

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GIOVANNY ORTIZ CIFUENTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA/SISTEMAS/TELECO
BOGOTÁ
2020

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

GIOVANNY ORTIZ CIFUENTES

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 TELECOMUNICACIONES
BOGOTÁ
2020**

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 22 de mayo de 2020

AGRADECIMIENTOS

Ante todo quiero agradecer primeramente a mi madre quien fue la que me inculco el amor por superarme. A mi esposa por ser mi compañera en este camino desde el primer día brindándome su apoyo incondicional.

A los tutores que estuvieron a lo largo de todo el camino de formación, y aquellos que me han brindado su apoyo a través de esta experiencia.

TABLA DE CONTENIDOS

AGRADECIMIENTOS	4
LISTA DE TABLAS.....	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN	11
ABSTRACT	11
ESCENARIO 1	13
1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2.....	14
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 <i>show ip route</i>	17
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.	19
Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando <i>show ip route</i>	20
ESCENARIO 2	22
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.....	23
2. Verifique las configuraciones mediante el comando <i>show vtp status</i>	27
B. Configurar DTP (Dynamic Trunking Protocol).....	28
4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es <i>dynamic auto</i> , solo un lado del enlace debe configurarse como <i>dynamic desirable</i>	28
5. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando <i>show interfaces trunk</i>	30
6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando <i>switchport mode trunk</i> en la interfaz F0/3 de SW-AA	31

7. Verifique el enlace "trunk" el comando <i>show interfaces trunk</i> en SW-AA	32
8. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.....	32
C. Agregar VLANs y asignar puertos.	34
9. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30)y Admon (99).....	34
10. Verifique que las VLANs han sido agregadas correctamente.	35
11. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla	37
12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.....	37
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.	39
14. En cada uno de los Switches asigne una dirección IP al SVI (<i>Switch Virtual Interface</i>) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.	42
E. Verificar la conectividad Extremo a Extremo	44
15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.....	44
16. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.....	50
17. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.....	52
CONCLUSIONES.....	54
REFERENCIAS BIBLIOGRÁFICA	55

LISTA DE TABLAS

Tabla 1: R1	13
Tabla 2: R2	13
Tabla 3: R3	13
Tabla 4: R4	14
Tabla 5: Puertos VLANs.....	37
Tabla 6: Direcciones IP.....	42

LISTA DE FIGURAS

Figura 1: Escenario 1	13
Figura 2: Simulación Escenario 1.....	14
Figura 3: Configuración R1	15
Figura 4: Configuración R2.....	16
Figura 5: Configuración R3	16
Figura 6: comprobación R2	17
Figura 7: Relación BGP R2	18
Figura 8: Relación BGP R3	18
Figura 9: Show ip route R2.....	19
Figura 10: show ip route R3	19
Figura 11: BGP R4	20
Figura 12: show ip route	21
Figura 13: Escenario 2 unad	22
Figura 14: Escenario 2 simulación	22
Figura 15: configuración SW-BB.....	25
Figura 16: configuración SW-AA	26
Figura 17: configuración SW-CC.....	26
Figura 18: Verificación SW-AA.....	27
Figura 19: Verificación SW-BB	27
Figura 20: Verificación SW-CC	28
Figura 21: Trunk SW-AA.....	29
Figura 22: Trunk SW-BB	30
Figura 23: Validación Trunk SW-AA	30
Figura 24: Validación Trunk SWBB	31
Figura 25: Trunk estático SSAA.....	32
Figura 26: Verificación SSAA.....	32
Figura 27: Trunk Permanente	33
Figura 28: verificación.....	34
Figura 29: Vlan	34
Figura 30: Vlans	35
Figura 31: show vlan brief.....	36
Figura 32: show vlan brief.....	36
Figura 33: show vlan brief.....	36
Figura 34: Configuración IP	37
Figura 35: Puerto F0/10 SWAA	38
Figura 36: Puerto F0/10 SWBB.....	38
Figura 37: Puerto F0/10 SWCC.....	39
Figura 38: Puerto F0/15/20 SWAA	40
Figura 39: Puerto F0/15/20 SWBB.....	40
Figura 40: Puerto F0/15/20 SWCC.....	41

Figura 41: Vlan 99 SWAA	42
Figura 42: Vlan 99 SWBB.....	43
Figura 43: Vlan 99 SWBB.....	44
Figura 44: Pings PC1	45
Figura 45: Pings PC2.....	45
Figura 46: Pings PC3	46
Figura 47: Pings PC4.....	47
Figura 48: Pings PC5	47
Figura 49: Pings PC6.....	48
Figura 50: Pings PC7.....	49
Figura 51: Pings PC8.....	49
Figura 52: Pings PC9.....	50
Figura 53: Pings SWAA	51
Figura 54: Pings SWBB.....	51
Figura 55: Pings SWCC.....	52
Figura 56: Pings SWAA a PCS	52
Figura 57: Pings SWBB a PCS.....	53
Figura 58: Pings SWCC a PCS.....	53

GLOSARIO

EIGRP: Protocolo diseñado para usar el de vector distancia para lograr la comunicación.

OSPF: Protocolo que consiste en realizar una comunicación mediante La ruta más corta y obtener beneficios para la comunicación.

Dirección IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina dirección IP dinámica (normalmente abreviado como IP dinámica).

Gateway – Pasarela o puerta de acceso: Computador que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, una puerta de acceso podría conectar una red de área local a un mainframe. Una puerta de acceso de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

VLAN - Red de Área Local Virtual: Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

VTP - VLAN Trunking Protocol: Es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

PROTOCOLOS DE RED: Son los procedimientos que se encuentran definidos o estandarizados para el uso y configuración adecuada de una red con el fin de que funcione de la mejor manera posible dependiendo de su topología, cantidad de dispositivos en la red y de las necesidades de funcionamiento de la red.

TOPOLOGÍA DE RED: Son las estructuras que están compuestas por los dispositivos de la red, para este trabajo conformadas routers y switches. Existen varios tipos: bus, estrella, anillo, árbol, malla, híbrida son algunas de las más importantes las cuales se seleccionan para construir una red de acuerdo a las necesidades de está.

RESUMEN

El presente documento tiene como objetivo el desarrollo de dos actividades de redes los cuales demuestran que se han adquirido los conocimientos requeridas para aprobar el diplomado Cisco CCNP, el cual fue diseñado para aquellos estudiantes de ingenierías y profesiones relacionadas con el mundo de las tecnologías de las comunicaciones que desean adquirir los conocimientos y habilidades en gestión de redes empresariales. Ofreciendo una gran experiencia de aprendizaje tanto teórica como práctica que abarca habilidades avanzadas de Routing, Switching, conmutación y enrutamientos en la resolución de problemas.

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

ABSTRACT

The objective of this document is to carry out two networking activities which demonstrate that the knowledge required to pass the Cisco CCNP diploma has been acquired, which was designed for those engineering students and professions related to the world of IT technologies. communications who want to acquire the knowledge and skills in business network management. Offering a great theoretical and practical learning experience that encompasses advanced Routing, Switching, Switching and Routing skills in problem solving.

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

INTRODUCCIÓN

A continuación en este trabajo veremos todo a nivel conceptual y practico vistos en el curso del diplomado CCNP lograr poner en práctica los conocimientos aprendidos durante este curso . para esto tenemos tres Escenarios donde debemos poner a prueba nuestros conocimientos sobre protocolos de enrutamientos OSPF EIGRP y BGP como tambien a nivel de switching ver temas de VTP y ser realizadas en Packet, debemos probar conectividad mediante diferentes pruebas de ping y tambien mostrar configuraciones a nivel de comandos Show para validar las configuraciones realizadas en los diferentes escenarios.

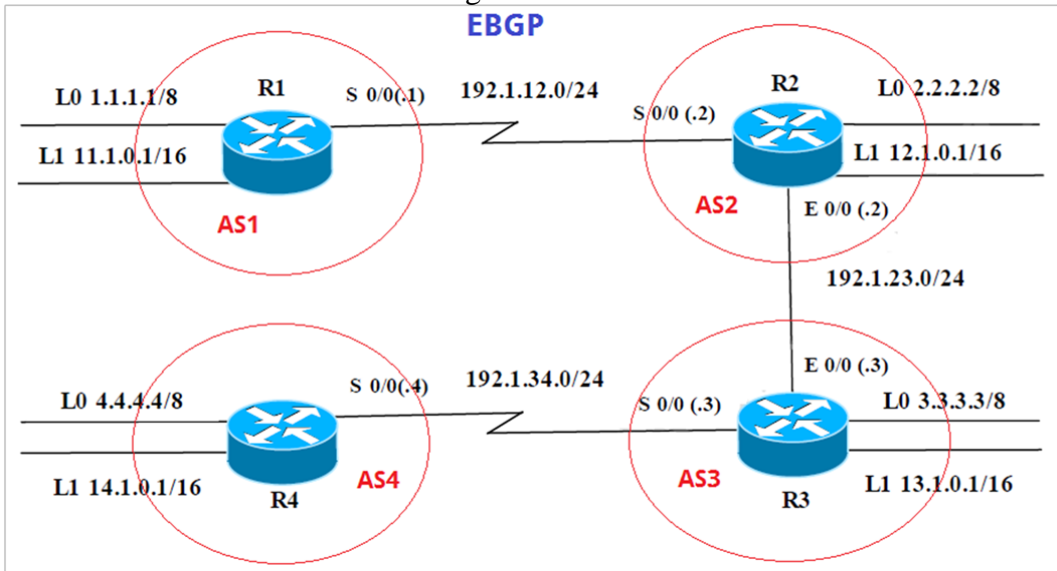
Para cumplir con los propósitos mencionados, se abordan temáticas como el enrutamiento dinámico a través de los protocolos OSPF y EIGRP, así como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback. Por último, se evidencia la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN.

En consecuencia, a continuación, se encuentra una descripción detallada del paso a paso necesario para cada una de las etapas realizadas durante el desarrollo de los escenarios planteados , además, del registro de los procesos de verificación de conectividad mediante el uso de comandos como *ping, show ip route, show vtp status, show interfaces trunk,* entre

DESCRIPCIÓN DE LOS ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

Figura 1: Escenario 1



Información para configuración de los Routers

Tabla 1: R1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 2/0	192.1.12.1	255.255.255.0

Tabla 2: 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 2/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 3: R3

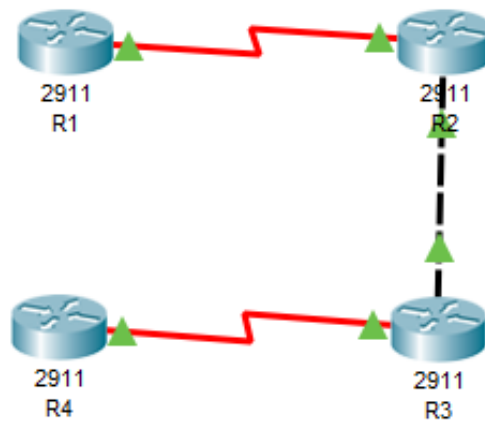
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0

S 2/0	192.1.34.3	255.255.255.0
-------	------------	---------------

Tabla 4: 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 2/0	192.1.34.4	255.255.255.0

Figura 2: Simulación Escenario 1



1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2.

Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando *show ip route*.

```
R1#configure terminal
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0

R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
```

```

R1(config-if)#no shutdown
R1(config-if)#exit
router bgp 1
  bgp router-id 22.22.22.22
  network 1.0.0.0 mask 255.0.0.0
  network 11.1.0.0 mask 255.255.0.0
  network 192.1.12.0 mask 255.255.255.0
  neighbor 192.1.12.2 remote-as 2

```

```

R2#configure terminal
R2(config)#interface 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 serial 0/0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface GigabitEthernet 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 3: Configuración R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed
state to up
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip address 192.1.12.1 255.255.255.0
Router(config-if)#no shutdown

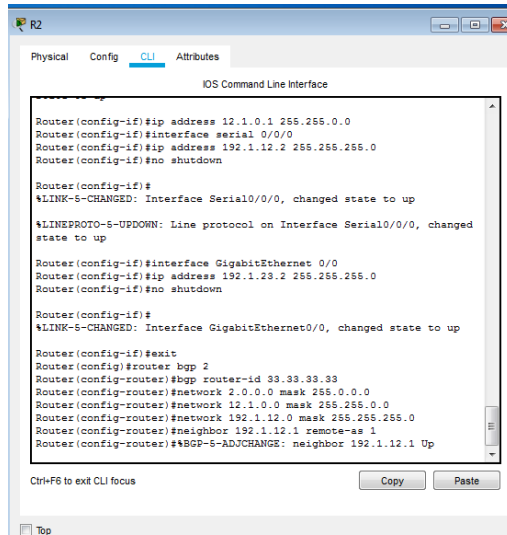
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
Router(config)#router bgp 1
Router(config-router)#bgp router-id 22.22.22.22 network 1.0.0.0 mask
255.0.0.0 network 11.1.0.0 mask 255.255.0.0 network 192.1.12.0 mask
255.255.255.0 neighbor 192.1.12.2 remote-as 2
^
% Invalid input detected at '^' marker.

Router(config-router)#bgp router-id 22.22.22.22
Router(config-router)#network 1.0.0.0 mask 255.0.0.0
Router(config-router)#network 11.1.0.0 mask 255.255.0.0
Router(config-router)#network 192.1.12.0 mask 255.255.255.0
Router(config-router)#neighbor 192.1.12.2 remote-as 2
Router(config-router)#no shutdown
^
% Invalid input detected at '^' marker.

Router(config-router)#exit
Router(config)#

```

Figura 4: Configuración R2



The screenshot shows the configuration of Router R2 in CLI mode. The configuration includes setting IP addresses for Serial0/0/0 and GigabitEthernet0/0, enabling the interfaces, and configuring BGP with router ID 33.33.33.33 and two networks: 12.1.0.0/16 and 192.1.12.0/24. A BGP neighbor is configured at 192.1.12.1.

```
Router(config-if)#ip address 12.1.0.1 255.255.0.0
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip address 192.1.12.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-6-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

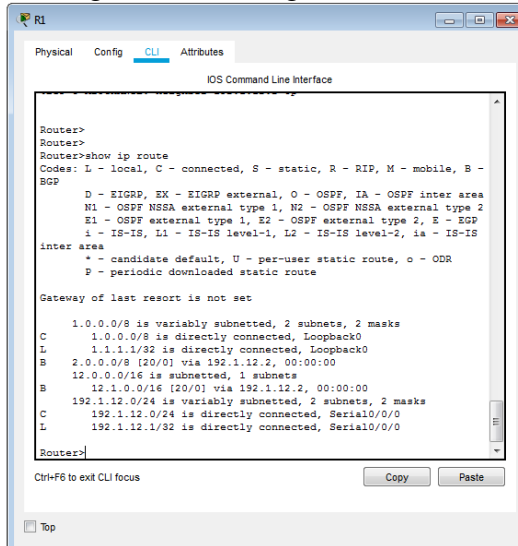
Router(config-if)#interface GigabitEthernet 0/0
Router(config-if)#ip address 192.1.23.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-6-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#router bgp 2
Router(config-router)#bgp router-id 33.33.33.33
Router(config-router)#network 2.0.0.0 mask 255.0.0.0
Router(config-router)#network 12.1.0.0 mask 255.255.0.0
Router(config-router)#network 192.1.12.0 mask 255.255.255.0
Router(config-router)#neighbor 192.1.12.1 remote-as 1
Router(config-router)#BGP-6-ADJCHANGE: neighbor 192.1.12.1 Up

Ctrl+F6 to exit CLI focus
```

Figura 5: Configuración R3



The screenshot shows the output of the 'show ip route' command on Router R1. It displays the routing table with various entries for local, connected, and BGP routes, including subnets and masks.

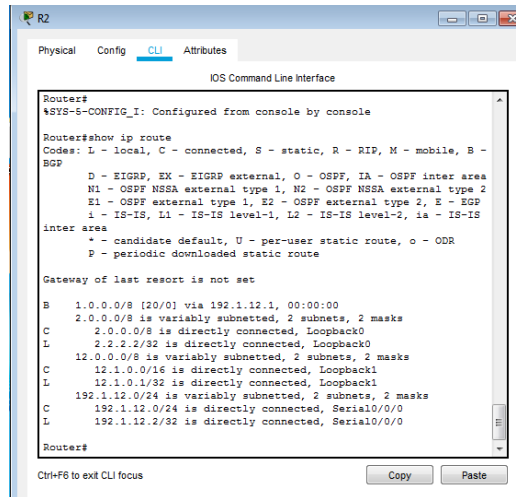
```
Router>
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS,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

Gateway of last resort is not set

1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 1.0.0.0/8 is directly connected, Loopback0
L 1.1.1.1/32 is directly connected, Loopback0
B 2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.12.0/24 is directly connected, Serial0/0/0
L 192.1.12.1/32 is directly connected, Serial0/0/0

Router>
```


Figura 6: comprobación R2



```
Router#
*SYS-5-CONFIG_I: Configured from console by console
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
EGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial0/0/0
L    192.1.12.2/32 is directly connected, Serial0/0/0

Router#
```

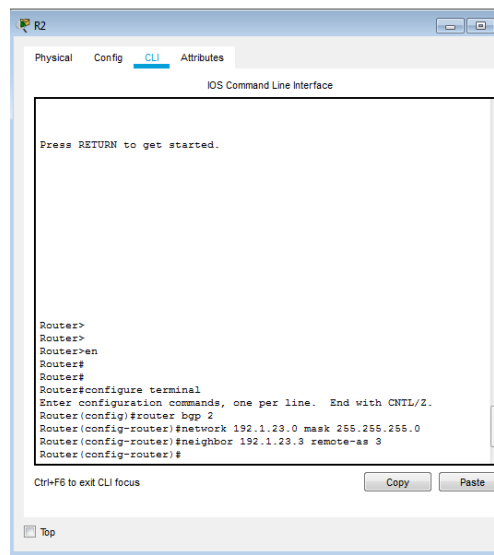
2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando *show ip route*.

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

```
R3#configure terminal
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface GigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 0/0/0
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
```

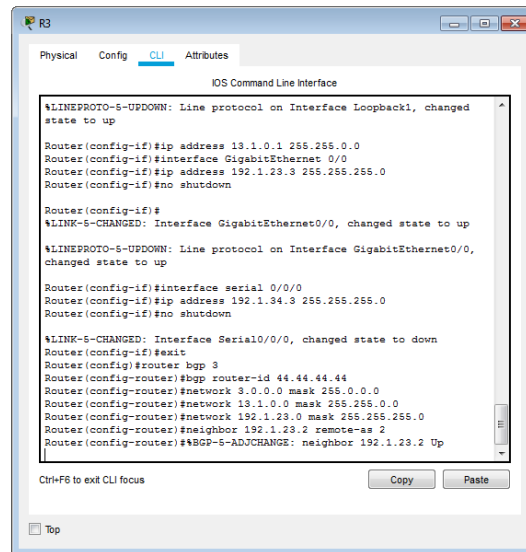
R3(config-router)#neighbor 192.1.23.2 remote-as 2

Figura 7: Relación BGP R2



```
Router>
Router>
Router>en
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 2
Router(config-router)#network 192.1.23.0 mask 255.255.255.0
Router(config-router)#neighbor 192.1.23.3 remote-as 3
Router(config-router)#
```

Figura 8: Relación BGP R3



```
Router(config-if)#ip address 13.1.0.1 255.255.0.0
Router(config-if)#interface GigabitEthernet 0/0
Router(config-if)#ip address 192.1.23.3 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

Router(config-if)#interface serial 0/0/0
Router(config-if)#ip address 192.1.34.3 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
Router(config)#router bgp 3
Router(config-router)#bgp router-id 44.44.44.44
Router(config-router)#network 3.0.0.0 mask 255.0.0.0
Router(config-router)#network 13.1.0.0 mask 255.255.0.0
Router(config-router)#network 192.1.23.0 mask 255.255.255.0
Router(config-router)#neighbor 192.1.23.2 remote-as 2
Router(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
```

A continuación, se puede evidenciar en el resultado que se obtiene del comando show ip route, que el router R2 ha actualizado su tabla de enrutamiento y ahora contiene también las direcciones de Loopback configuradas en el router R3, por tanto, este dispositivo ha aprendido hasta este momento 4 rutas a través del protocolo BGP las cuales identifica con el código B. De otro lado, el router R3 contiene en su tabla de enrutamiento las redes que reconoce conectadas directamente, es decir, las configuradas en sus interfaces Loopback y las redes que lo comunican con los routers R3 y R4 mediante las interfaces Ethernet

0/0 y serial 0/0/0 respectivamente. Además, este router (R3) ha actualizado su tabla de enrutamiento con las direcciones de red correspondientes a las interfaces Loopback que se configuraron en R2 y R1, rutas que aprendió mediante el protocolo BGP gracias a su relación de adyacencia con R2 y a que dichas redes se anunciaron en cada uno de los routers, así también, R3 contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP como lo evidencia el código B que la precede. Por último, se identifica que R3 alcanza todas estas redes a través de la interfaz GigaEthernet 0/0 que lo conecta con R2 (192.1.23.0/24)

Figura 9: Show ip route R2

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

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

Gateway of last resort is not set

B 1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
  2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 2.0.0.0/8 is directly connected, Loopback0
L 2.2.2.2/32 is directly connected, Loopback0
B 3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 12.1.0.0/16 is directly connected, Loopback1
L 12.1.0.1/32 is directly connected, Loopback1
  13.0.0.0/16 is subnetted, 1 subnets
B 13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.12.0/24 is directly connected, Serial0/0/0
--More--

Ctrl+F6 to exit CLI focus
Copy Paste
Top
  
```

Figura 10: show ip route R3

```

R3
Physical Config CLI Attributes
IOS Command Line Interface

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

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

Gateway of last resort is not set

B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
  2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
  3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.0.0.0/8 is directly connected, Loopback0
L 3.3.3.3/32 is directly connected, Loopback0
  12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
  13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 13.1.0.1/32 is directly connected, Loopback1
  192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
--More--

