DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARY ALEJANDRA HERNANDEZ LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA -ECBTI
INGENIERIA DE TELECOMUNICACIONES
AÑO 2020
EVALUACIÓN DE PRUEBAS DE HABILIDADES PRÁCTICAS CCNP

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARY ALEJANDRA HERNANDEZ LEON

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA -ECBTI
INGENIERIA DE TELECOMUNICACIONES
AÑO 2020
EVALUACIÓN DE PRUEBAS DE HABILIDADES PRÁCTICAS CCNP

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 22 de mayo de 2020

AGRADECIMIENTOS

En agradecimiento a este trabajo va dirigido principalmente a DIOS ya que sin su amor y bendición nada hubiera sido posible, también para todos los tutores por su apoyo y aportes de sus conocimientos, a mis padres por estar pendiente y apoyarme para que todo salga bien.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

PROTOCOLO BGP: Es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos

DIRECCIÓN IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo que utilice el protocolo.

DIRECCION LOOPBACK: Son las direcciones del rango '127.0.0.0/8', de las cuales se utiliza, de forma mayoritaria, la '127.0.0.1' por ser la primera de dicho rango, añadiendo '::1' para el caso de IPv6 ('127.0.0.1::1'). Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas. Son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP

ROUTER: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

RESUMEN

En el presente trabajo se relacionan las actividades correspondientes a la prueba de habilidades prácticas del Diplomado de Profundización CISCO CCNP, en el que se manejan diversos tópicos en el ámbito de la electrónica asociados con la configuración de diferentes parámetros de administración y gestión en redes en relación con enrutamiento y conmutación, orientados a la programación, verificación y puesta del uso de protocolos como BGP, DTP y VTP, presentando así el desarrollo de cada uno de los escenarios propuestos, debidamente documentados y simulados con el software datos Cisco Packet Tracer.

ABSTRACT

In This work lists the activities corresponding to the practical skills test of the CISCO CCNP Deepening Diploma, in which various topics are handled in the field of electronics associated with the configuration of different administration and networking management parameters in relation to with routing and switching, oriented to the programming, verification and implementation of protocols such as BGP, DTP and VTP, thus presenting the development of each of the proposed scenarios, duly documented and simulated with the Cisco Packet Tracer data software.

INTRODUCCIÓN

El presente documento contiene el desarrollo de la Prueba de Habilidades Practicas, del Diplomado de Profundización CCNP, la cual forma parte de las actividades evaluativas y busca identificar el grado de desarrollo de competencias y habilidades que logramos adquirir a lo largo del diplomado.

Consta de 2 escenarios propuestos mediante los cuales en el desarrollo de este documento se informa paso a paso el proceso realizado para dar solución a actividad planteada y el registro de los procesos de verificación de conectividad mediante el uso de comandos.

Para la prueba se obtuvo el apoyo del programa Cisco Packet tracer el cual nos ayudó mucho a la hora de la programación de cada tarea y escenario que se presentan en la guía de trabajo.

DESARROLLO DE LAS PRÁCTICAS

El desarrollo de ambas practicas se lleva a cabo en el simulador de redes PACKET TRACER versión 7.3, el cual es totalmente gratis y dispone de las imágenes necesarias para el desarrollo de lo que se pide.

2.1 ESCENARIO 1

TOPOLOGÍA

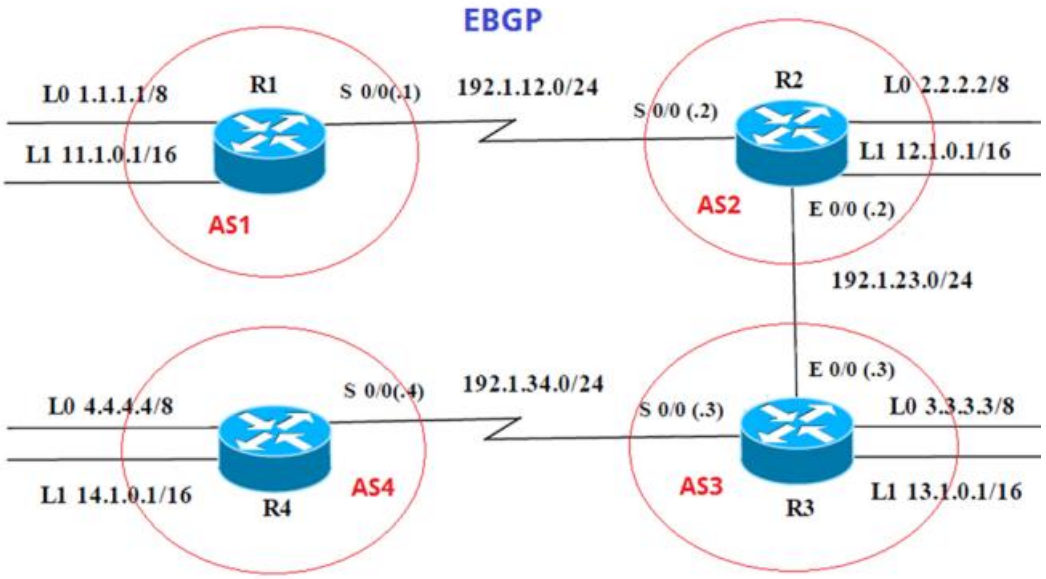

Figura 1. Escenario 1

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. Interfaces loopback para crear 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. Interfaces loopback para crear 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. Interfaces loopback para crear 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. Interfaces loopback para crear R4

SOLUCIÓN

Después de implementar la topología en el software con los routers PT se procede a configurar el direccionamiento a las interfaces asociadas a los 4 routers en la topología:

R1

- Router>en
- Router#conf t
- Router(config)#hostname R1
- R1(config)#int s1/0
- R1(config-if)#ip address 192.1.12.1 255.255.255.0
- R1(config-if)#no shutdown
- R1(config-if)#int lo 0
- R1(config-if)#ip address 1.1.1.1 255.0.0.0
- R1(config-if)#int lo 1
- R1(config-if)#ip address 11.1.0.1 255.255.0.0
- R1(config-if)#exit

R2

- Router>en
- Router#conf t
- Router(config)#hostname R2
- R2(config)#int s1/0
- R2(config-if)#ip address 192.1.12.2 255.255.255.0

- R2(config-if)#no shutdown
- R2(config-if)#int e2/0
- R2(config-if)#ip address 192.1.23.2 255.255.255.0
- R2(config-if)#no shutdown
- R2(config-if)#int lo 0
- R2(config-if)#ip address 2.2.2.2 255.0.0.0
- R2(config-if)#int lo 1
- R2(config-if)#ip address 12.1.0.1 255.255.0.0

R3

- Router>en
- Router#conf t
- Router(config)#hostname R3
- R3(config)#int s1/0
- R3(config-if)#ip address 192.1.34.3 255.255.255.0
- R3(config-if)#no shutdown
- R3(config-if)#int e2/0
- R3(config-if)#ip address 192.1.23.3 255.255.255.0
- R3(config-if)#no shutdown
- R3(config-if)#int lo 0
- R3(config-if)#ip address 3.3.3.3 255.0.0.0
- R3(config-if)#int lo 1
- R3(config-if)#ip address 13.1.0.1 255.255.0.0

R4

- Router>en
- Router#conf t
- Router(config)#hostname R4
- R4(config)#int s1/0
- R4(config-if)#ip address 192.1.34.4 255.255.255.0
- R4(config-if)#no shutdown
- R4(config-if)#int lo 0
- R4(config-if)#ip address 4.4.4.4 255.0.0.0
- R4(config-if)#int lo 1
- R4(config-if)#ip address 14.1.0.1 255.255.0.0
- R4(config-if)#exit

1. Parte 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 enrutadores 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.

