

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**LINA MARÍA MEDINA VÉLEZ**

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**LINA MARÍA MEDINA VÉLEZ**

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

PITALITO HUILA, 29 de noviembre de 2021

## **DEDICATORIA**

Dedico este trabajo a Dios porque su guía y sabiduría fue nuestra principal herramienta para su desarrollo, a mi familia, mi hijo y todos los que me han apoyado en este proceso para obtener este gran logro.

## **AGRADECIMIENTOS**

Agradezco primeramente a Dios por permitir y darnos la oportunidad de iniciar nuestras carreras, mostrarnos y enseñarnos el camino para formarnos como grandes profesionales a lo largo del tiempo.

Gracias a padres, hijo y esposo por su motivación, atención, apoyo y ánimo que nos brindaron en el transcurso de la carrera, así como el empeño que transmitieron para finalizar el proyecto de grado. Gracias a nuestros demás familiares y seres queridos, que de una u otra forma aportaron al desarrollo de este proyecto de vida profesional.

A aquellos docentes que aportaron sus conocimientos y su tiempo durante la construcción y elaboración de este trabajo, así como a las personas participantes que contribuyeron con su tiempo, trabajo e intelecto que permitió concluir el proyecto.

## CONTENIDO

GLOSARIO .....	12
RESUMEN .....	13
ABSTRACT .....	14
INTRODUCCIÓN .....	15
DESARROLLO .....	16
Objetivos.....	18
Escenario.....	18
Recursos necesarios .....	19
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces .....	20
Paso 1: Cablear la red como se muestra en la topología. ....	20
Paso 2: Configurar los parámetros básicos para cada dispositivo. ....	21
Código hecho Router R1 .....	22
Código hecho Router R2 .....	24
Código hecho Router R3 .....	26
Código hecho Switch D1 .....	28
Codigo hecho configuración Switch D2 .....	32
Codigo hecho Switch A1.....	36
Parte 2: Configurar la capa 2 de la red y el soporte de host .....	38
Solución.....	39
Código desarrollado D1 .....	43
Código desarrollado D2 .....	44
Código desarrollado A1 .....	46
Verificaciones .....	48
Parte 3: Configurar los protocolos de enrutamiento.....	53

Desarrollo de la tarea 3.1. ....	55
Configuración en R3.....	55
Configuración en D1.....	56
Configuración en D2.....	56
Desarrollo de la tarea 3.2.....	57
Configuración en R3.....	58
Configuración en D1.....	59
Desarrollo de la tarea 3.3.....	60
Configuración en R2.....	60
Desarrollo de la tarea 3.4.....	61
Simulaciones.....	62
Código demostración del problema   sección BGP en R1.....	62
Parte 4: Configurar la redundancia del primer salto (first hop redundancy).....	69
Desarrollo de la tarea 4.1.....	71
Desarrollo de la tarea 4.2.....	73
Desarrollo de la tarea 4.3.....	75
Parte 5: Seguridad.....	76
Desarrollo de la tarea 5.1 Y 5.2.....	77
Desarrollo de la tarea 5.3 Y 5.4.....	78
Desarrollo de la tarea 5.5 y 5.6.....	81
Parte 6: Configure las funciones de administración de red.....	85
Desarrollo de la tarea 6.1, 6.2, 6.3, 6.4 y 6,5.....	86
Verificaciones.....	93
CONCLUSIONES.....	94
BIBLIOGRAFIA.....	96

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	17
Tabla 2. Código Router R1 .....	22
Tabla 3. Código Router R2 .....	24
Tabla 4. Código Router R3 .....	26
Tabla 5. Código Switch D1 .....	28
Tabla 6. Código Switch D2 .....	33
Tabla 7. Código Switch A1.....	36
Tabla 8. Configurar la capa 2 de la red y el soporte de host.....	38
Tabla 9. Código desarrollado D1 .....	43
Tabla 10. Código desarrollado D2 .....	44
Tabla 11. Código desarrollado A1.....	46
Tabla 12. Verificación con el comando show int g3/0 .....	53
Tabla 13. Configuración en R1 .....	55
Tabla 14. Configuración en R3 .....	55
Tabla 16. Configuración en D2 .....	56
Tabla 17. Configuración en R1 .....	57
Tabla 18. Configuración en R3 .....	58
Tabla 19. D1# show run   section ^ipv6 router .....	58
Tabla 20. D2# show run   section ^ipv6 router .....	59
Tabla 21. Configuración en R2 .....	60
Tabla 22. Código demostración del problema   sección bgp en r1 .....	63
Tabla 23. Código en R2 .....	64
Tabla 24. Código en R3 .....	65

Tabla 26. Código en D2 .....	68
Tabla 27. Las tareas de configuración .....	69
Tabla 28. Código en D1 .....	72
Tabla 29. Switch D2.....	73
Tabla 30. Desarrollo de la tarea 4.3.....	75
Tabla 31. Configuración de seguridad .....	76
Tabla 32. Tareas 5.3 y 5.4 .....	78
Tabla 33. Tareas 5.5 y 5.6 .....	81
Tabla 34. Configuración de funciones de administración de red .....	85
Tabla 35. Código configuración Router R2 y Router R1 .....	87
Tabla 36. Código Router R3 .....	88
Tabla 37. Switch D1 .....	89
Tabla 38. Switch D2.....	90
Tabla 39. Switch A1 .....	91

## LISTA DE FIGURAS

Figura 1. Escenario propuesto (Topología de red).....	16
Figura 2. Recursos necesarios .....	19
Figura 3. Switch Cisco 3650 .....	19
Figura 4. Switch Cisco 2960 .....	19
Figura 5. PCs.....	19
Figura 6. Los cables Ethernet.....	20
Figura 7. Cablear la red como se muestra en la topología .....	21
Figura 8. Configuración básica Router R1 .....	22
Figura 9. Configuración básica Router R2.....	24
Figura 10. Configuración básica Router R3.....	26
Figura 11. Configuración básica del SWITCH D1.....	28
Figura 12. Configuración básica del SWITCH D2.....	32
Figura 13. Configuración básica del SWITCH A1 .....	36
Figura 14. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo RSPT EN D1.....	44
Figura 15. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo RSPT EN D2.....	46
Figura 16. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo rspt en a1.....	48
Figura 17. verificación con el comando show interface trunk.....	49
Figura 18. Verificación con el comando Show run   include spanning-tree.....	49
Figura 19. verificación con el comando show run int g2/3 .....	50
Figura 20. Verificación con el comando show int trunk .....	51
Figura 21. Verificación con el comando show INT G2/3 .....	52
Figura 22. Verificación con el comando show int g3/0.....	52

Figura 23. Simulación BGP en r1.....	62
Figura 24. Simulación BGP en R2 .....	64
Figura 25. Simulación BGP en r3.....	65
Figura 26. Simulación BGP en D1 .....	66
Figura 27. Simulación BGO en D2.....	68
Figura 28. Validación del estado de las IP SLA y d los Track en D1 .....	71
Figura 29. Asignación Scripypt Secret D1 .....	79
Figura 30. Asignación Scriptypt Secret D2 .....	79
Figura 31. Asignación Scriptypt secret A1 .....	79
Figura 32. Asignación alternativa Scripypt secret R1.....	80
Figura 33. Asignación Scripypt Secret R2 .....	80
Figura 34. Asignación Scripypt Secret D1 .....	81
Figura 35. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA.....	82
Figura 36. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA.....	82
Figura 37. Se habilitó AAA, se configuraron las especificaciones del servidor RADIUS y se configuró la lista de métodos de autenticación AAA. ....	83
Figura 38. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA.....	84
Figura 39. Se habilitó AAA, se configuraron las especificaciones del servidor RADIUS y se configuró la lista de métodos de autenticación AAA. ....	84
Figura 40. Verificación de acceso en R1 .....	85
Figura 41. Configuración del reloj local a la hora UTC actual .....	87
Figura 42. Verificación de la configuración R3.....	89
Figura 43. Verificación de la configuración de NTP en los equipos .....	91
Figura 44. Verificación de la configuración en A1 .....	92
Figura 45. Verificación en R1 #show run .....	93

## GLOSARIO

**DIRECCIÓN IP:** Cada ordenador se le asigna una dirección o un nombre que se conoce como dirección IP, y que es única para cada uno de ellos. Las direcciones IP están compuestas por cuatro cifras numéricas, separadas por puntos, cada una de ellas puede tomar valores comprendidos entre 0 y 255.

**SERVIDORES:** Es necesario que exista algún ordenador que organice un poco la comunicación entre unos equipos y otros.

**REDES DE ÁREA LOCAL (LAN):** Las redes de área local, generalmente llamadas LAN (local area networks), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cientos kilómetros de extensión.

**EL PROTOCOLO IP:** El protocolo de IP (Internet Protocol) es la base fundamental de la Internet. Se reconoce como aquel que contiene los datagramas de datos.

**ENRUTAMIENTO:** El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

## RESUMEN

En el presente documento se trabajaron escenarios propuestos a lo largo del desarrollo del curso basados en simulaciones que en este caso fueron apoyadas en GNS3 un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, donde básicamente mediante plataformas de conmutación basadas en switch, se hizo el uso de protocolos de STP y configuraciones de Vlans. Se realizó la configuración de direccionamiento de tipo ipv4 e ipv6 de tipo OSPF, EIGRP Y BGP; en el aprendizaje se implementaron escenarios LAN y WAN donde se evaluó a su vez el desempeño de los routers. Cabe destacar que el desarrollo de la actividad se afianzó con los conocimientos que se venían trabajando en diferentes escenarios, pero que contribuyeron significativamente en el aprendizaje como futura profesional.

**PALABRAS CLAVES:** CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

In this document, proposed scenarios were worked on throughout the development of the course based on simulations that in this case were supported in GNS3, a graphical network simulator that allows the design of complex network topologies and start up simulations on them, where basically through platforms Switch-based switching systems, the use of STP protocols and Vlans configurations was made. The IPv4 and ipv6 type addressing configuration of OSPF, EIGRP and BGP type was carried out; In the learning, LAN and WAN scenarios were implemented where the performance of the routers was evaluated. It should be noted that the development of the activity was consolidated with the knowledge that had been working in different scenarios, but that contributed significantly to learning as a future professional.

**KEY WORDS:** CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

El presente proyecto se redacta con carácter de Trabajo Profesional del diplomado de profundización CISCO, para la obtención por parte de quien lo suscribe del título de Ingeniero de telecomunicaciones, donde se trabajó en la simulación de una topología de red propuesta donde se buscó experimentar las habilidades que se habían desarrollado a lo largo del curso.

Como iniciativa fundamental de la actividad se completó la configuración de la red donde se buscaba una accesibilidad completa de un extremo a otro, donde los hosts cuentan con un soporte confiable de la puerta de enlace predeterminada (default gateway) y los protocolos establecidos en cada una de las etapas se encuentran totalmente configurados, estas etapas constan de seis partes donde la parte uno construye la topología de red propuesta se hicieron los ajustes básicos de cada componente y el direccionamiento de la interfaz, en la segunda parte se hizo la configuración de la capa dos de la red y el soporte de host, en la tercera etapa se hizo lo que fue la configuración de enrutamiento de los protocolos, en la cuarta etapa se configuró la redundancia del primer salto, en la quinta parte se configura todo que tiene que ver con seguridad y en la etapa final que sería la seis se configuraron las características de administración de red.

Por último, en el documento que se presentan a continuación, se recogen todos los datos y características que han sido obtenidos como resultado del escenario simulado de la red de compañía correspondiente, y que nos permiten marcar las líneas directrices para la materialización del proyecto a un futuro de ámbito profesional así mismo la redacción de cada uno de los códigos que se implementaron basados en las configuraciones solicitadas donde se tuvo en cuenta lo conceptos previamente desarrollados en cada una de las etapas formativas del curso.



Tabla 1. Tabla de direccionamiento

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

## Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.

Part 2: Configurar la capa 2 de la red y el soporte de Host.

Part 3: Configurar los protocolos de enrutamiento.

Part 4: Configurar la redundancia del primer salto.

Part 5: Configurar la seguridad.

Part 6: Configurar las características de administración de red.

## Escenario

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

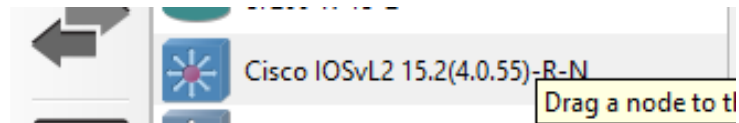
**Nota:** Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Catalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

**Nota:** Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.

**Nota:** La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global `sdm prefer dual-ipv4-and-ipv6 default`. Cambiar la plantilla requerirá el reinicio del switch.

