DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YENNY YOHANNA BLANCO ARIAS

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YENNY YOHANNA BLANCO ARIAS

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
TOCANCIPA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

TOCANCIPA, 22 de mayo de 2020

AGRADECIMIENTOS

Le agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Le doy gracias a mis padres Víctor y Gloria por apoyarme en todo momento, por los valores que me han inculcado, y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida. Sobre todo, por ser un excelente ejemplo de vida a seguir.

A mi esposo Mauricio por no dejarme caer y dejar mis estudios, siempre animándome y apoyándome a pesar de todas las falencias que tuve en el tiempo de mi carrera, a mi hijo Joseph por ser mi fuerza sin ti no hubiese salido adelante, para ti siempre quiero el mejor ejemplo.

Debo agradecer de manera especial y sincera a la universidad UNAD por brindarme la oportunidad de culminar mis estudios a mis tutores que con gran paciencia y apoyo me han brindado en el transcurso de la carrera especialmente al ingeniero Manuel Wagner por ser una persona que me ha escuchado y me ha orientado en la culminación de mis estudios.

Quiero expresar también al ingeniero Efraín Pérez y Gerardo Granados por acompañarnos en nuestra etapa final de nuestra carrera les deseo mil bendiciones en lo que hacen sin ustedes esto no sería posible, lograr un sueño cuando se llegó a ver muy lejano.

CONTENIDO

AGRADECIMIENTOS 4
CONTENIDO 5
LISTA DE TABLAS 6
LISTA DE FIGURAS 7
GLOSARIO 9
RESUMEN 10
ABSTRACT 10
INTRODUCCIÓN 11
DESARROLLO 12
Escenario 1 12
Escenario 2 22
CONCLUSIONES 44
BIBLIOGRAFIA 45

LISTA DE TABLAS

Tabla 1 Enrutamiento Router 1 13

Tabla 2 Enrutamiento Router 2 13

Tabla 3 Enrutamiento Router 3 13

Tabla 4 Enrutamiento Router 4 13

Tabla 5 Enrutamiento PC 31

Tabla 6 Enrutamiento PC según Vlan 33

Tabla 7 Enrutamiento Switches 37

LISTA DE FIGURAS

Figura 1 Toplogía escenario. 12
Figura 2 Topología escenario gns3 12
Figura 3 Configuración router 1 BGP 15
Figura 4 Configuración router 2 BGP 16
Figura 5 configuración router 2 bgp con rutas BGP router 3 18
Figura 6 Configuración router 3 18
Figura 7 configuración router 3 bgp con rutas hacia router 4 21
Figura 8 Configuración router 4 22
Figura 9 Escenario 2 22
Figura 10 Topología Packet Tracer 23
Figura 11 Show vpt status swhith SW-AA 24
Figura 12 Show vpt status switch SW-BB 25
Figura 13 Show vpt status switch SW-CC 25
Figura 14 Show interface trunk F0/1 SW-AA 26
Figura 15 Show interface trunk F 0/1 SW-BB 27
Figura 16 Show interface trunk F 0/3 SW-AA 27
Figura 17 Validación modo trunk SW-BB 28
Figura 18 Validación modo trunk SW-CC 28
Figura 19 Validación Creación de Vlans en SW-BB 30
Figura 20 Validación Creación de Vlans en SW-AA 30
Figura 21 Validación Creación de Vlans en SW-CC 31
Figura 22 Validación direccionamiento PC1 33
Figura 23 Validación direccionamiento PC2 33
Figura 24 Validación direccionamiento PC3 34
Figura 25 Validación direccionamiento PC4 34
Figura 26 Validación direccionamiento PC5 35
Figura 27 Validación direccionamiento PC6 35
Figura 28 Validación direccionamiento PC7 36

Figura 29 Validación direccionamiento PC7 36
Figura 30 Validación direccionamiento PC9 36
Figura 31 Validación ping PC1 a Pc 6 y Pc2 a Pc5 38
Figura 32 Validación ping Pc3 a Pc4 y Pc4 a Pc7 39
Figura 33 Validación ping Pc3 a Pc4 y Pc4 a Pc7 40
Figura 34 Validación ping Pc1 a Pc8 y Pc9 a Pc2 40
Figura 35 Validación ping SW-AA a SW-BB y SW-CC 41
Figura 36 Validación ping SW-BB a SW-AA y SW-CC 41
Figura 37 Validación ping SW-CC a SW-AA y SW-BB 42
Figura 38 Validación ping SW-AA a Pc 1-Pc2 y Pc3.....42
Figura 39 Validación ping SW-BB a Pc 1-Pc2 y Pc3.....43
Figura 40 Validación ping SW-CC a Pc7-Pc8 y Pc9 43

GLOSARIO

BGP: Es un protocolo de puerta de enlace de frontera o BGP mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Este intercambio de información de encaminamiento se hace entre los router externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

Vlan: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local

VLAN switch: Se conoce como Virtual LAN o VLAN a una división de carácter lógico del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. Se trata, por tanto, de una agrupación de un conjunto de dispositivos que pueden mantener comunicación entre sí.

Dirección IP: Dirección de protocolo de Internet, la forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un aparato de teléfono en una red telefónica. La dirección IP consta de cuatro números separados por puntos, en que cada número es menor de 256; por ejemplo 64.58.76.178. Dicho Número IP es asignado de manera permanente o temporal a cada equipo conectado a la red.

RESUMEN

Este trabajo consiste en el proceso de conceptualización de los diversos temas del área de networking y seguridad los cuales se apreciaron durante el semestre educativo, a su vez la aplicación práctica de los mismos sobre diversos esquemas topológicos de red para los módulos de CCNP ROUTE y CCNP SWITCH en ambientes de simulación lógica.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos escenarios, el estudiante deberá realizar el proceso de configuración de un escenario en el Laboratorio SmartLab y el otro mediante el uso de herramientas de Simulación (Puede ser Packet Tracer o GNS3). El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario.

PALABRAS CLAVE: Redes, CCNP, Enrutamiento, electrónica, Cisco.

ABSTRACT

This work consists of the conceptualization process of the various topics in the area of networks and security which will be appreciated during the educational semester, at the same time the practical application of the same on various network topological schemes for the CCNP ROUTE and CCNP SWITCH in logical simulation environments.

Taking into account that the Skills Test is made up of two scenarios, the student must carry out the process of setting up one scenario in the SmartLab Laboratory and the other through the use of Simulation tools (It can be Packet Tracer or GNS3). The student is free to choose under which technological mediation each scenario will solve.

INTRODUCCIÓN

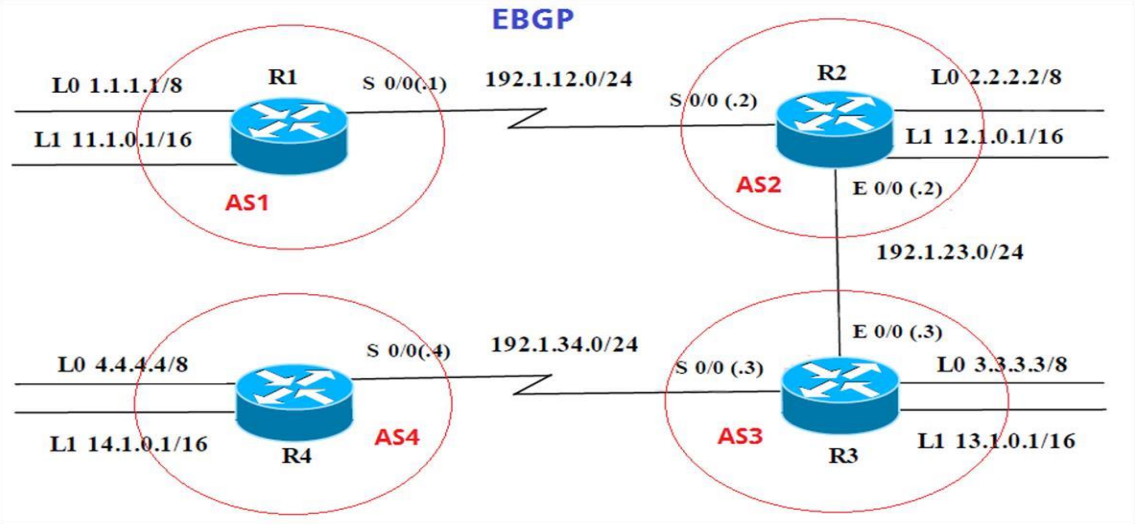
El Diplomado de Profundización CISCO CCNP, posee un plan de estudios que se concentran en el desarrollo de las habilidades necesarias para que el estudiante implemente redes escalables, construya redes que abarquen un campus, diseñe e instale intranets globales, así como la detección y solución de problemas.

El curso de profundización está constituido por dos módulos: CCNP ROUTE R&S V7 y CCNP SWITCH R&S V7), los cuales forman parte del currículo CCNP R&S adscrito a la Academia CISCO.

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas la cual consistirá en n brindar solución a dos escenarios de configuraciones correspondientes al diplomado de CCNP las cuales se desarrollarán en el programa de simulación packet tracer. dentro de este trabajo se verán imágenes con los protocolos empleados para la configuración de cada uno de los requerimientos con respecto al escenario.

DESARROLLO

Escenario 1



1 To

Figura 1 Topología escenario.