Aquí procedemos a configurar BGP en R1 t en R2:

R1

- R1(config)#router bgp 1
- R1(config-router)#bgp router-id 22.22.22.22
- R1(config-router)#network 192.1.12.0 mask 255.255.255.0
- 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)#neighbor 192.1.12.2 remote-as 2

R2

- R2(config)#router bgp 2
- R2(config-router)#bgp router-id 33.33.33.33
- R2(config-router)#network 192.1.12.0 mask 255.255.255.0
- 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 192.1.23.0 mask 255.255.255.0
- R2(config-router)#neighbor 192.1.12.1 remote-as 1
- R2(config-router)#neighbor 192.1.23.3 remote-as 3

Ahora con el commando show ip route en los dos routers validamos las rutas con la respectiva adyacencia

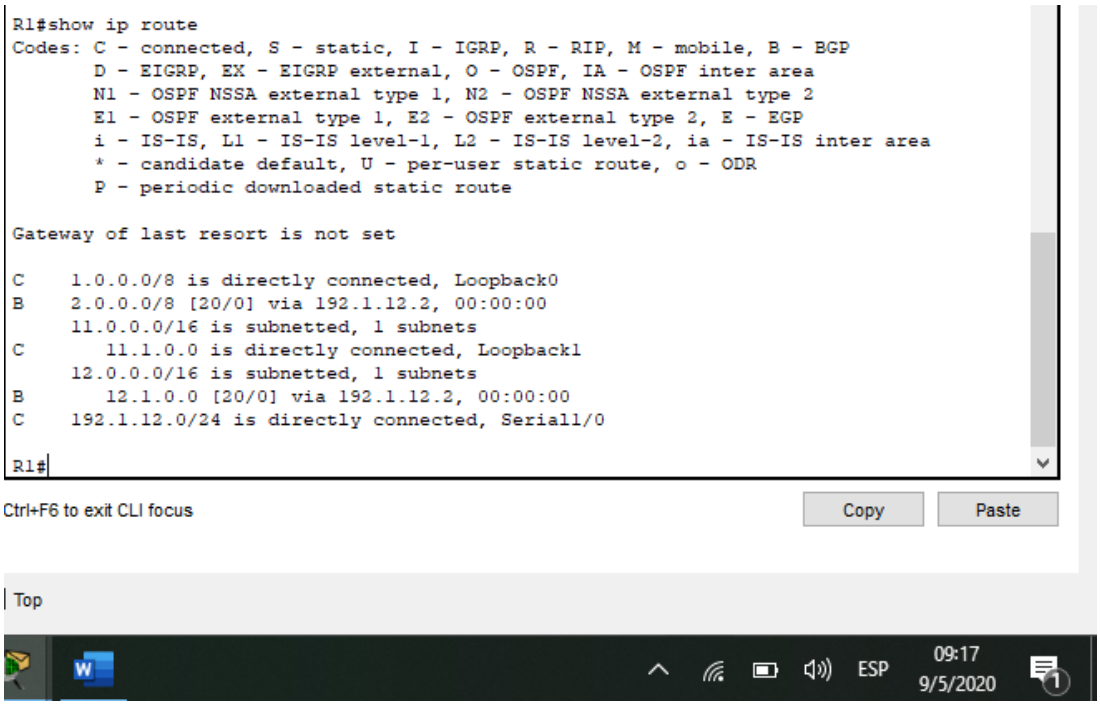

Figura 2. Comando en R1

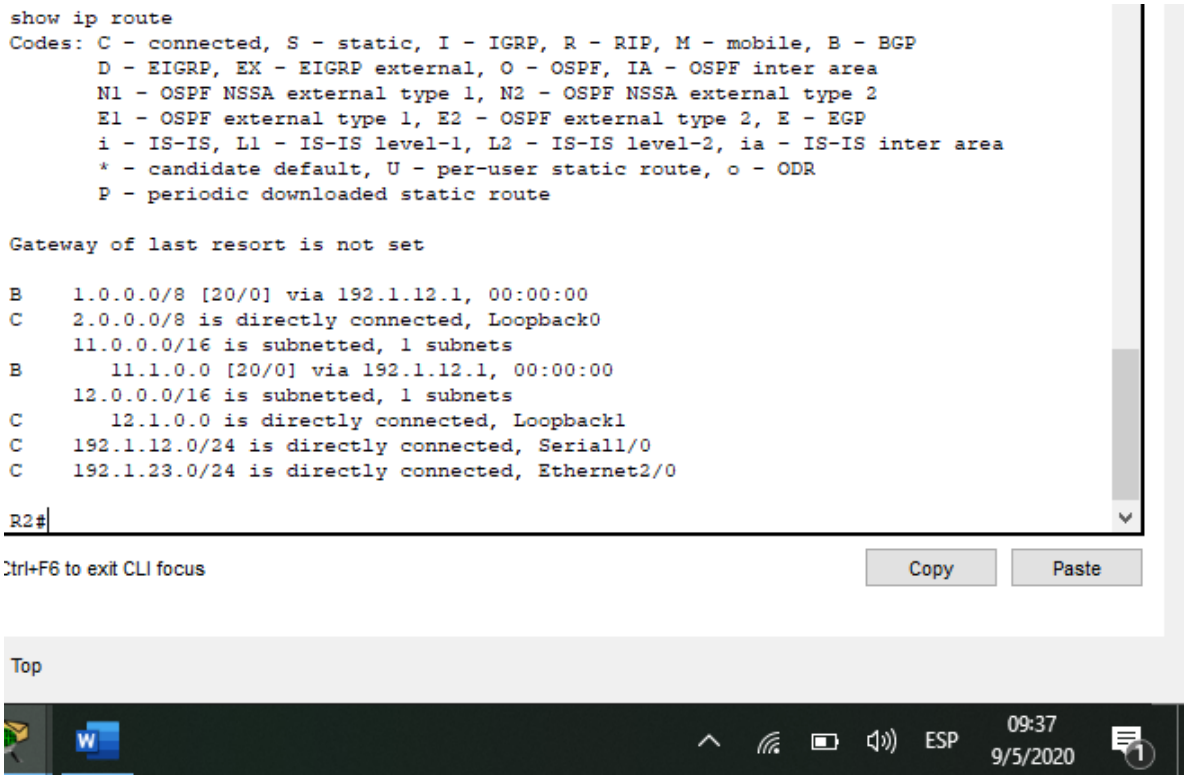

Figura 3. Comando en R2

2. Parte 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.

R3

- 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

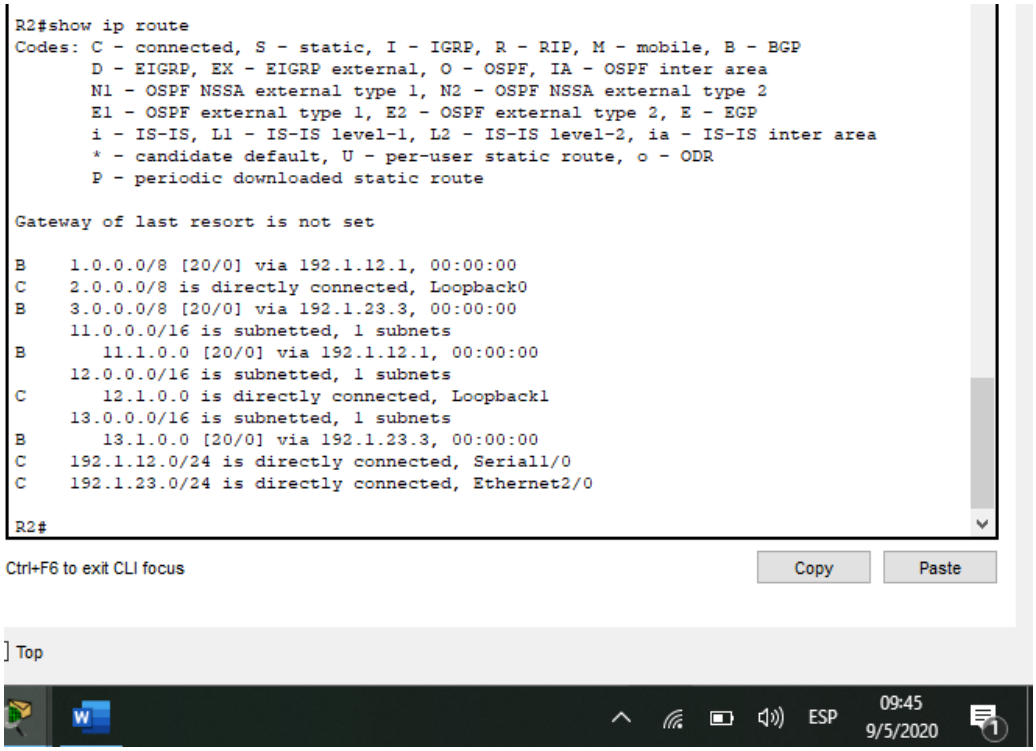

Figura 4. Comando en R3

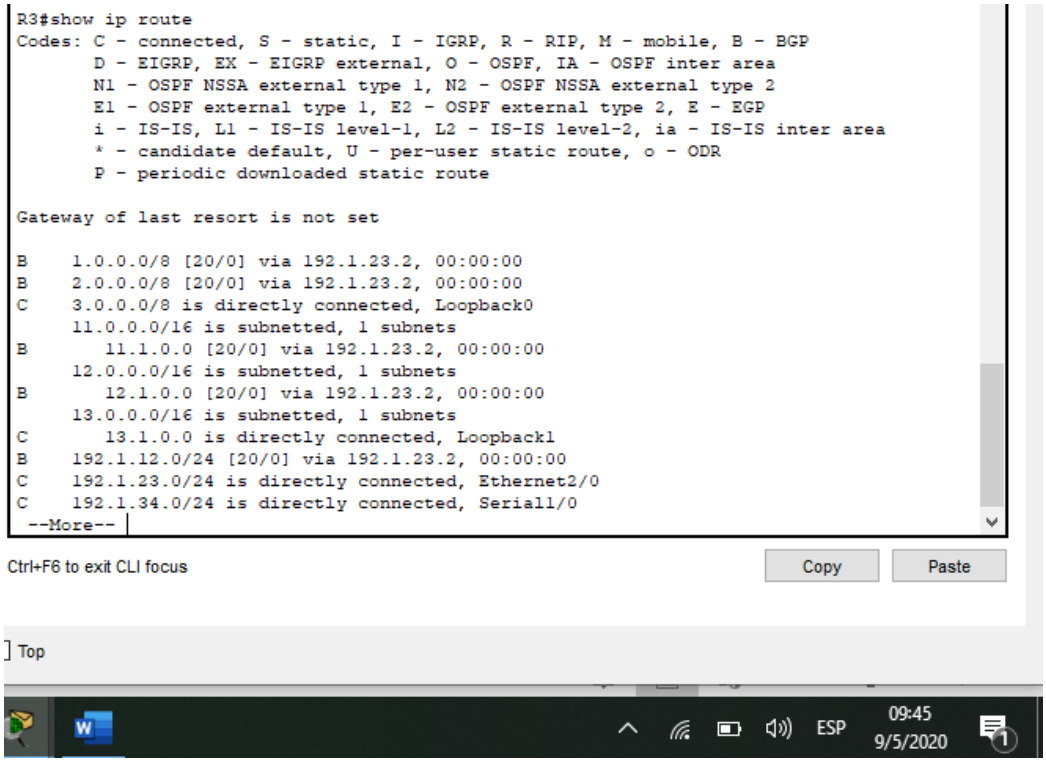

Figura 5. Comando en R4

3. Parte 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#conf t
- 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