Ctrl+F6 to exit CLI focus
Copy Paste
  
```

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

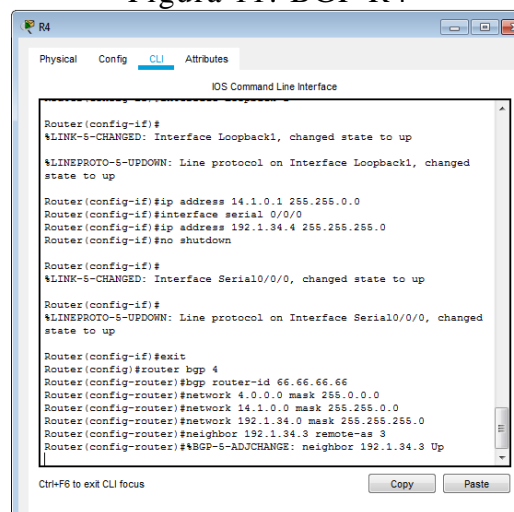
de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP.

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#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
```

```
R4#configure terminal
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

Figura 11: BGP R4



```
R4
Physical Config CLI Attributes
IOS Command Line Interface

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed
state to up

Router(config-if)#ip address 14.1.0.1 255.255.0.0
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip address 192.1.34.4 255.255.255.0
Router(config-if)#no shutdown

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

Router(config-if)#exit
Router(config)#router bgp 4
Router(config-router)#bgp router-id 66.66.66.66
Router(config-router)#network 4.0.0.0 mask 255.0.0.0
Router(config-router)#network 14.1.0.0 mask 255.255.0.0
Router(config-router)#network 192.1.34.0 mask 255.255.255.0
Router(config-router)#neighbor 192.1.34.3 remote-as 3
Router(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up

Ctrl+F6 to exit CLI focus
```

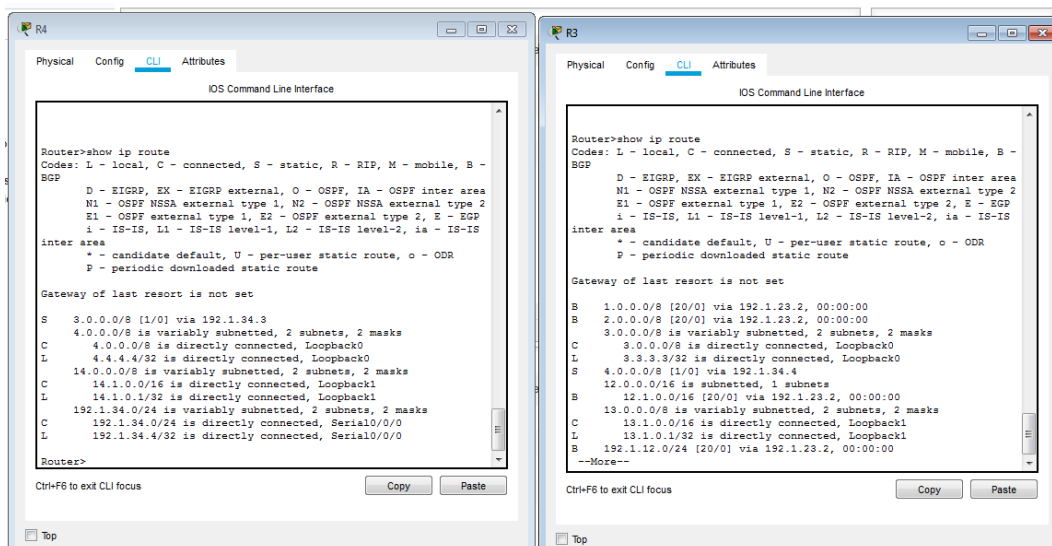
Para establecer las relaciones de adyacencia mediante las direcciones de Loopback, el router vecino necesita informar sobre el uso de esta interfaz en lugar de una interfaz física y, por tanto, se requiere una configuración adicional para establecer los vecinos:

```
R3#configure terminal
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
```

R4#configure terminal

```
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
```

Figura 12: show ip route



ESCENARIO 2

Figura 13: Escenario 2 unad

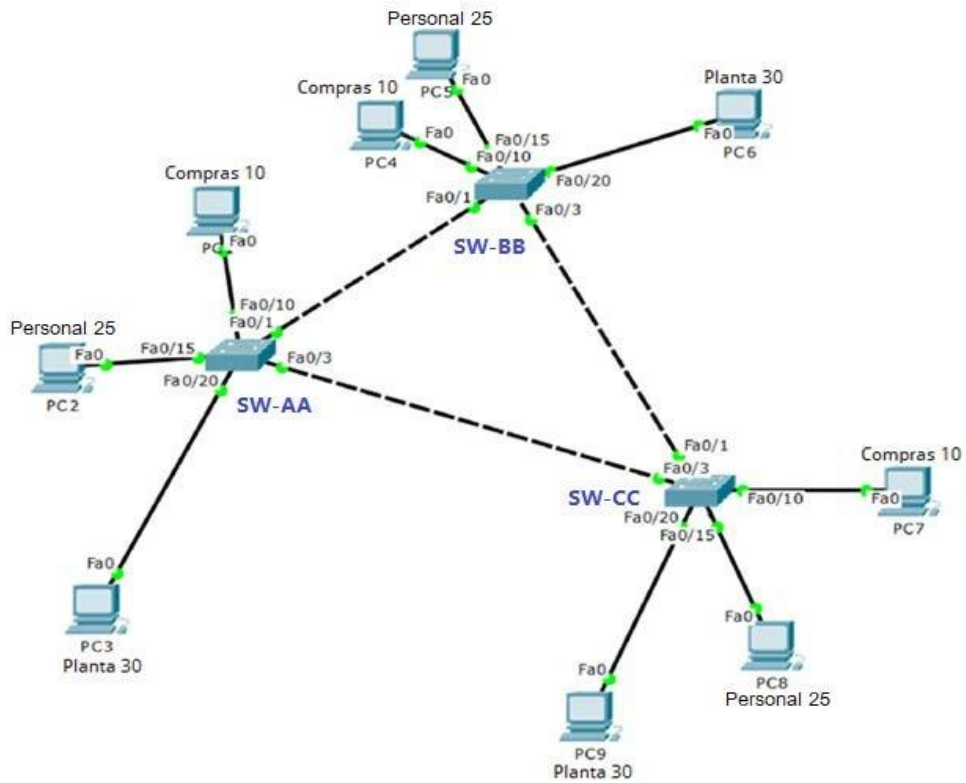
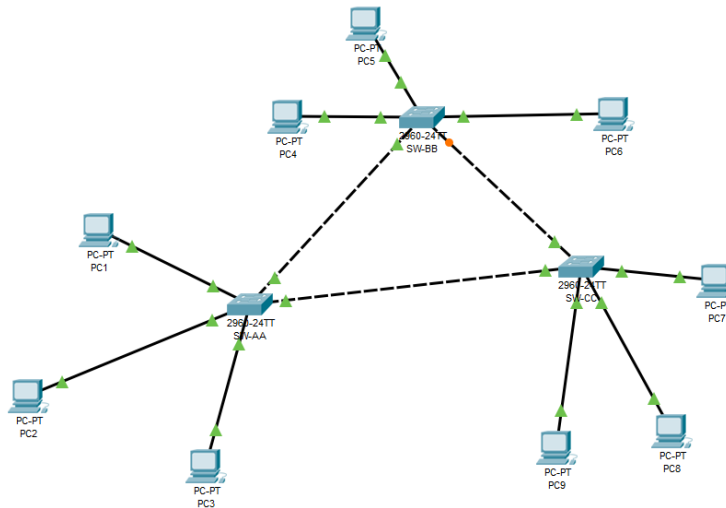


Figura 14: Escenario 2 simulación



A. Configurar VTP

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

Configuración inicial de los switch

SW-AA

```
SW-AA>
SW-AA>
SW-AA>EN
SW-AA#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface range f0/1
SW-AA(config-if-range)#no shutdown
SW-AA(config-if-range)#exit
SW-AA(config)#interface range f0/3
SW-AA(config-if-range)#no shutdown
SW-AA(config-if-range)#exit
SW-AA(config)#interface range f0/10
SW-AA(config-if-range)#no shutdown
SW-AA(config-if-range)#exit
SW-AA(config)#interface range f0/15
SW-AA(config-if-range)#no shutdown
SW-AA(config-if-range)#exit
SW-AA(config)#interface range f0/20
SW-AA(config-if-range)#no shutdown
SW-AA(config-if-range)#exit
SW-AA(config)#
```

SE-BB

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname SW-BB
SW-BB(config)#interface range f0/1
SW-BB(config-if-range)#no shutdown
SW-BB(config-if-range)#exit
```

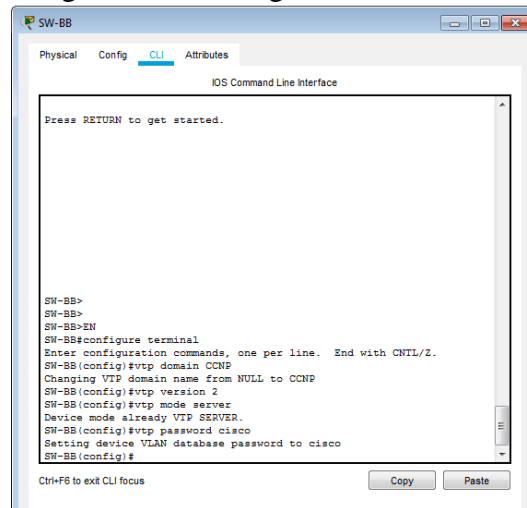
```
SW-BB(config)#interface range f0/3
SW-BB(config-if-range)#no shutdown
SW-BB(config-if-range)#exit
SW-BB(config)#interface range f0/10
SW-BB(config-if-range)#no shutdown
SW-BB(config-if-range)#exit
SW-BB(config)#interface range f0/15
SW-BB(config-if-range)#no shutdown
SW-BB(config-if-range)#exit
SW-BB(config)#interface range f0/20
SW-BB(config-if-range)#no shutdown
SW-BB(config-if-range)#exit
SW-BB(config)#
```