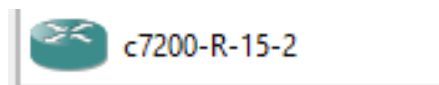
## Recursos necesarios

*Figura 2. Recursos necesarios*



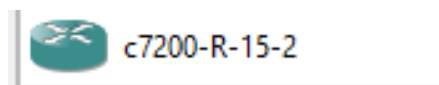
- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

*Figura 3. Switch Cisco 3650*



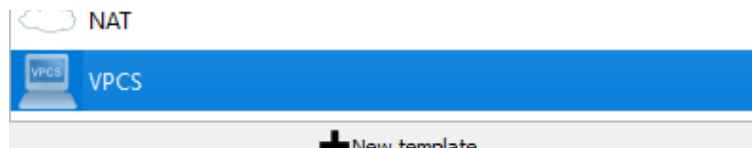
- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

*Figura 4. Switch Cisco 2960*



- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)

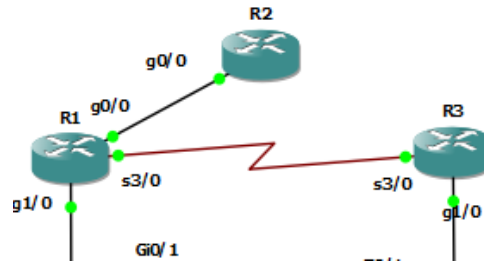
*Figura 5. PCs*



- 4 PCs (utilice el programa de emulación de terminal)

- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola.
- Los cables Ethernet y seriales van como se muestra en la topología

*Figura 6. Los cables Ethernet*

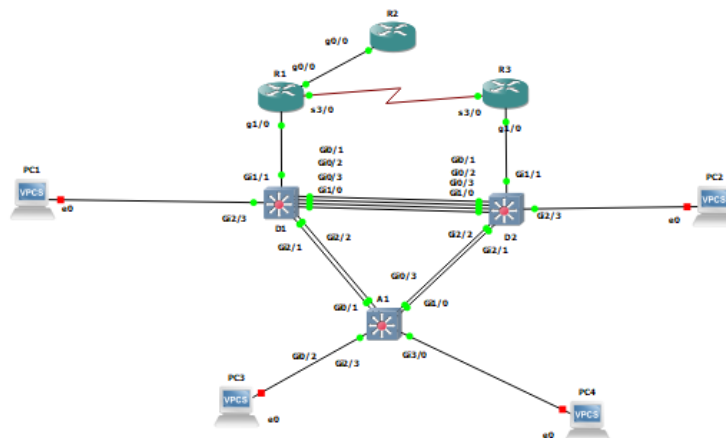


### **Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces**

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

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

Figura 7. Cablear la red como se muestra en la topología



## Paso 2: Configurar los parámetros básicos para cada dispositivo.

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



<pre> no ip domain lookup  banner motd # R1, ENCOR Skills Assessment, Scenario 1 #  exec-timeout 0 0  logging synchronous  exit  interface g0/0  ip address 209.165.200.225 255.255.255.224 ipv6 address fe80::1:1 link-local ipv6 address 2001:db8:200::1/64 no shutdown exit  interface g1/0 ip address 10.0.10.1  255.255.255.0 ipv6 address fe80::1:2 link-local ipv6 address 2001:db8:100:1010::1/64 no shutdown exit interface s3/0. ip address 10.0.13.1 255.255.255.0 </pre>	<p>Cree un aviso line con 0 ,linea de consola para la configuracion</p> <p>configuracion de linea de consola</p> <p>evitar que nos muestres mensajes inesperados configuracion de linea de consola</p> <p>salida</p> <p>Configure la dirección IP de acuerdo con la tabla de direcciones.</p> <p>ip y mascara asignadas</p> <p>habilita la interfaz salida</p> <p>Configure la dirección IP de acuerdo con la tabla de direcciones. ip y mascara asignadas</p> <p>se asigna la dirección ipv6 habilita la interfaz salida</p> <p>se asigna la direccion ipv4 y la mascara de subred</p> <p>se asigna la direccion link local</p>
--	--



<pre> no ip domain lookup  banner motd # R2, ENCOR Skills Assessment, Scenario 1 # line con 0  exec-timeout 0 0  logging synchronous  exit  interface g0/0. ip address 209.165.200.226 255.255.255.224  ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:200::2/64 no shutdown  exit  interface Loopback 0 ip address 2.2.2.2 255.255.255.255  ipv6 address fe80::2:3 link-local  ipv6 address 2001:db8:2222::1/128 no shutdown exit </pre>	<p>Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.</p> <p> Cree un aviso</p> <p> línea de configuración de consola</p> <p> no se agota el tiempo de consola en el puerto de la consola 0</p> <p> comando evita los mensajes inesperados</p> <p> salida</p> <p> Configure la dirección IP de acuerdo con la tabla de direcciones</p> <p> Dirección link local</p> <p> Dirección ipv6</p> <p> habilita la interfaz</p> <p> salida</p> <p> Establecer la interfaz Dirección ipv4 y la máscara de subred asignadas</p> <p> Asignación de la dirección link local</p> <p> Dirección ipv6</p> <p> habilita la interfaz</p> <p> salida</p>
--	---

Figura 10. Configuración básica Router R3

```

R1 R2 R3
*Nov 7 00:21:56.583: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
*Nov 7 00:21:56.571: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Nov 7 00:21:56.583: %LINK-5-CHANGED: Interface Serial3/0, changed state to administratively down
*Nov 7 00:21:56.611: %LINK-5-CHANGED: Interface Serial3/1, changed state to administratively down
*Nov 7 00:21:56.635: %LINK-5-CHANGED: Interface Serial3/2, changed state to administratively down
*Nov 7 00:21:56.663: %LINK-5-CHANGED: Interface Serial3/3, changed state to administratively down
*Nov 7 00:21:56.743: %LINK-5-CHANGED: Interface Serial4/0, changed state to administratively down
*Nov 7 00:21:56.771: %LINK-5-CHANGED: Interface Serial4/1, changed state to administratively down
*Nov 7 00:21:56.795: %LINK-5-CHANGED: Interface Serial4/2, changed state to administratively down
*Nov 7 00:21:56.799: %LINK-5-CHANGED: Interface Serial4/3, changed state to administratively down
R3#conf 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-timeout 0 0
R3(config-line)#logging synchronous
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 s3/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::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)#
*Nov 7 00:22:15.319: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Nov 7 00:22:15.743: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
*Nov 7 00:22:16.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
R3(config)#
*Nov 7 00:22:16.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
R3(config)#
R3(config)#
*Nov 7 00:22:39.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to down
R3(config)#

```

Código hecho Router R3

Tabla 4. Código Router R3

<pre> Router R3 Switch enable Switch conf term  hostname R3  ipv6 unicast-routing  no ip domain lookup </pre>	<p>Configuración en el router R3 Entramos al modo privilegiado configuración global</p> <p>asignamos al dispositivo un nombre este comando es necesario antes de poder configurar cualquier protocolo de routing IPv6</p> <p>Inhabilita la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.</p> <p>Cree un aviso</p>
---	---

<pre> banner motd # R3, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0  logging synchronous  exit  interface g1/0  ip address 10.0.11.1 255.255.255.0  ipv6 address fe80::3:2 link-local  ipv6 address 2001:db8:100:1011::1/64  no shutdown exit  interface s3/0  ip address 10.0.13.3 255.255.255.0  ipv6 address fe80::3:3 link-local  ipv6 address 2001:db8:100:1010::2/64  no shutdown  exit </pre>	<p>línea de consola para la configuración</p> <p>con este comando se evita los mensajes inesperados</p> <p>salida</p> <p>Configure la dirección IP de acuerdo con la tabla de direcciones.</p> <p>asigne la dirección ipv4 y su máscara subred</p> <p>asigne la dirección link local a la interfaz</p> <p>asigne la dirección ipv6</p> <p>habilite la interfaz</p> <p>salida</p> <p>Configure la dirección IP de acuerdo con la tabla de direcciones.</p> <p>Asigne la dirección ipv4 y su máscara subred</p> <p>Asigne la dirección link local</p> <p>Asignemos la dirección ipv6</p> <p>Habilite la interfaz</p> <p>Salida</p>
--	--

Figura 11. Configuración básica del SWITCH D1

```

D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-add
*Nov 7 00:51:35.390: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
*Nov 7 00:51:36.124: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to down
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.1
*Nov 7 00:51:36.757: %LINK-3-UPDOWN: Interface Vlan101, changed state to down
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range g0/0-3,g1/0,g1/2-3,g2/0-3,g3/0-3
D1(config-if-range)#shutdown
*Nov 7 00:51:38.200: %LINK-3-UPDOWN: Interface Vlan102, changed state to down
D1(config-if-range)#exit
*Nov 7 00:51:41.397: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
*Nov 7 00:51:41.401: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
*Nov 7 00:51:41.572: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
*Nov 7 00:51:41.689: %LINK-5-CHANGED: Interface GigabitEthernet0/3, changed state to administratively down
*Nov 7 00:51:41.766: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
*Nov 7 00:51:41.847: %LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to administratively down
D1(config-if-range)#exit
*Nov 7 00:51:42.004: %LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to administratively down
*Nov 7 00:51:42.102: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Nov 7 00:51:42.209: %LINK-5-CHANGED: Interface GigabitEthernet2/1, changed state to administratively down
*Nov 7 00:51:42.302: %LINK-5-CHANGED: Interface GigabitEthernet2/2, changed state to administratively down
*Nov 7 00:51:42.386: %LINK-5-CHANGED: Interface GigabitEthernet2/3, changed state to administratively down
*Nov 7 00:51:42.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Nov 7 00:51:42.940: %LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to administratively down
*Nov 7 00:51:42.942: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
D1(config-if-range)#exit
*Nov 7 00:51:43.209: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/1, changed state to down
*Nov 7 00:51:43.303: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/2, changed state to down
*Nov 7 00:51:43.307: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/3, changed state to down
D1(config-if-range)#exit
D1(config)#
  
```

Código hecho Switch D1

Tabla 5. Código Switch D1

<p>Switch D1 hostname D1</p> <p>ip routing</p> <p>ipv6 unicast-routing</p> <p>no ip domain lookup.</p>	<p>Configuración en el switch D1 asignamos nombre de dispositivo al switch</p> <p>habilitamos el routing</p> <p>este comando es necesario antes de poder configurar cualquier protocolo de routing IPv6.</p> <p>Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host</p>
--	--

<pre> banner motd # D1, ENCOR Skills Assessment, Scenario 1 # line con 0  exec-timeout 0 0  logging synchronous  exit  vlan 100 name Management  exit  vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit vlan 999 name NATIVE  exit  interface g1/1 </pre>	<p>Cree un aviso</p> <p>Configure la linea de la consola</p> <p>Se asigna para que el tiempo en la consola 0 no se agote</p> <p>evitar que nos muestres mensajes inesperados configuracion de linea de consola</p> <p>salida</p> <p>asignacion de ip a vlan</p> <p>asigne el nombre del host del dispositivo</p> <p>salida</p> <p>asignacion de ip a vlan</p> <p>asignamos nombre salida asignacion de ip a vlan</p> <p>asignamos nombre salida asignacion de ip a vlan</p> <p>asignamos nombre a la vlan nativa</p> <p>salida</p> <p>Configure la dirección IP de acuerdo con la tabla de direcciones</p>
--	--

<pre> no switchport  ip address 10.0.10.2 255.255.255.0  ipv6 address fe80::d1:1 link- local  ipv6 address 2001:db8:100:1010::2/64  no shutdown  exit  interface vlan 100 ip address 10.0.100.1 255.255.255.0 ipv6 address fe80::d1:2 link- local ipv6 address 2001:db8:100:100::1/64// direccion ip no shutdown exit interface vlan 101 ip address 10.0.101.1 255.255.255.0  ipv6 address fe80::d1:3 link- local </pre>	<p>Se agrega a la interface de capacidad 3</p> <p>puerto de capa 3</p> <p>asigne direccion y la mascara subred</p> <p>asignamos la direccion link local a la interface</p> <p>asignamos la direccion ipv6</p> <p>habilitamos la interfaz</p> <p>salida interfaces 100,101,.102</p> <p>modo de configuración de interfaz</p> <p>se asigna la configuración link local asignamos la dirección ipv6</p> <p>habilitamos la interfaz salida modo de configuración de interfaz asigne direccion ip y mascara subred</p> <p>asigne la direccion link local</p> <p>asigne la direccion ipv6</p> <p>habilite la interfaz</p> <p>salida</p>
--	---

<pre> ipv6 address 2001:db8:100:101::1/64  no shutdown  exit  interface vlan 102  ip address 10.0.102.1 255.255.255.0  ipv6 address fe80::d1:4 link- local  ipv6 address 2001:db8:100:102::1/64// direccion ip no shutdown exit  ip dhcp excluded-address 10.0.101.1 10.0.101.109  ip dhcp excluded-address 10.0.101.141 10.0.101.254 ip dhcp excluded-address 10.0.102.1 10.0.102.109 ip dhcp excluded-address 10.0.102.141 10.0.102.254 ip dhcp pool VLAN-101  network 10.0.101.0 255.255.255.0  default-router 10.0.101.254  exit  ip dhcp pool VLAN-102 </pre>	<pre> modo de configuración de interfaz  asigne la direccion y la mascara subred  identifique la interfaz de red Configurar la dirección link-local y seguir la dirección  se asigna la direccion ipv6  habilita la interfaz salida configuracion dhcp  se quita el rango de direcciones ipv4 que se especificaron  configura el enrutador para excluir configura el enrutador para excluir configura el enrutador para excluir  se configura el servidor dhcp para vlan 101  asigne la dirección de red y la máscara subred  puerta de enlace predeterminada  salida  se configura el servidor dhcp para vlan 102  asigne la dirección de red y la máscara subred  ruta predeterminada salida </pre>
--	---

<pre> network 10.0.102.0 255.255.255.0  default-router 10.0.102.254 exit  interface range g0/0- 3,g1/0,g1/2-3,g2/0-3,g3/0-3 shutdown exit  interface range g0/0- 3,g1/0,g1/2-3,g2/0-3,g3/0-3 shutdown exit </pre>	<p>apague todos los puertos exepto el 1/1</p> <p>se usan los siguientes rangos</p> <p>salida</p>
---	--

