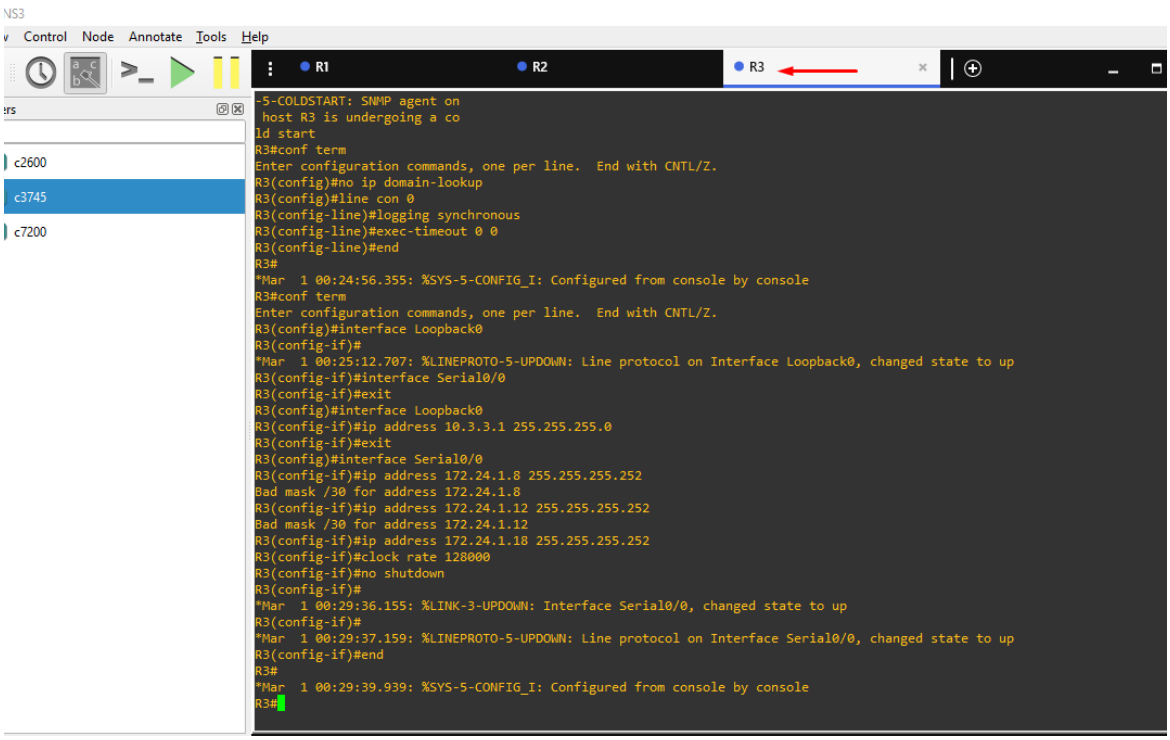
R2(config)# router bgp2

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)#

Figura 7. Aplicando código R3

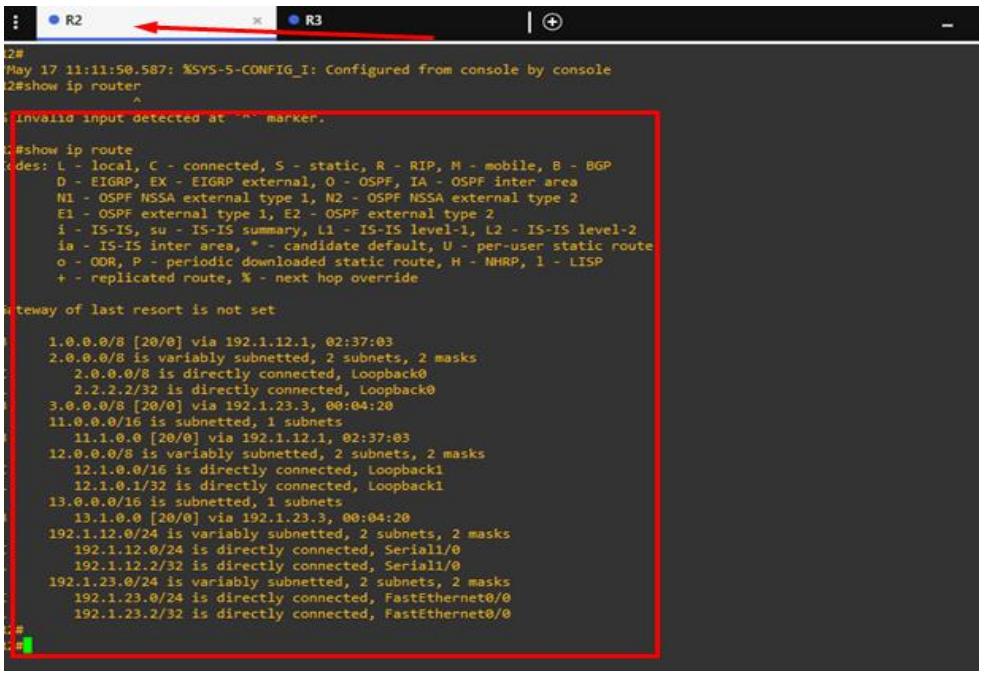


Por medio del commando show ip route se logró actualizar la tabla de enrutamiento y contienen las mismas direcciones del Reuters r3.

Router R3

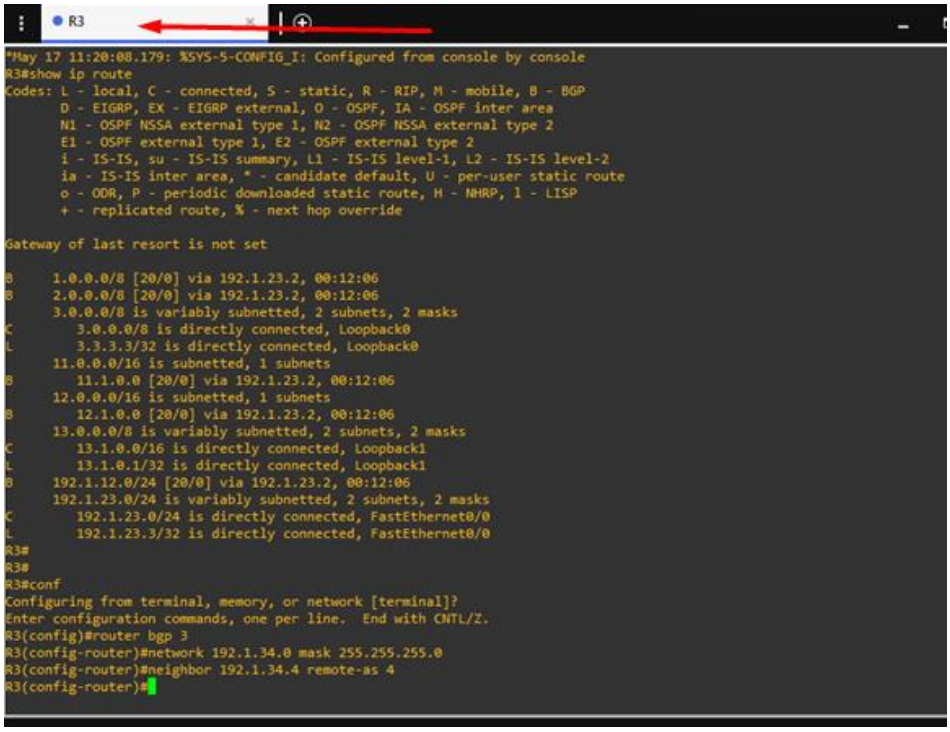
R3 enable
R3#configure term
R3(config)#intLoopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#int Loopback 1
R3(config-if)#ip add 13.1.0.1 255.255.0.0 R3(config-if)#interface fastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0 R3(config-if)#no shutdown
R3(config-if)#interface s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
 R3(config)#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
R3 (config-if)# no shutdownR3 (config-if)# exit

Figura 8. Aplicando código R2



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

Figura 9. Interfaces de Loopback en R3



Se configuro el BGP en AS3

Router R3

R3#configure ter

R3#configure terminal

R3(config)#router bgp 3

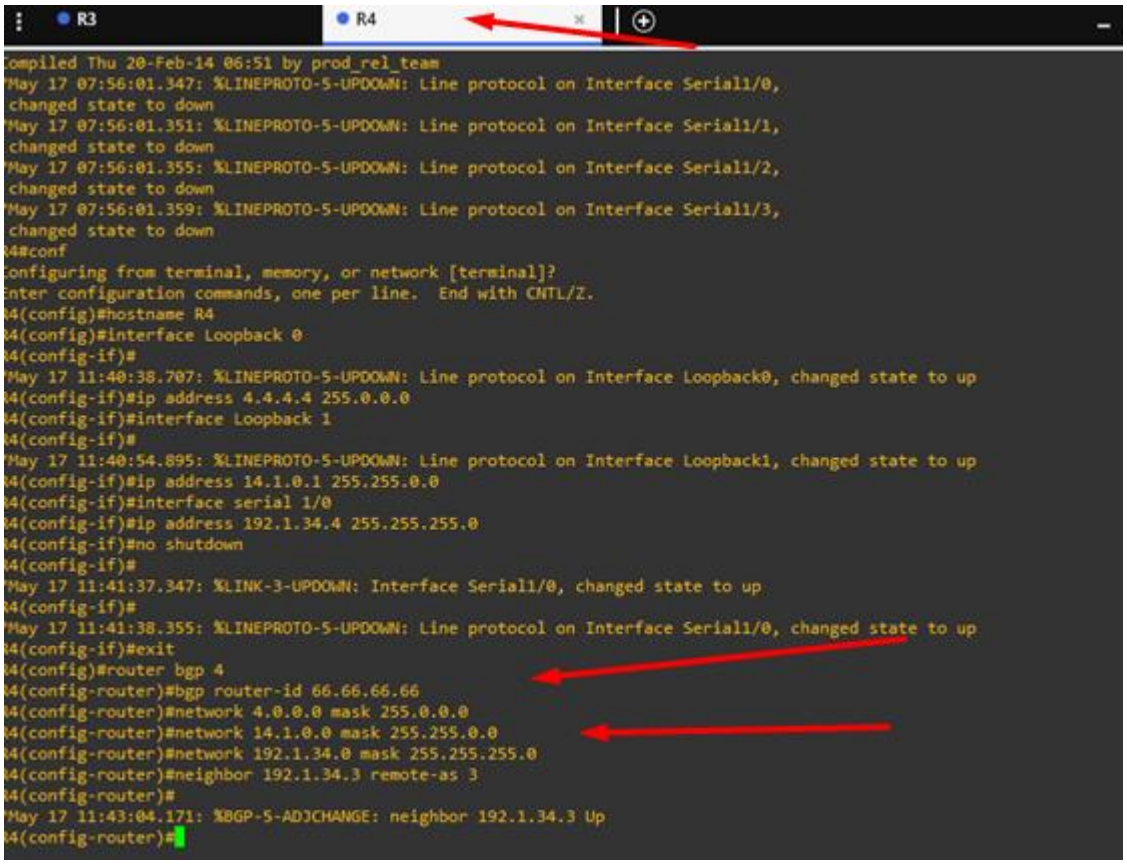
R3(config-router)#network192.1.34.0mask255.255.255.0

R3(config-router)#neighbor 192.1.34.4 remote-as 4

R3(config-router)#neighbor 192.1.34.4 remote-as 4

R3(config-router)#

Figura 10. Interfaces de Loopback en R4



Se configuro el BGP y se restable la comunicación del router Loopback con un intrfaz física y se le adiciona una configuración adicional.

