

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DAVID LEONARDO GUTIERREZ FORERO

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

INGENIERÍA ELECTRÓNICA

BOGOTA D.C

2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DAVID LEONARDO GUTIERREZ FORERO

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

DIRECTOR:

MSc. GERARDO GRANADOS ACUÑA

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

INGENIERÍA ELECTRÓNICA

BOGOTA D.C

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ D.C, 28 de noviembre de 2021

AGRADECIMIENTOS

Deseo agradecer en estas líneas la ayuda que muchas personas y colegas me han prestado durante el proceso de formación. En primer lugar, quisiera agradecer a mis padres que me han ayudado y apoyado en todo mi producto, a mis tutores, por haberme orientado en todos los momentos que necesité sus consejos.

Así mismo, deseo expresar mi reconocimiento a la universidad por brindar las herramientas necesarias para fortalecer mis conocimientos durante esta etapa, también por todas las atenciones e información brindada a lo largo del desarrollo de este diplomado.

A todos mis amigos, compañeros y futuros colegas que me ayudaron de una manera desinteresada, gracias infinitas por toda su ayuda y buena voluntad.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN.....	10
INTRODUCCIÓN	12
DESARROLLO	13
Parte 1: Construya la red y configure los ajustes básicos del dispositivo y el direccionamiento de la interfaz	15
Parte 2: Configurar la capa 2 de la red y el soporte de Host	30
Parte 3: Configurar los protocolos de enrutamiento.....	41
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).	57
Parte 5: Seguridad.....	67
Parte 6: Configure las funciones de Administración de Red.....	73
CONCLUSIONES	83
BIBLIOGRAFÍA.....	84

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento	14
Tabla 2. Configuración a aplicar en Switches -Parte 2	30
Tabla 3. Configuración a aplicar en red - ISP - Parte 3.....	41
Tabla 4. Ajuste de redundancia First Hop Redundancy	57
Tabla 5. Condiciones de seguridad.....	67
Tabla 6. Administración de red	73

LISTA DE FIGURAS

Figura 1. Topología de red a desarrollar	13
Figura 2. Topología implantada en GNS3.....	15
Figura 3. Configuración general router R1	18
Figura 4. Configuración general router R2.....	20
Figura 5. Configuración general router R3.....	22
Figura 6. Configuración general switch 1	24
Figura 7. Configuración general switch 2.....	27
Figura 8. Configuración general switch A1	29
Figura 9. IP del PC1.....	29
Figura 10. IP del PC4.....	30
Figura 11. Código capa 2 de la red y el soporte de Host implementado en GNS3 D1	34
Figura 12. Verificación de la configuración switch D1	35
Figura 13. Código capa 2 de la red y el soporte de Host implementado en GNS3 D2	36
Figura 14. Verificación de la configuración switch D2.....	37
Figura 15. Código capa 2 de la red y el soporte de Host implementado en GNS3 A1	39
Figura 16. Verificación de la configuración switch D2.....	39
Figura 17. Conexión PC1 ping con éxito.....	40
Figura 18. Conexión PC2 ping con éxito.....	40
Figura 19. Conexión PC3 ping con éxito.....	40
Figura 20. Conexión PC3 ping con éxito.....	41
Figura 21. Código de enrutamiento implementado en GNS3 R1	45
Figura 22. Verificación router ospf R1.....	45
Figura 23. Verificación ipv6 router R1	46
Figura 24. Verificación sección BGP R1	46
Figura 25. Verificación ipv4 R1	46
Figura 26. Verificación rutas ipv6 R1	47
Figura 27. Código de enrutamiento implementado en GNS3 R2.....	48
Figura 28. Verificación sección BGP R2	49
Figura 29. Código de enrutamiento implementado en GNS3 R3.....	50
Figura 30. Verificación router ospf R3.....	50
Figura 31. Verificación ipv6 router R3.....	51

Figura 32. Verificación ipv4 R3	51
Figura 33. OSPFv3 para IPv6	51
Figura 34. Código de enrutamiento implementado en GNS3 D1	53
Figura 35. Verificación router ospf D1	53
Figura 36. Verificación interfaz ipv6 ospf	54
Figura 37. Código de enrutamiento implementado en GNS3 D2	56
Figura 38. Verificación router ospf D1	56
Figura 39. Verificación interfaz ipv6 ospf	56
Figura 40. Código de redundancia implementado en GNS3 D1	63
Figura 41. Verificación de ip SLA D1	63
Figura 42. Verificación de las VLAN en cada grupo D1	64
Figura 43. Código de redundancia implementado en GNS3 D2	66
Figura 44. Verificación de ip SLA D1	66
Figura 45. Código de seguridad implementado en GNS3 R1	69
Figura 46. Verificación de seguridad R1	69
Figura 47. Código de seguridad implementado en GNS3 R2	69
Figura 48. Código de seguridad implementado en GNS3 R3	70
Figura 49. Verificación de seguridad R3	70
Figura 50. Código de seguridad implementado en GNS3 D1	71
Figura 51. Verificación de seguridad D1	71
Figura 52. Código de seguridad implementado en GNS3 D2	72
Figura 53. Verificación de seguridad D2	72
Figura 54. Código de seguridad implementado en GNS3 D2	73
Figura 55. Verificación de seguridad A1	73
Figura 56. Código de administración de red implementado en GNS3 R1	75
Figura 57. Verificación de los ajustes NTP R1	75
Figura 58. Verificación de los ajustes SNMP R1	76
Figura 59. Código de administración de red implementado en GNS3 R2	76
Figura 60. Verificación de los ajustes NTP R2	76
Figura 61. Código de administración de red implementado en GNS3 R3	77
Figura 62. Verificación de los ajustes SNMP R3	78
Figura 63. Código de administración de red implementado en GNS3 D1	79
Figura 64. Verificación de los ajustes SNMP D1	79
Figura 65. Código de administración de red implementado en GNS3 D2	80
Figura 66. Verificación de los ajustes SNMP D2	81
Figura 67. Código de administración de red implementado en GNS3 A1	82
Figura 68. Verificación de los ajustes SNMP A1	82

GLOSARIO

SWITCH: Dispositivo digital de interconexión, que se encarga de conectar dos o más equipos a una misma red.

VLAN: (Virtual LAN), filosofía de red la cual puede crear varias redes lógicas a través de una sola red física.

OSPF: (Open Shortest Path First), Protocolo de enrutamiento que trabaja a partir de la supervisión del enlace que a su vez detecta cambios de la topología.

DHCP: Dynamic Host Configuration Protocol, trabaja con el modelo cliente/servidor y suministra automáticamente direcciones IP y la información asociada como la máscara y el Gateway.

BGP: (Border Gateway Protocol), Protocolo que permite al intercambio de información asociada al enrutamiento en una red con un canal ethernet.

RSTP: (Rapid Spanning Tree Protocol), ajuste para a la capa 2 el cual minimiza ampliamente la convergencia de la topología cuando sucede algún cambio.

ETHERNETCHANNEL: Es un estándar Full-duplex Fast Ethernet, el cual logra interconectar diferentes dispositivos, suficientemente robusto con una convergencia rápida.

RESUMEN

El trabajo desarrollado durante la práctica está orientado a definir los conceptos de redes de comunicación, que se requieren para brindar solución a un problema en específico, ampliando habilidades propias de la profesión en el contexto social y profesional a través de atmósferas supuestas o reales, en medio de los procesos, se puede afirmar que siempre se busca de una solución a un problema en particular a través de los escenarios propuestos del diplomado CISCO CCNP.

Aplicando a la práctica los conocimientos adquiridos durante el desarrollo de este documento; poniéndolos a prueba para un buen desempeño en el reconocimiento de la capacidad de los diferentes métodos de configuración en diferentes dispositivos, solucionando los problemas y las necesidades lógicas por medio de las expresiones ya elaboradas, teniendo en cuenta los conceptos básicos y la trascendencia de la implementación de métodos y normas que rigen en las redes industriales.

En el desarrollo se describe en el paso a paso de la configuración de 10 dispositivos conectados en a través de diferentes medios a una topología redundante, donde se parte desde la asignación de nombres, configuraciones de IP, VLAN e interfaces para cada uno, después de configura los protocolos de enrutamiento, conmutación y por últimos se detalla la disposición de seguridad y administración de la red.

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

ABSTRACT

The work developed during the practice is aimed at defining the concepts of communication networks, which is required to provide a solution to a specific problem, expanding the skills of the profession in the social and professional context through supposed or real atmospheres, in Through the processes, it can be affirmed that a solution to a particular problem is always sought through the proposed scenarios of the CISCO CCNP diploma.

Applying to practice the knowledge acquired during the development of this document; putting them to the test for a good performance in the recognition of the capacity of the different configuration methods of different devices, solving the problems and the logical needs by means of the expressions already elaborated, taking into account the basic concepts and the importance of the implementation of methods and standards that govern industrial networks.

The development describes the step-by-step configuration of 10 devices connected through different means to a redundant topology, starting from the assignment of names, IP configurations, VLANs and interfaces for each one, after configuring the routing protocols, switching and finally the security configuration and network administration are detailed.

Keywords: CISCO, CCNP, Routing, commutation, Networking.

INTRODUCCIÓN

En la actualidad las redes de comunicación tienen un papel muy importante en el desarrollo de las diferentes actividades que se efectúan a diario, ya que se pueden implementar en diferentes sectores económicos y sociales con el propósito de facilitar el envío y recepción de información desde diferentes puntos, es por eso que con el desarrollo del diplomado CCNP, se fortalecen una serie de conocimientos enfocados en la configuración, administración y diseños de diferentes redes brindando solución a las diferentes atmósferas que se pueden encontrar en la cotidianidad del ejercicio.

En el trabajo desarrollado se describen los pasos necesarios para la configuración de una topología compleja la cual se efectúa mediante una secuencia de pasos que describen el desarrollo desde lo más básico hasta lo más complejo de los diferentes dispositivo, aplicando los métodos necesarios para satisfacer la necesidad que solicita el escenario, el cual propone diez dispositivos los cuales se interconectan a través de diferentes medios físicos, que al configurar de manera lógica se logra mejorar los recursos, obteniendo compatibilidad, redundancia, seguridad y conectividad por medio de los diferentes protocolos que se habilitan en la medida que se avance en cada uno de los seis pasos.

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S02/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	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	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/0	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	E1/0	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

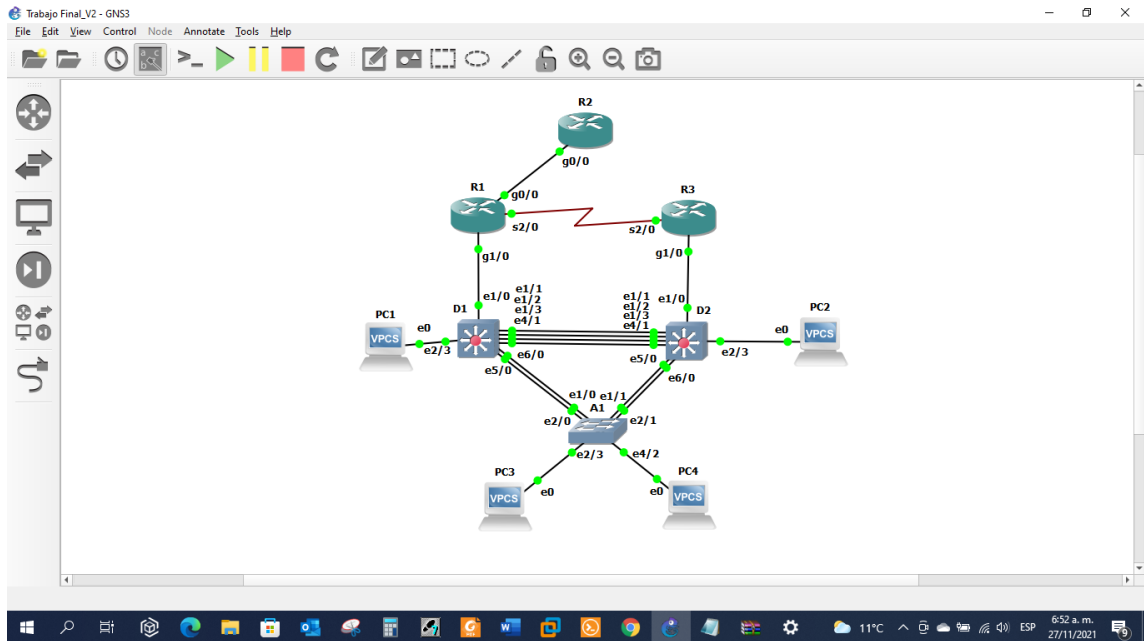
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte 1: Construya la red y configure los ajustes básicos del dispositivo y el direccionamiento de la interfaz

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

Para el desarrollo de este escenario se simuló en el software GNS3, donde se bosqueja la topología propuesta mediante las imágenes IOS encontradas en internet homologando los dispositivos solicitados en el escenario.