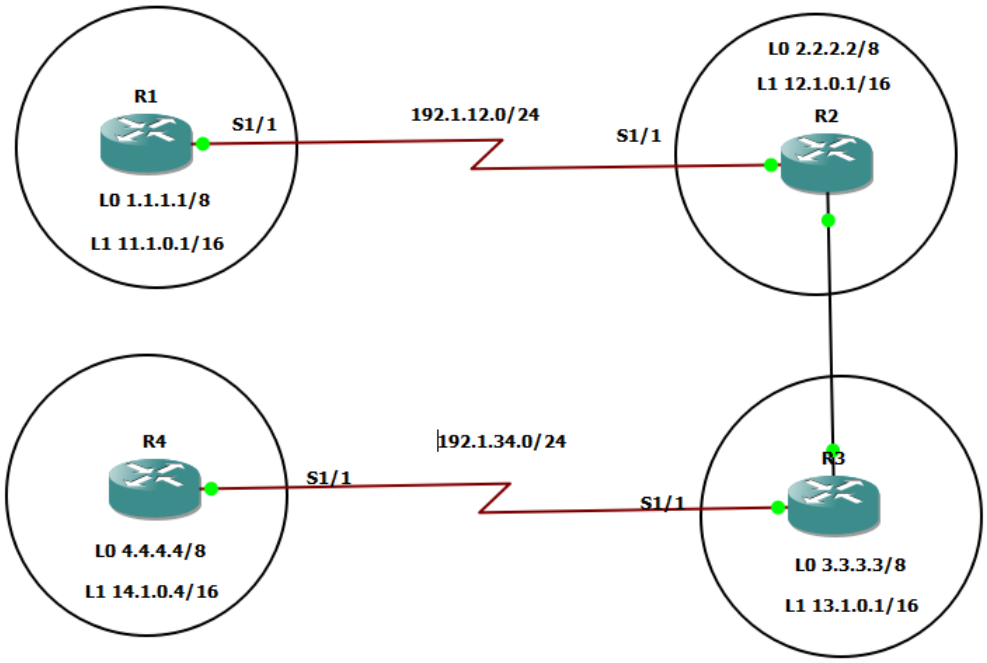


Figura 2 Topología escenario gns3

Información para la configuración de los Routers

R1

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

Tabla 1 Enrutamiento Router 1

R2

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

Tabla 2 Enrutamiento Router 2

R3

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

Tabla 3 Enrutamiento Router 3

R4

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

Tabla 4 Enrutamiento Router 4

R1(config-if)# ip address 1.1.1.1 255.0.0.0 Configuración Router 1 y Router2

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

Router#configure terminal
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# exit
R1(config)# interface Loopback 1
R1(config-if) # ip address 11.1.0.1 255.255.0.0
R1(config-if) # exit
R1(config)# interface Serial 1/1
R1(config-if)# description AS1 -> AS2
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if) # clock rate 128000
R1(config-if) # no shutdown
R1(config-if) # exit
R1(config)# router bgp 1
R1(config-router) #bgp router-id 22.22.22.22
R1(config-router) # network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router) # network 192.1.12.0 mask 255.255.255.0
R1(config-router) # neighbor 192.1.12.2 remote-as 2

R2

R2#configure terminal
R2(config)# interface Loopback 0
R2(config-if) # ip address 2.2.2.2 255.0.0.0
R2(config-if) # exit
R2(config)# interface Loopback 1
R2(config-if) # ip address 12.1.0.1 255.255.0.0
R2(config-if) # exit
R2(config)# interface Serial 1/1
R2(config-if)# description AS2 -> AS1
R2(config-if) # ip address 192.1.12.2 255.255.255.0
R2(config-if) # clock rate 128000

R2(config-if) # no shutdown
R2(config-if) # exit
R2(config)# interface fastethernet 0/0
R2(config-if)# description AS2 -> AS3
R2(config-if) # ip address 192.1.23.2 255.255.255.0
R2(config-if) # no shutdow
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

A continuación, se presenta el resultado obtenido del comando ***show ip route***, donde el router R1 y R2 contienen en su tabla de enrutamiento las direcciones Loopback y las direcciones de las redes a las cuales se encuentran conectados de forma directa, también vemos las redes configuradas en las interfaces Loopback de su respectivo router vecino. Estas redes se pueden identificar mediante el código **B** que las precede, estas redes son aprendidas a través del protocolo BGP, otro dato que se evidencia en esta tabla de enrutamiento de cada router es donde reconoce como vía para alcanzar esta ruta es la red 192.1.12.0/24 conectada a través de la interfaz serial 1/1, donde este es el enlace físico que conecta a estos dos router.

Router 1

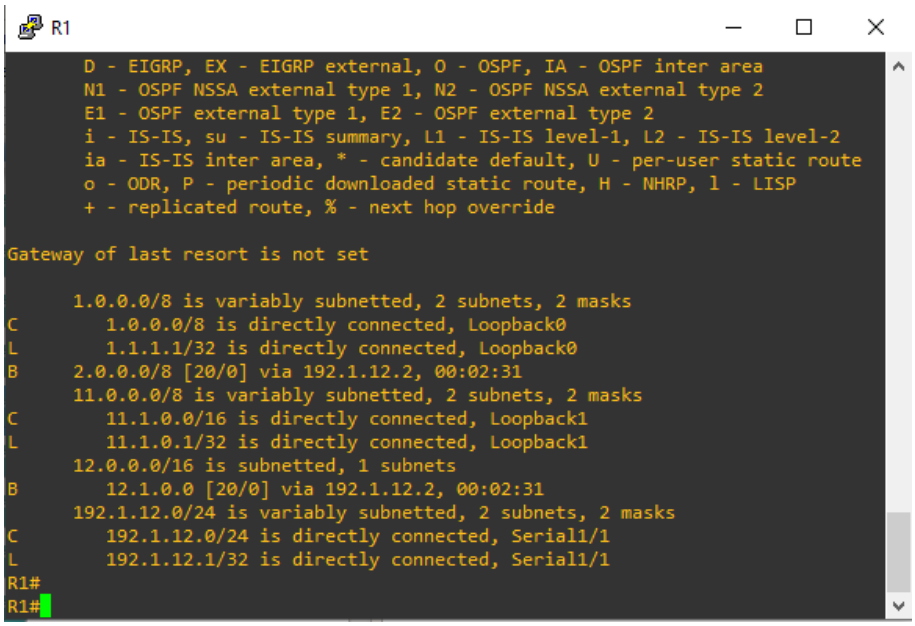


Figura 3 Configuración router 1 BGP

Router 2

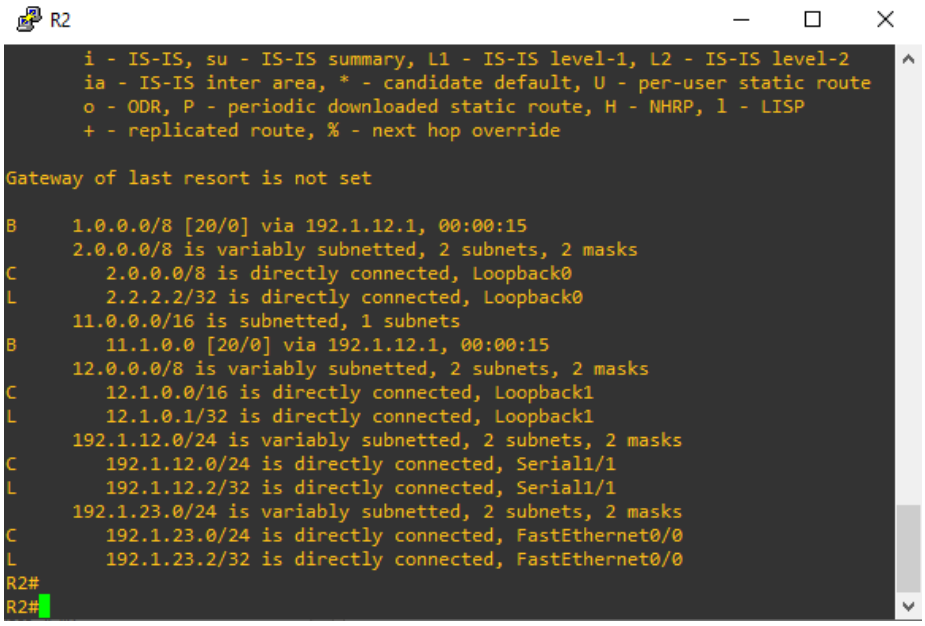


Figura 4 Configuración router 2 BGP

Configuración Router 2 a Router 3

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

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

R2(config-router)#exit

R2(config)#exit

R3

```
R3# configure terminal
R3(config)# interface Loopback 0
R3(config-if) # ip address 3.3.3.3 255.0.0.0
R3(config-if) # exit
R3(config)# interface Loopback 1
R3(config-if) # ip address 13.1.0.1 255.255.0.0
R3(config-if) # exit
R3(config)# interface fastethernet 0/0
R3(config-if)# description AS3 -> AS2
R3(config-if) # ip address 192.1.23.3 255.255.255.0
R3(config-if) # no shutdown
R3(config-if) # exit
R3(config)# interface Serial 1/1
R3(config-if)# description AS3 -> AS4
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
```

Realizada la configuración del R3 y la configuración de BGP en la R2 se puede evidenciar el resultado se obtiene con el comando Show ip route, donde el Router R2 se ha actualizado la tabla de enrutamiento y ahora vemos que tiene las direcciones de Loopback configuradas del router R3, por lo tanto, este dispositivo ha aprendido hasta este momento 4 rutas a través del protocolo BGP donde las cuales identifica se identifican con el código B.

El R3 contiene en su tabla de enrutamiento las redes que reconoce conectadas directamente, las interfaces Lookback y las redes que lo comunican con los routers R3 y R4 mediante las interfaces FasEthernet 0/0 y Serial 1/1 respectivamente, además este router (R3) se ha actualizado en su tabla de enrutamiento las direcciones de red correspondientes a las interfaces Lookback que se configuraron en R2 y R1, estas rutas las aprendió mediante el protocolo BGP estableciendo la relación adyacente con R2 y a que dichas redes se anunciaron en cada uno de los routers, en R3 también contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP con se evidencia en el código B el cual precede a la ip en la tabla de enrutamiento.

Se evidencia que R3 tiene alcance a todas las redes a través de la interfaz FasEthernet 0/0.