- R4(config)#router bgp 4
- R4(config-router)#bgp router-id 44.44.44.44
- 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

Después hay que establecer las relaciones de adyacencia mediante las direcciones loopback, para ello se requiere la siguiente configuración:

R3

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

R4

- 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(commando no soportado por packet tracer)
- R4(config-router)#neighbor 3.3.3.3 update-source loopback 0 (commando no soportado por packet tracer)
- R4(config-router)# neighbor 3.3.3.3 ebgp-multihop (commando no soportado por packet tracer)

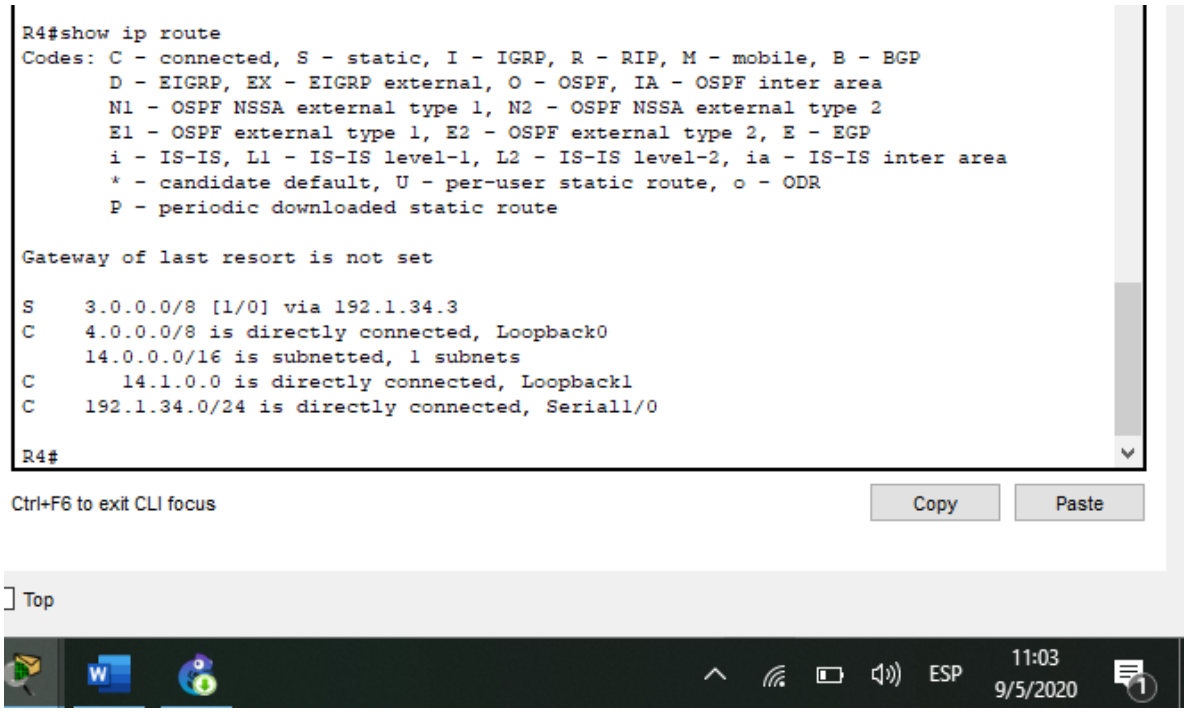

Figura 6. Comando en R4

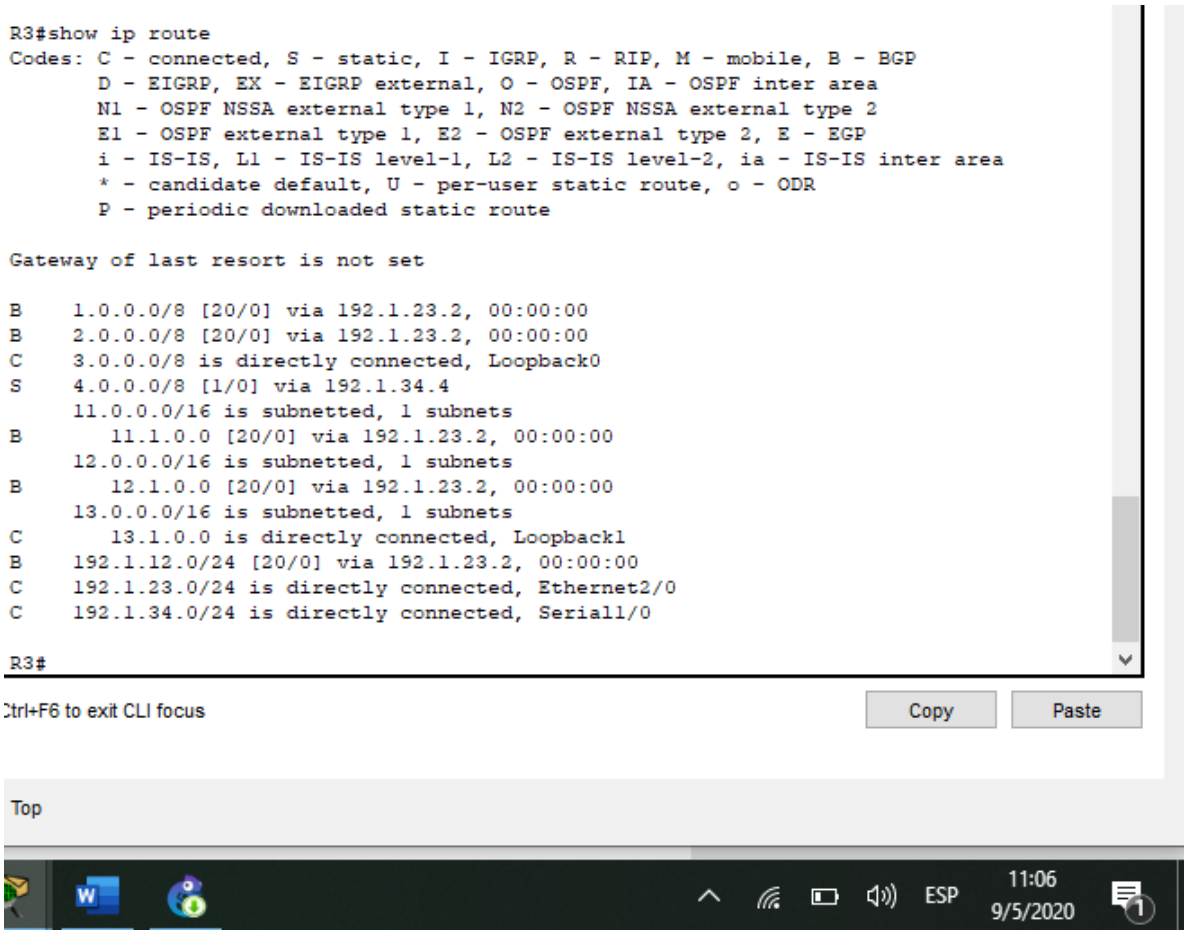

Figura 7. Comando en R3

2.2 ESCENARIO 2

TOPOLOGÍA

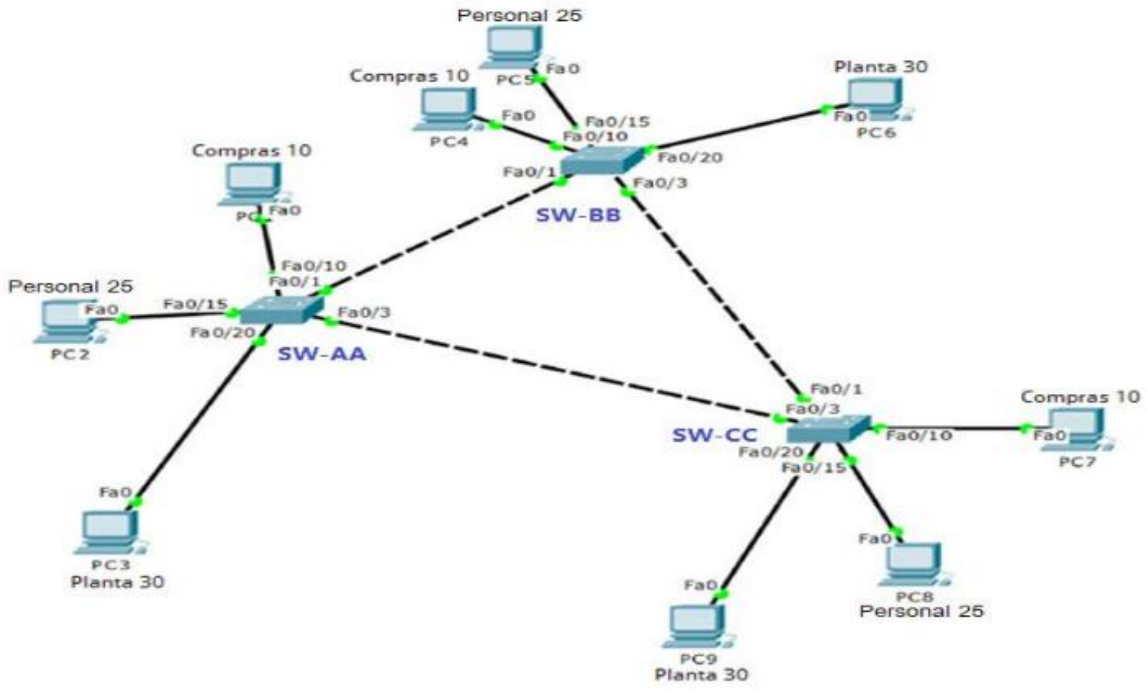

Figura 8. Escenario 2

En donde hay que desarrollar los siguientes pasos

a. Configurar VTP
b. Configurar DTP (Dynamic Trunking Protocol)
c. Agregar VLANs y asignar puertos.
d. Configurar las direcciones IP en los Switches.
e. Verificar la conectividad Extremo a Extremo

SOLUCIÓN