Figura 2. Topología implantada en GNS3



a. 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

R1#config term

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

R1(config)#hostname R1// modo configuración terminal

R1(config)#ipv6 unicast-routing // Nombra el equipo R1

R1(config)#no ip domain lookup // Visualiza si el comando no es valido

R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #

R1(config)#line con 0 // Ingreso a la consola 0

R1(config-line)# exec-time 0 0 // Excepciones de tiempo

R1(config-line)# logging sync // Inhabilita mensajes mientras e ingresa el comando

R1(config-line)# exit // Salir modo consola 0

R1(config)#interface g0/0 // Ingresa configuración global gigabit ethernet 0/0

R1(config-if)# ip add 209.165.200.225 255.255.255.224 // Asignación IP f0/0

R1(config-if)# ipv6 address fe80::1:1 link-local //Asignación red estática protocolo IPV6

R1(config-if)# ipv6 address 2001:db8:200::1/64 //Asignación red estática

R1(config-if)# no shut // Enciende la interface

R1(config-if)# exit // Salir modo configuración interface

R1(config)#interface g1/0 Ingresa configuración global gigabit ethernet 1/0


```
R1(config-if)# ip address 10.0.10.1 255.255.255.0 // Asignación IP f1/0

R1(config-if)# ipv6 address fe80::1:2 link-local //Asignación red estática protocolo
IPV6

R1(config-if)# ipv6 address 2001:db8:100:1010::1/64 //Asignación red estática

R1(config-if)# no shut // Enciende la interface

R1(config-if)# exit // Salir modo configuración interface

R1(config)#interface s2/0 // Ingresa configuración global s2/0

R1(config-if)# ip address 10.0.13.1 255.255.255.0 Asignación IP s0/1

R1(config-if)# ipv6 address fe80::1:3 link-local //Asignación red estática protocolo
IPV6

R1(config-if)# ipv6 address 2001:db8:100:1013::1/64 //Asignación red estática

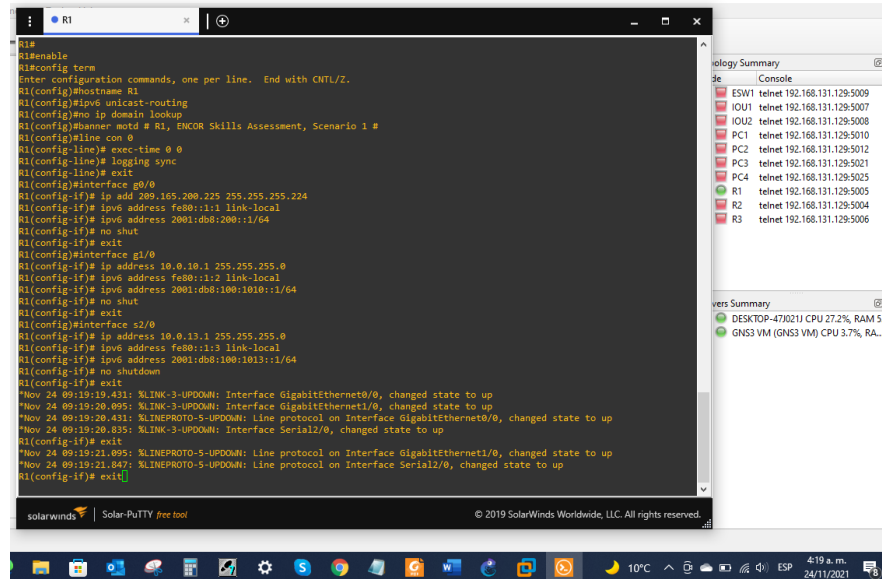
R1(config-if)# no shutdown // Enciende la interface

R1(config-if)# exit // Salir modo configuración interface

R1(config)#exit // Salir modo configuración global

Las descripciones de los comandos o líneas aplican para R2 y R3.
```

Figura 3. Configuración general router R1



Router R2

R2#enable

R2#config term

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 #

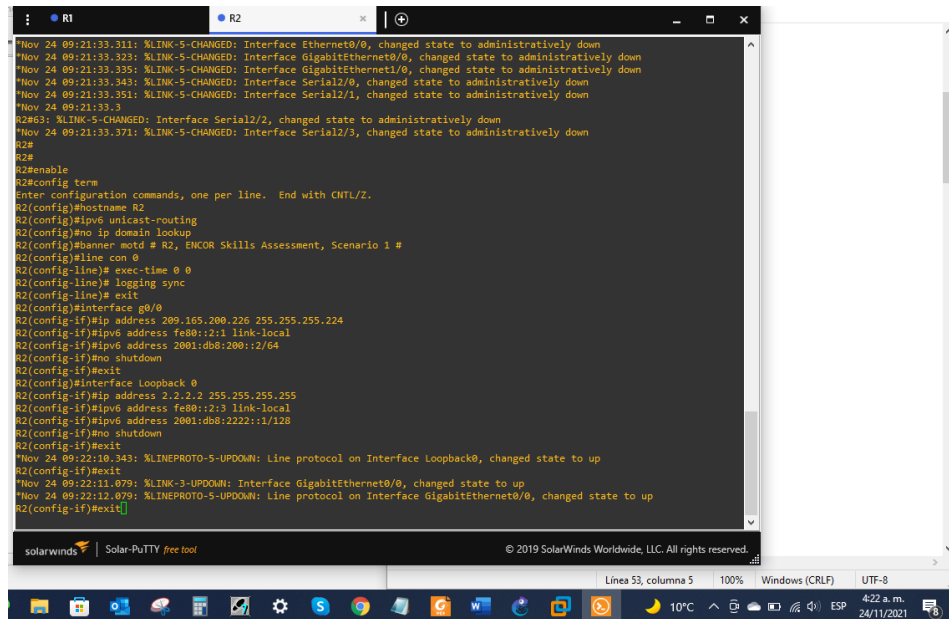
R2(config)#line con 0

R2(config-line)# exec-time 0 0

R2(config-line)# logging sync

```
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)#exit
R2(config)#interface Loopback 0
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
```

Figura 4. Configuración general router R2



```
Nov 24 09:21:33.311: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
Nov 24 09:21:33.323: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
Nov 24 09:21:33.335: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
Nov 24 09:21:33.343: %LINK-5-CHANGED: Interface Serial2/0, changed state to administratively down
Nov 24 09:21:33.351: %LINK-5-CHANGED: Interface Serial2/1, changed state to administratively down
Nov 24 09:21:33.357: %LINK-5-CHANGED: Interface Serial2/2, changed state to administratively down
R2#
R2#
R2#enable
R2#config term
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-time 0 0
R2(config-line)# logging sync
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)#exit
R2(config)#interface Loopback 0
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
Nov 24 09:22:10.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#exit
Nov 24 09:22:11.079: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Nov 24 09:22:12.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#exit
```

Router R3

R3#enable

R3#config term

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

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-time 0 0

R3(config-line)# logging sync

```
R3(config-line)# exit
R3(config)#interface g1/0
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)# exit
R3(config)#interface s2/0
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)# exit
R3(config)#exit
R3#
```



```
D1(config)#vlan 100 // Crear VLAN
D1(config-vlan)# name Management // Asignar nombre a la VLAN
D1(config-vlan)# exit // Salir modo configuración VLAN
D1(config)#vlan 101 // Crear VLAN
D1(config-vlan)# name UserGroupA // Asignar nombre a la VLAN
D1(config-vlan)# exit // Salir modo configuración VLAN
D1(config)#vlan 102 // Crear VLAN
D1(config-vlan)# name UserGroupB // Asignar nombre a la VLAN
D1(config-vlan)# exit // Salir modo configuración VLAN
D1(config)#vlan 999 // Crear VLAN
D1(config-vlan)# name NATIVE // Asignar nombre a la VLAN
D1(config-vlan)# exit // Salir modo configuración VLAN
D1(config)#interface e1/0 // Ingresar modo configuración interface ethernet 1/0
D1(config-if)# no switchport // Habilita la capa 3 y la dirección IP
D1(config-if)# ip address 10.0.10.2 255.255.255.0 // Asignación de ethernet IPV4
D1(config-if)# ipv6 address fe80::d1:1 link-local // Enciende la red estática protocolo IPV6
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64 // Asignación de la IPV6
D1(config-if)# no shutdown // Arranca la interface
D1(config-if)# exit // salir del modo configuración
D1(config)#interface vlan 100 // Ingreso a VLAN 100
D1(config-if)# ip address 10.0.100.1 255.255.255.0 // Asignación de ethernet IPV4
D1(config-if)# ipv6 address fe80::d1:2 link-local // Enciende la red estática protocolo IPV6
D1(config-if)# ipv6 address 2001:db8:100:100::1/64 // Asignación de la IPV6
D1(config-if)# no shutdown // Arranca la interface
```

D1(config-if)# exit // salir del modo configuración

D1(config)#interface vlan 101 // Ingreso a VLAN 101

D1(config-if)# ip address 10.0.101.1 255.255.255.0 0 // Asignación de ethernet IPV4

D1(config-if)# ipv6 address fe80::d1:3 link-local // Enciende la red estática protocolo IPV6

D1(config-if)# ipv6 address 2001:db8:100:101::1/64 // Asignación de la IPV6

D1(config-if)# no shutdown // Arranca la interface

D1(config-if)# exit // salir del modo configuración

D1(config)#interface vlan 102 // Ingreso a VLAN 102

D1(config-if)# ip address 10.0.102.1 255.255.255.0 // Asignación de ethernet IPV4

D1(config-if)# ipv6 address fe80::d1:4 link-local // Enciende la red estática protocolo IPV6

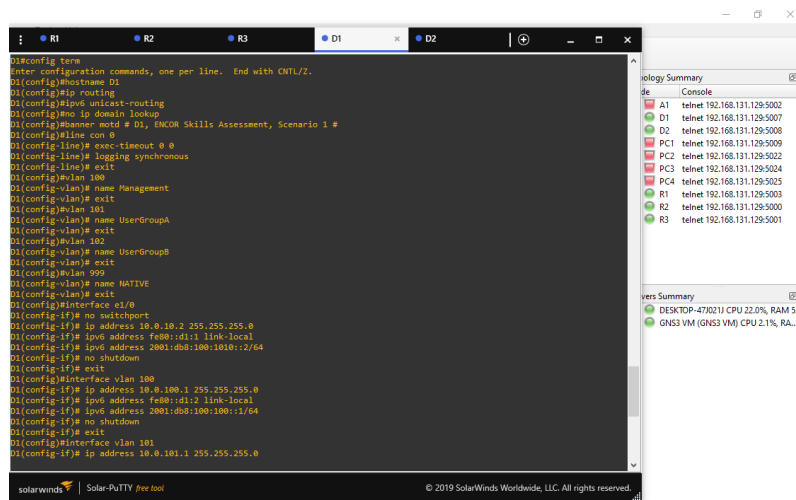
D1(config-if)# ipv6 address 2001:db8:100:102::1/64 // Asignación de la IPV6

D1(config-if)# no shutdown // Arranca la interface

D1(config-if)# exit // salir del modo configuración

Las descripciones de los comandos o líneas aplican para D2.

Figura 6. Configuración general switch 1



Switch D2

D2#config term

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

D2(config)#hostname D2

D2(config)#ip routing

D2(config)#ipv6 unicast-routing

D2(config)#no ip domain lookup

D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #

D2(config)#line con 0

D2(config-line)# exec-timeout 0 0

D2(config-line)# logging synchronous

D2(config-line)# exit

D2(config)#vlan 100

D2(config-vlan)# name Management

D2(config-vlan)# exit

D2(config)#vlan 101

D2(config-vlan)# name UserGroupA

D2(config-vlan)# exit

D2(config)#vlan 102

D2(config-vlan)# name UserGroupB

D2(config-vlan)# exit

D2(config)#vlan 999

D2(config-vlan)# name NATIVE

D2(config-vlan)# exit

D2(config)#interface e1/0

D2(config-if)# no switchport

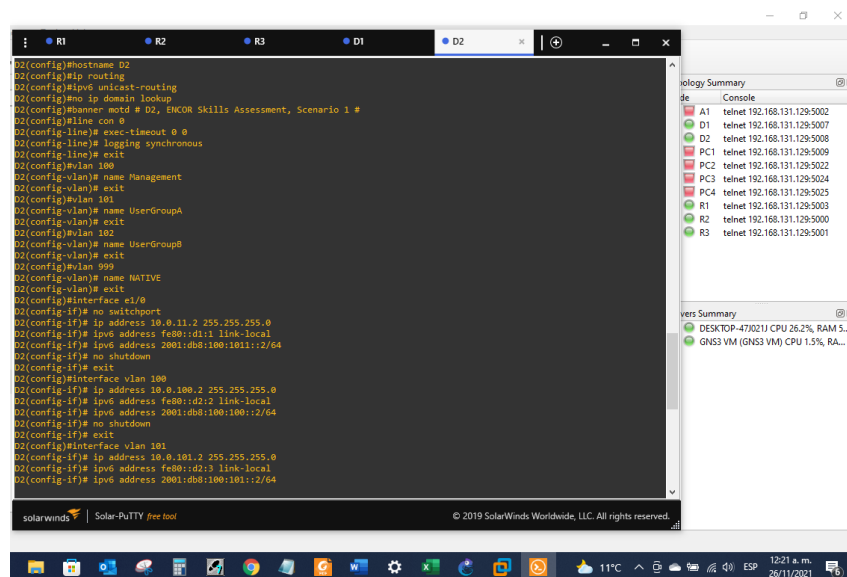
```
D2(config-if)# ip address 10.0.11.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d1:1 link-local
D2(config-if)# ipv6 address 2001:db8:100:1011::2/64
D2(config-if)# no shutdown
D2(config-if)# exit
D2(config)#interface vlan 100
D2(config-if)# ip address 10.0.100.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:2 link-local
D2(config-if)# ipv6 address 2001:db8:100:100::2/64
D2(config-if)# no shutdown
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# ip address 10.0.101.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:3 link-local
D2(config-if)# ipv6 address 2001:db8:100:101::2/64
D2(config-if)# no shutdown
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# ip address 10.0.102.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:4 link-local
D2(config-if)# ipv6 address 2001:db8:100:102::2/64
D2(config-if)# no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
```

```

D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)# network 10.0.101.0 255.255.255.0
D2(dhcp-config)# default-router 10.0.101.254
D2(dhcp-config)# exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)# network 10.0.102.0 255.255.255.0
D2(dhcp-config)# default-router 10.0.102.254
D2(dhcp-config)# exit
D2(config)#int range e1/0-3,e4/1,e5/0,e6/0,e2/3
interface range 1 invalid - command rejected
D2(config)# no shutdown
D2(config)# exit

```

Figura 7. Configuración general switch 2



Switch A1

A1#config term //

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

A1(config)#hostname A1 // Asigna nombre del switch

A1(config)#no ip domain lookup // Visualiza si el comando no es valido

A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #

A1(config)#line con 0 // Ingreso a la consola 0

A1(config-line)# exec-timeout 0 0 // Excepciones de tiempo

A1(config-line)# logging synchronous // Inhabilita mensajes mientras e ingresa el comando

A1(config-line)# exit // Salir de modo configuración consola 0

A1(config)#vlan 100 // Crear VLAN

A1(config-vlan)# name Management // Asignar nombre a la VLAN

A1(config-vlan)# exit // Salir modo configuración VLAN

A1(config)#vlan 101 // Crear VLAN

A1(config-vlan)# name UserGroupA // Asignar nombre a la VLAN

A1(config-vlan)# exit // Salir modo configuración VLAN

A1(config)#vlan 102 // Crear VLAN

A1(config-vlan)# name UserGroupB // Asignar nombre a la VLAN

A1(config-vlan)# exit // Salir modo configuración VLAN

A1(config)#vlan 999 // Crear VLAN

A1(config-vlan)# name NATIVE // Asignar nombre a la VLAN

A1(config-vlan)# exit // Salir modo configuración VLAN

A1(config)#interface vlan 100 // Ingreso a VLAN 100

A1(config-if)# ip address 10.0.100.3 255.255.255.0 // Asignación de ethernet IPV4

A1(config-if)# ipv6 address fe80::a1:1 link-local Enciende la red estática protocolo IPV6

A1(config-if)# ipv6 address 2001:db8:100:100::3/64 // Asignación de la IPV6

A1(config-if)# no shutdown // Arranca la interface

A1(config-if)#exit // salir del modo configuración

A1(config)#interface range e1/0-1,e2/0-3,e4/0-2 // rango de interface ethernet a configurar

A1(config-if-range)# shutdown // Encender interface

A1(config-if-range)# exit // Salir del modo configuración interface

Figura 8. Configuración general switch A1

```
A1(config)#line con 0
A1(config-line)# exec-timeout 0 0
A1(config-line)# logging synchronous
A1(config-line)# exit
A1(config)#vlan 100
A1(config-vlan)# name Management
A1(config-vlan)# exit
A1(config)#vlan 101
A1(config-vlan)# name UserGroupA
A1(config-vlan)# exit
A1(config)#vlan 102
A1(config-vlan)# name UserGroupB
A1(config-vlan)# exit
A1(config)#vlan 999
A1(config-vlan)# name NATIVE
A1(config-vlan)# exit
A1(config)#interface vlan 100
A1(config-if)# ip address 10.0.100.1 255.255.255.0
A1(config-if)# ip address fe80::1db8:110a::1ca4
A1(config-if)# ip address 2001:db8:100:100::1/64
A1(config-if)# no shutdown
A1(config-if)#exit
A1(config)#interface range e1/0-1,e2/0-3,e4/0-2
A1(config-if-range)# shutdown
A1(config-if-range)# exit
A1(config)#
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e1/0,e2/0
A1(config-if-range)# multiport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
A range command terminated because it failed on Ethernet/0
A1(config-if-range)# multiport trunk native vlan 999
A1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
A1(config-if-range)# no shutdown
A1(config-if-range)# exit
```

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

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.

