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
INGENERIA 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. Confuguración básica Router R3.....26
Figura 11. Configuración básica del SWITCH D1.....28
Figura 12. Configuración básica del SWITCH D2.....32
Figura 13. Configuracion 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. Verificacion 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 área networks), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuentos 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 construyo 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 configuro 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.

DESARROLLO

Figura 1. Escenario propuesto (Topología de red).

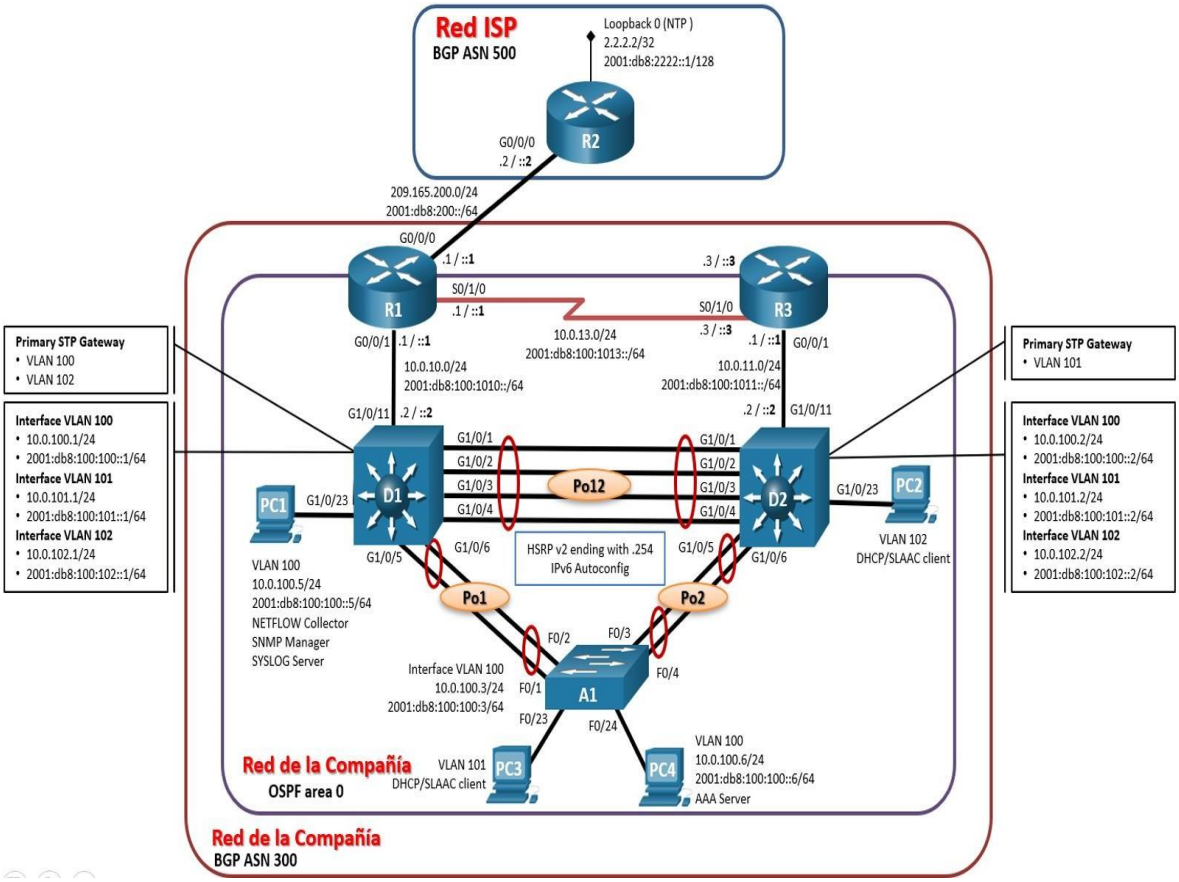


Tabla 1. Tabla de direccionamiento

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 Compañia" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

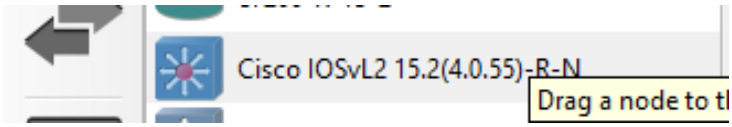
Nota: Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, 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.

