

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS CARLOS MENA MSOQUERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
MEDELLIN
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNP

LUIS CARLOS MENA MSOQUERA

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

DIRECTOR
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA DE TELECOMUNICACIONES
MEDELLIN
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLIN, 29 de noviembre de 2021

DEDICATORIA

Es un placer satisfactorio poder llegar hasta este punto y decir no fue fácil, pero lo logré, sacrificios metas duras, pero me hicieron cada día mejor dedico este título de profesional en ingeniería de telecomunicaciones a mi familia que tanto apoyo me brindaron durante este largo viaje

AGRADECIMIENTOS

Me siento muy agradecido con las personas que creyeron en mí en el momento que emprendí este proyecto de vida, se me presentaron muchos obstáculos en el camino, no fueron fáciles de superar, pero con la convicción de alcanzar mi sueño pude salir victorioso.

Hoy doy gracias a Dios y a mi familia de haber hecho de este tiempo el mejor de toda la vida, me hizo entender que todo tiene un propósito y el mío fue ser ingeniero de telecomunicaciones.

Estoy más que complacido gracias a la red de tutores de los diferentes cursos que ayudaron a hacer este sueño realidad, y las observaciones en cada uno de los foros de los compañeros quienes ayudaron con su granito de arena para poder mejorar y alcanzar los objetivos.

Al personal administrativo del CEAD Medellín, quienes fueron encargados de revisar mis avances y despejaron mis dudas, fue una grata experiencia en esta modalidad virtual donde obtuve un buen desempeño académicamente, muchas gracias UNAD.

CONTENIDO

LISTA DE TABLAS	7
LISTA DE ILUSTRACIONES	8
GLOSARIO	10
RESUMEN.....	11
INTRODUCCIÓN.....	12
DESARROLLO	13
1. Escenario 1	15
CONCLUSIONES	73
BIBLIOGRAFÍA.....	74

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento	14
Tabla 2. Tareas de configuración parte 2	25
Tabla 3. Tareas parte 3 protocolos de enrutamiento	33
Tabla 4. Tareas de configuración parte 4	40
Tabla 5. Tareas de configuración parte 5	49
Tabla 6. Tareas de configuración parte 6	57

LISTA DE ILUSTRACIÓN

Ilustración 1. Topología de la Red	13
Ilustración 2. Topología en GNS3.....	15
Ilustración 3. Configuración Router R1	16
Ilustración 4. Configuración Router R2	17
Ilustración 5. Configuración Router R3	18
Ilustración 6. Configuración Switch D1	20
Ilustración 7. Configuración Switch D2	22
Ilustración 8. Configuración Switch A1.....	23
Ilustración 9. Configuración IP - PC 1 y PC 4	24
Ilustración 10. Configuración Switch D1 parte 2	27
Ilustración 11. Configuración Switch D2 parte 2	28
Ilustración 12. Configuración Switch A1 parte 2.....	29
Ilustración 13. Verificación de la configuración 2.2	30
Ilustración 14. Verificación de la configuración 2.3	31
Ilustración 15. Verificación de la configuración 2.6	32
Ilustración 16. conectividad de la LAN local.....	32
Ilustración 17. Configuración R1 parte 3.....	35
Ilustración 18. Configuración R2 parte 3.....	36
Ilustración 19. Configuración R3 parte 3.....	37
Ilustración 20. Configuración Switch D1 parte 3	38
Ilustración 21. Configuración Switch D2 parte 3	39
Ilustración 22. Configuración Switch D1 parte 4	44
Ilustración 23. Configuración Switch D2 parte 4	46
Ilustración 24. Verificación tarea 4.1 y el punto 3 de la tarea 4.3.....	47
Ilustración 25. Verificación tarea 4.3	48
Ilustración 26. verificación tarea 4.2 y el punto 3 de la tarea 4.3	49
Ilustración 27. Configuración R1 parte 5.....	51
Ilustración 28. Configuración R2 parte 5.....	51
Ilustración 29. Configuración Switch A1 parte 5.....	52
Ilustración 30. Configuración R1 parte 5.....	52
Ilustración 31. Configuración R3 parte 5.....	53
Ilustración 32. verificación tarea paso 5.....	54
Ilustración 33. verificación tarea paso 5.....	54
Ilustración 34. verificación tarea paso 5.....	55
Ilustración 35. verificación pasos 5.3, 5.4 y 5.5.....	56
Ilustración 36. verificación pasos 5.3, 5.4 y 5.5.....	56
Ilustración 37. Configuración R2 parte 6.....	58
Ilustración 38. Configuración R1 parte 6.....	59
Ilustración 39. Configuración R1 parte 6.....	60
Ilustración 40. Configuración Switch D1 parte 6	61
Ilustración 41. Configuración Switch D2 parte 6	62

Ilustración 42. Configuración Switch A1 parte 6.....	63
Ilustración 43. verificación tarea paso 6.2.....	63
Ilustración 44. verificación tarea paso 6.3.....	64
Ilustración 45. verificación tarea paso 6.3.....	65
Ilustración 46. verificación tarea paso 6.3.....	65
Ilustración 47. verificación tarea paso 6.3.....	66
Ilustración 48. verificación tarea paso 6.3.....	66
Ilustración 49. verificación tarea paso 6.5.....	67
Ilustración 50. verificación tarea paso 6.5.....	68
Ilustración 51. verificación tarea paso 6.5.....	69
Ilustración 52. verificación tarea paso 6.5.....	70
Ilustración 53. verificación tarea paso 6.5.....	71
Ilustración 54. verificación tarea paso 6.5.....	72

GLOSARIO

IP: La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o que corresponde al nivel de red del modelo TCP/IP.

GNS3: GNS3 es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales

PACKET TRACER: Packet Tracer de Cisco es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red

PROTOCOLO: En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información.

REDES DE COMPUTADORES: Una red de computadoras es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos 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.

SIMULACIÓN: En las ciencias, la simulación es el artificio contextual que hace referencia a la investigación de una hipótesis o un conjunto de hipótesis de trabajo utilizando modelos un método perfecto para la enseñanza y aprendizaje.

RESUMEN

El presente documento corresponde al trabajo final del diplomado de profundización CISCO CCNP, es una prueba de habilidades prácticas, donde se pueden encontrar la solución al problema propuesto a través del software GNS3, además de configuraciones básicas de enrutamiento en cuanto a: OSPF, DHCPv4, IPV6 etc. Además de distintas pruebas de conexiones entre los distintos dispositivos de la topología empleada.

Palabras clave

IP, GNS3, PACKET TRACER, PROTOCOLO, REDES DE COMPUTADORES, SIMULACIÓN

ABSTRACT

This document corresponding to the final work of the CISCO CCNP in-depth diploma, is a test of practical skills, where the solution to the proposed problem can be found through the GNS3 software, in addition to basic routing configurations regarding: OSPF, DHCPv4, IPV6, etc. In addition to different tests of connections between the different devices of the topology used.

Keywords

IP, GNS3, PACKET TRACER, PROTOCOL, COMPUTER NETWORKS, SIMULATION

INTROUDCCION

En este trabajo el cual corresponde a una parte de la evaluación del diplomado CCNP, se pretende consolidar mediante escenarios prácticos profundizar y afianzar conceptos de enrutamiento, además busca identificar el grado de desarrollo de competencias y habilidades que se adquieren a lo largo del diplomado con énfasis en poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Mediante los comandos “show y comandos ping” se verificará la correcta programación de los diferentes dispositivos como router y switches con los debidos protocolos establecidos

En el transcurso del diplomado CISCO CCNP, se resolvieron diferentes laboratorios y casos de estudio donde se aplicaron los diferentes protocolos de enrutamientos y direccionamiento IP.

En el presente trabajo se consolidan y se implementan todos los conceptos estudiados a lo largo del diplomado para poder así solucionar el escenario propuestos

DESARROLLO

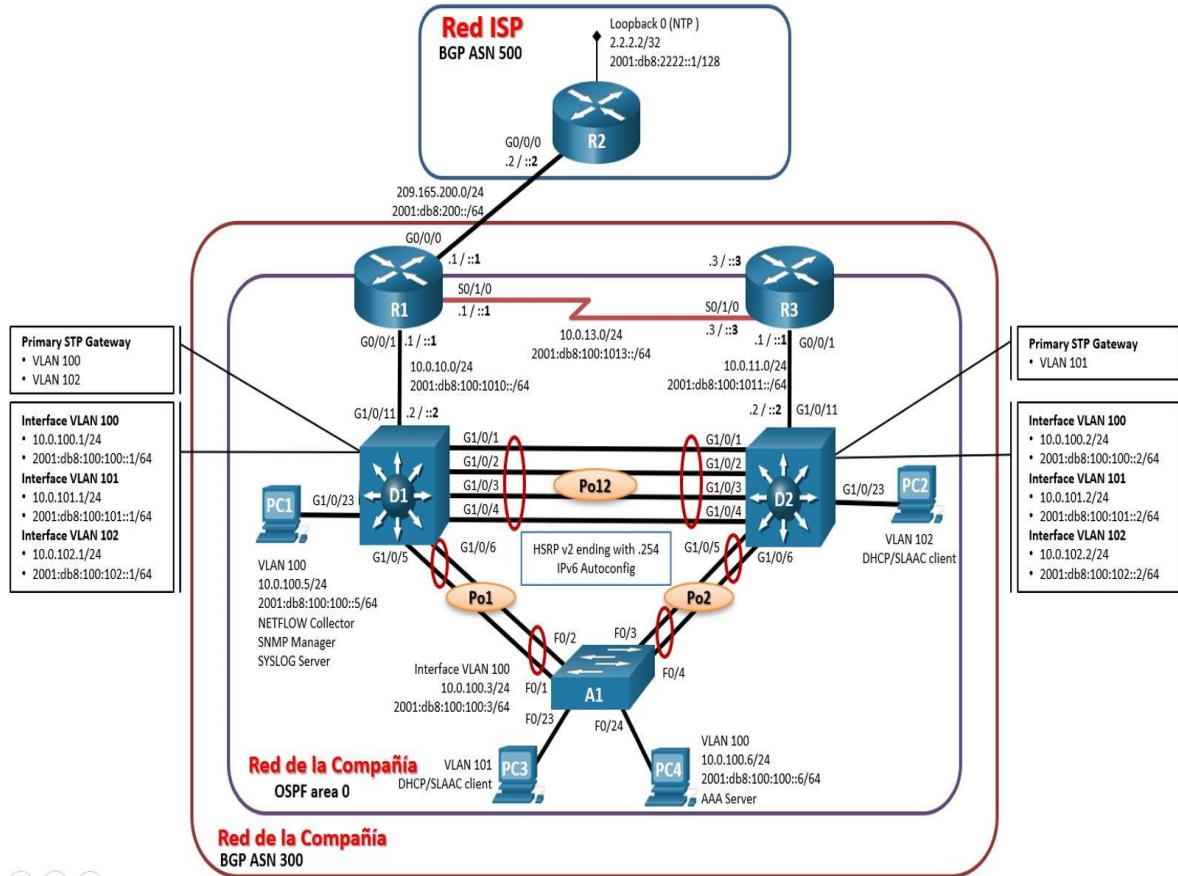


Ilustración 1. Topología de la Red

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

1. ESCENARIO 1

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Paso 1: Cablear la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

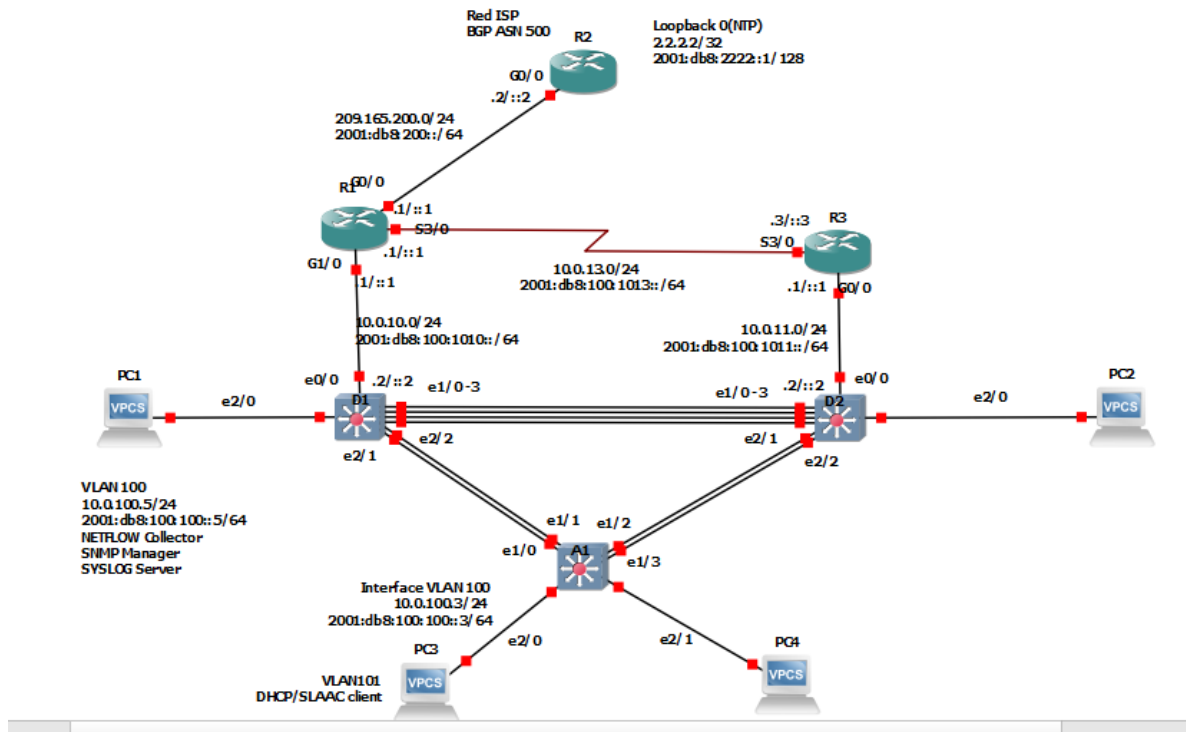


Ilustración 2. Topología en GNS3

Paso 2: Configurar los parámetros básicos para cada dispositivo.

- Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

Router R1

hostname R1

ipv6 unicast-routing

no ip domain lookup

Asigno nombre al router

habilitar IPv6 en un router

Habilita la traducción de nombre a dirección

banner motd # R1, ENCOR Skills Assessment, Scenario 1 # - configura mensaje
line con 0 configuración de línea de la consola
exec-timeout 0 0 establece el tiempo de espera inactivo de la sesión remota
logging synchronous mensaje de evento mientras se ingresa un comando
exit Salir
interface g0/0 Configurar interfaz g0/0
ip address 209.165.200.225 255.255.255.224 Asigno ip a la interface
ipv6 address fe80::1:1 link-local Se configura como la dirección IPv6
ipv6 address 2001:db8:200::1/64 -- Se configura dirección IPv6 unicast global
no shutdown Enciende la interfaz
exit salir
interface g1/0 Configurar interfaz g1/0
ip address 10.0.10.1 255.255.255.0 Asigno ip a la interface
ipv6 address fe80::1:2 link-local Se configura como la dirección IPv6
ipv6 address 2001:db8:100:1010::1/64 - Se configura dirección IPv6 unicast global
no shutdown Enciende la interfaz
exit salir del modo de configuracion de interfaz
interface s3/0 Configurar interfaz g0/0
ip address 10.0.13.1 255.255.255.0 Asigno ip a la interface
ipv6 address fe80::1:3 link-local Se configura como la dirección IPv6
ipv6 address 2001:db8:100:1013::1/64 - Se configura dirección IPv6 unicast global
no shutdown Enciende la interfaz
exit Salir del modo de configuracion
copy running-config startup-config-Copia el archivo de configuracion a la memoria
NVRAM