Figura 9. IP del PC1

```
PC1> ip 10.0.100.5 255.255.255.0 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.100.5/24 10.0.100.254 08:50:79:66:68:00 20048 127.0.0.1:20049
fe80::250:79ff:fe66:6800/64
2001:db8:100:100:2050:79ff:fe66:6800/64 eui-64

PC1>
```

Figura 10. IP del PC4

```
PC4> ip 10.0.100.6 255.255.255.0 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> SH
Bad command: "SH". Use ? for help.

PC4> sh

NAME      IP/WASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4      10.0.100.6/24  10.0.100.254  00:50:79:66:68:01  20046  127.0.0.1:20047
         fe80::250:79ff:fe66:6801/64
         2001:db8:100:100:2050:79ff:fe66:6801/64  eui-64

PC4> █
```

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 deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 2. Configuración a aplicar en Switches -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).
2.4	<p>En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.</p> <p>D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).</p>	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.	<p>Use los siguientes números de canales:</p> <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.	<p>Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.</p> <p>Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).</p>

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

Switch D1

D1(config)#

D1(config)#interface range e1/1-3, e4/1 //Determina el rango de interfaces ethernet

D1(config-if-range)#switchport trunk encapsulation dot1q // enlace troncal
encapsulation dot1q

D1(config-if-range)#switchport mode trunk // Enlace troncal para las interfaces

D1(config-if-range)#switchport trunk native vlan 999 // VLAN en la que se habilita el
protocolo encapsulation dot1q

D1(config-if-range)#channel-group 12 mode active // Canal que tiene el grupo activo

D1(config-if-range)#no shutdown // Activar interface

D1(config-if-range)#exit // Salir del modo configuración de rango

D1(config)#interface range e5/0,e6/0 //Determina el rango de interfaces ethernet

D1(config-if-range)#switchport trunk encapsulation dot1q // enlace troncal
encapsulation dot1q

D1(config-if-range)#switchport mode trunk // Enlace troncal para las interfaces

D1(config-if-range)#switchport trunk native vlan 999 // VLAN en la que se habilita el
protocolo encapsulation dot1q

D1(config-if-range)#channel-group 1 mode active // Canal que tiene el grupo activo

D1(config-if-range)#no shutdown // Activar interface

D1(config-if-range)#exit // Salir del modo configuración de rango

D1(config)#spanning-tree mode rapid-pvst // Configuración rápida pvst

D1(config)#spanning-tree vlan 100,102 root primary // Asignación de la prioridad
primaria

D1(config)#spanning-tree vlan 101 root secondary // Asignación de la prioridad
secundaria

D1(config)#interface e2/3 // Habilidadación del rango de interface ethernet

D1(config-if)#switchport mode Access // Acceso al puerto

D1(config-if)#switchport access vlan 100 // Fuerza la creación de una VLAN

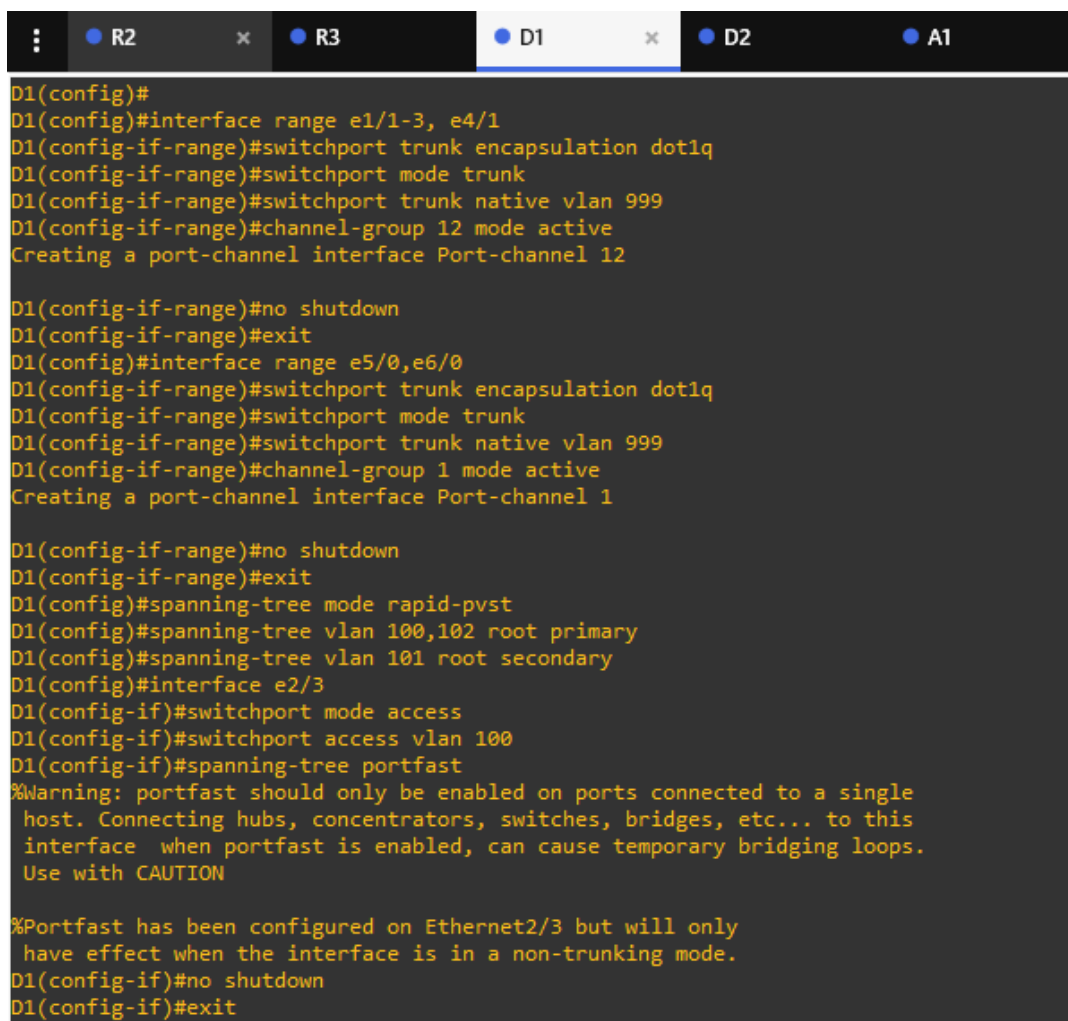
D1(config-if)#spanning-tree portfast // Habilita el portfast conexión rápida

D1(config-if)#no shutdown // Enciende la VLAN

D1(config-if)#exit // sale del modo configuración switchport

D1(config)#end // salir del modo configuración global

Figura 11. Código capa 2 de la red y el soporte de Host implementado en GNS3 D1



```
D1(config)#
D1(config)#interface range e1/1-3, e4/1
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range e5/0,e6/0
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface e2/3
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet2/3 but will only
have effect when the interface is in a non-trunking mode.
D1(config-if)#no shutdown
D1(config-if)#exit
```

Figura 12. Verificación de la configuración switch D1

```
Port      Mode      Encapsulation  Status      Native vlan
Et1/1    on        802.1q         trunking    999
Po1      on        802.1q         trunking    999
Po12     on        802.1q         trunking    999

Port      Vlans allowed on trunk
Et1/1    none
Po1      1-4094
Po12     1-4094

Port      Vlans allowed and active in management domain
Et1/1    none
Po1      1,100-102,999
Po12     1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Et1/1    none
Po1      1,100-102,999
Po12     1,100-102,999
D1#show run | include spanning-tree
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
D1#show run inter g1/0
^
% Invalid input detected at '^' marker.

D1#show run inter e2/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/3
 switchport access vlan 100
 switchport mode access
```

Las descripciones de los comandos o líneas aplican para D2.

Switch D2

```
D2(config)#interface range e5/0,e6/0
```

```
D2(config-if-range)# switchport trunk encapsulation dot1q
```

```
D2(config-if-range)# switchport mode trunk
```

```
D2(config-if-range)# switchport trunk native vlan 999
```

```
D2(config-if-range)# channel-group 2 mode active
```

```
D2(config-if-range)# no shutdown
```

```

D2(config-if-range)# exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 101,102 root secondary
D2(config)#interface e2/3
D2(config-if)# switchport mode access
D2(config-if)# switchport access vlan 102
D2(config-if)# spanning-tree portfast
D2(config-if)# no shutdown
D2(config-if)# exit
D2(config)#end

```

Figura 13. Código capa 2 de la red y el soporte de Host implementado en GNS3 D2

```

D2#config term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#interface range e1/1-3, e4/1
D2(config-if-range)# switchport trunk encapsulation dot1q
D2(config-if-range)# switchport mode trunk
D2(config-if-range)# switchport trunk native vlan 999
D2(config-if-range)# channel-group 12 mode active
D2(config-if-range)# no shutdown
D2(config-if-range)# exit
D2(config)#interface range e5/0,e6/0
D2(config-if-range)# switchport trunk encapsulation dot1q
D2(config-if-range)# switchport mode trunk
D2(config-if-range)# switchport trunk native vlan 999
D2(config-if-range)# channel-group 2 mode active
D2(config-if-range)# no shutdown
D2(config-if-range)# exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 101,102 root secondary
D2(config)#interface e2/3
D2(config-if)# switchport mode access
D2(config-if)# switchport access vlan 102
D2(config-if)# spanning-tree portfast
D2(config-if)# no shutdown
D2(config-if)# exit
D2(config)#end
D2#

```

Figura 14. Verificación de la configuración switch D2



```
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 101-102 priority 28672
spanning-tree portfast edge
D2#show run interface e2/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/3
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
end
D2#
```

Switch A1

A1(config)#

A1(config)#spanning-tree mode rapid-pvst // Configuración más rápido pvst

A1(config)#interface range e1/0,e2/0 // Selección del rango de las interfaces ethernet

A1(config-if-range)# switchport mode trunk // configuración modo trunk

A1(config-if-range)# switchport trunk native vlan 999 // Asociar VLAN

A1(config-if-range)# channel-group 1 mode active //Activación del grupo

A1(config-if-range)# no shutdown // Encender la configuración

A1(config-if-range)# exit // Salir del modo de configuración rango

```
A1(config)#interface range e1/1,e2/1 // Selección del rango de las interfaces ethernet
A1(config-if-range)# switchport mode trunk // configuración modo trunk
A1(config-if-range)# switchport trunk native vlan 999 // Asociar VLAN
A1(config-if-range)# channel-group 2 mode active //Activación del grupo
A1(config-if-range)# no shutdown // Encender la configuración
A1(config-if-range)# exit // Salir del modo de configuración rango
A1(config)#interface e2/3 // Selección del rango de las interfaces ethernet
A1(config-if)# switchport mode Access // Acceso al puerto de interfaz del swicht
A1(config-if)# switchport access vlan 101 // Puerto con acceso a VLAN 101
A1(config-if)# spanning-tree portfast // Conexión de puertos rápida
A1(config-if)# no shutdown // Encender configuración
A1(config-if)# exit // Salir del modo de configuración interface
A1(config)#interface e4/2 // Selección del rango de las interfaces ethernet
A1(config-if)# switchport mode access // Acceso al puerto de interfaz del swicht
A1(config-if)# switchport access vlan 100 // Puerto con acceso a VLAN 100
A1(config-if)# spanning-tree portfast // Conexión de puertos rápida
A1(config-if)# no shutdown // Encender configuración
A1(config-if)# exit // Salir del modo de configuración interface
A1(config)#end // Finalizar configuración del switch
```

Figura 15. Código capa 2 de la red y el soporte de Host implementado en GNS3 A1

```

A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e1/0,e2/0
A1(config-if-range)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
% Range command terminated because it failed on Ethernet1/0
A1(config-if-range)# switchport trunk native vlan 999
A1(config-if-range)# channel-group 1 mode active
A1(config-if-range)# no shutdown
A1(config-if-range)# exit
A1(config)#interface range e1/1,e2/1
A1(config-if-range)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
% Range command terminated because it failed on Ethernet1/1
A1(config-if-range)# switchport trunk native vlan 999
A1(config-if-range)# channel-group 2 mode active
A1(config-if-range)# no shutdown
A1(config-if-range)# exit
A1(config)#interface e2/3
A1(config-if)# switchport mode access
A1(config-if)# switchport access vlan 101
A1(config-if)# spanning-tree portfast
A1(config-if)# no shutdown
A1(config-if)# exit
A1(config)#interface e4/2
A1(config-if)# switchport mode access
A1(config-if)# switchport access vlan 100
A1(config-if)# spanning-tree portfast
A1(config-if)# no shutdown
A1(config-if)# exit
A1(config)#end
A1#
```

Figura 16. Verificación de la configuración switch D2

```

*Nov 27 23:15:30.689: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on E
999).
A1#
*Nov 27 23:15:32.157: %LINK-3-UPDOWN: Interface Port-channel2, changed state to down
*Nov 27 23:15:32.177: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
*Nov 27 23:15:33.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, ch
*Nov 27 23:15:33.178: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, ch
A1#
*Nov 27 23:15:39.628: %LINK-3-UPDOWN: Interface Port-channel2, changed state to up
*Nov 27 23:15:40.383: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Nov 27 23:15:40.629: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, ch
A1#
*Nov 27 23:15:41.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, ch
A1#
A1#show run interface e2/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/3
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end

A1#show run interface e4/2
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet4/2
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end

A1#
```

Figura 17. Conexión PC1 ping con éxito

```
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.254 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.309 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.292 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.272 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.310 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.542 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.631 ms
10.0.100.2 icmp_seq=3 timeout
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.644 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.052 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.349 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=0.527 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.488 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.809 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.397 ms

PC1>
```

Figura 18. Conexión PC2 ping con éxito

```
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=38.119 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=12.925 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=17.104 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=20.351 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=23.185 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=14.236 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=4.638 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=6.096 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=12.384 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=7.646 ms

PC2>
```

Figura 19. Conexión PC3 ping con éxito

```
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=33.724 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=21.641 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=24.729 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=25.503 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=31.104 ms

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=41.112 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=22.212 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=15.939 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=37.948 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=21.162 ms

PC3>
```


Figura 20. Conexión PC3 ping con éxito

```

PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.258 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.398 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.908 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.661 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.408 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.232 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.631 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.854 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.498 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.407 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.233 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.896 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.692 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.657 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.664 ms

PC4>
    
```

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.