Figura 12. Configuración básica del SWITCH D2

```

D2(config-if)#ip address fe80::d2:d4 link-local
D2(config-if)#
Nov 7 01:11:13.111: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to down
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.200
D2(config)#ip dhcp
Nov 7 01:11:13.847: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
Nov 7 01:11:14.992: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to down
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.200
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.102.25
Nov 7 01:11:15.526: %LINK-3-UPDOWN: Interface Vlan101, changed state to down
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
Nov 7 01:11:17.138: %LINK-3-UPDOWN: Interface Vlan102, changed state to down
D2(config)#interface range g0/0-3,g1/0,g1/2-3,g2/0-3,g3/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
Nov 7 01:11:22.809: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
Nov 7 01:11:22.827: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
Nov 7 01:11:22.853: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
Nov 7 01:11:22.876: %LINK-5-CHANGED: Interface GigabitEthernet0/3, changed state to administratively down
Nov 7 01:11:22.847: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
Nov 7 01:11:22.842: %LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to administratively down
Nov 7 01:11:22.845: %LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to administratively down
Nov 7 01:11:22.935: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
Nov 7 01:11:23.008: %LINK-5-CHANGED: Interface GigabitEthernet2/1, changed state to administratively down
Nov 7 01:11:23.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to down
Nov 7 01:11:23.176: %LINK-5-CHANGED: Interface GigabitEthernet2/2, changed state to administratively down
Nov 7 01:11:23.209: %LINK-5-CHANGED: Interface GigabitEthernet2/3, changed state to administratively down
D2(config-if-range)#exit
Nov 7 01:11:23.693: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
Nov 7 01:11:24.409: %LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to administratively down
Nov 7 01:11:24.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to down
D2(config-if-range)#exit
D2(config)#

```

## Codigo hecho configuración Switch D2

Tabla 6. Código Switch D2

<pre> Switch D2 hostname D2  ip routing  ipv6 unicast-routing no ip domain lookup  banner motd # D2, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0  logging synchronous exit vlan 100 name Management  exit vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit vlan 999 name NATIVE exit interface g1/1 no switchport </pre>	<p>Configuración en switch D2 asignamos el nombre del dispositivo del switch</p> <p>habilite el routing ipv4</p> <p>habilite el routing ipv6 se habilita la traducción del nombre a dirección basado en el DNS del host</p> <p> Cree un aviso</p> <p>configure la línea de consola no se agotará el tiempo de espera en la consola 0 en el puerto evite mensajes inesperados salida</p> <p>asignación de ip a vlan asigne el nombre del host del dispositivo salida</p> <p>configure la vlan 101 asigne nombre al grupo salida</p> <p>configure la vlan 102 asigne nombre al grupo salida</p> <p>configure la vlan 999 asigne nombre salida</p> <p>configure la interfaz aporte capacidad a la interfaz de capa 3</p> <p>asigne dirección ipv4 y máscara subred</p>
---	---

<pre> ip address 10.0.11.2 255.255.255.0 ipv6 address fe80::d1:1 link- local  ipv6 address 2001:db8:100:1011::2/64  no shutdown exit  interface vlan 100 ip address 10.0.100.2 255.255.255.0  ipv6 address fe80::d2:2 link- local ipv6 address 2001:db8:100:100::2/64 no shutdown exit// salida interface vlan 101 ip address 10.0.101.2 255.255.255.0  ipv6 address fe80::d2:3 link- local  ipv6 address 2001:db8:100:101::2/64 no shutdown exit interface vlan 102 ip address 10.0.102.2 255.255.255.0 ipv6 address fe80::d2:4 link- local  ipv6 address 2001:db8:100:102::2 /64 </pre>	<p>asigne direccion ipv6 en link local y siga la direccion</p> <p>se asigna la dirección ipv6</p> <p>habilite la interfaz vlan 102 salida interfaces 100,101,102</p> <p>configure la vlan 100 se asigna la dirección ipv4 y la mascara subred</p> <p>se asigna la dirección link local</p> <p>asignamos la dirección ipv6</p> <p>salida configuramos en la vlan 101</p> <p>asignamos la dirección ipv4 y la mascara subred</p> <p>asignamos dirección link local</p> <p>Se asigna la dirección link local a la interface. Salida Configuramos la vlan 102 Asignamos la dirección ip y la mascara subred Configuramos la dirección en link local</p> <p>direccion ipV6 asignada</p>
---	--

<pre> no shutdown exit  ip dhcp excluded-address 10.0.101.1 10.0.101.209  ip dhcp excluded-address 10.0.101.241 10.0.101.254  ip dhcp excluded-address 10.0.102.1 10.0.102.209  ip dhcp excluded-address 10.0.102.241 10.0.102.254  ip dhcp pool VLAN-101  network 10.0.101.0 255.255.255.0 default-router 10.0.101.254 exit ip dhcp pool VLAN-102  network 10.0.102.0 255.255.255.0  default-router 10.0.102.254 exit  interface range g0/0- 3,g1/0,g1/2-3,g2/0-3,g3/0-3 shutdown// apagar exit </pre>	<pre> salida  configuracion dhcp  configura el enrutador para excluir  configura el enrutador para excluir  configura el enrutador para excluir  configura el enrutador para excluir  se configura el servidor en la vlan 101 se asigna la dirección de red con la mascara subred asigne la dirección de red con la mascara subred salida se configura el servidor en la vlan 102 se asigna la dirección de la red con la mascara subred  ruta predeterminada salida  apague todos los puertos exepto g1/1  se usan los siguientes rangos  salida </pre>
---	--

Figura 13. Configuración básica del SWITCH A1

```

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 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db0:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range g1/1-3,g2/0-3,g3/0-3
*Nov 7 01:40:44.937: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to down
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#
*Nov 7 01:40:47.994: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
A1(config)#
*Nov 7 01:40:49.003: %LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to administratively down
*Nov 7 01:40:49.142: %LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to administratively down
*Nov 7 01:40:49.495: %LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to administratively down
*Nov 7 01:40:49.641: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to administratively down
*Nov 7 01:40:49.763: %LINK-5-CHANGED: Interface GigabitEthernet2/1, changed state to administratively down
*Nov 7 01:40:49.923: %LINK-5-CHANGED: Interface GigabitEthernet2/2, changed state to administratively down
A1(config)#
*Nov 7 01:40:50.056: %LINK-5-CHANGED: Interface GigabitEthernet2/3, changed state to administratively down
*Nov 7 01:40:50.180: %LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to administratively down
*Nov 7 01:40:50.265: %LINK-5-CHANGED: Interface GigabitEthernet3/1, changed state to administratively down
*Nov 7 01:40:50.470: %LINK-5-CHANGED: Interface GigabitEthernet3/2, changed state to administratively down
*Nov 7 01:40:50.635: %LINK-5-CHANGED: Interface GigabitEthernet3/3, changed state to administratively down
*Nov 7 01:40:51.030: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/3, changed state to down
*Nov 7 01:40:51.038: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to down
A1(config)#
  
```

## Código hecho Switch A1

Tabla 7. Código Switch A1

<p>Switch A1 Switch en Switch conf term hostname A1 no ip domain lookup</p> <p>banner motd # A1, ENCOR Skills Assessment, Scenario 1 #línea de consola line con 0 exec-timeout 0 0</p> <p>logging synchronous</p>	<p>Configuración en switch A1 modo enable modo de configuración asigne el nombre habilite la traducción del nombre en la dirección basada en DNS del host cree un aviso y configure la línea de consola</p> <p>en este puerto consola 0 no se agota el tiempo</p> <p>evitar que nos muestren mensajes inesperados configuración de línea de consola</p>
---	---

<pre> exit  vlan 100 name Management  exit vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit vlan 999 name NATIVE exit interface vlan 100 ip address 10.0.100.3 255.255.255.0 ipv6 address fe80::a1:1 link- local ipv6 address 2001:db8:100:100::3/64 no shutdown exit interface range g1/1-3,g2/0-3,g3/0-3 shutdown exit//salida </pre>	<pre> salida  asignacion de ip a vlan 100,101,102,999  asignamos vlan 100 asigne el nombre del host al dispositivo  salida asignamos vlan 101 asigne nombre salida configuramos la vlan 102 asignamos nombre salida asignamos vlan 999 asignamos nombre salida modo de configuración de interfaz asignamos direccion ip y mascara subred asignamos direccion link local  asigne la direccion ipv6  salida apague todos los puertos excepto 0/1 0/2 0/3 </pre>
--	---

- 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.

## 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 8. Configurar la capa 2 de la red y el soporte de host*

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"><li>• D1 and D2</li><li>• D1 and A1</li><li>• D2 and A1</li></ul>
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	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"><li>• D1 a D2 – Port channel 12</li><li>• D1 a A1 – Port channel 1</li><li>D2 a A1 – Port channel 2</li></ul>

2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.  Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC4: 10.0.100.6</li> </ul> PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> </ul> PC1: 10.0.100.5

## Solución

### Código

#### switch D1

**2.1** interface range g1/0/1-4 // enlace troncal 1 a 4

**2.1** switchport mode trunk// para que se troncal

**2.2** switchport trunk native vlan 999

**2.5** channel-group 12 mode active // configure los puertos de acceso del host

**2.5** no shutdown //encender y asegurar que el rango de las interfaces este activado

exit

**2.1** interface range g1/0/5-6 //enlace troncal de 5-6

**2.1** switchport mode trunk// para que sea troncal

**2.2** switchport trunk native vlan 999 //activamos la vlan para los enlaces troncales

**2.5** channel-group 1 mode active // configure los puertos de acceso del host

**2.5** no shutdown // encender y asegurar que el rango de la interfaces este activado

exit

**2.3** spanning-tree mode rapid-pvst // Se ejecuta en el modo de configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN Spanning Tree.

// D1 puente raiz para vlan 100 y 102

**2.4** spanning-tree vlan 100,102 root primary // asegurar que un switch tenga el valor de prioridad de puente más bajo

**2.4** spanning-tree vlan 101 root secondary // respaldo en caso de falla Este comando establece la prioridad para el switch en el valor predeterminado, haciendo uso de otro puente de raíz

// configuración de los puertos de acceso host

interface g1/0/23

switchport mode access

**2.6**switchport access vlan 100

**2.6**spanning-tree portfast // ayuda a que la transición sea inmediata

**2.6** no shutdown

exit

end

## **switch D2**

**2.1** interface range g1/0/1-4 //enlace troncal de 1-4

**2.1** switchport mode trunk// para que sea troncal

**2.2** switchport trunk native vlan 999 //activamos la vlan para los enlaces troncales

**2.5** channel-group 12 mode active // configure los puertos de acceso del host

**2.5** no shutdown // encender y asegurar que el rango de las interfaces este activado

exit

**2.1** interface range g1/0/5-6 //enlace troncal de 5-6

**2.1** switchport mode trunk// para que sea troncal

**2.2** switchport trunk native vlan 999 //activamos la vlan para los enlaces troncales

**2.5** channel-group 2 mode active // configure los puertos de acceso del host

**2.5** no shutdown // encender y asegurar que el rango de las interfaces este activado

**2.5** exit // salida

!

**2.3** spanning-tree mode rapid-pvst // Se ejecuta en el modo de

configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN Spanning Tree.

// puente raíz para 101

**2.4** spanning-tree vlan 101 root primary // asegurar que un switch tenga el valor de prioridad de puente más bajo

**2.4** spanning-tree vlan 100,102 root secondary// respaldo en caso de falla Este comando establece la prioridad para el switch en el valor predeterminado, haciendo uso de otro puente de raíz

!

// configuración de los puertos de acceso host

**2.6** interface g1/0/23

**2.6** switchport mode access

**2.6** switchport access vlan 102 // modo de acceso

spanning-tree portfast //ayuda a que la transición sea inmediata

**2.6** no shutdown

**2.6** exit

**2.6** end

**switch A1**

**2.3** spanning-tree mode rapid-pvst //  
Se ejecuta en el modo de configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN Spanning Tree.