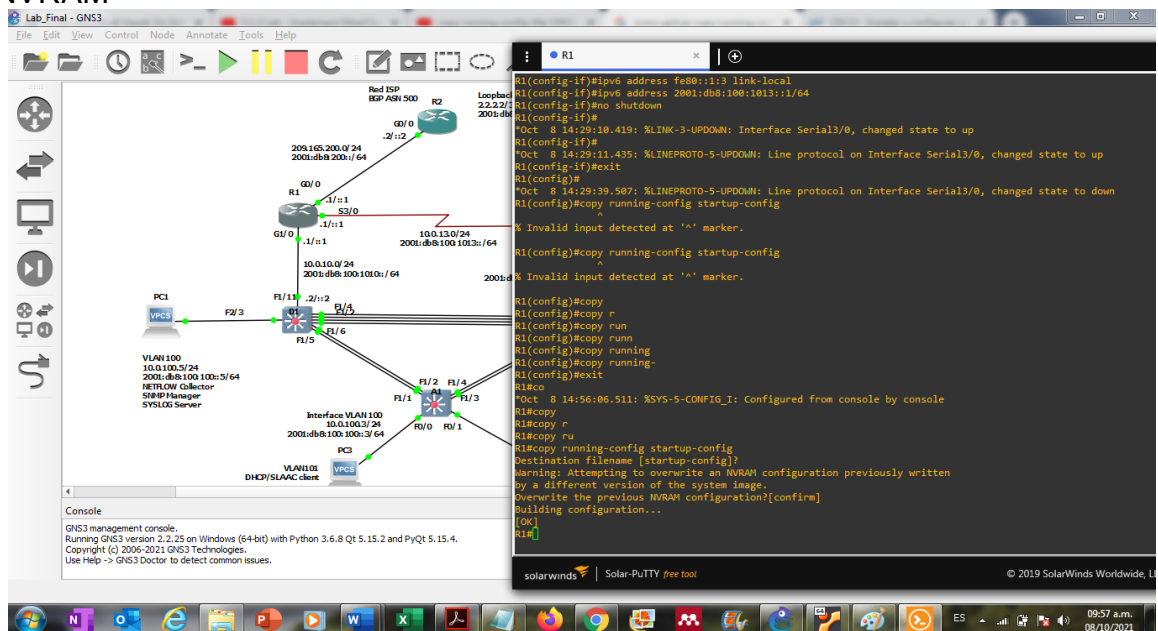


Ilustración 3. Configuración Router R1

Router R2

hostname R2

ipv6 unicast-routing

no ip domain lookup

banner motd # R2, ENCOR Skills Assessment, Scenario 1 #

line con 0

exec-timeout 0 0

logging synchronous

exit

interface g0/0

ip address 209.165.200.226 255.255.255.224

ipv6 address fe80::2:1 link-local

ipv6 address 2001:db8:200::2/64

no shutdown

exit

interface Loopback 0

ip address 2.2.2.2 255.255.255.255

ipv6 address fe80::2:3 link-local

ipv6 address 2001:db8:2222::1/128

no shutdown

exit

The screenshot displays the GNS3 interface with a network diagram on the left and a configuration terminal window on the right. The network diagram shows Router R1 connected to Router R2. R1 has interfaces G0/0, G0/1, G0/2, G0/3, G0/4, G0/5, G0/6, G0/7, G0/8, G0/9, G0/10, G0/11, G0/12, G0/13, G0/14, G0/15, G0/16, G0/17, G0/18, G0/19, G0/20, G0/21, G0/22, G0/23, G0/24, G0/25, G0/26, G0/27, G0/28, G0/29, G0/30, G0/31, G0/32, G0/33, G0/34, G0/35, G0/36, G0/37, G0/38, G0/39, G0/40, G0/41, G0/42, G0/43, G0/44, G0/45, G0/46, G0/47, G0/48, G0/49, G0/50, G0/51, G0/52, G0/53, G0/54, G0/55, G0/56, G0/57, G0/58, G0/59, G0/60, G0/61, G0/62, G0/63, G0/64, G0/65, G0/66, G0/67, G0/68, G0/69, G0/70, G0/71, G0/72, G0/73, G0/74, G0/75, G0/76, G0/77, G0/78, G0/79, G0/80, G0/81, G0/82, G0/83, G0/84, G0/85, G0/86, G0/87, G0/88, G0/89, G0/90, G0/91, G0/92, G0/93, G0/94, G0/95, G0/96, G0/97, G0/98, G0/99, G0/100. R2 has interfaces G0/0, G0/1, G0/2, G0/3, G0/4, G0/5, G0/6, G0/7, G0/8, G0/9, G0/10, G0/11, G0/12, G0/13, G0/14, G0/15, G0/16, G0/17, G0/18, G0/19, G0/20, G0/21, G0/22, G0/23, G0/24, G0/25, G0/26, G0/27, G0/28, G0/29, G0/30, G0/31, G0/32, G0/33, G0/34, G0/35, G0/36, G0/37, G0/38, G0/39, G0/40, G0/41, G0/42, G0/43, G0/44, G0/45, G0/46, G0/47, G0/48, G0/49, G0/50, G0/51, G0/52, G0/53, G0/54, G0/55, G0/56, G0/57, G0/58, G0/59, G0/60, G0/61, G0/62, G0/63, G0/64, G0/65, G0/66, G0/67, G0/68, G0/69, G0/70, G0/71, G0/72, G0/73, G0/74, G0/75, G0/76, G0/77, G0/78, G0/79, G0/80, G0/81, G0/82, G0/83, G0/84, G0/85, G0/86, G0/87, G0/88, G0/89, G0/90, G0/91, G0/92, G0/93, G0/94, G0/95, G0/96, G0/97, G0/98, G0/99, G0/100. The configuration terminal window shows the following commands:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#
*Oct 8 15:06:02.119: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Oct 8 15:06:03.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#interface Loopback 0
R2(config-if)#
*Oct 8 15:06:20.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
R2#
*Oct 8 15:07:02.463: %SYS-5-CONFIG I: Configured from console by console
R2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```

Ilustración 4. Configuración Router R2

Router R3

```
hostname R3
```

```
ipv6 unicast-routing
```

```
no ip domain lookup
```

```
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
```

```
line con 0
```

```
exec-timeout 0 0
```

```
logging synchronous
```

```
exit
```

```
interface g0/0
```

```
ip address 10.0.11.1 255.255.255.0
```

```
ipv6 address fe80::3:2 link-local
```

```
ipv6 address 2001:db8:100:1011::1/64
```

```
no shutdown
```

```
exit
```

```
interface s3/0
```

```
ip address 10.0.13.3 255.255.255.0
```

```
ipv6 address fe80::3:3 link-local
```

```
ipv6 address 2001:db8:100:1010::2/64
```

```
no shutdown
```

```
exit
```

The screenshot displays the GNS3 interface with a network diagram on the left and a terminal window on the right. The network diagram shows three routers: R1 (Red ISP BGP ASN 500), R2, and R3. R1 is connected to R2 via G0/0 (10.0.10.0/24) and S3/0 (10.0.13.0/24). R2 is connected to R3 via G0/0 (10.0.11.0/24) and S3/0 (10.0.13.0/24). R3 is connected to R2 via G0/0 (10.0.11.0/24) and S3/0 (10.0.13.0/24). R3 is also connected to a PC (VPCS) via S3/0 (10.0.13.0/24). The terminal window shows the configuration for Router R3:

```
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface g0/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#
*Oct 8 15:13:32.543: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Oct 8 15:13:33.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R3(config-if)#exit
R3(config)#interface s3/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#
*Oct 8 15:14:13.507: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
R3(config-if)#exit
*Oct 8 15:14:14.523: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
R3(config-if)#exit
R3(config)#exit
R3#copy running-config startup-config
*Oct 8 15:14:37.991: %SYS-5-CONFIG I: Configured from console by console
R3#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```

Ilustración 5. Configuración Router R3

Switch D1

hostname D1	asigno nombre al switch
ip routing	Tabla de direccionamiento
ipv6 unicast-routing	Habilita direcciones IPV6
no ip domain lookup	Habilita la traducción de nombre a dirección
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	Habilita mensaje
line con 0	configuración de línea de la consola
exec-timeout 0 0	establece el tiempo de espera inactivo de la sesión remota
logging synchronous	mensaje de evento mientras se ingresa un comando
exit	Salir
vlan 100	Crea Vlan 100
name Management	Se asigna un nombre a la VLAN
exit	Salir
vlan 101	Crea Vlan 101
name UserGroupA	Nombre a la Vlan
exit	salir
vlan 102	Cra Vlan 12
name UserGroupB	Nombre de la Vlan
exit	Exit
vlan 999	Crea Vlan 999
name NATIVE	Nombre de la vilan
exit	Exit
interface e0/0	Configura Interface e0/0
no switchport	aporta a la interfaz capacidad de Capa 3
ip address 10.0.10.2 255.255.255.0	Asigna direccion ip
ipv6 address fe80::d1:1 link-local	Se configura como la dirección IPv6
ipv6 address 2001:db8:100:1010::2/64	- Se configura dirección IPv6 unicast global
no shutdown	Enciende la interfaz
exit	Salir
interface vlan 100	Ingresa a la conifuracion de la vlan como interfaz
ip address 10.0.100.1 255.255.255.0	Asigna direction IP
ipv6 address fe80::d1:2 link-local	Se configura como la dirección IPv6
ipv6 address 2001:db8:100:100::1/64	- Se configura dirección IPv6 unicast global
no shutdown	Enciende la interfaz
exit	Salir
interface vlan 101	
ip address 10.0.101.1 255.255.255.0	
ipv6 address fe80::d1:3 link-local	
ipv6 address 2001:db8:100:101::1/64	
no shutdown	
exit	
interface vlan 102	
ip address 10.0.102.1 255.255.255.0	

```

ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109 - Excluir IP específicas
ip dhcp excluded-address 10.0.101.141 10.0.101.254 - Excluir IP específicas
ip dhcp excluded-address 10.0.102.1 10.0.102.109 Excluir IP específicas
ip dhcp excluded-address 10.0.102.141 10.0.102.254 Excluir IP específicas
ip dhcp pool VLAN-101 crea un conjunto de ip's con el nombre elegido
network 10.0.101.0 255.255.255.0 Direccion de red
default-router 10.0.101.254 Direccion por decto
exit Salir
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range e1/0 -3, e2/1 -2, e2/0
shutdown Configura un rango de interfaz
Apaga las interfaz
exit Salir
copy running-config startup-config

```

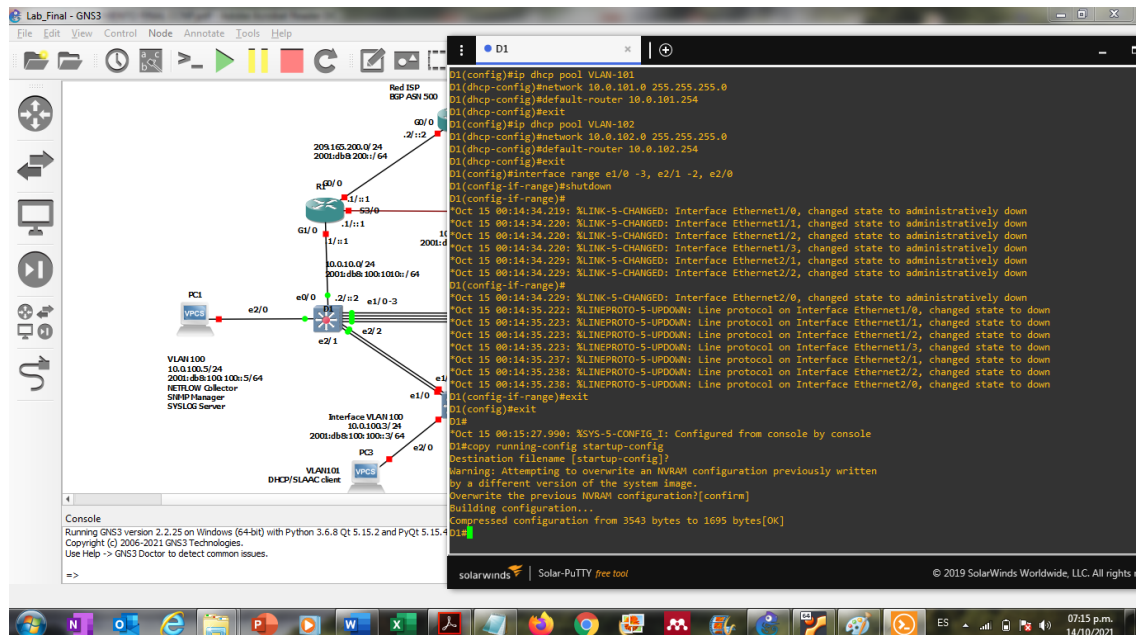


Ilustración 6. Configuración Switch D1

Switch D2
hostname D2
ip routing

```
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e0/0
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
```

```

exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range e1/0 -3, e2/1 -2, e2/0
shutdown
exit
copy running-config startup-config

```

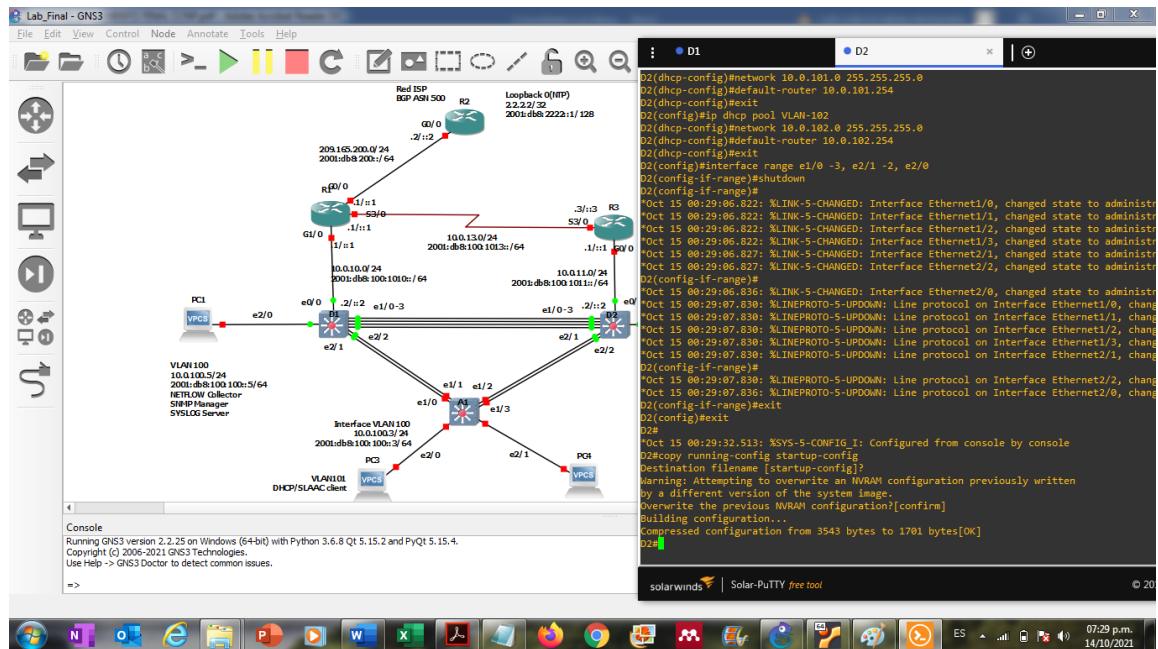


Ilustración 7. Configuración Switch D2

```

Switch A1
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0

```

```

logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range e2/ -3
shutdown
exit
copy running-config startup-config

```

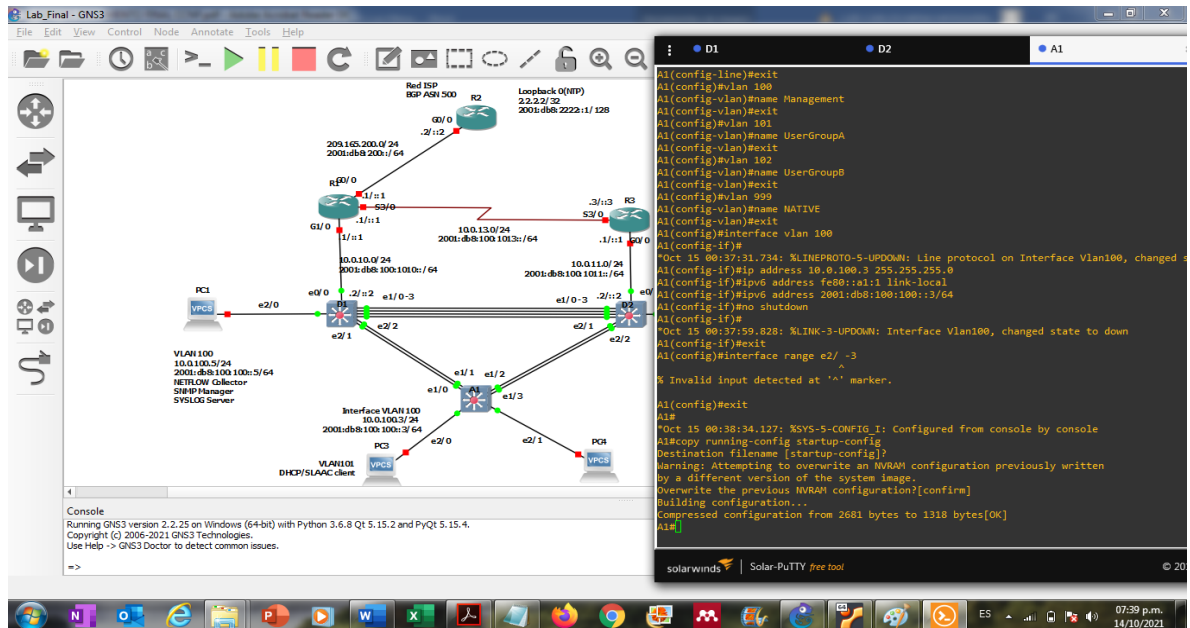


Ilustración 8. Configuración Switch A1

- b. Copie el archivo running-config al archivo startup-config en todos los dispositivos.

Para esto se utiliza el comando *copy running-config startup-config*

- c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

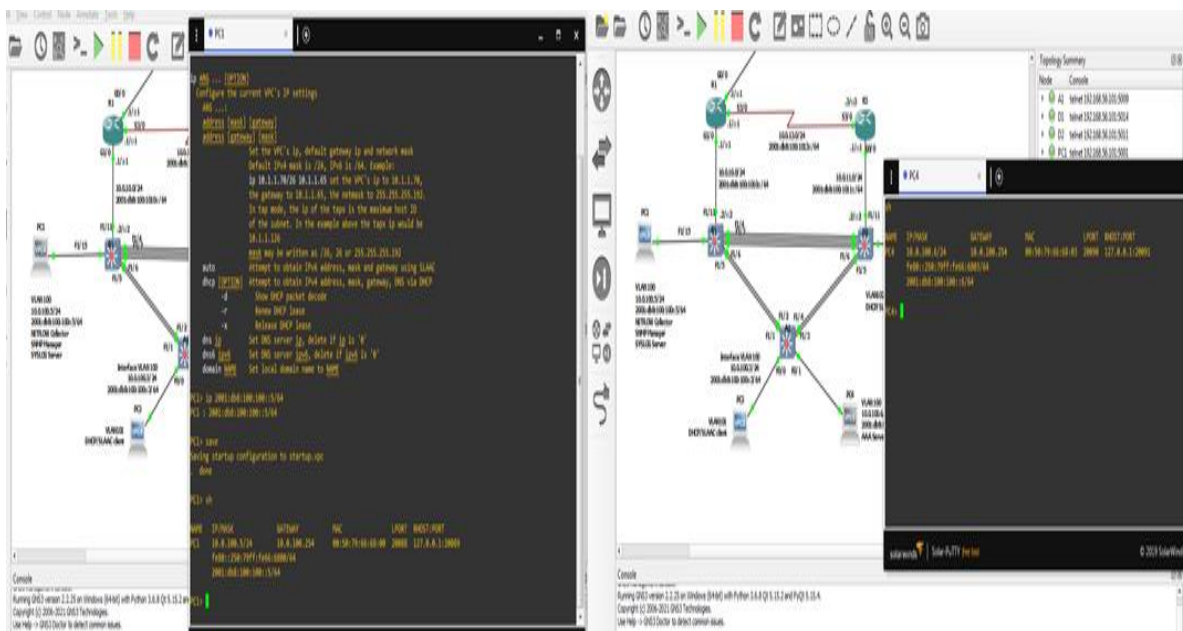


Ilustración 9. Configuración IP - PC 1 y PC 4

Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 2. Tareas de configuración parte 2

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).

Tarea#	Tarea	Especificación
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5
-----	---	---

A continuación, se agregan las respectivas configuraciones de cada dispositivo para el cumplimiento de las tareas propuestas en la tabla (Tabla 2. Tareas de configuración parte 2)

Switch D1

interface range e1/0 -3	Configura interfaz
switchport trunk encapsulation dot1q	Crea modo de encapsulacion
switchport mode trunk	Configura en modo troncal
switchport trunk native vlan 999	Crea Vlan nativa
channel-group 12 mode active	Crea Eterchannel o grupo de interfaz
no shutdown	Enciende la interfaz
exit	Salir
interface range e2/1 -2	
switchport trunk encapsulation dot1q	
switchport mode trunk	
switchport trunk native vlan 999	
channel-group 1 mode active	
no shutdown	
exit	
spanning-tree mode rapid-pvst	Configura redundancia
spanning-tree vlan 100,102 root primary	Asigna prioridades
spanning-tree vlan 101 root secondary	Asigna prioridad
interface e2/0	Configura interfaz e2/0
switchport mode Access	Configura interfaz en modo acceso
switchport access vlan 100	Asigna Vlan 100 como acceso
spanning-tree portfast	Configura redundancia
no shutdown	Enciende la interfaz
exit	Salir

end Sale del modo privilegiado

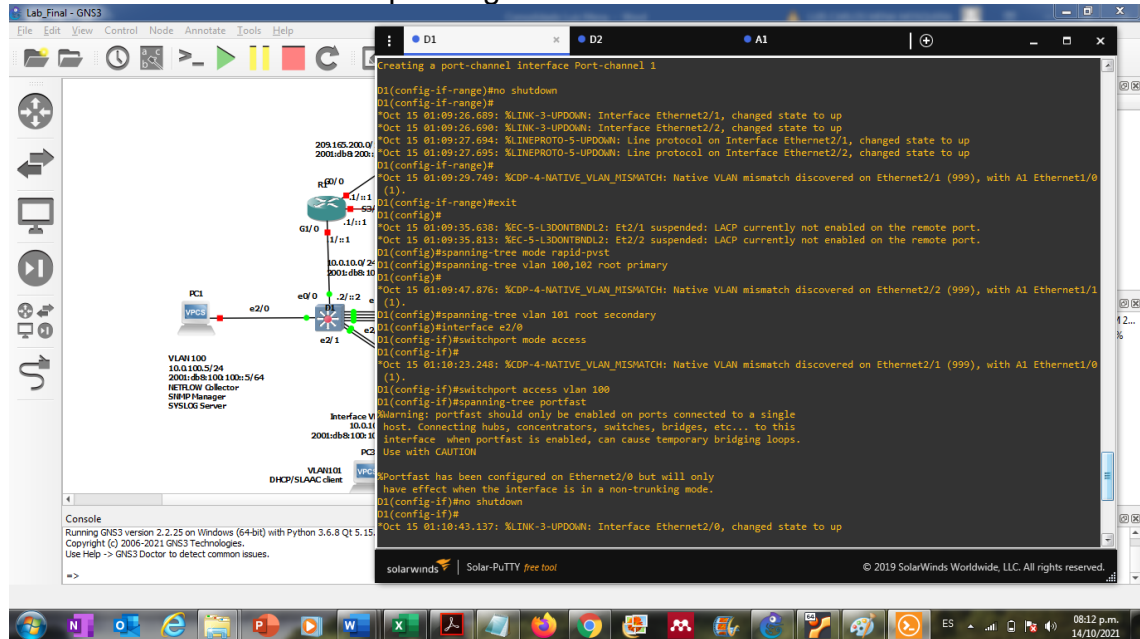


Ilustración 10. Configuración Switch D1 parte 2

Switch D2

