

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

DEIVIS STIVEN OSORIO CLAVIJO

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

DEIVIS STIVEN OSORIO CLAVIJO

Diplomado de opción de grado presentado para optar el título de INGENIERO  
ELECTRÓNICO

MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Popayán, 22 de Mayo del 2020

## **AGRADECIMIENTOS**

Quiero empezar agradeciendo a las personas que me acompañaron y apoyaron en todo el transcurso de esta carrera ya que sin su colaboración constante no hubiese sido posible culminar esta etapa de mi vida. De igual forma, agradezco a cada uno de mis tutores por brindarme su acompañamiento en el desarrollo de las actividades propuestas ya que fueron espacios de gran enriquecimiento tanto personal como profesional.

## TABLA DE CONTENIDO

AGRADECIMIENTOS.....	4
TABLA DE CONTENIDO .....	5
LISTADO DE TABLAS.....	6
LISTADO DE FIGURAS.....	7
GLOSARIO .....	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN.....	12
DESARROLLO .....	13
1. Escenario 1 .....	13
2. Escenario 2 .....	26
CONCLUSIONES .....	46
REFERENCIAS BIBLIOGRÁFICAS.....	47

## Listado de Tablas

Tabla 1 Configuración R1 .....	13
Tabla 2 Configuración R2 .....	13
Tabla 3 Configuración R3 .....	14
Tabla 4 Configuración R4 .....	14
Tabla 5 Asociación de puertos VLAN .....	33
Tabla 6 Direcciones IP Switches.....	38
Tabla 7 SW-AA VLAN 99.....	39
Tabla 8 SW-BB VLAN 99.....	39

## Listado de Figuras

Figura 1 Configuración R1 .....	15
Figura 2 Configuración R2 .....	16
Figura 3 Salida del comando show ip route. ....	17
Figura 4 Salida del comando show ip route R2.....	18
Figura 5 relación de vecino BGP R2.....	18
Figura 6 relación de vecino BGP R3.....	19
Figura 7 salida Show IP Route punto 2.....	20
Figura 8 Salida show IP Route punto 2 R3 .....	21
Figura 9 relación vecino BGP punto 3 R3.....	21
Figura 10 relación vecino BGP punto 3 R4.....	22
Figura 11 configuración adicional 1 .....	23
Figura 12 configuración adicional 2 .....	23
Figura 13 salida show IP Route punto 3 .....	24
Figura 14 salida show IP Route punto 3 R4.....	25
Figura 15 escenario final completado .....	25
Figura 16 Escenario 2 primera impresión .....	26
Figura 17 SW-AA Client.....	27
Figura 18 SW-BB Server .....	27
Figura 19 SW-CC Client .....	27
Figura 20 show ip status SW-AA .....	28
Figura 21 show ip status SW-BB .....	28
Figura 22 show ip status SW-CC.....	28
Figura 23 trunk SW-BB .....	29
Figura 24 trunk SW-AA show interfaces trunk .....	29
Figura 25 trunk SW-BB show interfaces trunk .....	30
Figura 26 SW-AA switchport mode trunk .....	30
Figura 27 show interfaces trunk SW-AA .....	30
Figura 28 configuración trunk SW-CC .....	31
Figura 29 show interface trunk SW-CC.....	31
Figura 30 show interface trunk SW-BB.....	31
Figura 31 Adición de VLANs SW-BB .....	32
Figura 32 verificación de VLANs en SW-AA .....	32
Figura 33 verificación de VLANs en SW-BB .....	33
Figura 34 verificación de VLANs en SW-CC.....	33
Figura 35 Asociación de puertos VLAN SW-AA.....	34
Figura 36 Configuración PC-1.....	34
Figura 37 configuración PC-2 .....	34
Figura 38 configuración PC-3 .....	35
Figura 39 Asociación de puertos VLAN SW-BB.....	35
Figura 40 configuración PC-4 .....	35
Figura 41 configuración PC-5 .....	36
Figura 42 configuración PC-6 .....	36
Figura 43 Asociación de puertos VLAN SW-CC .....	36

Figura 44 configuración PC-7 .....	37
Figura 45 configuración PC-8 .....	37
Figura 46 configuración PC-9 .....	37
Figura 47 Asignación VLAN 10 SW-AA .....	38
Figura 48 Asignación VLAN 10 SW-BB .....	38
Figura 49 Asignación VLAN 10 SW-CC .....	38
Figura 50 SW-CC VLAN 99 .....	39
Figura 51 Verificación de PC ping 1.....	40
Figura 52 Verificación de PC ping 2.....	41
Figura 53 Verificación de PC ping 3.....	42
Figura 54 Switch Ping 1 .....	43
Figura 55 Switch Ping 2 .....	43
Figura 56 Switch Ping 2 .....	43
Figura 57 Switch a PC ping 1.....	44
Figura 58 Switch a PC ping 2.....	45



## GLOSARIO

- CISCO:** es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
- CCNP:** es una certificación de CISCO que por sus siglas Cisco Certified Network Professional (CCNP) significan certificación de enrutamiento y conmutación, el cual valida la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia y trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, inalámbrica y video.
- Conmutación:** es conocida como la acción de un extremo a extremo entre dos puntos, emisor (TX) y un receptor (RX) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.
- Electrónica:** es una rama de la educación el cual implica la física, la ingeniería, tecnología y las aplicaciones que tratan con la emisión, el flujo y el control de los electrones u otras partículas cargadas eléctricamente en el vacío y la materia.
- Enrutamiento:** también definida como encaminamiento, esta es la encargada de un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.
- Redes:** es un término muy ambiguo y también muy amplio en cuanto a sus derivadas, ya que es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios

## RESUMEN

El contenido programático desarrollado durante la carrera, el diplomado de profundización CISCO CCNP y el trabajo en sí, nos preparó a los estudiantes para la instalación, configuración, administración y para mí lo más importante la resolución de problemas en redes pequeñas y empresariales, LAN y WAN, este trabajo se desarrolló en conjunto con el soporte constante de especialistas del área, con el fin de mejorar las habilidades obtenidas y trabajar de manera independiente en el diseño de redes complejas. Esa actividad afianzó los conocimientos sobre protocolos de enrutamiento avanzados como IGRP, RIP, OSPF, se utilizó tanto el direccionamiento IPV4 e IPV6, y sobre todo se hizo especial énfasis en la seguridad un tema que está tomando demasiada importancia y que cada día es relevante a momento del diseño de una red. El presente trabajo valida estas habilidades y nos da una visión más clara de lo que muy posiblemente nos vamos a enfrentar, además es la mejor manera de evaluar los conocimientos adquiridos a través del desarrollo de los módulos que componen el curso, así como la formación autodidacta que el curso demanda.

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

## **ABSTRACT**

The programmatic content developed during the degree, the CISCO CCNP deepening diploma and the work itself, prepared the students for the installation, configuration, administration and for me the most important problem solving in small and business networks, LAN and WAN, this work was developed in conjunction with the constant support of specialists in the area, in order to improve the skills obtained and work independently in the design of complex networks. This activity strengthened the knowledge about advanced routing protocols such as IGRP, RIP, OSPF, both IPV4 and IPV6 addressing were used, and above all, special emphasis was placed on security, an issue that is becoming too important and that is relevant every day. moment of network design. This work validates these skills and gives us a clearer vision of what we are very likely to face, it is also the best way to assess the knowledge acquired through the development of the modules that make up the course, as well as self-taught training. that the course demands.