**2.1** interface range f0/1-2 // troncal 1-2

**2.1** switchport mode trunk // para que se troncal

**2.2** switchport trunk native vlan 999 //activamos la vlan para los enlaces troncales

**2.5** channel-group 1 mode active

**2.5** no shutdown // encender y asegurar que el rango de las interfaces este activado

exit

**2.1** interface range f0/3-4 //troncal 3-4

**2.1** switchport mode trunk para que sea troncal

**2.2** switchport trunk native vlan 999 // //activamos la vlan para los enlaces troncales

**2.5** channel-group 2 mode active // configure los puertos de acceso del host

**2.5** no shutdown // encender y asegurar que el rango de las interfaces este activado

exit // salida

// configuración de los puertos de acceso host

**2.6** interface f0/23

**2.6** switchport mode access

**2.6** switchport access vlan 101 // modo de acceso

**2.6** spanning-tree portfast // ayuda a que la transición sea inmediata

**2.6** no shutdown // encender

**2.6** exit // salida

// // configuración de los puertos de acceso host

**2.6** interface f0/24

**2.6** switchport mode access

**2.6** switchport access vlan 100 // modo de acceso

**2.6** spanning-tree portfast // ayuda a que la transición sea inmediata

**2.6** no shutdown // encender

exit // salida

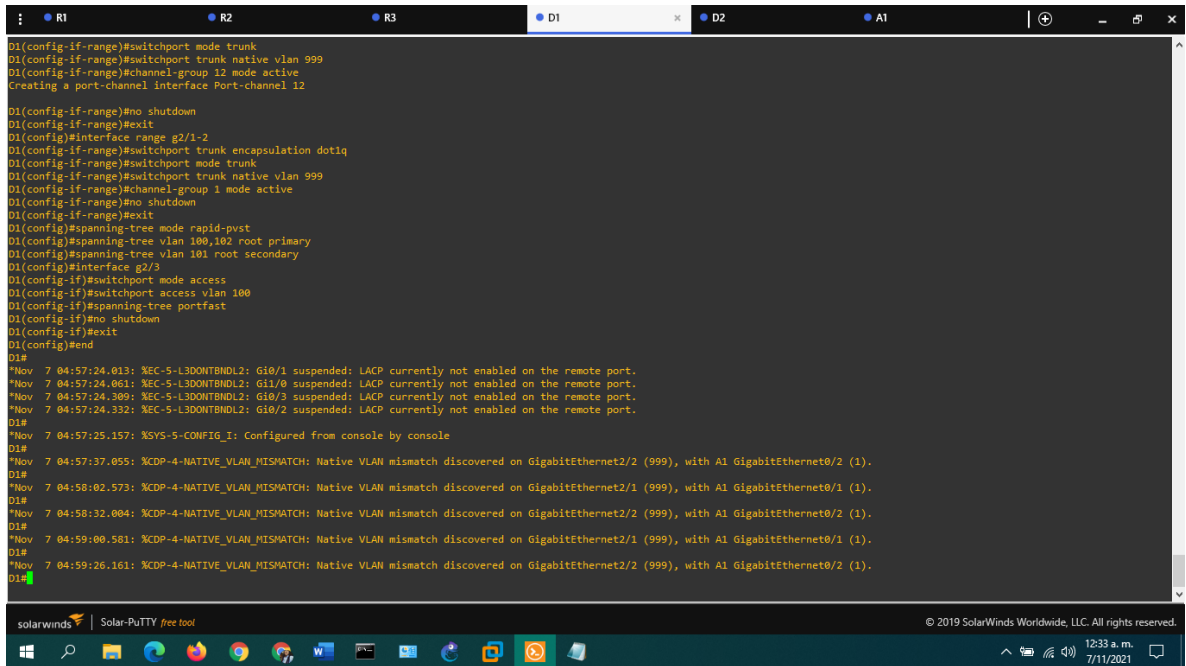
end

## Código desarrollado D1

Tabla 9. Código desarrollado D1

Switch D1	
<pre>interface range g0/1-3,g1/0 switchport trunk encapsulation dot1q switchport mode trunk  switchport trunk native vlan 999 channel-group 12 mode active active  no shutdown exit  interface range g2/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 999 channel-group 1 mode active no shutdown exit  spanning-tree mode rapid-pvst  no shutdown spanning-tree vlan 100,102 root primary spanning-tree vlan 101 root secondary interface g2/3 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end</pre>	<p>enlace troncal 1 a 4 para que sea troncal</p> <p>configure los puertos de acceso de host</p> <p>encender y asegurar que el rango de las interfaces este activado salida</p> <p>configuración de los puertos de acceso host</p> <p>encender y asegurar que el rango de las interfaces este activado salida</p> <p>ayuda a que la transición sea inmediata</p> <p>encender y asegurar que el rango de las interfaces este activado salida</p> <p>asegurar que un switch tenga el valor de prioridad de puente más bajo // respaldo en caso de falla Este comando establece la prioridad para el switch en el valor predeterminado, haciendo uso de otro puente de raíz</p>

Figura 14. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo RSPT EN D1



## Código desarrollado D2

Tabla 10. Código desarrollado D2

Switch D2	
interface range g0/1-3,g1/0	enlace troncal
switchport trunk encapsulation dot1q	
switchport mode trunk	para que sea troncal
switchport trunk native vlan 999	
channel-group 12 mode active	
no shutdown	configure los puertos de acceso del host se activa el protocolo LACP de manera incondicional

<pre> exit interface range g2/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 999 channel-group 2 mode active no shutdown  exit ! spanning-tree mode rapid-pvst Spanning Tree.  spanning-tree vlan 101 root primary  spanning-tree vlan 100,102 root secondary !  interface g2/3  switchport mode Access  switchport access vlan 102  spanning-tree portfast // no shutdown exit end </pre>	<p>configure la terminal</p> <p>se activa el modo trunk</p> <p>se activa en modo trunk</p> <p>configure los puertos de acceso del host</p> <p>salida</p> <p>Se ejecuta en el modo de configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN</p> <p>asegurar que un switch tenga el valor de prioridad de puente más bajo</p> <p>respaldo en caso de falla Este comando establece la prioridad para el switch en el valor predeterminado, haciendo uso de otro puente de raíz</p> <p>enlace troncal</p> <p>modo de acceso</p> <p>ayuda a que la transición sea inmediata</p> <p>salida</p>
---	---

Figura 15. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo RSPT EN D2

```

D2#
*Nov 7 05:11:39.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/3, changed state to up
D2#
*Nov 7 05:11:44.199: %EC-5-L3DONTBDL2: G12/2 suspended: LACP currently not enabled on the remote port.
*Nov 7 05:11:44.375: %EC-5-L3DONTBDL2: G12/1 suspended: LACP currently not enabled on the remote port.
D2#co
*Nov 7 05:11:46.234: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet2/2 (999), with A1 GigabitEthernet1/0 (1).
D2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#interface range g0/1-3,g1/9
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
Creating a port-channel interface Port-channel 12
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface range g2/1-2
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)#
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#!
D2(config)#interface g2/3
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
*Nov 7 05:11:59.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel12, changed state to up
D2#
*Nov 7 05:12:04.543: %SYS-5-CONFIG_I: Configured from console by console
D2#

```

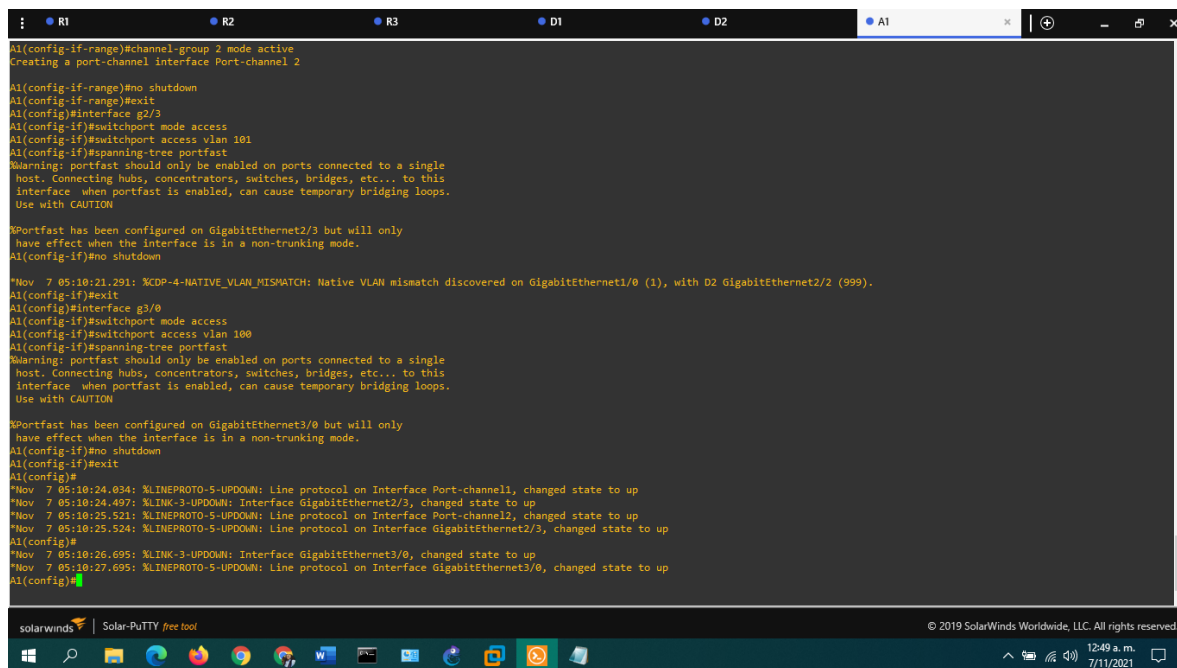
## Código desarrollado A1

Tabla 11. Código desarrollado A1

Switch A1	
switch A1	
spanning-tree mode rapid-pvst Spanning Tree.	Se ejecuta en el modo de configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN troncal 1-2
interface range g0/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 999 channel-group 1 mode active	para que se troncal encender y asegurar que el rango de las interfaces este activado

<pre> no shutdown exit// salida  interface range g0/3,g1/0 switchport trunk encapsulation dot1q switchport mode trunk switchport access vlan 999 channel-group 2 mode active no shutdown exit // salida interface g2/3 switchport mode access switchport access vlan 101 spanning-tree portfast no shutdown exit interface g3/0 switchport mode access switchport access vlan 100 spanning-tree portfast/ / ayuda a que la transición sea inmediata no shutdown no shutdown exit </pre>	<pre> salida  configuración de los puertos de acceso host modo de acceso encender y asegurar que el rango de las interfaces este activado  salida troncal  ayuda a que la transición sea inmediata  salida  ayuda a que la transición sea inmediata  salida </pre>
---	--

Figura 16. Imagen de simulación verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo rspt en a1



```
AI(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2

AI(config-if-range)#no shutdown
AI(config-if-range)#exit
AI(config)#interface g2/3
AI(config-if)#switchport mode access
AI(config-if)#switchport access vlan 101
AI(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 GigabitEthernet2/3 but will only
have effect when the interface is in a non-trunking mode.
AI(config-if)#no shutdown

*Nov 7 05:10:21.291: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0 (1), with D2 GigabitEthernet2/2 (999).
AI(config-if)#exit
AI(config)#interface g3/0
AI(config-if)#switchport mode access
AI(config-if)#switchport access vlan 100
AI(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 GigabitEthernet3/0 but will only
have effect when the interface is in a non-trunking mode.
AI(config-if)#no shutdown
AI(config-if)#exit
AI(config)#
*Nov 7 05:10:24.034: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
*Nov 7 05:10:24.497: %LINK-3-UPDOWN: Interface GigabitEthernet2/3, changed state to up
*Nov 7 05:10:25.521: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
*Nov 7 05:10:25.524: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/3, changed state to up
AI(config)#
*Nov 7 05:10:26.695: %LINK-3-UPDOWN: Interface GigabitEthernet3/0, changed state to up
*Nov 7 05:10:27.695: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to up
AI(config)#
```

-2.7 y 2.8

## Verificaciones

SHOW INTERFACE TRUNK // verificar múltiples elementos de la operación de los enlaces troncales

Conexión po1 conexión A1

Conexión po12 conexión D2

Native vlan 999

Figura 17. verificación con el comando show interface trunk

```
*Nov 7 05:13:07.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channell, changed state to up
D1#SHOW INTERFACE TRUNK

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

Port      Vlans allowed on trunk
Po12     1-4094
Po1      1-4094

Port      Vlans allowed and active in management domain
Po12     1,100-102,999
Po1      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po12     1,100-102,999
```

solarwinds | Solar-PuTTY free tool

## SHOW RUN | INCLUDE SPANNING-TREE

El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión

Figura 18. Verificación con el comando Show run | include spanning-tree

```
% Invalid input detected at '^' marker.

D1#show run |include spanning-tree
^
% Invalid input detected at '^' marker.

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#
D1#
```

**Puente raíz: spanning-tree vlan 100,102 priority 24576**  
**Secundario: spanning-tree vlan 101 priority 28672**

### **SHOW RUN INT G2/3**

Ayudar a determinar el estado actual **de** un router, ya que muestra el archivo **de** configuración activo que se ejecuta en la RAM.

*Figura 19. verificación con el comando show run int g2/3*

```
Building configuration...

Current configuration : 152 bytes

interface GigabitEthernet2/3
switchport access vlan 100
switchport mode access
media-type rj45
negotiation auto
spanning-tree portfast edge
end

S1#
```

Puertos de acceso ,la conexión a pc vlan 100 modo de acceso

A1

**SHOW INT TRUNK** Este comando permite verificar múltiples elementos **de** la operación **de** los enlaces troncales

Figura 20. Verificación con el comando show int trunk

```
A1#show interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    1
Po1       on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po2       1-4094
Po1       1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po1       1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,101,999
Po1       1,100,102,999
A1#
```

PO2 CONEXIÓN D2

PO1 CONEXIÓN D1

Nativa vlan

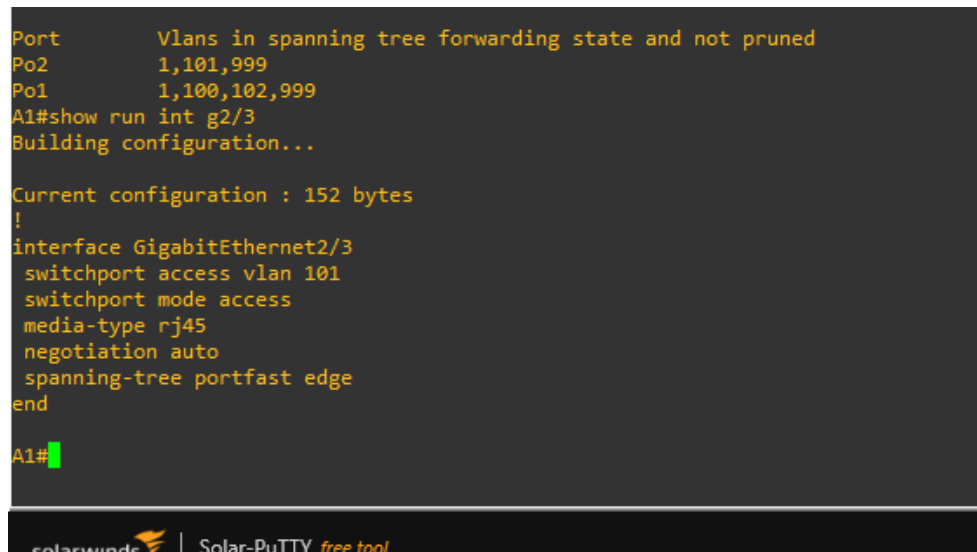
### SHOW RUN INT G2/3

Ayudar a determinar el estado actual **de** un router, ya que muestra el archivo **de** configuración activo que se ejecuta en la RAM.