A. Configurar VTP

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

Se configuran nombres y vtp:

SW-AA

- Switch>en
- Switch#conf t
- Switch(config)#h SW-AA

- SW-AA(config)#vtp domain CCNP
- SW-AA(config)#vtp mode client
- SW-AA(config)#vtp pass cisco
- SW-AA(config)#vtp versión 2

SW-BB

- Switch>en
- Switch#conf t
- Switch(config)#H SW-BB
- SW-BB(config)#vtp domain CCNP
- SW-BB(config)#vtp mode server
- SW-BB(config)#vtp pass cisco
- SW-BB(config)#vtp versión 2

SW-CC

- Switch>en
- Switch#conf t
- Switch(config)#H SW-CC
- SW- CC(config)#vtp domain CCNP
- SW- CC(config)#vtp mode server
- SW- CC(config)#vtp pass cisco
- SW- CC(config)#vtp versión 2

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

Comando show vtp status en SW-AA

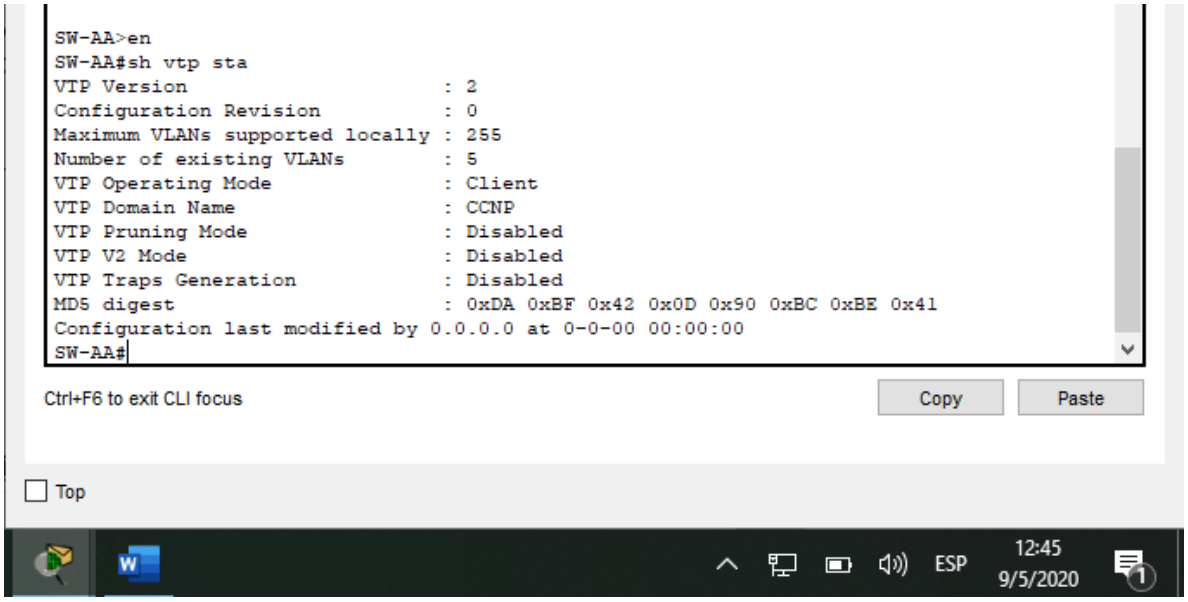

Figura 9. Comando en SW-AA

Comando show vtp status en SW-BB

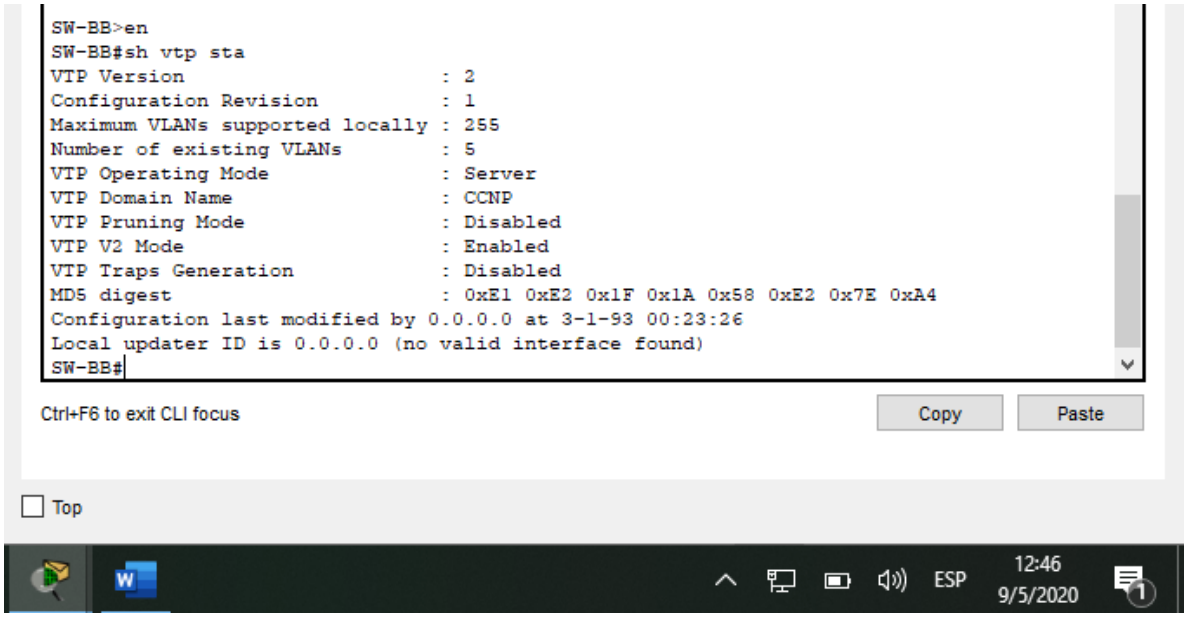

Figura 10. Comando en SW-BB

Comando show vtp status en SW-CC

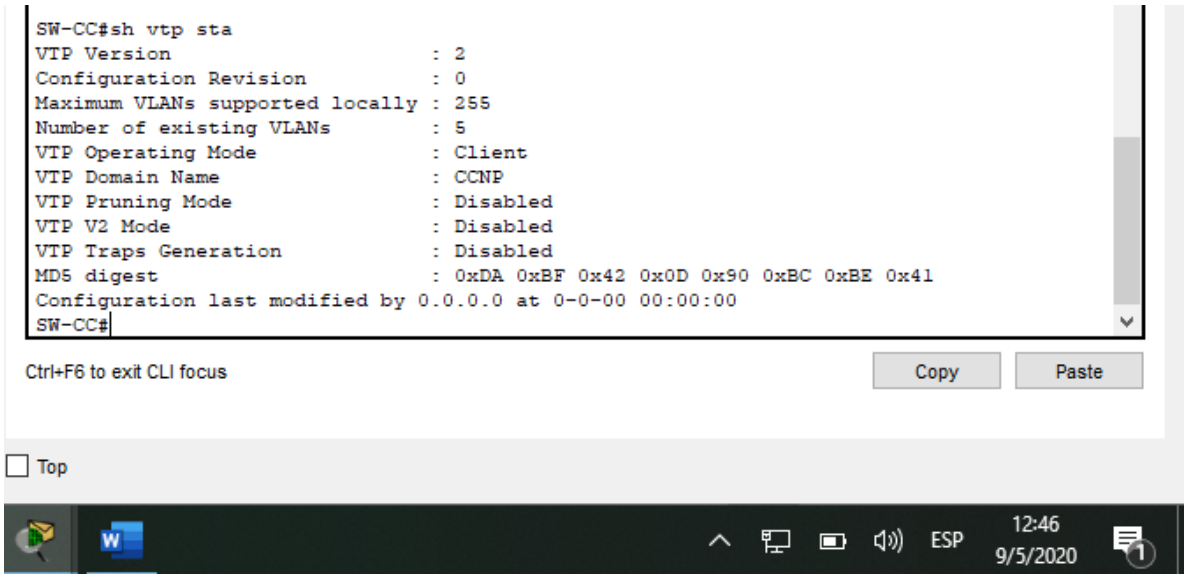

Figura 11. Comando en SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Configuración troncal en SW-AA