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

## INTRODUCCIÓN

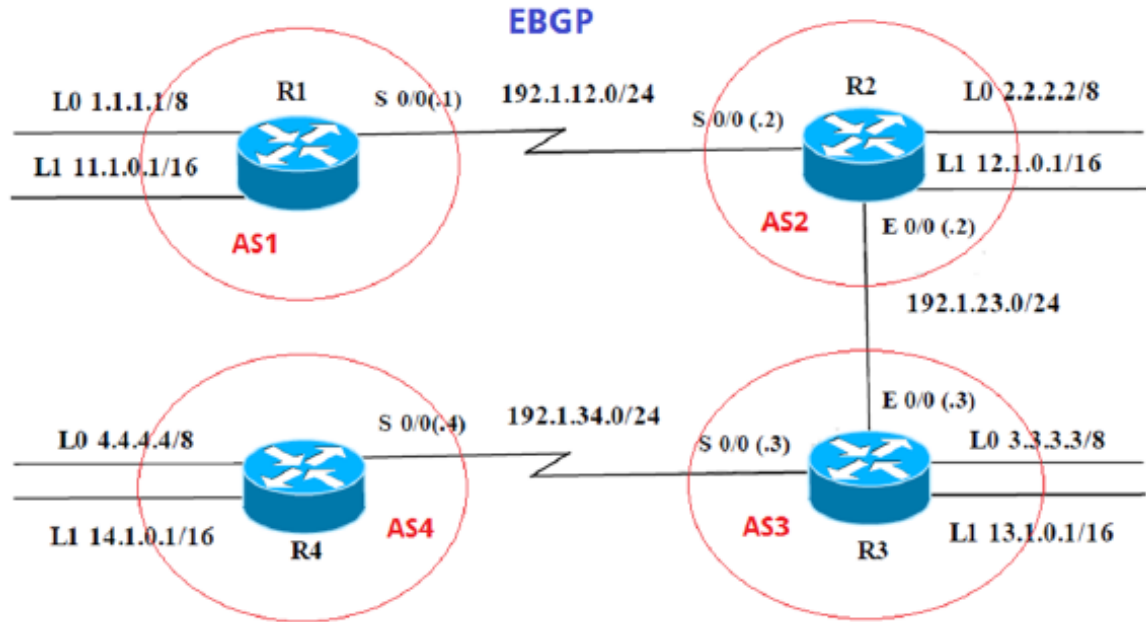
La prueba de habilidades prácticas propuesta por el curso del diplomado de profundización en CISCO CCNP, el cual se desarrolla en el presente documento, se contemplan dos escenarios de gran nivel de complejidad donde abarca la configuración por parte de Routers y Switch; de tal manera que se visualizara la correcta solución y explicación de los mismos con sus respectivas líneas de comandos.

En el escenario 1 se trabaja un protocolo de ruteo BGP, el cual es muy utilizado en sistemas autónomos y básicos para la configuración de Routers, en donde se aplica mediante un protocolo exterior que de una u otra manera es enfocado de tipo path Vector y Hierarchy Required. De esta manera se entiende que como primer ejercicio es la establecer comunicación con el vecino a través de los Routers y sus correspondientes Loopbacks siendo la principal actividad del primer escenario.

Para el segundo ejercicio Escenario 2, se contemplan que el principal objetivo es implementar una configuración troncal entre los diferentes Switch que se presentan en el diseño de red; estos Switch son direccionados por las diferentes interfaces de las VLANS con el apoyo de la configuración VTP (Vlan Trunking Protocol); teniendo como resultado la administración y configuración de VLANS de los diferentes dispositivos que se tienen en el segundo escenario.

## DESARROLLO

### 1. ESCENARIO 1



Información para 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 Configuración R1

#### 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 Configuración R2

### 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 Configuración R3*

### 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 Configuración R4*

## SOLUCION EJERCICIO

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**.

## Configuración de R1

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#interface Loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

R1(config-if)#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)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

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

R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 0/1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#exit
R1(config)#
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#exit
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 1 Configuración R1

## Configuración R2



```
R2>
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Loopback 0

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

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

R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1

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

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

R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 0/1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

R2(config-if)#interfa
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to
up

^
% Invalid input detected at '^' marker.

R2(config-if)#interface Gig0/0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

R2(config-router)#exit
R2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 2 Configuración R2



A continuación, se puede evidenciar en resultado obtenido del comando show ip route, que tanto el router R1 como el router R2 contienen en su tabla de enrutamiento las direcciones de Loopback y las direcciones de las redes a las cuales se encuentran conectados de forma directa, además, de las redes configuradas en las interfaces Loopback de su respectivo router vecino.

Salida del comando **show ip route**.

```
R1>enable
R1#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
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.1.0.0/16 is directly connected, Loopback1
L       11.1.0.1/32 is directly connected, Loopback1
      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, Serial0/1/0
L       192.1.12.1/32 is directly connected, Serial0/1/0

R1#
```

---

Figura 3 Salida del comando show ip route.

```

R2>enable
R2#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
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 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
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial0/1/0
L    192.1.12.2/32 is directly connected, Serial0/1/0

R2#

```

*Figura 4 Salida del comando show ip route R2*

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

```

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#exit
R2(config)#

```

*Figura 5 relación de vecino BGP R2*

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface Loopback 0

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

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

R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1

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

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

R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface Gig0/0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up

R3(config-if)#interface serial 0/1/1
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up

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

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 6 relación de vecino BGP R3

## Salida del comando *show ip route*

```
R2>enable
R2#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
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 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, Serial0/1/0
L    192.1.12.2/32 is directly connected, Serial0/1/0
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0/0

R2#
R2#|
```

*Figura 7 salida Show IP Route punto 2*

```

R3>enable
R3#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
B    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
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
    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
B    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
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0/0

R3#
R3#

```

Figura 8 Salida show IP Route punto 2 R3

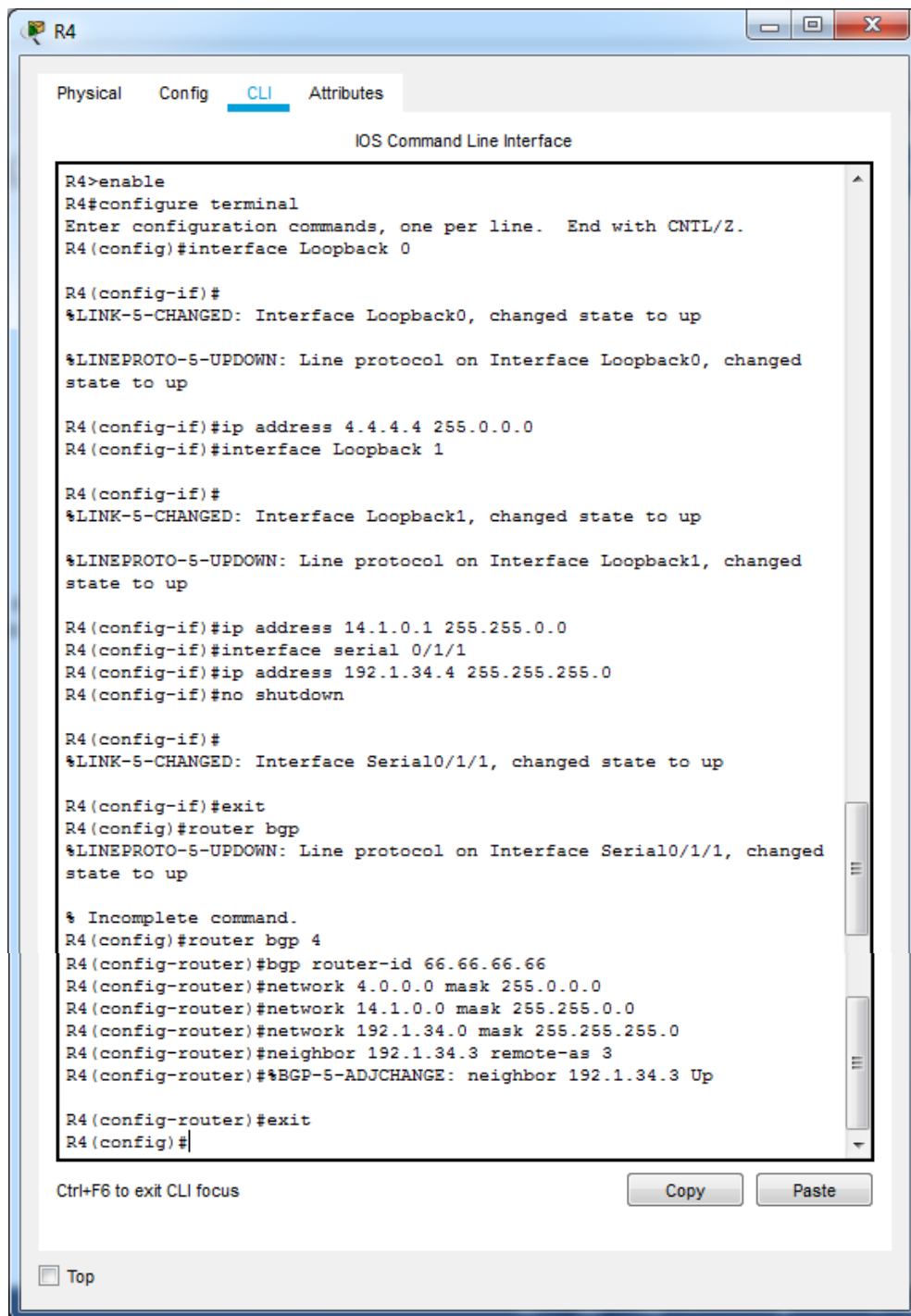
3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback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

```

R3#
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit
R3(config)#

```

Figura 9 relación vecino BGP punto 3 R3



The screenshot shows a window titled 'R4' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

```
R4>enable
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#interface Loopback 0

R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1

R4(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

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

R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 0/1/1
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown

R4(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

R4(config-if)#exit
R4(config)#router bgp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed
state to up

% Incomplete command.
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)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up

R4(config-router)#exit
R4(config)#
```

At the bottom of the window, there is a 'Ctrl+F6 to exit CLI focus' message, 'Copy' and 'Paste' buttons, and a 'Top' button.

Figura 10 relación vecino BGP punto 3 R4

## Configuración adicional

```
R3#
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#route 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)#
R3(config-router)#
```

---

Figura 11 configuración adicional 1

```
R4>enable
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#routebgp 4
      ^
% Invalid input detected at '^' marker.