```
interface range e1/0 -3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range e2/1 -2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
interface e2/0
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
```

exit
end

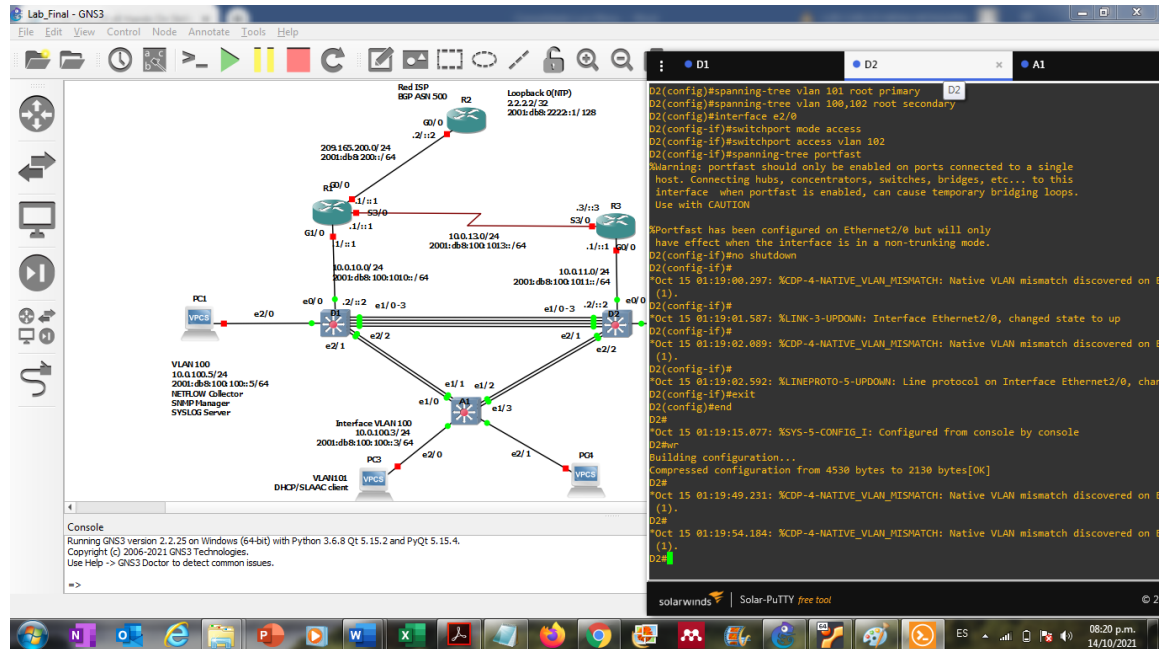


Ilustración 11. Configuración Switch D2 parte 2

Switch A1
spanning-tree mode rapid-pvst
interface range e1/0 -1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range e1/2 -3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface e2/0
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit

```

interface e2/1
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

```

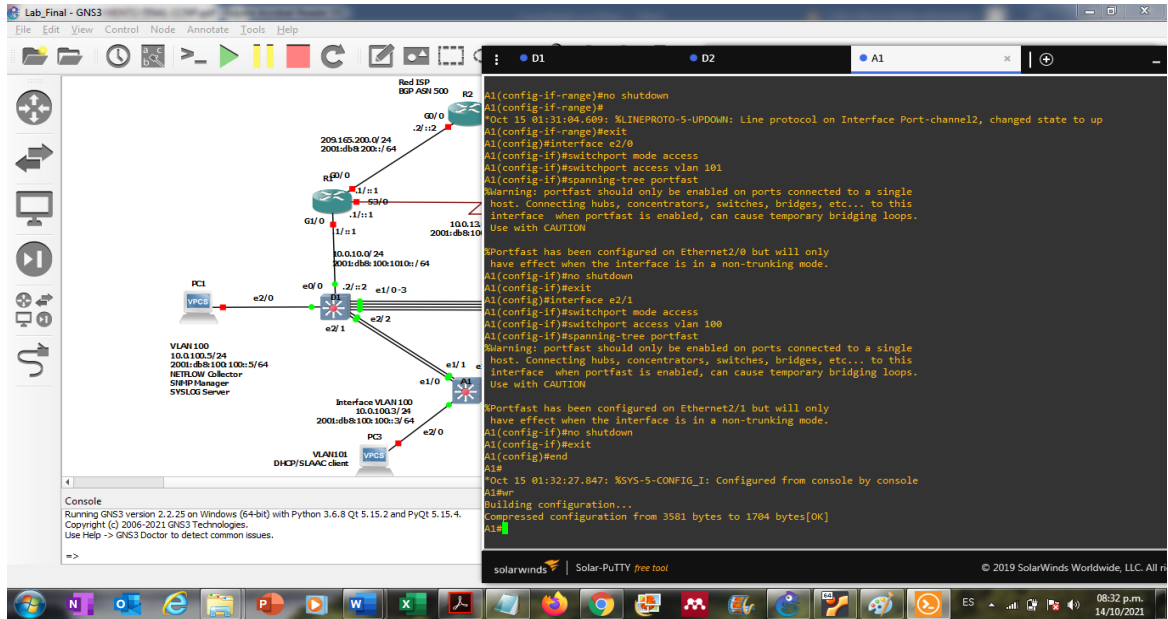


Ilustración 12. Configuración Switch A1 parte 2

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

D1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	999
Po12	on	802.1q	trunking	999

Port Vlans allowed on trunk

Po1	1-4094
Po12	1-4094

Port Vlans allowed and active in management domain

Po1	1,100-102,999
Po12	1,100-102,999

Port Vlans in spanning tree forwarding state and not pruned

Po1	1,100-102,999
-----	---------------

Po12 1,100-102,999

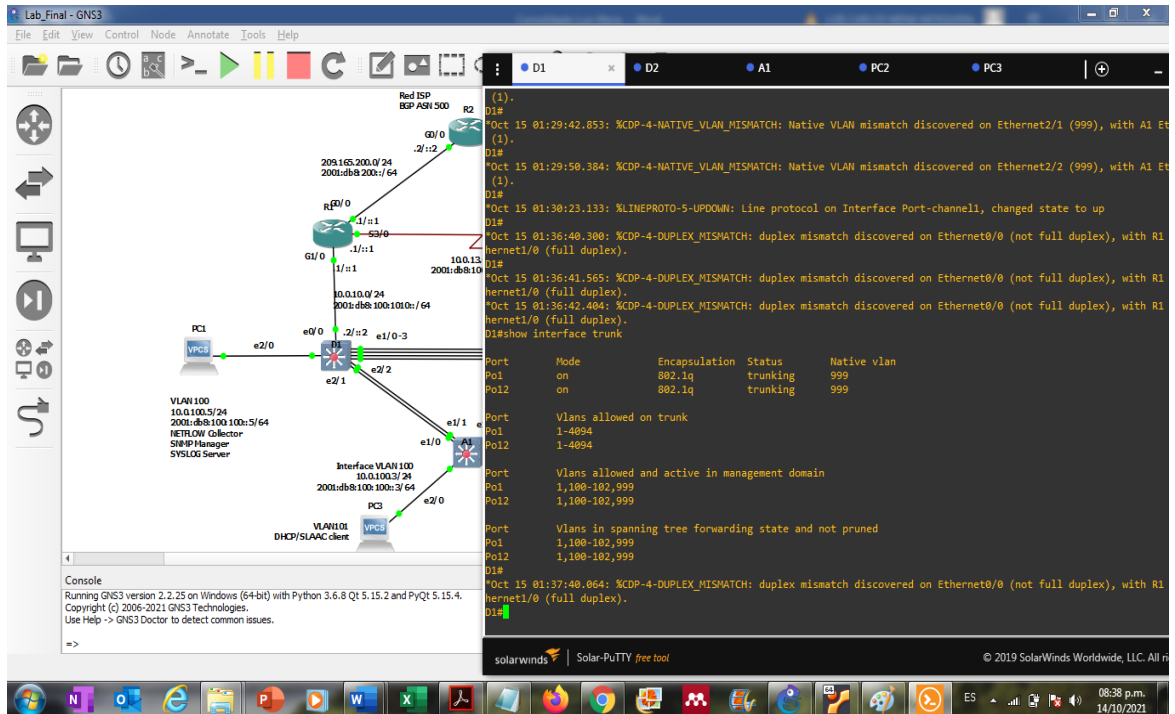


Ilustración 13. Verificación de la configuración 2.2

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.

D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

```
D1#show run | include spanning-tree Muestra configuración protocolo SPT
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast Edge
```

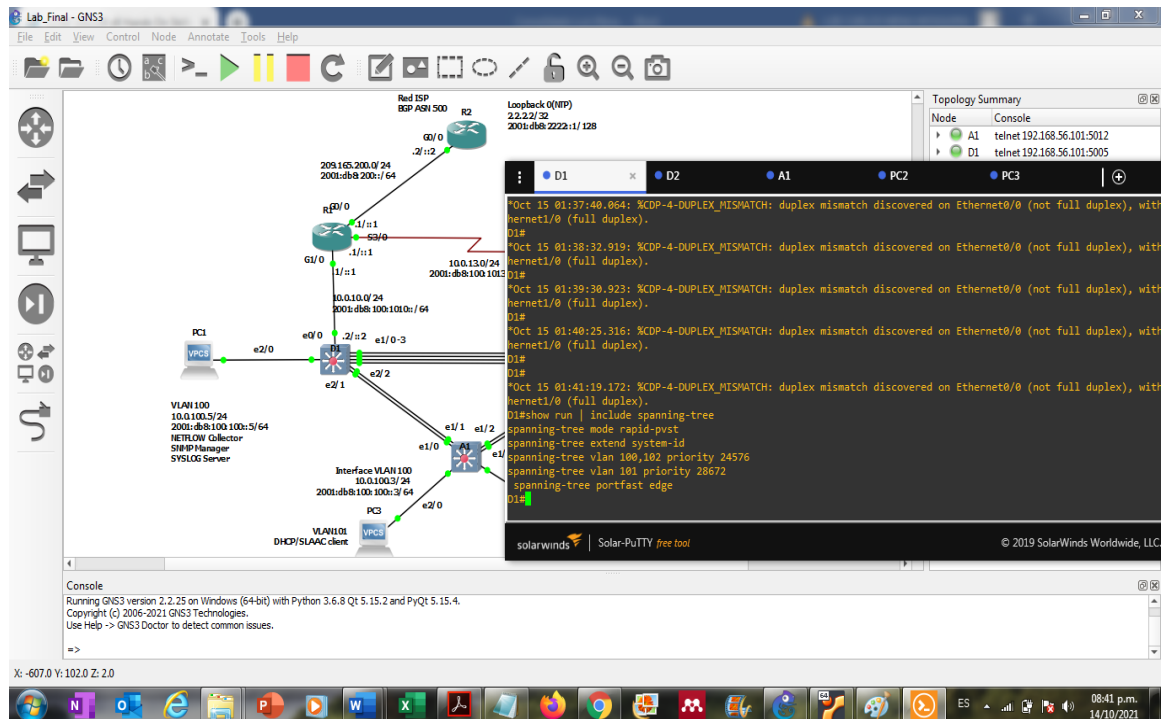


Ilustración 14. Verificación de la configuración 2.3

2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

D1#show run interface e2/0
Building configuration...

Muestra configuración de la interfaz e2/0

Current configuration : 110 bytes
!

```

interface Ethernet2/0
switchport access vlan 100
switchport mode access
spanning-tree portfast edge

```

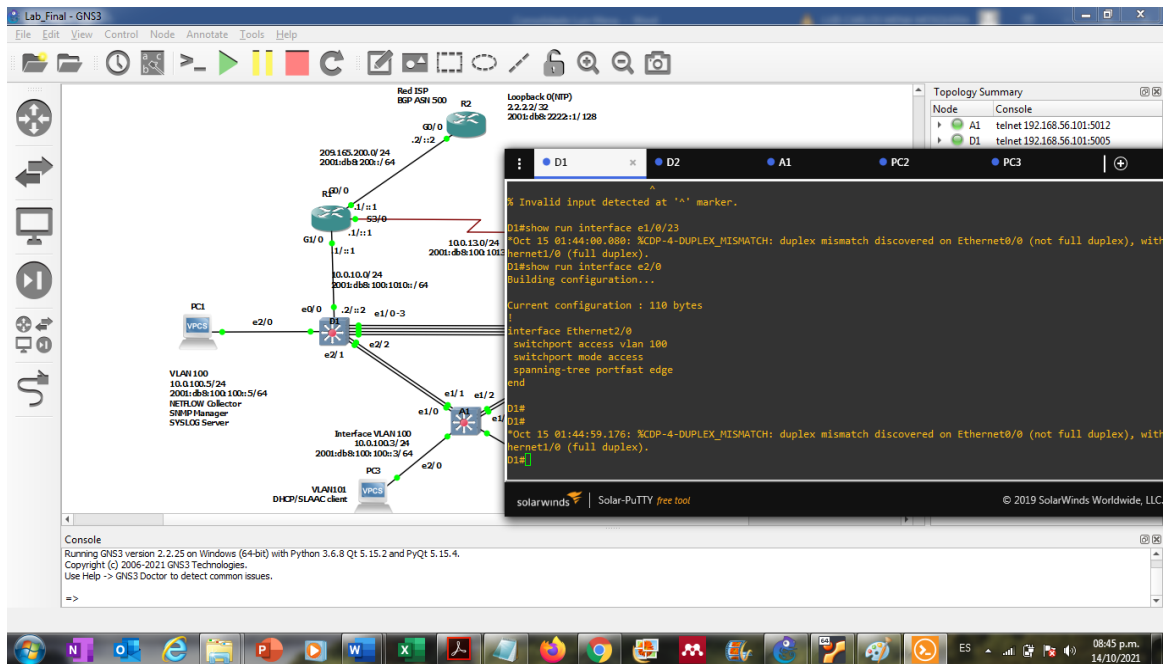


Ilustración 15. Verificación de la configuración 2.6

2.8 Verifique la conectividad de la LAN local

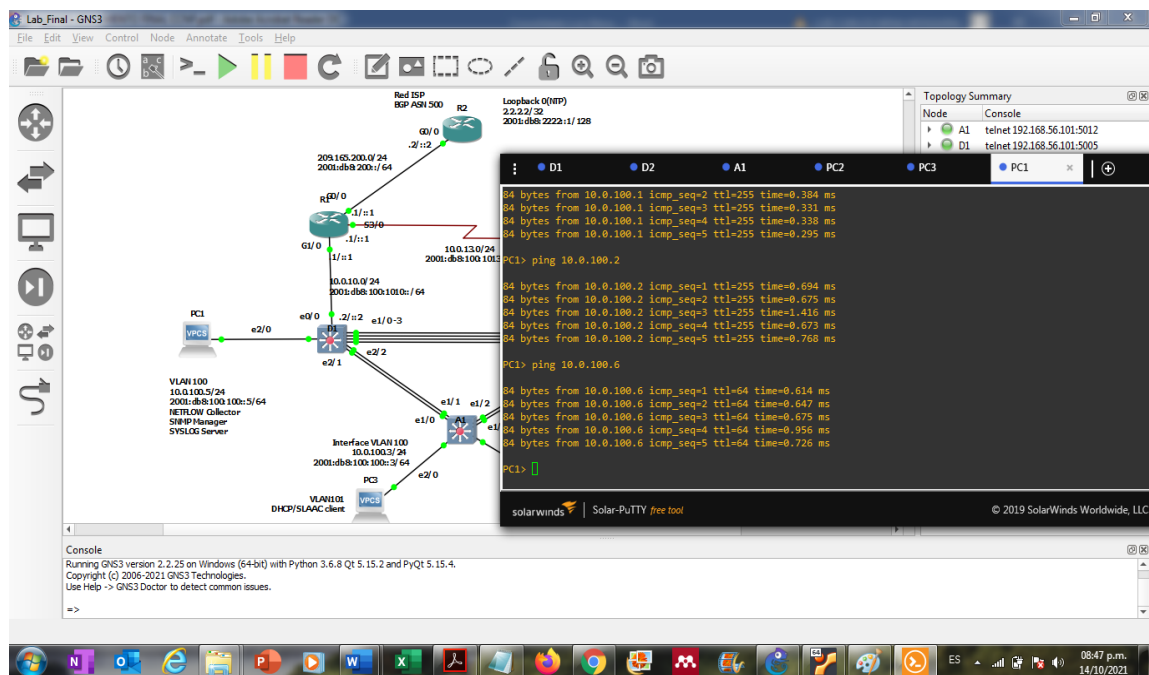


Ilustración 16. conectividad de la LAN local

Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Las tareas de configuración son las siguientes:

Tabla 3. Tareas parte 3 protocolos de enrutamiento

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces deinterconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none">• D1 and D2• D1 and A1• D2 and A1
2.2	En todos los switches cambie la VLAN nativaen los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).

Tarea#	Tarea	Especificación
2.4	En D1 y D2, configure los puentes raíz RSTP(root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en casode falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades deapoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none">• D1 a D2 – Port channel 12• D1 a A1 – Port channel 1• D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que seconectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, comose muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de

		reenvío(forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Router R1