Router R4

R4#enable

R4#configure ter

R4#configure terminal

R4(config)#int Loopback 0

R4(config-if)#ip add 4.4.4.4 255.0.0.0

R4(config-if)#int Loopback 1

R4(config-if)#ip add 14.1.0.1 255.255.0.0

R4(config-if)#interface s1/0

R4(config-if)#ip address 192.1.34.4 255.255.255.0

R4(config-if)#no shut

R4(config-if)#exit R4(config)

#router bgp 4

R4(config-router)#bgp router-id 66.66.66.66

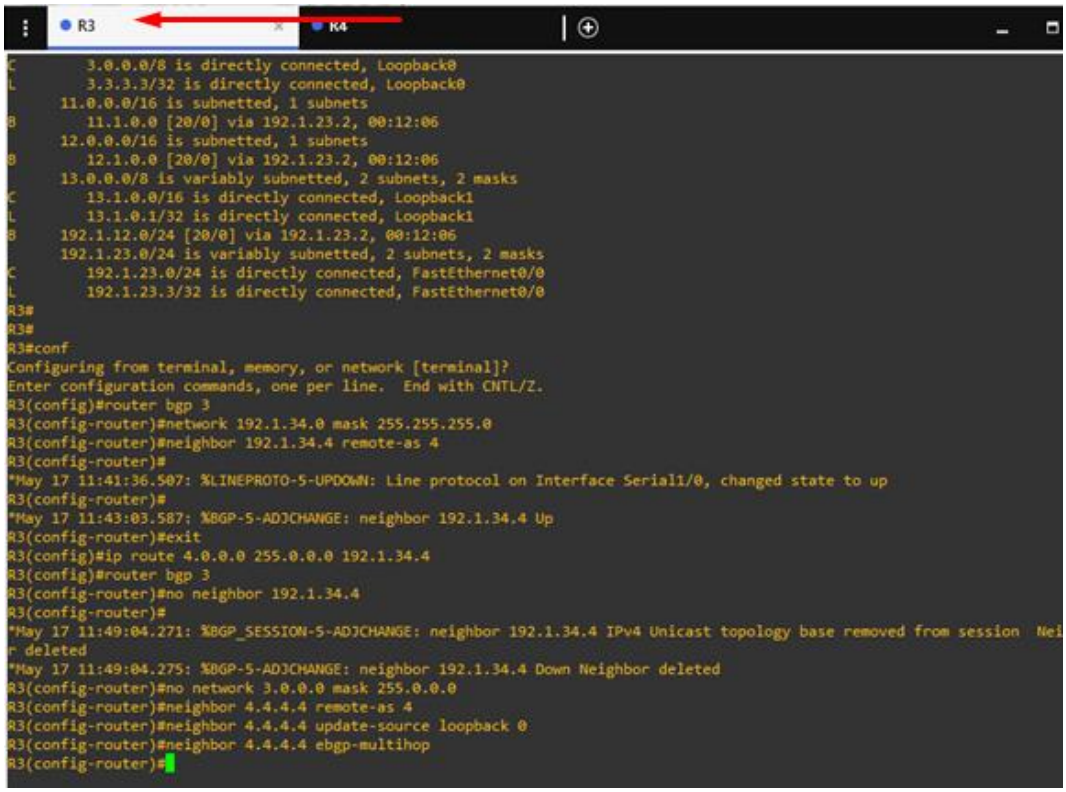
R4(config-router)#network 4.0.0.0 mask 255.0.0.0

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 R3



Se configura la BGP del router

Router R3

R3#enable

R3#configure ter

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

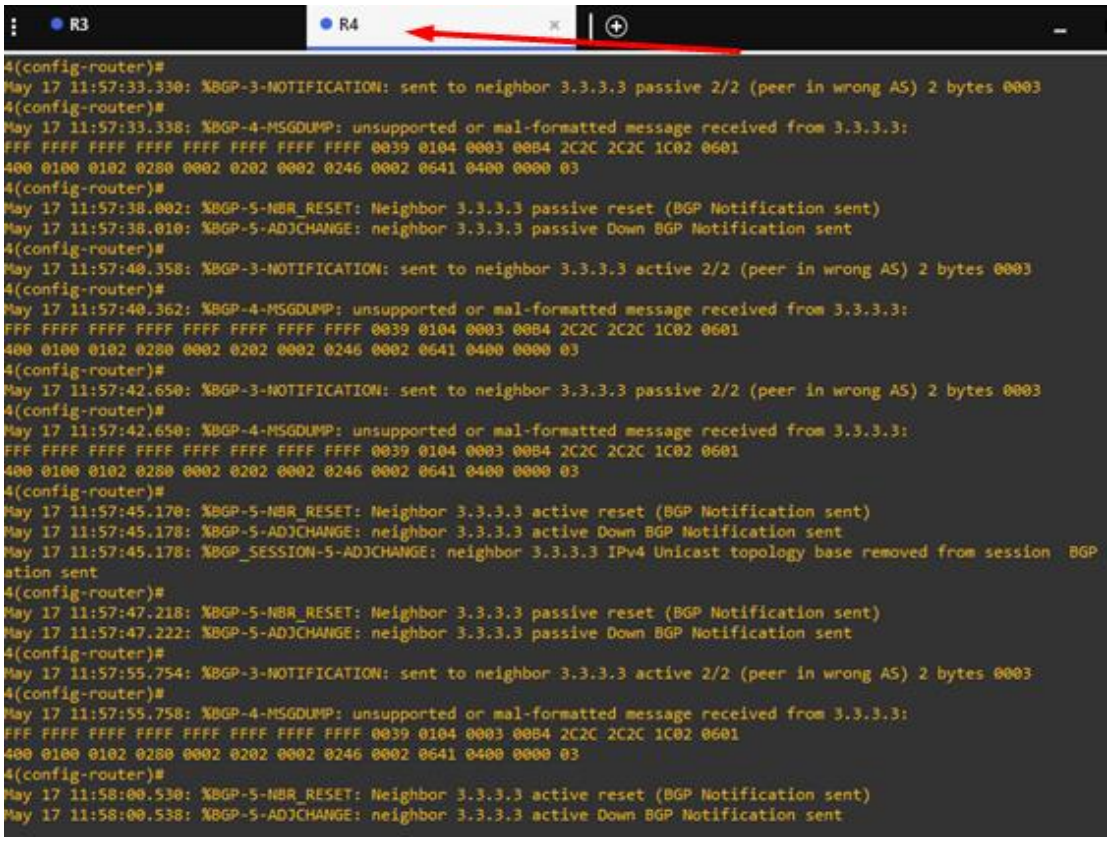
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0

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 R4



Se obtiene los resultados de del comando show ip route de la tabla de enrutamiento y se puede identificar las direcciones de las interfaces mediante el protocolo de BGP. Se puede obtener los resultados de la ruta estática que se creó en R3.

Router R4

R3#enable

R3#configure ter

R3#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 4

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

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

R4(config-router)# R4(config-router)#

Figura 13. Commando show ip route

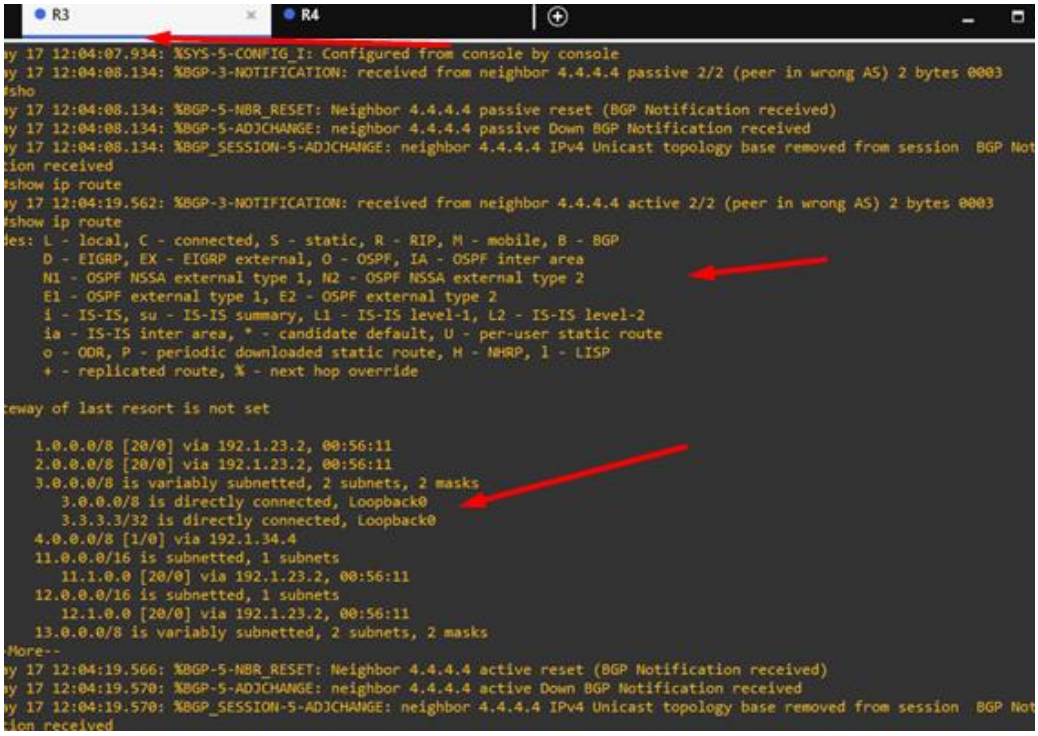
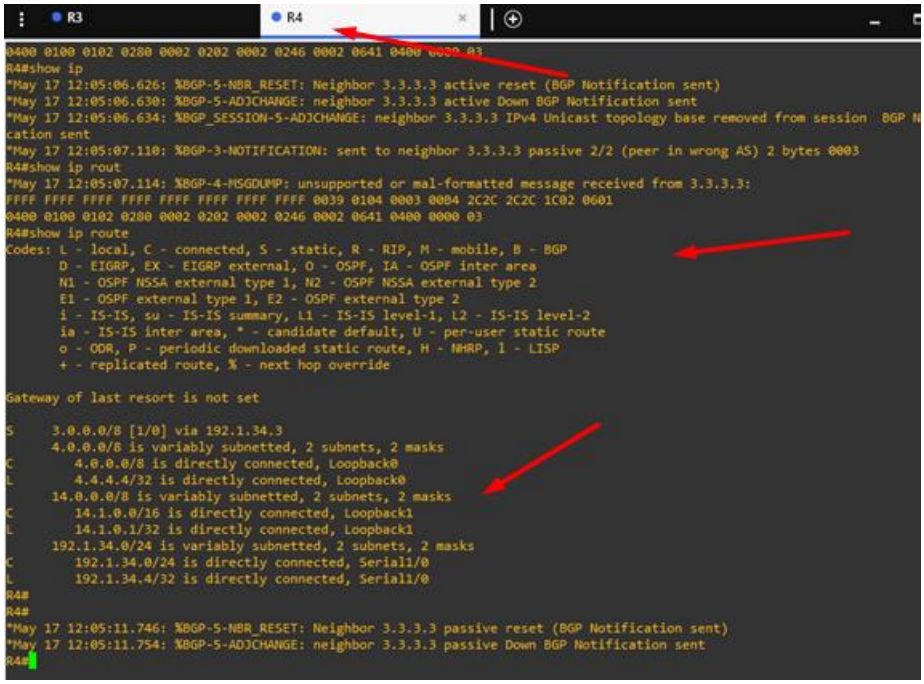