R4(config)#route bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)%%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Down Neighbor
deleted

%BGP-3-NOTIFICATION: sent to neighbor 192.1.34.3 6/0 (unsupported) 0
bytes

R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#
R4(config-router)#
```

---

Figura 12 configuración adicional 2

## Salida de comando **Show ip route**

```
R3#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
B    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
S    4.0.0.0/8 [1/0] via 192.1.34.4
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     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
B    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
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/1/1
L    192.1.34.3/32 is directly connected, Serial0/1/1

R3#
```

Figura 13 salida show IP Route punto 3



```

R4#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

S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
C    14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/1/1
L    192.1.34.4/32 is directly connected, Serial0/1/1

R4#

```

Figura 14 salida show IP Route punto 3 R4

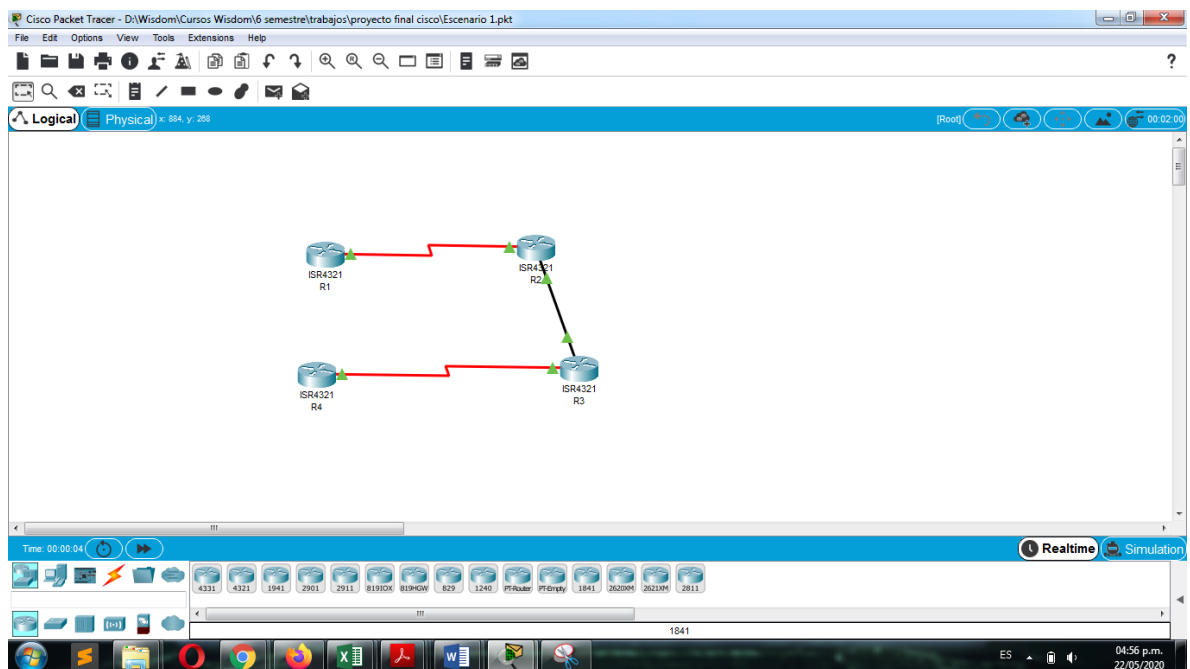
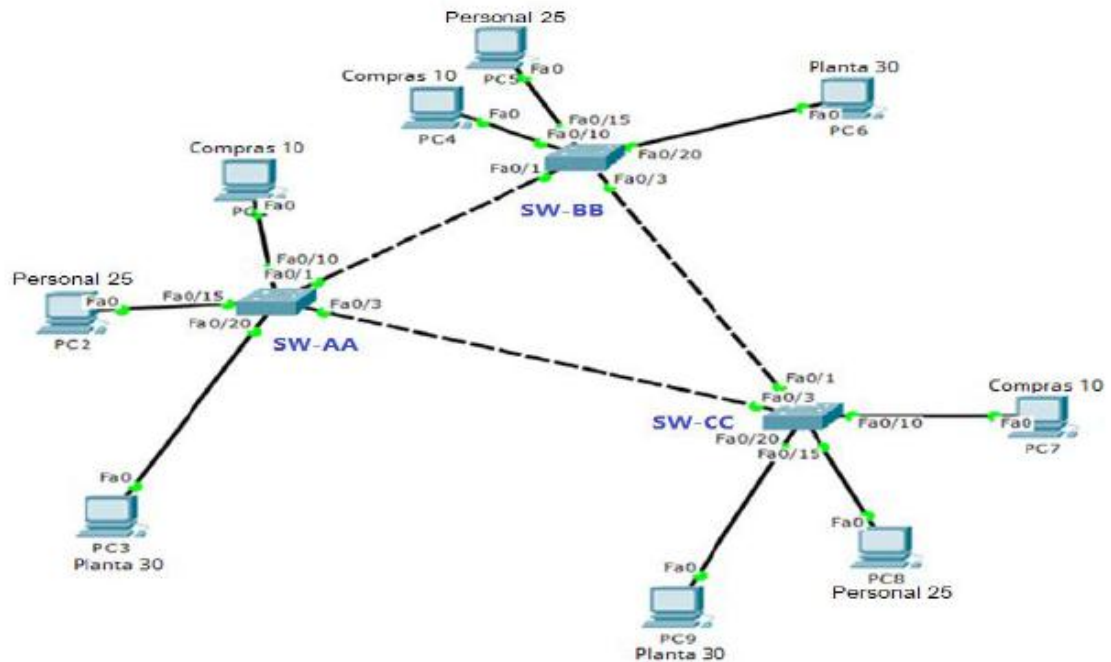


Figura 15 escenario final completado

## 2. Escenario 2



### A. Configurar VTP

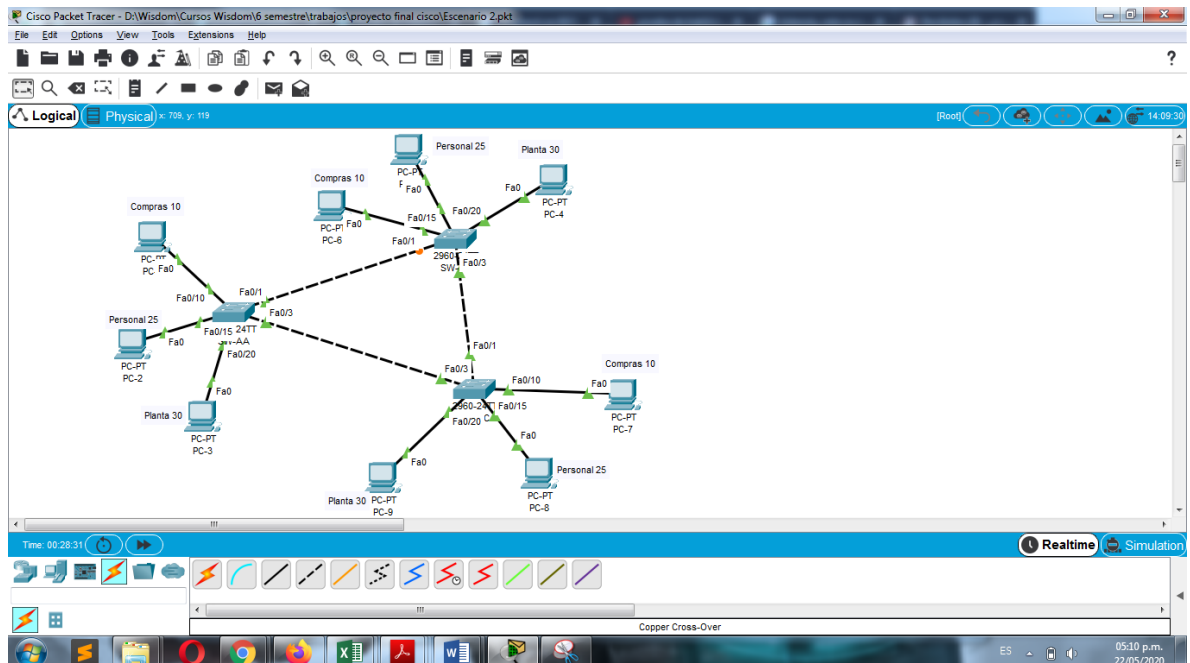


Figura 16 Escenario 2 primera impresión

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

*Figura 17 SW-AA Client*

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

*Figura 18 SW-BB Server*

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

*Figura 19 SW-CC Client*

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