Router 2

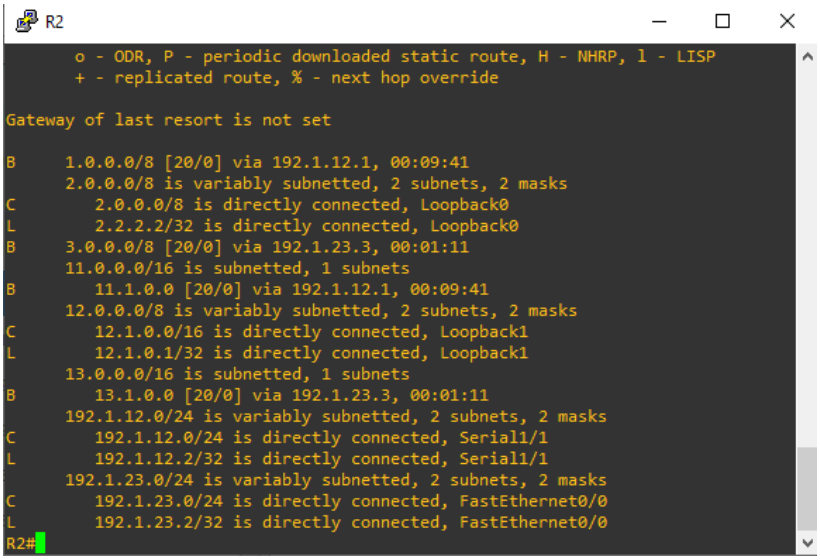


Figura 5 configuración router 2 bgp con rutas BGP router 3

Router 3

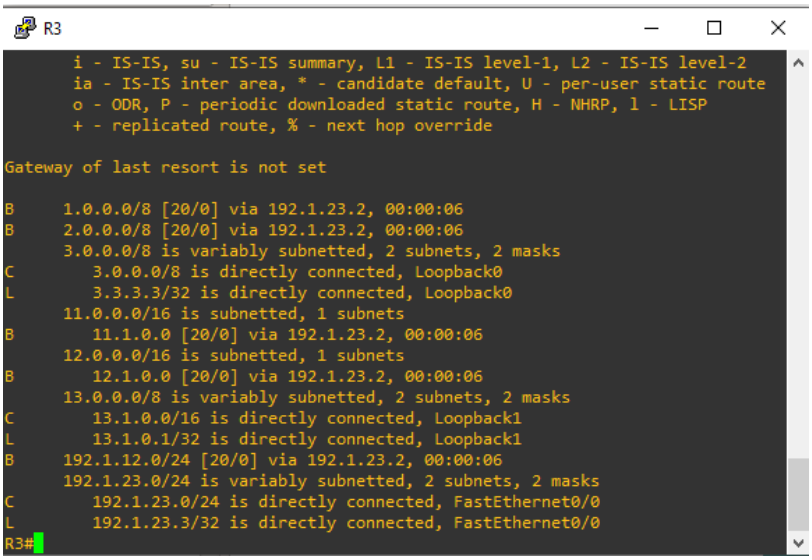


Figura 6 Configuración router 3

Configuración Router 3 a Router 4

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

R3

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

R3(config-router) #exit

R3(config)#exit

R4

R4#configure terminal

R4(config)# interface Loopback 0

R4(config-if) # ip address 4.4.4.4 255.0.0.0

R4(config-if) # exit

R4(config)# interface Loopback 1

R4(config-if) # ip address 14.1.0.1 255.255.0.0

R4(config-if) # exit

R4(config)# interface Serial 1/1

R4(config-if)# description AS4 -> AS3

R4(config-if) # ip address 192.1.34.4 255.255.255.0

R4(config-if) # no shutdown

R4(config-if) # exit

R4(config)# router bgp 4

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

R4(config-router) # network 4.0.0.0 mask 255.0.0.0

R4(config-router) # network 14.1.0.0 mask 255.255.0.0

R4(config-router) # network 192.1.34.0 mask 255.255.255.0

R4(config-router) # neighbor 192.1.34.3 remote-as 3

R4(config-router) #exit

R4(config)#exit

Para establecer la relación de adyacentes utilizando las direcciones Loopback, del router vecino se necesita informar sobre el uso de cada una de estas interfaces en lugar de la interfaz física por tal razón se requiere una configuración adicional para establecer los vecinos esta configuración se realizar en R3 y R4.

R3

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
R3(config-router) #exit
R3(config)#exit

R4

R4#configure terminal
R4(config)# ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router) # no neighbor 192.1.34.3
R4(config-router) # neighbor 3.3.3.3 remote-as 3
R4(config-router) # neighbor 3.3.3.3 update-source Loopback 0
R4(config-router) # neighbor 3.3.3.3 ebgp-multihop
R4(config-router) #exit
R4(config)#exit

Se presenta a continuación el resultado del comando Show ip route, donde el R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este dispositivo con R4 ha cambiado tomando la dirección de Lookback 0, la cual aparece como dirección estática, dado que así se estableció en la configuración que se realizó anteriormente, vemos que pese a que se usa la dirección lógica de la interface Loopback 0 para establecer la adyacencia, la via de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 1/1. También se puede identificar que la dirección de red de la interfaz Loopback 1 esta sigue aprendiendo mediante el protocolo BGP, pero no se alcanza mediante la interfaz Loopback 0 de R4 (4.4.4.4). en la tabla de enrutamiento los demás vecinos no sufrieron cambios, continúan los mismos vecinos.

La tabla de enrutamiento del router R4 se puede evidenciar que la dirección por la cual se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3.
Router 3