Figura 14. Comando show ip route



ESCENARIO 2

1. Para este escenario se utilizó el Packet Tracer

Figura 15. Escenario 2

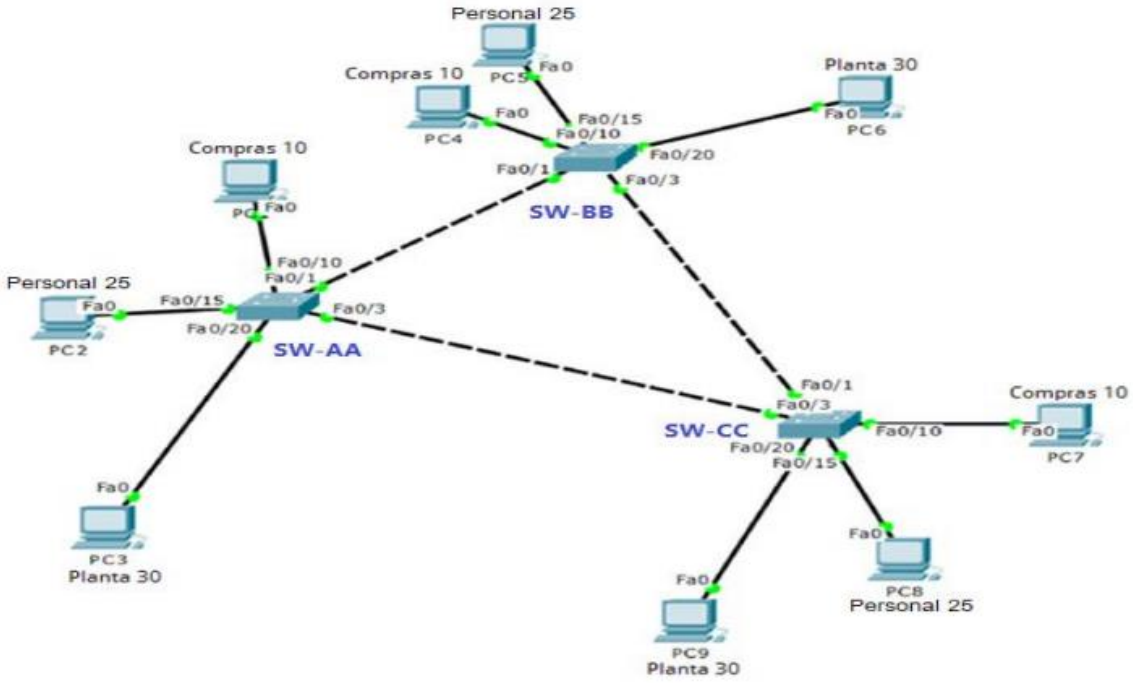
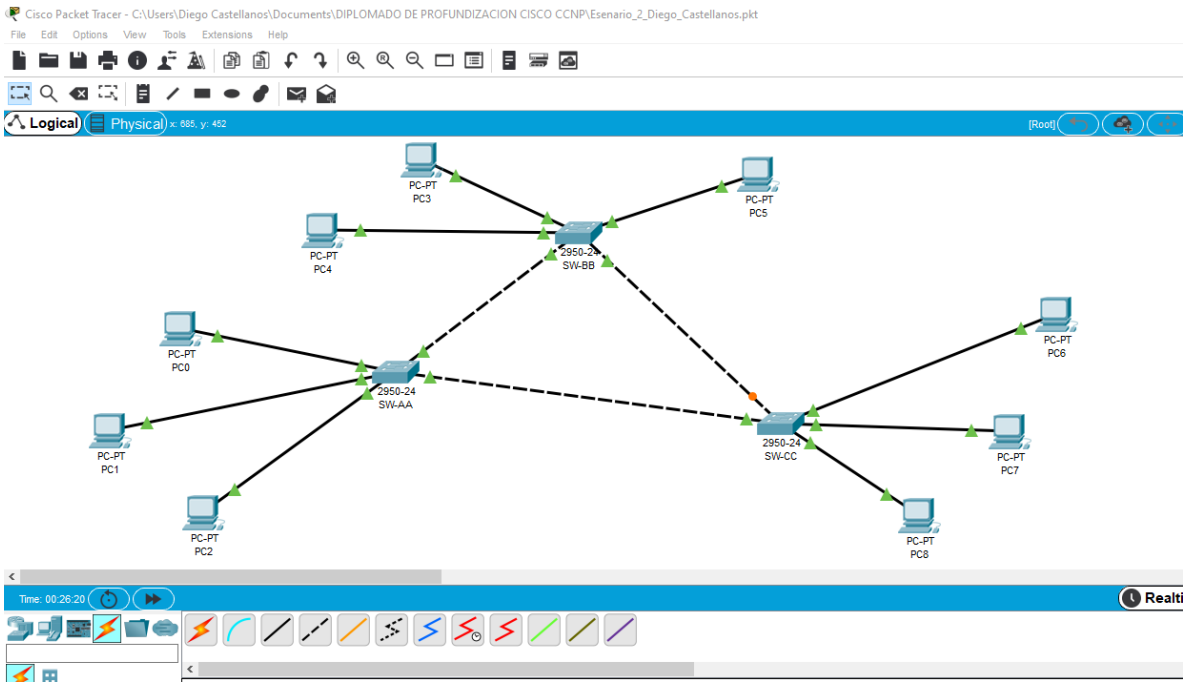


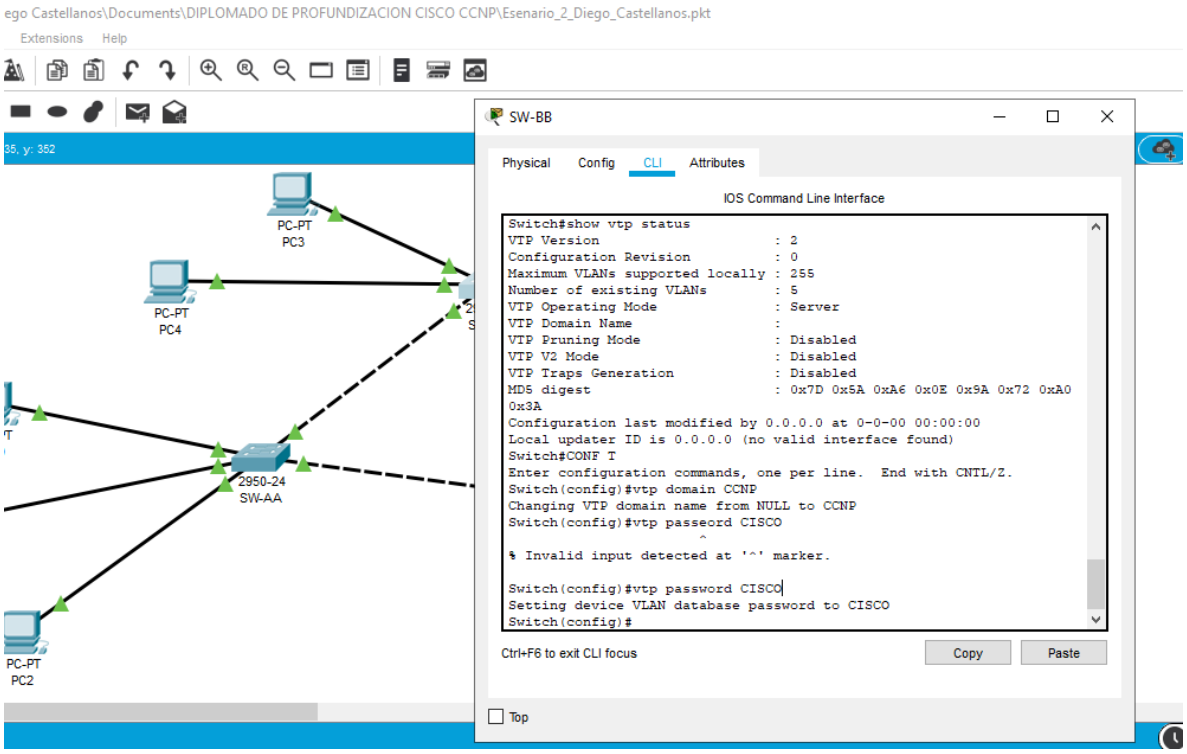
Figura 16. Simulación del escenario 2



Configurar VTP

2.1. 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

Figura 17. Configuración switch SW-BB



El switch SW-BB se configuro como el servidor en el dominio VPT llamado CCNP y usando la contraseña CISCO, se configura la VLAN 10 y 20. Los puertos que van del 0/1-3 los convertimos en modo troncal.

Switch#

Switch#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 :

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A

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)

Switch#CONF T

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vtp domain CCNP

Changing VTP domain name from NULL to **CCNP**

Switch(config)#vtp passeord CISCO

Switch(config)#vtp password CISCO

Setting device VLAN database password to **CISCO**

Switch(config)#do wr

Building configuration...

[OK]

Switch(config)#vlan 10

Switch(config-vlan)#name AAA

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name BBB

Switch(config-vlan)#exit

Switch(config)#interface

% Incomplete command.