```
SW-AA#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#
SW-AA#
```

Figura 20 show ip status SW-AA

```
SW-BB#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode         : Server
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 21 show ip status SW-BB

```
SW-CC#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MDS digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
SW-CC#
```

Figura 22 show ip status 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**.

```
SW-BB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface Fa0/1
SW-BB(config-if)#switchport mode dynamic desirable

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

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

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

Figura 23 trunk SW-BB

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

```
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#
```

Figura 24 trunk SW-AA show interfaces trunk

```

SW-BB#show interfaces trunk
Port      Mode           Encapsulation  Status      Native vlan
Fa0/1     desirable     n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

SW-BB#

```

Figura 25 trunk SW-BB show interfaces trunk

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#
SW-AA#conf t
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)#

```

Figura 26 SW-AA switchport mode trunk

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

```

SW-AA#show interfaces trunk
Port      Mode           Encapsulation  Status      Native vlan
Fa0/1     auto           n-802.1q       trunking    1
Fa0/3     on             802.1q         trunking    1

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

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1

SW-AA#

```

Figura 27 show interfaces trunk SW-AA

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

```
SW-CC#conf t
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)#
%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-CC(config-if)#
```

Figura 28 configuración trunk SW-CC

```
SW-CC#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/3     auto      n-802.1q      trunking    1

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

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1

SW-CC#
```

Figura 29 show interface trunk SW-CC

```
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q      trunking    1
Fa0/3     auto      n-802.1q      trunking    1

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

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
Fa0/3     1

SW-BB#
```

Figura 30 show interface trunk SW-BB

### 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).

```
SW-BB#
SW-BB#conf t
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
SW-BB(config)#
```

Figura 31 Adición de VLANs SW-BB

10. Verifique que las VLANs han sido agregadas correctamente.

```
SW-AA#
SW-AA#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   compras                active
25   personal                active
30   planta                  active
99   admon                   active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default         active
SW-AA#
```

Figura 32 verificación de VLANs en SW-AA



```

SW-BB#
SW-BB#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   compras                active
25   personal                active
30   planta                  active
99   admon                   active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
SW-BB#

```

Figura 33 verificación de VLANs en SW-BB

```

SW-CC#
SW-CC#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   compras                active
25   personal                active
30   planta                  active
99   admon                   active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
SW-CC#

```

Figura 34 verificación de VLANs en SW-CC

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

Tabla 5 Asociación de puertos VLAN

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 20	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

```

SW-AA#
SW-AA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#int fa0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int fa0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int fa0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#

```

Figura 35 Asociación de puertos VLAN SW-AA

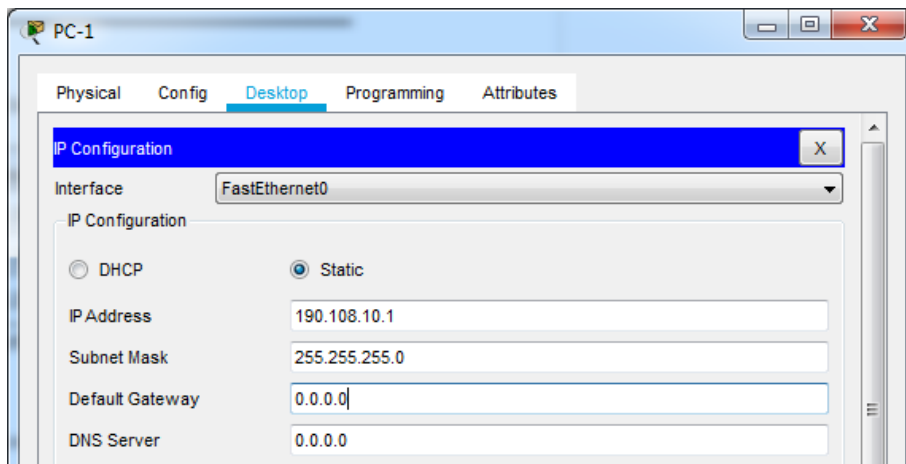


Figura 36 Configuración PC-1

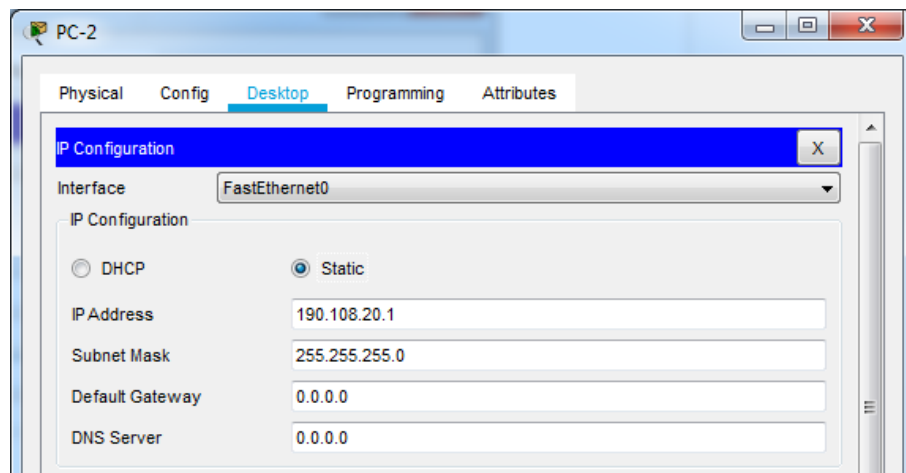


Figura 37 configuración PC-2

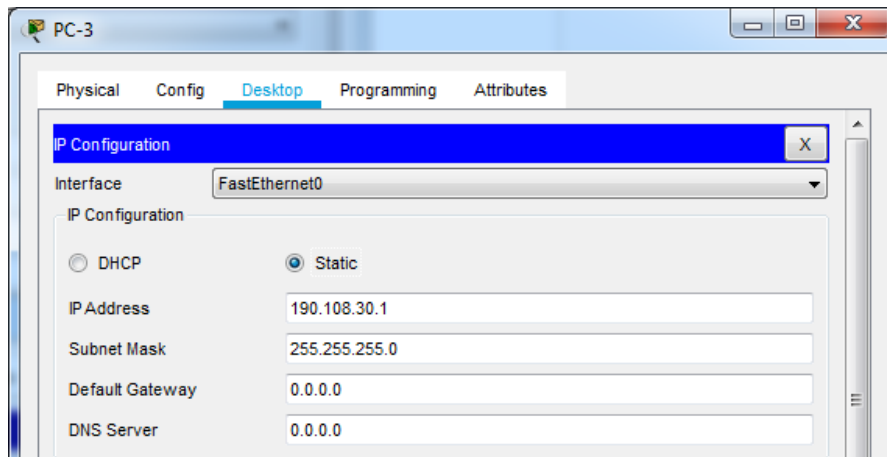


Figura 38 configuración PC-3

```

SW-BB>enable
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int fa0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int fa0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int fa0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#