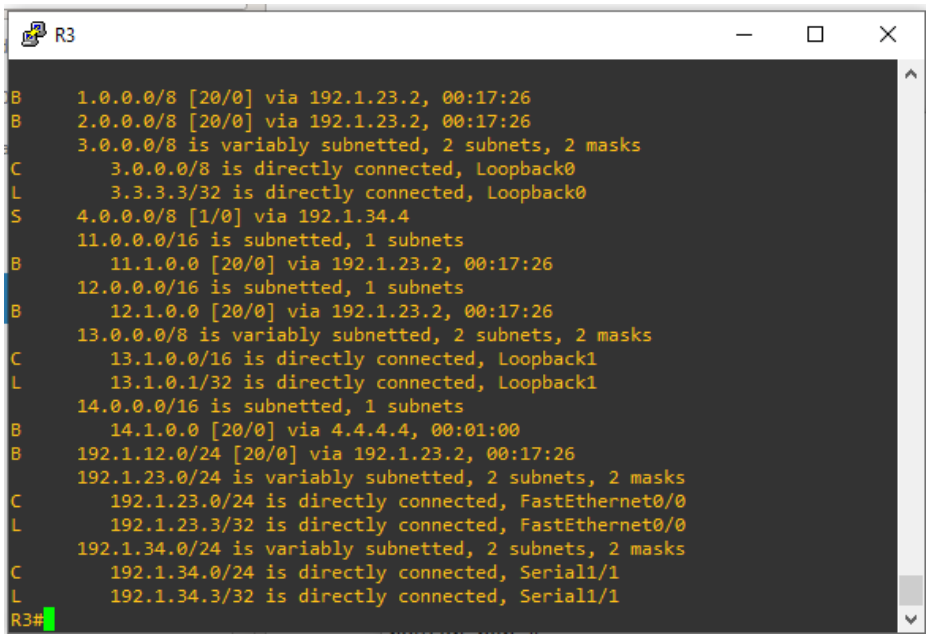


Figura 7 configuración router 3 bgp con rutas hacia router

Router 4

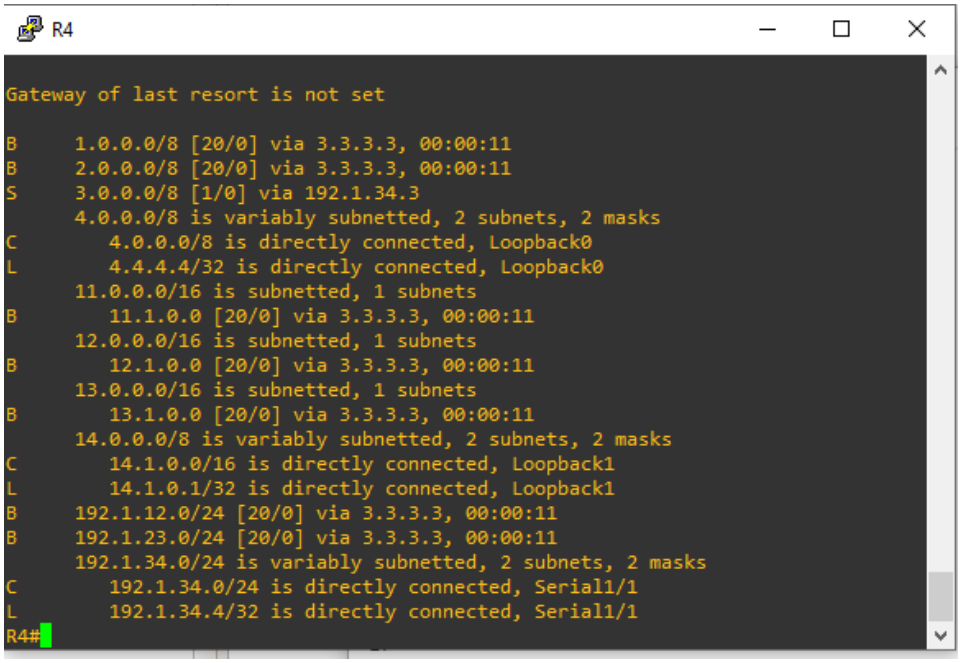


Figura 8 Configuración router 4

Escenario 2

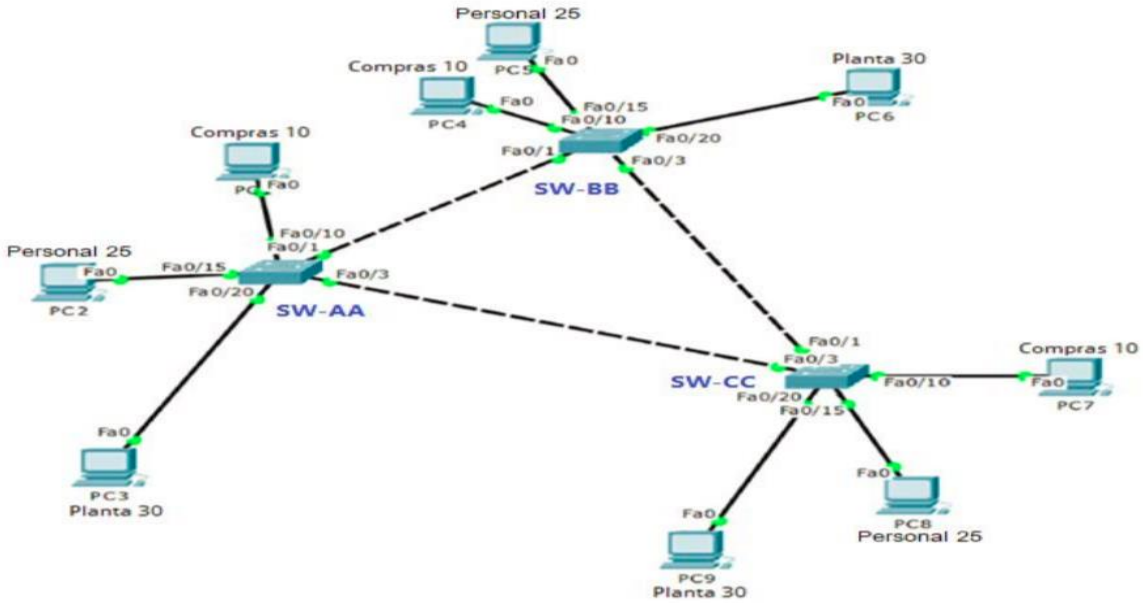


Figura 9 Escenario 2

Topología en Packet Tracer escenario 2

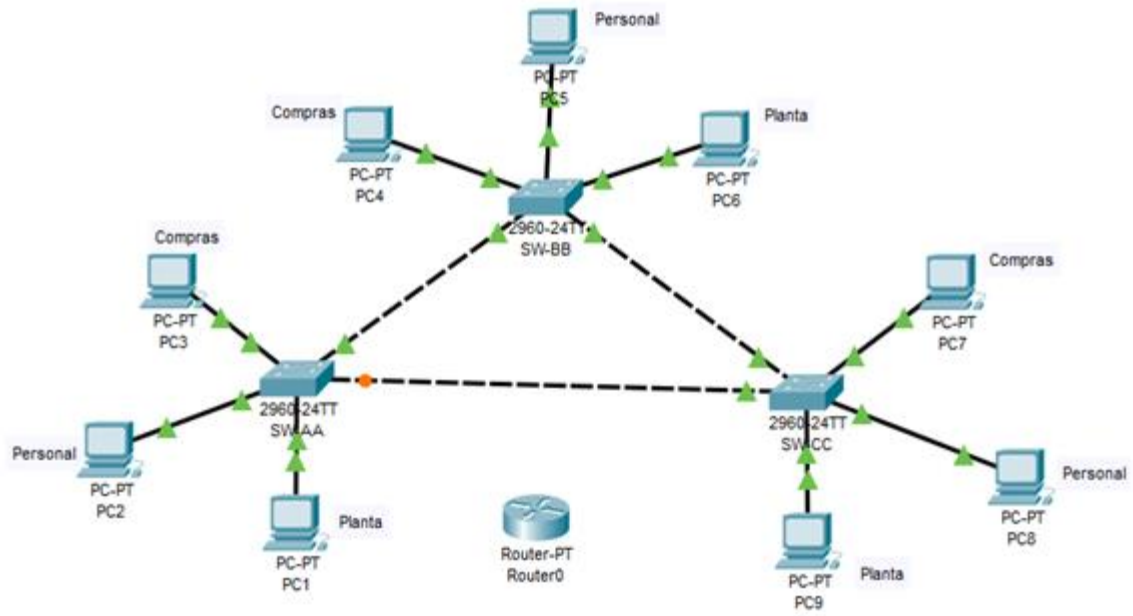


Figura 10 Topología Packet Tracer

Configuración 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> Enable

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

SW-BB> Enable

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> Enable

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 cisc

2. Verificar las configuraciones mediante el comando ***Show vtp status***

Switch SW-AA

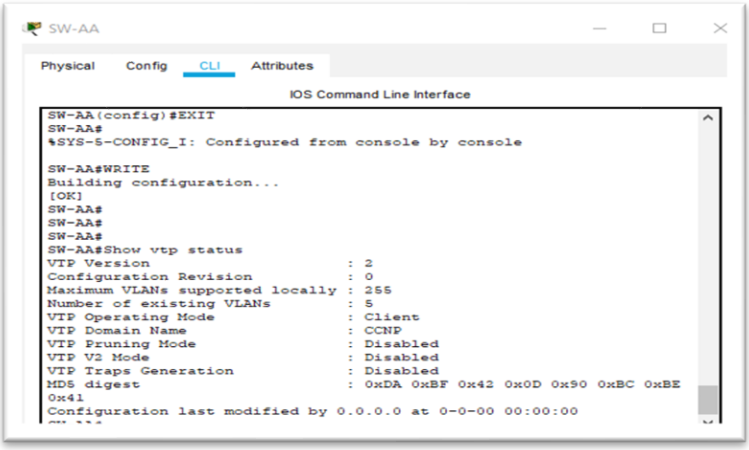


Figura 11 Show vpt status swhith SW-AA

Switch SW-BB

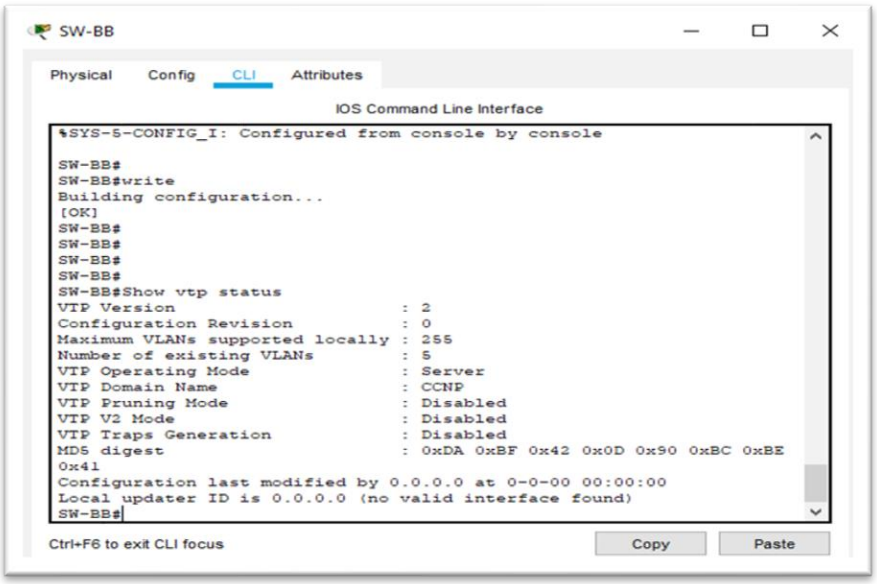


Figura 12 Show vpt status switch SW-BB

Switch SW-CC

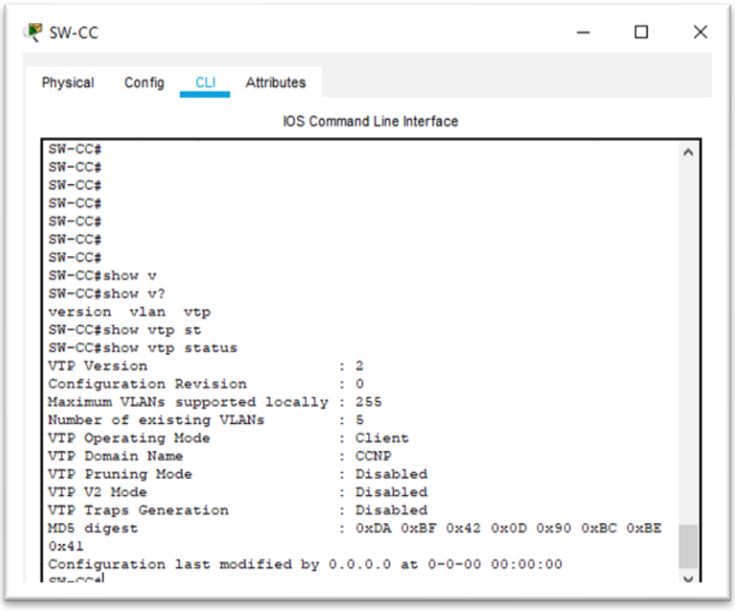


Figura 13 Show vpt status switch SW-CC

Configurar DTP (dynamic Trunking protocol)

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***.

