DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ÁLVARO JOSÉ CÁNDELO SÁNCHEZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ÁLVARO JOSÉ CÁNDELO SÁNCHEZ

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

Como un testimonio de cariño y eterno agradecimiento por mi existencia, valores morales y formación profesional. Porque sin escatimar esfuerzo alguno, han sacrificado gran parte de su vida para formarme y porque nunca podré pagar todos sus desvelos ni aún con las riquezas más grandes del mundo. Por lo que soy y por todo el tiempo que les despojé pensando en mí, gracias con amor y respeto.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CCNA: Significa cisco Certified Network Associated que alude a un programa de certificación para ingenieros de redes de nivel básico que ayuda a aumentar su inversión en conocimiento de redes fundacional y aumenta el valor de la red de su empleador.

CCNP: Esta certificación indica que su titular posee conocimientos avanzados sobre redes que le permiten instalar, configurar y manejar redes LAN, WAN y servicios de acceso para organizaciones de 500 ordenadores aproximadamente.

ROUTER: El enrutador (calco del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI.

SWITCH: Es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes. Switch es una palabra en inglés usada en el área de informática para referirse al controlador de interconexión entre varios dispositivos.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10Mbps, por lo tanto, tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN)en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

EGP: (Exterior Gateway Protocol) - Protocolo de ruteo usado para intercambiar información de ruteo entre sistemas autónomos.

IGP: (Interior Gateway Protocol) - Protocolo de ruteo usado para intercambiar información de ruteo dentro de un sistema autónomo.

TRUNK: Es una configuración de canal para puertos de switch que estén en una red Ethernet, que posibilita que se pueda pasar varias VLAN por un único link, o sea, un link de troncal es un canal que puede ser switch-switch o switch-router, por donde se pasan informaciones originadas y con destino a más de una VLAN.; así el link de la troncal no pertenece a ninguna VLAN individualmente.

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

LOOPBACK: El dispositivo de red loopback es una interfaz de red virtual. Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers. y son usualmente 10 utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

RESUMEN

El Diplomado de Profundización CCNP Routing and Switching desarrollado por la compañía CISCO SISTEMS, tiene un plan de estudios que se agrupa en el desarrollo de las habilidades necesarias para que el estudiante realice redes escalables, construya redes que abarquen un campus, diseñe e instale intranets globales, electrónica, así como la detección, prevención y solución de problemas de enrutamiento.

Este curriculum avanzado capacita a los estudiantes para instalar, configurar y operar redes locales y de área amplia, y para brindar servicios de acceso por conmutación a organizaciones que tienen redes desde 100 hasta 500 nodos con diversos tipos de protocolos y tecnologías.

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

ABSTRACT

The CCNP Routing and Switching Deepening Diploma developed by the company CISCO SISTEMS, has a curriculum that is grouped in the development of the necessary skills for the student to make scalable networks, build networks that cover a campus, design and install global intranets , electronics, as well as the detection, prevention and solution of routing problems.

This advanced curriculum enables students to install, configure, and operate local and wide area networks, and to provide access services for switching to organizations that have networks from 100 to 500 nodes with various types of protocols and technologies.

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

INTRODUCCIÓN

En el desarrollo del presente diplomado busca desarrollar en el universitario desarrollar esas competencias y habilidades de redes de nivel empresarial, profesionales TI que desean expandir sus habilidades básicas en enrutamiento, conmutación y solución de problemas de red para avanzar en su carrera, personal que haya realizado la formación en la Academia CISCO, que desean avanzar en su conocimiento base o en otros casos que estrictamente personas que desean obtener la certificación CCNP Routing and Switching.

Este curso se enfoca en routers Cisco conectando LANs y WANs en redes de mediano a gran tamaño, orientado para conocer cómo elegir e implementar servicios Cisco IOS para redes enrutadas y escalables.

Cisco Networking Academy con este curso identifica y desarrolla las destrezas que los cada uno de nosotros para prosperar en una economía cambiante, preparando un personal idóneo para el futuro del campo laboral.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología solicitada en el escenario 1

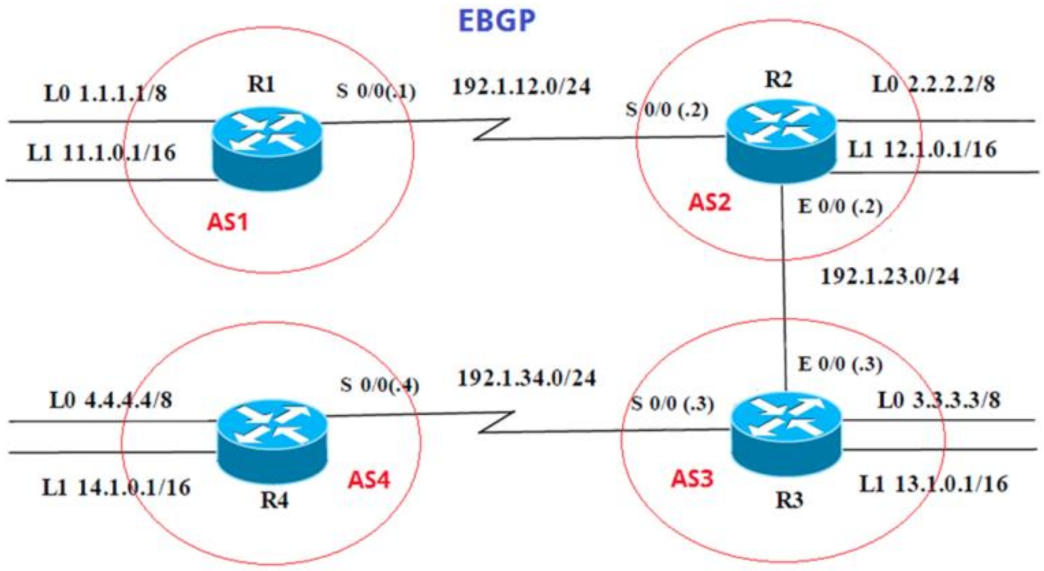


Figura 2. Topología generada Packet Tracer escenario 1

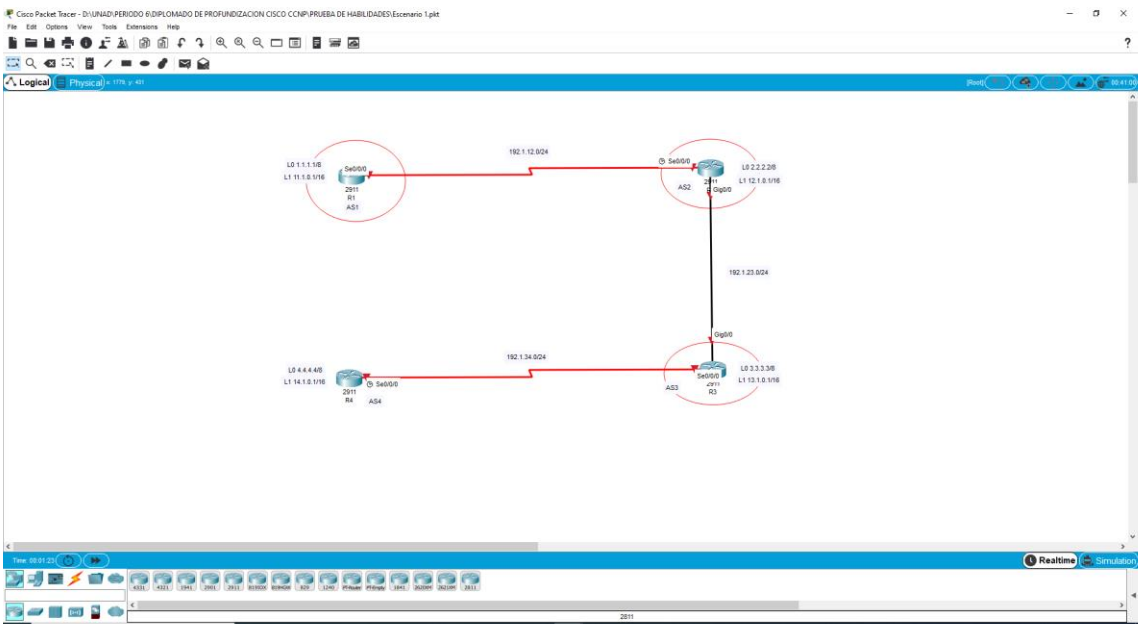


Tabla 1. Información para configuración de los Routers

	Interfaz	Dirección IP	Máscara
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
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
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
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

Configuración R1

R1#enable
R1#configure terminal
R1(config)#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
R1(config)#interface loopback0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface loopback1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit

Configuración R2
R2#enable
R2#configure terminal
R2(config)#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)#exit
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip address 192.1.23.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface loopback0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface loopback1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit

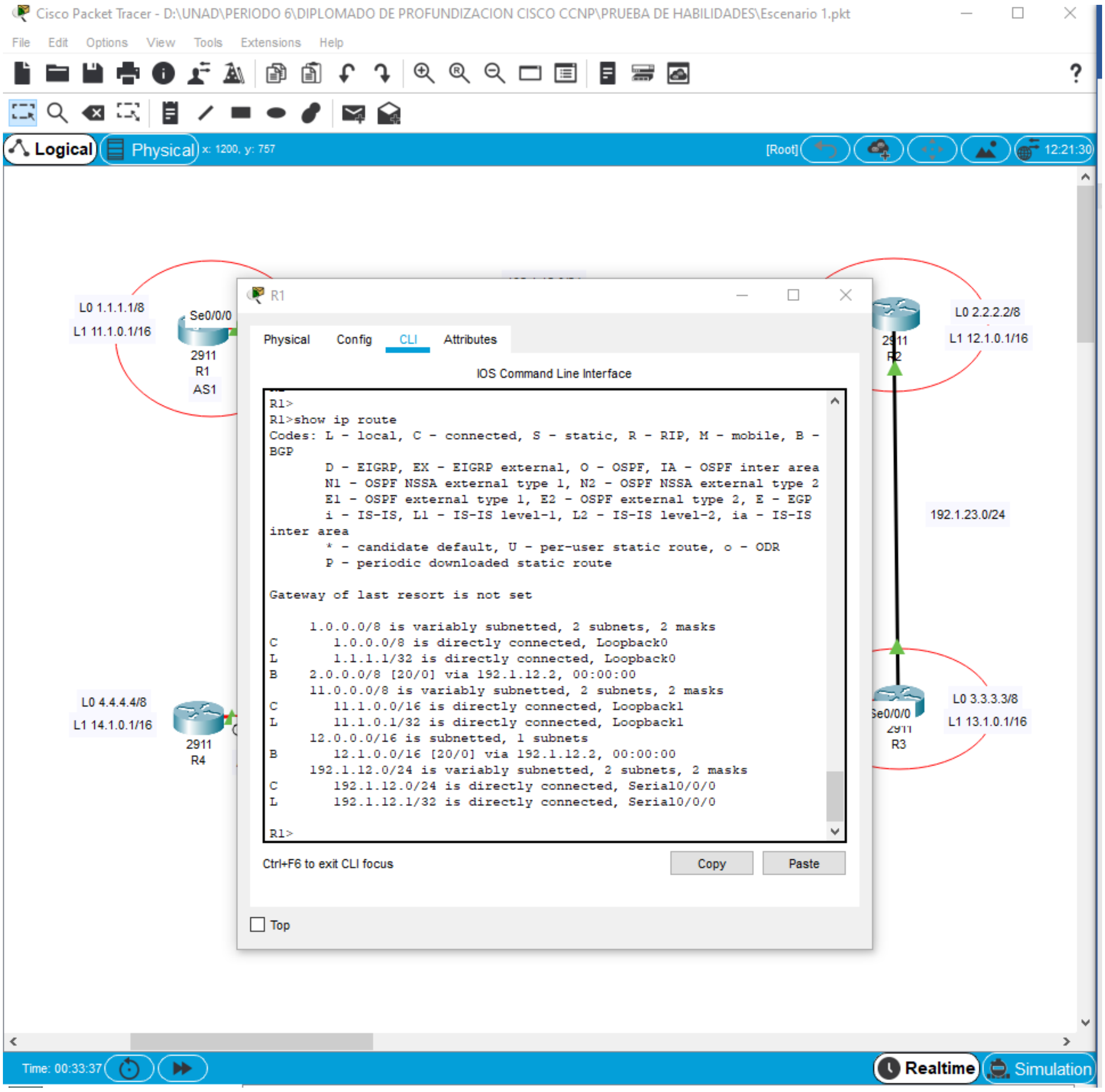
Configuración R3
R3#enable
R3#configure terminal
R3(config)#interface serial 0/0/0
R3(config-if)#ip address 192.1.34.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface loopback1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit

Configuración R4
R4#enable
R4#configure terminal
R4(config)#interface serial 0/0/0
R4(config-if)#ip address 192.1.34.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface loopback0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface loopback1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit

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.

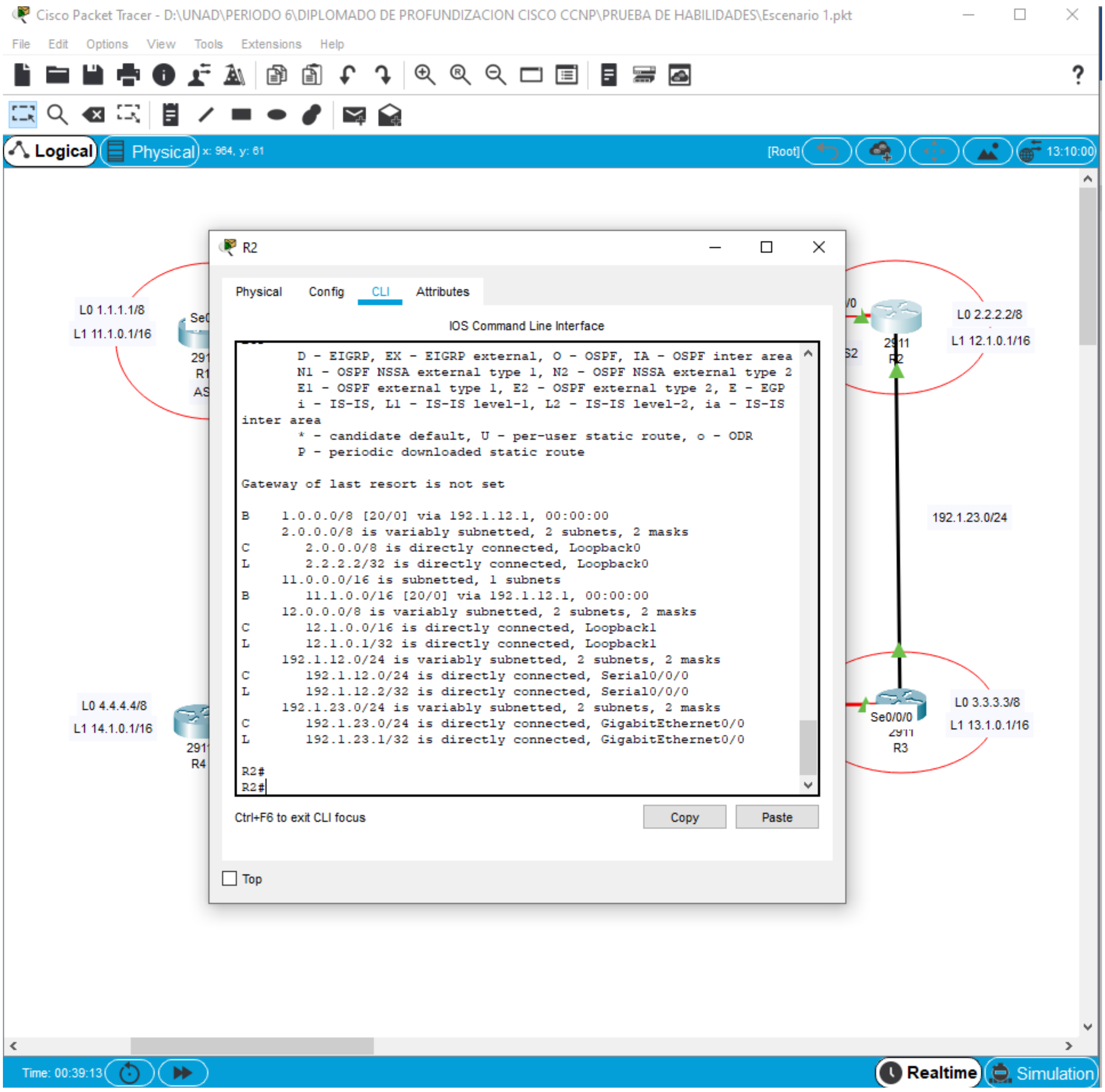
R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#bgp router-id 22.22.22.22

Figura 3. Relación de vecino BGP entre R1 y R2



R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.2.2.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#bgp router-id 33.33.33.33

Figura 4. Relación de vecino BGP entre R2 y R1



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(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.2 remote-as 3

R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.1 remote-as 2
R3(config-router)#network 3.3.3.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44