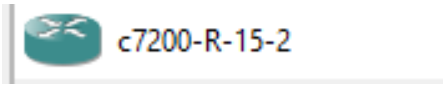
Recursos necesarios

Figura 2. Recursos necesarios



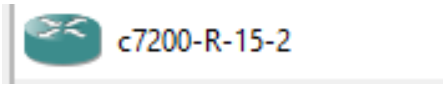
• 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

Figura 3. Switch Cisco 3650



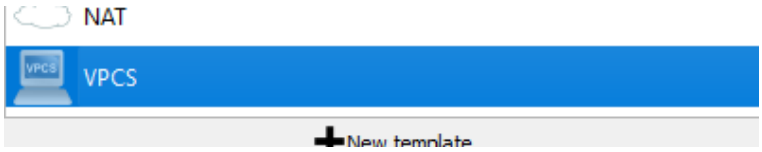
• 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

Figura 4. Switch Cisco 2960



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

Figura 5. PCs

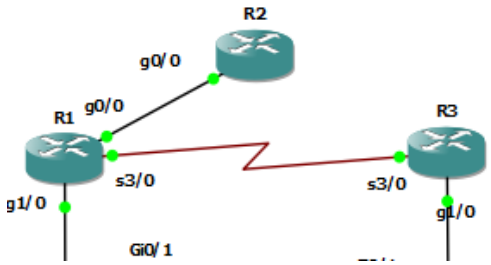


• 4 PCs (utilice el programa de emulación de terminal)

• 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

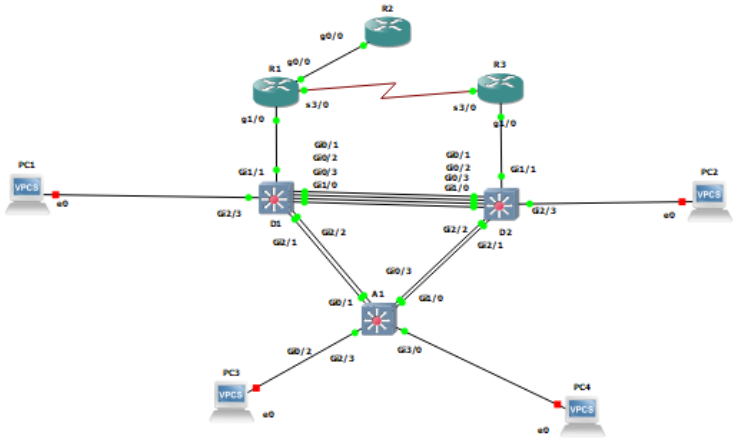


Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

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.