SW-BB> Enable

SW-BB#configure terminal

SW-BB(config)# interface fastEthernet 0/1

SW-BB(config-if)# switchport mode dynamic desirable

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

SW-AA validación modo trunk

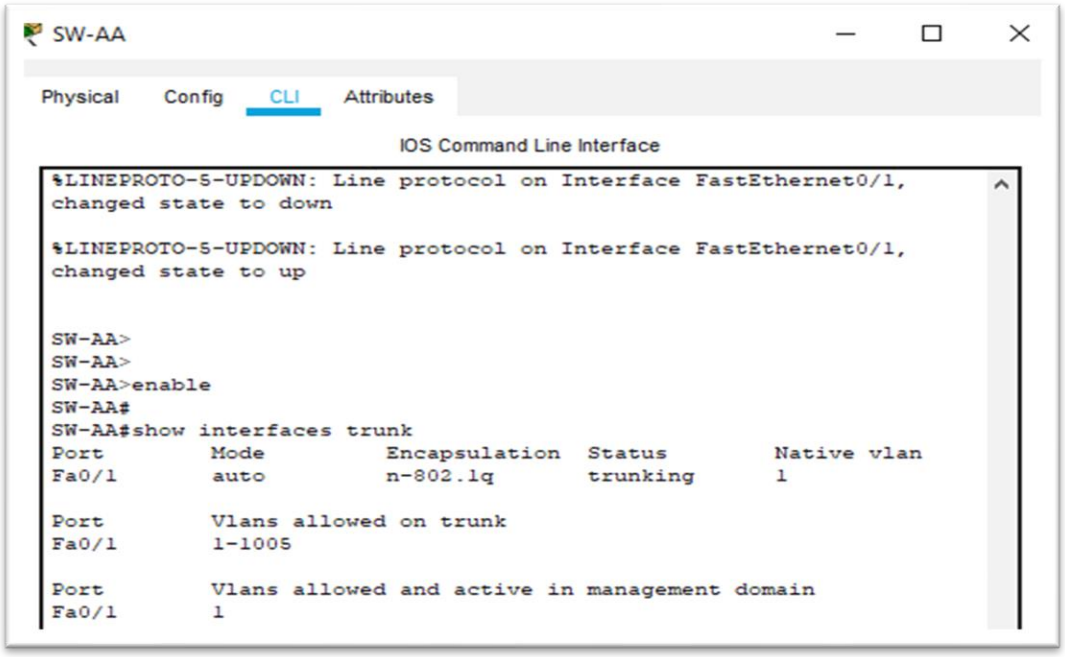


Figura 14 Show interface trunk F0/1 SW-AA

SW-BB validación modo trunk

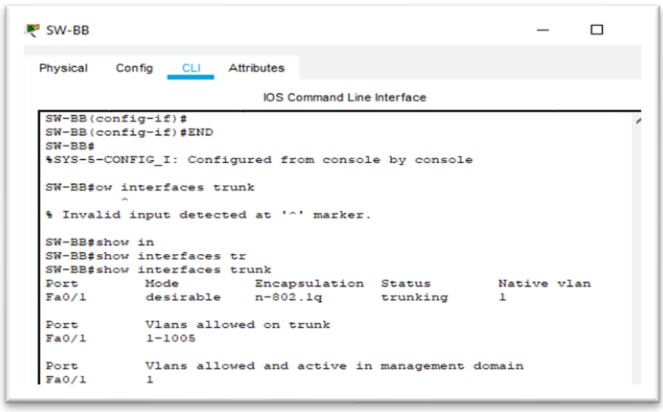


Figura 15 Show interface trunk F 0/1 SW-BB

6. 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> Enable

   SW-AA#configure terminal

   SW-AA(config)# interface fastEthernet 0/3

   SW-AA(config-if)# switchport mode trunk

7. Verifique el enlace "trunk" el comando ***show interfaces trunk*** en SW-AA.

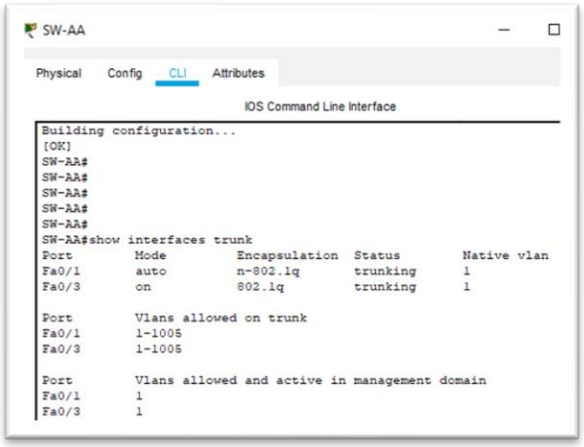


Figura 16 Show interface trunk F 0/3 SW-AA

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

   SW-CC> Enable

SW-CC#configure terminal

SW-CC(config)# interface fastEthernet 0/1

SW-CC(config-if)# switchport mode trunk

Validación enlace “trunk” entre SW-BB y SW-CC

SW-BB Mode trunk

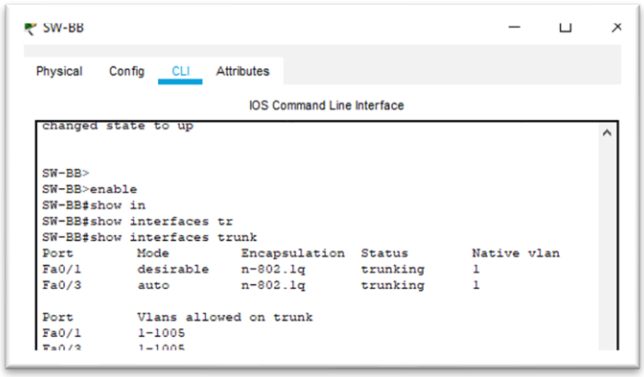


Figura 17 Validación modo trunk SW-BB

SW-CC Mode trunk

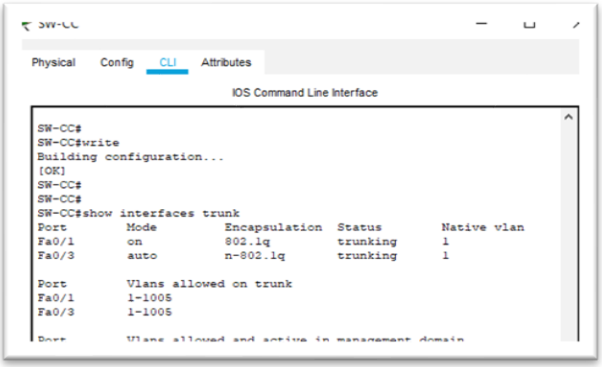


Figura 18 Validación modo trunk SW-CC

Agregar VLANs y asignar puertos

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

SW-AA> Enable
SW-AA#configure terminal
SW-AA(config)# vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode

```
SW-AA#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name planta
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#exit

10. Verifique que las VLANs han sido agregadas correctamente

SW-BB

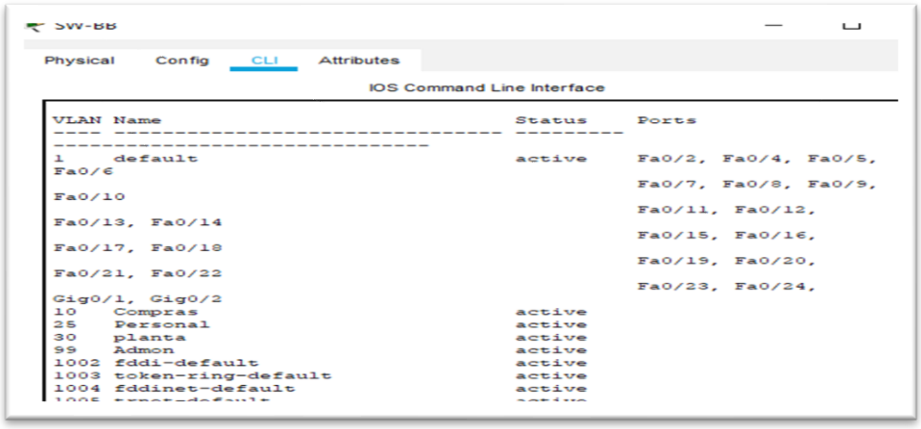


Figura 19 Validación Creación de Vlans en SW-BB

SW-AA

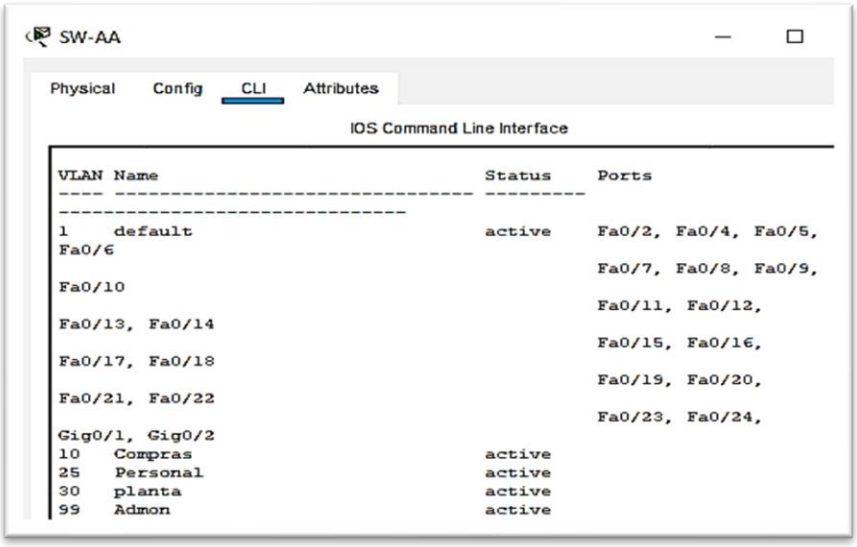


Figura 20 Validación Creación de Vlans en SW-AA

SW-CC

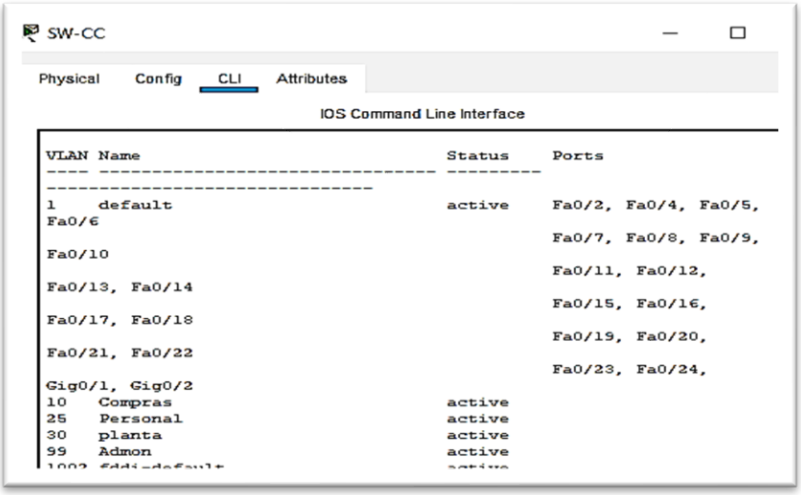


Figura 21 Validación Creación de Vlans en SW-CC

11. 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 5 Enrutamiento PC

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

13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba

SW-AA# configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10 / Compras
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 / Personal