Tabla 3. Configuración a aplicar en red - ISP - Parte 3

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single área OSPFv2 en área 0.	Use OSPF Process ID 4 y asigne los siguientes router IDs: <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Área 0.

		<ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	<p>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.</p>	<p>Use OSPF Process ID 6 y asigne los siguientes router IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Área 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	<p>En R2 en la “Red ISP”, configure MP BGP.</p>	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id</p>

		<p>2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la "Red ISP", configure MP BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48

Router R1

R1(config)#router ospf 4 // Habilitar medio ospf en proceso 4

R1(config-router)# router-id 0.0.4.1 // Nombre del router ID ospf

R1(config-router)# network 10.0.10.0 0.0.0.255 área

0 // Asignación de la ruta del área 0

R1(config-router)# default-information originate // Ruta predeterminada

```
R1(config-router)# exit // salir del modo configuración router
R1(config-router)# ipv6 router ospf 6 // Habilitar medio ospf en proceso 6
R1(config-rtr)# router-id 0.0.6.1 // Nombre del router ID ospf
R1(config-rtr)# default-information originate // Ruta predeterminada
R1(config-rtr)# exit // salir del modo configuración router
R1(config)#interface s2/0 // Modo de configuración interface
R1(config-if)# ipv6 ospf 6 área 0 // Habilitar el ospf en el proceso 6 área 0
R1(config-if)# interface g1/0 // Modo de configuración interface
R1(config-if)# ipv6 ospf 6 área 0 // Habilitar el ospf en el proceso 6 área 0
R1(config-if)# exit // salir del modo configuración interface
R1(config)#ip route 10.0.0.0 255.0.0.0 null0 // Configura la IP route submask
255.0.0.0 con interface null0
R1(config)#ipv6 route 2001:db8:100::/48 null0 // Configura ruta estatica ipv6
R1(config)#router bgp 300 // Utiliza BGP ASN 300
R1(config-router)#bgp router-id 1.1.1.1 // Configura el ID del router BGP
R1(config-router)#neighbor 209.165.200.226 remote-as 500 // Habilita relación con
ipv4 con R2 en ASN 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500 // Habilita relación con
ipv4 con R2 en ASN 500
R1(config-router)#address-family ipv4 unicast // Reconoce una familia de
direcciones y evita el intercambio de direcciones ipv4
R1(config-router-af)#neighbor 209.165.200.226 activate // Activacion de la dirección
del adyacente en ipv4
R1(config-router-af)#no neighbor 2001:db8:200::2 activate // Excluye ipv6 del
adyacente
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0 // Informando que pertenece
a la familia de direcciones ipv6
R1(config-router)#address-family ipv6 unicast // Habilitar interface del adyacente en
ipv6
```

R1(config-router-af)#neighbor 2001:db8:200::2 activate // Encendido de la dirección ipv6 del contiguo

R1(config-router-af)#network 2001:db8:100::/48 // Referencia la dirección de la red Loopback

R1(config-router-af)#exit-address-family // salir del modo de configuración interface del adyacente ipv6

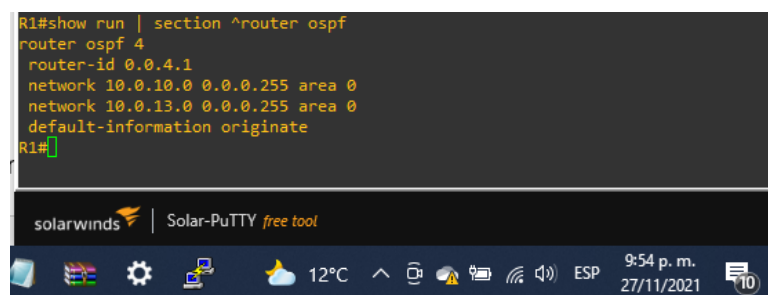
R1(config-router)#end // Finaliza configuración

Figura 21. Código de enrutamiento implementado en GNS3 R1



```
R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)# router-id 0.0.4.1
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate
R1(config-router)# exit
R1(config)#interface g0/0
R1(config-if)# router ospf 4
R1(config-router)# default-information originate
R1(config-router)# ipv6 router ospf 6
R1(config-rtr)# router-id 0.0.6.1
R1(config-rtr)# exit
R1(config)#interface s2/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# interface g1/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
R1(config)# ipv6 route ::/0 g0/0
R1(config)# ipv6 router ospf 6
R1(config-rtr)# default-information originate
R1(config-rtr)# exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#no bgp default ipv4-unicast
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family
R1(config-router)#end
R1#
```

Figura 22. Verificación router ospf R1



```
R1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
R1#
```

Figura 23. Verificación ipv6 router R1

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#
```

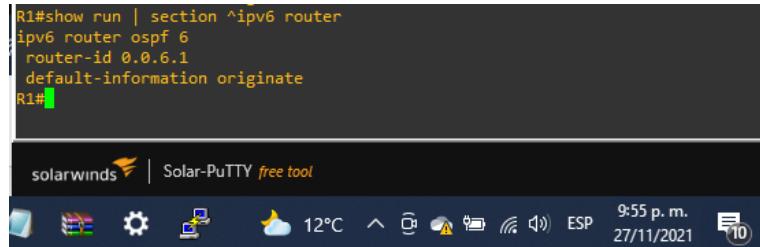


Figura 24. Verificación sección BGP R1

```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    neighbor 209.165.200.226 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
  snmp-server enable traps bgp
R1#
```

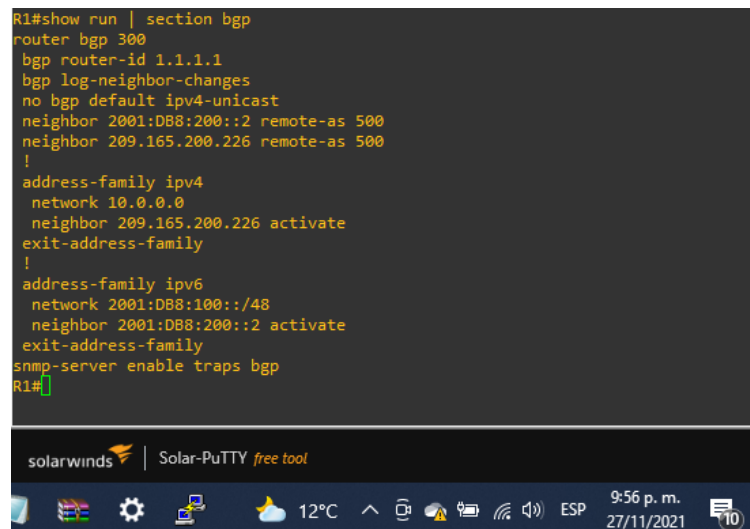


Figura 25. Verificación ipv4 R1

```
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
B
2.2.2.2 [20/0] via 209.165.200.226, 01:09:22
O
10.0.11.0/24 [110/65] via 10.0.13.3, 00:32:34, Serial2/0
O
10.0.100.0/24 [110/2] via 10.0.10.2, 01:09:10, GigabitEthernet1/0
O
10.0.101.0/24 [110/2] via 10.0.10.2, 01:09:10, GigabitEthernet1/0
O
10.0.102.0/24 [110/2] via 10.0.10.2, 01:09:10, GigabitEthernet1/0
R1#
```

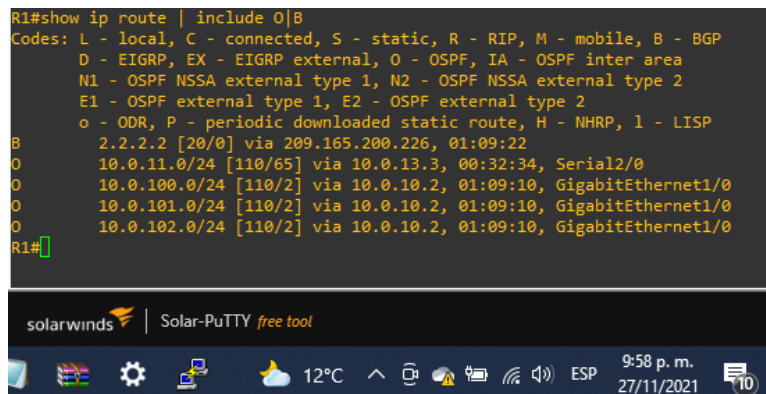


Figura 26. Verificación rutas ipv6 R1

```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
S ::0 [1/0]
  via GigabitEthernet0/0, directly connected
S 2001:DB8:100::/48 [1/0]
  via Null0, directly connected
O 2001:DB8:100:100::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
O 2001:DB8:100:101::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
O 2001:DB8:100:102::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
C 2001:DB8:100:1010::/64 [0/0]
  via GigabitEthernet1/0, directly connected
L 2001:DB8:100:1010::1/128 [0/0]
  via GigabitEthernet1/0, receive
O 2001:DB8:100:1011::/64 [110/65]
  via FE80::3:3, Serial2/0
C 2001:DB8:100:1013::/64 [0/0]
  via Serial2/0, directly connected
L 2001:DB8:100:1013::1/128 [0/0]
  via Serial2/0, receive
C 2001:DB8:200::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:200::1/128 [0/0]
  via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
R1#
```

Router R2

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 // Configuración de rutas estáticas en ipv4

R2(config)#ipv6 route ::0 loopback 0 // Configuración de rutas estáticas em ipv6

R2(config)#router bgp 500 // Utiliza BGP ASN 500

R2(config-router)#bgp router-id 2.2.2.2 // Configura el ID del router BGP

R2(config-router)#neighbor 209.165.200.225 remote-as 300 // Habilita relación con el adyacente ipv4 con R1

R2(config-router)#neighbor 2001:db8:200::1 remote-as 300 // Habilita relación con el adyacente ipv6 con R1

```

R2(config-router)#address-family ipv4 unicast // Habilita relación con el adyacente
ipv4 con R1 en ASN300
R2(config-router-af)#neighbor 209.165.200.225 activate // Habilita dirección del
adyacente en ipv4
R2(config-router-af)#no neighbor 2001:db8:200::1 activate// Descarta dirección del
adyacente en ipv6
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255 // ID del router
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0 // Asignación de ruta por defecto
R2(config-router-af)#exit // Salir del modo de configuración direcciones familiares
R2(config-router)#address-family ipv6 //Entrar al modo configuración direcciones
familiares ipv6
R2(config-router-af)#neighbor 2001:db8:200::1 activate // Encendido de
direcciones familiares
R2(config-router-af)#network 2001:db8:2222::/128 // Dirección de la red loopback
R2(config-router-af)#network ::/0 // Asignación de ruta por defecto
R2(config-router-af)#exit-address-family // salir del modo de configuración de
direcciones familiares
R2(config-router)#end // Finalizar configuración

```

Figura 27. Código de enrutamiento implementado en GNS3 R2

```

R2#config term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#no bgp default ipv4-unicast
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4 unicast
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0
R2(config-router-af)#exit
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#end
R2#

```


Figura 28. Verificación sección BGP R2