- SW-AA(config)#int fa0/1
- SW-AA(config-if)#switchport mode trunk
- SW-AA(config-if)# switchport mode dynamic desirable

Configuración troncal en SW-BB

- SW-BB(config)#int fa0/1
- SW-BB (config-if)#switchport mode trunk

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

Comando show interfaces trunk en SW-AA

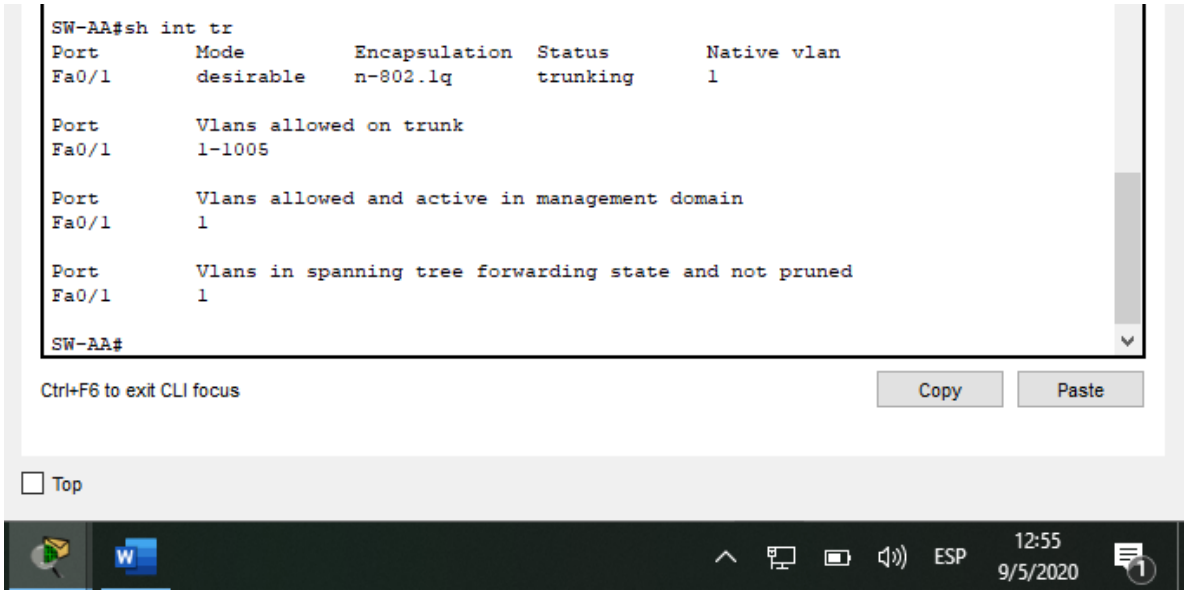

Figura 12. Configuración troncal en SW-AA

Comando show interfaces trunk en SW-BB

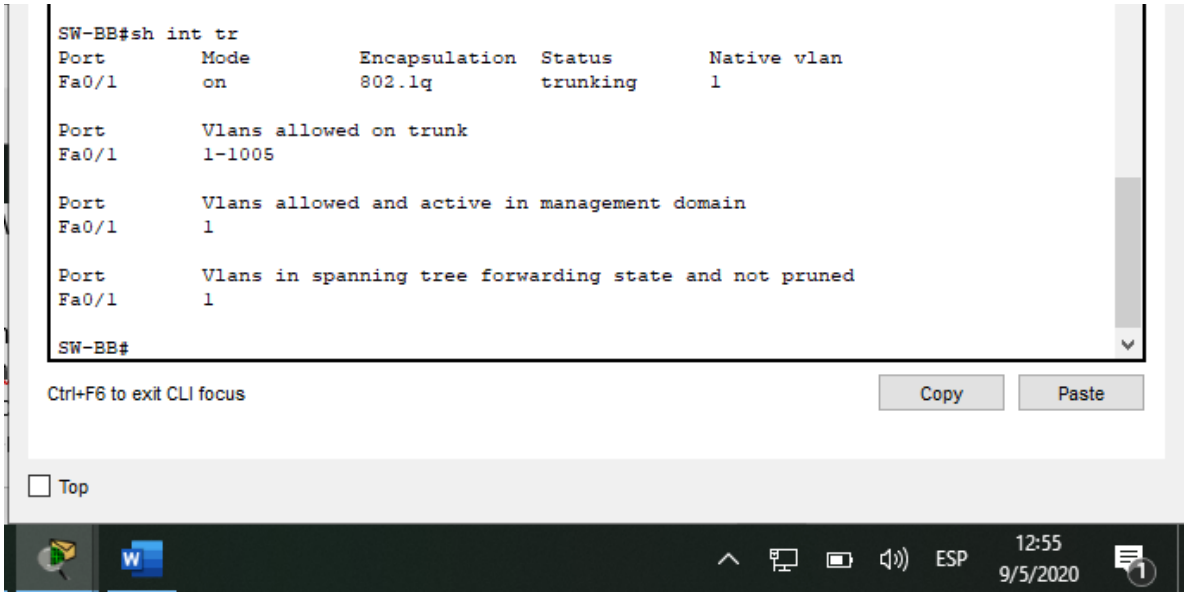

Figura 13. Configuración troncal en SW-BB

3. Entre SWT-AA y SWT-CC configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SWT-AA

SW-AA

- SW-AA(config)#int fa0/3
- SW-AA(config-if)#switchport mode trunk

SW-CC

- SW-CC(config)#int fa0/3
- SW-CC(config-if)#switchport mode trunk

4. Verifique el enlace "trunk" el comando show interfaces trunk en SWT-AA

Comando show interfaces trunk en SWT-AA

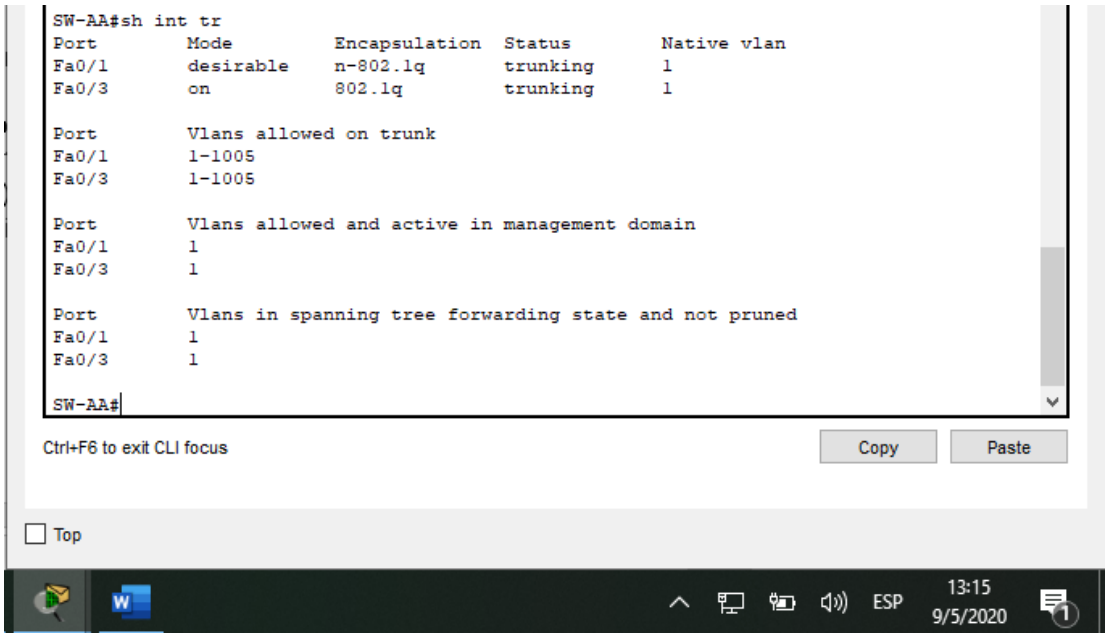

Figura 14. Comando show interfaces trunk en SWT-AA

5. Configure un enlace "trunk" permanente entre SWT-BB y SWT-CC

SWT-BB

- SW-BB(config)#int fa0/3
- SW-BB(config-if)#switchport mode trunk

SWT-CC

- SW-CC(config)#int fa0/1
- SW-CC(config-if)#switchport mode trunk

C. Agregar VLANs y asignar puertos.

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

SW-AA

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

SW-BB

- 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

2. Verifique que las VLANs han sido agregadas correctamente.

Ejecutamos el comando show vlan en SW-BB

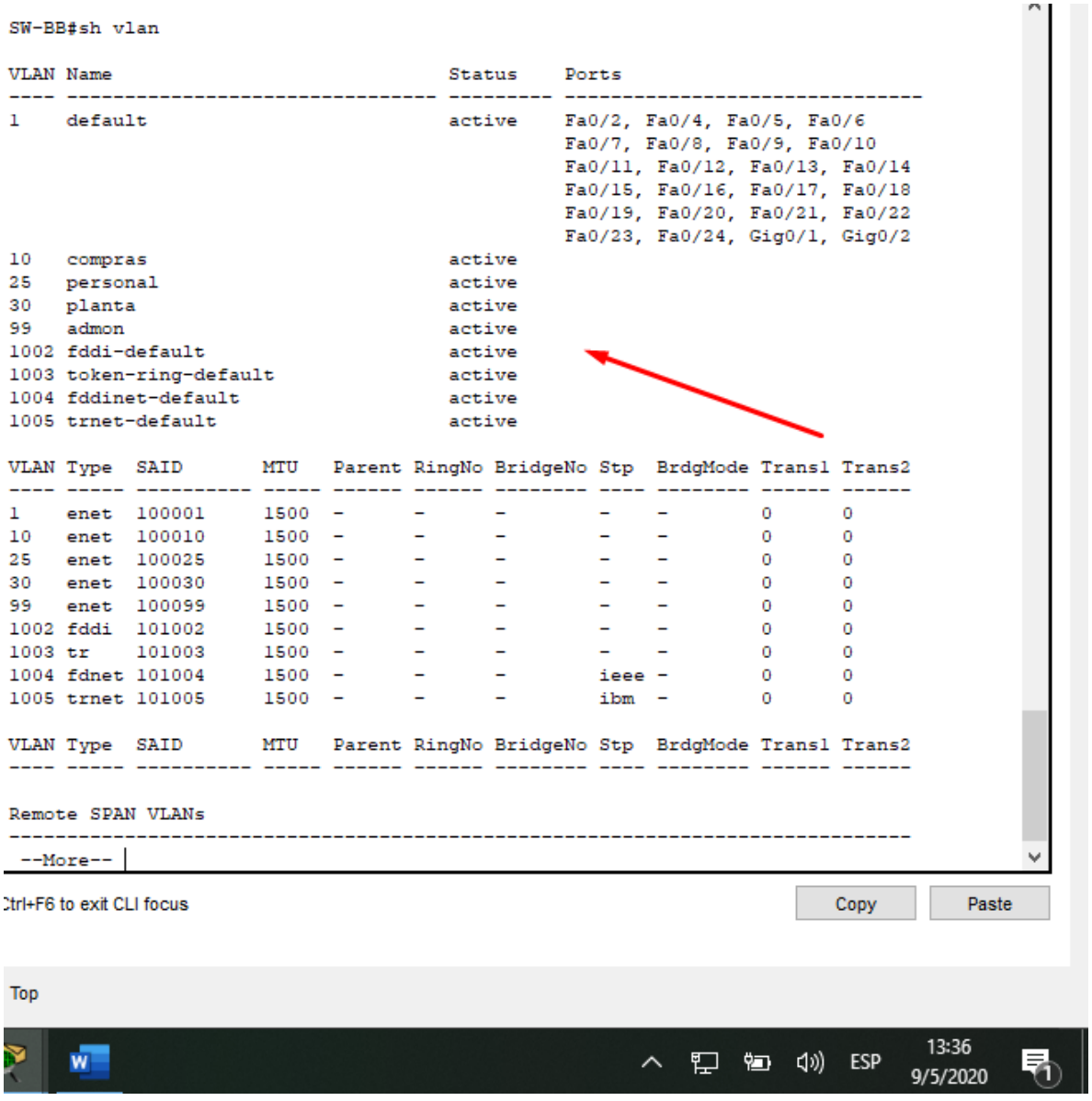

Figura 15. Comando show vlan en SW-BB

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

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

Tabla 5. Direcciones IP interfaces

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

SW-AA

- SW-AA(config)#int fa0/10
- SW-AA(config-if)#switchport access vlan 10

SW-BB

- SW-BB(config)#int fa0/10
- SW-BB(config-if)#switchport access vlan 10

SW-CC

- SW-CC(config)#int fa0/10
- SW-CC(config-if)#switchport access vlan 10

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

SW-AA

- SW- AA(config)#int fa0/15
- SW- AA(config-if)#switchport acces vlan 25
- SW- AA(config)#int fa0/20
- SW- AA(config-if)#switchport acces vlan 30