Switch(config)#inter

Switch(config)#interface rage

Switch(config)#interface rage fas

Switch(config)#interface rage fasE

Switch(config)#interface range f

Switch(config)#interface range fastEthernet 0/1-3

Switch(config-if-range)#swit

Switch(config-if-range)#
%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

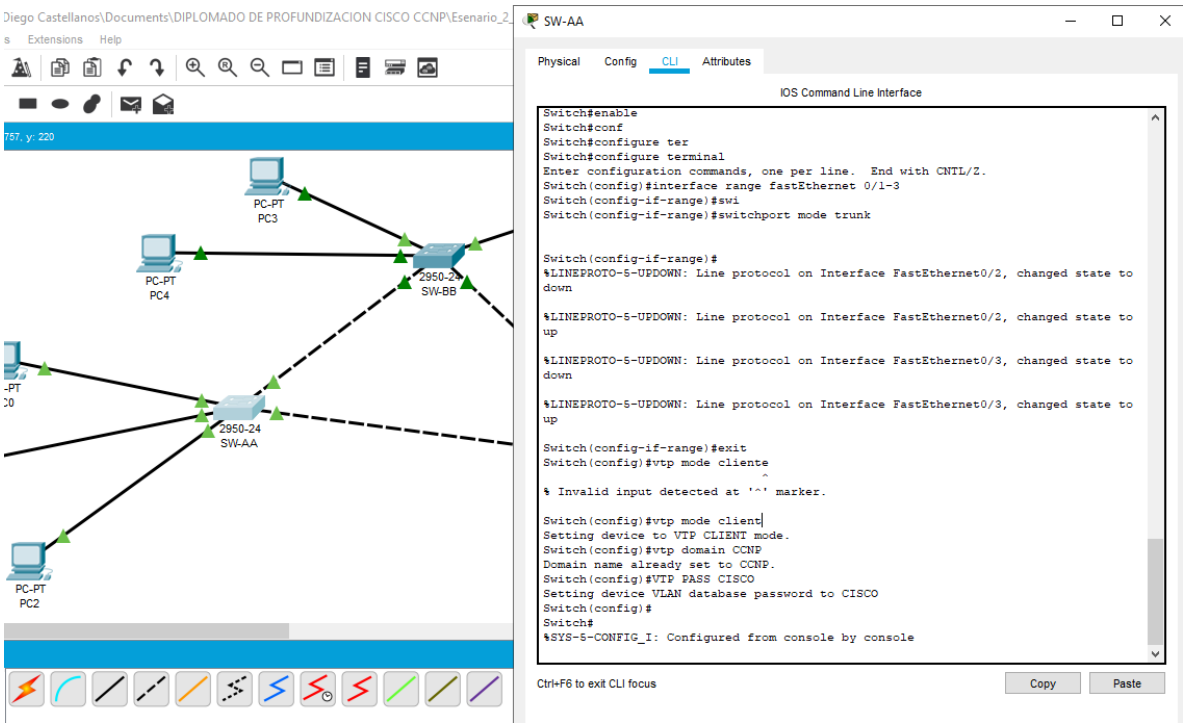
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Figura 18. Configuración switch SW-AA



El switch SW-AA se configuro como Los puertos que van del 0/1-3 los convertimos en modo troncal, Tambien su configuración VPT como dodo cliente llamado CCNP y usando la contraseña CISCO.

SS-AA

Switch#enable

Switch#conf

Switch#configure ter

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface range fastEthernet 0/1-3

Switch(config-if-range)#swi

Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if-range)#exit

Switch(config)#vtp mode cliente

Switch(config)#vtp mode client

Setting device to VTP CLIENT mode.

Switch(config)#vtp domain CCNP

Domain name already set to CCNP.

Switch(config)#VTP PASS CISCO

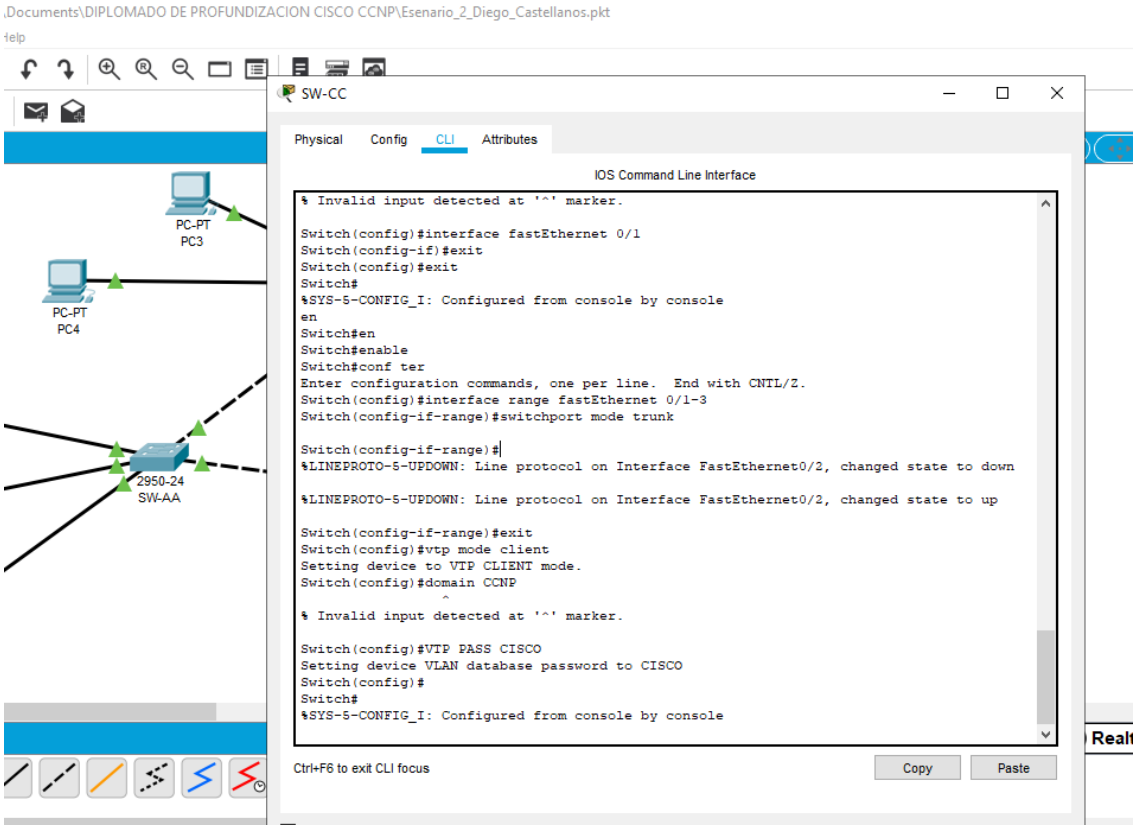
Setting device VLAN database password to CISCO

Switch(config)#

Switch#

%SYS-5-CONFIG_I: Configured from console by console

Figura 19. Configuración switch SW-CC



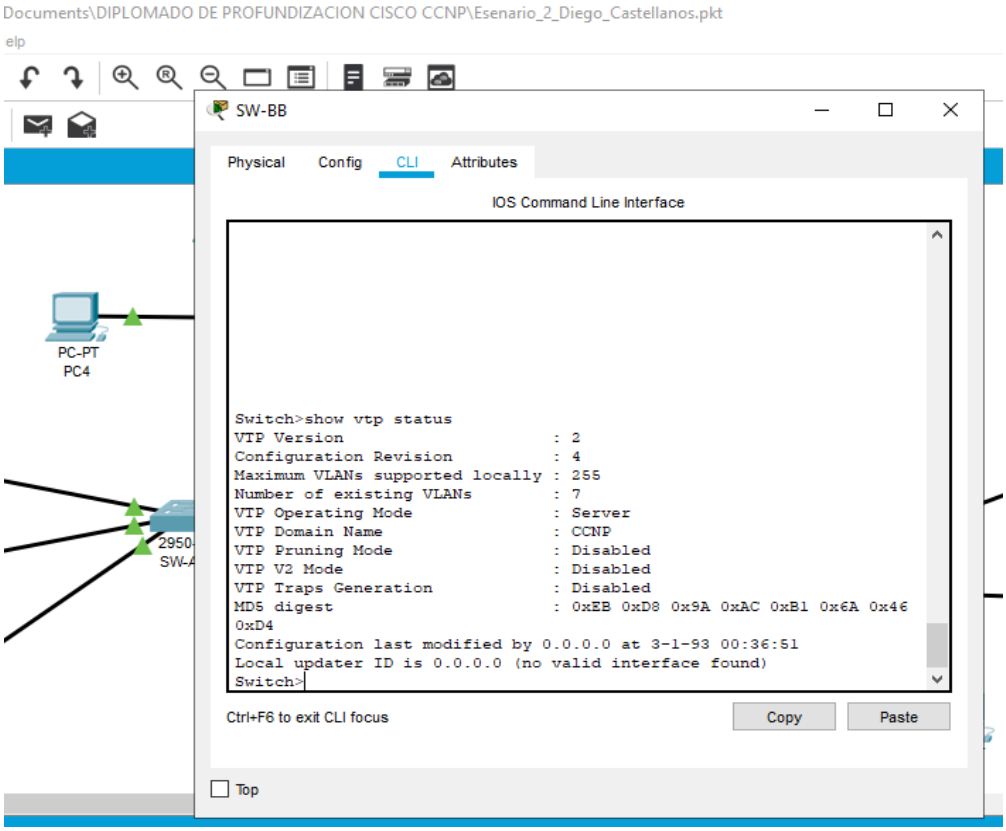
El switch SW-CC se configuro como Los puertos que van del 0/1-3 los convertimos en modo troncal, También su configuración VPT como dodo cliente llamado CCNP y usando la contraseña CISCO.