Figura 21. Verificación con el comando show INT G2/3

```
Port      Vlans in spanning tree forwarding state and not pruned
Po2      1,101,999
Po1      1,100,102,999
A1#show run int g2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```



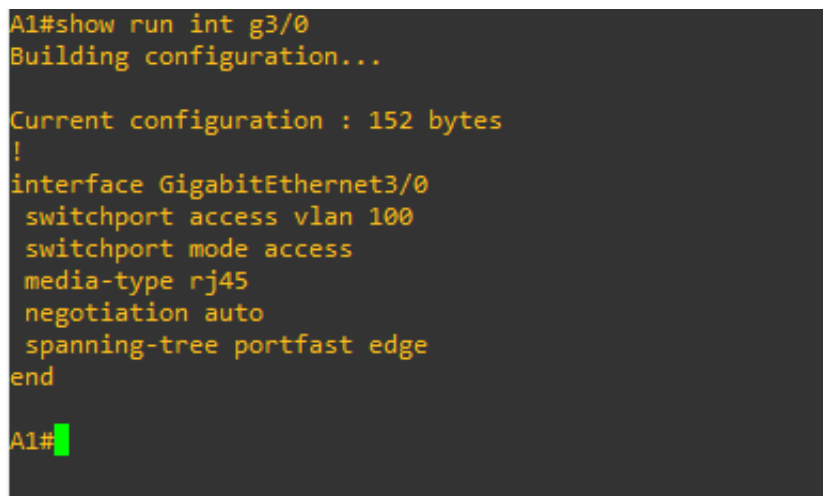
### SHOW RUN INT G3/0

Ayudar a determinar el estado actual **de** un router, ya que muestra el archivo **de** configuración activo que se ejecuta en la RAM.

Figura 22. Verificación con el comando show int g3/0

```
A1#show run int g3/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet3/0
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```



### 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.

**Nota:** Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

*Tabla 12. Verificación con el comando show int g3/0*

C	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.	Use OSPF Process ID 4 y asigne los siguientes router- IDs: <ul style="list-style-type: none"><li>• R1: 0.0.4.1</li><li>• R3: 0.0.4.3</li><li>• D1: 0.0.4.131</li><li>• D2: 0.0.4.132</li></ul> En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. <ul style="list-style-type: none"><li>• En R1, no publique la red R1 – R2.</li><li>• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li></ul> Deshabilite las publicaciones OSPFv2 en: <ul style="list-style-type: none"><li>• D1: todas las interfaces excepto G1/0/11</li><li>• D2: todas las interfaces excepto G1/0/11</li></ul>

3.2	<p>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.</p>	<p>Use OSPF Process ID <b>6</b> y asigne los siguientes router- IDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.6.1</li> <li>• R3: 0.0.6.3</li> <li>• D1: 0.0.6.131</li> <li>• D2: 0.0.6.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul>
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"> <li>• Una ruta estática predeterminada IPv4.</li> <li>• Una ruta estática predeterminada IPv6.</li> </ul> <p>Configure R2 en BGP ASN <b>500</b> y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/32).</li> <li>• La ruta por defecto (0.0.0.0/0).</li> </ul> <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/128).</li> </ul> <p>La ruta por defecto (::/0).</p>

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

### Desarrollo de la tarea 3.1.

// sección ^ router ospf en R1, R3, D1 y D2

### Configuración en R1

*Tabla 13. Configuración en R1*

<pre>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</pre>	<pre>id de proceso id del router 1 notificación de red 10.0 notificación de red 13.0 propague la ruta por defecto</pre>
--	---

### Configuración en R3

*Tabla 14. Configuración en R3*

<pre>R3# show run   section ^router ospf router ospf 4 router-id 0.0.4.3</pre>	<pre>id de proceso id del router 3</pre>
--	--

network 10.0.11.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0	notificación de red 11.0 notificación de red 13.0
--	--

## Configuración en D1

*Tabla 15. Configuración en D1*

D1# show run   section ^router ospf router ospf 4 router-id 0.0.4.131 passive-interface default no passive-interface GigabitEthernet1/0/11	id de proceso id del router 131 interfaces sea pasiva desactive todas las interfaces excepto 11
---	---

## notificación de 4 redes

network 10.0.10.0 0.0.0.255 area 0	notificación de red 10.0
network 10.0.100.0 0.0.0.255 area 0	notificación de red 100.0
network 10.0.101.0 0.0.0.255 area 0	notificación de red 101.0
network 10.0.102.0 0.0.0.255 area 0	notificación de red 102.0

## Configuración en D2

*Tabla 16. Configuración en D2*

D2# show run   section ^router ospf router ospf 4 router-id 0.0.4.132 passive-interface default	id de proceso id del router 132 para que la interfaz sea pasiva
--	---

no passive-interface GigabitEthernet1/0/11	desactive todas las interfaces excepto 11
---	--

### notificación de 4 redes

network 10.0.11.0 0.0.0.255 area 0/	notificación de red 11.0
network 10.0.100.0 0.0.0.255 area 0	notificación de red 100.0
network 10.0.101.0 0.0.0.255 area 0	notificación de red 101.0
network 10.0.102.0 0.0.0.255 area 0	notificación de red 102.0

### Desarrollo de la tarea 3.2

sección ^ enrutador ipv6 y muestra el resumen de la interfaz ipv6 ospf en R1, R3, D1 y D2.

### Configuración en R1

R1# show run | section ^ipv6 router

*Tabla 17. Configuración en R1*

<pre> ipv6 router ospf 6 router-id 0.0.6.1 default-information originate </pre>	<pre> id del proceso id del proceso en r1 es 1 propague la ruta por defecto </pre>
<pre> R1# show ipv6 ospf interface brief Interface  PID Area      Intf ID Cost  State Nbrs F/C </pre>	

**// notifique las rutas creadas por defecto**

S3/0	6	0	7	49	P2P	1/1	conexión serial
Gi1/0	6	0	6	1	DR	1/1	conexión con el router

### Configuración en R3

**R3# show run | section ^ipv6 router**

*Tabla 18. Configuración en R3*

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	id del proceso id del proceso en r3 es 3
--	---

**// solo dos interfaces**

Se0/1/0	6	0	7	50	P2P	1/1	conexión al serial
Gi0/0/1	6	0	6	1	DR	1/1	conexión al router

*Tabla 19. D1# show run | section ^ipv6 router*

ipv6 router ospf 6 router-id 0.0.6.131 passive-interface default no passive-interface GigabitEthernet1/0/11	id del proceso en d1 el id del proceso 131  todas las interfaces pasivas excepto la 11
---	--

**D1# show ipv6 ospf interface brief**

**// vlan 102,101,100 ,0/11**

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
VI102	6	0	41	1	DR	0/0	
VI101	6	0	40	1	DR	0/0	
VI100	6	0	39	1	DR	0/0	
Gi1/0/11	6	0	38	1	BDR	1/1	

### Configuración en D1

*Tabla 20. D2# show run | section ^ipv6 router*

ipv6 router ospf 6 router-id 0.0.6.132 passive-interface default no passive-interface GigabitEthernet1/0/11	id del proceso d2 el id del proceso 132  // todas las interfaces pasivas exepcto la 11
---	--

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
VI102	6	0	41	1	DR	0/0	// vlan 102
VI101	6	0	40	1	DR	0/0	// vlan 101
VI100	6	0	39	1	DR	0/0	// vlan 100
Gi1/0/11	6	0	38	1	BDR	1/1	// interfaz 11

### Desarrollo de la tarea 3.3

#### Sección bgp y show run | incluir ruta en R2

#### Configuración en R2

Tabla 21. Configuración en R2

R2	
R2# show run   section router bgp router bgp 500  bgp router-id 2.2.2.2  bgp log-neighbor-changes 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 no neighbor 2001:DB8:200::1 activate// active el vecino neighbor 209.165.200.225 activate exit-address-family ! address-family ipv6// acceda a la familia de ipv6 network ::/0 network 2001:DB8:2222::/128 neighbor 2001:DB8:200::1 exit-address-family // salida  R2# show run   include route	Se define el proceso BGP en R2 y el número de ASN al que pertenece  Se asigna el id del protocolo BGP.  configuración del enrutador.  configure el vecino para ipv4 sistema autónomo 300  configure el vecino para ipv6 sistema autónomo 300  ruta por defecto  desactivar el vecino ipv6 salida  dirección loopback ipv6 active el vecino ipv6 salida

<pre>router bgp 500   bgp route-id 2.2.2.2   ip route 0.0.0.0 0.0.0.0 Loopback0   ipv6 route ::/0 Loopback0 //</pre>	<pre>lconfigure la ruta estatica  loopback0 interfaz de salida</pre>
--	--

### Desarrollo de la tarea 3.4

**Ejecutar la demostración del problema | sección bgp en R1.**

**R1# show run | section bgp**

```
Ip route 10.0.0.0 255.0.0.0 null0          interfaces de salida null 0
Ipv6 route 2001:db8:100::/48 null0       ipv6 con interface de salida null 0
router bgp 300                            sistema autónomo 300 configuración
  bgp router-id 1.1.1.1                   id del router 1
  bgp log-neighbor-changes                configuración del enrutador.
  neighbor 2001:DB8:200::2 remote-as 500  configure el vecino para ipv sistema
autónomo 500 ipv6
  neighbor 209.165.200.226 remote-as 500  configure el vecino para ipv sistema
autónomo 500
```

!

```
address-family ipv4                        configuramos para ipv4 la familia de dirección
  network 10.0.0.0                          notifique la red
  no neighbor 2001:DB8:200::2               activate
  neighbor 209.165.200.226                 activate
exit-address-family                        salida
```

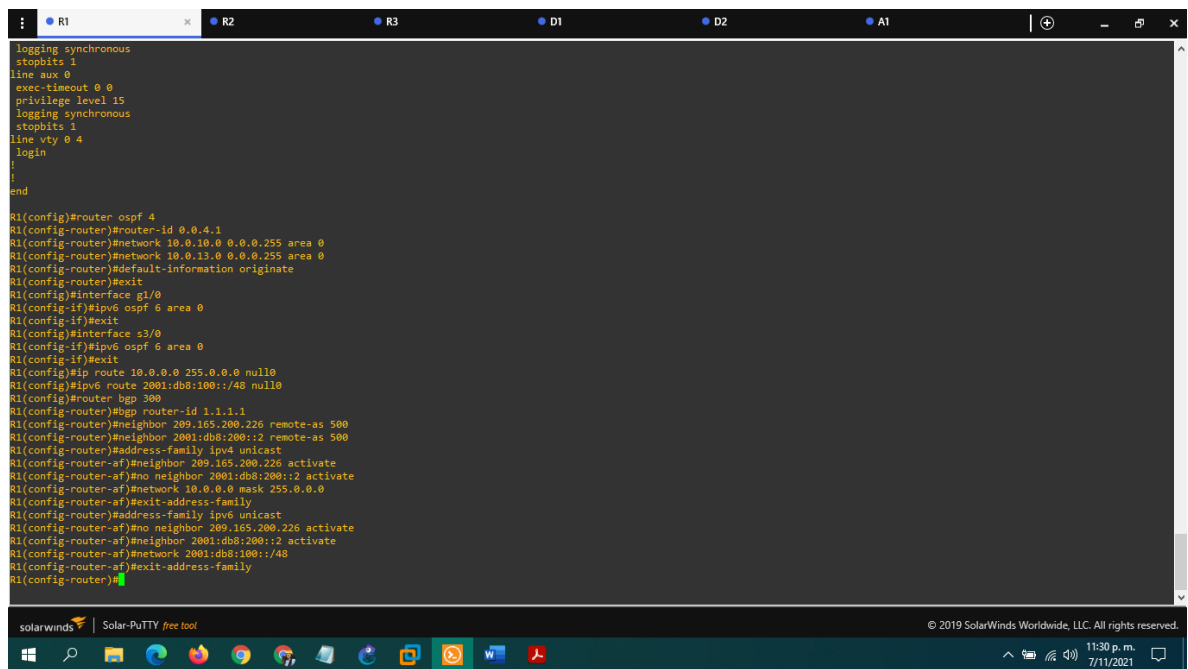
!

address-family ipv6	configuramos para ipv6 , la familia de dirección
network 2001:DB8:100::/48	notifique la red
neighbor 2001:DB8:200::2	active
exit-address-family	salida

## Simulaciones

### R1

Figura 23. Simulación BGP en R1



```
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end

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 g1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface s3/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#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)#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)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
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)#
```

## Código demostración del problema | sección BGP en R1

Tabla 22. Código demostración del problema | sección bgp en r1

<pre> router ospf 4 router-id 0.0.4.1 // id del router 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 exit// salidan interface g1/0 ipv6 ospf 6 area 0 exit interface s3/0  ipv6 ospf 6 area 0 exit ip route 10.0.0.0 255.0.0.0 null0 ipv6 route 2001:db8:100::/48 null0// ipv6 con interface de salida null 0 router bgp 300 bgp router-id 1.1.1.1 // id del router 1 neighbor 209.165.200.226 remote-as 500 neighbor 2001:db8:200::2 remote-as 500 address-family ipv4 unicast  neighbor 209.165.200.226 activate no neighbor 2001:db8:200::2 activate network 10.0.0.0 mask 255.0.0.0 // exit-address-family address-family ipv6 unicast no neighbor 209.165.200.226 activate neighbor 2001:db8:200::2 activate network 2001:db8:100::/48 exit-address-family </pre>	<pre> id de proceso notificación de red 10.0 notificación de red 13.0 propague la ruta por defecto  conexión router id del proceso area 0 salida serial conexión  id del proceso salida interfaces de salida null 0  sistema autónomo 300 configuración  configure el vecino para ipv sistema autónomo 500  configure el vecino para ipv sistema autónomo 500 ipv6 configuramos para ipv4 la familia de dirección actíivate  salida  actíivate actíivate notifique la red salida </pre>
--	---

R2

Figura 24. Simulación BGP en R2

```
R1 R2 R3 D1
R2(config-router)#network 2.2.2.2 mask 255.255.255.255
R2(config-router)#network 0.0.0.0
R2(config-router)#exit - address-family
^
% Invalid input detected at '^' marker.
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
% Specify remote-as or peer-group commands first
R2(config-router-af)#neighbor 2001:db8::200::1 activate
% Specify remote-as or peer-group commands first
R2(config-router-af)#network 2001:db8:2222::128
% Incomplete command.
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#exit
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)#neighbor 209.165.200.225 activate
% Specify remote-as or peer-group commands first
R2(config-router)#no neighbor 2001:db8.200::1 activate
% Specify remote-as or peer-group commands first
R2(config-router)#network 2.2.2.2 mask 255.255.255.255
R2(config-router)#network 0.0.0.0
R2(config-router)#exit - address-family
^
% Invalid input detected at '^' marker.
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
% Specify remote-as or peer-group commands first
R2(config-router-af)#neighbor 2001:db8::200::1 activate
% Specify remote-as or peer-group commands first
R2(config-router-af)#network 2001:db8:2222::128
% Incomplete command.
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
```