SW-CC

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#interface range f0/1
SW-CC(config-if-range)#no shutdown
SW-CC(config-if-range)#exit
SW-CC(config)#interface range f0/3
SW-CC(config-if-range)#no shutdown
SW-CC(config-if-range)#exit
SW-CC(config)#interface range f0/10
SW-CC(config-if-range)#no shutdown
SW-CC(config-if-range)#exit
SW-CC(config)#interface range f0/15
SW-CC(config-if-range)#no shutdown
SW-CC(config-if-range)#exit
SW-CC(config)#interface range f0/20
SW-CC(config-if-range)#no shutdown
SW-CC(config-if-range)#exit
```

A continuación, se darán los comandos para configurar vtp en SW-BB y se configurara en modo servidor y se nombrará el dominio como CCNP, adicionalmente se le asignara la contraseña indicada por el ejercicio:

Figura 15: configuración SW-BB

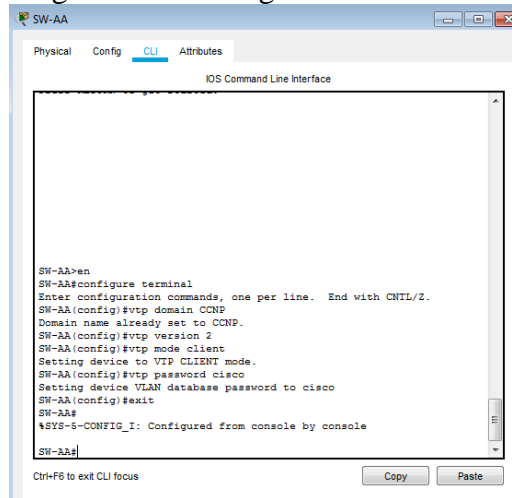


```
SW-BB>EN  
SW-BB#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SW-BB(config)#vtp domain CCNP  
Changing VTP domain name from NULL to CCNP  
SW-BB(config)#vtp version 2  
SW-BB(config)#vtp mode server  
Device mode already VTP SERVER.  
SW-BB(config)#vtp password cisco  
Setting device VLAN database password to cisco  
SW-BB(config)
```

Está configuración se repite para los SW-AA y SW-CC como clientes

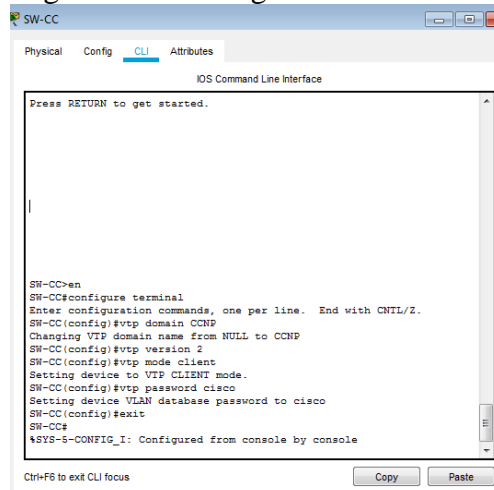
```
SW-AA>en  
SW-AA#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SW-AA(config)#vtp domain CCNP  
Domain name already set to CCNP.  
SW-AA(config)#vtp version 2  
SW-AA(config)#vtp mode client  
Setting device to VTP CLIENT mode.  
SW-AA(config)#vtp password cisco  
Setting device VLAN database password to cisco  
SW-AA(config)#exit
```

Figura 16: configuración SW-AA



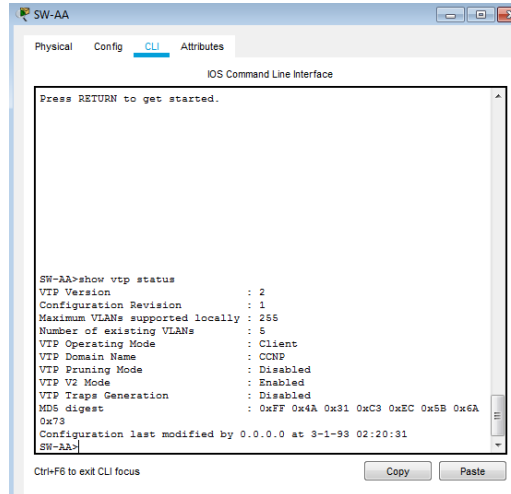
```
SW-CC>en
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#exit
```

Figura 17: configuración SW-CC



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

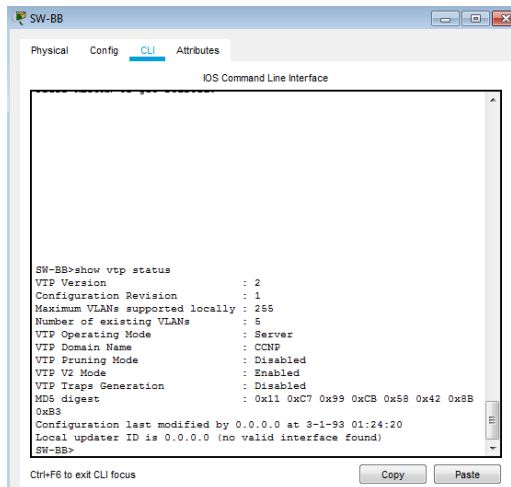
Figura 18: Verificación SW-AA



The screenshot shows the CLI of switch SW-AA. The command `show vtp status` has been executed, resulting in the following output:

```
SW-AA>show vtp status
VTP Version                : 2
Configuration Revision     : 1
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xFF 0x4A 0x31 0xC3 0xEC 0x5B 0x6A
0x79
Configuration last modified by 0.0.0.0 at 3-1-93 02:20:31
SW-AA>
```

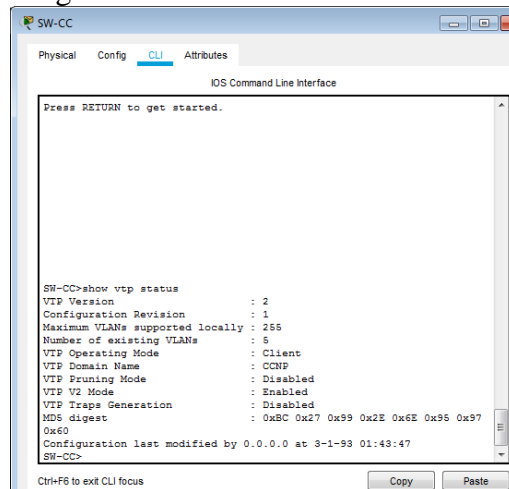
Figura 19: Verificación SW-BB



The screenshot shows the CLI of switch SW-BB. The command `show vtp status` has been executed, resulting in the following output:

```
SW-BB>show vtp status
VTP Version                : 2
Configuration Revision     : 1
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x11 0xC7 0x39 0xCB 0x58 0x42 0x8B
0xB3
Configuration last modified by 0.0.0.0 at 3-1-93 01:24:20
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB>
```

Figura 20: Verificación SW-CC



B. 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*.

Comandos para SW-AA

```
SW-AA>EN
```

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

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

```
SW-AA(config)#interface fa0/1
```

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

```
SW-AA(config-if)#
```

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

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

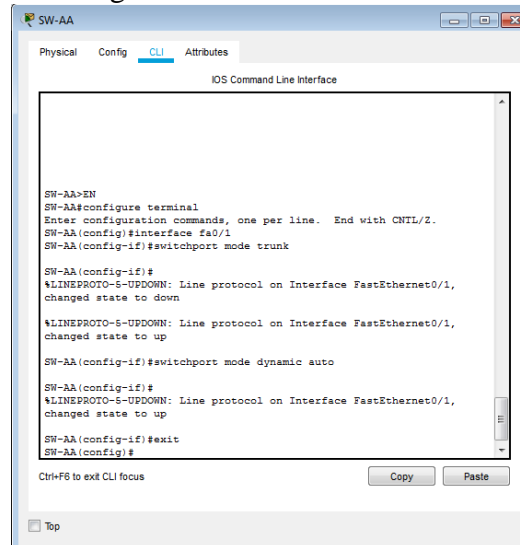
```
SW-AA(config-if)#switchport mode dynamic auto
```

```
SW-AA(config-if)#
```

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

SW-AA(config-if)#exit

Figura 21: Trunk SW-AA



Comandos para SW-BB

SW-BB>EN

SW-BB#configure terminal

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

SW-BB(config)#interface f0/1

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

SW-BB(config-if)#

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

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

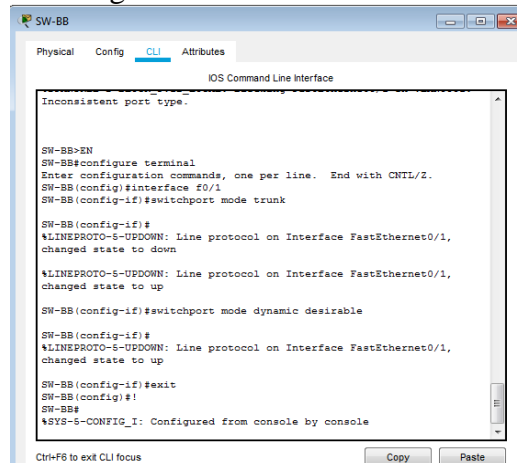
SW-BB(config-if)#switchport mode dynamic desirable

SW-BB(config-if)#

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

SW-BB(config-if)#exit

Figura 22: Trunk SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
Inconsistent port type.

SW-BB>EN
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB (config)#interface f0/1
SW-BB (config-if)#switchport mode trunk

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

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

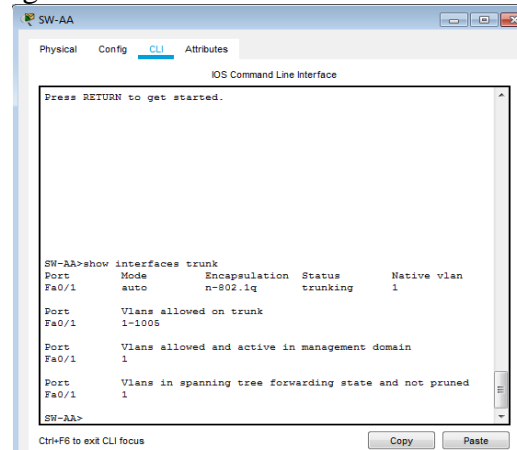
SW-BB (config-if)#
%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

SW-BB (config-if)#exit
SW-BB (config)#!
SW-BB#
%SYS-S-CONFIG_I: Configured from console by console

Ctrl+F8 to exit CLI focus
Copy Paste
```

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

Figura 23: Validación Trunk SW-AA



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

SW-AA>show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

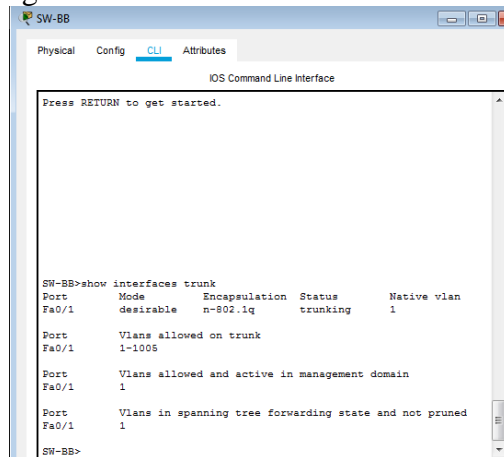
Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

SW-AA>

Ctrl+F8 to exit CLI focus
Copy Paste
```

Figura 24: Validación Trunk SWBB



6. 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

```
SW-AA>en
```

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

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