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 / Planta
SW-AA(config)#end

SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10 / Compras
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25 / Personal
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30 / Planta
SW-BB(config)#end
SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10 / Compras
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25 / Personal
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30 / Planta
SW-CC(config)#end

Direccionamiento de los pc

Interfaz	VLAN	N pc	Direcciones IP de los PCs
F0/10	VLAN 10	3	190.108.10.1 / 24
		4	190.108.10.2 / 24
		7	190.108.10.3 / 24
F0/15	VLAN 25	2	190.108.20.1 /24
		5	190.108.20.2 /24
		8	190.108.20.3 /24
F0/20	VLAN 30	1	190.108.30.1 /24
		6	190.108.30.2 /24
		9	190.108.30.3 /24

Tabla 6 Enrutamiento PC según Vlan

SW-AA

Pc 1 Planta

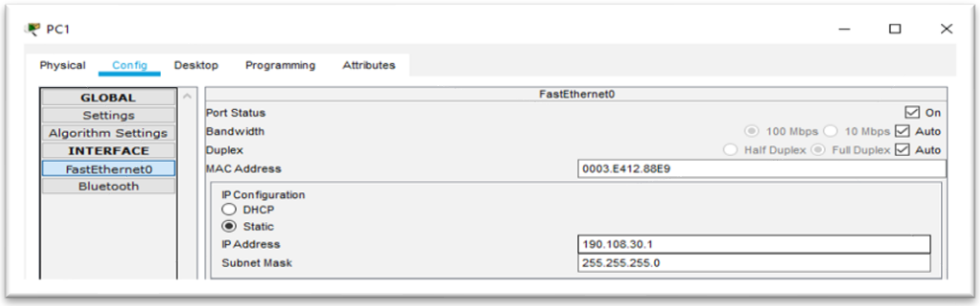


Figura 22 Validación direccionamiento PC

Pc 2 Personal

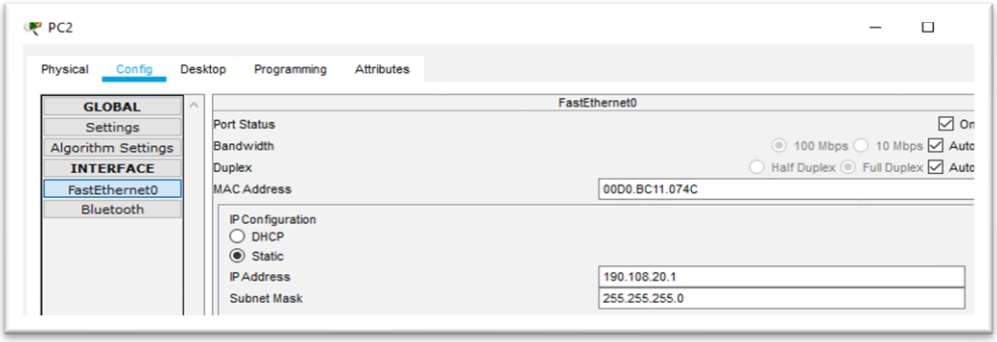


Figura 23 Validación direccionamiento PC2

Pc 3 Compras

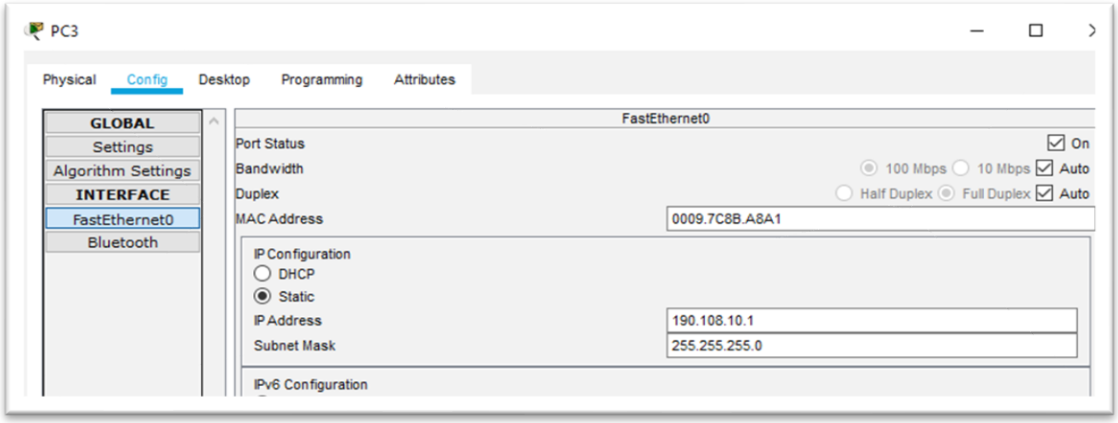


Figura 24 Validación direccionamiento PC3

SW-BB

Pc 4 Compras

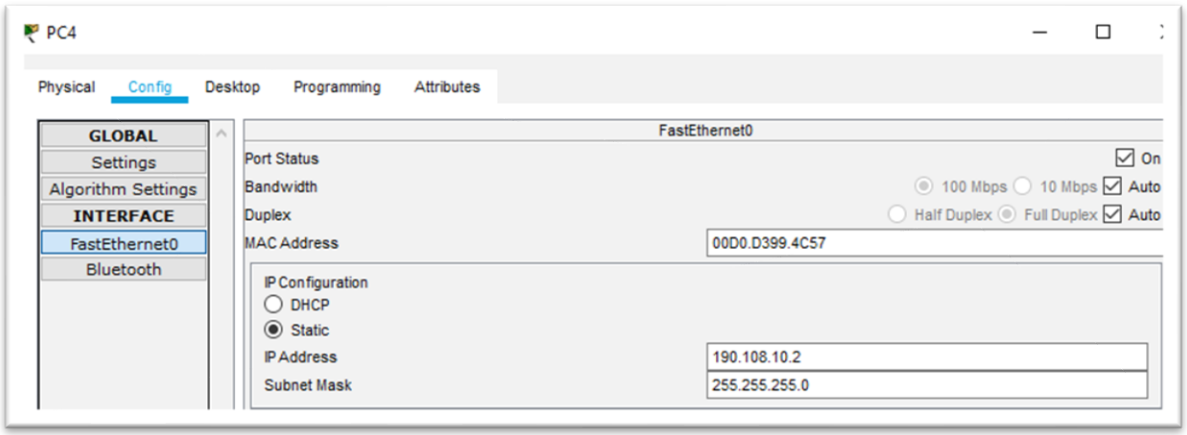


Figura 25 Validación direccionamiento PC4

Pc 5 Personal

Figura 26 Validación direccionamiento PC5

Pc 6 Planta

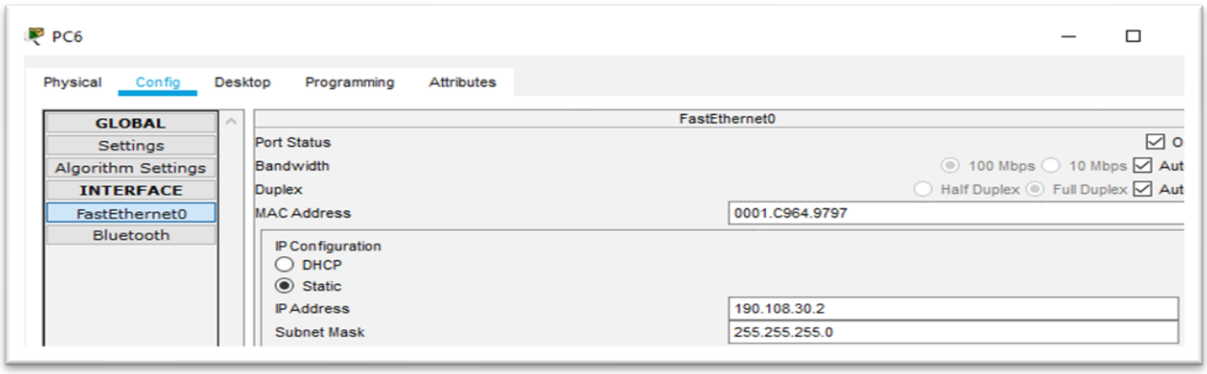


Figura 27 Validación direccionamiento PC6

Pc 7 Compras

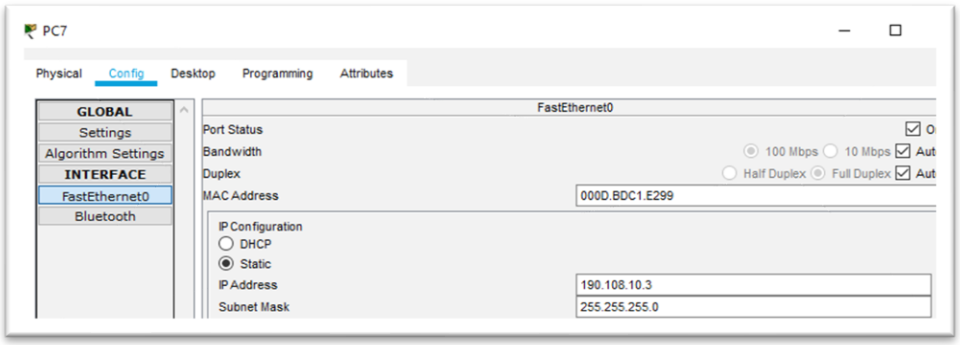


Figura 28 Validación direccionamiento PC7

Pc 8 Personal

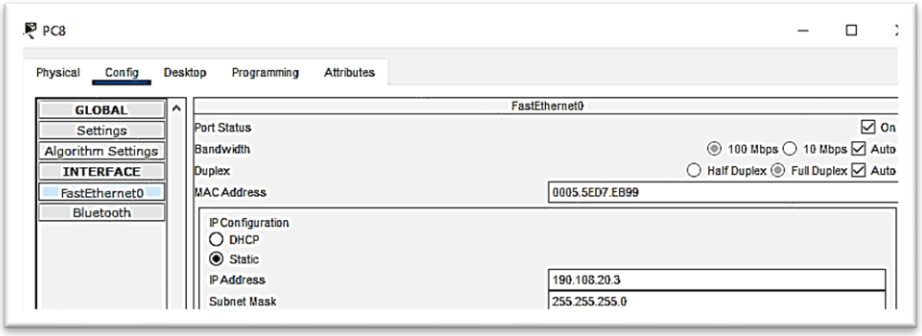


Figura 29 Validación direccionamiento PC7

Pc 9 Planta

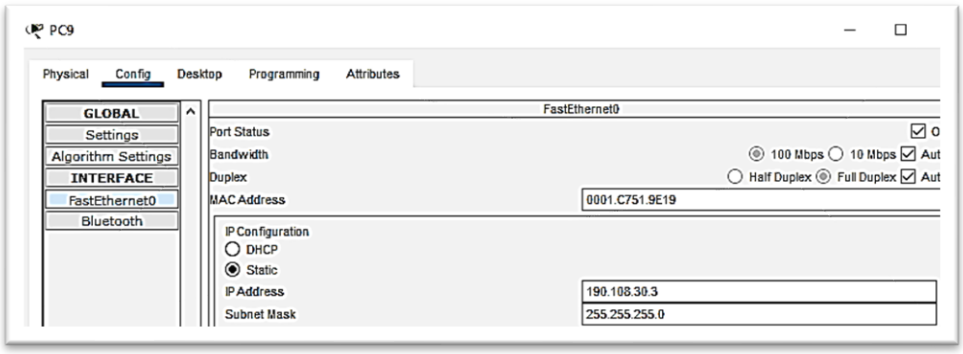


Figura 30 Validación direccionamiento PC9

Configurar las direcciones ip en los switches

14. 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 7 Enrutamiento Switches

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)# exit

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)# exit

SW-CC>

SW-CC# configure terminal

SWT3(config)# interface vlan 99

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

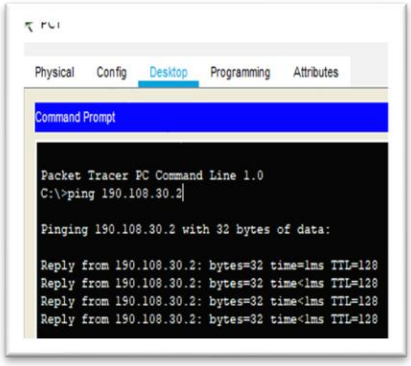
SW-CC(config-if)# exit.

Verificación de conectividad Extremo a Extremo