### Código

Tabla 23. Código en R2

ip route 0.0.0.0 0.0.0.0 loopback 0	lconfigure la ruta estatica loopback0
ipv6 route ::/0 loopback 0	interfaz de salida
router bgp 500	ruta estaica // loopback ruta sa salida
bgp router-id 2.2.2.2	
neighbor 209.165.200.225 activate	actívate
no neighbor 2001:db8.200::1 activate	active el vecino
network 2.2.2.2 mask 255.255.255.255	
network 0.0.0.0	notifique la red
exit - address-family	salida
address-family ipv6	salida
no neighbor 209.165.200.225	activate

neighbor 2001:db8::200::1 network 2001:db8:2222::128 // network ::0 exit-address-family // salida	notifique la red salida
--	----------------------------

Figura 25. Simulación BGP en R3

```
R3 con0 is now available

Press RETURN to get started.

*Nov  8 05:06:26.351: %SYS-5-CONFIG_I: Configured from console by console R3, ENCOR Skills Assessment, Scenario 1
R3#conf 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 s3/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#end
*Nov  8 05:09:16.283: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial3/0 from LOADING to FULL, Loading Done
*Nov  8 05:09:17.275: %OSPFV3-5-ADJCHG: Process 6, Nbr 209.165.200.225 on Serial3/0 from LOADING to FULL, Loading Done
R3(config)#end
```

## Código

Tabla 24. Código en R3

router-id 0.0.4.3	id del router 3
network 10.0.11.0 0.0.0.255 area 0	notificación de la red
notificación de red 11.0	
network 10.0.13.0 0.0.0.255 area 0	notificación de la red 13.0
notificación de red 13.0	
exit/ salida	
ipv6 router ospf 6	id del proceso
router-id 0.0.6.3	ide del proceso en r3 es 3
exit// salida	salida
interface g1/0	conexión router

<pre> ipv6 ospf 6 area 0 exit interface s3/0 ipv6 ospf 6 area 0 // ipv6 exit // salida end </pre>	<p>conexión al serial ipv6 Salida</p>
---	---

Figura 26. Simulación BGP en D1

```

spanning-tree vlan 101 priority 28672
spanning-tree portfast edge
D1#
D1#show run int g2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

D1#CONF 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)#passive-interface default
D1(config-router)#no passive-interface g1/1
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.
D1(config)#router-id 0.0.6.131
^
% Invalid input detected at '^' marker.
D1(config)#passive-interface default
^
% Invalid input detected at '^' marker.
D1(config)#no passive-interface g1/1
^
% Invalid input detected at '^' marker.

```

## Código

### router ospf 4

#### notificación de 4 redes

router-id 0.0.4.131

id de proceso

network 10.0.100.0 0.0.0.255 area 0

notificación de red 100.0

network 10.0.101.0 0.0.0.255 area 0

notificación de red 101.0

network 10.0.102.0 0.0.0.255 area 0	notificación de red 102.0
network 10.0.10.0 0.0.0.255 area 0	notificación de red 10.0

*Tabla 25. Todas las interfaces pasivas excepto la 1*

<pre> passive-interface default no passive-interface g1/1 exit ipv6 router ospf 6 router-id 0.0.6.131 passive-interface default  no passive-interface g1/1 exit interface g1/1 ipv6 ospf 6 area 0 exit interface vlan 100 // vlan 100 ipv6 ospf 6 area 0 exit/ interface vlan 101 //vlan 101 ipv6 ospf 6 area 0 exit interface vlan 102// vlan 102 ipv6 ospf 6 area 0 exit end </pre>	<p>para no anunciar las rutas al vecino, pero el siguiente salto si ve la ruta salida</p> <p>todas las interfaces pasivas excepto la 1</p> <p>todas las interfaces pasivas exceto la 1</p> <p>todas las interfaces pasivas excepto la 1</p> <p>todas las interfaces pasivas excepto la 1</p> <p>todas las interfaces pasivas excepto la 1</p> <p>Salida</p>
---	---

Figura 27. Simulación BGO en D2

```

banner login ^C
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
banner motd ^C D2, ENCOR Skills Assessment, Scenario 1 ^C
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
!
end

D2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#int g1/1
D2(config-if)#duplex full
^
% Invalid input detected at '^' marker.

D2(config-if)#duplex full
D2(config-if)#exit
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 g1/1
D2(config-router)# exit
D2(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.
    
```

Código

Tabla 26. Código en D2

router ospf 4 router-id 0.0.4.132	id de proceso id del router 132 notificación de 4 redes
network 10.0.100.0 0.0.0.255 area 0 network 10.0.101.0 0.0.0.255 area 0	notificación de red 100.0 notificación de red 101.0
network 10.0.102.0 0.0.0.255 area 0 network 10.0.11.0 0.0.0.255 area 0 passive-interface default no passive-interface g1/1 exit	notificación de red 102.0 notificación de red 11.0
ipv6 router ospf 6 router-id 0.0.6.132 passive-interface default no passive-interface g1/1 exit	//desactive todas las interfaces excepto 1
interface g1/ 1	Salida Interface g1/1 salida



		<ul style="list-style-type: none"> <li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li> <li>• Use el número de rastreo <b>6</b> para la IP SLA 6.</li> </ul> <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"> <li>• Use la SLA número <b>4</b> para IPv4.</li> <li>• Use la SLA número <b>6</b> para IPv6.</li> </ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 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"> <li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li> <li>• Use el número de rastreo <b>6</b> para la SLA 6.</li> </ul> <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</p>

		a Down después de 15 segundos.
--	--	--------------------------------

## Desarrollo de la tarea 4.1

En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

**(FHRP/SLA)**

**Switch D1**

*Figura 28. Validación del estado de las IP SLA y de los Track en D1*

```

D1(config-if)# standby 124 preempt
D1(config-if)# standby 124 track 4 decrement 60
D1(config-if)# standby 126 ipv6 autoconfig
D1(config-if)# standby 126 priority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60
D1(config-if)# exit
D1(config)#end
D1#
Nov  8 05:33:09.963: N5YS-5-CONFIG_I: Configured from console by console
Nov  8 05:33:11.587: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
D1#
Nov  8 05:33:15.819: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
D1#
Nov  8 05:33:21.138: %HSRP-5-STATECHANGE: Vlan101 Grp 110 state Standby -> Active
D1#
Nov  8 05:33:26.301: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby -> Active
D1#
Nov  8 05:33:29.363: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Active
D1#
Nov  8 05:33:32.612: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
D1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#ip sla sched
Nov  8 05:34:00.354: %TRACK-6-STATE: 6 ip sla 6 state Down -> Up
D1(config)#ip sla schedule 6 life forever start-time now
Cannot modify schedule. Operation may have started.

D1(config)#interface vlan 102
D1(config-if)#standby version ?
  <1-2>  Version number

D1(config-if)#standby version 2
D1(config-if)#
Nov  8 05:36:39.888: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Speak
D1(config-if)#
Nov  8 05:36:41.261: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Active -> Speak
D1(config-if)#
Nov  8 05:36:52.081: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
Nov  8 05:36:52.363: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby
D1(config-if)#

```

## Código

Tabla 28. Código en D1

<pre> ip sla 4 icmp-echo 10.0.10.1 frequency 5 // cada 5 segundos exit ip sla 6 icmp-echo 2001:db8:100:1010::1 frequency 5 exit  ip sla schedule 4 life forever start-time now  ip sla schedule 6 life-forever start-time now track 4 ip sla 4  delay down 10 up 15 exit//salida track 6 ip sla 6 delay down 10 up 15  exit// salida interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 priority 150 standby 104 preempt  standby 104 track 4 decrement 60//grupo 4 drecrementar la prioridad 60 standby 106 ipv6 autoconfig  standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 60 exit//salida interface vlan 101 standby version 2 </pre>	<pre> ipsla 4 para ipv4 ipv4 address cada 5 segundos salida isla 6 para ipv6 ipv6 address cada 5 segundos  programa sla sin termino de tiempo para ipv4 que inicie inmediato  numero track 4  retardo de caido 10 a levantado 15 salida numero track 6 retardo de caido 10 a levantado 15  salida configure el grupo 4 para la vlan 100 versión 2 HSRP grupo 4 asigne la ip virtual  grupo 4 VLAN prioridad 150  decrementar la prioridad 60 salida  asigne la ip virtual </pre>
--	--

<pre>standby 114 ip 10.0.101.254 standby 114 preempt standby 114 track 4 decrement 60 standby 116 ipv6 autoconfig standby 116 preempt standby 116 track 6 decrement 60 exit interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 priority 150 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 priority 150 standby 126 preempt standby 126 track 6 decrement 60 exit end</pre>	<pre>active preamp  decrementar 60 salida  124 para la vlan 102 versión 2 grupo 124 asigne ip virtual prioridad 150  decrementar 60  prioridad 150  dercrementar a 60  salida</pre>
---	---

## Desarrollo de la tarea 4.2

En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

*Tabla 29. Switch D2*

<pre>ip sla 4 icmp-echo 10.0.11.1 frequency exit ip sla 6 icmp-echo 2001:db8:100:1011::1 ipv6 address frequency exit//salida  ip sla schedule 4 life forever start-time now programa sla  ip sla schedule 6 life forever start-time now programa sla</pre>	<pre>ipsla 4 para ipv4 ipv4 address salida  Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4  sin termino de tiempo para ipv4 que inicie inmediato  sin termino de tiempo para ipv6 que inicie inmediato</pre>
--	--

<pre> track 4 ip sla 4  delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit interface vlan 100 standby version 2// versión 2 standby 104 ip 10.0.100.254 standby 104 preempt standby 104 track 4 decrement 60 standby 106 ipv6 autoconfig standby 106 preempt standby 106 track 6 decrement interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 priority 150 standby 114 preempt standby 114 track 4 decrement 60 standby 116 ipv6 autoconfig standby 116 priority 150 standby 116 preempt standby 116 track 6 decrement 60 exit  interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60 exit end </pre>	<pre> numero track 4  retardo de caido 10 a levantado 15 salida numero track 6 retardo de caido 10 a levantado 15 salida  interface 100 grupo 104 asigne ip virtual  decrementar prioridad 60 grupo 106 vlan 100 // autoconfiguración 60 // drecrementar la prioridad a 60 salida configure ipv6 HSRP grupo 116 ip virtual asigne // prioridad 150  drecrementar a 60 // autoconfiguración // prioridad 150  decrementar prioridad 60 salida  configure la vlan 102 para grupo 26 asigne io virtual  grupo 124 decremente la prioridad a 60 autoconfigure grupo 126 decremente la prioridad a 60 salida </pre>
--	--

### Desarrollo de la tarea 4.3

Tabla 30. Desarrollo de la tarea 4.3

<pre> interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 priority 150  standby 104 preempt  standby 104 track 4 decrement 60 standby 106 ipv6 autoconfig standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 60 exit//salida interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 preempt standby 114 track 4 decrement 60 standby 116 ipv6 autoconfig standby 116 preempt standby 116 track 6 decrement 60 exit interface vlan 102 standby version 2  standby 124 ip 10.0.102.254  standby 124 priority 150// prioridad 150 standby 124 preempt  standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 priority 150 standby 126 preempt </pre>	<pre> configure el grupo 4 para la vlan 100 versión 2 HSRP grupo 4 asigne la ip virtual grupo 4 VLAN prioridad 150  grupo 4 active preamp  grupo 4 drecrementar la prioridad 60 prioridad 150  decrementar la prioridad 60  salida  asigne la ip virtual active preamp decrementar 60 decrementar 60  124 para la vlan 102 versión 2  grupo 124  asigne ip virtual decrementar 60 Se inicia la configuración IPv6 HSRP grupo 126 para la VLAN 102. Se asigna la dirección IP virtual usando ipv6 autoconfig. </pre>
---	---

standby 126 track 6 decrement 60 exit// salida end	Se rastrea el objeto 6 y se decrementa en 60.
--	---

## Parte 5: Seguridad

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

*Tabla 31. Configuración de seguridad*

Las tareas de configuración son las siguientes: <b>Tarea#</b>	<b>Tarea</b>	<b>Especificación</b>
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: <b>sadmin</b> • Nivel de privilegio 15 • Contraseña: <b>cisco12345cisco</b>
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.: • Dirección IP del servidor RADIUS es 10.0.100.6.

		<ul style="list-style-type: none"> <li>• Puertos UDP del servidor RADIUS son 1812 y 1813.</li> <li>• Contraseña: <b>\$strongPass</b></li> </ul>
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"> <li>• Use la lista de métodos por defecto</li> <li>• Valide contra el grupo de servidores RADIUS</li> <li>• De lo contrario, utilice la base de datos local.</li> </ul>
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: <b>raduser</b> y la contraseña: <b>upass123</b> .

### Desarrollo de la tarea 5.1 Y 5.2

Todos los dispositivos:

Habilite el secreto de SCRYPT de tipo algoritmo cisco12345cisco

```
enable algorithm-type SCRYPT secret cisco12345cisco //asignamos contraseña
de tipo de algoritmo script , ciframos con secret y la contraseña es
cisco12345cisco
```

Para: R1

Para R2:

Para R3:

Para D1:

Para A1:

```
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
//creamos un usuario local con el algoritmo script
```

### Desarrollo de la tarea 5.3 Y 5.4

En todos los dispositivos (excepto r2), habilite AAA.