```

Figura 39 Asociación de puertos VLAN SW-BB

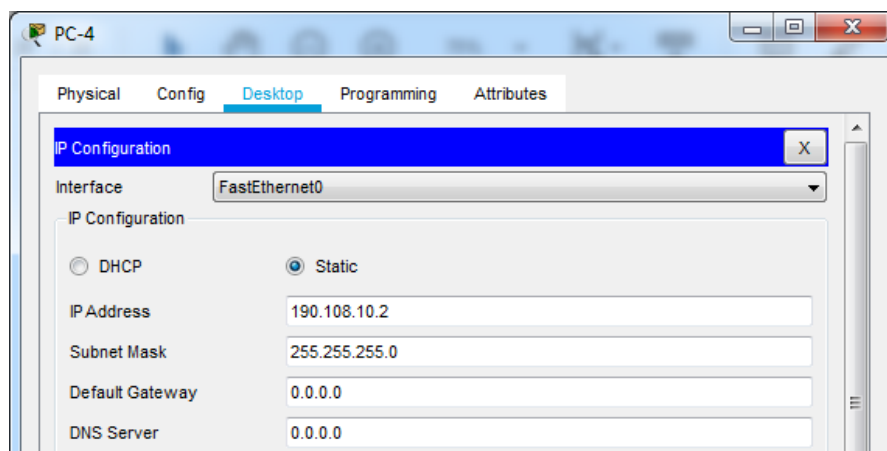


Figura 40 configuración PC-4

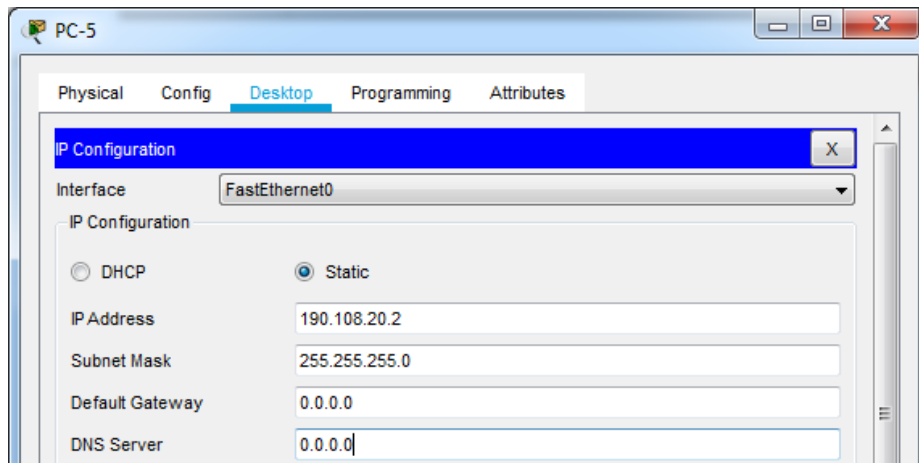


Figura 41 configuración PC-5

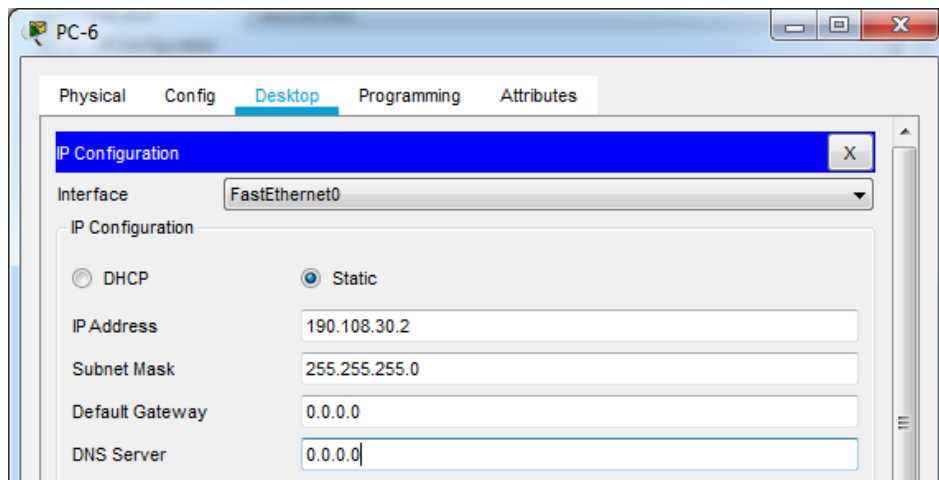


Figura 42 configuración PC-6

```

SW-CC>enable
SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#int fa0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int fa0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int fa0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#

```

Figura 43 Asociación de puertos VLAN SW-CC

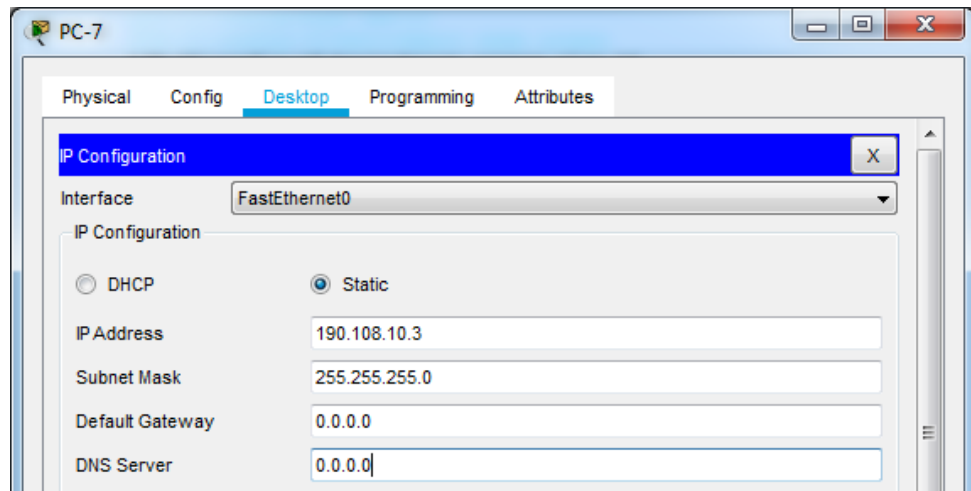


Figura 44 configuración PC-7

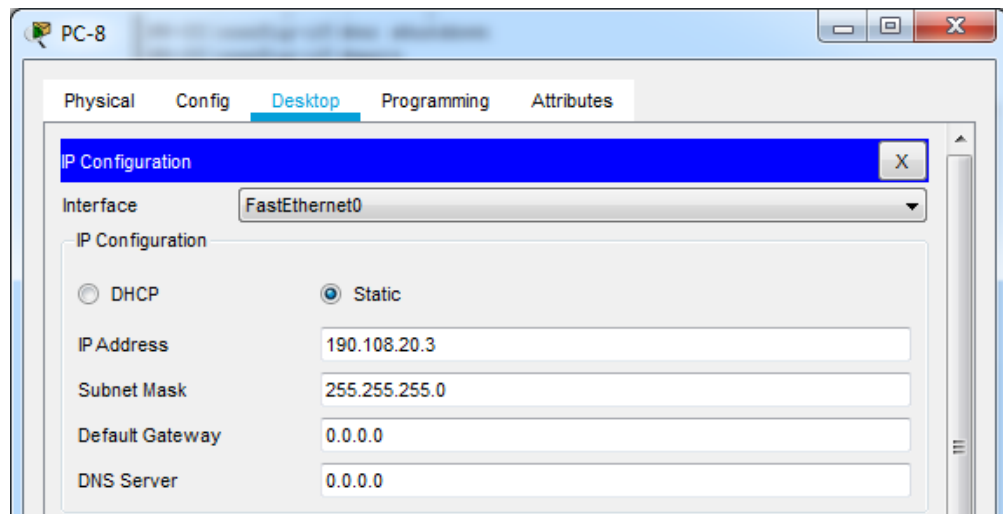


Figura 45 configuración PC-8

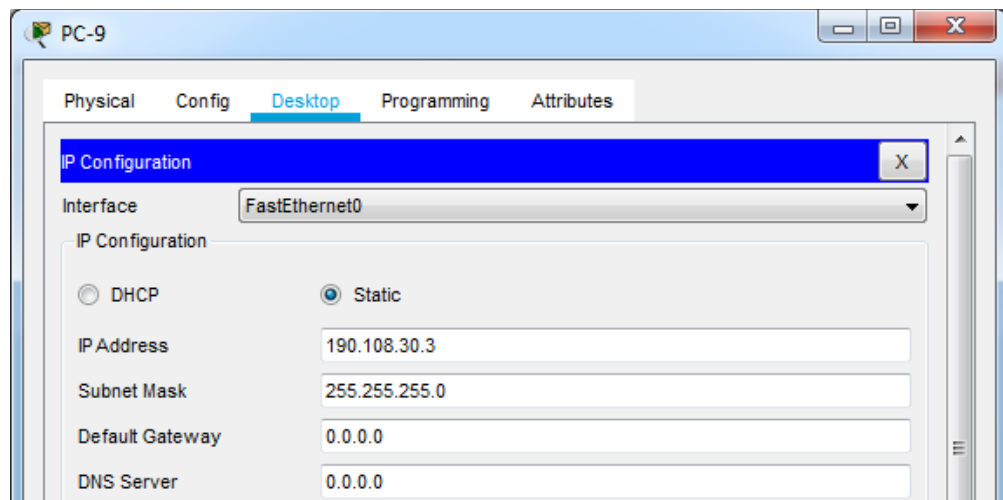


Figura 46 configuración PC-9

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

```
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#int fa0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
```