SW-BB

- SW-BB(config)#int f0/15
- SW-BB(config-if)#switchport acces vlan 25
- SW-BB(config-if)#int f0/20
- SW-BB(config-if)#switchport acces vlan 30

SW-CC

- SW-CC(config)#int f0/15

- SW-CC(config-if)#switchport acces vlan 25
- SW-CC(config-if)#int f0/20
- SW-CC(config-if)#switchport acces vlan 30

D. Configurar las direcciones IP en los Switches.
En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

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

Tabla 6. Direcciones IP equipos

SW-AA
- SW-AA(config-if)#int vlan 99
- SW-AA(config-if)#ip add 190.108.99.1 255.255.255.0
- SW-AA(config-if)#no shut

Y ahora deshabilitamos las interfaces que no estamos usando
- SW-AA(config)#int fa0/2
- SW-AA(config)#shutdown
- SW-AA(config)#exit
- SW-AA(config)#int range fa0/4-9
- SW-AA(config)#shutdown
- SW-AA(config)#exit
- SW-AA(config)#int range fa0/11-14
- SW-AA(config)#shutdown
- SW-AA(config)#exit
- SW-AA(config)#int range fa0/16-19
- SW-AA(config)#shutdown
- SW-AA(config)#exit
- SW-AA(config)#int range fa0/21-24
- SW-AA(config)#shutdown

SW-BB
- SW-BB(config-if)#int vlan 99
- SW-BB(config-if)#ip add 190.108.99.2 255.255.255.0

- SW-BB(config-if)#no shut

Y ahora deshabilitamos las interfaces que no estamos usando

- SW-BB(config)#int f0/2
- SW-BB(config-if)#shut
- SW-BB(config-if)#exit
- SW-BB(config)#int range f0/4-9
- SW-BB(config-if-range)#shut
- SW-BB(config-if-range)#exit
- SW-BB(config)#int range f0/11-14
- SW-BB(config-if-range)#shut
- SW-BB(config-if-range)#ex
- SW-BB(config)#int range f0/16-19
- SW-BB(config-if-range)#shut
- SW-BB(config-if-range)#ex
- SW-BB(config)#int range f0/21-24
- SW-BB(config-if-range)#shut

SW-CC

- SW-CC(config)#int vlan 99
- SW-CC(config-if)#ip add 190.108.99.3 255.255.255.0
- SW-CC(config-if)#no shut

Y ahora deshabilitamos las interfaces que no estamos usando

- SW-CC(config)#int fa0/2
- SW-CC(config-if)#shut
- SW-CC(config-if)#ex
- SW-CC(config)#int range f0/4-9
- SW-CC(config-if-range)#shut
- SW-CC(config-if-range)#ex
- SW-CC(config)#int range f0/11-14
- SW-CC(config-if-range)#shut
- SW-CC(config-if-range)#ex
- SW-CC(config)#int range f0/16-19
- SW-CC(config-if-range)#shut
- SW-CC(config-if-range)#ex
- SW-CC(config)#int range f0/21-24
- SW-CC(config-if-range)#shut