*Tabla 32. Tareas 5.3 y 5.4*

<pre>aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  key \$strongPass  exit// salida aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key \$strongPass exit// salida aaa authentication login default group radius local radius end</pre>	<p>activamos AAA RADIUS Sera el nombre</p> <p>asignamos la ipv4 // puerto de autenticación del 1812 a 1813</p> <p>contraseña salida</p> <p>Se especifica la dirección IP y los puertos Se especifica la dirección IP y los puertos UDP</p> <p>autenticación por defecto // validamos ante el servidor usar la base de datos local</p>
---	---

Figura 29. Asignación Scrypt Secret D1

```
-Traceback= 1DBB7C0z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 3460025z 345FF57z 7EA1DFz - Process "Per-minute Jobs", CPU hog, PC 0x03DF1567
*Nov 8 05:47:04.433: %SYS-3-CPUHOG: Task is running for (1998)msecs, more than (2000)msecs (0/0),process = Per-minute Jobs.
D1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#
```

Figura 30. Asignación Scrypt Secret D2

```
!
!
end

D2# conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)#
```

solarwinds | Solar-PuTTY free tool

Figura 31. Asignación Scrypt secret A1

```
A1#
-Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 347270Dz 348
*Nov 8 04:52:20.034: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)msec
A1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#
```

solarwinds | Solar-PuTTY free tool




Figura 32. Asignación alternativa Scrypt secret R1

```
R1(config)#
*Nov 8 06:41:17.359: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEth
R1(config)#
*Nov 8 06:42:43.455: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEth
R1(config)#
*Nov 8 06:44:10.095: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEth
R1(config)#
*Nov 8 06:45:48.214: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEth
R1(config)#
*Nov 8 06:47:12.574: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEth
R1(config)#enable secret cisco12345cisco
R1(config)#username sadmin privilege 15 secret cisco12345cisco
R1(config)#
```

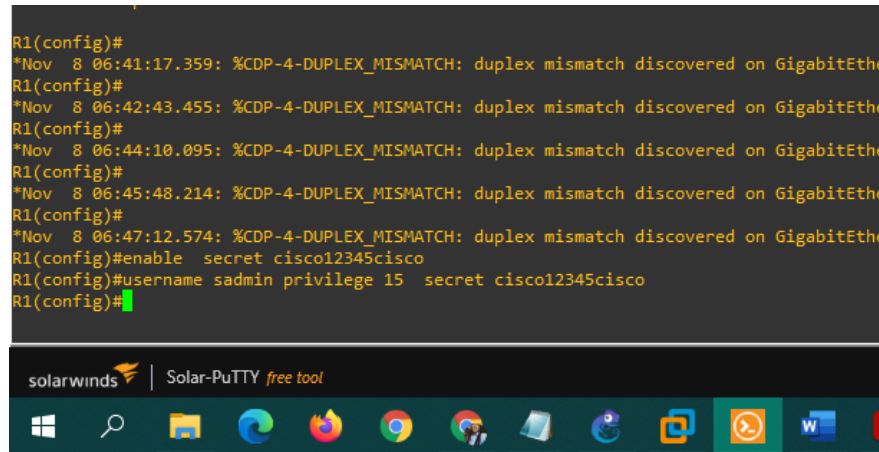


Figura 33. Asignación Scrypt Secret R2

```
L 209.165.200.226/32 is directly connected, GigabitEthernet0/0
R2#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, 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, 1 - LISP
S  ::/0 [1/0]
   via Loopback0, directly connected
C  2001:DB8:200::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:200::2/128 [0/0]
   via GigabitEthernet0/0, receive
LC 2001:DB8:2222::1/128 [0/0]
   via Loopback0, receive
L  FF00::/8 [0/0]
   via Null0, receive
R2#CONF TERM
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret cisco12345cisco
R2(config)#username sadmin privilege 15 secret cisco12345cisco
```

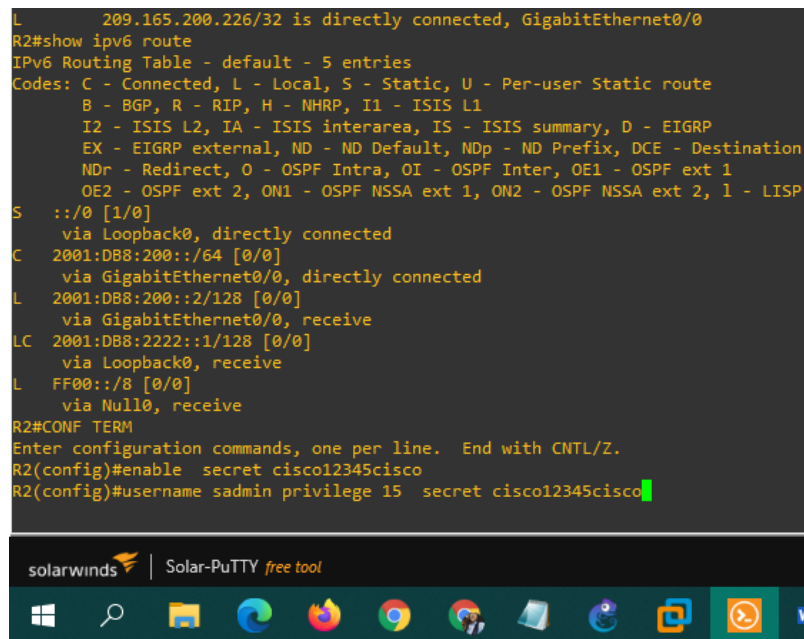


Figura 34. Asignación Scrypt Secret D1

```

R2#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, 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 - LIS
S    ::0 [1/0]
    via Loopback0, directly connected
C    2001:DB8:200::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L    2001:DB8:200::2/128 [0/0]
    via GigabitEthernet0/0, receive
LC   2001:DB8:2222::1/128 [0/0]
    via Loopback0, receive
L    FF00::/8 [0/0]
    via Null0, receive
R2#CONF TERM
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret cisco12345cisco
R2(config)#username sadmin privilege 15 secret cisco12345cisco

```

### Desarrollo de la tarea 5.5 y 5.6

En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

Tabla 33. Tareas 5.5 y 5.6

<pre> aaa new-model radius server RADIUS  address ipv4 10.0.100.6 auth-port  1812 acct-port 1813  key \$strongPass  exit aaa authentication login default group  radius local end </pre>	<p>servidor RADIUS</p> <p>Se asigna la contraseña al servidor RADIUS</p> <p>Se especifica la dirección IP y los puertos UDP</p> <p>Salida</p>
--	---



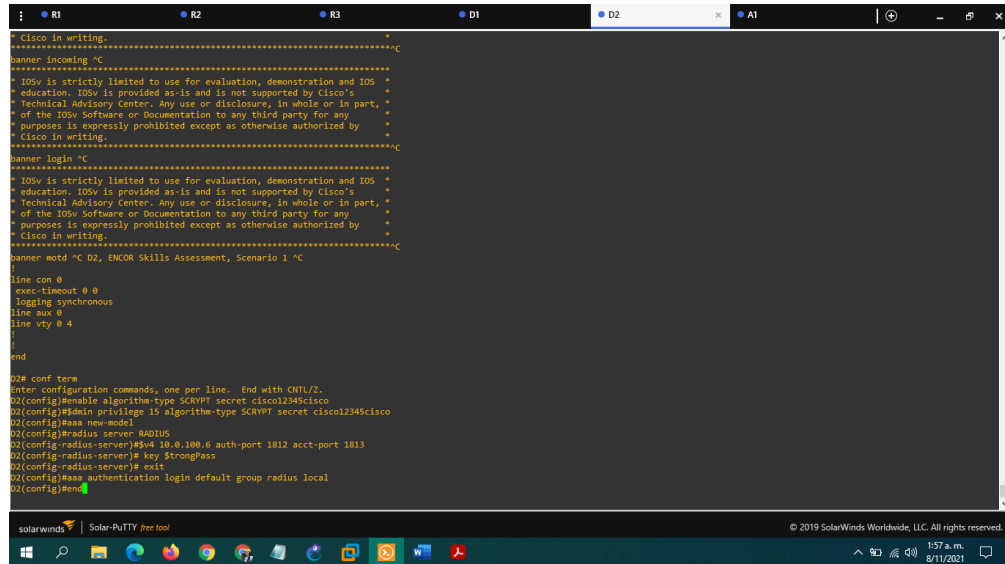
D1

Figura 37. Se habilitó AAA, se configuraron las especificaciones del servidor RADIUS y se configuró la lista de métodos de autenticación AAA.

```
Cannot modify schedule. Operation may have started.
D1(config)#interface vlan 100
D1(config-if)#standby version 7
  <-1-2> Version number
D1(config-if)#standby version 2
D1(config-if)#
Nov  8 05:16:19.000: NSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Speak
D1(config-if)#
Nov  8 05:16:41.261: NSRP-5-STATECHANGE: Vlan101 Grp 116 state Active -> Speak
D1(config-if)#
Nov  8 05:16:52.001: NSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
Nov  8 05:16:52.261: NSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby
D1(config-if)#end
D1#
Nov  8 05:43:43.536: NQVS-5-COMP2G_1: Configured from console by console
D1#show standby brief
      P Indicates configured to preempt.
      S indicates standby is suppressed.
Interface  Grp  Pri  P  State  Active      Standby      Virtual IP
-----
V1100     104  150  P  Active  local      FE80::0212  10.0.100.254
V1100     106  150  P  Active  local      FE80::0212  FE80::573FF:FEA0:6A
V1101     114  100  P  Standby 10.0.101.2 local      10.0.101.254
V1101     116  100  P  Standby FE80::0213 local      FE80::573FF:FEA0:74
V1102     124  150  P  Active  local      10.0.102.2  10.0.102.254
V1102     126  150  P  Active  local      FE80::0214  FE80::573FF:FEA0:7E
V1103
-Traceback- ID007C0: 800FE5: 90522E: 904F50: 90405D: 900F45: 90187B: 90180F: 3460025: 345FF57: 7EA1DF: - Process "Per-minute Jobs", CPU hog, PC 0x030F1567
Nov  8 05:47:04.413: NQVS-3-CPUK00: Task is running for (1998)secs, more than (2000)secs (0/0),process = Per-minute Jobs.
D1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#admin 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 $trongpass
D1(config-radius-server)#exit
D1(config)#aaa authentication login default group radius local
D1(config)#end
```

D2

Figura 38. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA



```

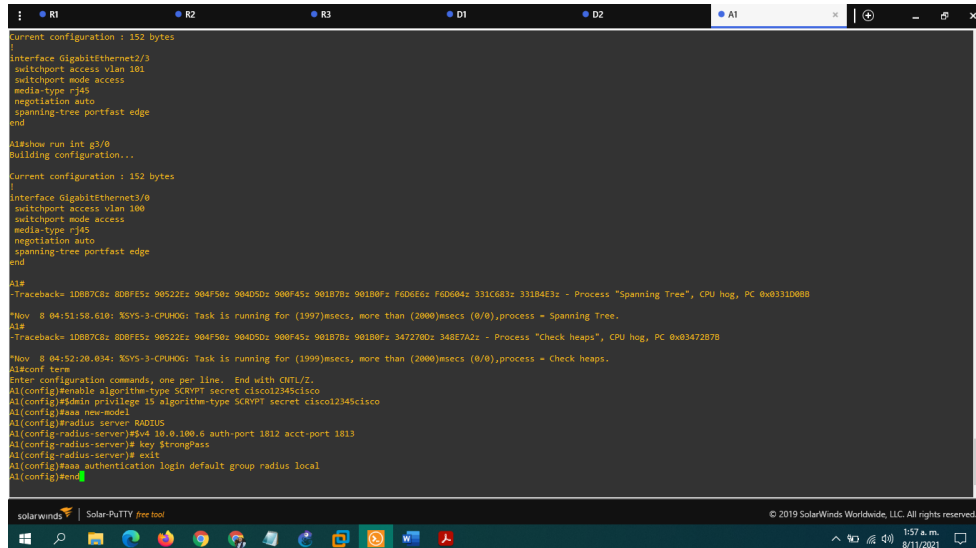
Cisco in writing.
*****
banner incoming ^C
*****
IOSv is strictly limited to use for evaluation, demonstration and IOS
education. IOSv is provided as-is and is not supported by Cisco's
Technical Advisory Center. Any use or disclosure, in whole or in part,
of the IOSv Software or Documentation to any third party for any
purpose is expressly prohibited except as otherwise authorized by
Cisco in writing.
*****
banner login ^C
*****
IOSv is strictly limited to use for evaluation, demonstration and IOS
education. IOSv is provided as-is and is not supported by Cisco's
Technical Advisory Center. Any use or disclosure, in whole or in part,
of the IOSv Software or Documentation to any third party for any
purpose is expressly prohibited except as otherwise authorized by
Cisco in writing.
*****
banner motd ^C D2, ENCOR Skills Assessment, Scenario 1 ^C
*****
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 4
!
end

D2# conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#enable algorithm-type SCVPV1 secret cisco12345cisco
D2(config)#admin privilege ls algorithm-type SCVPV1 secret cisco12345cisco
D2(config)#aaa new-model
D2(config)#radius server R00100
D2(config-radius-server)#sv 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

```

D3

Figura 39. Se habilitó AAA, se configuraron las especificaciones del servidor RADIUS y se configuró la lista de métodos de autenticación AAA.



```

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

A1#show run int g3/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet3/0
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

A1#
-Traceback- 1D8D7C8: 8D8FE5: 90522E: 904F50: 90405D: 900F45: 90107B: 90100F: F6D66E: F6D66E: 331C63: 33104E3: - Process "Spanning Tree", CPU hog, PC 0x031100B0
Nov  8 04:51:58.618: XSYS-3-CPUHOG: Task is running for (1997)usecs, more than (2000)usecs (0/0),process = Spanning Tree.
A1#
-Traceback- 1D8D7C8: 8D8FE5: 90522E: 904F50: 90405D: 900F45: 90107B: 90100F: 347270D: 348E7A2: - Process "Check heaps", CPU hog, PC 0x03472070
Nov  8 04:52:20.034: XSYS-3-CPUHOG: Task is running for (1999)usecs, more than (2000)usecs (0/0),process = Check heaps.
A1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#enable algorithm-type SCVPV1 secret cisco12345cisco
A1(config)#admin privilege ls algorithm-type SCVPV1 secret cisco12345cisco
A1(config)#aaa new-model
A1(config)#radius server R00100
A1(config-radius-server)#sv 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $StrongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#end