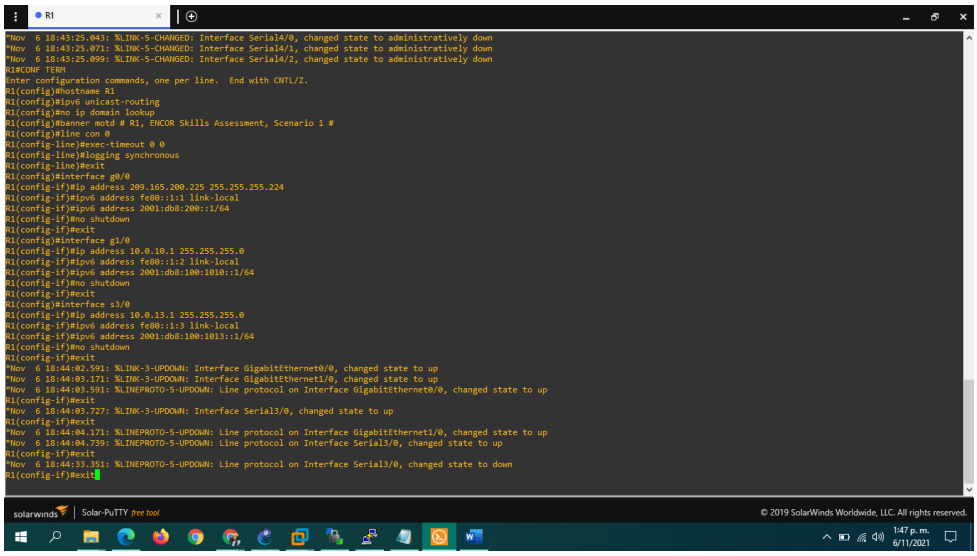
Figura 7. Cablear la red como se muestra en la topología



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Figura 8. Configuración básica Router R1



Código hecho Router R1

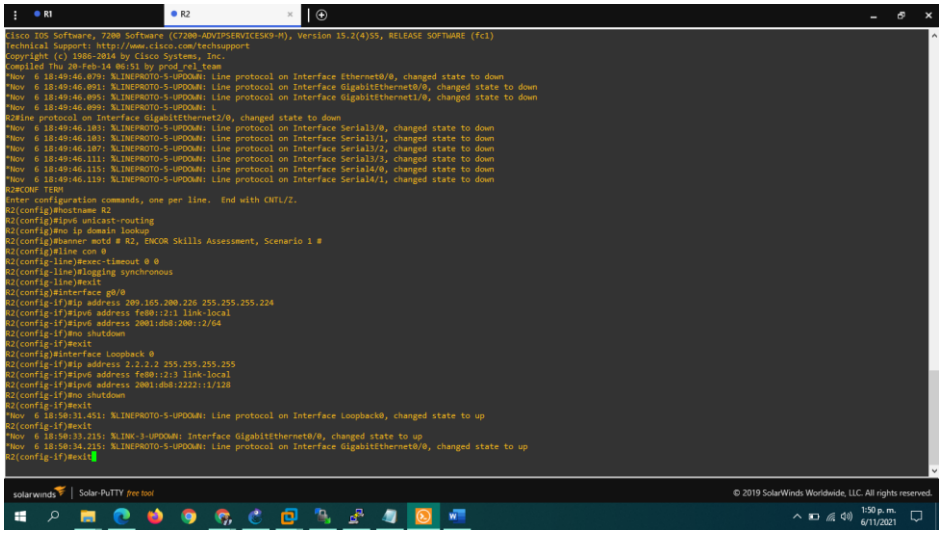
Tabla 2. Código Router R1

Switch enable Switch configure terminal	(en) entramos al modo priveligiado enable conf term // configuracion global
Router R1 hostname R1	}router R1 asignamos nombre de dispositivo al router
ipv6 unicast-routing	este comando es necesario antes de poder configurar cualquier protocolo de routing IPv6.
	desactivamos la traducción de nombres

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

ipv6 address fe80::1:3 link-local ipv6 address 2001:db8:100:1013::1/64 no shutdown exit	 direccion ipv6 habilita la interfaz salida