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

En la realización del ping entre los PCs pertenecientes a diferentes Vlans no tuvo éxito, al realizar ping entre los PCs de la misma Vlan este si tiene éxito, la no realización de ping entre todos los PCs y diferentes Vlans se presenta ya que cada PC pertenece a un segmento de red diferente que está configurado por en las Vlans. Para lograr establecer comunicación con todas las Vlan y los PC se necesitaría agregar a la topología un switch de capa 3 el cual brindaría la función de enrutador entre las Vlans configuradas, así se lograría comunicar todo el tráfico ICMP generado en la red.

Ping de PC1 a PC 6



Ping de PC2 a PC5

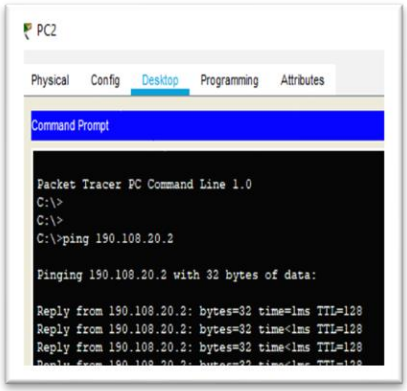
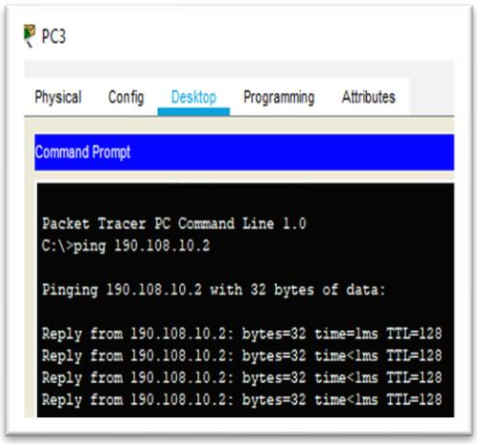


Figura 31 Validación ping PC1 a Pc 6 y Pc2 a Pc5

Ping de PC3 a PC 4



Ping de PC4 a PC7

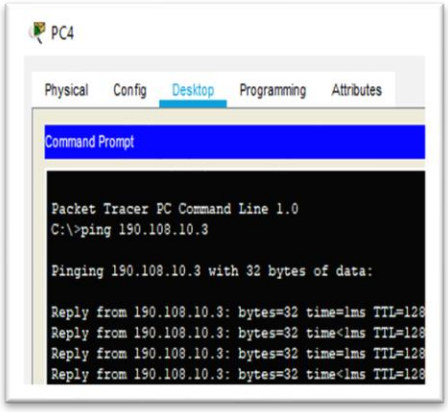
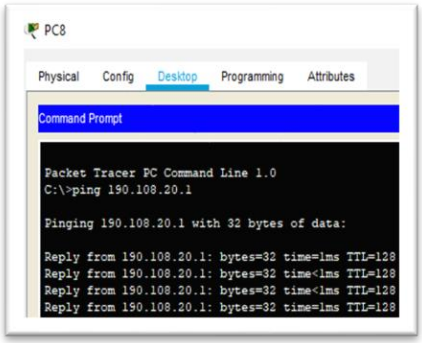


Figura 32 Validación ping Pc3 a Pc4 y Pc4 a Pc7

Ping de PC8 a PC 2



Ping de PC9 a PC1

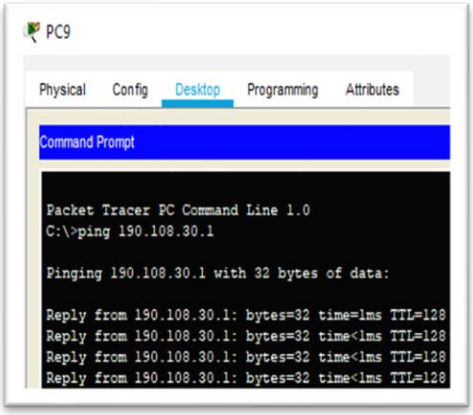
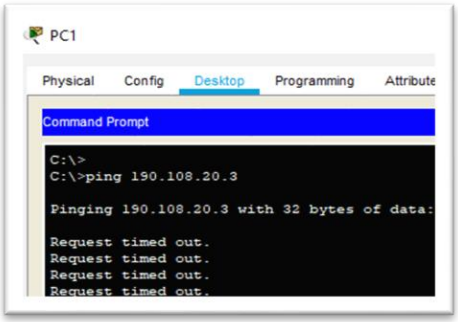


Figura 33 Validación ping Pc3 a Pc4 y Pc4 a Pc7

Ping de PC1 a PC 8



Ping de PC9 a PC2

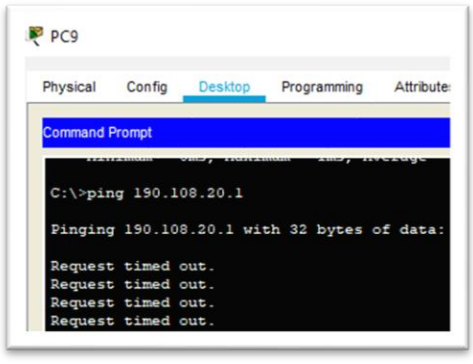


Figura 34 Validación ping Pc1 a Pc8 y Pc9 a Pc2

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

Al realizar ping entre los Switches es exitoso, dado que las interfaces físicas por estas se envían los datos al switch destino del ping este los recibe a través del protocolo ICMP, entre los Switches están configuradas en modo troncal, estas comparten el mismo tipo de encapsulamiento donde se validó con el comando ***show interfaces trunk*** y estas se encuentran en modo compatible.

Ping del SW-AA a SW-BB Y SW-CC

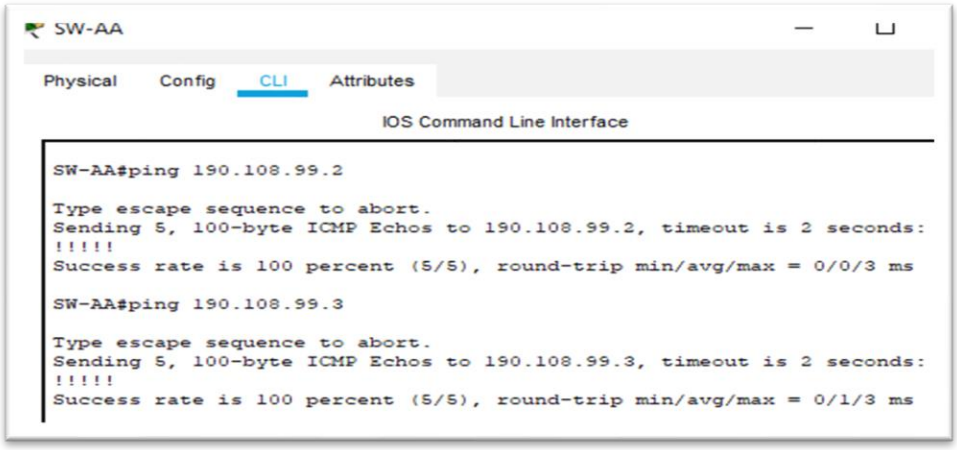


Figura 35 Validación ping SW-AA a SW-BB y SW-CC

Ping del SW-BB a SW-AA Y SW-CC

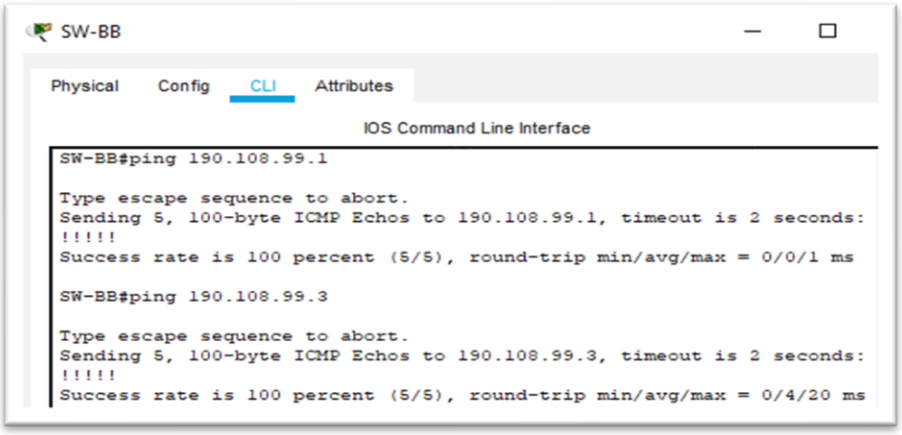


Figura 36 Validación ping SW-BB a SW-AA y SW-CC

Ping del SW-CC a SW-AA Y SW-BB

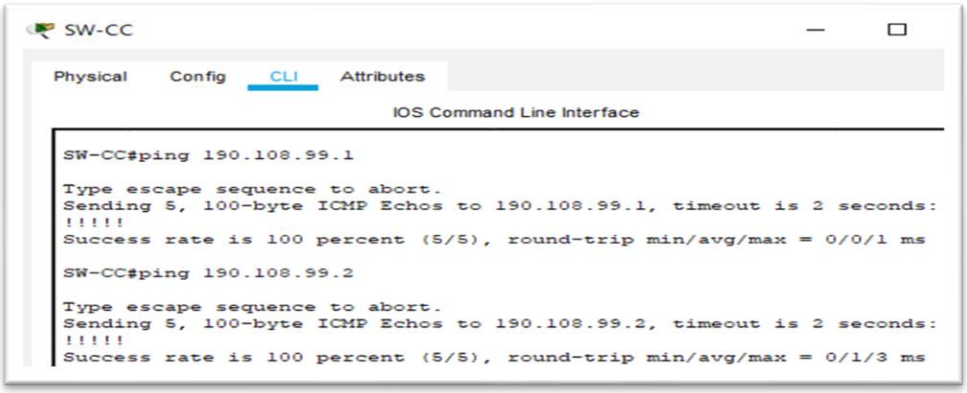


Figura 37 Validación ping SW-CC a SW-AA y SW-BB

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