```

Figura 40. Verificación de acceso en R1

```
R1 con0 is now available

Press RETURN to get started.

R1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
```

Usuario y contraseña : sadmin – cisco12345cisco

### Parte 6: Configure las funciones de administración de red

Tabla 34. Configuración de funciones de 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"> <li>• R1 debe sincronizar con R2.</li> <li>• R3, D1 y A1 para sincronizar la hora con R1.</li> <li>• D2 para sincronizar la hora con R3.</li> </ul>
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"> <li>• Únicamente se usará SNMP en modo lectura (Read-Only).</li> <li>• Limite el acceso SNMP a la dirección IP de la PC1.</li> <li>• Configure el valor de contacto SNMP con su nombre.</li> <li>• Establezca el <i>community string</i> en <b>ENCORSA</b>.</li> <li>• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.</li> <li>• En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>.</li> <li>• En A1, habilite el envío de <i>traps config</i>.</li> </ul>

### Desarrollo de la tarea 6.1, 6.2, 6.3, 6.4 y 6,5

**//Configure el reloj local a la hora UTC actual.**

Clock set 13:00:00 29 october 2021 // configuración reloj

Figura 41. Configuración del reloj local a la hora UTC actual

```

GigabitEthernet1/1 (half duplex).
R1(config)#Clock set 13:00:00 29 october 2021
*Nov  8 07:25:02.718: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/0 (not half duplex), with D1 Gi
gabitEthernet1/1 (half duplex).
R1(config)#Clock set 13:00:00 29 october 2021

```

Tabla 35. Código configuración Router R2 y Router R1

<p><b>Router R2:</b>  ntp master 3  stratum nivel 3  end</p> <p><b>Router R1:</b>  ! enable and enter password</p> <p>ntp server 2.2.2.2  logging trap warning  logging host 10.0.100.5  logging on  ip access-list standard SNMP-NMS  permit host 10.0.100.5  exit</p> <p>snmp-server contact Cisco Student  snmp-server community ENCORSA ro  SNMP-NMS  snmp-server host 10.0.100.5 version  2c ENCORSA</p> <p>snmp-server ifindex persist  snmp-server enable traps bgp  snmp-server enable traps config</p>	<p>configuración en r2  Se configura R2 como NTP maestro en el nivel de estrato 3.</p> <p>loopback en r2 para sincronizar  Configure Syslog</p> <p>active login  lista de acceso  permitir solo al pc 1  salida</p> <p>creamos la comunidad ENCORSA</p> <p>host pc1 con la versión y la comunidad</p> <p>habilite el envío de <i>traps bgp, config, y ospf.</i></p>
---	---

Tabla 36. Código Router R3

<pre> ntp server 10.0.10.1 logging trap warning logging host 10.0.100.5 logging on  ip access-list standard SNMP-NMS   permit host 10.0.100.5  exit // salida snmp-server contact Cisco lina medina snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA//  snmp-server ifindex persist snmp-server enable traps config snmp-server enable traps ospf end// salida </pre>	<p>sincroniza con r1 Configure Syslog</p> <p>active login</p> <p>lista de acceso</p> <p>permitir solo a la pc 1</p> <p>servidor de contacto se establece el "community string" en encorsa y se especifica el uso de snmpv2 como solo lectura. host pc1 con la versión y la comunidad</p> <p>se habilita el envío de traps: config, y ospf</p>
---	---

Figura 42. Verificación de la configuración R3

```

NOV  8 07:31:12.778: %SYS-5-CONFIG_I: Configured from console by console
R3#Clock set 13:00:00 29 october 2021
R3#
*Oct 29 13:00:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 07:31:17 UTC
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# ntp server 10.0.10.1
R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
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 contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end

```

Tabla 37. Switch D1

<pre> ntp server 10.0.11.1 logging trap warning  logging host 10.0.100.5 logging on// active login ip access-list standard SNMP- NMS//lista de acceso permit host 10.0.100.5 exit// salida  snmp-server contact Lina medina  snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA  snmp-server ifindex persist snmp-server enable traps config snmp-server enable traps ospf end </pre>	<pre> sincronice r3 Configure Syslog  Se limita el acceso SNMP a la dirección IP  permitir solo a la pc 1  creamos la comunidad ENCORSA // servidor de contacto  // solo lectura  // host pc1 con la versión y la comunidad </pre>
---	--

Tabla 38. Switch D2

<pre>ntp server 10.0.10.1 logging trap warning  logging host 10.0.100.5 logging on ip access-list standard SNMP-NMS permit host 10.0.100.5 exit// salida  snmp-server contact Cisco lina medina snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA snmp-server enable traps config snmp-server enable traps ospf end</pre>	<pre>// sincronice con r1 // Configure Syslog  // active login  //lista de acceso  //permitir solo a la pc 1 // creamos la comunidad ENCORSA // servidor de contacto  // host pc1 con la versión y la comunidad</pre>
--	---

Figura 43. Verificación de la configuración de NTP en los equipos

```

line vty 0 4
!
end

D2# conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#enable algorithm-type SCRIPT secret cisco12345cisco
D2(config)#admin privilege 15 algorithm-type SCRIPT secret cisco12345cisco
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#sv4 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
-Traceback- 10B87C8z 8DBFE5z 90522Ez 904F50z 90405Dz 900F45z 90187Bz 90180Fz 345FFC7z 7EA1DFz - Process "Per-minute Jobs", CPU hog, PC 0x0347E990
*Nov  8 06:10:52.540: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (0/0),process = Per-minute Jobs.
D2(config)#end
D2#clock set 13:00:00 29 october 2021
*Nov  8 06:20:48.262: %SYS-5-CONFIG_I: Configured from console by console
D2#clock set 13:00:00 29 october 2021
D2#co
*Oct 29 13:00:00.003: %SYS-6-CLOCKUPDATE: System clock has been updated from 06:24:48 UTC Mon Nov 8 2021 to 13:00:00 UTC Fri Oct 29 2021, configured from console by console.nf
D2#co
Enter configuration commands, one per line. End with CNTL/Z.
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 Student
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 config
^
% Invalid input detected at '^' marker.
D2(config)# snmp-server enable traps ospf

```

Tabla 39. Switch A1

<pre> ntp server 10.0.10.1 logging trap warning logging host 10.0.100.5 logging on ip access-list standard SNMP-NMS permit host 10.0.100.5 exit// salida  snmp-server contact Cisco lina medina snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA  snmp-server ifindex persist </pre>	<pre> sincronice con r1 Configure Syslog  active login lista de acceso permitir solo a la pc 1 Salida creamos la comunidad ENCORSA servidor de contacto  host pc1 con la versión y la comunidad </pre>
--	--

<pre>snmp-server enable traps config snmp-server enable traps ospf end</pre>	<p>En A1, habilite el envío de <i>traps config</i>.</p>
--	---

Figura 44. Verificación de la configuración en A1

```

R1 R2 R3 D1 D2 A1
-Traceback= 10B87C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 90187Bz 90180Fz F6D664z F6D604z 331C683z 331B4E3z - Process "Spanning Tree", CPU hog, PC 0x0331D008
*Nov  8 04:51:58.610: %SYS-3-CPUHOG: Task is running for (1997)msecs, more than (2000)msecs (0/0),process = Spanning Tree.
A1#
-Traceback= 10B87C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 90187Bz 90180Fz 347270Dz 348E7A2z - Process "Check heaps", CPU hog, PC 0x03472B7B
*Nov  8 04:52:20.034: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)msecs (0/0),process = Check heaps.
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#enable algorithm-type SCRIPT secret cisco12345cisco
A1(config)#sdm privilege 15 algorithm-type SCRIPT secret cisco12345cisco
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#sv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $StrongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#end
A1#clock set 13:00:00 29 october 2021
*Nov  8 06:28:20.901: %SYS-5-CONFIG I: Configured from console by console
A1#clock set 13:00:00 29 october 2021
A1#
*Oct 29 13:00:00.004: %SYS-6-CLOCKUPDATE: System clock has been updated from 06:28:42 UTC Mon Nov 8 2021 to 13:00:00 UTC Fri Oct 29 2021, configured from console by console.
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
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 Student
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 config
^
% Invalid input detected at '^' marker.
A1(config)# snmp-server enable traps ospf
A1(config)#end

```

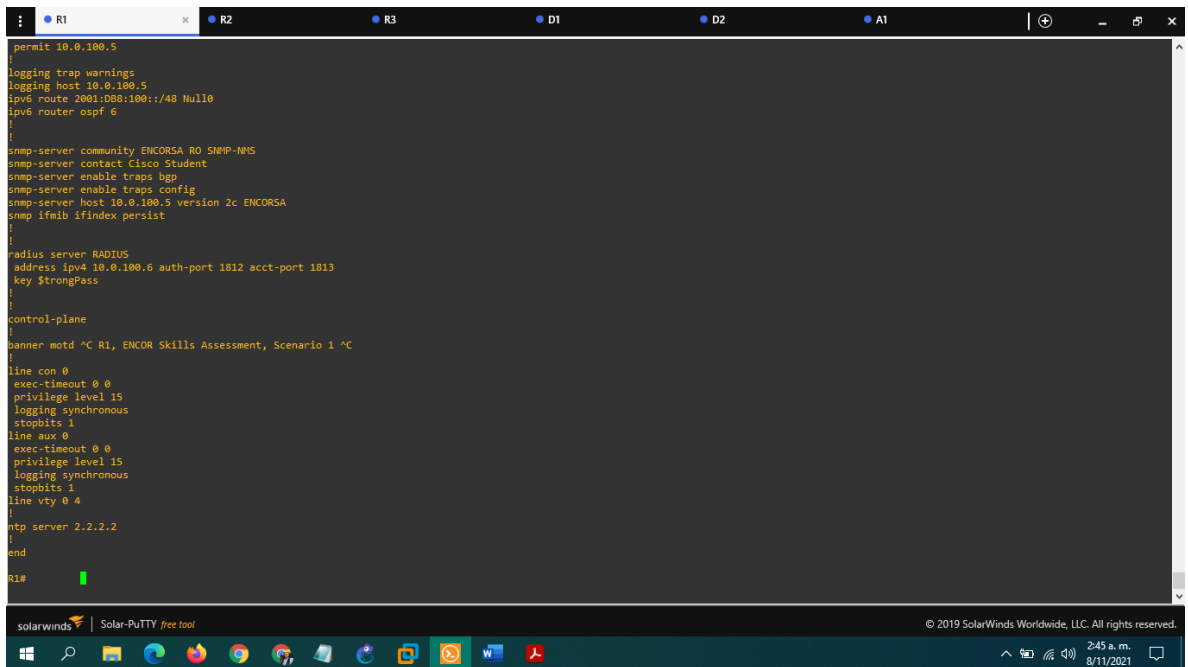
solarWinds Solar-PUTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 2:42 a. m. 8/11/2021

## Verificaciones

Router R1

R1# show run

Figura 45. Verificación en R1 #show run



```

R1# show run
permit 10.0.100.5
!
logging trap warnings
logging host 10.0.100.5
ipv6 route 2001:DB8:100::/48 Null0
ipv6 router ospf 6
!
!
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
!
!
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $StrongPass
!
!
control-plane
!
banner motd ^C R1, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
!
ntp server 2.2.2.2
!
end
R1#
```

## CONCLUSIONES

Para finalizar, en el desarrollo del presente trabajo se evidencia como es la topología de la red y los componentes que tienen, como se fraccionan según su tamaño, y sus características propias según como sea el modelo de conexión físico y/o inalámbrico, igual ambos tienen la misma función que es la transmisión de datos que viajan dentro de la red.

Por otro lado, se pudo comprender que el protocolo RSTP (Rapid Spanning Tree Protocol) es el encargado de detectar las topologías de red para proporcionar una convergencia más rápida y para crear una red sin los loops. Esto es la más eficaz cuando la topología de red es naturalmente árbol estructurado.

De igual importancia, se pudo evidenciar que el fraccionamiento de la red en redes más pequeñas, usando las soluciones VLSM y redes locales virtuales (Vlans), es una necesidad imperiosa para evitar un tráfico innecesario de red, permitir un uso eficiente del ancho de banda hacia todas las localidades remotas y poder disponer de una infraestructura eficiente, escalable y segura.

Por último, en el presente trabajo titulado "prueba de habilidades técnicas" se pudo dar solución a los escenarios propuestos de las configuraciones indicadas al diplomado CCNP, ejecutadas en el programa de simulación asignado que arrojó las

imágenes de las configuraciones de cada escenario según los requerimientos que estos tenían.

## BIBLIOGRAFIA

Temática: Overlay Tunnels

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Overlay Tunnels. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Wireless Signals and Modulation

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Signals and Modulation. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Wireless Infrastructure

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Infrastructure. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Understanding Wireless Roaming and Location Services

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Understanding Wireless Roaming and Location Services. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Authenticating Wireless Clients

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Troubleshooting Wireless Connectivity

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Troubleshooting Wireless Connectivity. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Enterprise Network Architecture

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Fabric Technologies

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Fabric Technologies. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Network Assurance

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Assurance. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Secure Access Control

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Network Device Access Control and Infrastructure Security

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Virtualization

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Virtualization. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Foundational Network Programmability Concepts

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Temática: Introduction to Automation Tools

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Introduction to Automation Tools. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUqUBthk8>