E. Verificar la conectividad Extremo a Extremo

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

Desde pc compras SW-CC a pc compras SW-AA

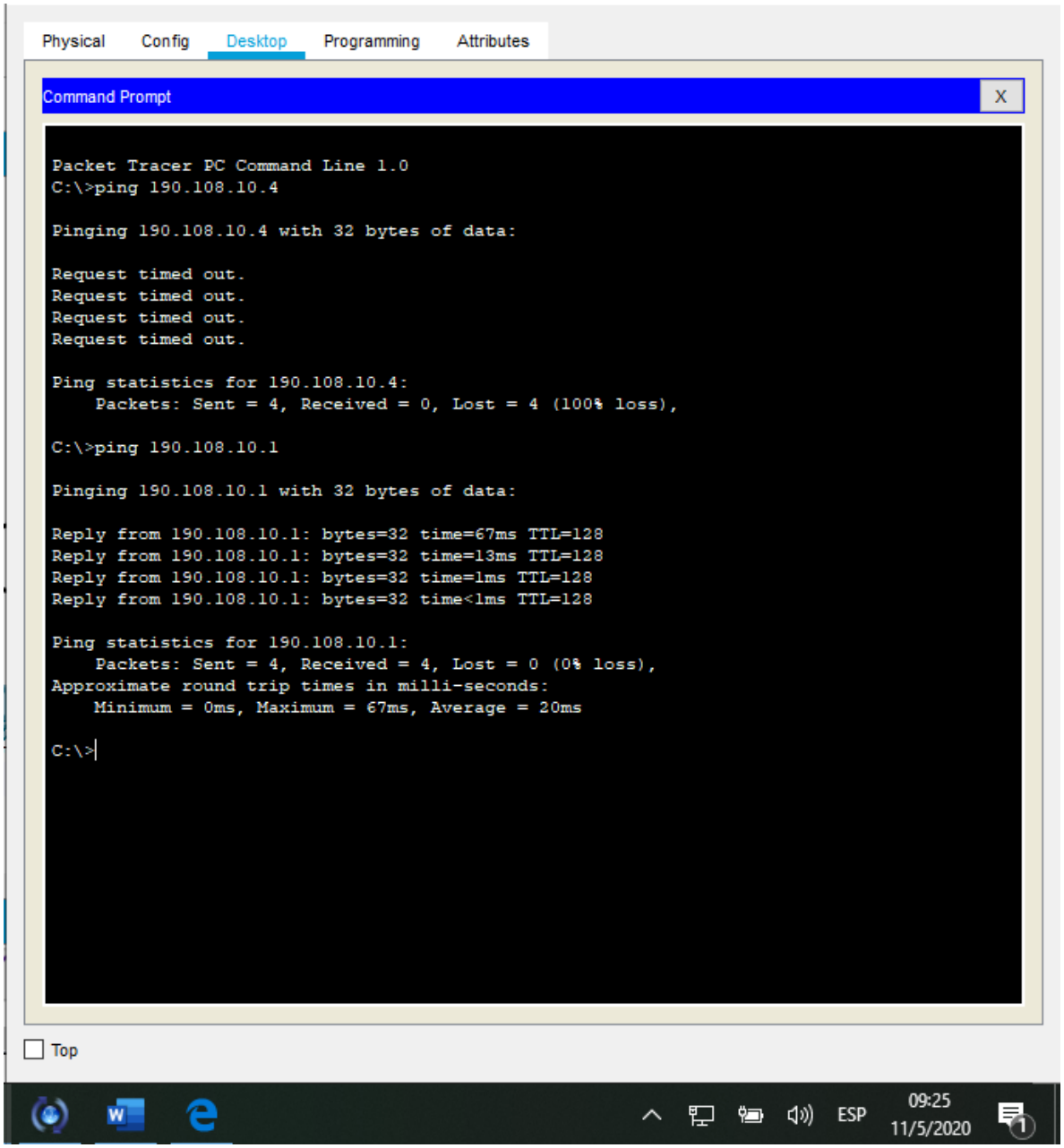

Figura 16. Ping desde pc compras SW-CC a pc compras SW-AA

Tuvo éxito porque los dos equipos están en la misma vlan

Desde pc compras SW-CC a pc personal SW-AA

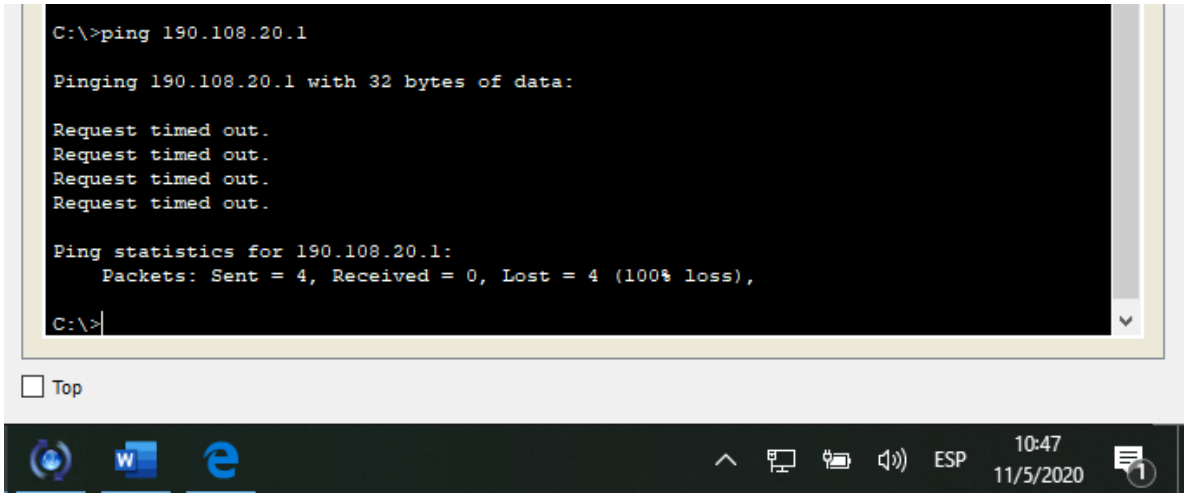

Figura 17. Ping desde pc compras SW-CC a pc personal SW-AA

El ping no tuvo éxito porque están en diferentes vlan y no se realizó una configuración para que compartan información entre ellas