```
R2#show run | section router bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network ::/0
    network 2001:DB8:2222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
R2#
```

Router R3

R3(config)#router ospf 4 // Habilitar medio ospf en proceso 4

R3(config-router)# router-id 0.0.4.3 // Nombre del router ID ospf

R3(config-router)# network 10.0.11.0 0.0.0.255 área 0 // Asignación de la ruta del área 0

R3(config-router)# network 10.0.13.0 0.0.0.255 área 0 // Asignación de la ruta del área 0

R3(config-router)# exit // salir del modo configuración router

R3(config)#ipv6 router ospf 6 // Habilitar el ospf en el proceso 6

R3(config-rtr)# router-id 0.0.6.3 3 // Nombre del router ID ospf

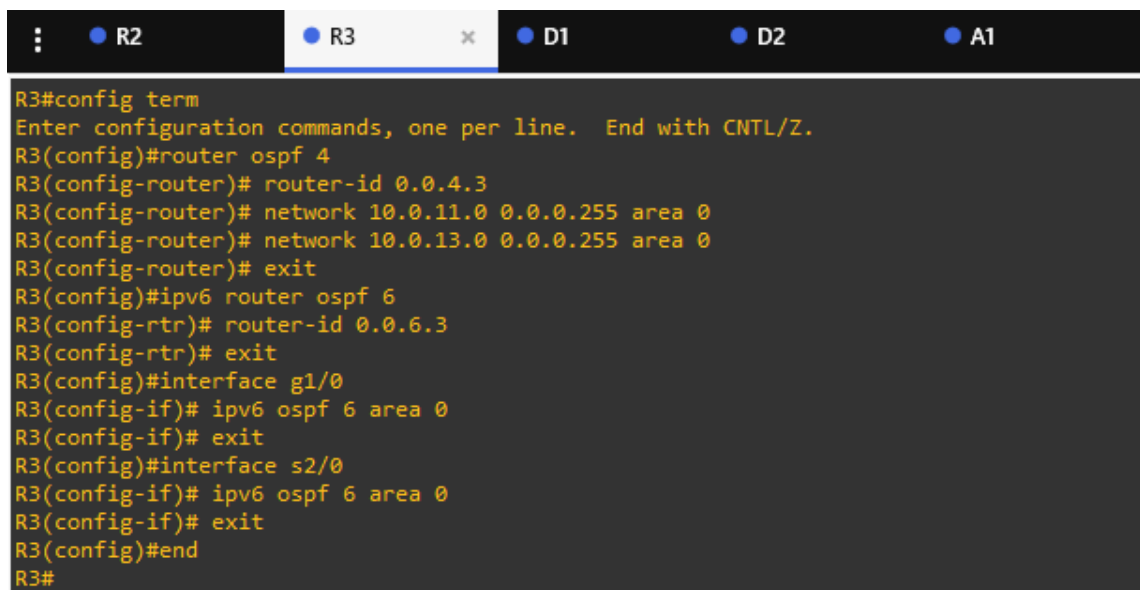
R3(config-rtr)# exit // salir del modo configuración router

R3(config)#interface g1/0 // configuración en modo interface ethernet

R3(config-if)# ipv6 ospf 6 área 0 // enciende el ospf en proceso 6 área 0 publicando rutas

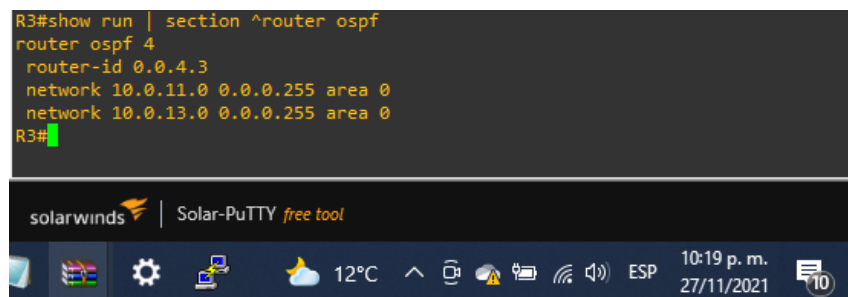
```
R3(config-if)# exit // salir del modo de configuración interface ethernet
R3(config)#interface s2/0 // configuración en modo interface s2/0
R3(config-if)# ipv6 ospf 6 área 0 // enciende el ospf en proceso 6 área 0
publicando rutas
R3(config-if)# exit // salir del modo de configuración interface
R3(config)#end // finalizar configuración
```

Figura 29. Código de enrutamiento implementado en GNS3 R3



```
R3#config term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 4
R3(config-router)# router-id 0.0.4.3
R3(config-router)# network 10.0.11.0 0.0.0.255 area 0
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0
R3(config-router)# exit
R3(config)#ipv6 router ospf 6
R3(config-rtr)# router-id 0.0.6.3
R3(config-rtr)# exit
R3(config)#interface g1/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#interface s2/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#end
R3#
```

Figura 30. Verificación router ospf R3



```
R3#show run | section ^router ospf
router 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
R3#
```

Figura 31. Verificación ipv6 router R3

```
R3# show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface      PID  Area      Intf ID   Cost  State Nbrs F/C
Se2/0          6   0         6         64   P2P   1/1
Gi1/0          6   0         5          1   BDR   1/1
R3#
```

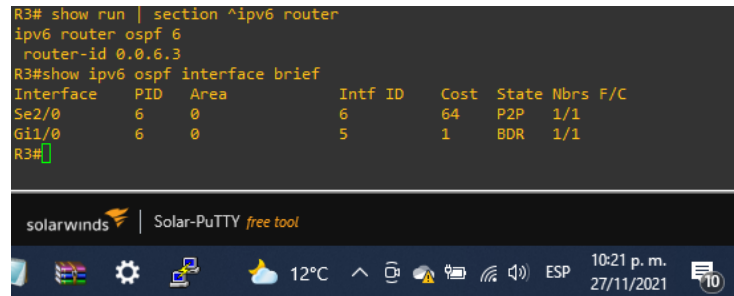


Figura 32. Verificacion ipv4 R3

```
R3#show ip route ospf | begin Gateway
Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 00:52:38, Serial2/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O      10.0.10.0/24 [110/65] via 10.0.13.1, 00:52:38, Serial2/0
O      10.0.100.0/24 [110/2] via 10.0.11.2, 00:52:33, GigabitEthernet1/0
O      10.0.101.0/24 [110/2] via 10.0.11.2, 00:52:33, GigabitEthernet1/0
O      10.0.102.0/24 [110/2] via 10.0.11.2, 00:52:33, GigabitEthernet1/0
R3#
```

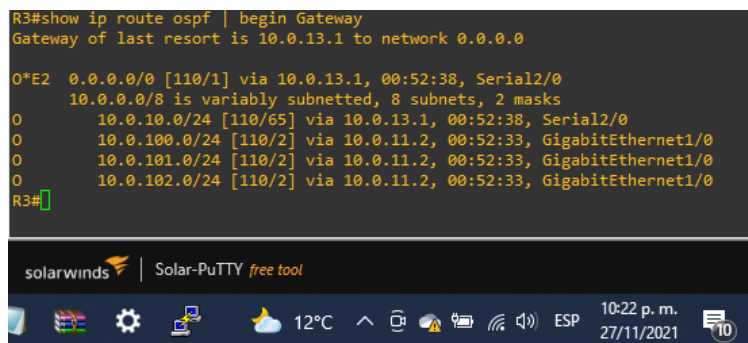
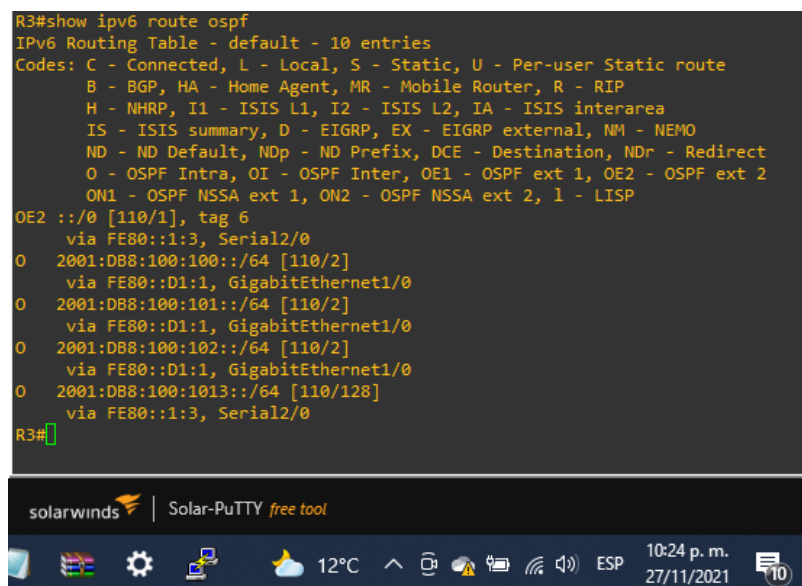


Figura 33. OSPFv3 para IPv6

```
R3#show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - IISP
OE2 ::/0 [110/1], tag 6
      via FE80::1:3, Serial2/0
O  2001:DB8:100:100::/64 [110/2]
      via FE80::D1:1, GigabitEthernet1/0
O  2001:DB8:100:101::/64 [110/2]
      via FE80::D1:1, GigabitEthernet1/0
O  2001:DB8:100:102::/64 [110/2]
      via FE80::D1:1, GigabitEthernet1/0
O  2001:DB8:100:1013::/64 [110/128]
      via FE80::1:3, Serial2/0
R3#
```



Switch D1

```
D1(config)#router ospf 4 // Habilitar medio ospf en proceso 4
```

```
D1(config-router)# router-id 0.0.4.131 Habilitar ruta ospf en proceso 4
```

```
D1(config-router)# network 10.0.100.0 0.0.0.255 área 0 // Habilitar red de la ruta del área 0
```

```
D1(config-router)# network 10.0.101.0 0.0.0.255 área 0 // Habilitar red de la ruta del área 0
```

```
D1(config-router)# network 10.0.102.0 0.0.0.255 área 0 // Habilitar red de la ruta del área 0
```

```
D1(config-router)# network 10.0.10.0 0.0.0.255 área 0 // Habilitar red de la ruta del área 0
```

```
D1(config-router)# passive-interface default // Apagar las publicaciones ospfv2
```

```
D1(config-router)# no passive-interface e1/0 // No apagar publicaciones interface
```

```
D1(config-router)# exit // salir del modo de configuración router
```

```
D1(config)#ipv6 router ospf 6 // Habilitar red de la ruta del ospf en proceso 6
```

```
D1(config-rtr)# router-id 0.0.6.131 // Habilitar red de la ruta del ospf en proceso 6
```

```
D1(config-rtr)# passive-interface default // Apagar las publicaciones ospfv3
```

```
D1(config-rtr)# no passive-interface e1/0 // No apagar publicaciones interface
```

```
D1(config-rtr)# exit // salir del modo de configuración router
```

```
D1(config)#interface e1/0 //Modo de configuración interface ethernet
```

```
D1(config-if)# ipv6 ospf 6 área 0 // Habilitar red de la ruta del ospf en proceso 6
```

```
D1(config-if)# exit // salir del modo de configuración router
```

```
D1(config)#interface vlan 100 //Modo de configuración interface VLAN
```

```
D1(config-if)# ipv6 ospf 6 área 0 // Habilitar red de la ruta del ospf en proceso 6
```

```
D1(config-if)# exit // salir del modo de configuración interface VLAN
```

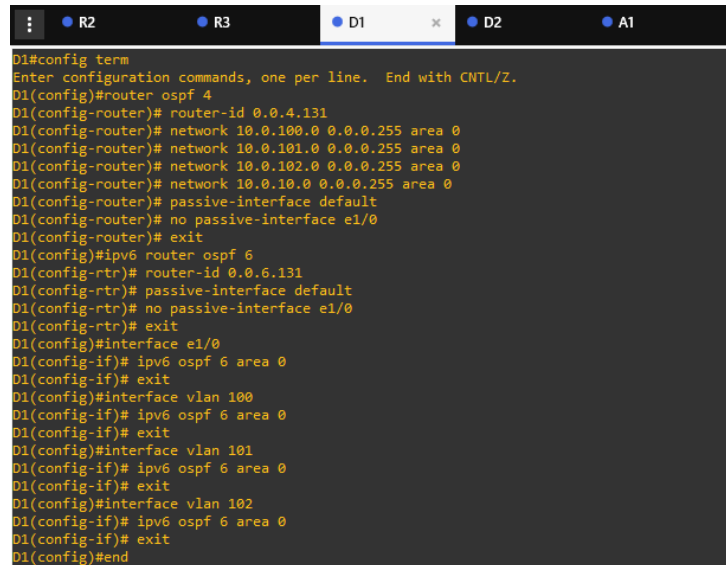
```
D1(config)#interface vlan 101 //Modo de configuración interface VLAN
```

```

D1(config-if)# ipv6 ospf 6 área 0 // Habilitar red de la ruta del ospf en proceso 6
D1(config-if)# exit // salir del modo de configuración interface VLAN
D1(config)#interface vlan 102 //Modo de configuración interface VLAN
D1(config-if)# ipv6 ospf 6 área 0 // Habilitar red de la ruta del ospf en proceso 6
D1(config-if)# exit // salir del modo de configuración interface VLAN
D1(config)#end // Finalizar configuración

```

Figura 34. Código de enrutamiento implementado en GNS3 D1

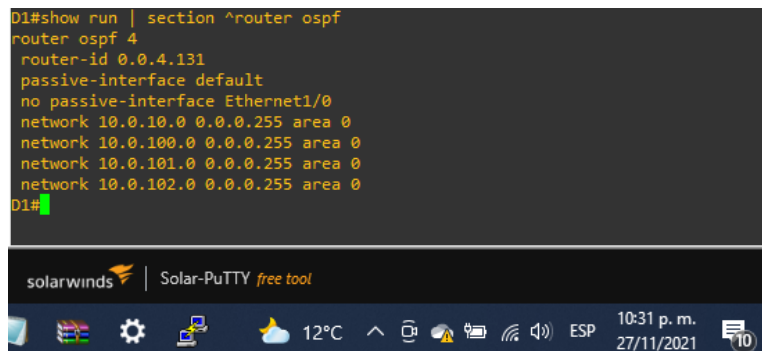


```

D1#config term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
D1(config-router)# network 10.0.100.0 0.0.0.255 area 0
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0
D1(config-router)# passive-interface default
D1(config-router)# no passive-interface e1/0
D1(config-router)# exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)# router-id 0.0.6.131
D1(config-rtr)# passive-interface default
D1(config-rtr)# no passive-interface e1/0
D1(config-rtr)# exit
D1(config)#interface e1/0
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 100
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 101
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#end

```

Figura 35. Verificación router ospf D1



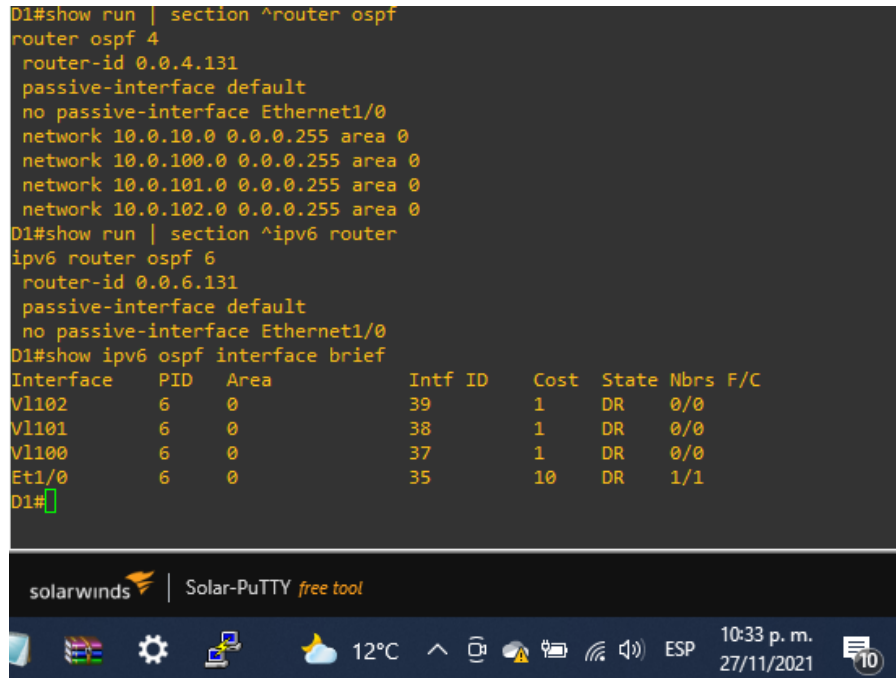
```