Figura 5. Relación de vecino BGP entre R2 y R3

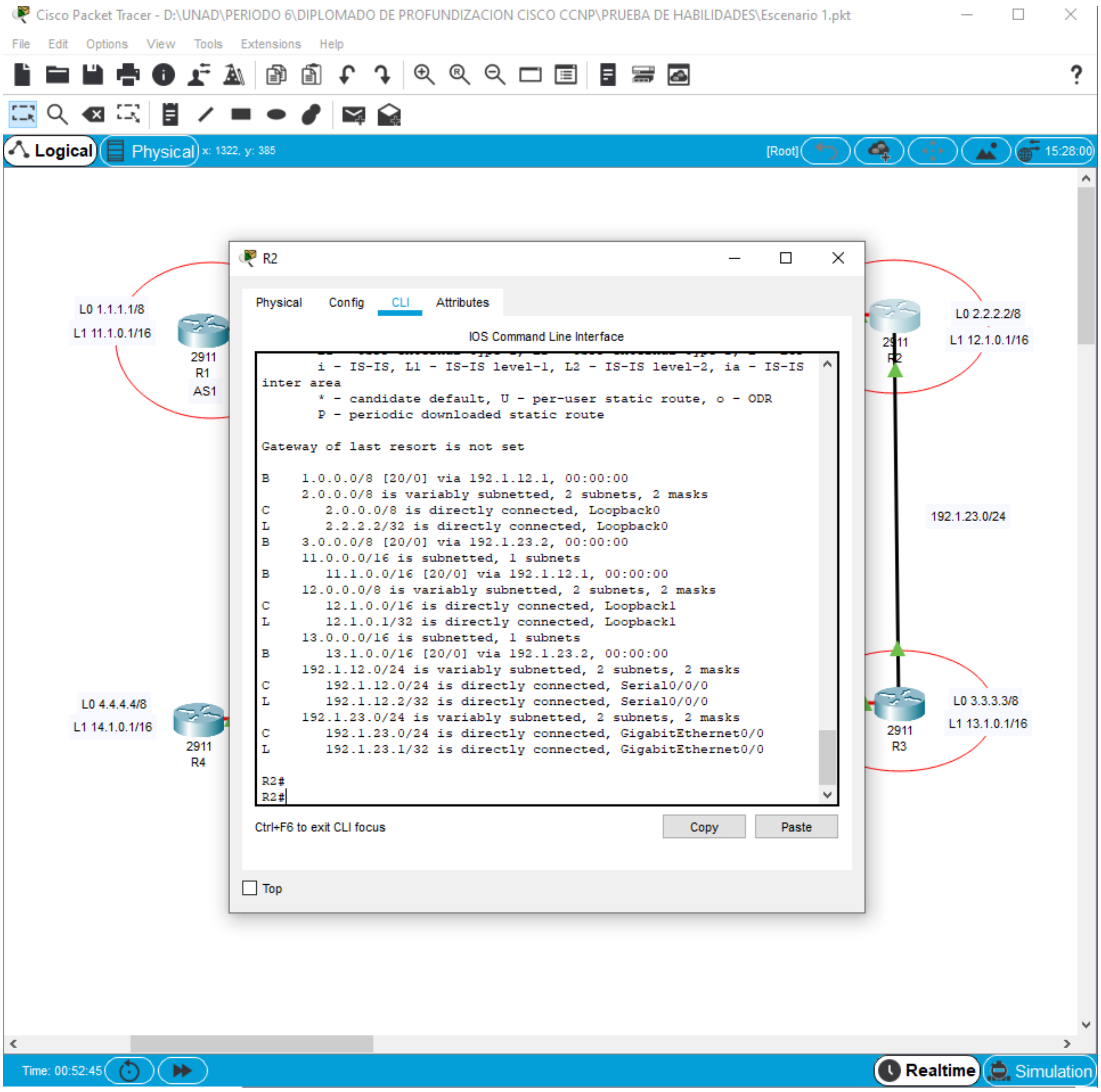
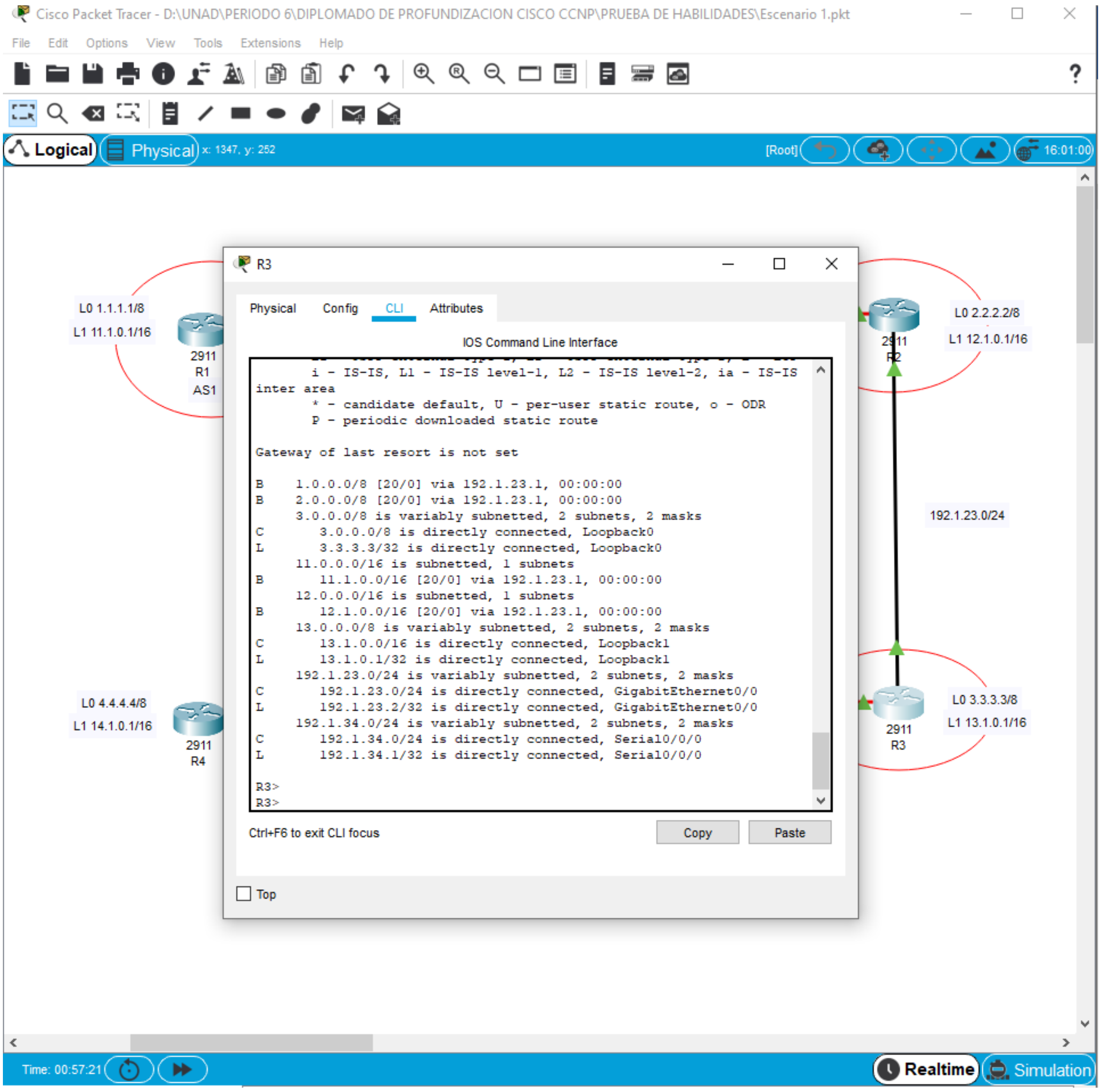


Figura 6. Relación de vecino BGP entre R3 y R2



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(config)#router bgp 3
R3(config-router)# neighbor 4.4.4.0 remote-as 4
R3(config-router)#exit
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.2

R4(config)#router bgp 4
R4(config-router)#neighbor 3.3.3.0 remote-as 3
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.1