Figura 47 Asignación VLAN 10 SW-AA

```
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int fa0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
```

Figura 48 Asignación VLAN 10 SW-BB

```
SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#int fa0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
```

Figura 49 Asignación VLAN 10 SW-CC

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 solución de este punto es la misma solución del paso 11.**

#### 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.

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

Tabla 6 Direcciones IP Switches

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

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

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

*Tabla 7 SW-AA VLAN 99*

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

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

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

*Tabla 8 SW-BB VLAN 99*

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

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

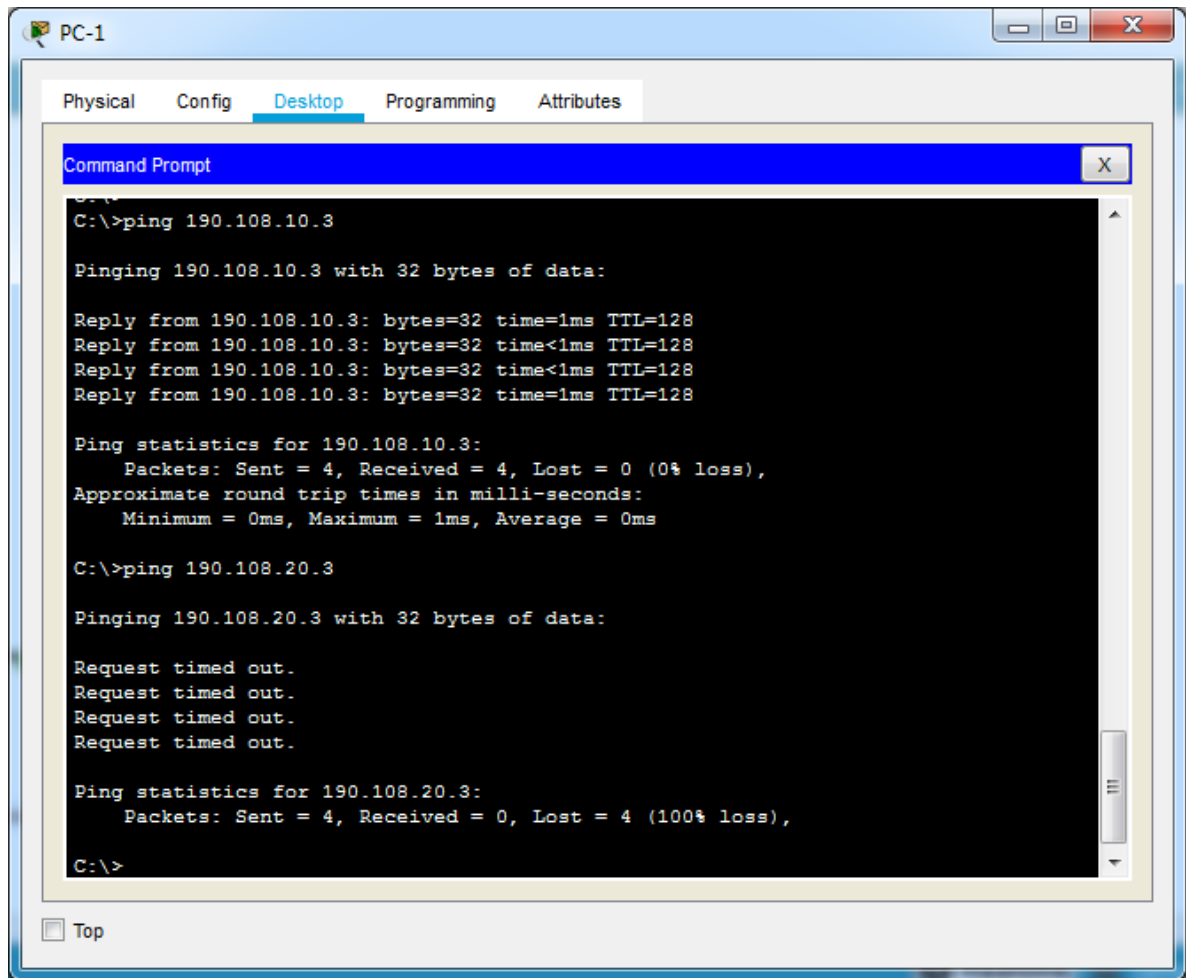
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#
```

*Figura 50 SW-CC VLAN 99*

## 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.

### PC1 – PC7 y PC1 – PC8



The screenshot shows a Command Prompt window titled "Command Prompt" with a blue header bar. The window is open on a desktop environment with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. The Command Prompt shows the following text:

```
C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

Reply from 190.108.10.3: bytes=32 time=1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

At the bottom left of the Command Prompt window, there is a "Top" button.