D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/0
network 10.0.10.0 0.0.0.255 area 0
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
D1#

```

Figura 36. Verificación interfaz ipv6 ospf

```
D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/0
network 10.0.10.0 0.0.0.255 area 0
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
D1#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet1/0
D1#show ipv6 ospf interface brief
Interface      PID  Area      Intf ID  Cost  State  Nbrs F/C
Vl102          6    0         39       1    DR    0/0
Vl101          6    0         38       1    DR    0/0
Vl100          6    0         37       1    DR    0/0
Et1/0          6    0         35      10    DR    1/1
D1#
```



Las descripciones de los comandos o líneas aplican para D2.

Switch D2

```
D2(config)#router ospf 4
```

```
D2(config-router)# router-id 0.0.4.132
```

```
D2(config-router)# network 10.0.100.0 0.0.0.255 área 0
```

```
D2(config-router)# network 10.0.101.0 0.0.0.255 área 0
```

```
D2(config-router)# network 10.0.102.0 0.0.0.255 área 0
```

```
D2(config-router)# network 10.0.11.0 0.0.0.255 área 0
```

```
D2(config-router)# passive-interface default
```

```
D2(config-router)# no passive-interface e1/0
```

```
D2(config-router)# exit
```

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)# router-id 0.0.6.132
D2(config-rtr)# passive-interface default
D2(config-rtr)# no passive-interface e1/0
D2(config-rtr)# exit
D2(config)#interface e1/0
D2(config-if)# ipv6 ospf 6 área 0
D2(config-if)# exit
D2(config)# interface vlan 100
D2(config-if)# ipv6 ospf 6 área 0
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# ipv6 ospf 6 área 0
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# ipv6 ospf 6 área 0
D2(config-if)# exit
D2(config)# end
```

Figura 37. Código de enrutamiento implementado en GNS3 D2

```
D2#config term
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
D2(config-router)# network 10.0.100.0 0.0.0.255 area 0
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface e1/0
D2(config-router)# exit
D2(config)#ipv6 router ospf 6
D2(config-rtr)# router-id 0.0.6.132
D2(config-rtr)# passive-interface default
D2(config-rtr)# no passive-interface e1/0
D2(config-rtr)# exit
D2(config)#interface e1/0
D2(config-if)# ipv6 ospf 6 area 0
D2(config-if)# exit
D2(config)# interface vlan 100
D2(config-if)# ipv6 ospf 6 area 0
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# ipv6 ospf 6 area 0
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# ipv6 ospf 6 area 0
D2(config-if)# exit
D2(config)#
```

Figura 38. Verificación router ospf D1

```
D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
network 10.0.11.0 0.0.0.255 area 0
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
D2#
```

Figura 39. Verificación interfaz ipv6 ospf

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface Ethernet1/0
D2#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
Vl102     6   0     39       1    DR    0/0
Vl101     6   0     38       1    DR    0/0
Vl100     6   0     37       1    DR    0/0
Et1/0     6   0     35      10    DR    1/1
D2#
```


Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

Tabla 4. Ajuste de redundancia First Hop Redundancy

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. Programe 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</p>

		<p>G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. 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>
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</p>

		<p>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.
	<p>En D2, configure HSRPv2</p>	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. 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 e
--	--	--

Switch D1

```

D1(config)#ip sla 4 // Se genera SLA número 4 para ipv4
D1(config-ip-sla)# icmp-echo 10.0.10.1 // Verificación de conectividad
D1(config-ip-sla-echo)# frequency 5 // Verificación de disponibilidad cada 5 s
D1(config-ip-sla-echo)# exit // salir de modo de configuración SLA 4
D1(config)#ip sla 6 // Se genera SLA número 6 para ipv6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1 // Verificación de
conectividad
D1(config-ip-sla-echo)# frequency 5 // Verificación de disponibilidad cada 5s
D1(config-ip-sla-echo)# exit // salir de modo de configuración SLA 6
D1(config)#ip sla schedule 4 life forever start-time now // ip SLA objeto para
SLA 4
D1(config)#ip sla schedule 6 life forever start-time now // ip SLA objeto para
SLA 6
D1(config)#track 4 ip sla 4 // Número 4 de identificación de la ip SLA 4
D1(config-track)# delay down 10 up 15 // Cambio de estado de up – down cada
10s y down – up cada 15s
D1(config-track)# exit // salir de modo de configuración SLA 4
D1(config)#interface vlan 100 // Configuración modo VLAN ipv4 HSRP
D1(config-if)# standby version 2 // Configuración de HSRP version 2
D1(config-if)# standby 104 ip 10.0.100.254 // ip virtual del grupo 104
D1(config-if)# standby 104 priority 150 // Prioridad del grupo en 150
D1(config-if)# standby 104 preempt // Activación de preferencia
D1(config-if)# standby 104 track 4 decrement 60 // Rastreo de objeto

```

```
D1(config-if)# standby 106 ipv6 autoconfig // ip virtual automática
D1(config-if)# standby 106 priority 150 // Prioridad de grupo 150
D1(config-if)# standby 106 preempt // Activación de preferencia
D1(config-if)# standby 106 track 6 decrement 60 // Rastreo de objeto
D1(config-if)# exit // Salir del modo de configuración VLAN
D1(config)#interface vlan 101 // Configuración modo VLAN ipv4 HSRP
D1(config-if)# standby version 2 // Configuración de HSRP version 2
D1(config-if)# standby 114 ip 10.0.101.254 // ip virtual del grupo 114
D1(config-if)# standby 114 preempt // Activación de preferencia
D1(config-if)# standby 114 track 4 decrement 60 // Rastreo de objeto
D1(config-if)# standby 116 ipv6 autoconfig // ip virtual automática
D1(config-if)# standby 116 preempt // Activación de preferencia
D1(config-if)# standby 116 track 6 decrement 60 // Rastreo de objeto
D1(config-if)# exit // Salir del modo de configuración VLAN
D1(config)#interface vlan 102 // Configuración modo VLAN ipv4 HSRP
D1(config-if)# standby version 2 // Configuración de HSRP version 2
D1(config-if)# standby 124 ip 10.0.102.254 // ip virtual del grupo 124
D1(config-if)# standby 124 priority 150 // Activación de prioridad
D1(config-if)# standby 124 preempt // Activación de preferencia
D1(config-if)# standby 124 track 4 decrement 60 // Rastreo de objeto
D1(config-if)# standby 126 ipv6 autoconfig // ip virtual automática
D1(config-if)# standby 126 priority 150 // Activación de prioridad
D1(config-if)# standby 126 preempt // Activación de preferencia
D1(config-if)# standby 126 track 6 decrement 60 // Rastreo de objeto
D1(config-if)# exit // Salir del modo de configuración VLAN
D1(config)#end // Finalizar configuración
```

Figura 40. Código de redundancia implementado en GNS3 D1

```
D1#config term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)#ip sla 6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#track 4 ip sla 4
D1(config-track)# delay down 10 up 15
D1(config-track)# exit
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 104 track 4 decrement 60
D1(config-if)# standby 106 ipv6 autoconfig
D1(config-if)# standby 106 priority 150
D1(config-if)# standby 106 preempt
D1(config-if)# standby 106 track 6 decrement 60
D1(config-if)# exit
D1(config)#interface vlan 101
D1(config-if)# standby version 2
D1(config-if)# standby 114 ip 10.0.101.254
D1(config-if)# standby 114 preempt
D1(config-if)# standby 114 track 4 decrement 60
D1(config-if)# standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track 6 decrement 60
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# standby version 2
D1(config-if)# standby 124 ip 10.0.102.254
D1(config-if)# standby 124 priority 150
D1(config-if)# standby 124 preempt
D1(config-if)# standby 124 track 4 decrement 60
D1(config-if)# standby 126 ipv6 autoconfig
```

Figura 41. Verificación de ip SLA D1

```
D1#show run | section ip sla
track 4 ip sla 4
  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
D1#
```

solarwinds | Solar-PuTTY free tool

11:31 p. m. 27/11/2021

Figura 42. Verificación de las VLAN en cada grupo D1

```
D1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P  State  Active        Standby        Virtual IP
Vl100     104  150  P  Active  local         10.0.100.2    10.0.100.254
Vl100     106  150  P  Active  local         FE80::D2:2    FE80::5:73FF:FEA0:6A
Vl101     114  100  P  Standby 10.0.101.2    local         10.0.101.254
Vl101     116  100  P  Standby FE80::D2:3    local         FE80::5:73FF:FEA0:74
Vl102     124  150  P  Active  local         10.0.102.2    10.0.102.254
Vl102     126  150  P  Active  local         FE80::D2:4    FE80::5:73FF:FEA0:7E
D1#
```

Las descripciones de los comandos o líneas aplican para D2.

Switch D2

```
D2(config)#ip sla 4
```

```
D2(config-ip-sla)# icmp-echo 10.0.11.1
```

```
D2(config-ip-sla-echo)# frequency 5
```

```
D2(config-ip-sla-echo)# exit
```

```
D2(config)#ip sla 6
```

```
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1
```

```
D2(config-ip-sla-echo)# frequency 5
```

```
D2(config-ip-sla-echo)# exit
```

```
D2(config)#ip sla schedule 4 life forever start-time now
```

```
D2(config)#ip sla schedule 6 life forever start-time now
```

```
D2(config)#track 4 ip sla 4
```

```
D2(config-track)# delay down 10 up 15
```

```
D2(config-track)# exit
```

```
D2(config)#interface vlan 100
```

```
D2(config-if)# standby version 2
```

```
D2(config-if)# standby 104 ip 10.0.100.254
```



```
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)# standby 114 track 4 decrement 60
D2(config-if)# standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 124 track 4 decrement 60
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
D2(config-if)# exit
D2(config)#end
```

Figura 43. Código de redundancia implementado en GNS3 D2

```
D1 D2 A1
D2(config-if)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)# exit
D2(config)#ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)# exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)# standby 114 track 4 decrement 60
D2(config-if)# standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 124 track 4 decrement 60
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
D2(config-if)# exit
```

Figura 44. Verificación de ip SLA D1

```
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.11.1
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
D2#
```

solarwinds | Solar-PuTTY free tool © 20

12°C 11:37 p. m. 27/11/2021

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. Condiciones de seguridad

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.	Especificaciones del servidor RADIUS.: <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: \$strongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none">• Use la lista de métodos por defecto• Valide contra el grupo de servidores RADIUS

		<ul style="list-style-type: none"> • 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.

Router R1

R1(config)#enable algorithm-type scrypt secret cisco12345cisco // Activación del algoritmo

R1(config)#username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco // Definición de Usuario y contraseña

R1(config)#aaa new-mode // Activación de Auditoria, Autenticación y Autorización

R1(config)#radius server RADIUS // Acceso a la interfaz RADIUS

R1(config-radius-server)#v4 10.0.100.6 auth-port 1812 acct-port 1813 // Habilita ip del servidor RADIUS

R1(config-radius-server)# key \$trongPass // Se establece la contraseña

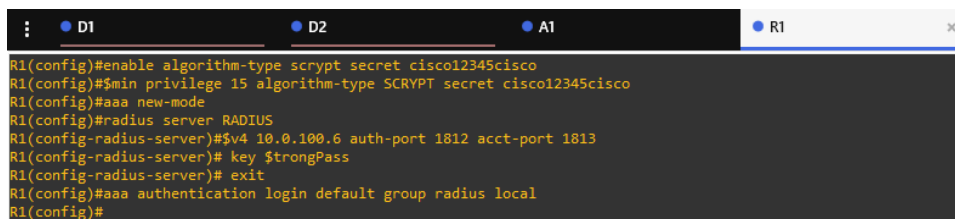
R1(config-radius-server)# exit // Salir del modo configuración interfaz RADIUS

R1(config)#aaa authentication login default group radius local // Autenticación

R1(config)#end // Finaliza configuración

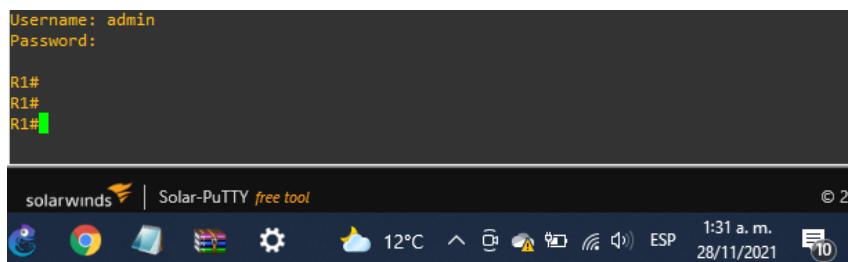
Las descripciones de los comandos o líneas aplican para R2, R3, D1, D2 y A1.

Figura 45. Código de seguridad implementado en GNS3 R1



```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
R1(config)#$min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R1(config)#aaa new-mode
R1(config)#radius server RADIUS
R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# exit
R1(config)#aaa authentication login default group radius local
R1(config)#
```

Figura 46. Verificación de seguridad R1



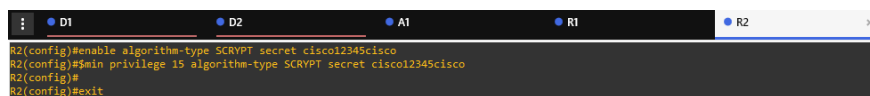
```
Username: admin
Password:

R1#
R1#
R1#
```

Router R2

```
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R2(config)#end
```

Figura 47. Código de seguridad implementado en GNS3 R2



```
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R2(config)#$min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R2(config)#
R2(config)#exit
```

Router R3