SS-CC

```
Switch#enable
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up

Switch(config-if-range)#exit
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#domain CCNP
Switch(config)#VTP PASS CISCO
Setting device VLAN database password to CISCO
Switch(config)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

2.2 Verifique las configuraciones mediante el comando show vtp status

Figura 20. Correcta configuración de SW-BB



SW-BB

Switch>show vtp status

VTP Version : 2

Configuration Revision : 4

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : CCNP

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

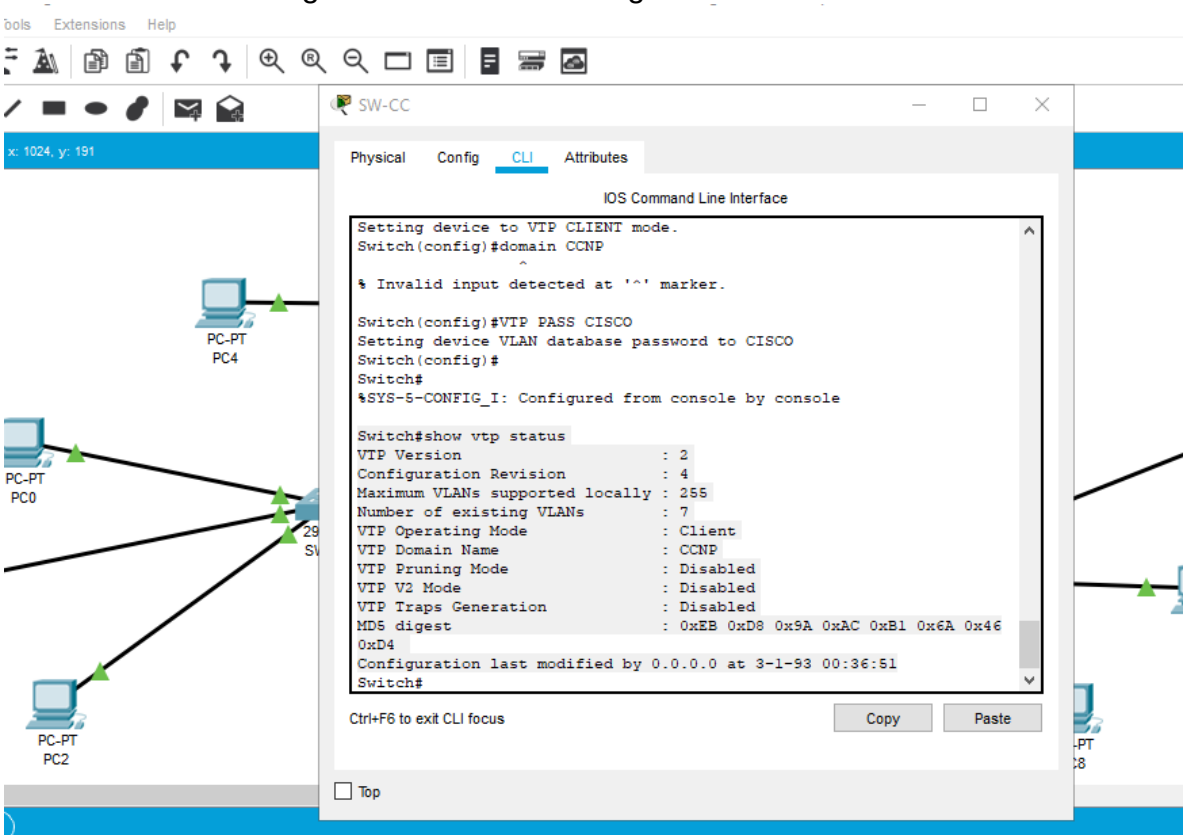
VTP Traps Generation : Disabled

MD5 digest : 0xEB 0xD8 0x9A 0xAC 0xB1 0x6A 0x46 0xD4

Configuration last modified by 0.0.0.0 at 3-1-93 00:36:51

Local updater ID is 0.0.0.0 (no valid interface found)

Figura 21. Correcta configuración de SW-CC



SW-CC

Switch#show vtp status

VTP Version : 2

Configuration Revision : 4

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

VTP Operating Mode : Client

VTP Domain Name : CCNP

VTP Pruning Mode : Disabled

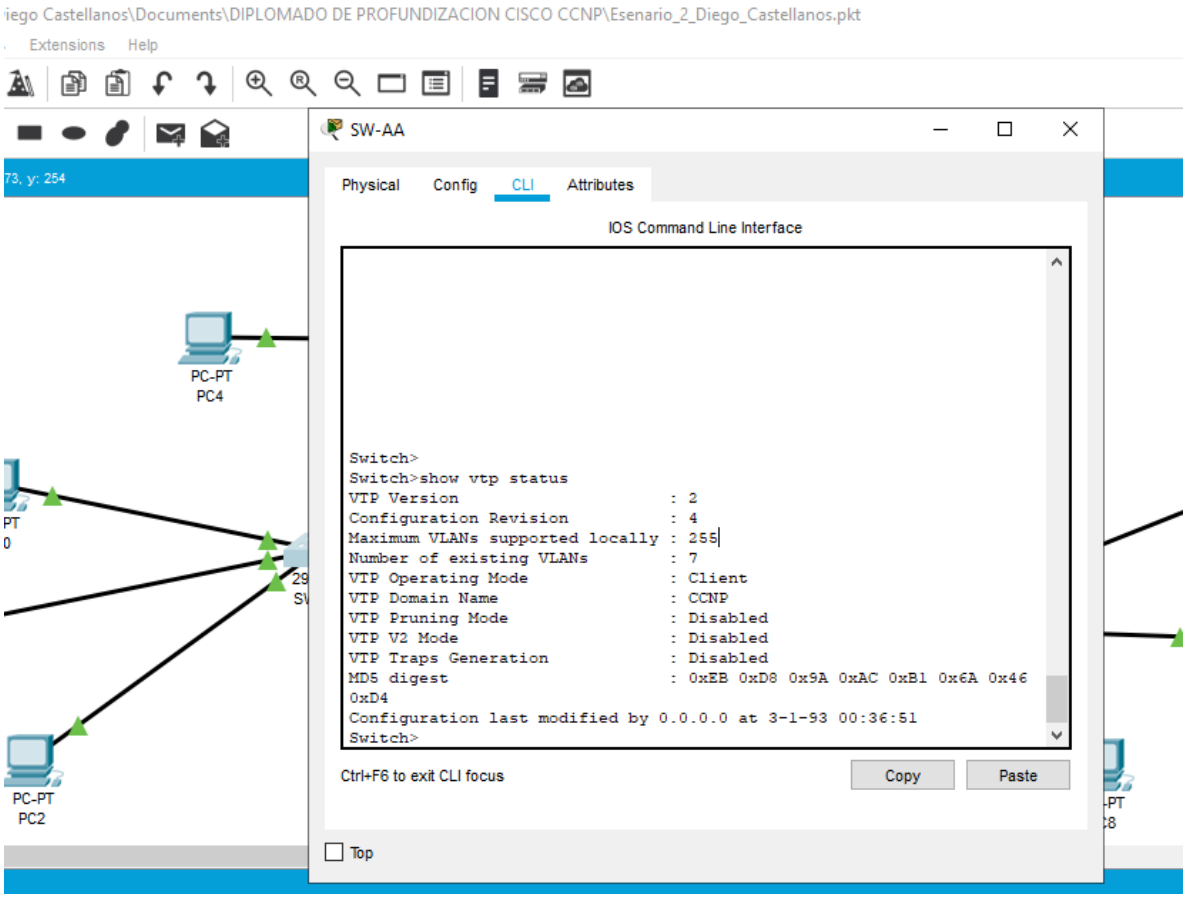
VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0xEB 0xD8 0x9A 0xAC 0xB1 0x6A 0x46 0xD4

Configuration last modified by 0.0.0.0 at 3-1-93 00:36:51

Figura 22. Correcta configuración de SW-AA



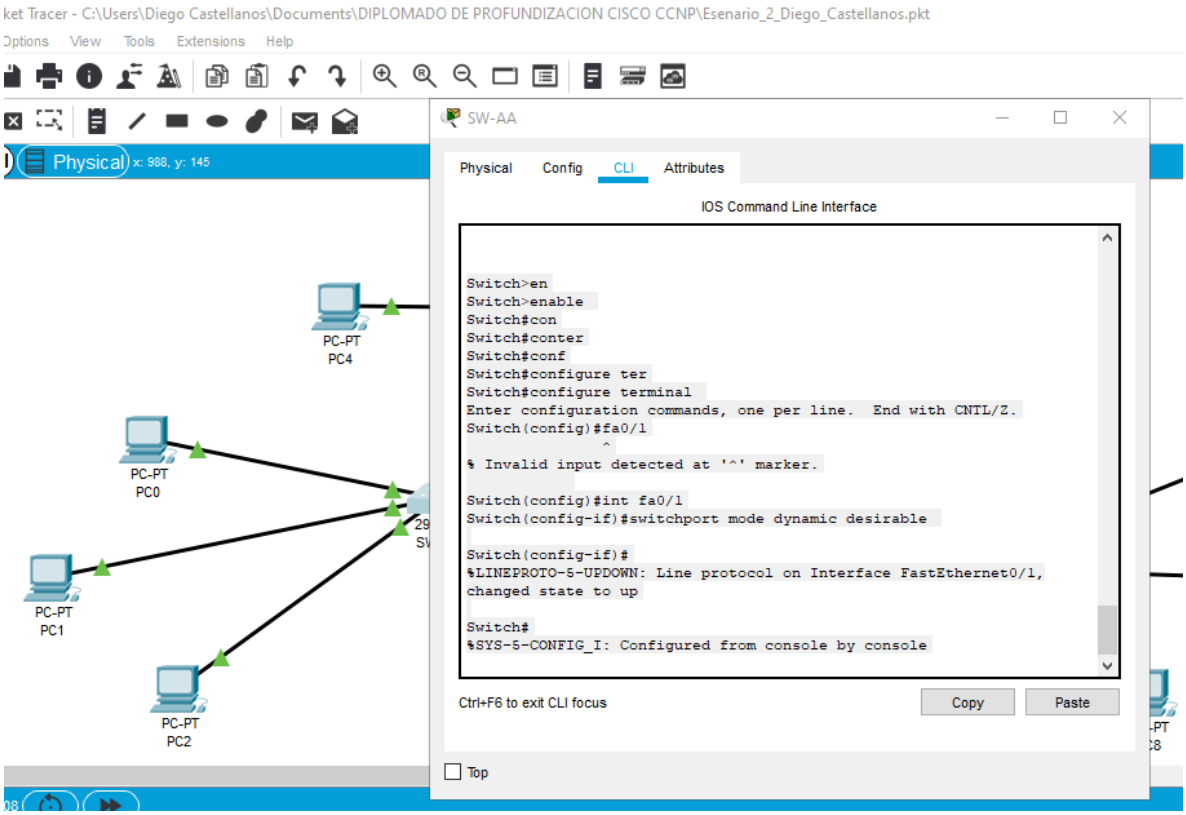
Switch>