Figura 9. Configuración básica Router R2



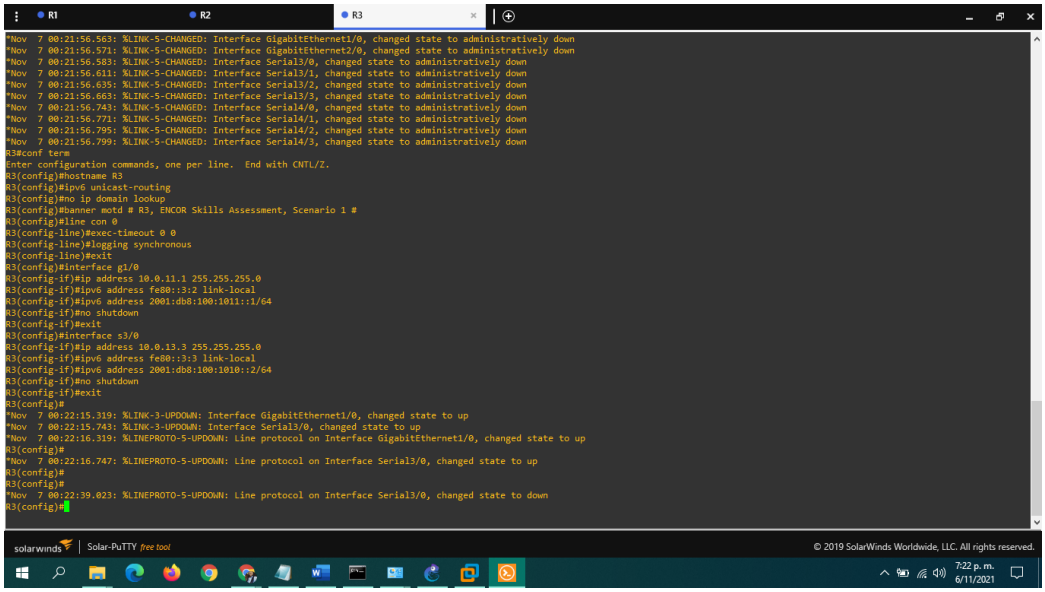
Código hecho Router R2

Tabla 3. Código Router R2

Router R2 Switch en Switch conf ter hostname R2 ipv6 unicast-routing	Configuracion en router R2 entramos al modo proveligiado configuracion global del router asignamos al dispositivo un nombre asignamos este comando que es necesario antes de poder configurar cualquier protocolo de routing IPv6.