```
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#aaa new-model
```

```

R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $strongPass
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#end

```

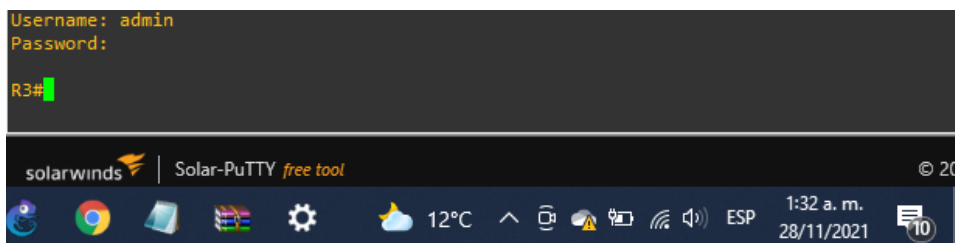
Figura 48. Código de seguridad implementado en GNS3 R3

```

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)#$min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $strongPass
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#exit

```

Figura 49. Verificación de seguridad R3



Switch D1

```

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $strongPass

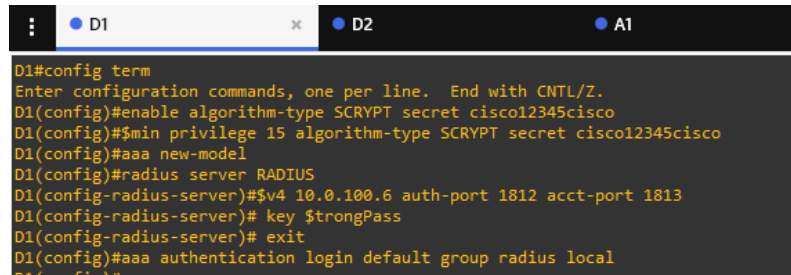
```

```
D1(config-radius-server)# exit
```

```
D1(config)#aaa authentication login default group radius local
```

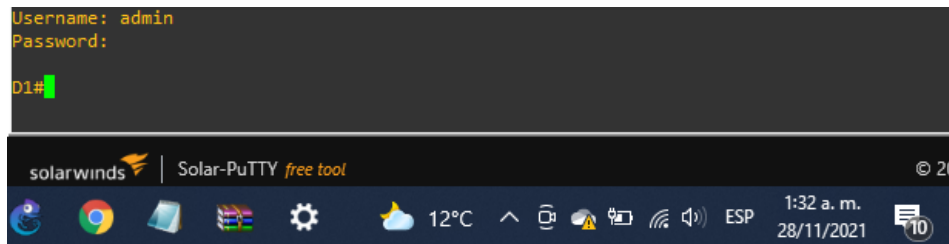
```
D1(config)#end
```

Figura 50. Código de seguridad implementado en GNS3 D1



```
D1#config term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#$min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $strongPass
D1(config-radius-server)# exit
D1(config)#aaa authentication login default group radius local
D1(config)#
```

Figura 51. Verificación de seguridad D1



```
Username: admin
Password:
D1#
```

solarwinds | Solar-PuTTY free tool © 20

12°C 1:32 a. m. 28/11/2021

Switch D2

```
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
```

```
D2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
D2(config)#aaa new-model
```

```
D2(config)#radius server RADIUS
```

```
D2(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
```

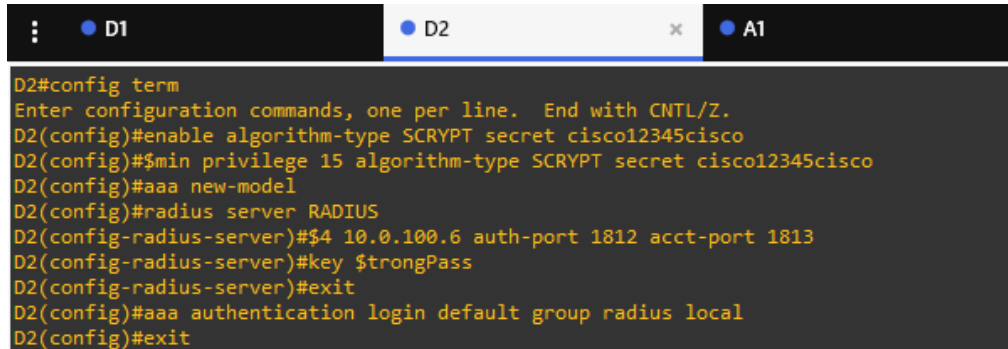
```
D2(config-radius-server)#key $strongPass
```

```
D2(config-radius-server)#exit
```

```
D2(config)#aaa authentication login default group radius local
```

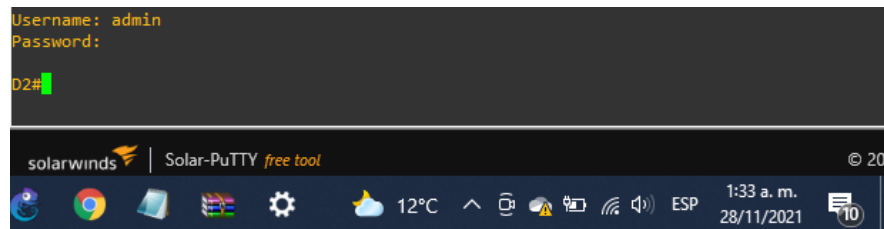
```
D2(config)#end
```

Figura 52. Código de seguridad implementado en GNS3 D2



```
D2#config term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D2(config)#$min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $trongPass
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local
D2(config)#exit
```

Figura 53. Verificación de seguridad D2



```
Username: admin
Password:
D2#
```

Switch A1

```
A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#end
```


Figura 54. Código de seguridad implementado en GNS3 D2

```

A1#config term
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
A1(config)#min privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#exit
A1#
  
```

Figura 55. Verificación de seguridad A1

```

Username: admin
Password:
A1#
  
```

Parte 6: Configure las funciones de Administración de Red.

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tabla 6. Administración de red

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.

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). • Límite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el community string en ENCORSA. • En R3, D1, y D2, habilite el envío de traps config y ospf. • En R1, habilite el envío de traps bgp, config, y ospf. • En A1, habilite el envío de traps config

Router R1

R1(config)#clock timezone UTC -5 // Reloj local hora UTC

R1(config)#ntp server 209.165.200.226 // Se habilita NTP para sincronizar con R2

R1(config)#logging host 10.0.100.5 // Se activa Syslog para PC1

R1(config)#logging trap warnings // Se configura nivel de Syslog

R1(config)#snmp-server community ENCORSA RO // Se establece comunidad

R1(config)#snmp-server host 10.0.100.5 ENCORSA // Acceso SNMP

R1(config)#snmp-server contact DAVID GUTIERREZ // S establece valor de contacto

R1(config)#snmp-server enable traps bgp // Activa mensajes de cambio de estado del portocolo

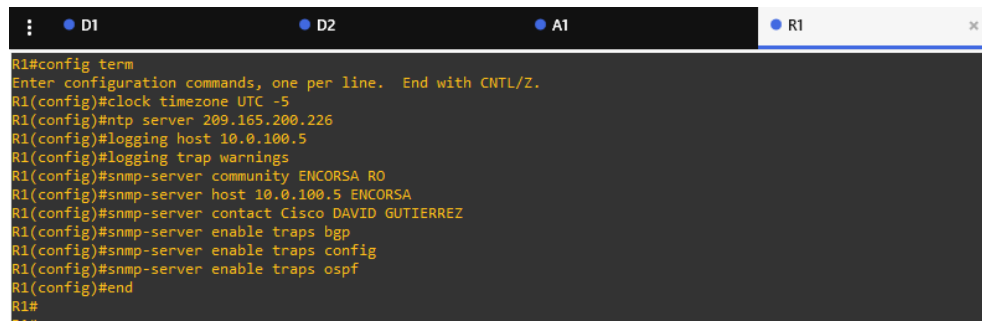
R1(config)#snmp-server enable traps config // Activa mensajes de configuración

R1(config)#snmp-server enable traps ospf Activa mensajes de cambio de estado del portocolo

R1(config)#end // Finaliza la configuración

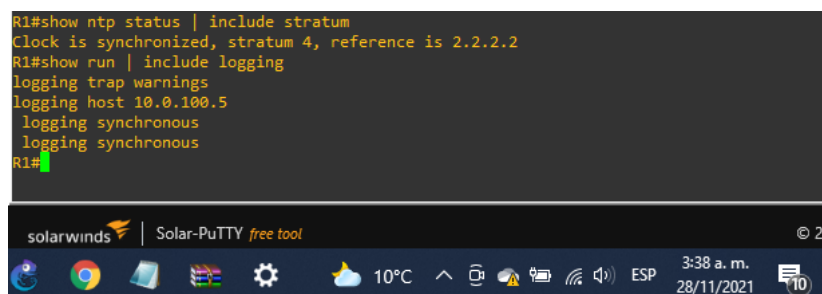
Las descripciones de los comandos o líneas aplican para R3.

Figura 56. Código de administración de red implementado en GNS3 R1



```
R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#clock timezone UTC -5
R1(config)#ntp server 209.165.200.226
R1(config)#logging host 10.0.100.5
R1(config)#logging trap warnings
R1(config)#snmp-server community ENCORSA RO
R1(config)#snmp-server host 10.0.100.5 ENCORSA
R1(config)#snmp-server contact Cisco DAVID GUTIERREZ
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#end
R1#
```

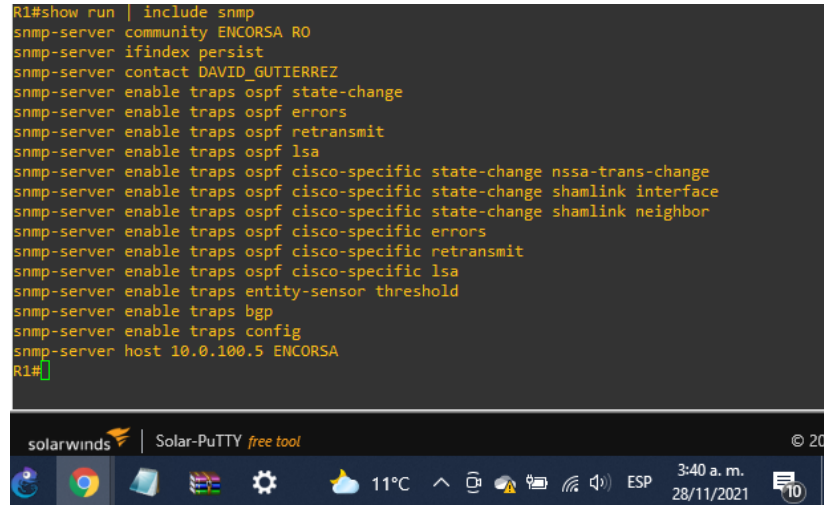
Figura 57. Verificación de los ajustes NTP R1



```
R1#show ntp status | include stratum
Clock is synchronized, stratum 4, reference is 2.2.2.2
R1#show run | include logging
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
R1#
```

Figura 58. Verificación de los ajustes SNMP R1

```
R1#show run | include snmp
snmp-server community ENCORSA RO
snmp-server ifindex persist
snmp-server contact DAVID_GUTIERREZ
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 entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 ENCORSA
R1#
```



Router R2

R2(config)#clock timezone UTC -5 // Reloj local hora UTC

R2(config)#ntp master 3 // Activación como NTP maestro

R2(config)#end // Finaliza la configuración

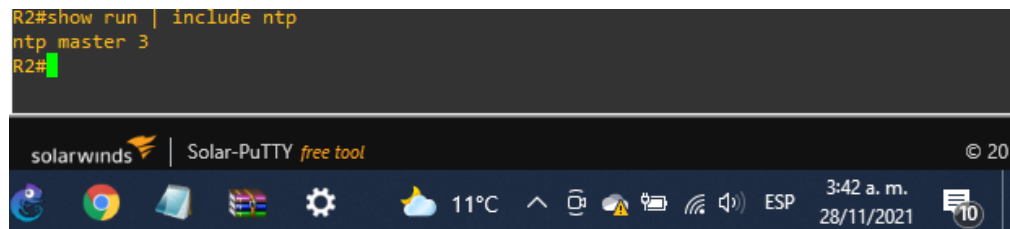
Figura 59. Código de administración de red implementado en GNS3 R2

```
R2#config term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#clock timezone UTC -5
R2(config)#ntp master 3
R2(config)#end
```



Figura 60. Verificación de los ajustes NTP R2

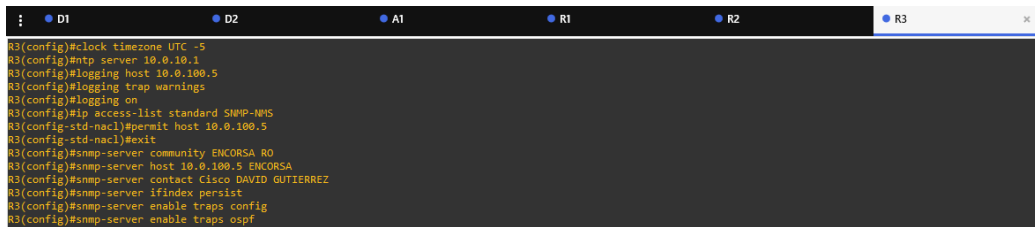
```
R2#show run | include ntp
ntp master 3
R2#
```



Router R3

```
R3(config)#ntp server 10.0.10.1
R3(config)#logging host 10.0.100.5
R3(config)#logging trap warnings
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config)#snmp-server community ENCORSA RO
R3(config)#snmp-server host 10.0.100.5 ENCORSA
R3(config)#snmp-server contact Cisco DAVID GUTIERREZ
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#exit
```

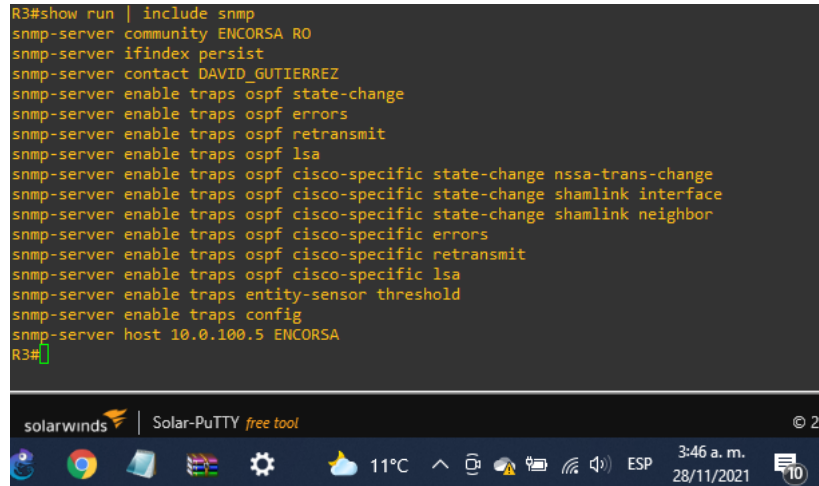
Figura 61. Código de administración de red implementado en GNS3 R3