Figura 7. Relación de vecino BGP entre R3 y R4

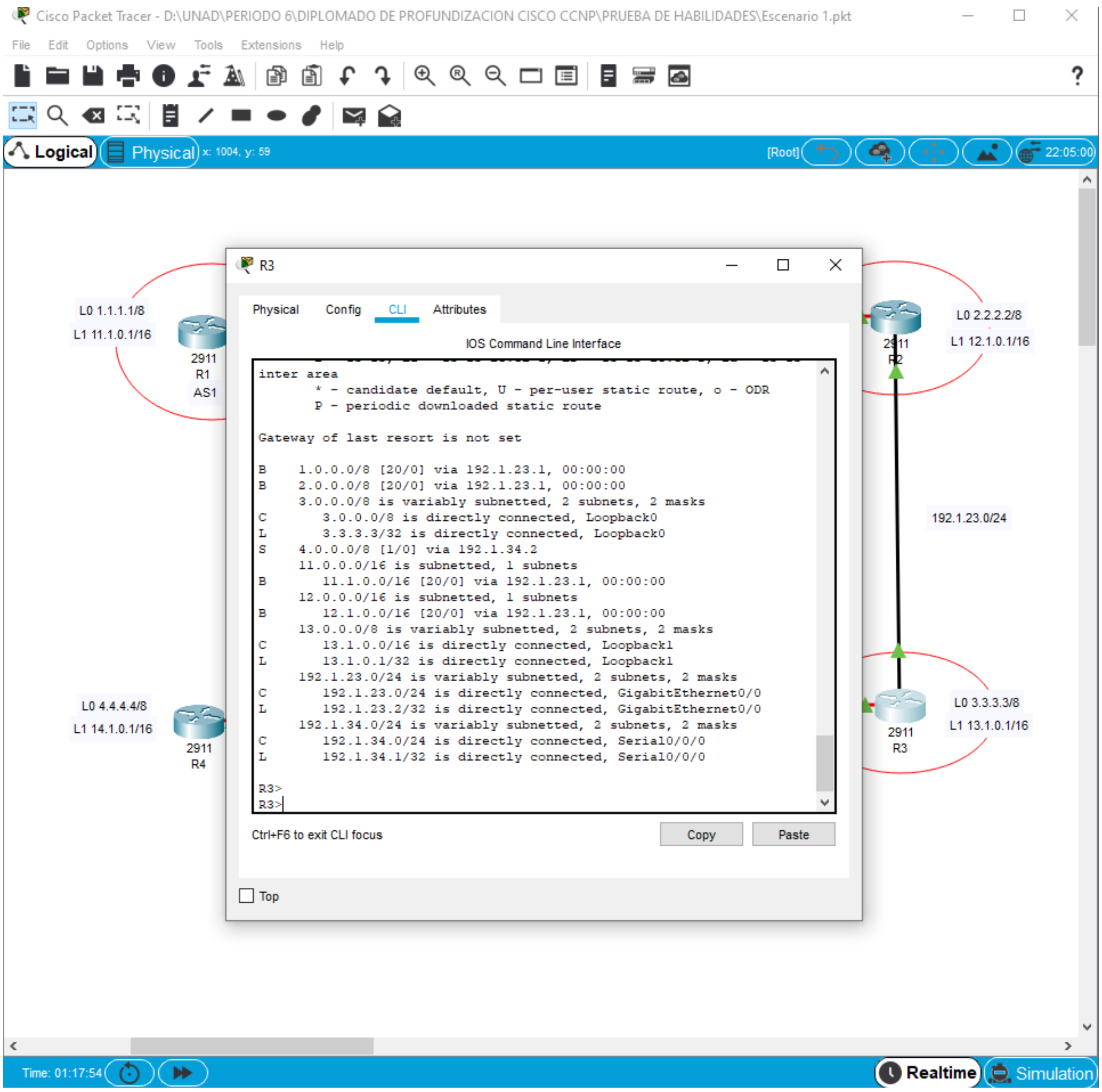
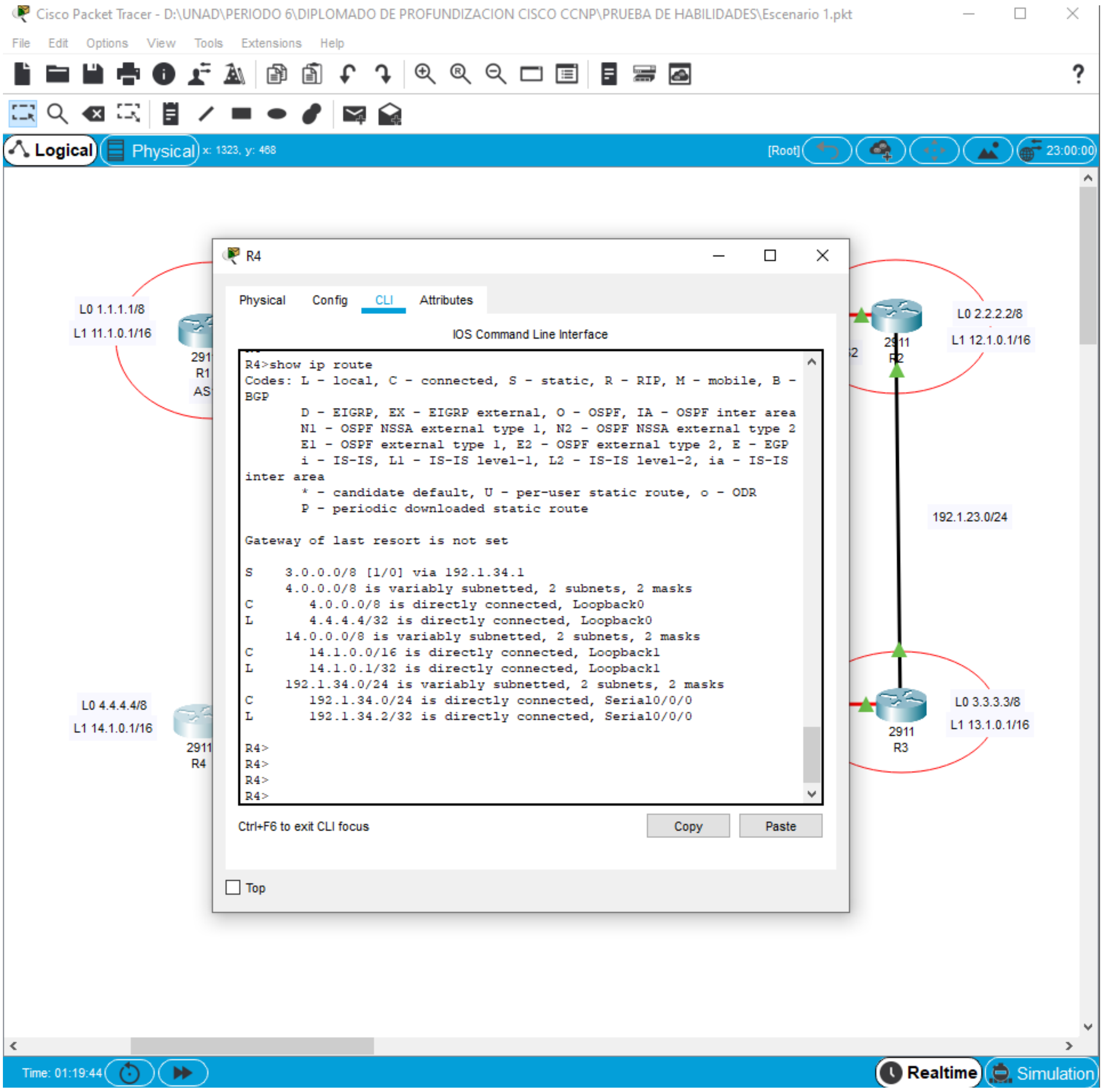