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

Figura 10. Confuguración básica Router R3



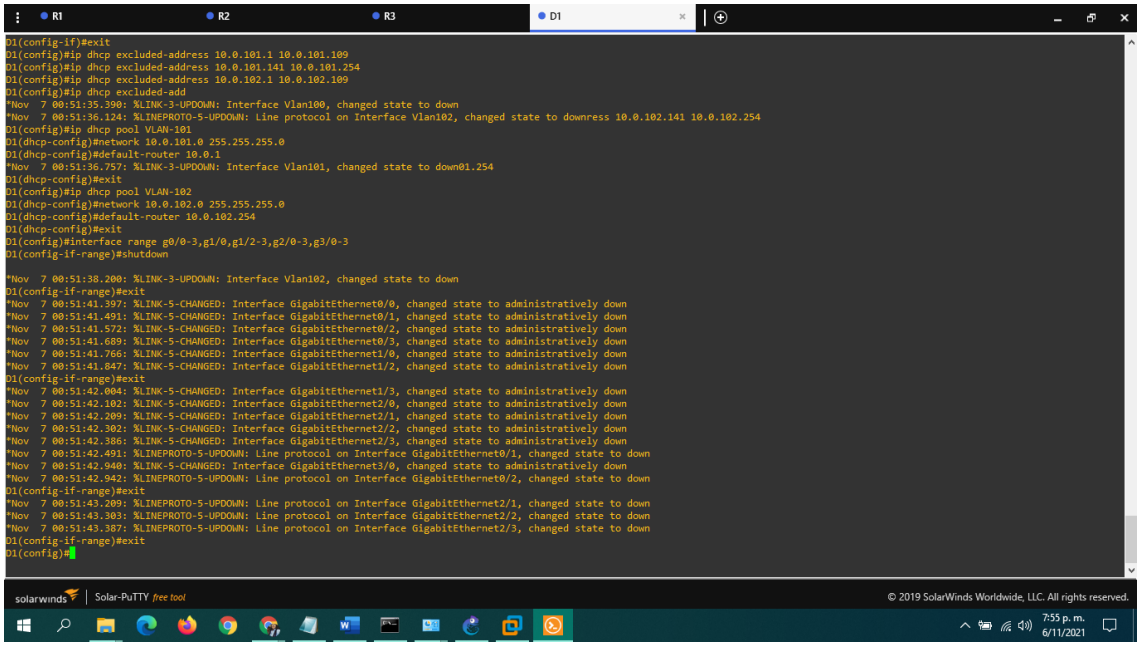
Código hecho Router R3

Tabla 4. Código Router R3

Router R3 Switch enable Switch conf term	Configuracion en el router R3 Entramos al modo priveligiado configuracion global
hostname R3	asigamos al dispositivo un nombre
ipv6 unicast-routing	este comando es necesario antes de poder configurar cualquier protocolo de routing IPv6
no ip domain lookup	Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
	Cree un aviso

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

Figura 11. Configuración básica del SWITCH D1



Código hecho Switch D1

Tabla 5. Código Switch D1

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

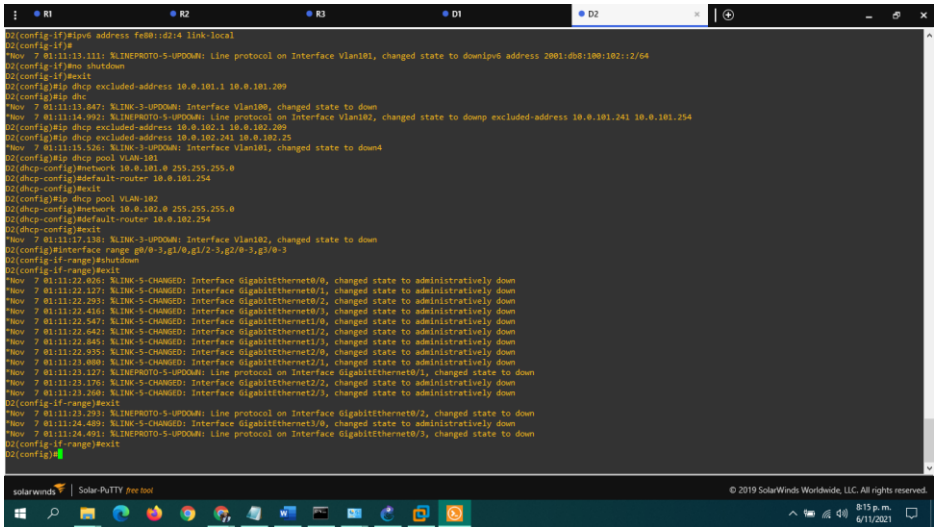
	Cree un aviso
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	
line con 0	Configure la linea de la consola
exec-timeout 0 0	Se asigna para que el tiempo en la consola 0 no se agote
logging synchronous	evitar que nos muentres mensajes inesperados configuracion de linea de consola
exit	salida
vlan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