```
R3(config)#clock timezone UTC -5
R3(config)#ntp server 10.0.10.1
R3(config)#logging host 10.0.100.5
R3(config)#logging trap warnings
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config)#snmp-server community ENCORSA RO
R3(config)#snmp-server host 10.0.100.5 ENCORSA
R3(config)#snmp-server contact Cisco DAVID GUTIERREZ
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
```

Figura 62. Verificación de los ajustes SNMP R3

```
R3#show run | include snmp
snmp-server community ENCORSA RO
snmp-server ifindex persist
snmp-server contact DAVID_GUTIERREZ
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 entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 ENCORSA
R3#
```



Switch D1

D1(config)#clock timezone UTC -5 // Reloj local hora UTC

D1(config)#ntp server 10.0.10.1 // Se habilita NTP para sincronizar con R1

D1(config)#logging trap warning // Se configura nivel de Syslog

D1(config)#logging host 10.0.100.5 // Se activa Syslog para PC1

D1(config)#logging on // Activa configuración

D1(config)#ip access-list standard SNMP-NMS // Modo configuración *SNMPv2c*

D1(config-std-nacl)#permit host 10.0.100.5 // Restringe acceso SNMP

D1(config-std-nacl)#exit // Salir del modo de configuración *SNMPv2c*

D1(config)#snmp-server contact Cisco DAVID GUTIERREZ // Configura valor contacto Nombre

D1(config)#snmp-server community ENCORSA ro SNMP-NMS // Se establece comunidad

D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA // Acceso SNMP

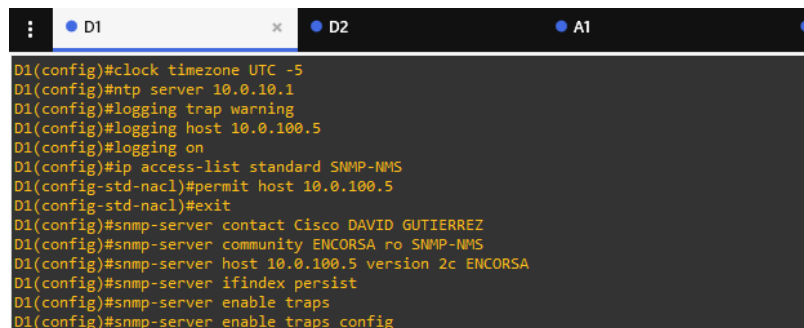
D1(config)#snmp-server ifindex persist // Identifica cada interfaz SNMP

D1(config)#snmp-server enable traps // Activa mensajes de cambio de estado del protocolo

D1(config)#snmp-server enable traps ospf // Activa mensajes OSPF

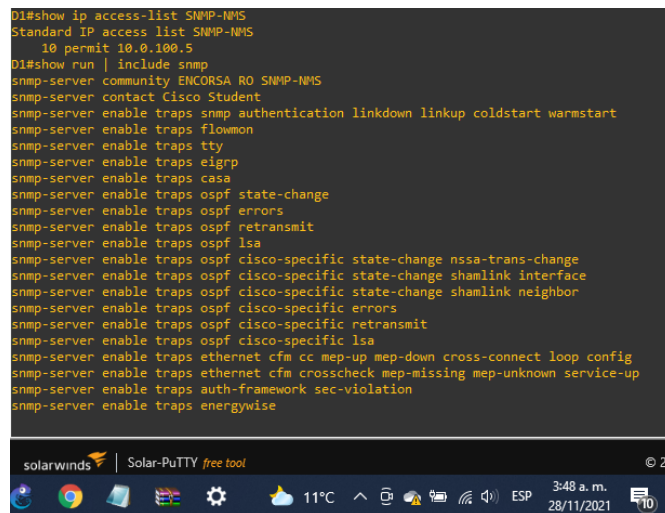
D1(config)#end // Finalizar configuración

Figura 63. Código de administración de red implementado en GNS3 D1



```
D1
x
A1
D1(config)#clock timezone UTC -5
D1(config)#ntp server 10.0.10.1
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco DAVID GUTIERREZ
D1(config)#snmp-server community ENCORSAS ro SNMP-NMS
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSAS
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps
D1(config)#snmp-server enable traps config
```

Figura 64. Verificación de los ajustes SNMP D1



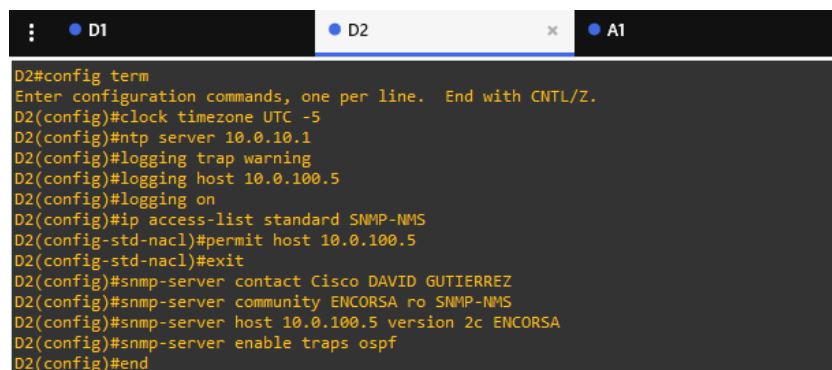
```
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D1#show run | include snmp
snmp-server community ENCORSAS RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
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 ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
```

Las descripciones de los comandos o líneas aplican para D2 y A1.

Switch D2

```
D2(config)#clock timezone UTC -5
D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#exit
D2(config)#snmp-server contact Cisco DAVID GUTIERREZ
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server enable traps ospf
D2(config)#end
```

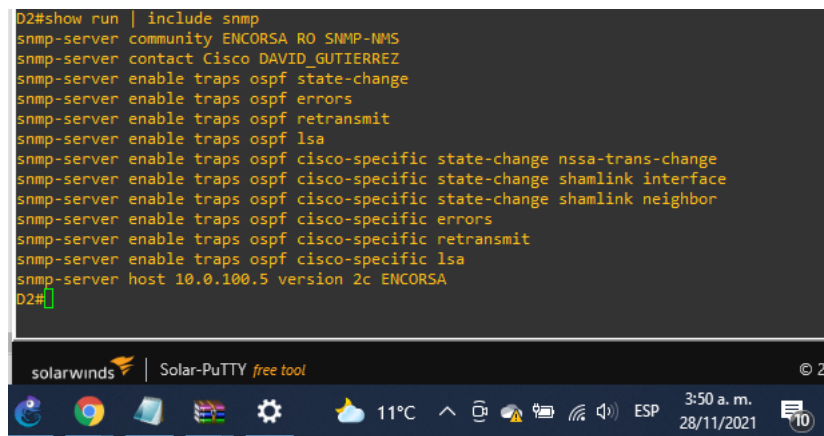
Figura 65. Código de administración de red implementado en GNS3 D2



```
D1 D2 A1
D2#config term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#clock timezone UTC -5
D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#exit
D2(config)#snmp-server contact Cisco DAVID GUTIERREZ
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server enable traps ospf
D2(config)#end
```


Figura 66. Verificación de los ajustes SNMP D2

```
D2#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco DAVID_GUTIERREZ
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
D2#
```



Switch A1

```
A1(config)#clock timezone UTC -5
```

```
A1(config)#ntp server 10.0.10.1
```

```
A1(config)#logging trap warning
```

```
A1(config)#logging host 10.0.100.5
```

```
A1(config)#logging on
```

```
A1(config)#ip access-list standard SNMP-NMS
```

```
A1(config-std-nacl)#permit host 10.0.100.5
```

```
A1(config-std-nacl)#exit
```

```
A1(config)#snmp-server contact Cisco DAVID GUTIERREZ
```

```
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
```

```
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
```

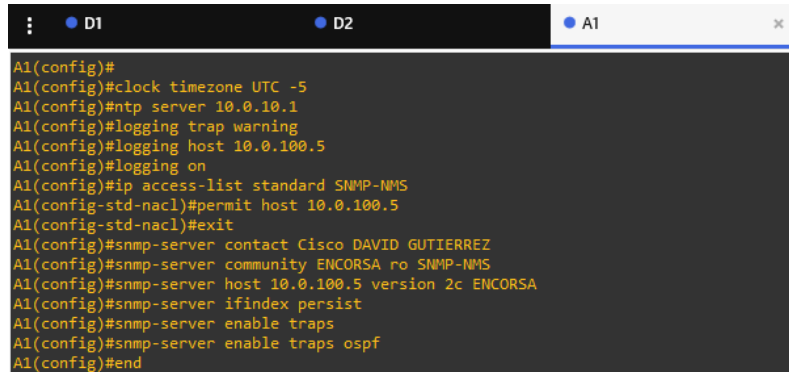
```
A1(config)#snmp-server ifindex persist
```

```
A1(config)#snmp-server enable traps
```

```
A1(config)#snmp-server enable traps ospf
```

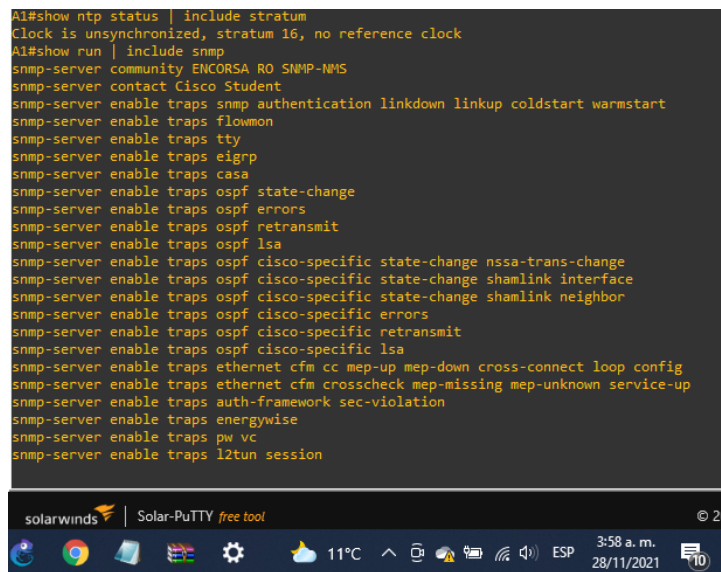
```
A1(config)#end
```

Figura 67. Código de administración de red implementado en GNS3 A1



```
A1(config)#
A1(config)#clock timezone UTC -5
A1(config)#ntp server 10.0.10.1
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)#logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco DAVID GUTIERREZ
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server ifindex persist
A1(config)#snmp-server enable traps
A1(config)#snmp-server enable traps ospf
A1(config)#end
```

Figura 68. Verificación de los ajustes SNMP A1



```
A1#show ntp status | include stratum
Clock is unsynchronized, stratum 16, no reference clock
A1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
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 ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
```

CONCLUSIONES

El desarrollo del ejercicio mediante la simulación del software GNS3, muestra un entorno real en el cual cada dispositivo seleccionado debe soportar los protocolos que generan confiabilidad en la implementación de la red a su vez nos demuestra el detalle que se debe tener en cuanto a características como capacidad de memoria, tipos de puertos, protocolos etcétera para la necesidad del caso.

Los protocolos implementados en la etapa de enrutamiento son útiles para cualquier tipo de topología ya que el OSPF enruta de manera interna y mantiene el estado de la topología y se si afecta la actualiza automáticamente, sin embargo, para la implementación de este protocolo fue necesario habilitar las interfaces troncales (switchport trunk encapsulation dot1q), y el comando ipv6 unicast-routing con el propósito de actualizar las tablas de enrutamiento.

El escenario propuesto muestra redundancia ante la caída de un canal, a través de sus conexiones físicas, con la implementación de los canales lógicos los cuales resisten altas velocidades, se conservan constantes ante la oscilación de cargas y redireccionan el tráfico dependiendo del canal, se logra mantener la red estable y se optimizan al máximo los medios físicos y tecnológicos, siempre y cuando se ajuste el EthernetChannel de manera correcta.

Los comandos de seguridad del escenario demuestran la importancia de proteger las redes el protocolo implementado demuestra que se requiere una autorización, una autenticación y una auditoria; autorización cuando se solicita el usuario, autenticación a través de la contraseña y auditoria simplemente registra el acceso del usuario, supervisa los cambios y establece el tiempo de la conexión, esta configuración es simple ya que solo se debe definir el usuario y la contraseña ya que los comandos se encuentra predefinidos en su algoritmo.

BIBLIOGRAFÍA

ARIGANELLO, Ernesto. "Redes Cisco CCNP a fondo". (En línea). (13 septiembre de 2021) {En línea} {02 septiembre de 2021} Disponible en: (<https://books.google.com.co/books?id=ZofDwAAQBAJ&lpg=PA796&dq=importancia%20del%20ccnp%20cisco&pg=PP1#v=onepage&q&f=false>). Obtenido de Con qué elementos se desarrolla el CCNP en la ingeniería de redes: (<https://formatalent.com/con-que-elementos-se-desarrolla-elccnp-en-la-ingenieria-de-redes/>)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCOR 350-401. {En línea} {11 septiembre de 2021} Disponible en: (<https://1drv.ms/b/s!AAIGg5JUgUBthk8>)

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. {En línea} {25 noviembre de 2021} Disponible en: (<https://1drv.ms/b/s!AmIJYeINT1IlnWR0hoMxgBNv1CJ>)

ROMERO, Christian. "Establecer IOU L2 e IOU L3 en GNS3". {En línea}. {20 noviembre de 2021} disponible en: (www.youtube.com/watch?v=ZXfseiLKIgl)

The bryantadvantage.com. (2017). CCNP SWITCH Tutorial: EtherChannel Fundamentals. {En línea} {10 octubre de 2021} Disponible en: (<https://www.thebryantadvantage.com/videos-andtutorials/ccnp-switch-tshoot-tutorials/etherchannel-fundamentals/>)