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

Ping desde SW-AA

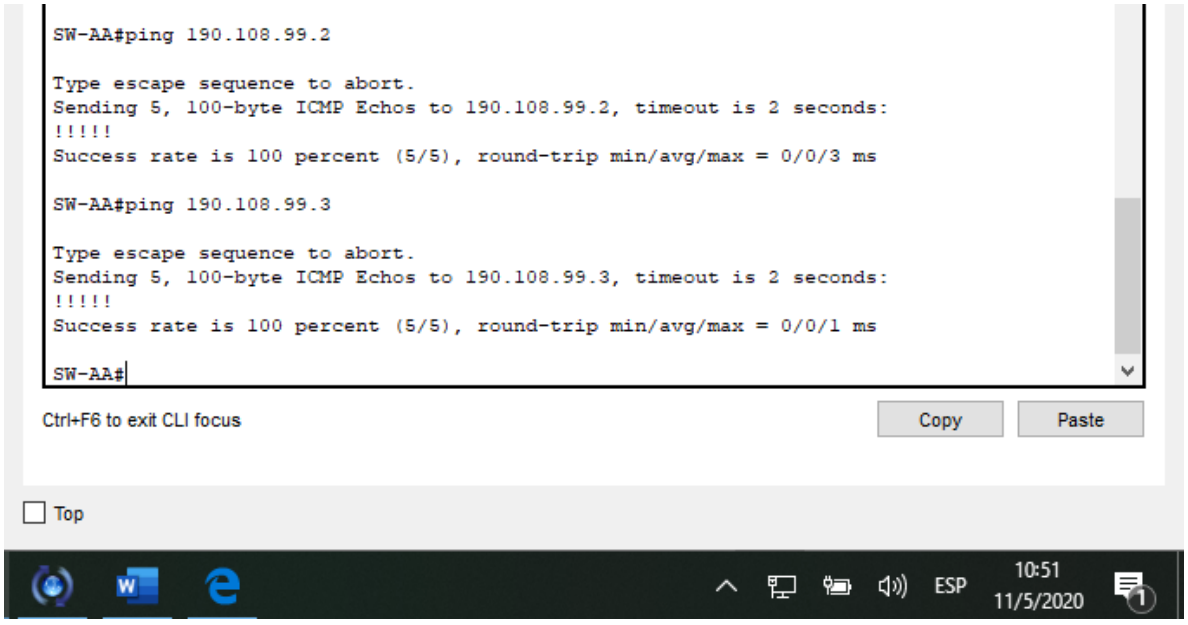

Figura 18. Ping desde SW-AA

Ping desde SW-BB

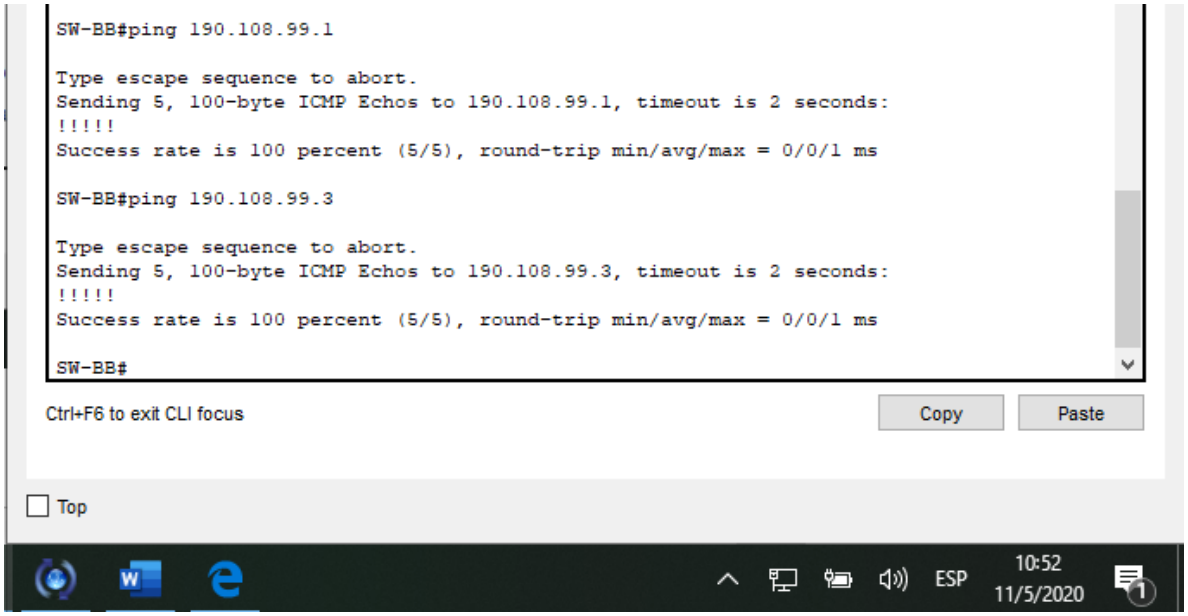

Figura 19. Ping desde SW-BB

Ping desde SW-CC

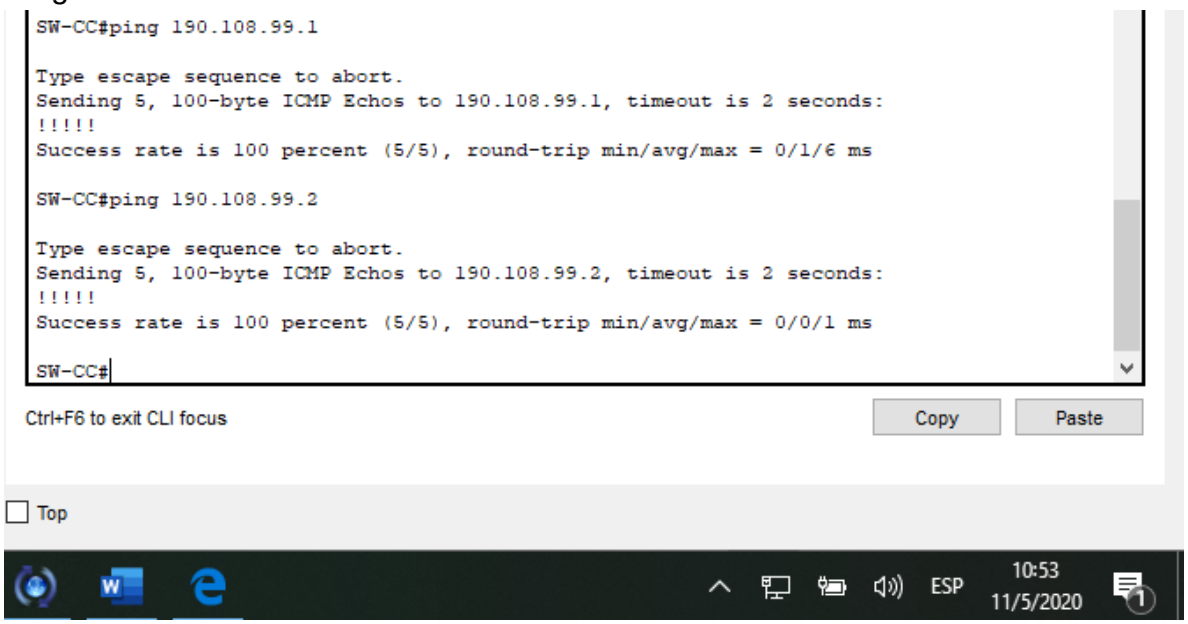

Figura 20. Ping desde SW-CC

El ping entre los tres switches es exitoso porque están dentro de la misma vlan y además cuentan con puertos trunk y estos permiten el paso de paquetes

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

Ping desde SW-AA a los pcs

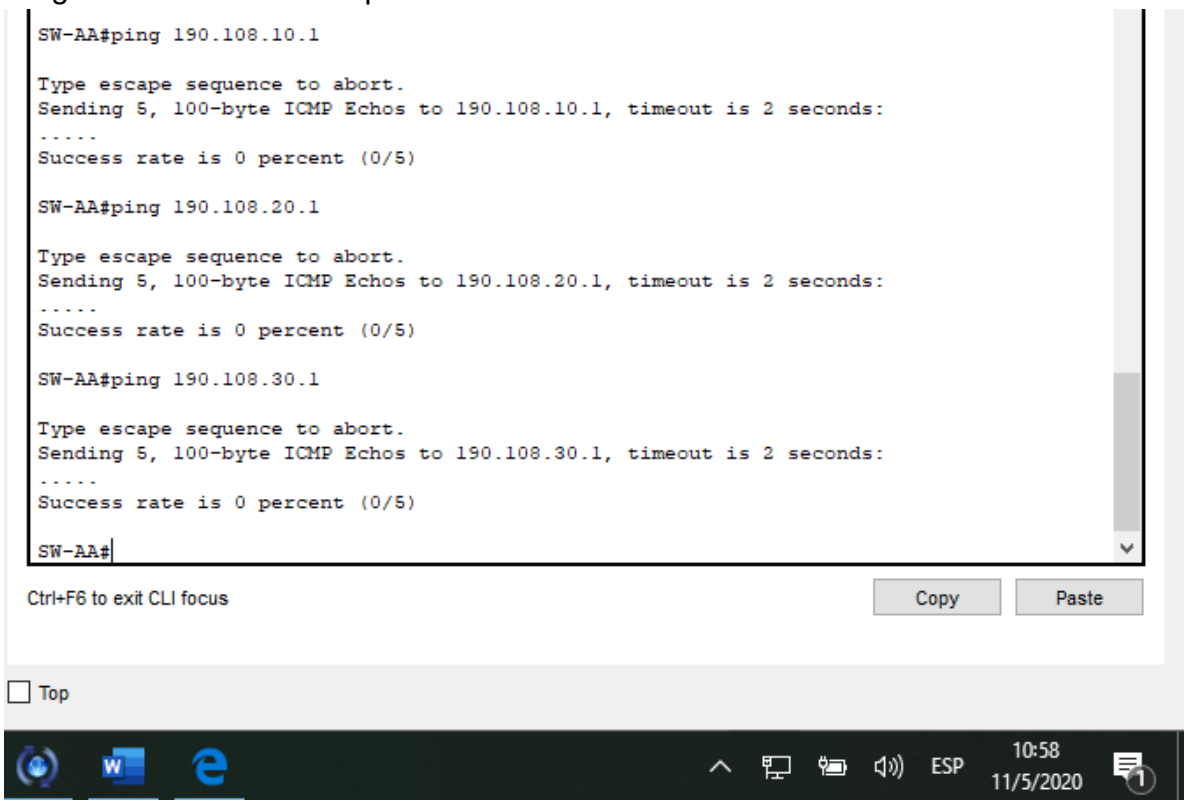

Figura 21. Ping desde SW-AA a los pcs

Ninguno tuvo éxito porque en ningún switch se configuro una dirección ip a una vlan.

CONCLUSIONES

La herramienta Packet Tracer fue de gran ayuda durante todo el curso porque se pudo simular cada ejercicio propuesto en los entornos de las diferentes plataformas y variar los parámetros para comprender más a fondo las características de los dispositivos necesarios en las diferentes prácticas.

Por medio de este curso adquirí distintas habilidades de gestión de redes que están ligadas hoy en día en el mundo de las telecomunicaciones, y que además son indispensables para planificar, asegurar, mantener e implementar y solucionar conflictos de redes convergentes.

Cuando se configura VTP es importante elegir el modo adecuado, ya que VTP es una herramienta muy potente y puede crear problemas en la red. En un mismo dominio VTP la información de VLAN configurada en el servidor se transmite a todos los clientes.

En el último escenario al realizar la verificación final de la conectividad de todos los dispositivos, se logra afianzar los conocimientos obtenidos tras el cumplimiento del curso sobre estas temáticas, al tener que analizar las posibles causas de los fallos en la búsqueda de paquetes mediante los pings realizados entre los dispositivos, identificando las configuraciones faltantes en dichos dispositivos y las soluciones más factibles para estos errores de conectividad.

BIBLIOGRAFÍA

Casos Prácticos de BGP. (30 de octubre de 2008). Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocolbgp/26634-bgp-toc.html

Curso online. Switching y routing CCNA: Introducción a redes. (2018). Obtenido de: https://www.netacad.com

García, V. S. (04 de Julio de 2017). Diseño de Redes con BGP. Obtenido de Universitat Politècnica de València: https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20-%20Dise%C3%B1o%20de%20redes%20con%20BGP.pdf?sequence=1

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