```

router ospf 4                habilita el enrutamiento OSPF
router-id 0.0.4.1           signar manualmente el valor a cada proceso de OSPF
network 10.0.10.0 0.0.0.255 area 0   Direccion de red del área
network 10.0.13.0 0.0.0.255 area 0   Direccion de red
default-information originate   propaga la ruta estática predeterminada
exit                           Salir
ipv6 router ospf 6          habilita el enrutamiento ipv6OSPF
router-id 0.0.6.1           signar manualmente el valor a cada proceso de OSPF
default-information originate   propaga la ruta estática predeterminada
exit                           Salir
interface g1/0              Configura interfaz g1/0
ipv6 ospf 6 area 0          Configurar área en ipv6 ospf
exit                          Salir
interface s3/0              Configura interfaz S3/0
ipv6 ospf 6 area 0          Configurar área en ipv6 ospf
exit                          Salir
ip route 10.0.0.0 255.0.0.0 null0   Crea ruta estatica a la null0
ipv6 route 2001:db8:100::/48 null0   Asigna ip a la null0

```

router bgp 300	habilita el enrutamiento bgp 300
bgp router-id 1.1.1.1	signar manualmente el valor a cada proceso de BGP
neighbor 209.165.200.226 remote-as 500	configura Vecino BGP
neighbor 2001:db8:200::2 remote-as 500	configura Vecino BGP
address-family ipv4 unicast	Configura dirección unicast
neighbor 209.165.200.226 activate	Activa vecino
no neighbor 2001:db8:200::2 activate	Desactiva vecino
network 10.0.0.0 mask 255.0.0.0	Asigna dirección de red y mascara
exit-address-family	Salir de configuración family
address-family ipv6 unicast	Configura dirección unicast
no neighbor 209.165.200.226 activate	Desactiva vecino
neighbor 2001:db8:200::2 activate	Activa vecino
network 2001:db8:100::/48	Asigna dirección de red y mascara
exit-address-family	Salir de configuración family

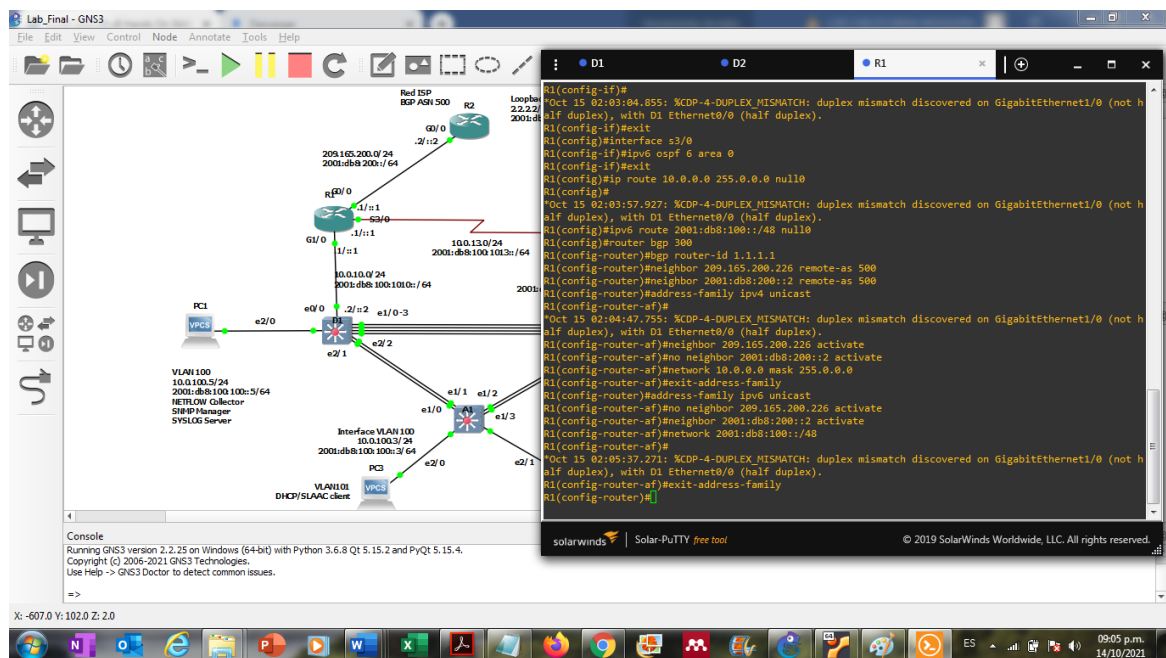


Ilustración 17. Configuración R1 parte 3

<u>Router R2</u>	
ip route 0.0.0.0 0.0.0.0 loopback 0	Habilita enrutamiento loopback 0
ipv6 route ::/0 loopback 0	Habilita IPV6 en loopback 0
router bgp 500	Habilita bgp 500
bgp router-id 2.2.2.2	signar manualmente id
neighbor 209.165.200.225 remote-as 300	Habilita vecino
neighbor 2001:db8:200::1 remote-as 300	Habilita vecino

address-family ipv4	Habilita direcciones ipv4
neighbor 209.165.200.225 activate	Activa vecino
no neighbor 2001:db8:200::1 activate	Desabilita vecino
network 2.2.2.2 mask 255.255.255.255	Direccion de red y mascara
network 0.0.0.0	Ip por defecto
exit-address-family	Salir de modo configuración family
address-family ipv6	Habilita direcciones ipv6
no neighbor 209.165.200.225 activate	
neighbor 2001:db8:200::1 activate	
network 2001:db8:2222::/128	
network ::/0	
exit-address-family	

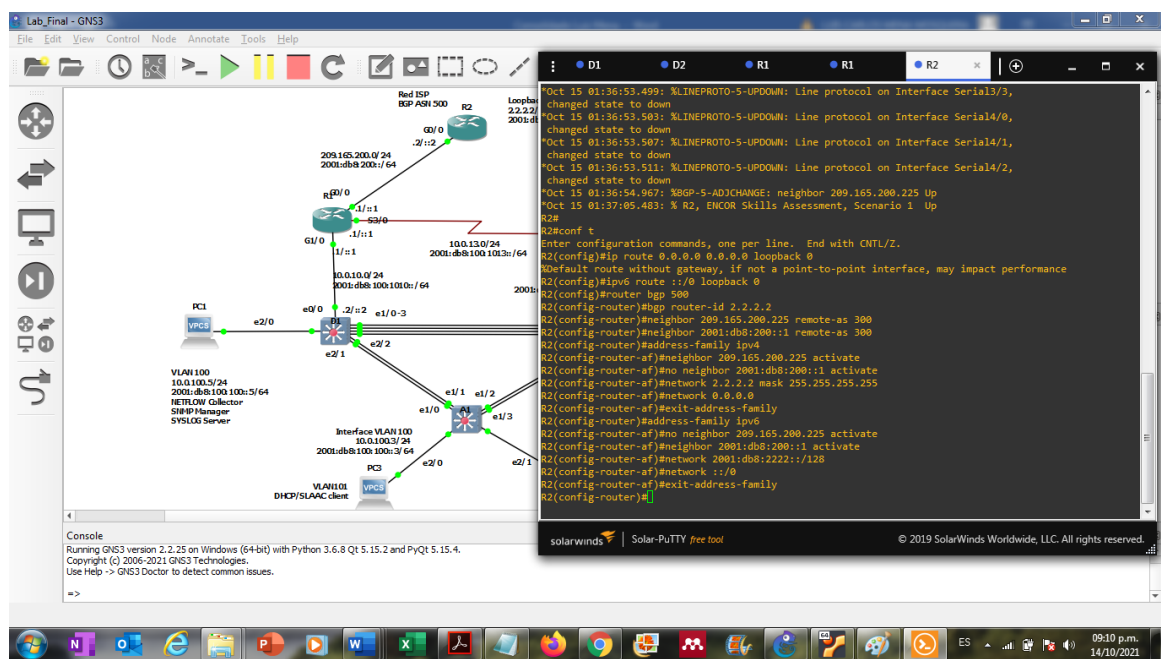


Ilustración 18. Configuración R2 parte 3

<u>Router R3</u>	
router ospf 4	Habilita ospf 4
router-id 0.0.4.3	
network 10.0.11.0 0.0.0.255 area 0	
network 10.0.13.0 0.0.0.255 area 0	
exit	
ipv6 router ospf 6	
router-id 0.0.6.3	
exit	
interface g0/0	

```

ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
end

```

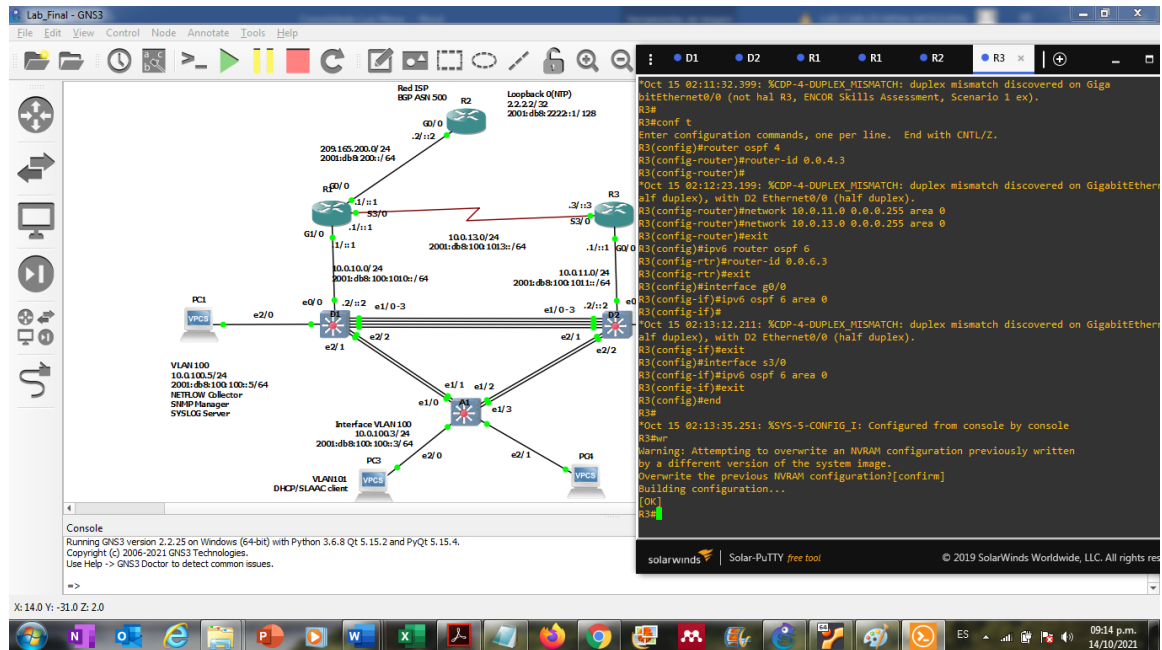


Ilustración 19. Configuración R3 parte 3

```

Switch D1
router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e0/0
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e0/0
exit
interface e0/0

```

```

ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end

```

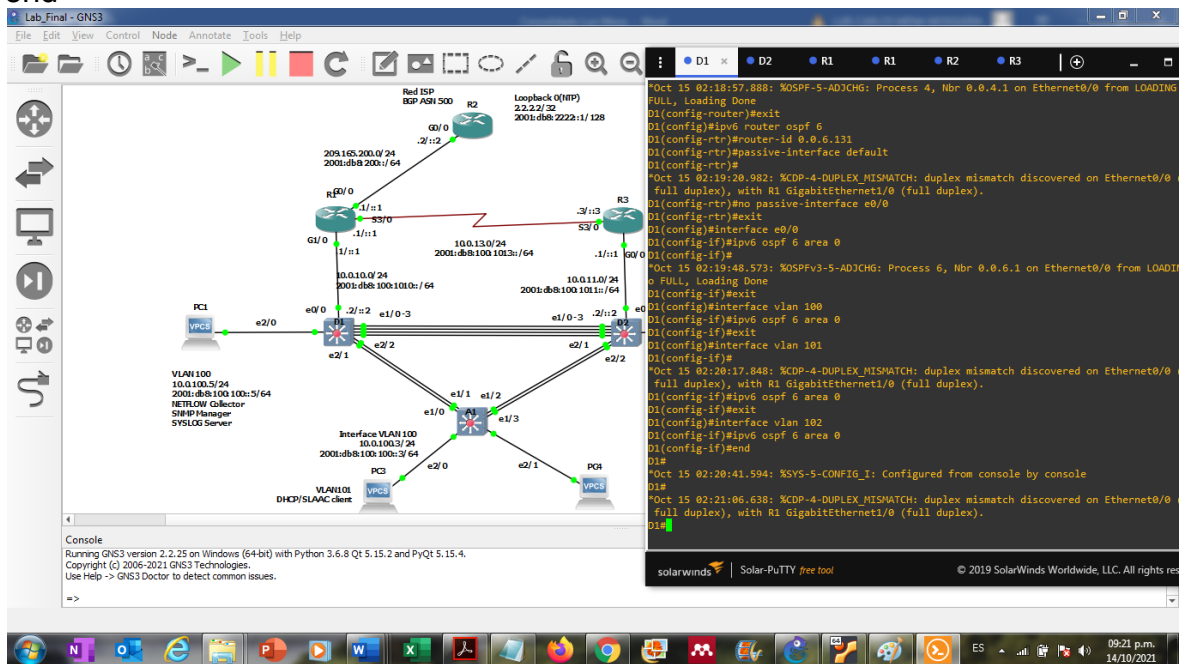


Ilustración 20. Configuración Switch D1 parte 3

Switch D2

```

router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e0/0
exit
ipv6 router ospf 6

```

```

router-id 0.0.6.132
passive-interface default
no passive-interface e0/0
exit
interface e0/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end

```

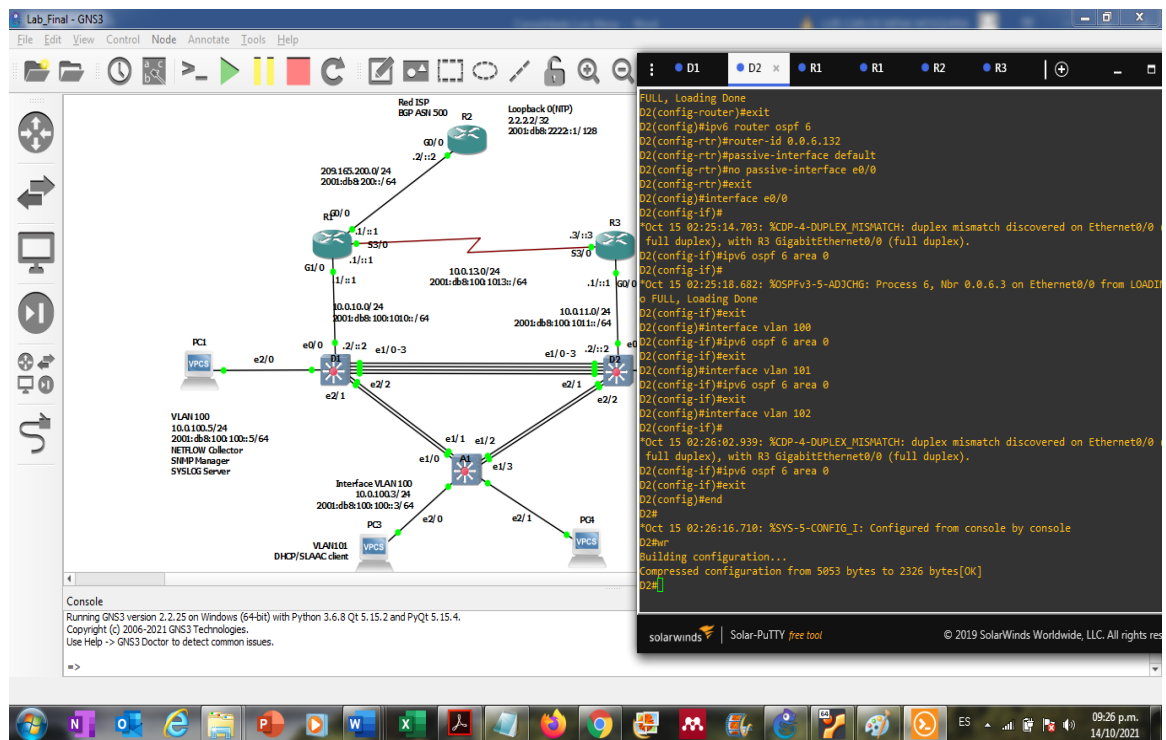


Ilustración 21. Configuración Switch D2 parte 3

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)
 En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los host en la “Red de la Compañía”.
 Las tareas de configuración son las siguientes:

Tabla 4. Tareas de configuración parte 4

Tarea #	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</p> <p>Programa la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.</p> <p>Programa la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

Tarea #	Tarea	Especificación
4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.

Tarea#	Tarea	Especificación
	En D2, configure HSRPv2.	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

Switch D1

ip sla 4 Este comando es para definir el # de la "sesión" del SLA4
icmp-echo 10.0.10.1 Comprueba la conectividad de nivel IP
frequency 5 indica cada cuanto tiempo se va a enviar el mensaje, cada 5s
exit Salir
ip sla 6 Este comando es para definir el # de la "sesión" del SLA6
icmp-echo 2001:db8:100:1010::1 Comprueba la conectividad de nivel IP
frequency 5 indica cada cuanto tiempo se va a enviar el mensaje, cada 5s
exit Salir
ip sla schedule 4 life forever start-time now Habilita el **IP SLA** e indica el tiempo
ip sla schedule 6 life forever start-time now Habilita el **IP SLA** e indica el tiempo
track 4 ip sla 4 Crea el tarck
delay down 10 up 15 Establece el retraso
exit Salir
track 6 ip sla 6 Crea el tarck de la sla6
delay down 10 up 15 Establece el retraso
exit Salir
interface vlan 100 modo de Configuración Vlan 100
standby version 2
standby 104 ip 10.0.100.254 Asigna grupo y dirección ip de prioridad
standby 104 priority 150 Asigna prioridad 150 a la interfaz
standby 104 preempt Convierte en enrutador activo cuando la prioridad es mayor
standby 104 track 4 decrement 60 disminuir la prioridad
standby 106 ipv6 autoconfig Auto configura grupo ipv6
standby 106 priority 150 Asigna prioridad 150
standby 106 preempt Convierte en enrutador activo cuando la prioridad es may
standby 106 track 6 decrement 60 disminuir la prioridad
exit Salir
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150