Figura 51 Verificación de PC ping 1



## PC5 – PC8 y PC5 – PC9

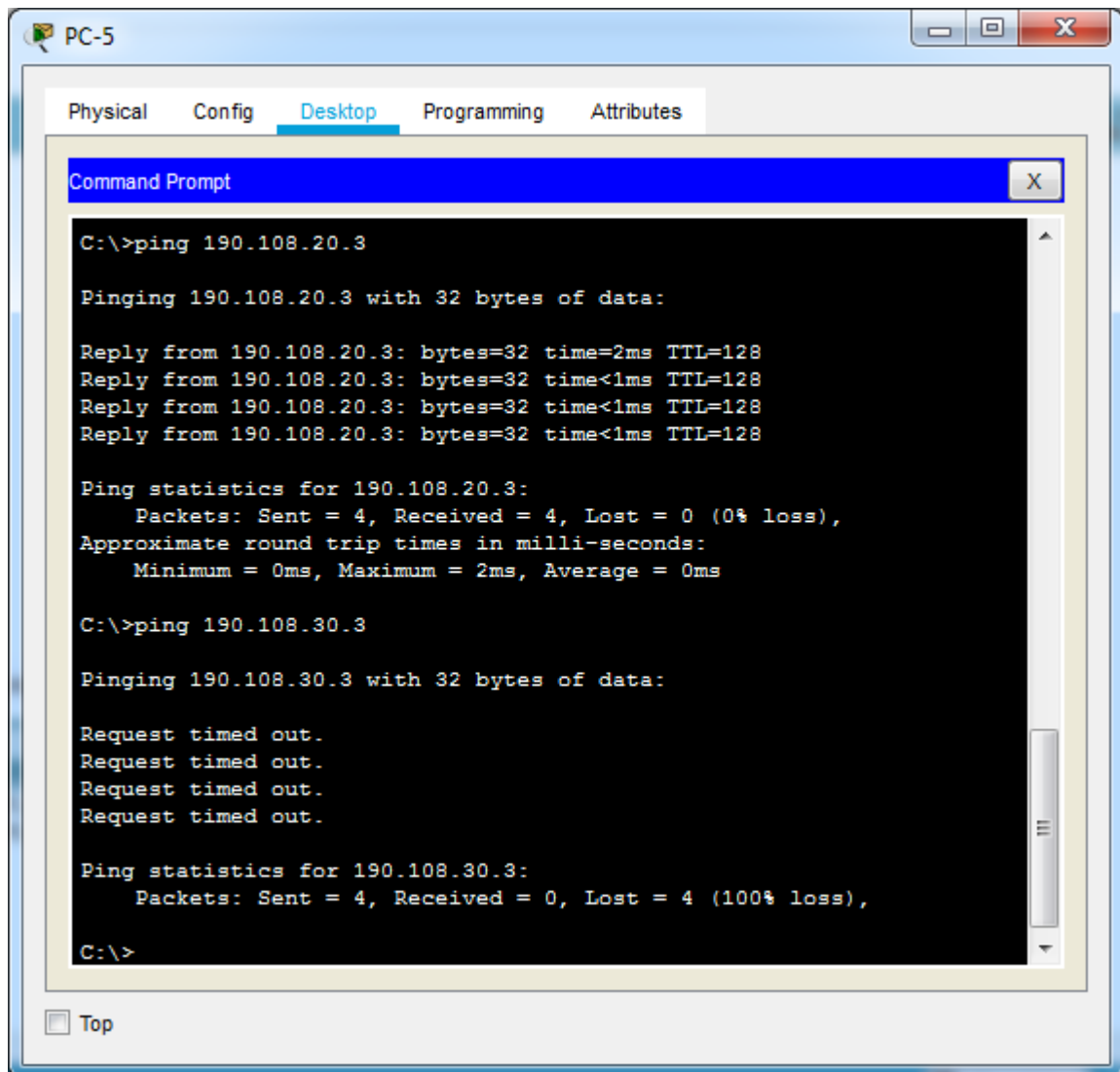
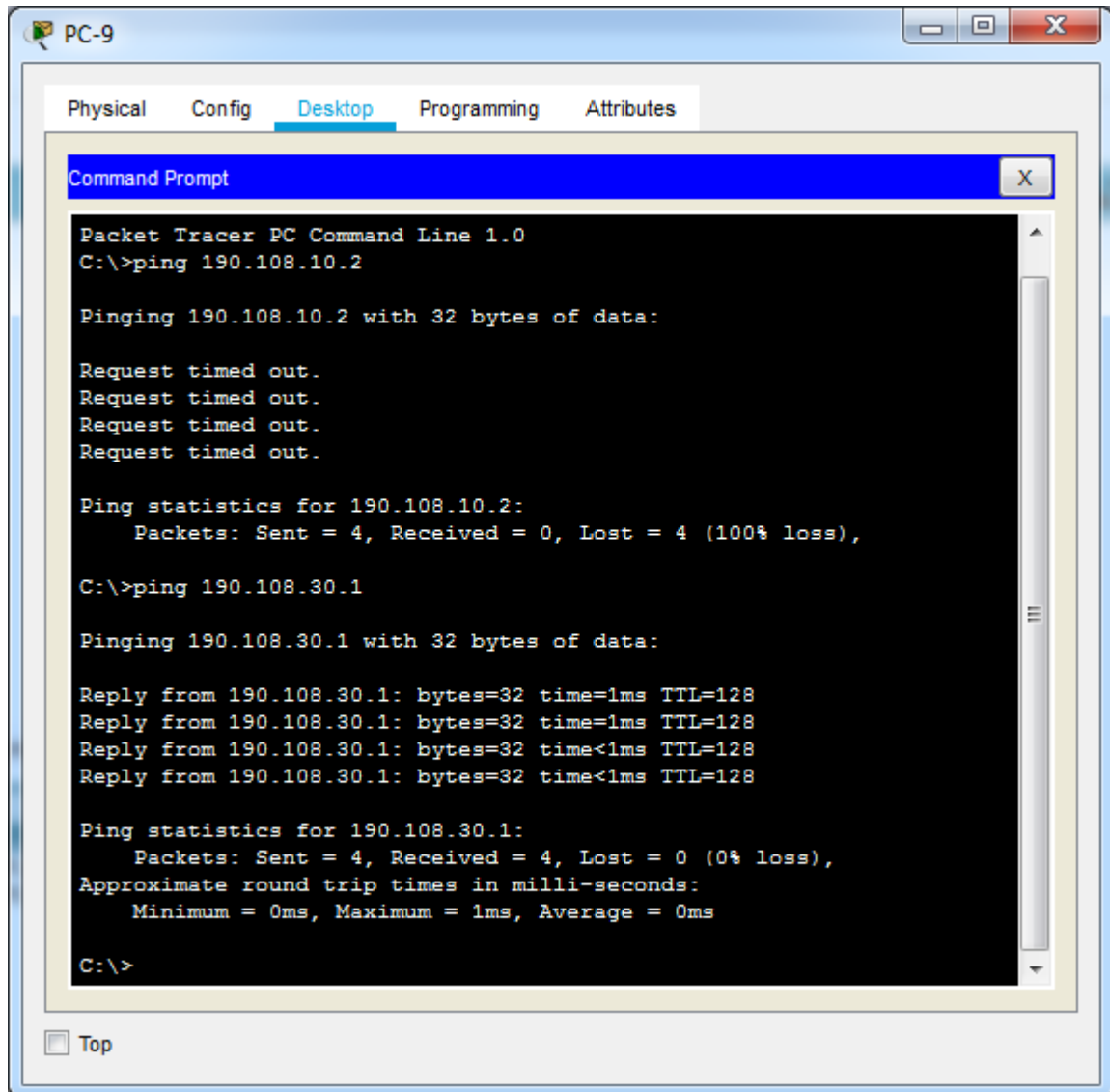


Figura 52 Verificación de PC ping 2

## PC9 – PC6 y PC9 – PC3



The screenshot shows a Packet Tracer PC window titled 'PC-9' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.1

Pinging 190.108.30.1 with 32 bytes of data:

Reply from 190.108.30.1: bytes=32 time=1ms TTL=128
Reply from 190.108.30.1: bytes=32 time=1ms TTL=128
Reply from 190.108.30.1: bytes=32 time<1ms TTL=128
Reply from 190.108.30.1: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 53 Verificación de PC ping 3

**Análisis:** Se comprende que el ping realizado a diferentes VLANs no se obtuvo éxito de ninguna manera y tampoco tiempo de respuesta, esto es debido a que las VLANs que son de diferentes red. Sin embargo, los PC que se realizó ping hacia PC de VLANs con la misma red, el tiempo de respuesta ha sido satisfactorio.

En conclusión se entiende que para solucionar este Error se tendría como necesidad incorporar un Switch o enrutador de capa 3 (Switch Multicapa), el cual estos tiene como objetivo o funcionalidad el enrutamiento entre varias VLANs independientemente si se encuentran o no en la misma red.

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

```
SW-AA>en
SW-AA#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#
```

Figura 54 Switch Ping 1

```
SW-BB>en
SW-BB#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-BB#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-BB#
```

Figura 55 Switch Ping 2

```
SW-CC>en
SW-CC#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW-CC#ping 190.108.99.2

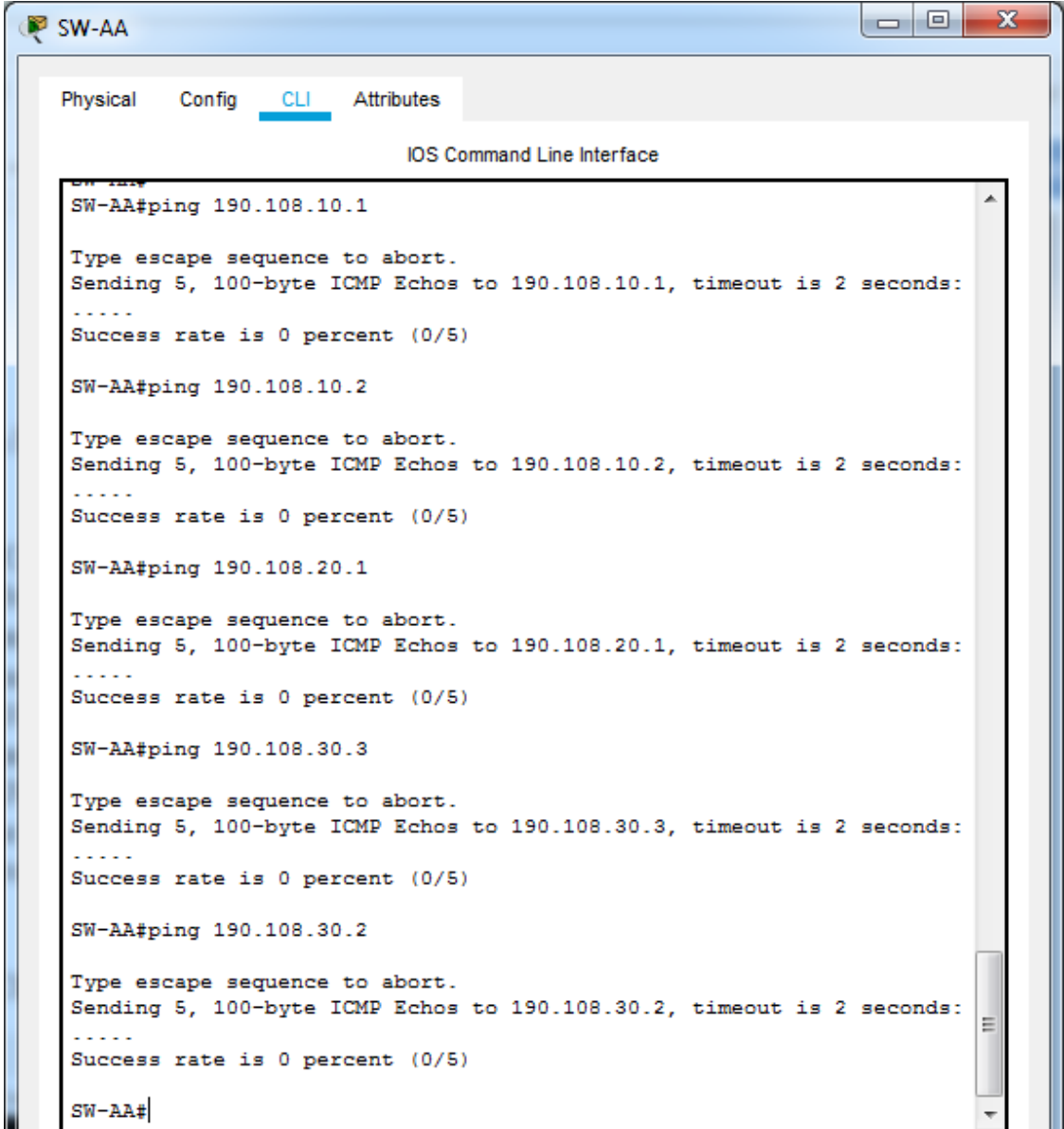
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-CC#
```