```
SW-AA(config)#interface fa0/3
```

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

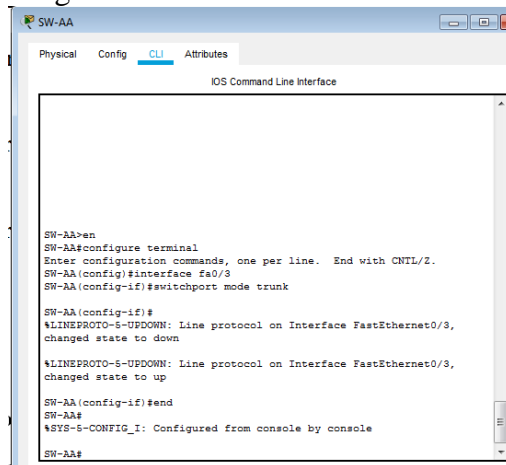
```
SW-AA(config-if)#
```

```
%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
```

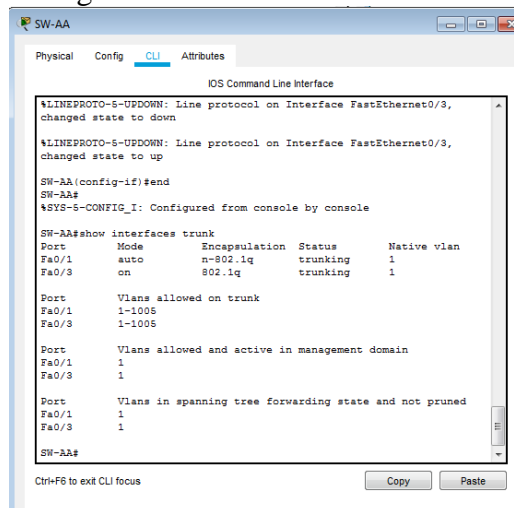
```
SW-AA(config-if)#end
```

Figura 25: Trunk estático SSAA



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

Figura 26: Verificación SSAA



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

Los comandos utilizados son:

SW-BB>en

SW-BB#configure terminal

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

SW-BB(config)#interface fa0/3


```
SW-BB(config-if)#switchport mode trunk
```

```
SW-BB(config-if)#
```

```
%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
```

```
SW-BB(config-if)#end
```

```
SW-CC>en
```

```
SW-CC#configure terminal
```

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

```
SW-CC(config)#interface fa0/1
```

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

```
SW-CC(config-if)#end
```

Figura 27: Trunk Permanente

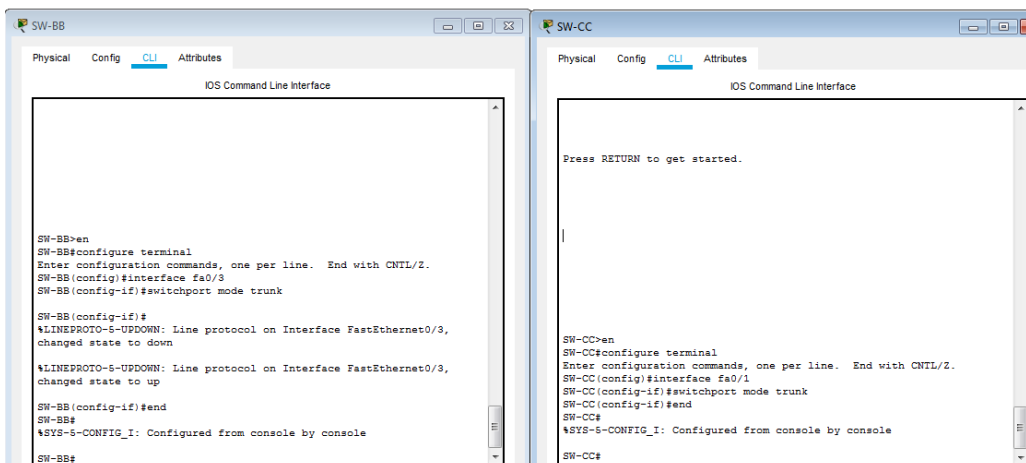
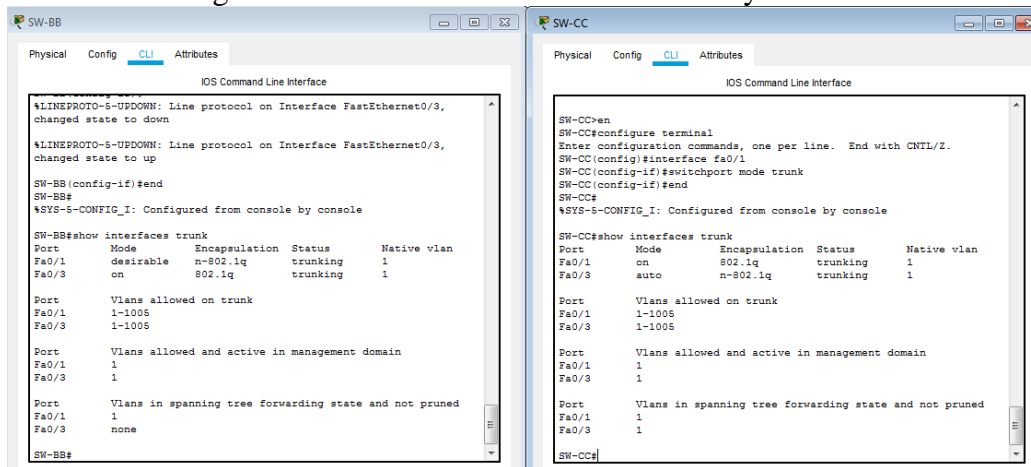


Figura 28: verificación Trunk SW-BB y SW-CC



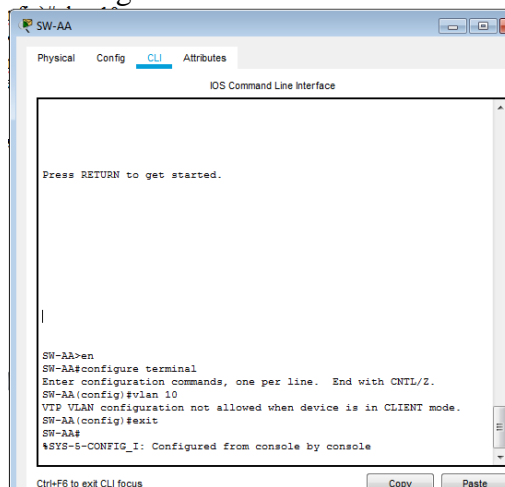
C. Agregar VLANs y asignar puertos.

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

Para SW-AA

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

Figura 29: Vlan SW-AA

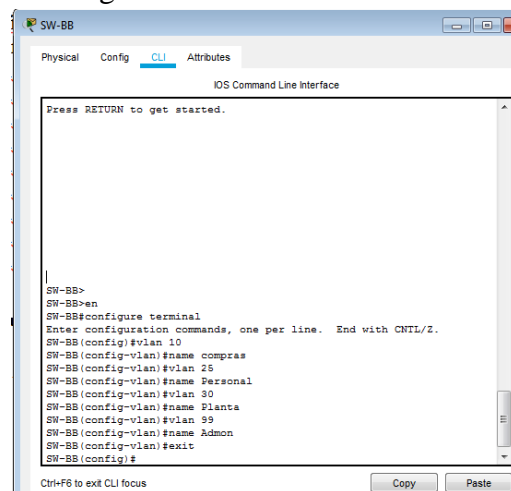


Para SW-BB se agregan las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

```
SW-BB>en
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)#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 30: Vlans SW-BB



10. Verifique que las VLANs han sido agregadas correctamente.

Para esto se utiliza el comando `show vlan brief`

Figura 31: show vlan brief

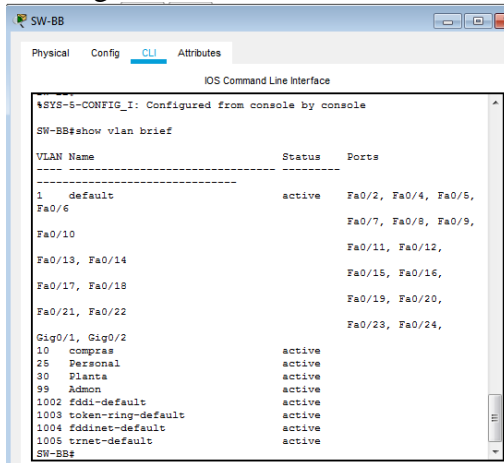


Figura 32: show vlan brief

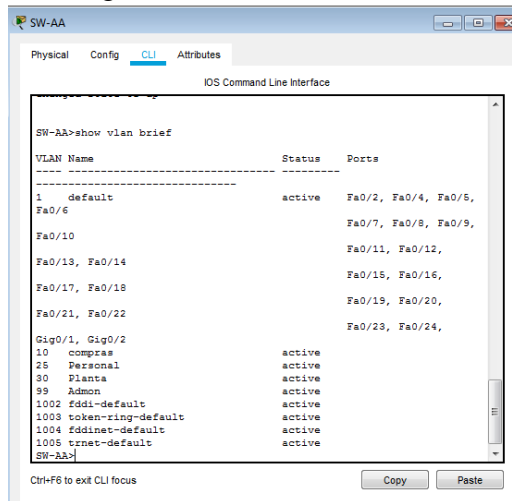
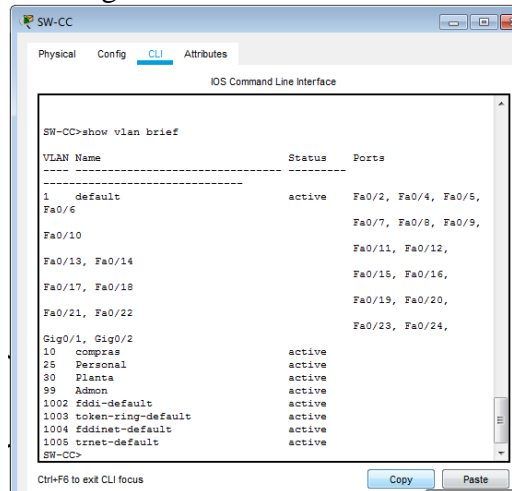


Figura 33: show vlan brief



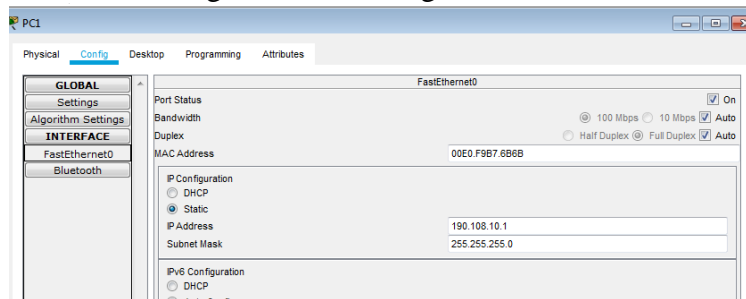
11. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla

Tabla 5: Puertos VLANs

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

Figura 34: Configuración IP



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

La lista de comandos utilizada es la siguiente:

```
SW-AA>en
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
```

```
SW-BB>en
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface f0/10
```

```
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
```

```
SW-CC>en
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
```