```
Switch>show vtp status
VTP Version : 2
Configuration Revision : 4
Maximum VLANs supported locally : 255
Number of existing VLANs : 7
VTP Operating Mode : Client
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xEB 0xD8 0x9A 0xAC 0xB1 0x6A 0x46 0xD4
Configuration last modified by 0.0.0.0 at 3-1-93 00:36:51
Switch>
```

Configurar DTP (Dynamic Trunking Protocol)

2.4 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.

Figura 23. Configuración de DTP SW-AA



Con el comando show int fa0/3 switchport podemos ver que el enlace se encuentra en trunk y si no lo podemos cambiar con el comando switchport mode dynamic desirable

Switch>en

Switch>enable

Switch#con

Switch#conter

Switch#conf

Switch#configure ter

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#fa0/1

% Invalid input detected at '^' marker.

Switch(config)#int fa0/1

Switch(config-if)#switchport mode dynamic desirable

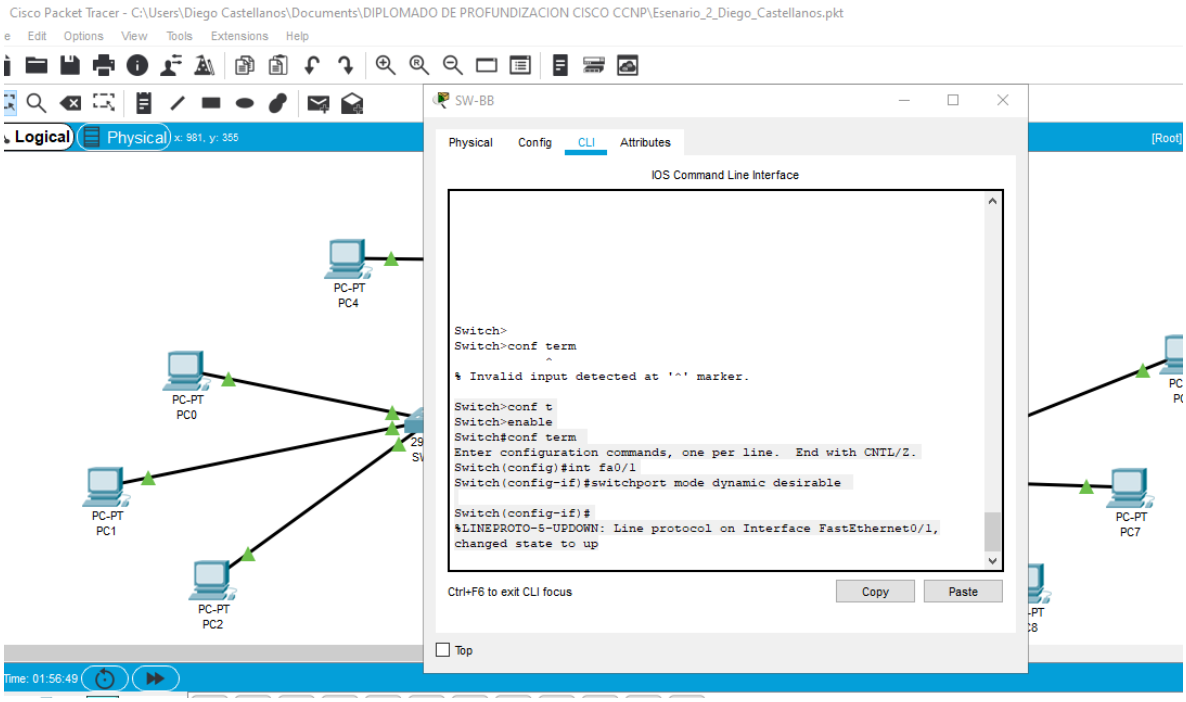
Switch(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch#

%SYS-5-CONFIG_I: Configured from console by console

Figura 24. Configuración de DTP SW-BB



Con el comando show int fa0/1 switchport podemos ver que el enlace se encuentra en trunk y si no lo podemos cambiar con el comando switchport mode

dynamic desirable

Switch>conf t

Switch>enable

Switch#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#int fa0/1

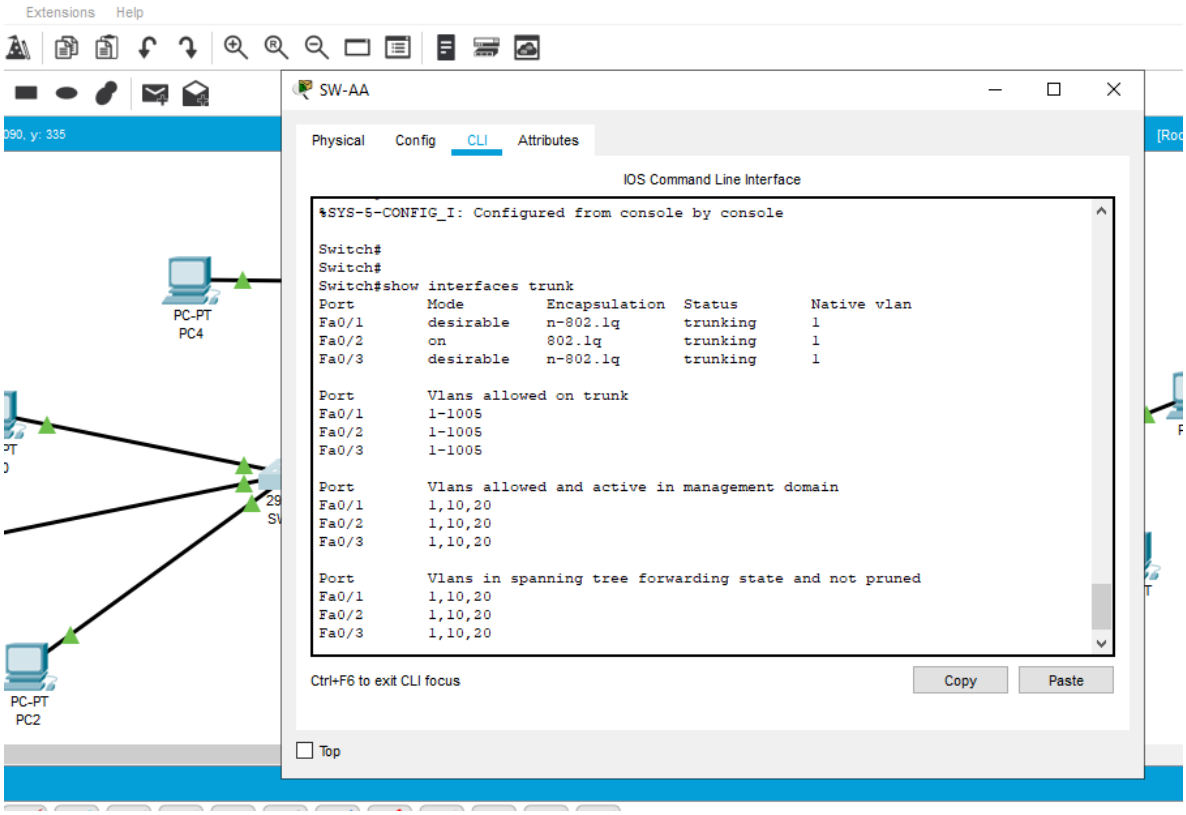
Switch(config-if)#switchport mode dynamic desirable

Switch(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

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

Figura 25. Verificación de trunk SW-AA



Switch#show interfaces trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 desirable n-802.1q trunking 1

Fa0/2 on 802.1q trunking 1

Fa0/3 desirable n-802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-1005

Fa0/2 1-1005

Fa0/3 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,10,20

Fa0/2 1,10,20

Fa0/3 1,10,20

Port Vlans in spanning tree forwarding state and not pruned

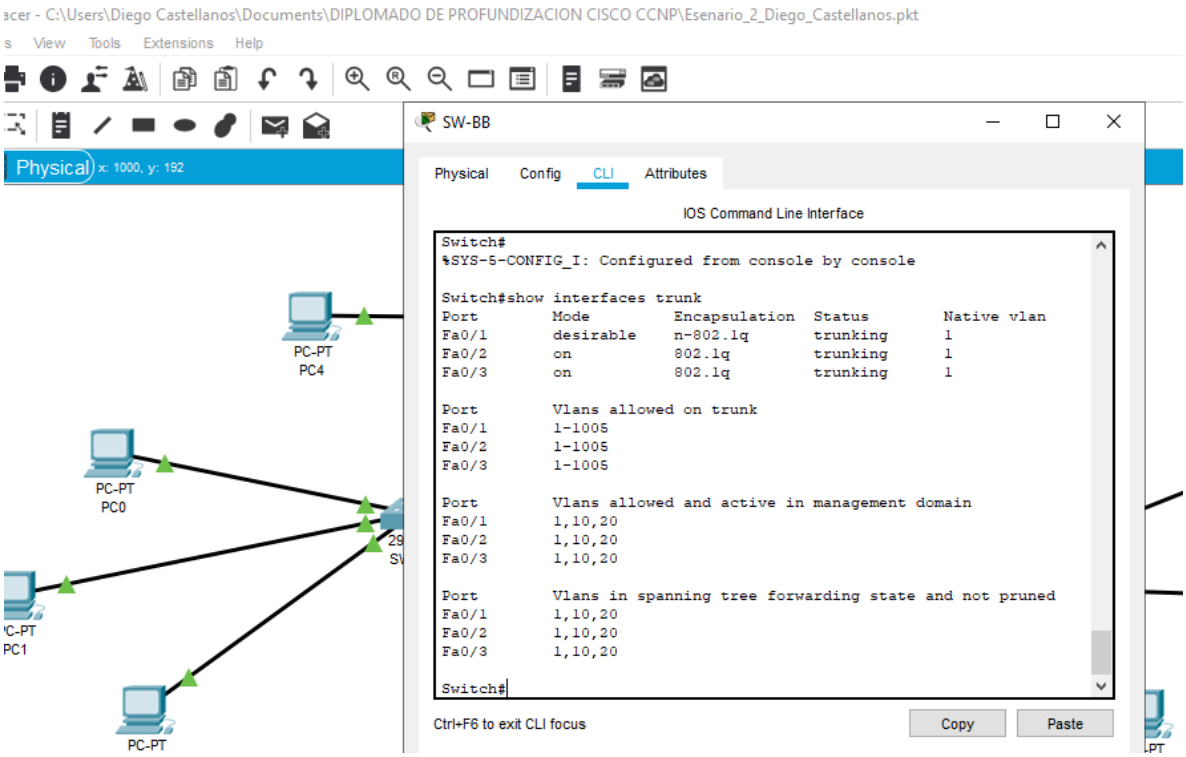
Fa0/1 1,10,20

Fa0/2 1,10,20

Fa0/3 1,10,20

Switch#

Figura 26. Verificación de trunk SW-BB



Switch#

%SYS-5-CONFIG_I: Configured from console by console

Switch#show interfaces trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 desirable n-802.1q trunking 1

Fa0/2 on 802.1q trunking 1

Fa0/3 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-1005

Fa0/2 1-1005

Fa0/3 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,10,20

Fa0/2 1,10,20

Fa0/3 1,10,20

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20

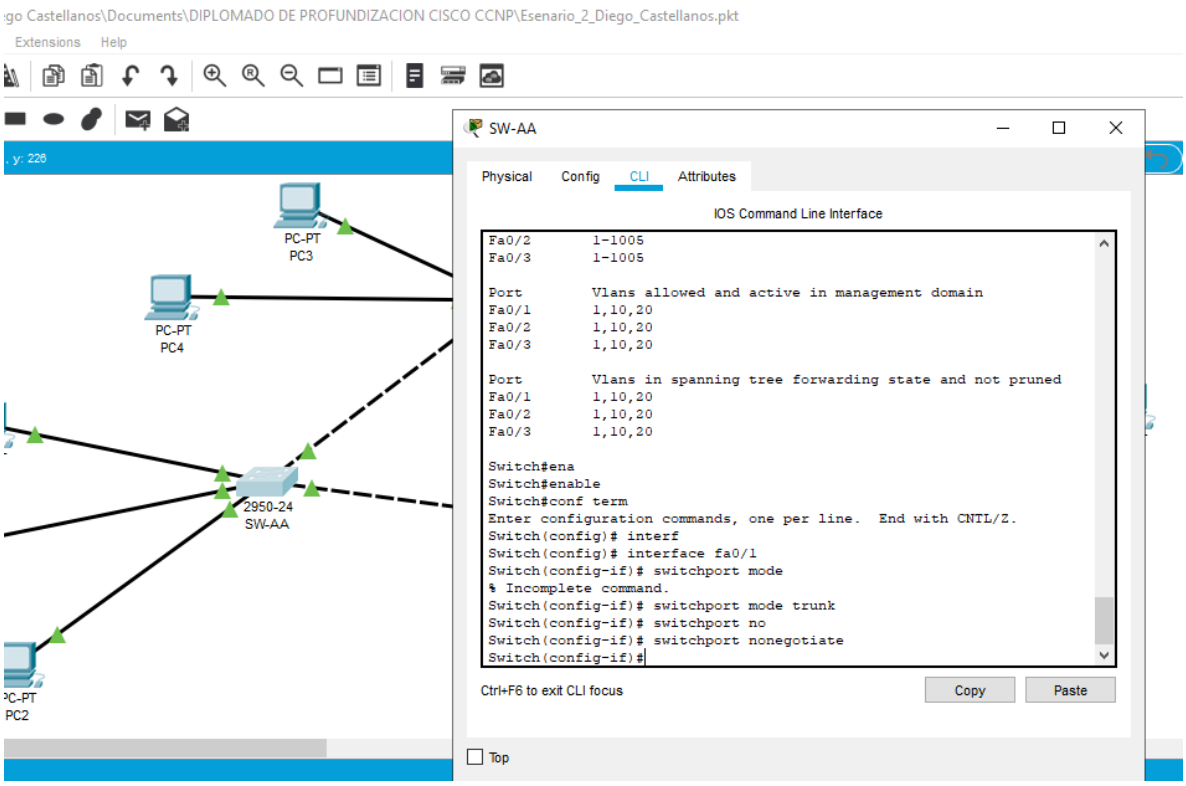
Fa0/2 1,10,20

Fa0/3 1,10,20

Switch#

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

Figura 27. Configuración de trunk SW-AA y SW-BB



Switch#ena

Switch#enable

Switch#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interf

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode

% Incomplete command.

Switch(config-if)# switchport mode trunk

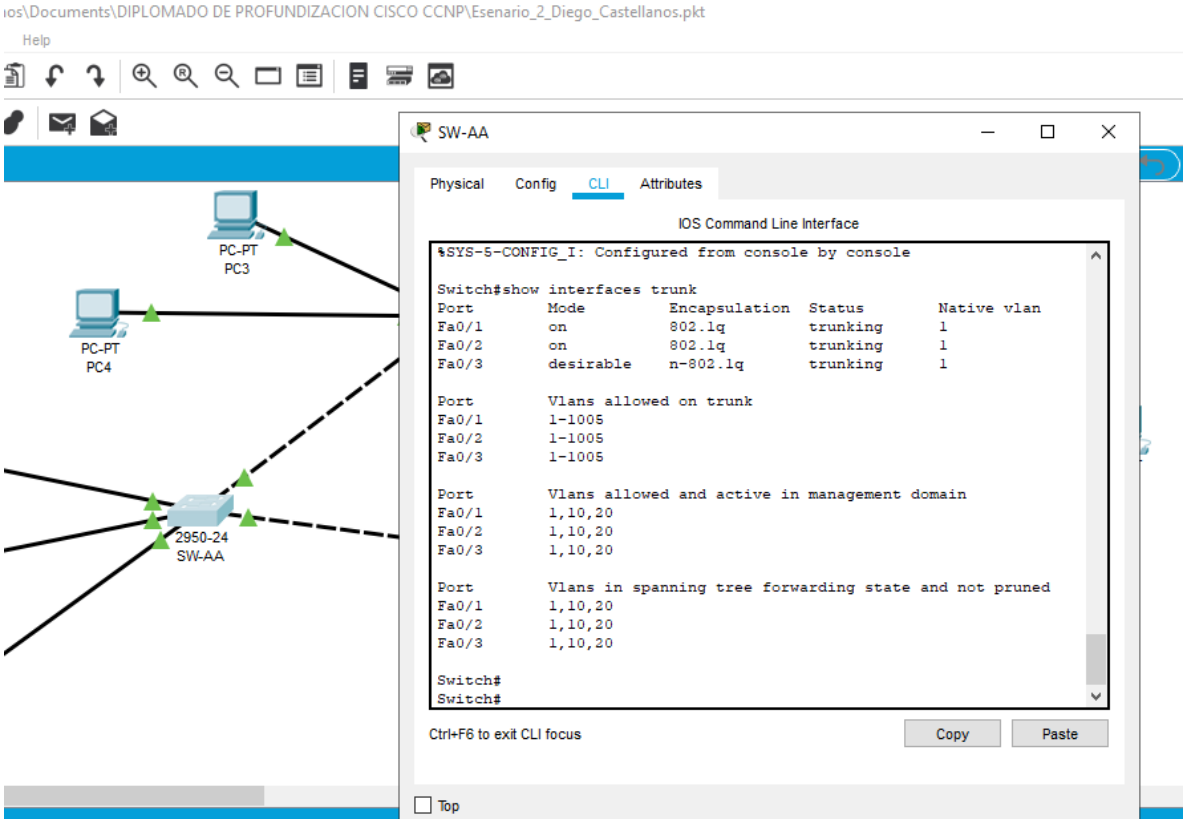
Switch(config-if)# switchport no

Switch(config-if)# switchport nonegotiate

Switch(config-if)#

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

Figura 28. Verifique el enlace trunk en SW-AA



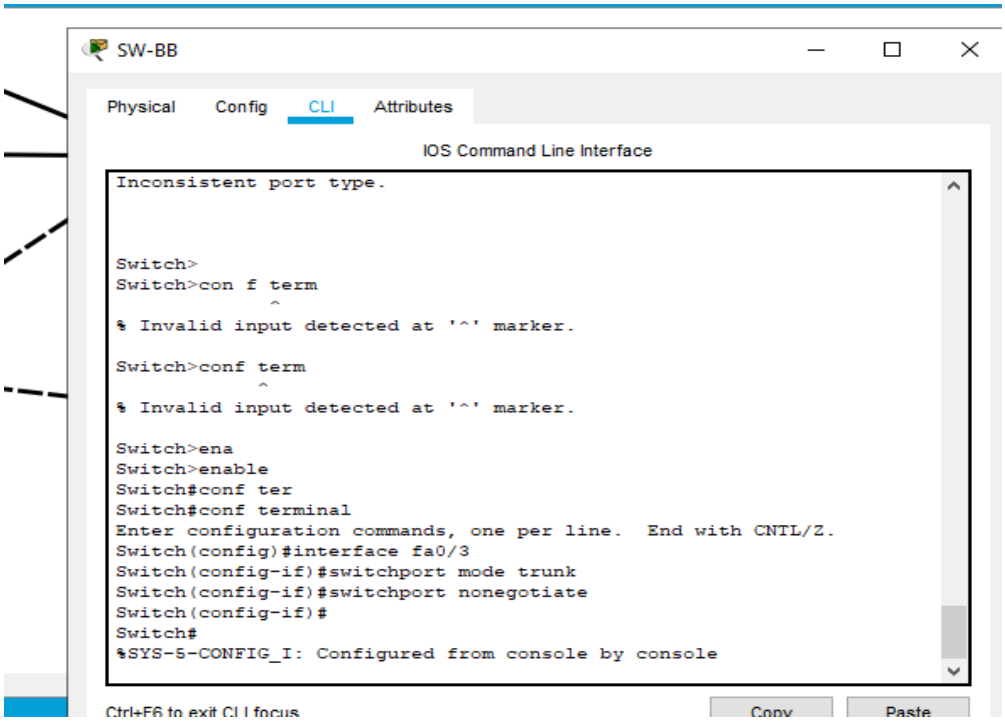
Switch#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1
Fa0/3 desirable n-802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005
Fa0/2 1-1005
Fa0/3 1-1005

Port Vlans allowed and active in management domain
Fa0/1 1,10,20
Fa0/2 1,10,20
Fa0/3 1,10,20

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20
Fa0/2 1,10,20
Fa0/3 1,10,20

Figura 29. Configuración de enlace trunk SW-BB y SW-CC



witch>ena

Switch>enable

Switch#conf ter

Switch#conf terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface fa0/3

Switch(config-if)#switchport mode trunk

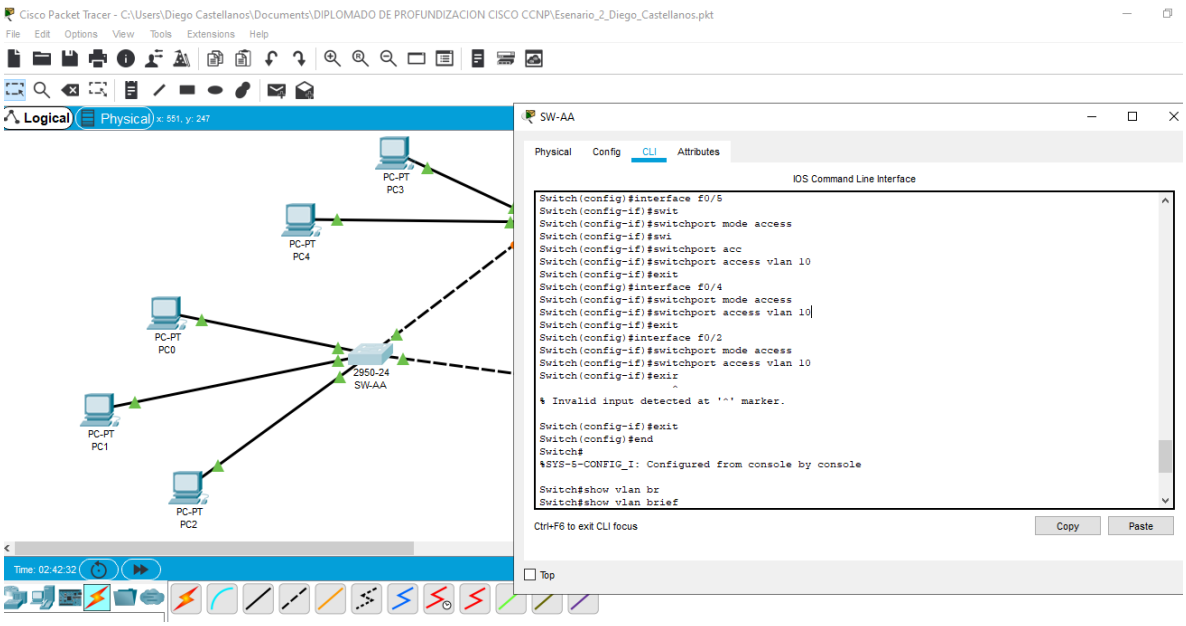
Switch(config-if)#switchport nonegotiate

Switch(config-if)#

Agregar VLANs y asignar puertos.

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

Figura 30. Configuración VLAN SW-AA Y SW-BB



SW-AA

Se asignara a cada puerto las VLAN correspondientes y se verificara han sido agregadas correctamente