Al realizar ping desde los switches a los PC este no es exitoso, esto se debe a que no se tiene configurada una dirección ip y una máscara de sured en cada una de las interfaces Vlan de los switches, para esto que el ping sea éxitos se debe realizar esta asignación a cada una de las Vlans con una dirección ip del mismo segmento a la cual está conectada el pc y definir la Valn nativa de dichas interfaces.

Ping desde SW-AA a PC1-PC2 y PC 3

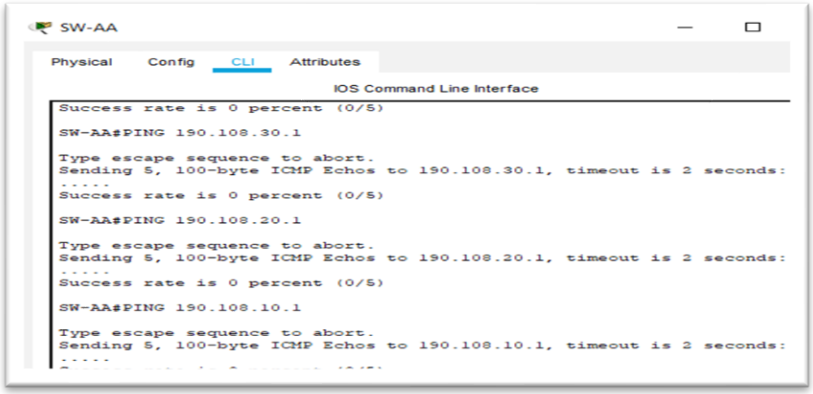


Figura 38 Validación ping SW-AA a Pc 1-Pc2 y Pc

Ping desde SW-BB a PC4-PC5 y PC6

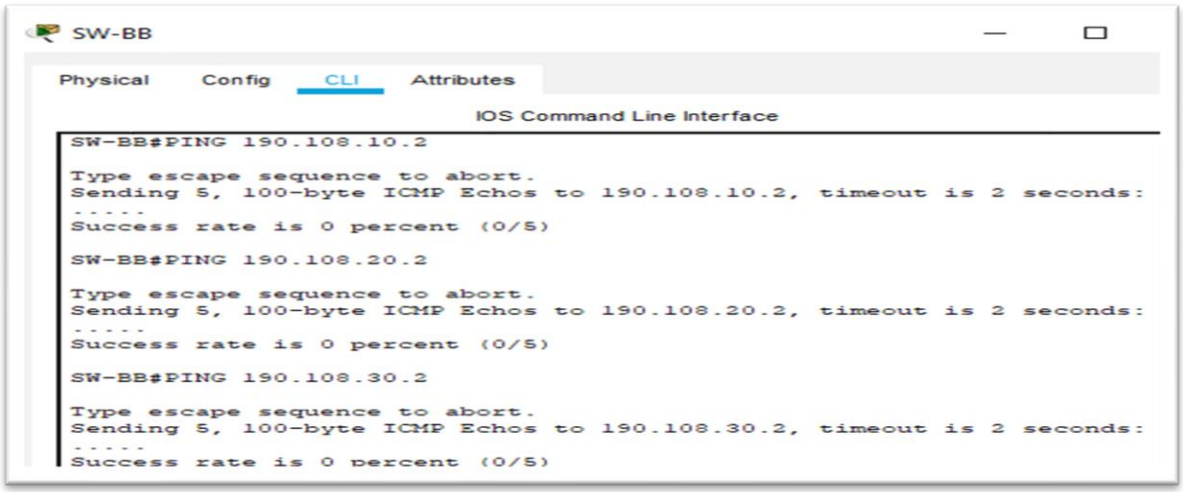


Figura 39 Validación ping SW-BB a Pc 1-Pc2 y Pc3

Ping desde SW-CC a PC7-PC8 y PC9

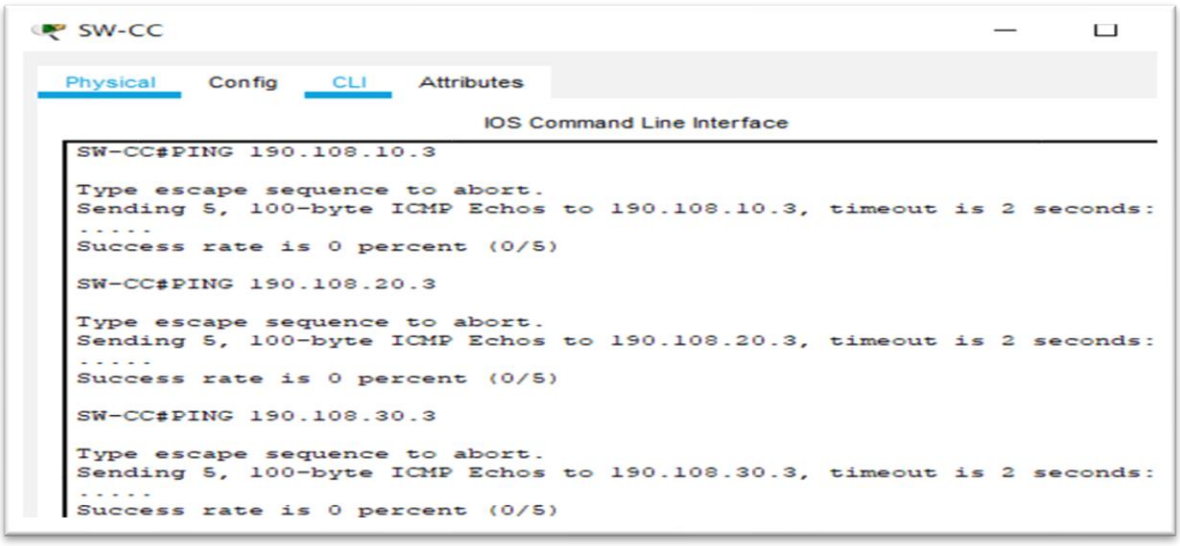


Figura 40 Validación ping SW-CC a Pc7-Pc8 y Pc9

CONCLUSIONES

En el módulo CCNP ROUTE se abordarán conceptos principales como protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas Multi VPN, VRF Lite y protocolos en IPv6., y en el módulo CCNP SWITCH se abordarán conceptos como operaciones y puertos de swtiches, VLANs y troncales, Spanning Tree, ataques de spoofing y configuración de usuarios.

Con el desarrollo del ejercicio de habilidades prácticas permitió evidenciar los diferentes problemas que pueden llegarse a presentar y como solucionarlos, también permitió el uso de diferentes herramientas de simulación que afianzaron las habilidades y competencias adquiridas durante el desarrollo del diplomado de profundización de CCNP.

Adquirir habilidades de gestión de redes orientadas hacia el mundo profesional y corporativo, además necesarios para planificar, implementar, asegurar, mantener y solucionar problemas de redes convergentes.

Los escenarios propuestos afianzaron las capacidades en configuración de dispositivos como router y switches, configuración de Vlan, puertos troncales, configuración de redes primarias y secundarias.

BIBLIOGRAFIA

Amberg, E. (2014). CCNA 1 Powertraining : ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperadode http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

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!AmIJYeiNT1IlnMfy2rhPZHwEoWx

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYeiNT1IhgL9QChD1m9EuGqC