Figura 35: Puerto F0/10 SWAA

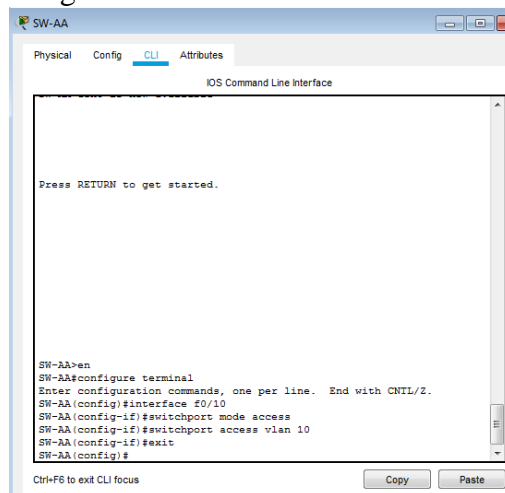


Figura 36: Puerto F0/10 SWBB

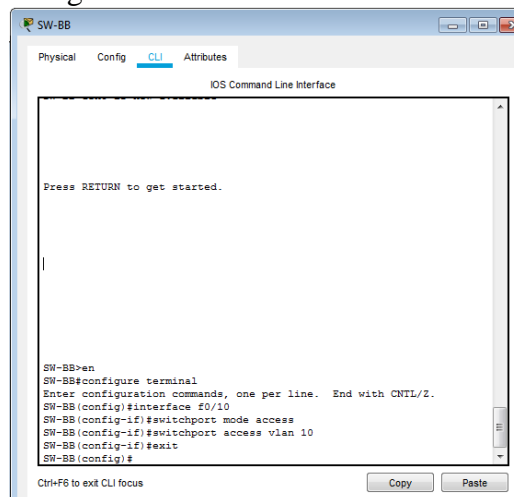
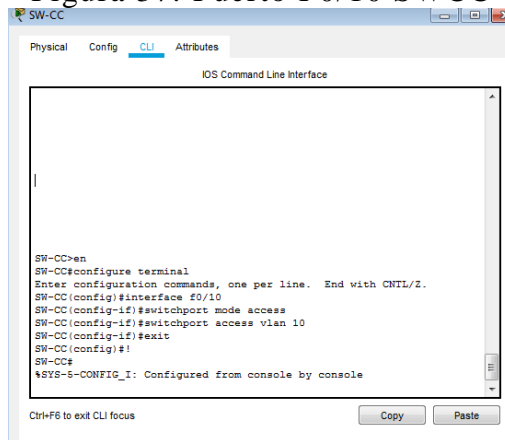


Figura 37: Puerto F0/10 SWCC



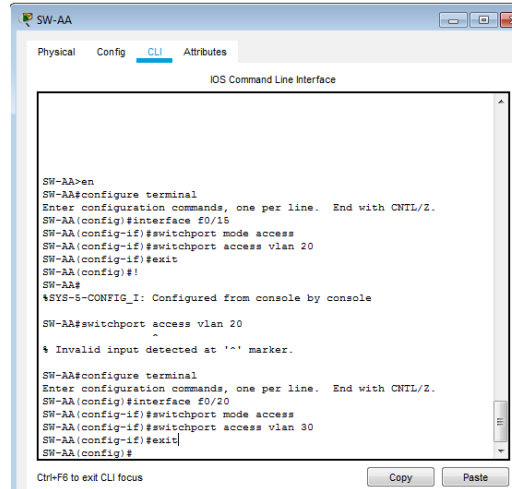
13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

La lista de comandos utilizada es la siguiente y con estos comandos se asocia las respectivas interfaces o puertos con la vlan20 y vlan30 en cada switch

```
SW-AA>en
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 20
SW-AA(config-if)#exit
SW-AA(config)#!
SW-AA#
```

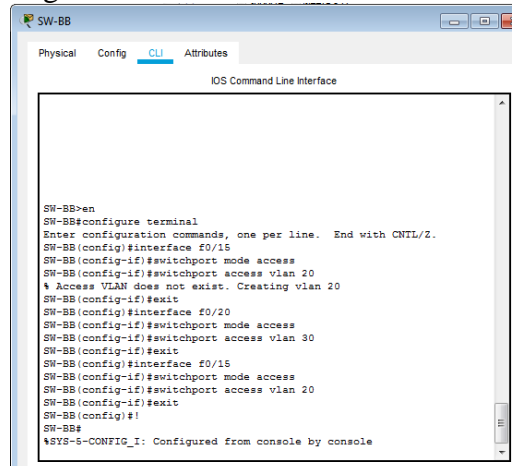
```
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
```

Figura 38: Puerto F0/15/20 SWAA



```
SW-BB>en
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-BB(config-if)#exit
SW-BB(config)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
```

Figura 39: Puerto F0/15/20 SWBB

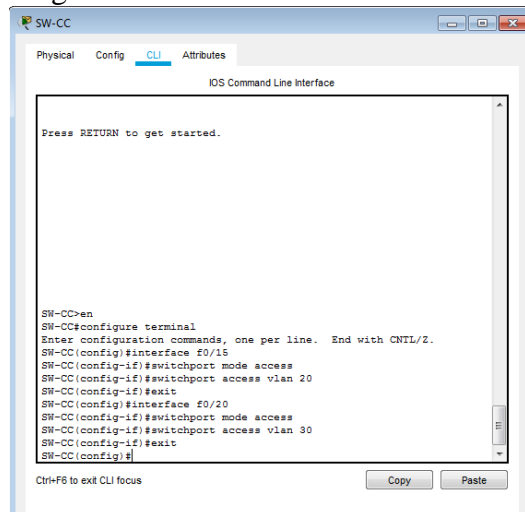


```
SW-CC>en
```



```
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 20
SW-CC(config-if)#exit
SW-CC(config)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
```

Figura 40: Puerto F0/15/20 SWCC



Configuración de las ip de los PC como lo vemos en la lista:

PC1: ip address 190.108.10.1 255.255.255.0

PC2: ip address 190.108.20.2 255.255.255.0

PC3: ip address 190.108.30.3 255.255.255.0

PC4: ip address 190.108.10.4 255.255.255.0

PC5: ip address 190.108.20.5 255.255.255.0

PC6: ip address 190.108.30.6 255.255.255.0

PC7: ip address 190.108.10.7 255.255.255.0

PC8: ip address 190.108.20.8 255.255.255.0

PC9: ip address 190.108.30.9 255.255.255.0

D. 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.

Tabla 6: Direcciones IP

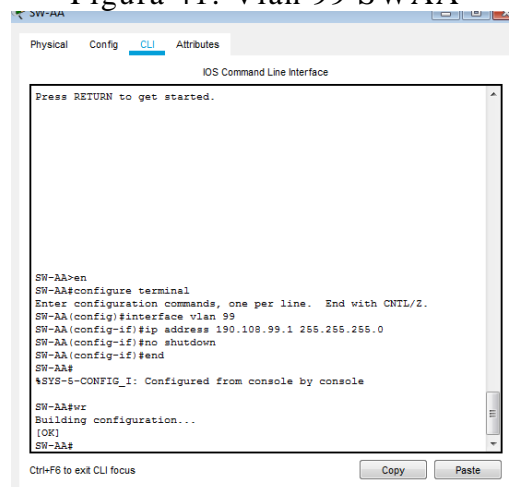
Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Comandos utilizados para la asignación de las direcciones ip se debe de agregar los comandos END y WR para que la configuración quede guardada.

```
SW-AA>en
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
SW-AA(config-if)#end
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
SW-AA#wr
```

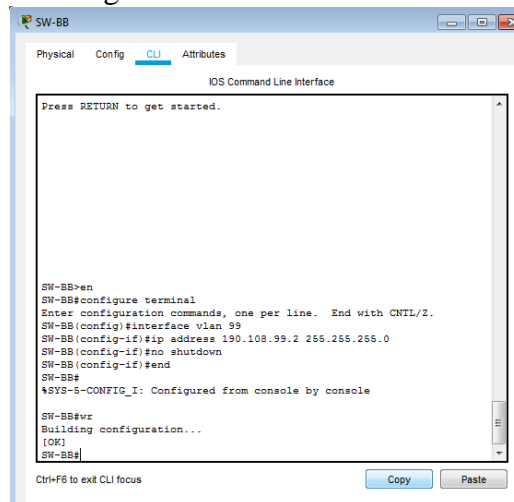
Figura 41: Vlan 99 SWAA



```
SW-BB>en
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
SW-BB(config-if)#end
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console
```

```
SW-BB#wr
```

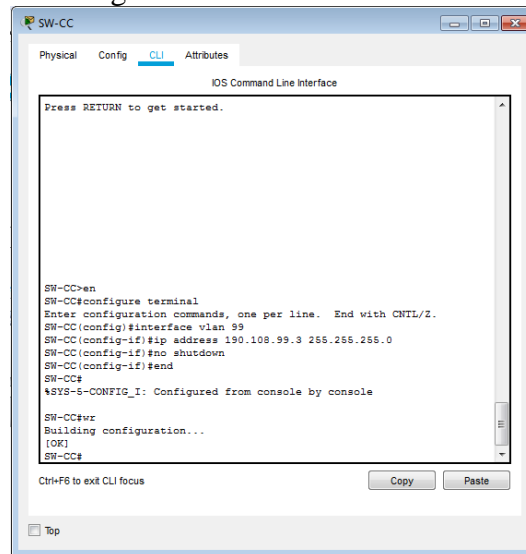
Figura 42: Vlan 99 SWBB



```
SW-CC>en
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
SW-CC(config-if)#end
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
```

```
SW-CC#wr
```

Figura 43: Vlan 99 SWBB



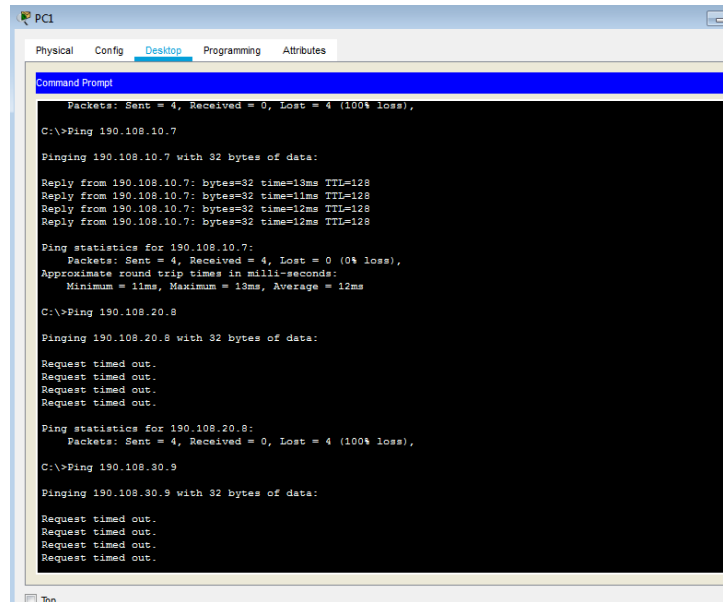
E. Verificar la conectividad Extremo a Extremo