Figura 8. Relación de vecino BGP entre R4 y R3



2. ESCENARIO 2

Figura 9. Topología solicitada en el escenario 2

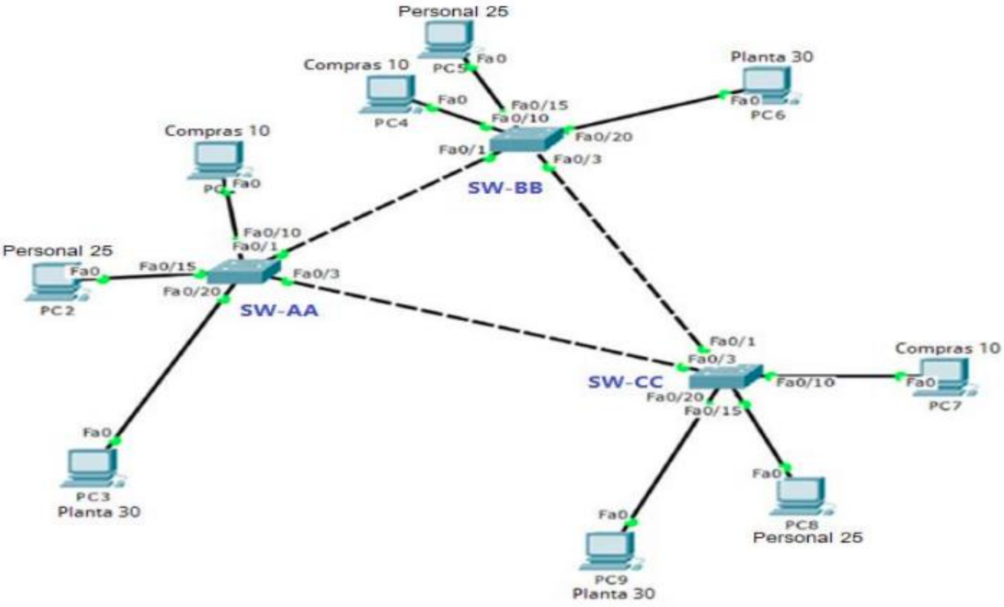
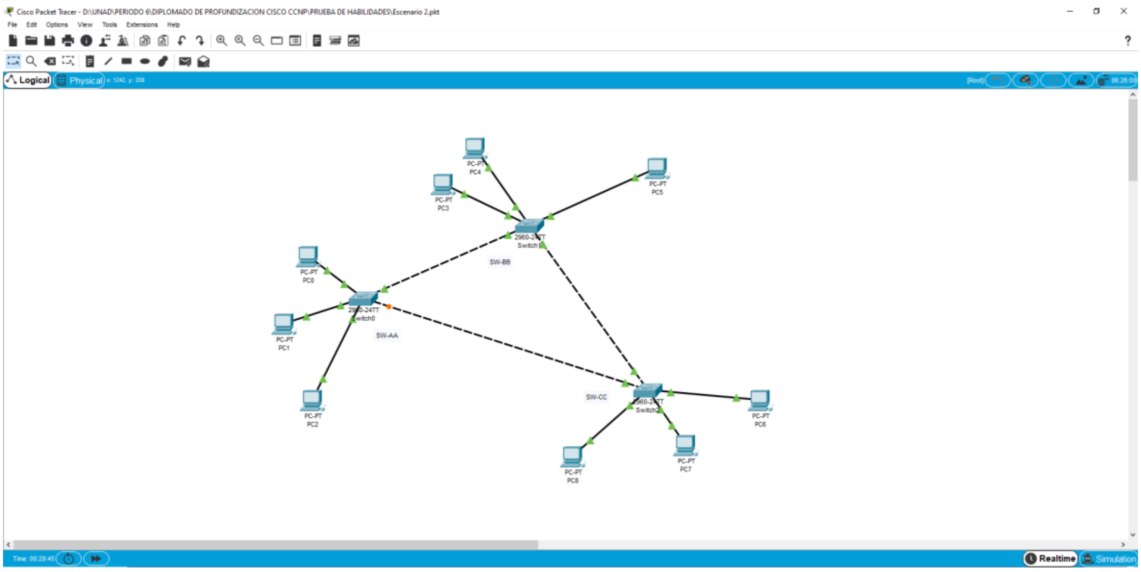


Figura 10. Topología generada Packet Tracer escenario 1



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.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BB
SW-BB(config)#vtp domain CCNP
SW-BB (config)#vtp mode server
SW-BB (config)#vtp password cisco

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-AA
SW-AA (config)#vtp domain CCNP
SW-AA(config)#vtp mode client
SW-AA (config)#vtp password cisco