```
Switch#ena
Switch#enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inte
Switch(config)#interface f0/5
Switch(config-if)#swit
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exir
% Invalid input detected at '^' marker.
Switch(config-if)#exit
Switch(config)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan br
Switch#show vlan brief
```

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active 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

10 AAA active Fa0/2, Fa0/4, Fa0/5

20 BBB active

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

Switch#

SW-BB

Switch>ena

Switch>enable

Switch#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface f0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

Switch(config)#interface f0/4

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 25

Switch(config-if)#switchport access vlan 25

Switch(config-if)#exit

Switch(config)#interface f0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 30

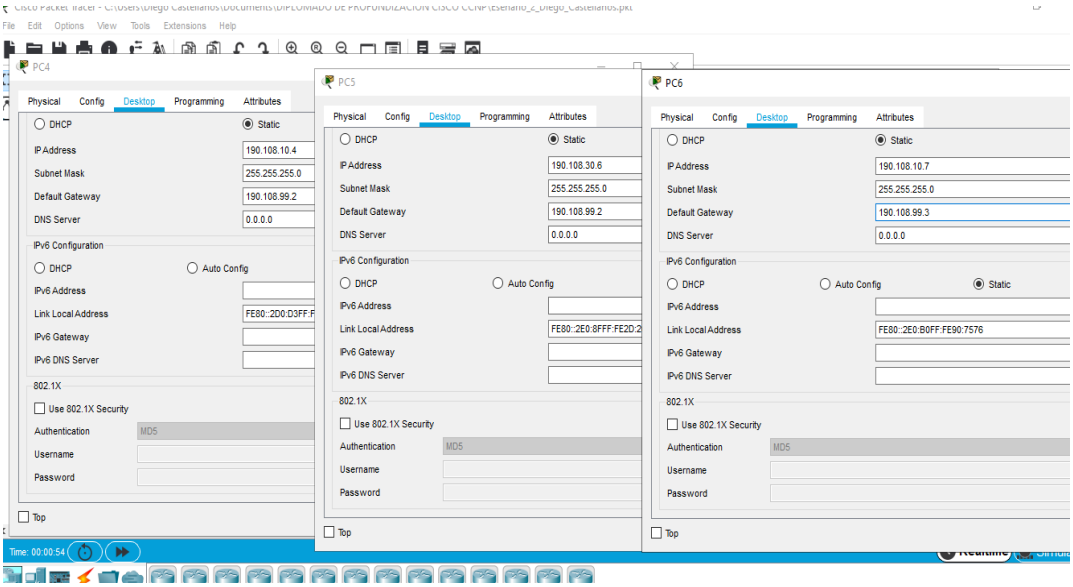
%SYS-5-CONFIG_I: Configured from console by console

2.7 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

Se configuraron los puertos de cada VLAN con su IP respectiva

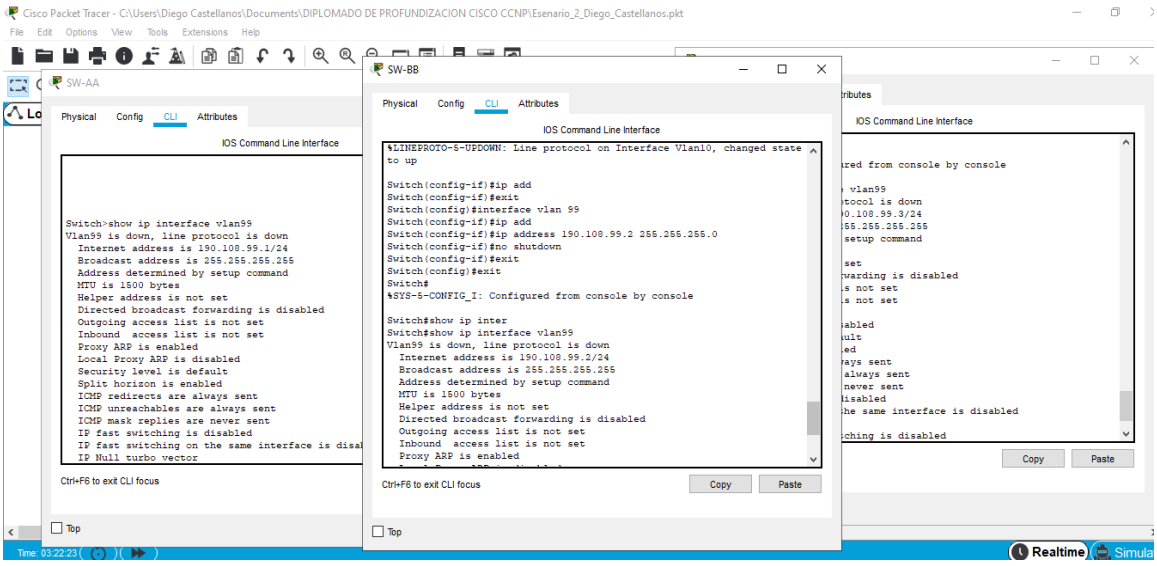
Figura 31. Configuración VLAN SW-AA Y SW-BB



Configurar las direcciones IP en los Switches.

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

Figura 32. Configuración direcciones IP en los Switches.



Reconfiguro cada una de los Switch SW-AA, SW-BB y SW-CC en la VLAN 99 con su dirección IP y su máscara.

Switch SW-AA

Switch#ena

Switch#enable

Switch#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#inter

Switch(config)#interface vlan99