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

Pings desde la PC 1

- Ping 190.108.20.2 fallo
- Ping 190.108.30.3 fallo
- Ping 190.108.10.4 exitoso
- Ping 190.108.20.5 fallo
- Ping 190.108.30.6 fallo
- Ping 190.108.10.7 exitoso
- Ping 190.108.20.8 fallo
- Ping 190.108.30.9 fallo

Figura 44: Pings PC1

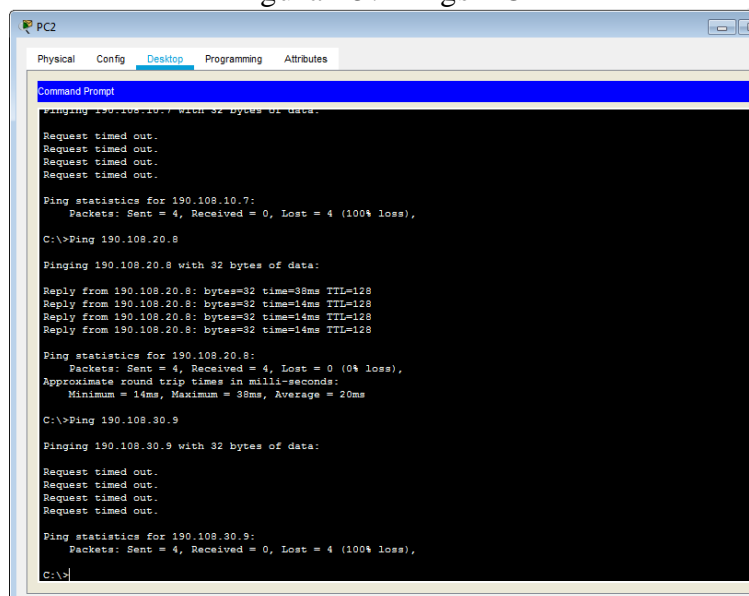


```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.10.7
Pinging 190.108.10.7 with 32 bytes of data:
Reply from 190.108.10.7: bytes=32 time=13ms TTL=128
Reply from 190.108.10.7: bytes=32 time=11ms TTL=128
Reply from 190.108.10.7: bytes=32 time=12ms TTL=128
Reply from 190.108.10.7: bytes=32 time=12ms TTL=128
Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms
C:\>Ping 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Pings desde la PC 2

- Ping 190.108.10.1 fallo
- Ping 190.108.30.3 fallo
- Ping 190.108.10.4 fallo
- Ping 190.108.20.5 exitoso
- Ping 190.108.30.6 fallo
- Ping 190.108.10.7 fallo
- Ping 190.108.20.8 exitoso
- Ping 190.108.30.9 fallo

Figura 45: Pings PC2

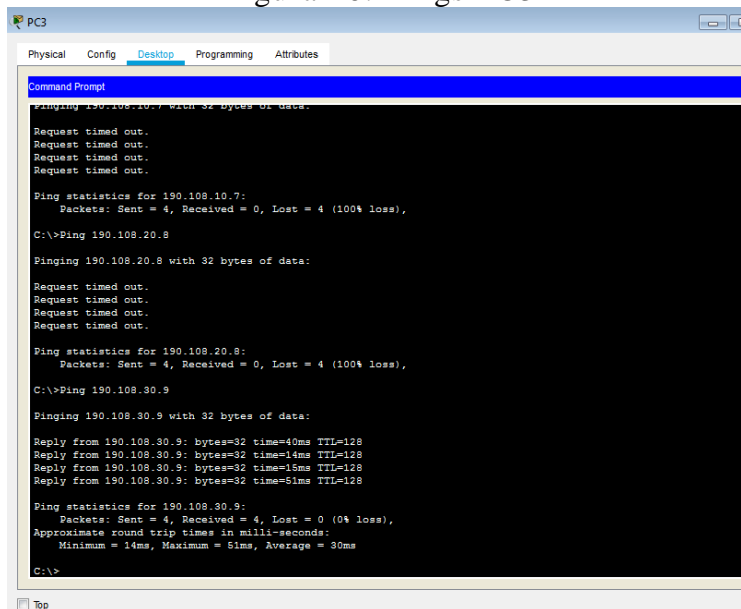


```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Reply from 190.108.20.8: bytes=32 time=38ms TTL=128
Reply from 190.108.20.8: bytes=32 time=14ms TTL=128
Reply from 190.108.20.8: bytes=32 time=14ms TTL=128
Reply from 190.108.20.8: bytes=32 time=14ms TTL=128
Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 38ms, Average = 20ms
C:\>Ping 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Pings desde la PC 3

Ping 190.108.10.1 fallo
Ping 190.108.20.2 fallo
Ping 190.108.10.4 fallo
Ping 190.108.20.5 fallo
Ping 190.108.30.6 exitoso
Ping 190.108.10.7 fallo
Ping 190.108.20.8 fallo
Ping 190.108.30.9 exitoso

Figura 46: Pings PC3

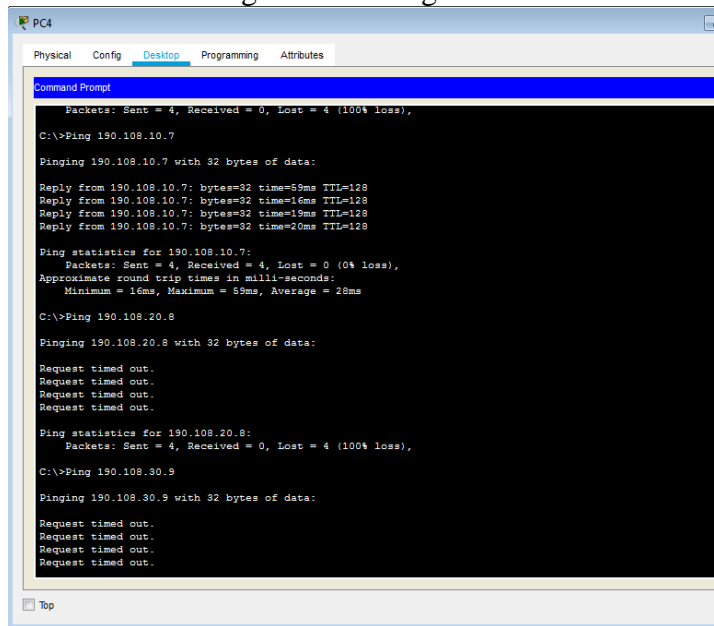


```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Reply from 190.108.30.9: bytes=32 time=40ms TTL=128
Reply from 190.108.30.9: bytes=32 time=14ms TTL=128
Reply from 190.108.30.9: bytes=32 time=15ms TTL=128
Reply from 190.108.30.9: bytes=32 time=51ms TTL=128
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 51ms, Average = 30ms
C:\>
```

Pings desde la PC 4

Ping 190.108.10.1 exitoso
Ping 190.108.20.2 fallo
Ping 190.108.30.3 fallo
Ping 190.108.20.5 fallo
Ping 190.108.30.6 fallo
Ping 190.108.10.7 exitoso
Ping 190.108.20.8 fallo
Ping 190.108.30.9 fallo

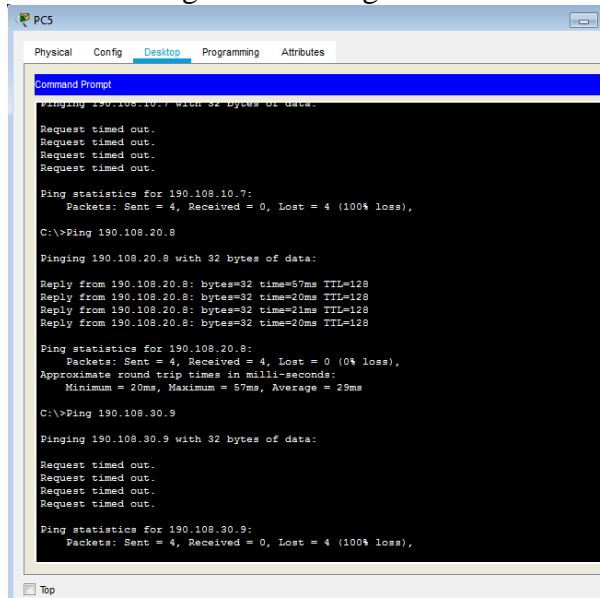
Figura 47: Pings PC4



Pings desde la PC 5

- Ping 190.108.10.1 fallo
- Ping 190.108.20.2 exitoso
- Ping 190.108.30.3 fallo
- Ping 190.108.10.4 fallo
- Ping 190.108.30.6 fallo
- Ping 190.108.10.7 fallo
- Ping 190.108.20.8 exitoso
- Ping 190.108.30.9 fallo

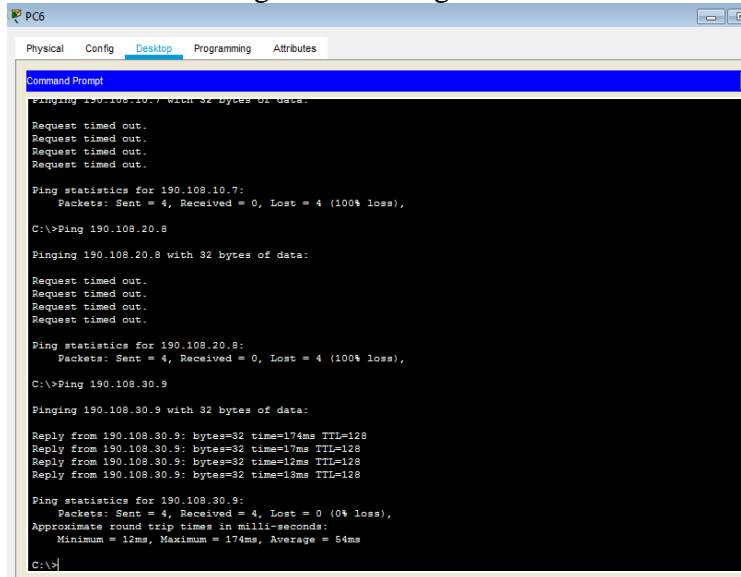
Figura 48: Pings PC5



Pings desde la PC 6

Ping 190.108.10.1 fallo
Ping 190.108.20.2 fallo
Ping 190.108.30.3 exitoso
Ping 190.108.10.4 fallo
Ping 190.108.20.5 fallo
Ping 190.108.10.7 fallo
Ping 190.108.20.8 fallo
Ping 190.108.30.9 exitoso

Figura 49: Pings PC6



```
PC6
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>Ping 190.108.20.8

Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>Ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:
Reply from 190.108.30.9: bytes=32 time=174ms TTL=128
Reply from 190.108.30.9: bytes=32 time=17ms TTL=128
Reply from 190.108.30.9: bytes=32 time=12ms TTL=128
Reply from 190.108.30.9: bytes=32 time=13ms TTL=128

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 174ms, Average = 54ms

C:\>
```

Pings desde la PC 7

Ping 190.108.10.1 exitoso
Ping 190.108.20.2 fallo
Ping 190.108.30.3 fallo
Ping 190.108.10.4 exitoso
Ping 190.108.20.5 fallo
Ping 190.108.30.6 fallo
Ping 190.108.20.8 fallo
Ping 190.108.30.9 fallo