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp mode client
SW-CC (config)#vtp password cisco
```

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

Figura 11. VTP de SW-BB

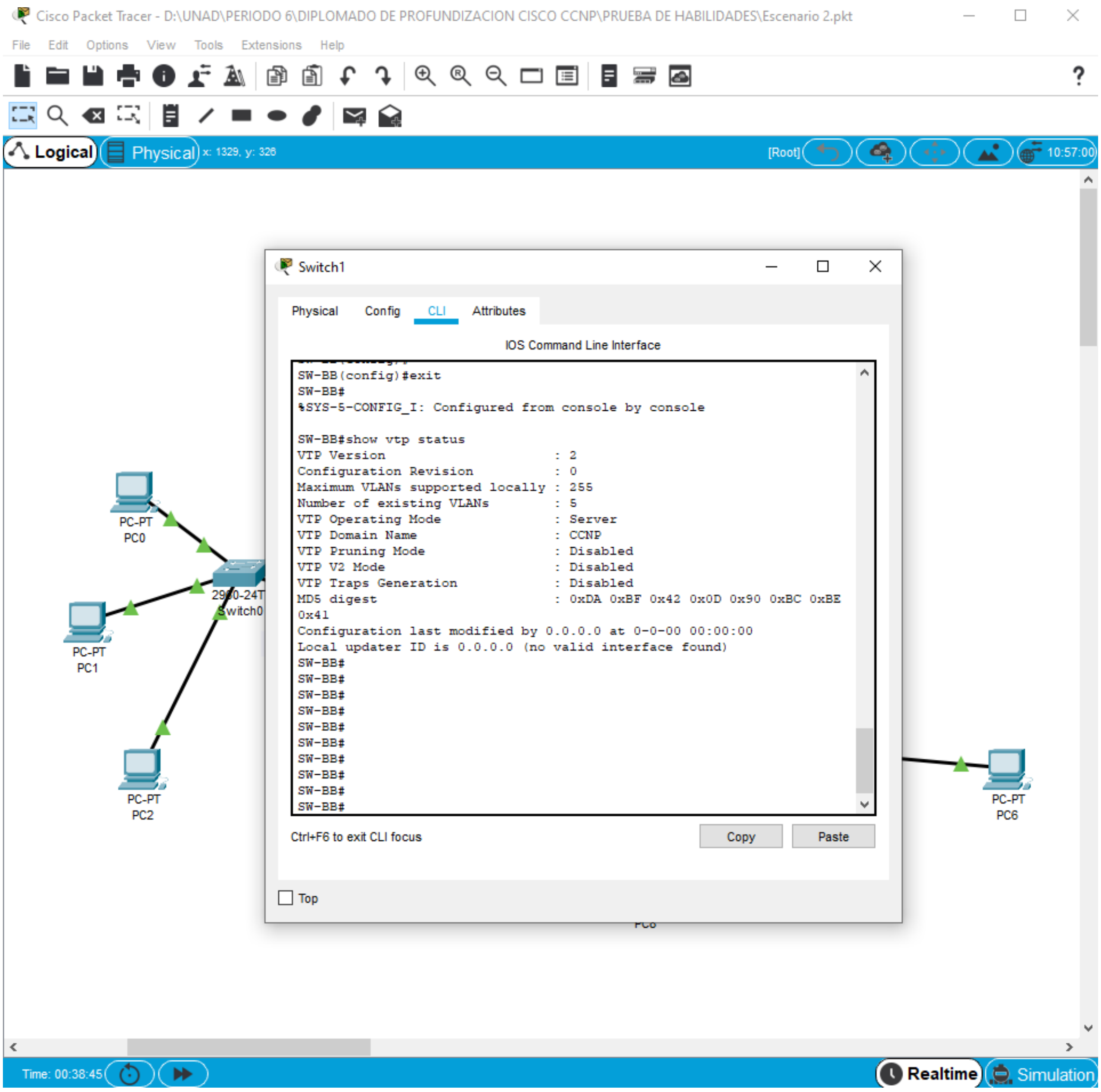


Figura 12. VTP de SW-AA

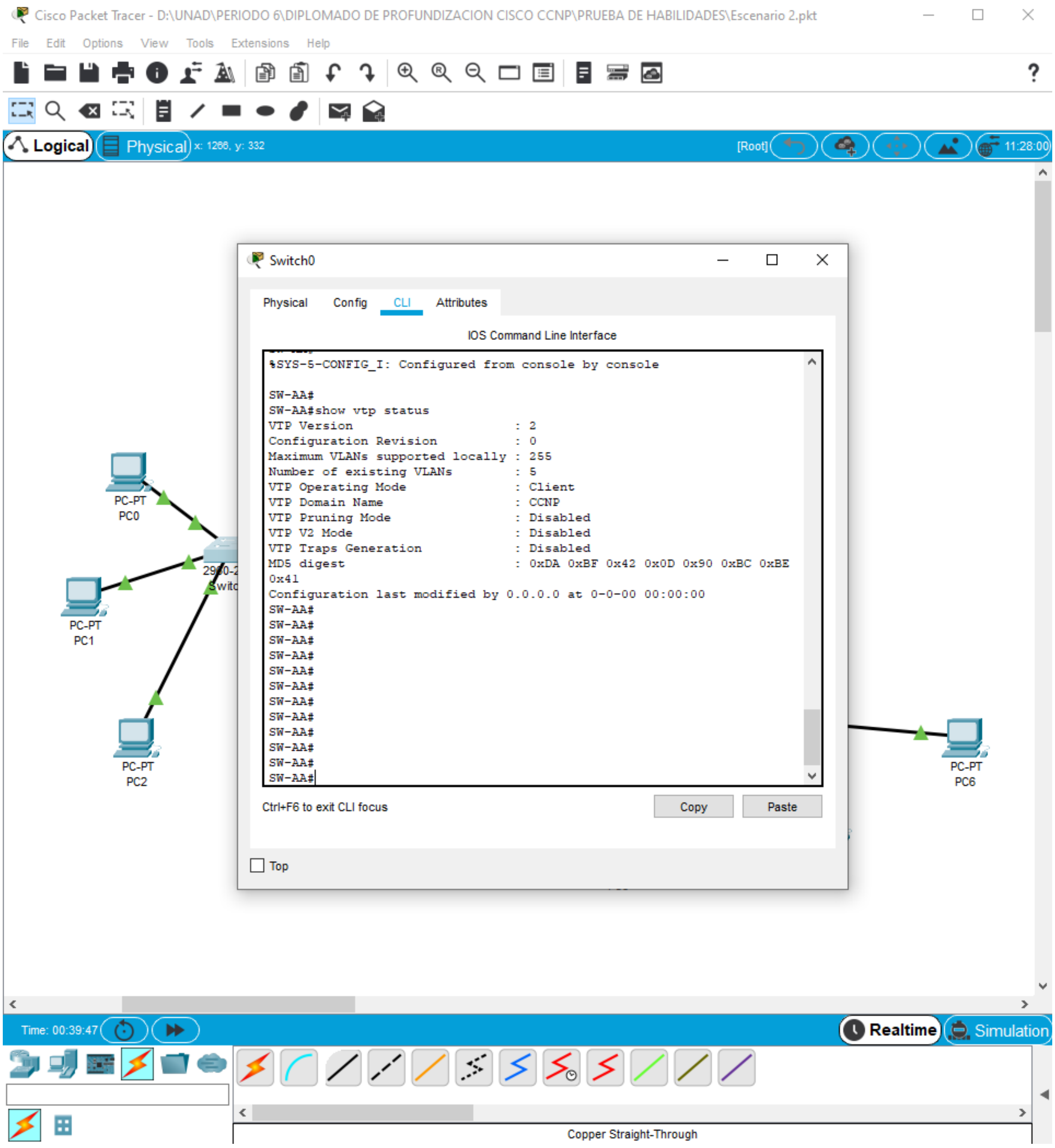
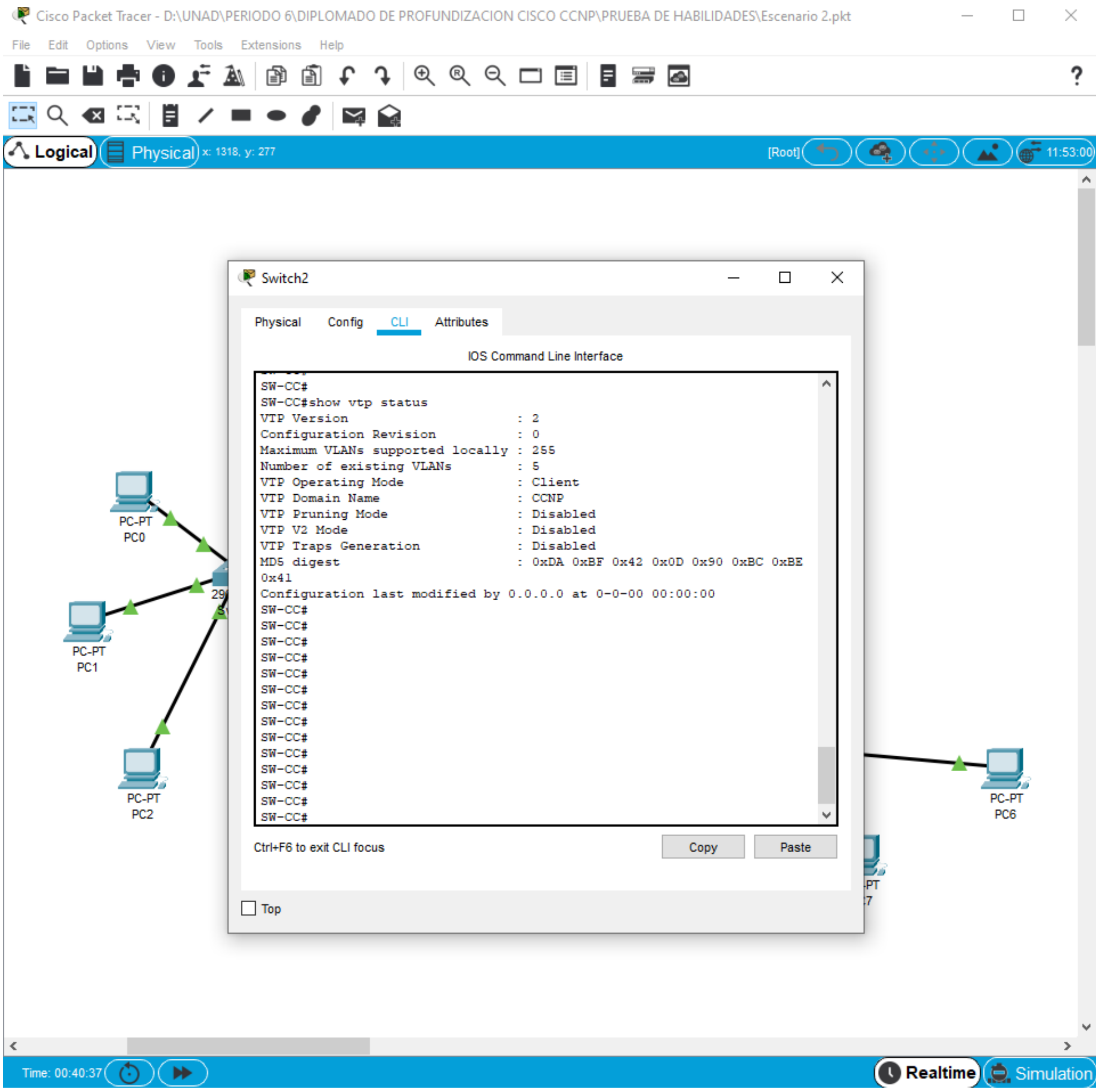


Figura 13. VTP de SW-CC



B. Configurar DTP (Dynamic Trunking Protocol)

3. 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(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable

SW-AA(config)# interface fastEthernet 0/1
SW-AA(config)# switchport mode trunk

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

Figura 14. Troncal SW-BB

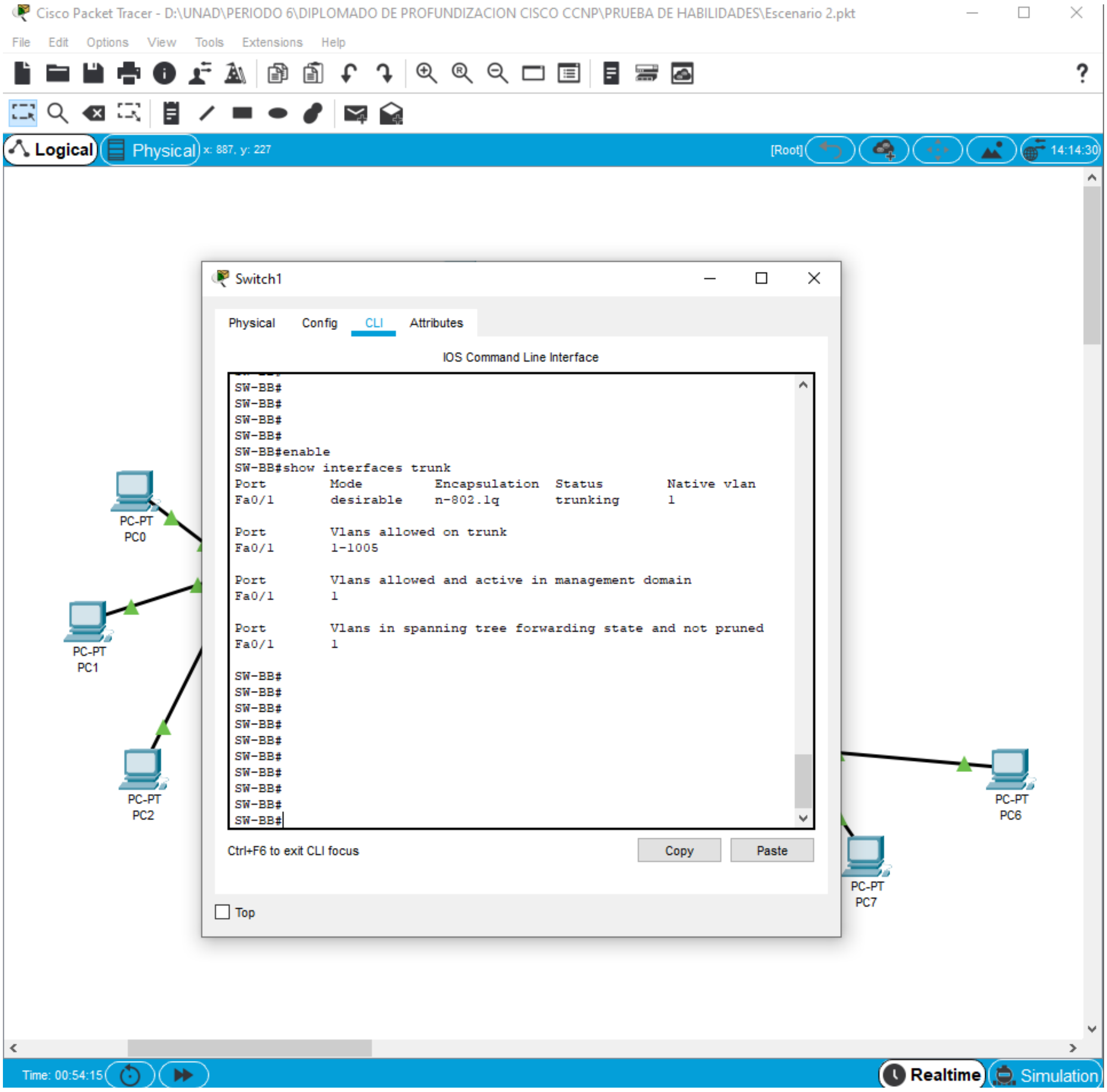
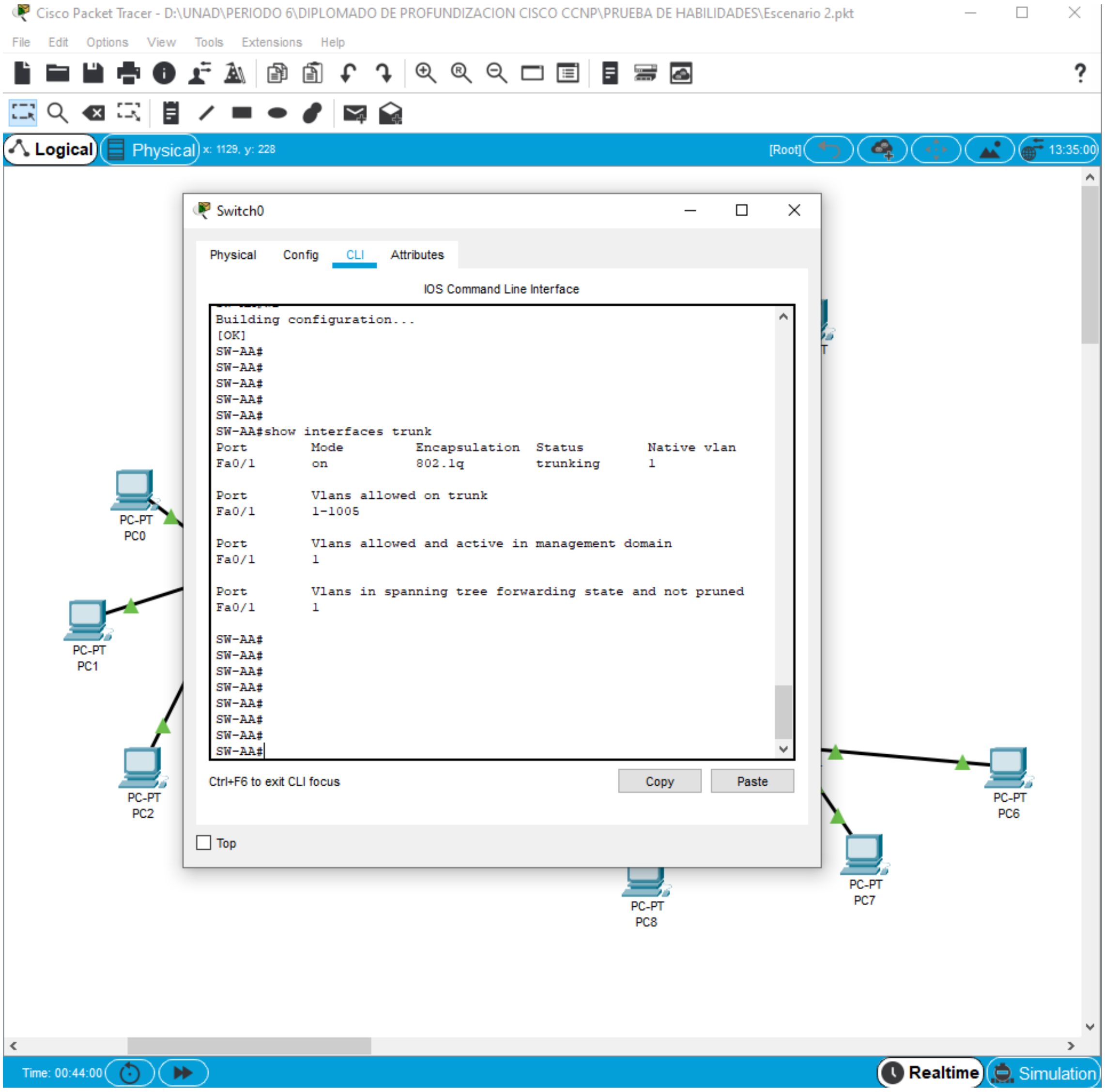


Figura 15. Troncal SW-AA

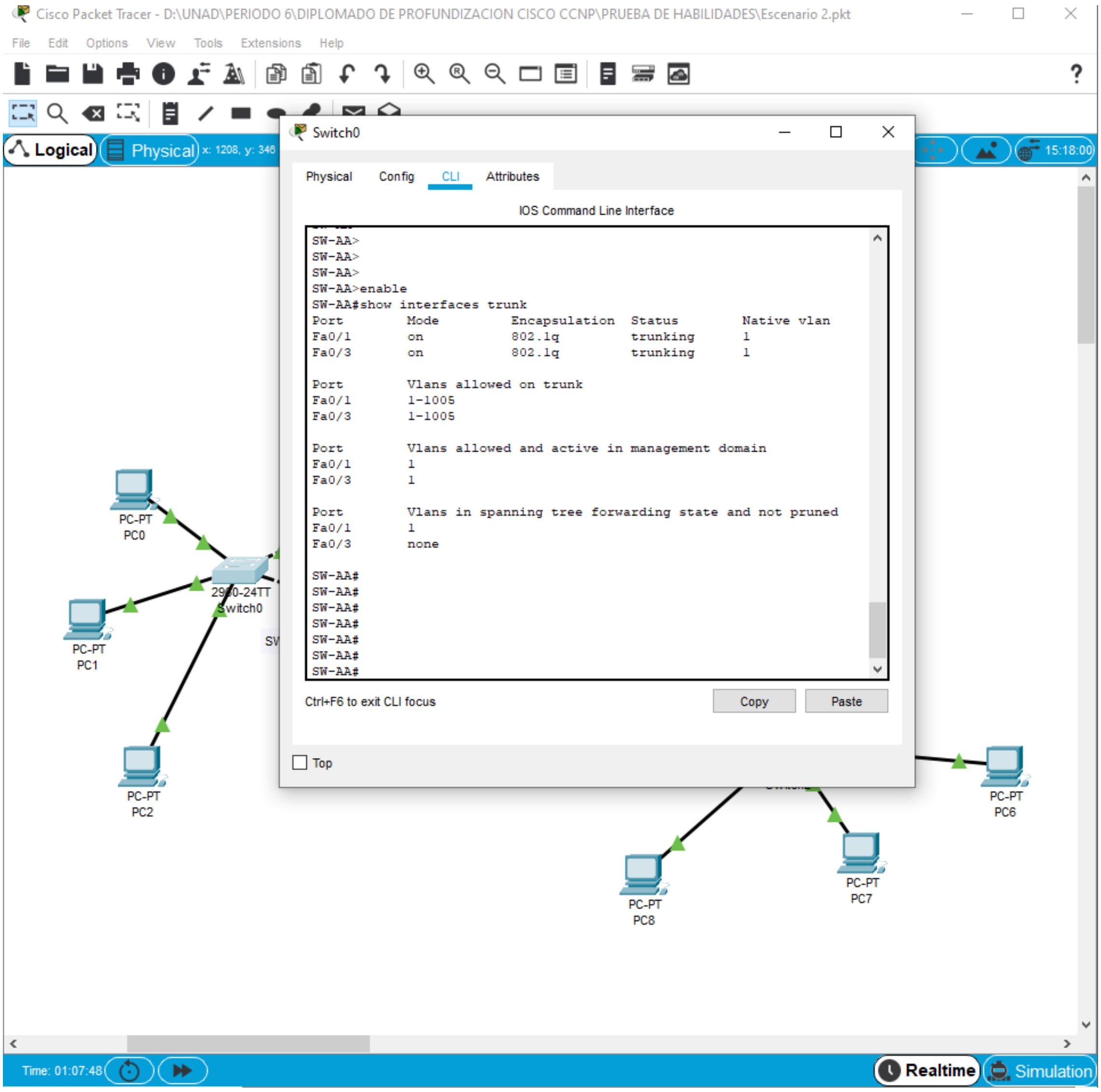


5. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

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

Figura 16. Troncal SW-AA



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

SW-BB(config)#interface fastEthernet 0/3
SW-BB(config-if)#switchport mode trunk

SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk

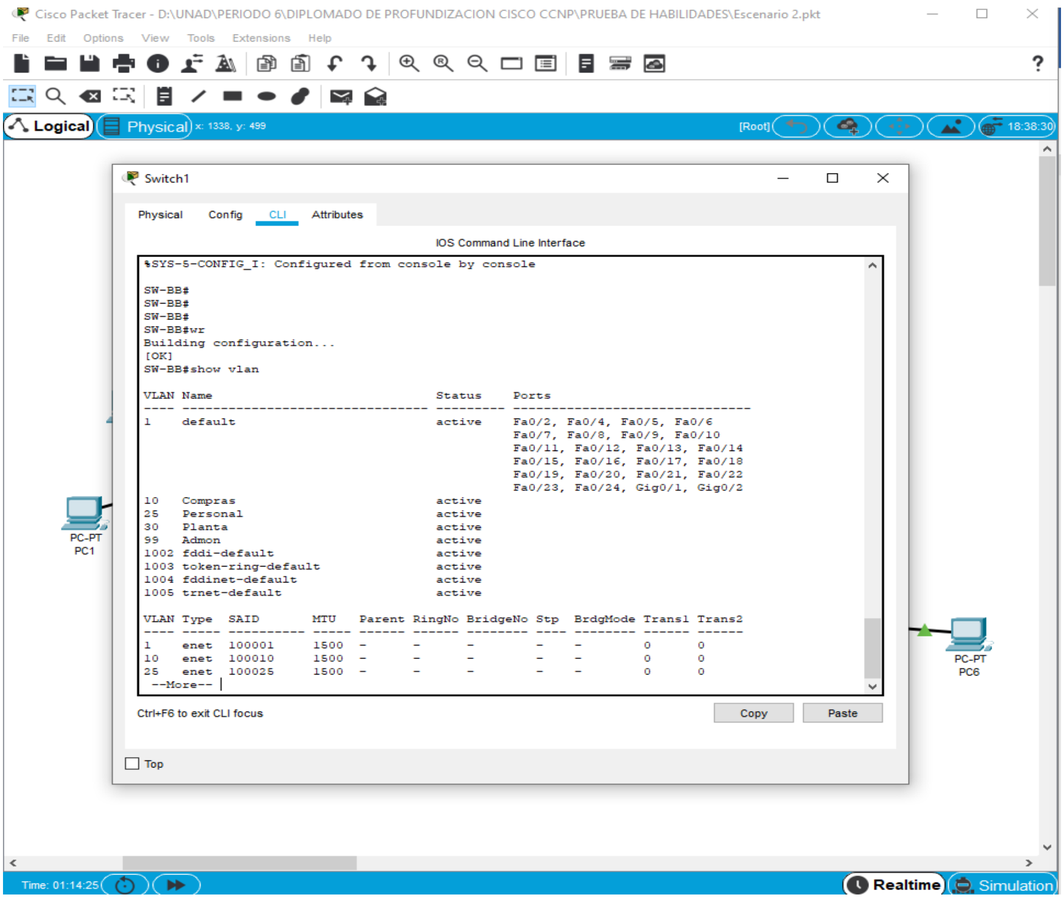
C. Agregar VLANs y asignar puertos.

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

SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config)#exit

9. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLANs en SW-BB



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