```

standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

```

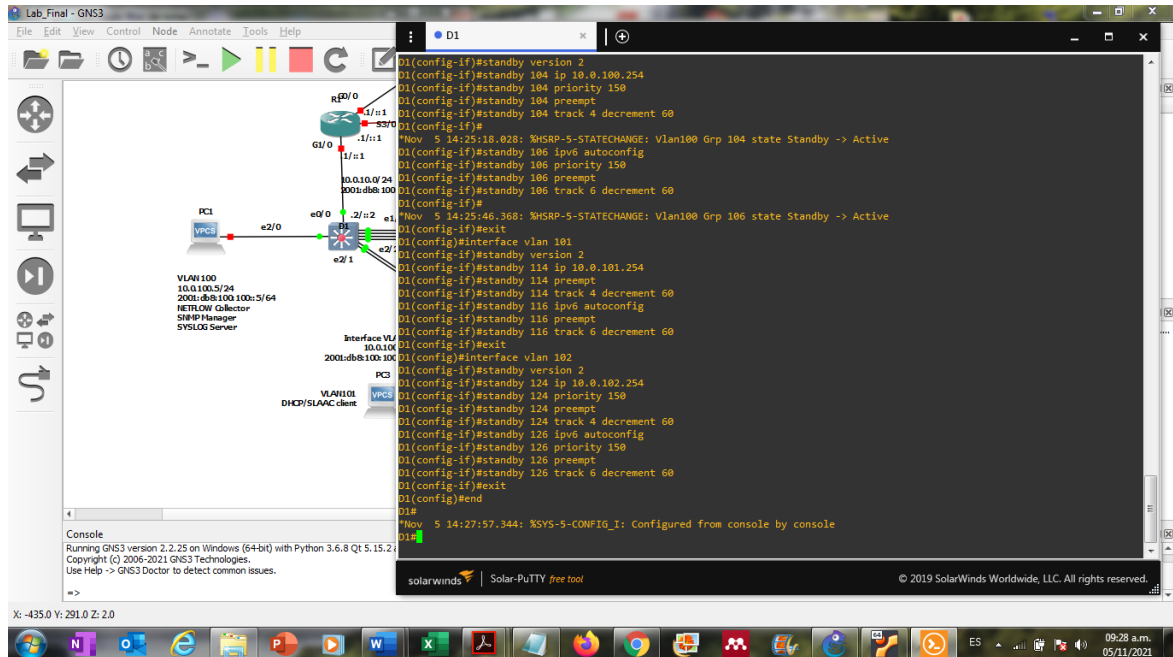


Ilustración 22. Configuración Switch D1 parte 4

```

Switch D2
ip sla 4
icmp-echo 10.0.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15

```

```
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

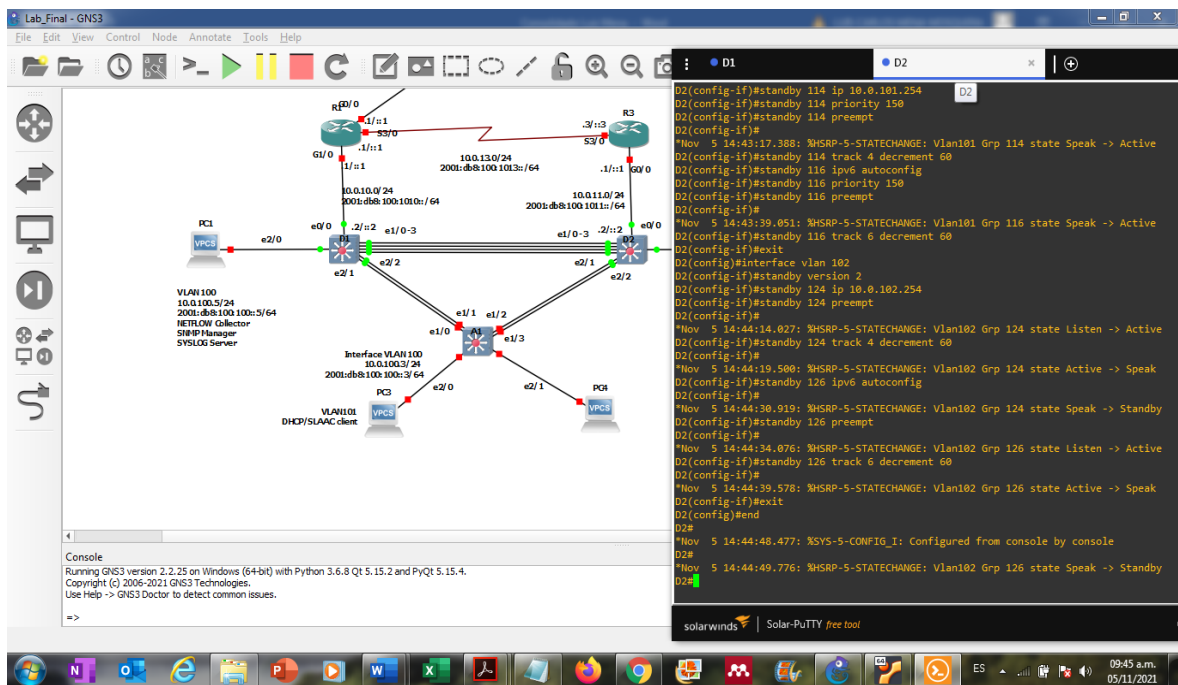


Ilustración 23. Configuración Switch D2 parte 4

Verificamos la configuración con el comando show run | section ip sla

Se Verifica la tarea 4.1 y el punto 3 de la tarea 4.3

```

D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
  
```

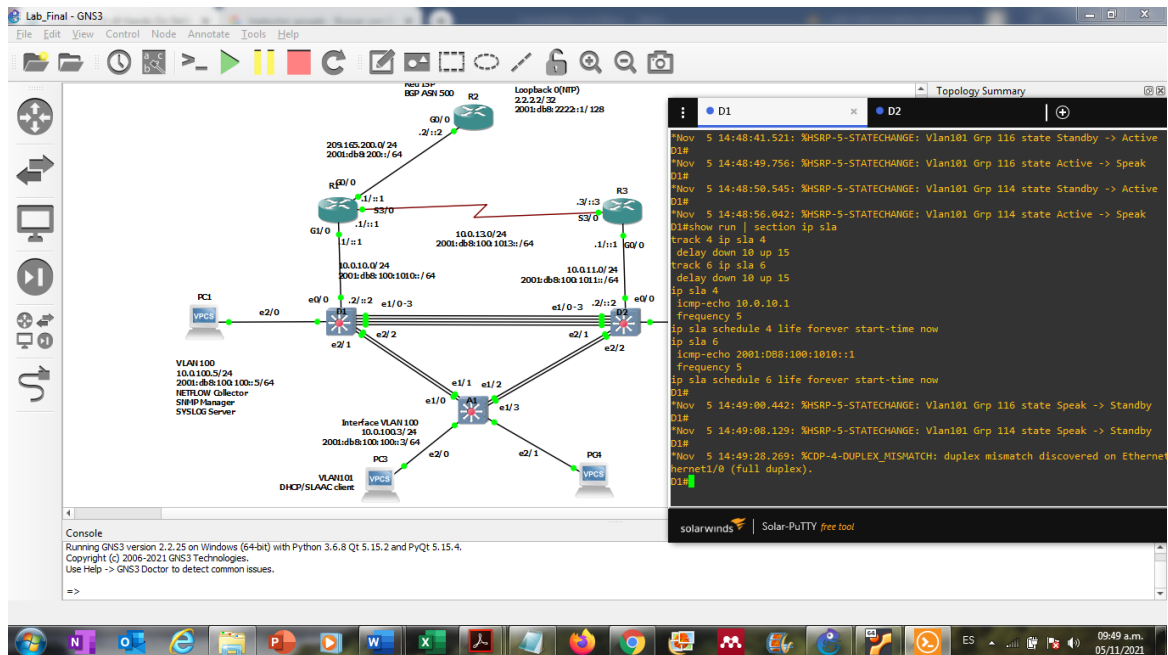


Ilustración 24. Verificación tarea 4.1 y el punto 3 de la tarea 4.3

Verificando la tarea 4.3 aplicamos el comando: show standby brief
D1#show standby brief

P indicates configured to preempt.

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
VI100	104	150	P	Active	local	10.0.100.2	10.0.100.254
VI100	106	150	P	Active	local	FE80::D2:2	FE80::5:73FF:FEA0:6A
VI101	114	100	P	Standby	10.0.101.2	local	10.0.101.254
VI101	116	100	P	Standby	FE80::D2:3	local	FE80::5:73FF:FEA0:74
VI102	124	150	P	Active	local	10.0.102.2	10.0.102.254
VI102	126	150	P	Active	local	FE80::D2:4	FE80::5:73FF:FEA0:7E

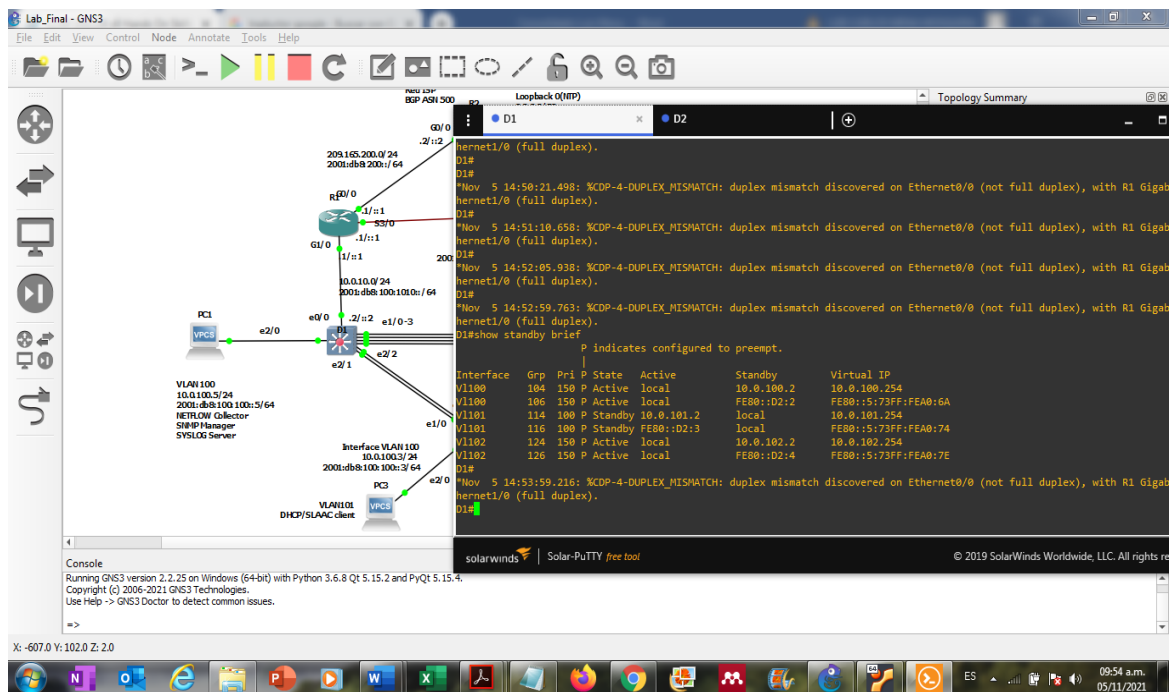


Ilustración 25. Verificación tarea 4.3

Se verifica la tarea 4.2 y el punto 3 de la tarea 4.3 para el Switch D2

```
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
```

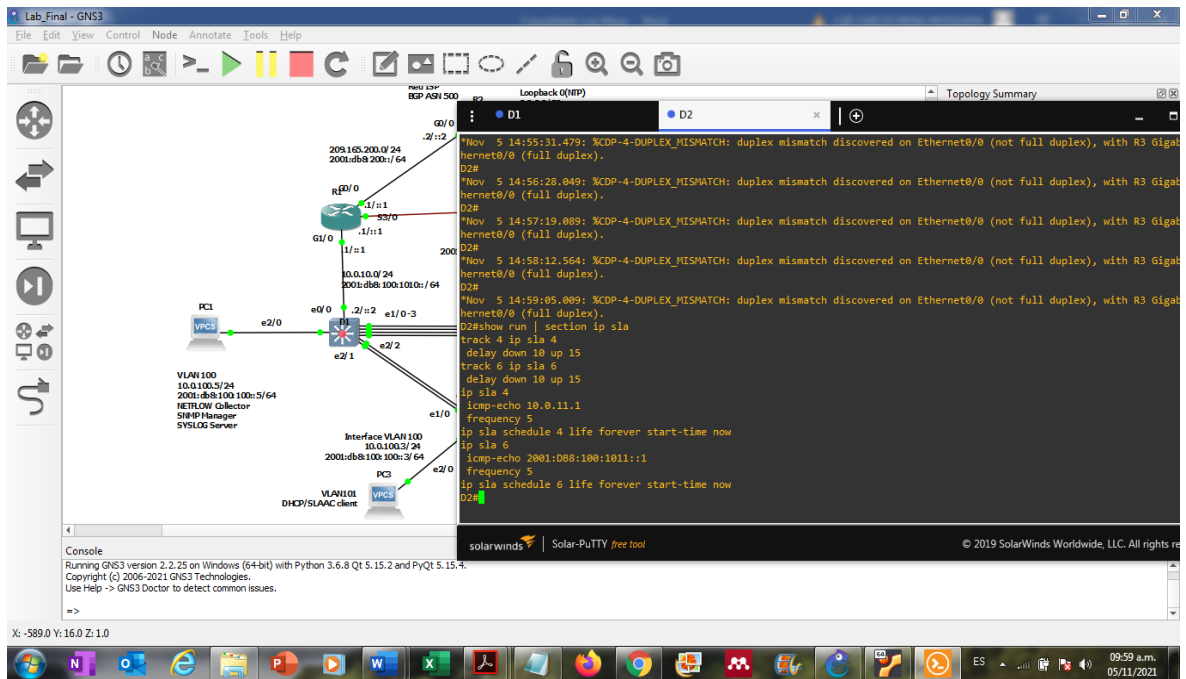


Ilustración 26. verificación tarea 4.2 y el punto 3 de la tarea 4.3

Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 5. Tareas de configuración parte 5

Tarea #	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"> Nombre de usuario Local: sadmin Nivel de privilegio 15 Contraseña: cisco12345cisco

5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	<p>Especificaciones del servidor RADIUS.:</p> <ul style="list-style-type: none"> • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: \$trongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	<p>Especificaciones de autenticación AAA:</p> <ul style="list-style-type: none"> • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123 .

```
enable algorithm-type SCRYPT secret cisco12345cisco
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
! All devices except R2:
aaa new-model
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit
aaa authentication login default group radius local
end
```