Figura 50: Pings PC7

```
PC7
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.4 with 32 bytes of data:
Reply from 190.108.10.4: bytes=32 time=42ms TTL=128
Reply from 190.108.10.4: bytes=32 time=15ms TTL=128
Reply from 190.108.10.4: bytes=32 time=15ms TTL=128
Reply from 190.108.10.4: bytes=32 time=15ms TTL=128
Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 42ms, Average = 22ms
C:\>Ping 190.108.20.5
Pinging 190.108.20.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.30.6
Pinging 190.108.30.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pings desde la PC 8

- Ping 190.108.10.1 fallo
- Ping 190.108.20.2 exitoso
- Ping 190.108.30.3 fallo
- Ping 190.108.10.4 fallo
- Ping 190.108.20.5 exitoso
- Ping 190.108.30.6 fallo
- Ping 190.108.10.7 fallo
- Ping 190.108.30.9 fallo

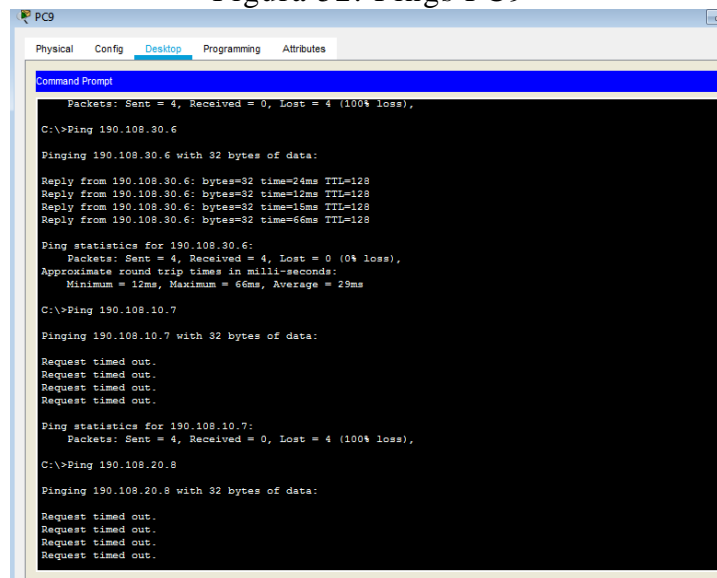
Figura 51: Pings PC8

```
PC8
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.20.5
Pinging 190.108.20.5 with 32 bytes of data:
Reply from 190.108.20.5: bytes=32 time=37ms TTL=128
Reply from 190.108.20.5: bytes=32 time=19ms TTL=128
Reply from 190.108.20.5: bytes=32 time=13ms TTL=128
Reply from 190.108.20.5: bytes=32 time=17ms TTL=128
Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 37ms, Average = 21ms
C:\>Ping 190.108.30.6
Pinging 190.108.30.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pings desde la PC 9

Ping 190.108.10.1 fallo
Ping 190.108.20.2 fallo
Ping 190.108.30.3 exitoso
Ping 190.108.10.4 fallo
Ping 190.108.20.5 fallo
Ping 190.108.30.6 exitoso
Ping 190.108.10.7 fallo
Ping 190.108.20.8 fallo

Figura 52: Pings PC9



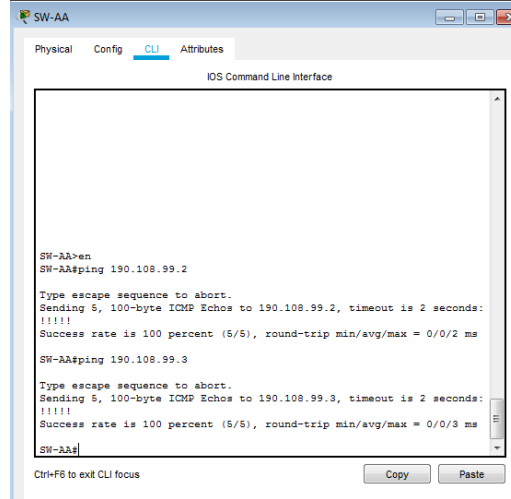
```
PC9
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.30.6
Pinging 190.108.30.6 with 32 bytes of data:
Reply from 190.108.30.6: bytes=32 time=24ms TTL=128
Reply from 190.108.30.6: bytes=32 time=12ms TTL=128
Reply from 190.108.30.6: bytes=32 time=15ms TTL=128
Reply from 190.108.30.6: bytes=32 time=66ms TTL=128
Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 66ms, Average = 29ms
C:\>Ping 190.108.10.7
Pinging 190.108.10.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>Ping 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

De todos los pings realizados solo seis(6) tuvieron éxito de respuesta, esto debido a que existen tres (3) vlans diferentes las cuales son 10,20 y 30 y tres equipos se conecta a través de cada una de estas, por consiguiente solo responde los equipos que están en la misma vlan.

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

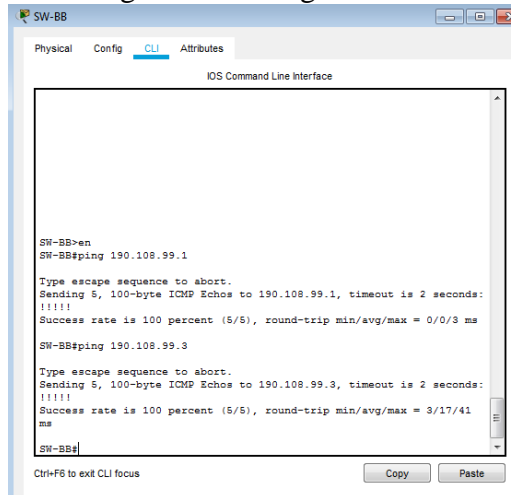
Ping desde el SW-AA ping 190.108.99.2 ping 190.108.99.3

Figura 53: Pings SWAA



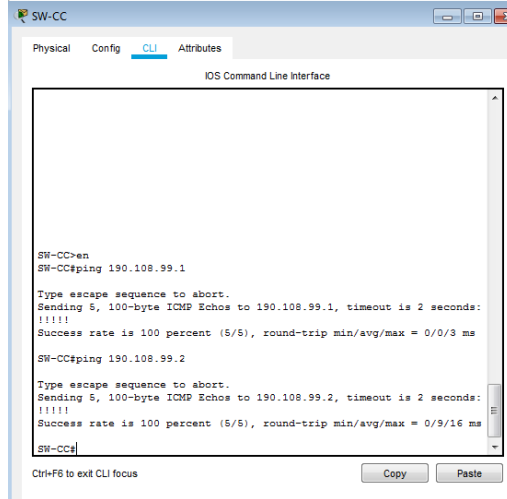
Ping desde el SW-BB ping 190.108.99.1 ping 190.108.99.3

Figura 54: Pings SWBB



Ping desde el SW-CC ping 190.108.99.1 ping 190.108.99.2

Figura 55: Pings SWCC



Los pings ejecutados desde cada switch a los demás fueron exitosos, dado a que estos están comunicados mediante la vlan 99 Admon y poseen su respectivas direcciones ip.

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

- PC1: Ping 190.108.10.1
- PC2: Ping 190.108.20.2
- PC3: Ping 190.108.30.3
- PC4: Ping 190.108.10.4
- PC5: Ping 190.108.20.5
- PC6: Ping 190.108.30.6
- PC7: Ping 190.108.10.7
- PC8: Ping 190.108.20.8
- PC9: Ping 190.108.30.9

Figura 56: Pings SWAA a PCS

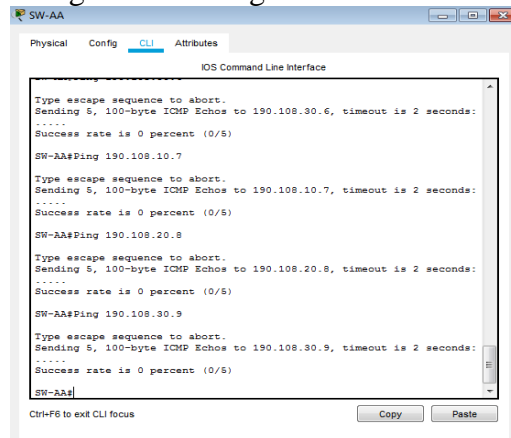


Figura 57: Pings SWBB a PCS

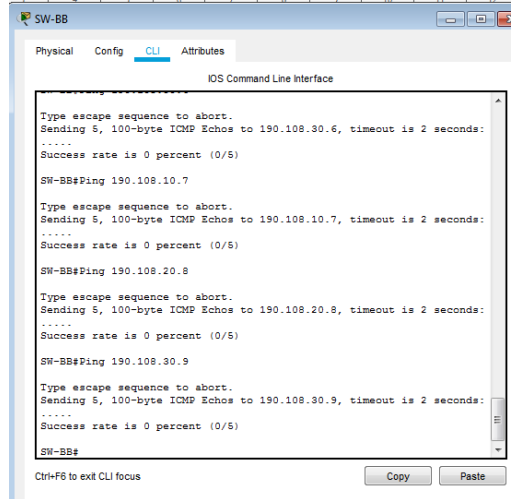
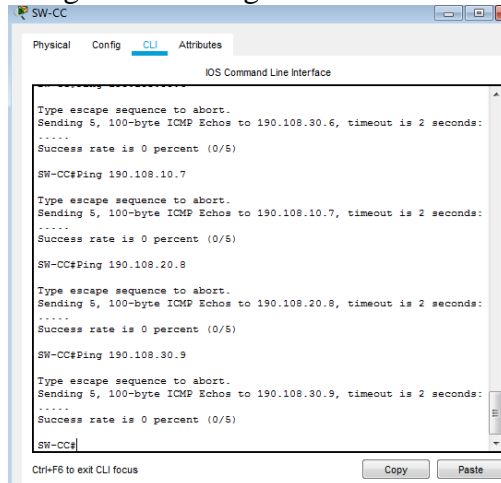


Figura 58: Pings SWCC a PCS



Ninguna de las pruebas ping tuvo éxito, esto debido a que se encuentran en vlans diferentes dado que los switches están en la vlan 99 y los pc están en la vlans 10,20 y 30 por consiguiente no hay comunicación.

CONCLUSIONES

Con el desarrollo de la presente actividad se puede demostrar los conocimientos adquiridos a lo largo de las actividades que se desarrollaron sobre CCNP R&S route y CCNP R&S switch, logrando resolver las actividades propuestas en la prueba de habilidades.

Demostrando tal competencia en la programación adecuada tanto de los routers como de los switches mediante los comandos indicados para resolver los escenarios propuestos de tal manera que cumplieran con los requerimientos solicitados.

Finalmente se evidenció con algunos comandos como comandos ping, traceroute, show ip route, entre otros que permitieron evidenciar las configuraciones realizadas y observar si hay o no comunicación entre los dispositivos.

REFERENCIAS BIBLIOGRÁFICA

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Security. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

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>

UNAD (2015). Switch CISCO Security Management [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IlyVeVJCCezJ2QE5c>