Tabla 2. IP de equipos.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.25.X / 24
F0/20	VLAN 30	190.108.30.X / 24
X= número de cada PC particular		

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

SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10

SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10

SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10

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

SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

D. Configurar las direcciones IP en los Switches.

13. 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 3. IP de Switch

Equipo	Interfaz	Dirección	Masacra
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

SW-BB(config)#interface VLAN 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0

SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0

E. Verificar la conectividad Extremo a Extremo

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

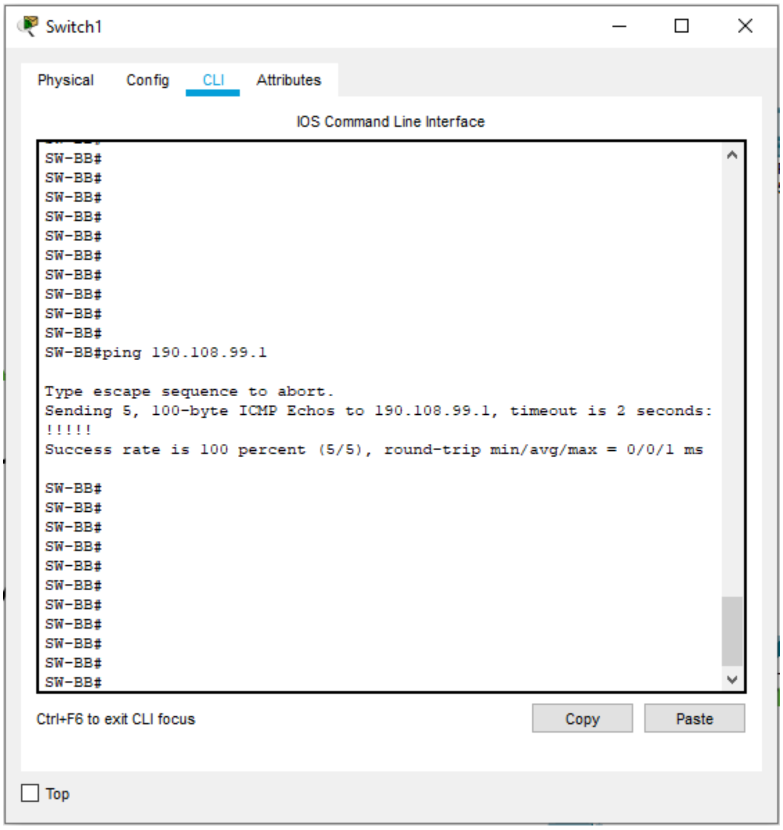
Se realiza ping entre los diferentes equipos, observándose lo siguiente:

- Cuando se realiza en ping o envió de paquetes entre equipos que estén conectados en la misma VLAN el ping es exitoso

- Cuando se realiza en ping o envío de paquetes entre equipos ubicados en VLAN diferente el ping es fallido.

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

Figura 18. PING SW-BB



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

En el siguiente paso se ejecutó un ping desde cada uno de los Switch direccionado hacia los diferentes equipos, los pings fueron fallidos, esto a raíz que no existe una discreción IP en cada una de las Vlan de los switch, que desarrollan la actividad de enlace predeterminada para los equipos.

CONCLUSIONES

Dado al presente diplomado de profundización se adquieren conocimientos más concretos y enfáticos sobre el Routing and Switching en la tecnología de redes CISCO, generando en el universitario ambientes de interacción con plataformas y simuladoras en implementación de redes, donde se realizan las pruebas y laboratorios requeridos en el diplomado.

Las temáticas y talleres planteados en Cisco proporcionan una colección de recursos que ayudan al universitario a prepararse y fortalecer competencias para los exámenes de certificación CCNP.

El curso se centra en proveer herramientas y habilidades que debe tener un profesional en redes de telecomunicaciones para detectar, aislar y resolver fallas en redes empresariales complejas. Los casos de estudio abarcan todos los conceptos y tecnologías asociadas al enrutamiento y conmutación avanzada enfatizando en el uso de dispositivos de Cisco.

BIBLIOGRAFÍA

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). First Hop Redundancy Protocols. 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). v. 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). High Availability. 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