Figura 56 Switch Ping 2

**Análisis:** Se puede interpretar en las figuras anteriores que el ping realizado entre los Switch ha sido exitoso, ya que dado a las diferentes interfaces físicas que enrutan los diferentes datos que son enviado a través del protocolo ICMP, están configuradas en el modo troncal y según pruebas anteriores desarrolladas se verifico con el comando **show interfaces trunk**, donde se resaltas que tienen el mismo tipo de encapsulamiento y se encuentran en el mismo modo compatible.

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



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Figura 57 Switch a PC ping 1

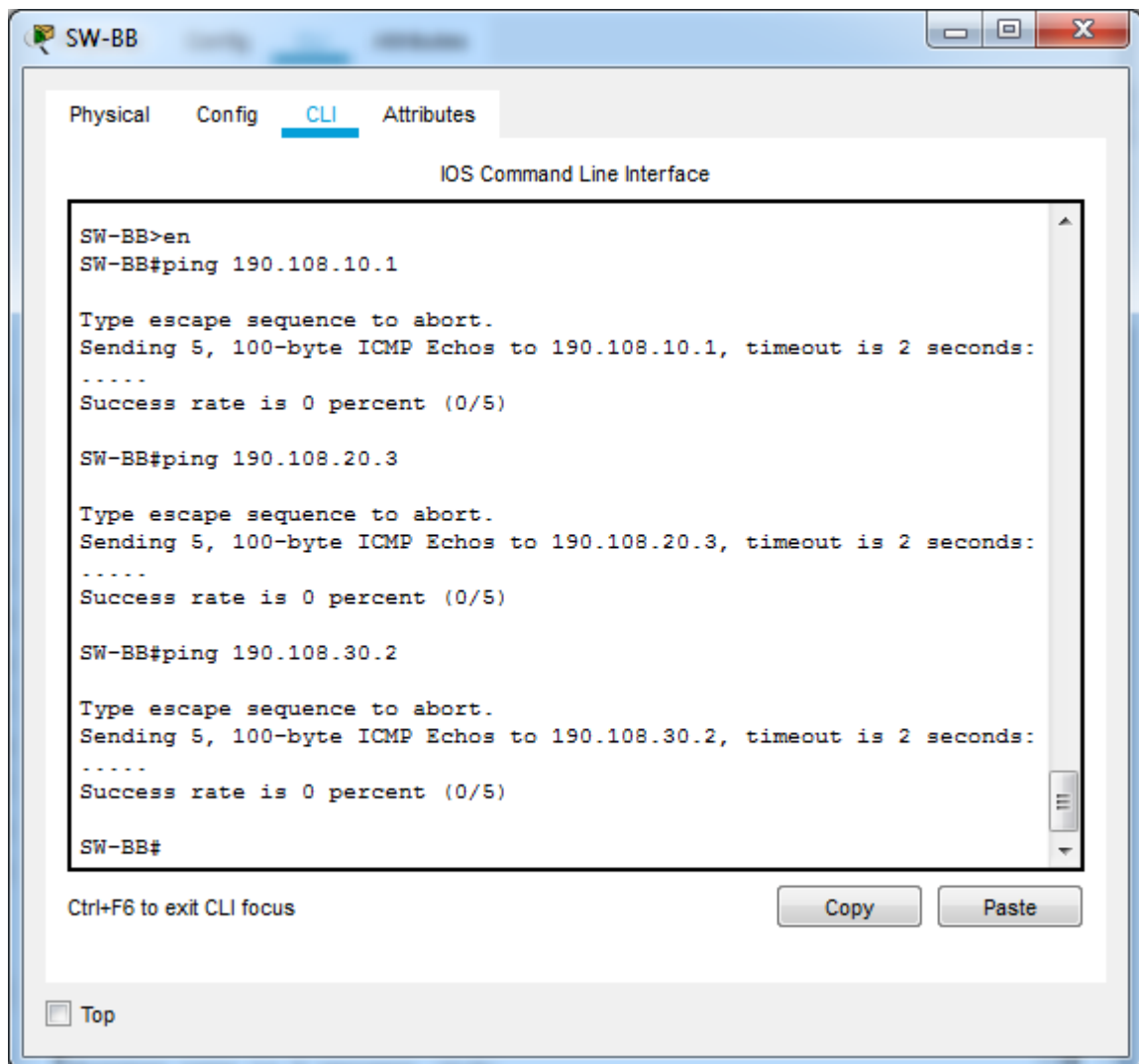


Figura 58 Switch a PC ping 2

**Análisis:** Se realizó el ping desde los Switches a los diferentes PCs de la red pero ninguno obtuvo éxito, debido a que a pesar de que se ha realizado el proceso correcto en cuanto a la habilitación de las VLANs en cada uno de los Switches y con el protocolo VTP y sumado a eso la configuración de cada una de las interfaces, se entiende que hace falta la configuración del enrutamiento IP en las VLANs creadas (10 compras, 25 personal y 30 planta).

Para solucionar este error entonces se hace necesario configurar cada una de las direcciones IP y máscaras de subred en cada una de las VLANs de los Switches configurados, con el objetivo de que pertenezcan al mismo segmento de red de cada PC y de tal manera se determine la VLAN nativa en cada una de las interfaces.

## CONCLUSIONES

Como entendimiento en los diferentes escenarios presentados en la evaluación final del curso, se comprende a través de la solución de habilidades prácticas presentadas en las herramientas como GNS3, Packet Tracer y SamrtLab de cisco. Sumado a esto se identifica que en el primer escenario se realiza el uso de los protocolos de enrutamiento en cada uno de los escenarios, con el objetivo de anunciar rutas que se aprenden por otros medios, como otro protocolo de enrutamiento, rutas estáticas o rutas directamente conectadas.

El protocolo VTP, permite administrar y configurar las VLANs asignada a cada Switch, al tener diferente Switch con dispositivos conectados a interfaces que están asignado a ciertas VLANs, se necesita configurar los Switch en el protocolo DTP para establecer canales troncales donde se puede conectar con diferentes VLANs.

Las redes de comunicación se han apoyado en sus protocolos de comunicación y configuración para establecer diferentes características de comunicación en red, haciéndola diversa y dinámica. Permitiendo las diferentes características que contamos actualmente en los dispositivos de red y sus topologías.

## REFERENCIAS BIBLIOGRÁFICAS

Froom, R., Frahim, E. (2015). CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {En línea}. {Consultado junio 2009}. Disponible en: [http://www.ICONTEC.org/BancoConocimiento/C/compendio de tesis y otros trabajos de grado/compendio de tesis y otros trabajos de grado.asp?CodIdioma=ESP](http://www.ICONTEC.org/BancoConocimiento/C/compendio%20de%20tesis%20y%20otros%20trabajos%20de%20grado/compendio%20de%20tesis%20y%20otros%20trabajos%20de%20grado.asp?CodIdioma=ESP).

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnMfy2rhPZHwEoWx>