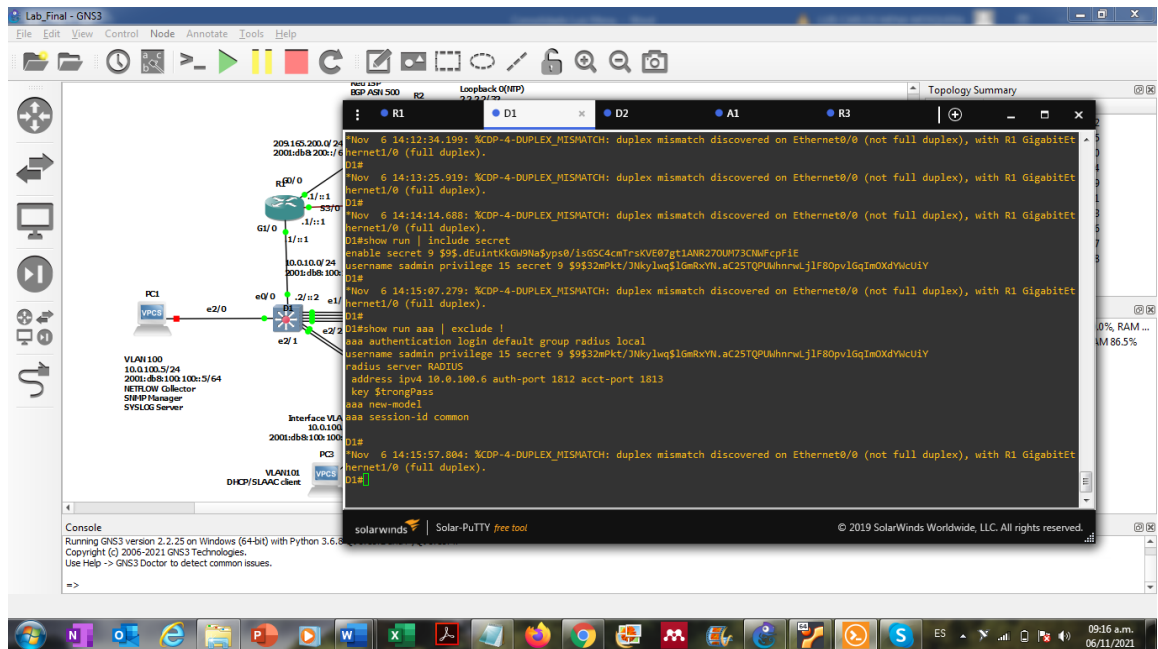



Ilustración 32. verificación tarea paso 5

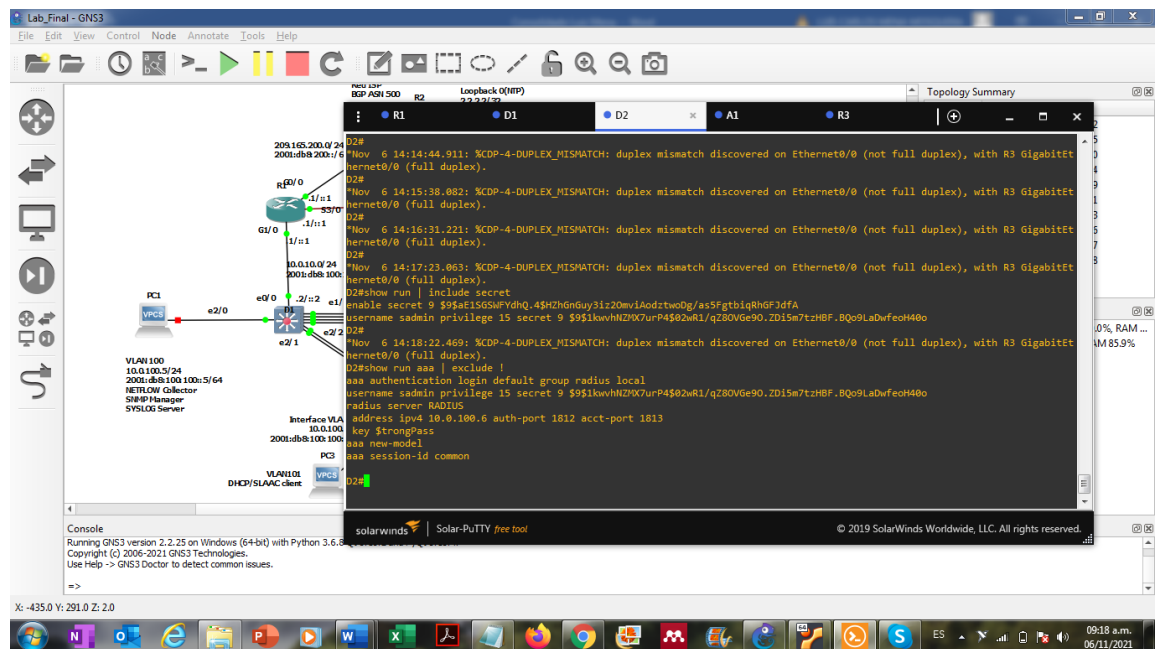


Ilustración 33. verificación tarea paso 5

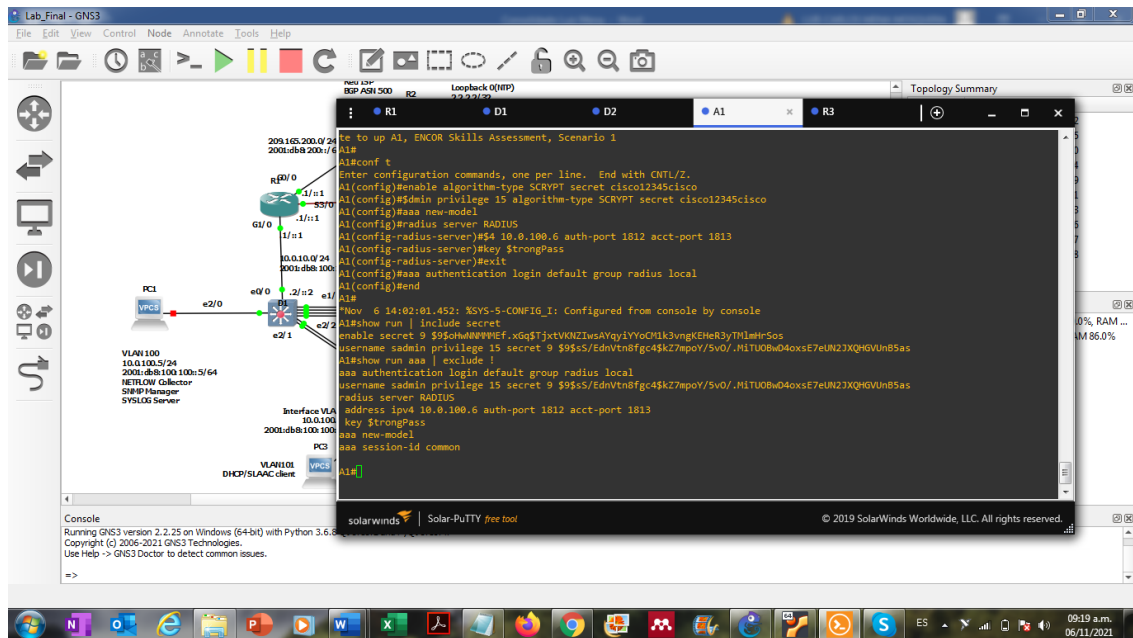


Ilustración 34. verificación tarea paso 5

Para verificar pasos 5.3, 5.4 y 5.5, se aplica el comando `show run aaa | exclude !` en todos los dispositivos excepto R2

<code>R1#show run aaa exclude !</code>	Habilita autenticación AAA
<code>aaa authentication login default group radius local</code>	
<code>radius server RADIUS</code>	Crea servidor radius
<code>address ipv4 10.0.100.6 auth-port 1812 acct-port 1813</code>	configura direccion ip
<code>key \$strongPass</code>	Clave de ingreso
<code>aaa new-model</code>	Activa modelo de autenticación AAA
<code>aaa session-id common</code>	Registro de la sesiones

Tabla 6. Tareas de configuración parte 6

Tarea #	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.

Tarea #	Tarea	Especificación
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: <ul style="list-style-type: none"> • Únicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el <i>community string</i> en ENCORSA. • En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>. • En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>. • En A1, habilite el envío de <i>traps config</i>.

```

R2#conf t          Ingresar al modo privilegiado
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3  obtener la hora correcta de los servidores NTP
R2(config)#end     Salir del modo privilegiado (Configuración)
    
```

R2#

Nov 6 14:26:31.251: %SYS-5-CONFIG_I: Configured from console by console

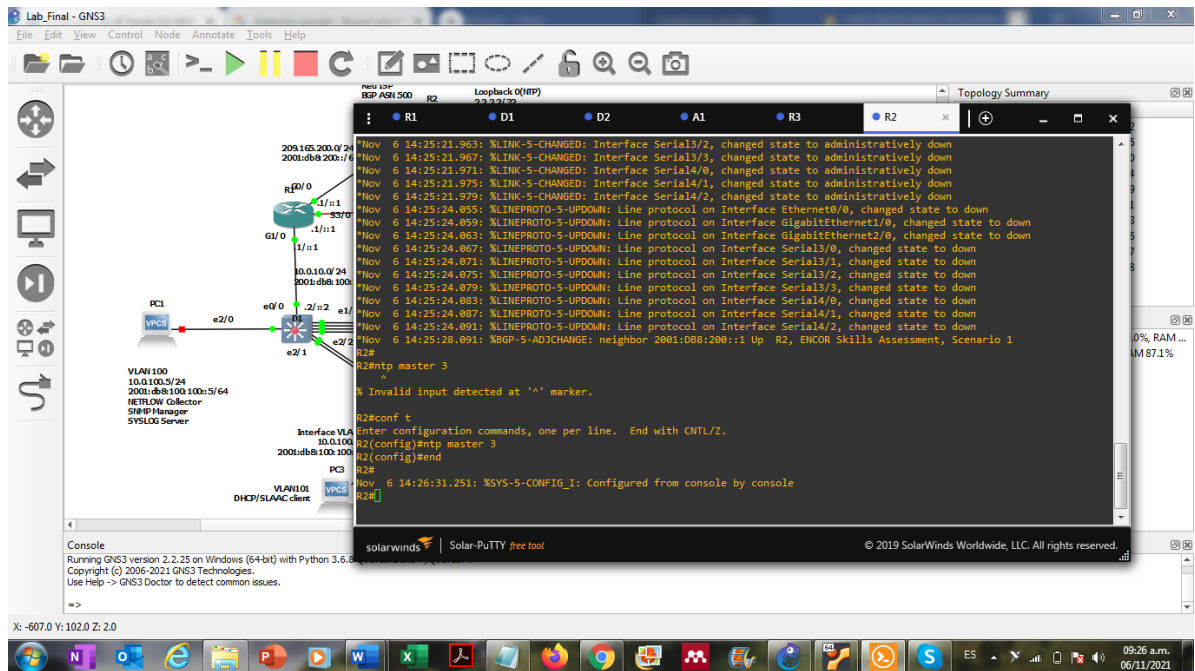


Ilustración 37. Configuración R2 parte 6

Router R1

! enable and enter password

ntp server 2.2.2.2	Configura servidor NTP
logging trap warning	Configuración de mensajes syslog
logging host 10.0.100.5	Dirección del servidor
logging on	Activa el servidor
ip access-list standard SNMP-NMS	Lista de acceso SNMP
permit host 10.0.100.5	Permite el host 10.0.100.5
exit	Salir
snmp-server contact Cisco Student	Habilitar configuración de nodos
snmp-server community ENCORSA ro SNMP-NMS	
snmp-server host 10.0.100.5 version 2c ENCORSA	
snmp-server ifindex persist	
snmp-server enable traps bgp	
snmp-server enable traps config	
snmp-server enable traps ospf	
end	

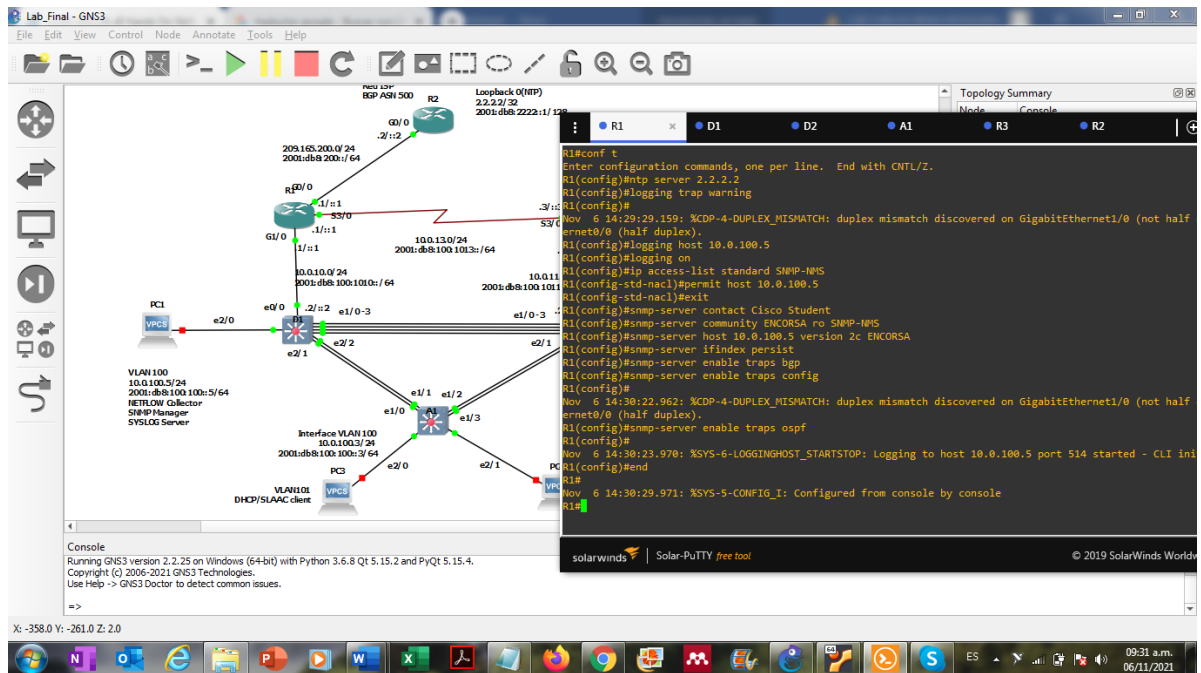


Ilustración 38. Configuración R1 parte 6

Router R3

```

ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end

```

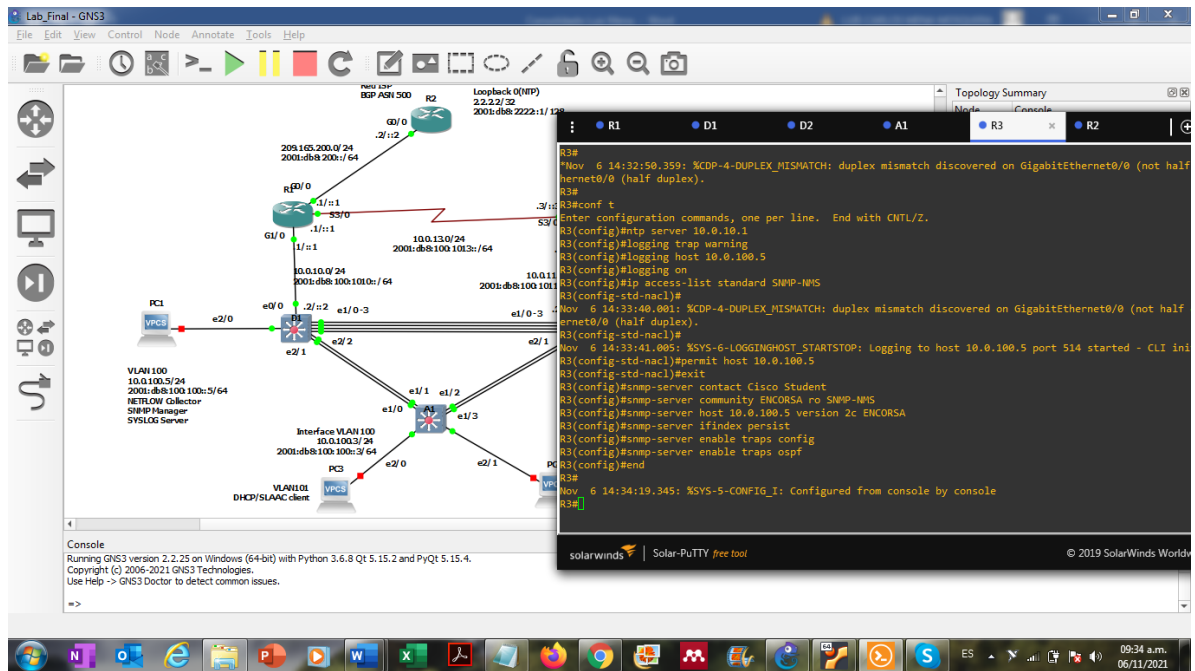


Ilustración 39. Configuración R3 parte 6

Switch D1

```

ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSARo SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSARo
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end

```

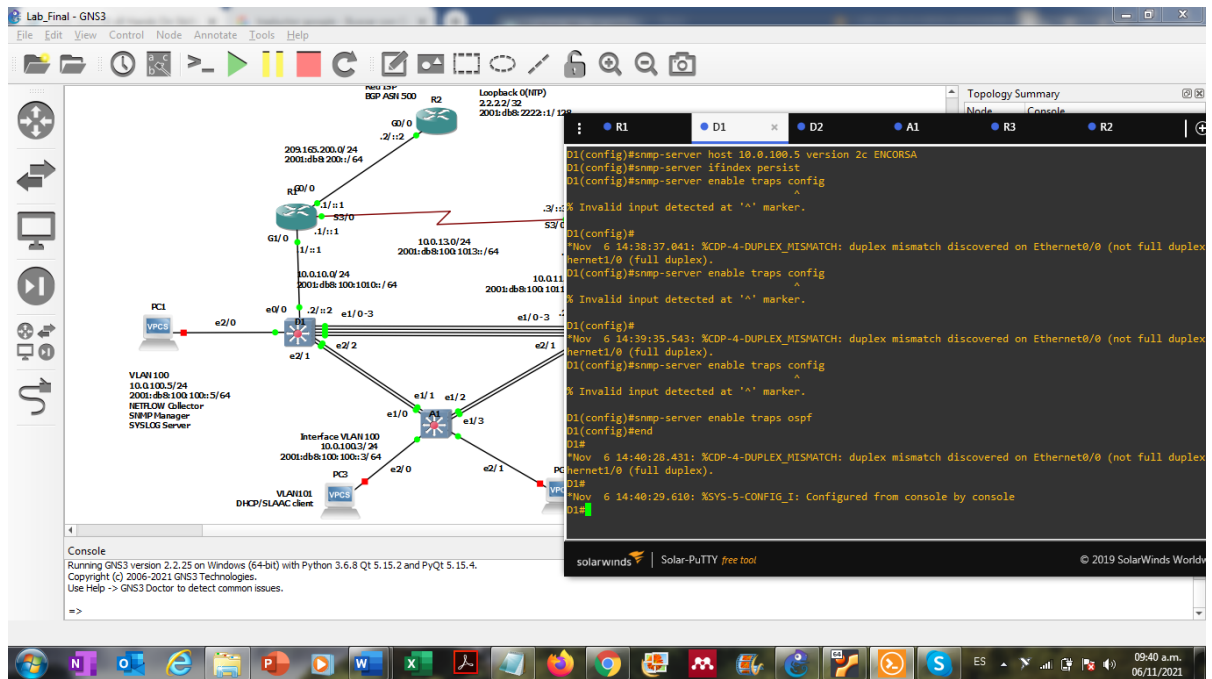


Ilustración 40. Configuración Switch D1 parte 6

Switch D2

```

ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf
end

```

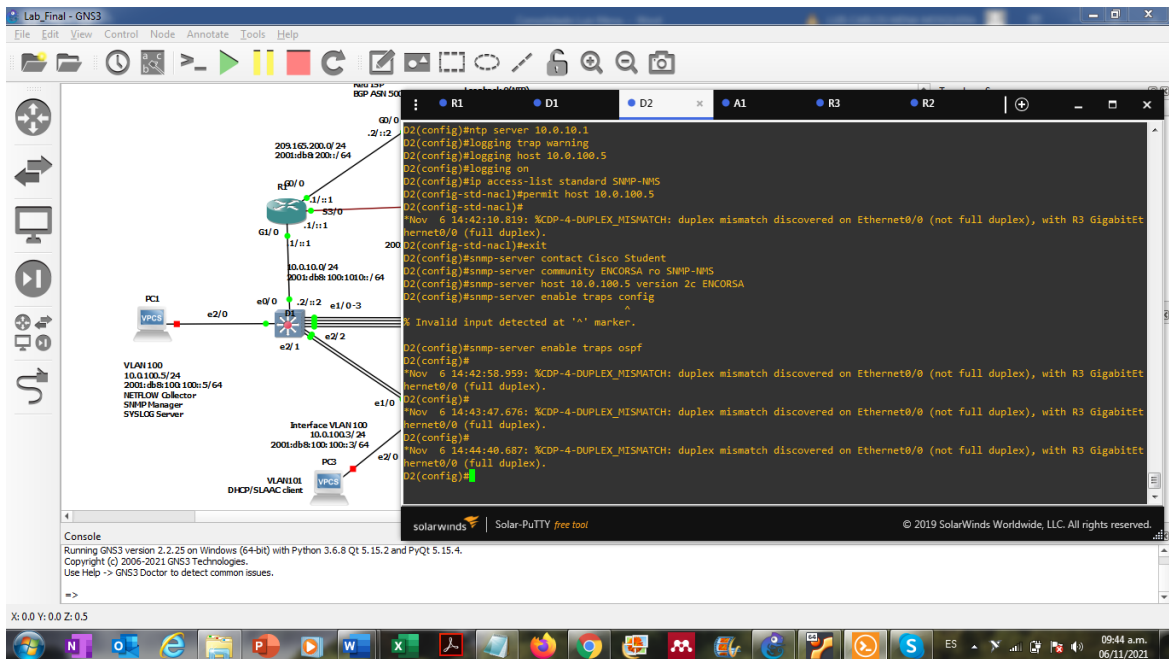


Ilustración 41. Configuración Switch D2 parte 6

Switch A1

`ntp server 10.0.10.1` Determina a qué servidor se deben enviar los archivos de registro del sistema