```
Switch(config-if)#ip add
Switch(config-if)#ip address 190.108.99.1 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#
Switch#
Switch>show ip interface vlan99
Vlan99 is down, line protocol is down
Internet address is 190.108.99.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Null turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are None
 --More--
```

Switch SW-BB

witch(config-if)#exit
Switch(config)#interface vlan 99
Switch(config-if)#ip add
Switch(config-if)#ip address 190.108.99.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip inter
Switch#show ip interface vlan99
Vlan99 is down, line protocol is down
Internet address is 190.108.99.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent

ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Null turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are None
--More--

Switch SW-BB

Switch>ena
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#190.108.99.3
^
% Invalid input detected at '^' marker.
Switch(config-if)#ip add
Switch(config-if)#ip address 190.108.99.3 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exi
Switch#
%SYS-5-CONFIG_I: Configured from console by console

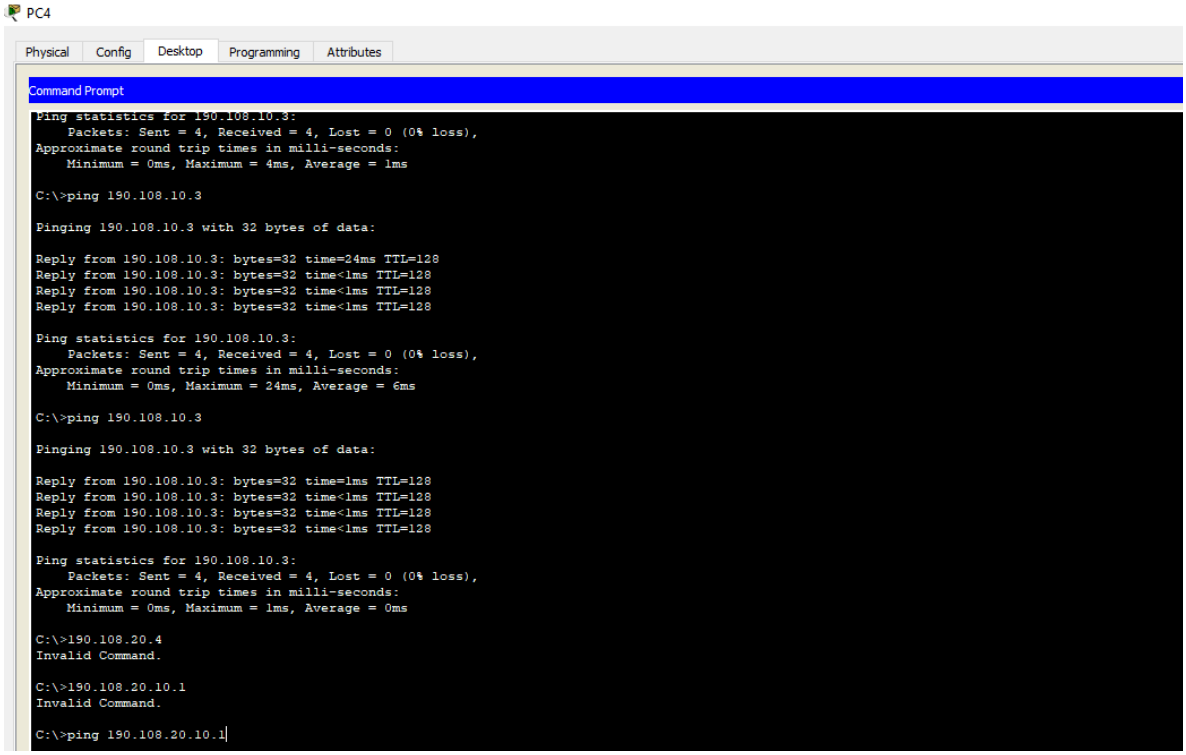
Switch#show ip interface vlan99
Vlan99 is down, line protocol is down

Internet address is 190.108.99.3/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Null turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are None

2.6. Verificar la conectividad Extremo a Extremo

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

Figura 33. Ping



Se pueden hacer los pings sin ningún tipo de problema, pero en caso de tener unos pc en VLAN 10 y otros en la VLAN20, los intervalos se pueden comunicar en capa 3, pero si la VLAN20 tiene un PC y la VLAN15 Estos Equipos Pueden Estar Direccionados De Manera Diferente y si se realiza el ping desde otro puede llegar sin ningún problema por que usaría ACLs para poder comprobar su funcionamiento.

CONCLUSIONES

El tipo de configuración que se utilizó para cada uno de los escenarios o topologías se logró ejecutar con éxito en cada uno de los Routers, Switch y PC con cierto tipo de conexiones en serie, dando un paso a paso en cada uno de los escenarios plantados y se logró dar una simulación perfecta.

Se empleó en el escenario uno el software GNS3 y se establecieron una conexión entre los cuatro Routers, por medio de la configuración AS1, AS2, y AS3 donde anunciabas las conexiones del Loopback en BGP. Con el comando show ip route, se verifico la información utilizada en los enrutamiento. Se elaboró un paso a paso del escenario plantado.

Se logró ejecutar el escenario dos con el uso del software Packet Tracer, se creó un protocolo de enrutamiento para los switches y computadores de escritorio. Se logra verificar la configuración VTP y la actualización de las VLAN en los switch, como y computadores de escritorio. Por medio de un ping entre los PC y los Switch se debe comprobó su conexión.

BIBLIOGRÁFIA

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

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

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