`logging trap warning` Controle los mensajes que se envían al servidor de syslog

`logging host 10.0.100.5` Dirección del servidor

`logging on` Activa el servidor

`ip access-list standard SNMP-NMS` Especifica la lista de acceso

`permit host 10.0.100.5` Permite la dirección del servidor

`exit` Salir

`snmp-server contact Cisco Student` Administrar nodos

`snmp-server community ENCORSA ro SNMP-NMS`

`snmp-server host 10.0.100.5 version 2c ENCORSA`

`snmp-server ifindex persist`

`snmp-server enable traps config`

`snmp-server enable traps ospf`

`end`

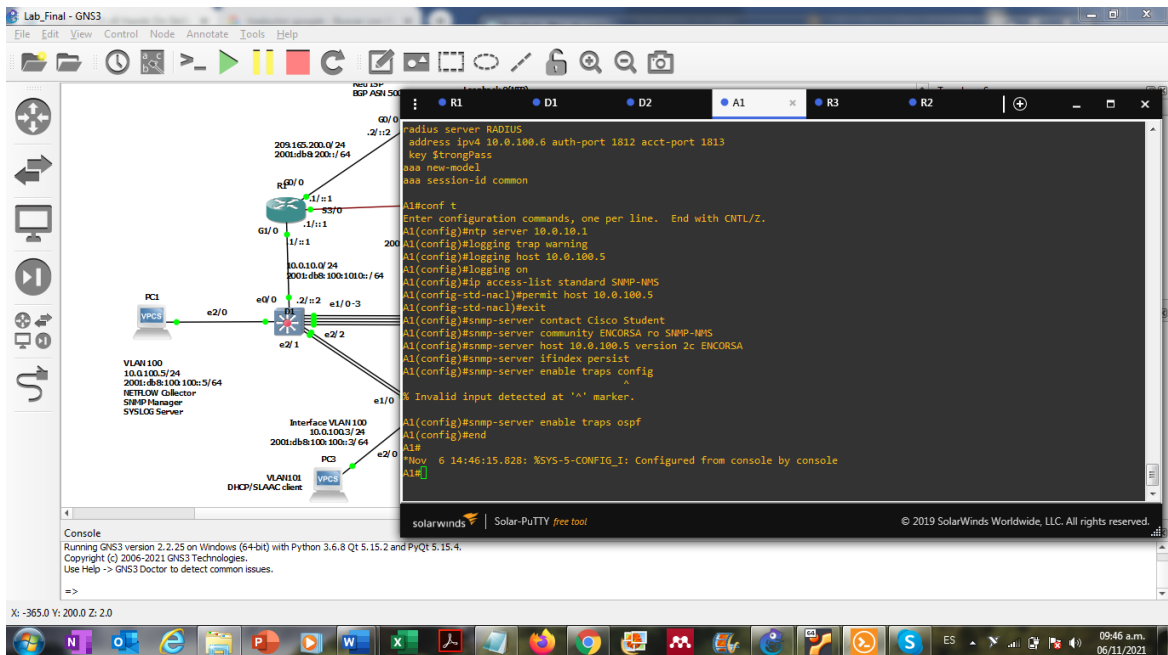


Ilustración 42. Configuración Switch A1 parte 6

Verificando la tarea 6.2 aplicamos el comando show run | include ntp en R2

R2# show run | include ntp -Muestra estado de la sincronización de NTP ntp master 3

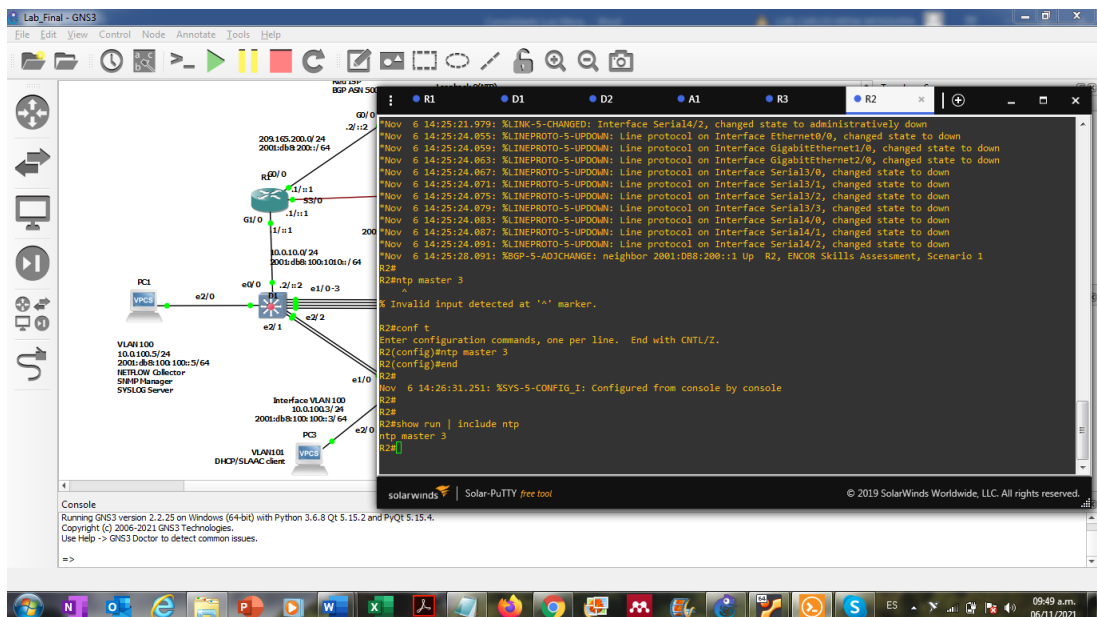


Ilustración 43. verificación tarea paso 6.2

Verificando la tarea 6.3 aplicamos el comando show ntp status | include stratum en R1

R1#show ntp status | include stratum -Muestra estado de la sincronización de NTP
Clock is synchronized, stratum 4, reference is 2.2.2.2

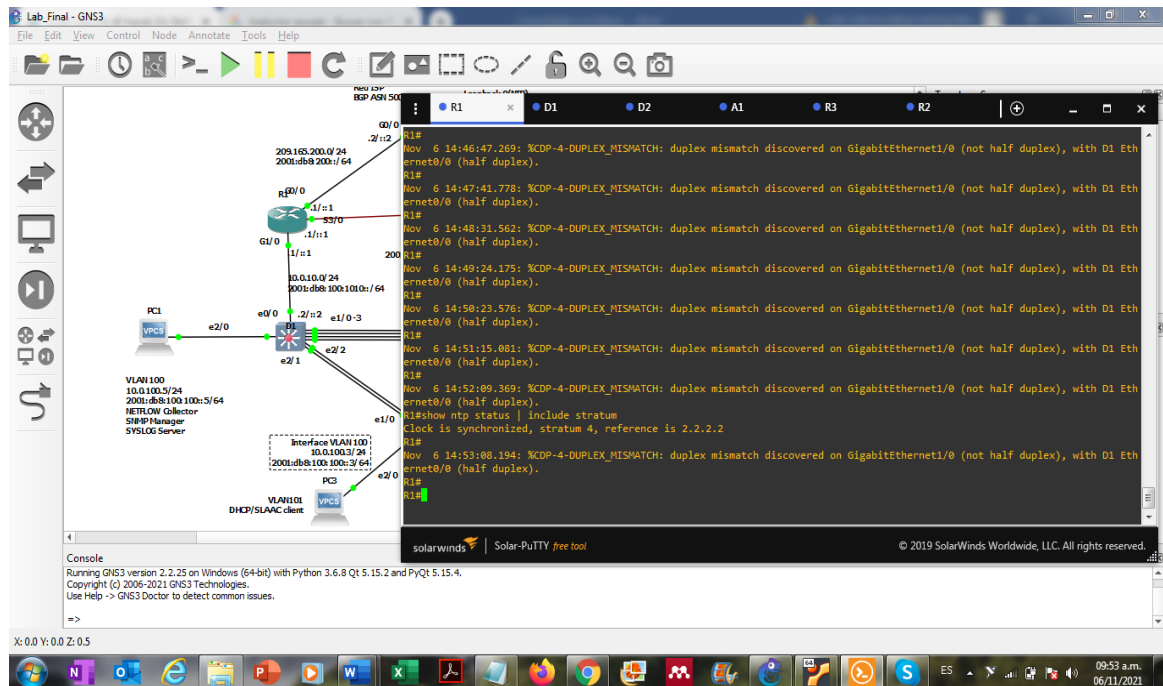


Ilustración 44. verificación tarea paso 6.3

Verificando la tarea 6.3 aplicamos el comando show ntp status | include stratum en R3, D1, D2, and A1

D1#show ntp status | include stratum -Muestra estado de la sincronización de NTP
Clock is unsynchronized, stratum 5, reference is 10.0.10.1

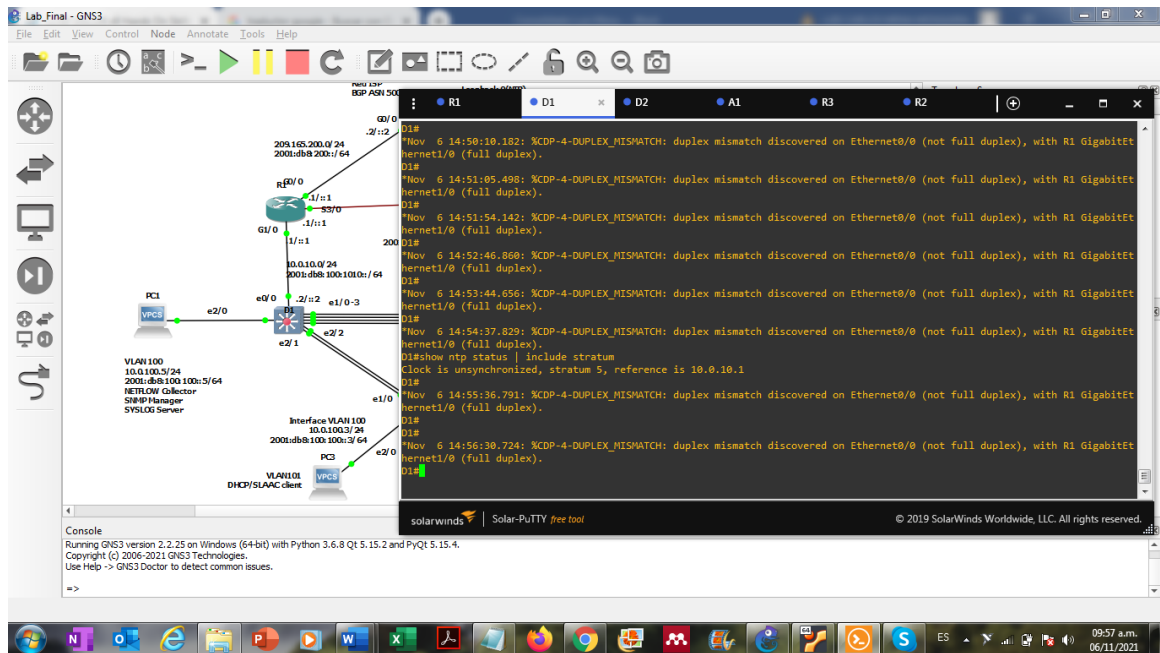


Ilustración 45. verificación tarea paso 6.3

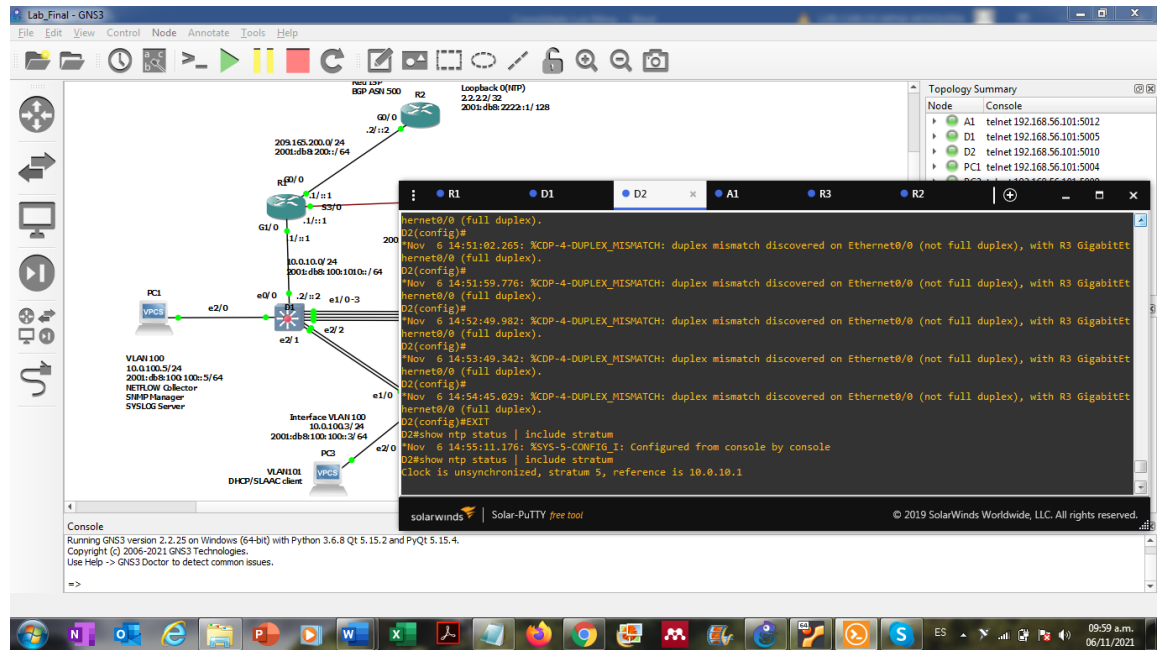


Ilustración 46. verificación tarea paso 6.3

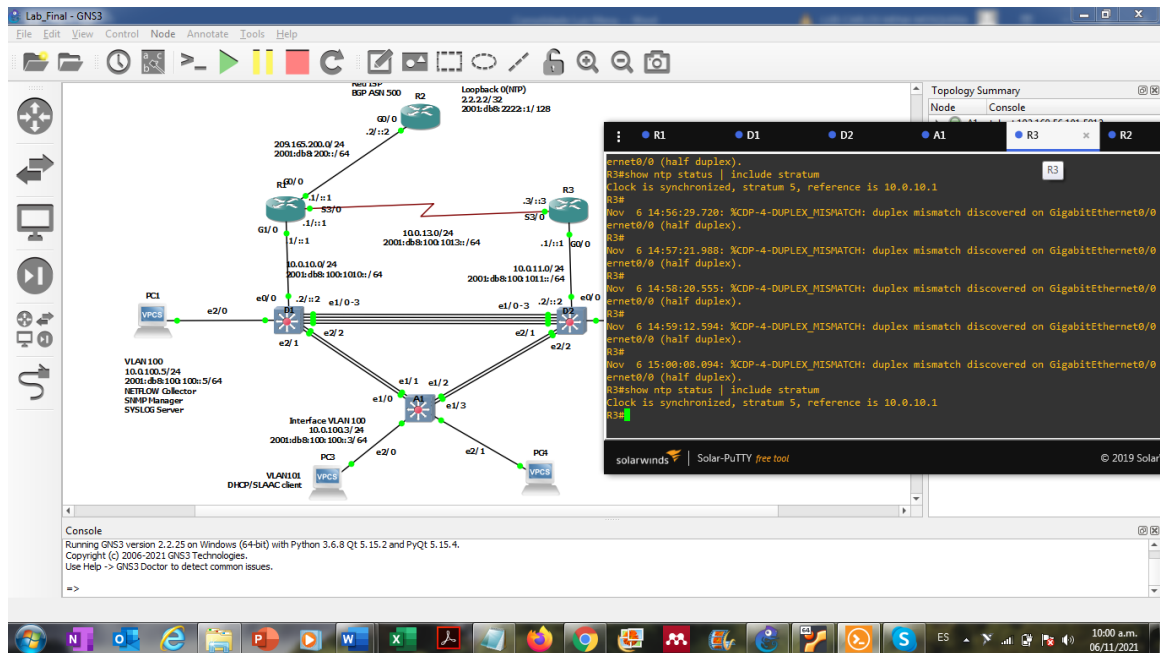


Ilustración 47. verificación tarea paso 6.3

Usamos el comando show run | include logging para verificar la tarea 6.4
R1#show run | include logging
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous

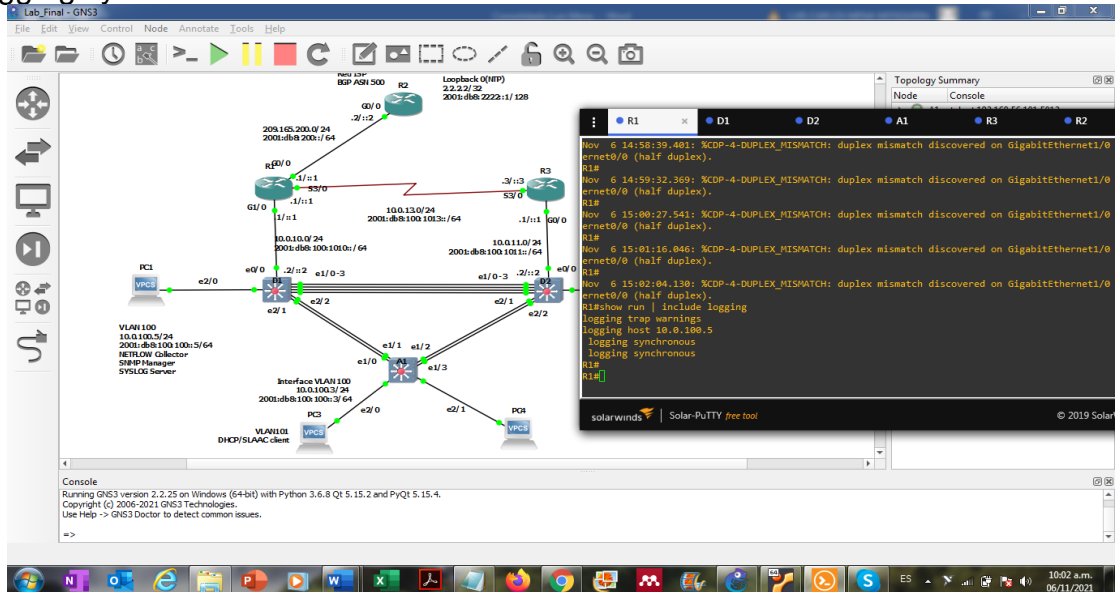


Ilustración 48. verificación tarea paso 6.3

Usamos el comando show ip access-list SNMP-NMS en todos los dispositivos para verificar la tarea 6.5

D1#show ip access-list SNMP-NMS Muestra la lista de direcciones SNMP
Standard IP access list SNMP-NMS
10 permit 10.0.100.5

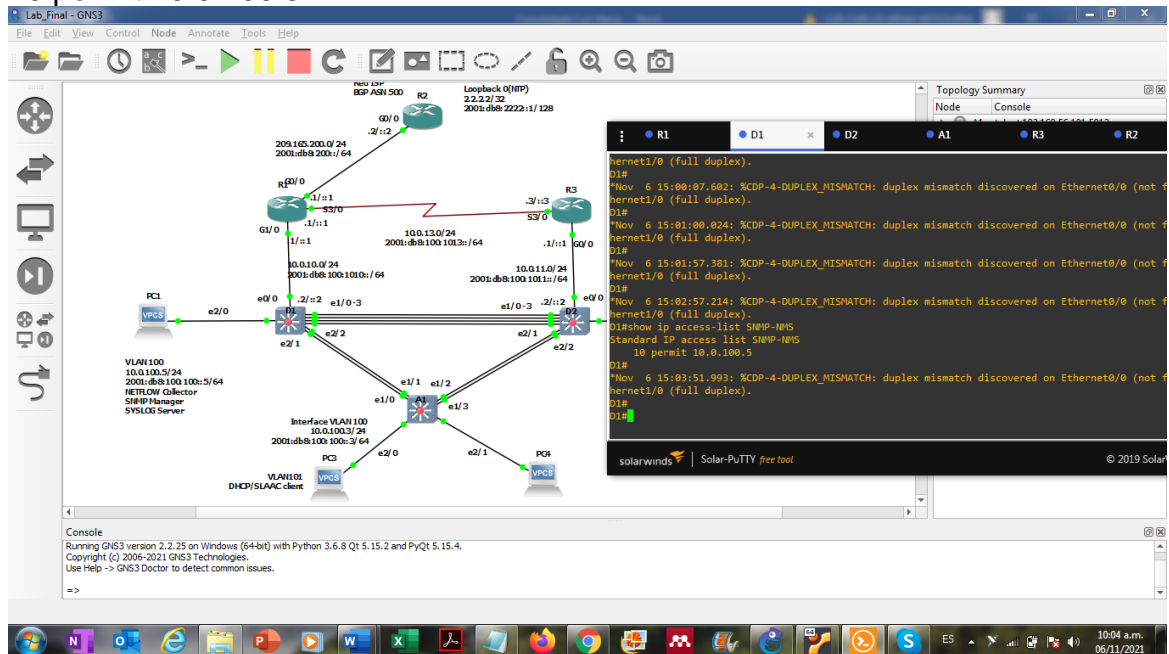


Ilustración 49. verificación tarea paso 6.5

Se aplica el comando show run | include snmp en todos los dispositivos excepto R2; la salida debe aparecer como se muestra a continuación. Esto verifica el punto 2 de la tarea 6.5.

R1#show run | include snmp Muestra la configuración específica snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit

```

snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSAS
snmp ifmib ifindex persist

```

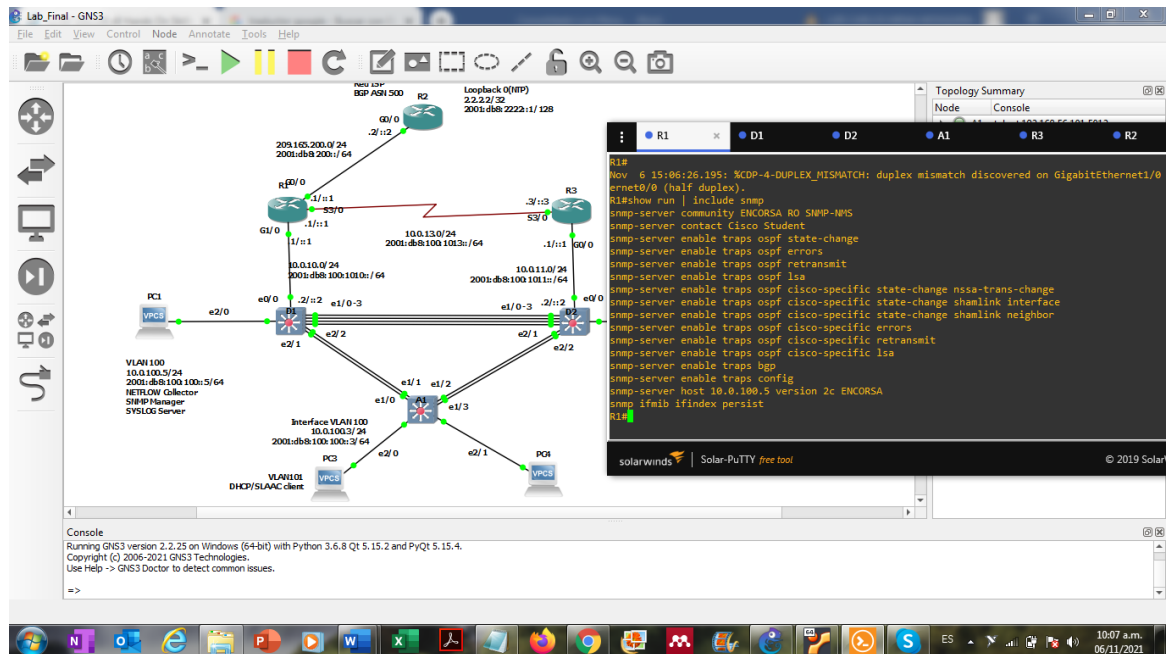


Ilustración 50. verificación tarea paso 6.5

```

R3#show run | include snmp          Muestra la configuración específica snmp
snmp-server community ENCORSAS RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSAS
snmp ifmib ifindex persist

```

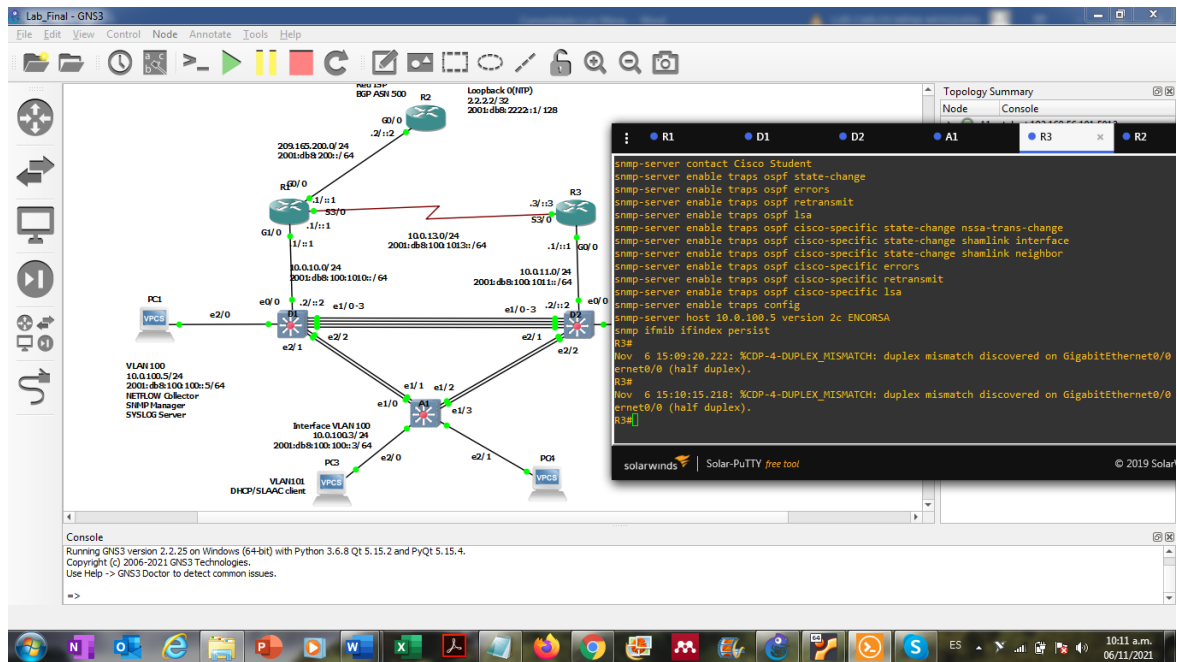


Ilustración 51. verificación tarea paso 6.5

D1#show run | include snmp Muestra la configuración específica snmp

```

snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist

```

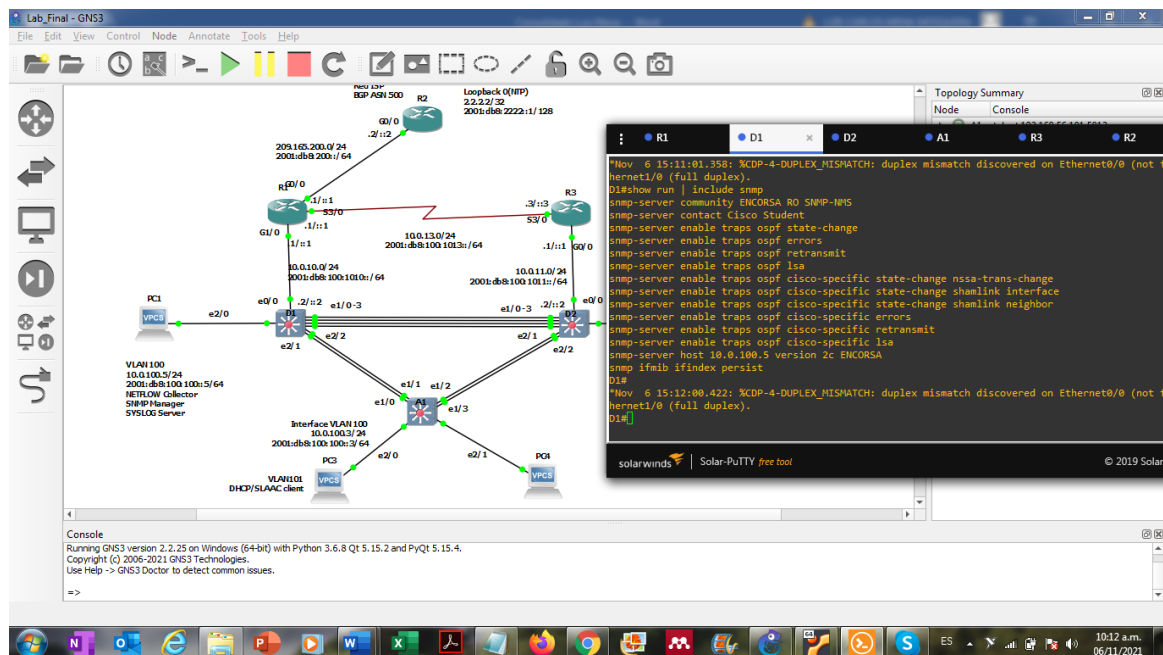


Ilustración 52. verificación tarea paso 6.5

D2#show run | include snmp Muestra la configuración específica
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA

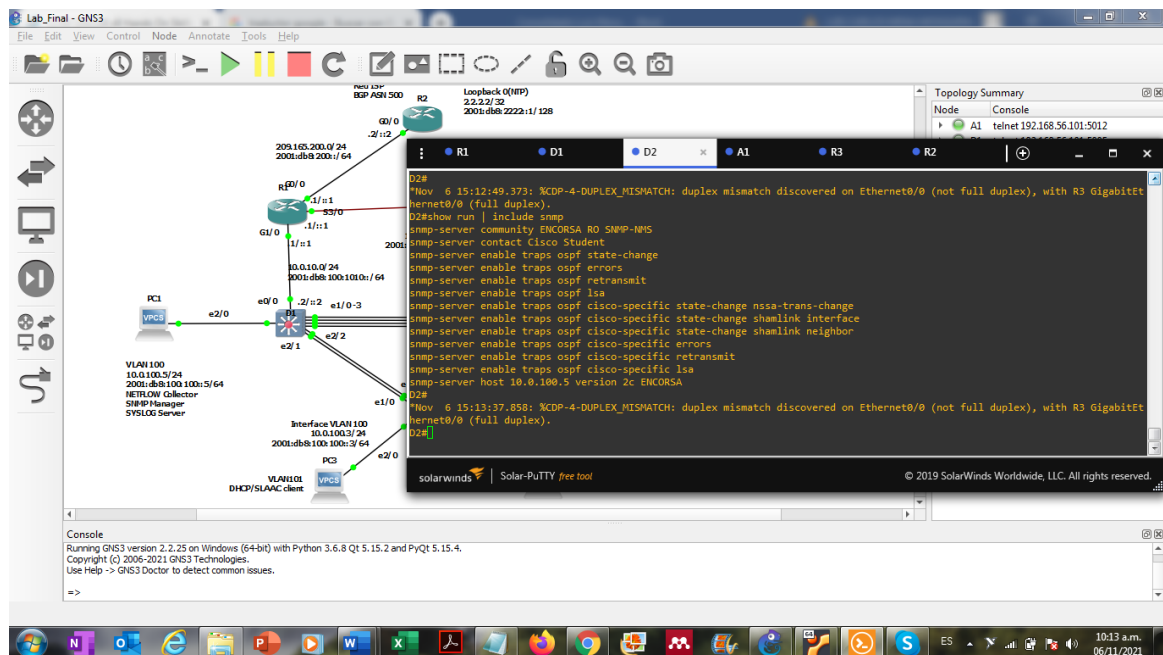


Ilustración 53. verificación tarea paso 6.5

A1#show run | include snmp Muestra la configuración específica snmp

```

snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
  
```

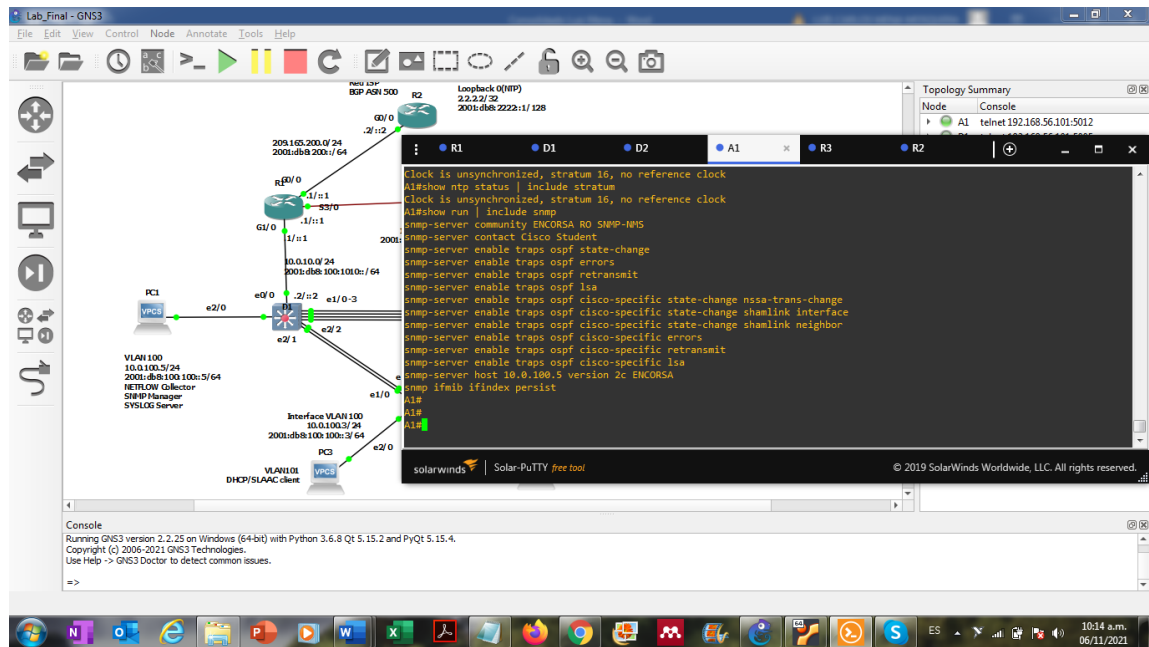


Ilustración 54. verificación tarea paso 6.5

CONCLUSIONES

Al finalizar el desarrollo del primer escenario se logra desarrollar el tema principal del curso, el cual se centra en el desarrollo de las habilidades necesarias para que la implementación de redes BGP, así como la detección y solución de problemas.

Se logró realizar el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Se comprendió que una VLAN es una red virtual que en caso de ser necesario podemos gestionar a través del Switch con el fin de dividir está en varios switches virtuales para grandes redes. Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten las mismas Vlan.

Se logra familiarizar apropiar y alcanzar los conceptos y tecnologías básicos de red aplicando configuración BGP, OSPF. Utilizado para definir la relación entre diferentes sistemas autónomos en una red de IP.

BIBLIOGRAFÍA

- Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>
- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>
- 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>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>
- UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>