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

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

Figura 12. Configuración básica del SWITCH D2



Codigo hecho configuración Switch D2

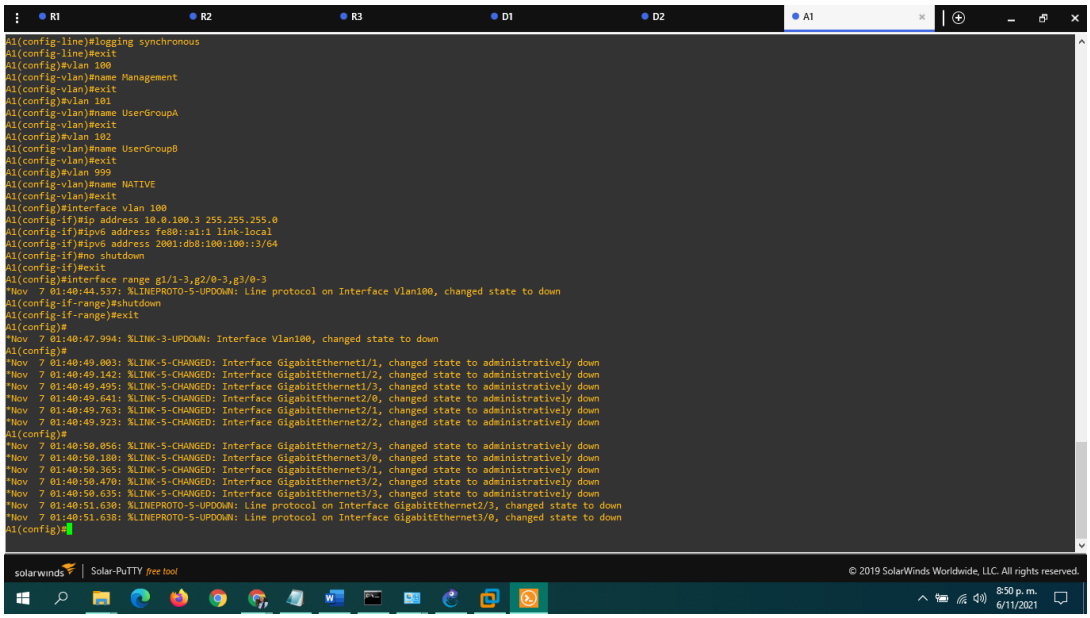
Tabla 6. Código Switch D2

Switch D2	Configuracion en switch D2
hostname D2	asignamos el nombre del dispositivo del switch
ip routing	habilite el routing ipv4
ipv6 unicast-routing	habilite el routing ipv6
no ip domain lookup	se habilita la traduccion del nombre a direccion basado en el DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	cree un aviso
line con 0	configure la linea de consola
exec-timeout 0 0	no se agotara el tiempo de espera en la consola 0 en el puerto
logging synchronous	evite mensajes inesperados
exit	salida
vlan 100	asignacion de ip a vlan
name Management	asigne el nombre del host del dispositivo
exit	salida
vlan 101	configure la vlan 101
name UserGroupA	asigne nombre el grupo
exit	salida
vlan 102	configure la vlan 102
name UserGroupB	asigne nombre del grupo
exit	salida
vlan 999	configure la vlan 999
name NATIVE	asigne nombre
exit	salida
interface g1/1	configure la interfaz
no switchport	aporte capacidad a la interfaz de capa 3
	asigne direccion ipv4 y mascara subred

ip address 10.0.11.2 255.255.255.0 ipv6 address fe80::d1:1 link-local	asigne direccion ipv6 en link local y siga la direccion
ipv6 address 2001:db8:100:1011::2/64	se asigna la dirección ipv6
no shutdown exit	habilite la interfan vlan 102 salida interfaces 100,101,102
interface vlan 100 ip address 10.0.100.2 255.255.255.0	configure la vlan 100 se asigna la dirección ipv4 y la mascara subred
ipv6 address fe80::d2:2 link-local	se asigna la dirección 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	asignamos la dirección ipv6 salida configuramos en la vlan 101 asignamos la dirección ipv4 y la mascara subred
ipv6 address fe80::d2:3 link-local	asignamos dirección 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	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
ipv6 address 2001:db8:100:102::2 /64	direccion ipV6 asignada

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

Figura 13. Configuracion básica del SWITCH A1



Codigo hecho Switch A1

Tabla 7. Código Switch A1

Switch A1 Switch en Switch conf term hostname A1 no ip domain lookup banner motd # A1, ENCOR Skills Assessment, Scenario 1 # linea de consola line con 0 exec-timeout 0 0 logging synchronous	Configuracion en switch A1 modo enable modo de configuracion asigne el nombre habilte la traduccion del nombre en la direccion basada en DNS del host cree un aviso y configure la linea de consola en este puerto consola 0 no s egota el tiempo evitar que nos muentres mensajes inesperados configuracion de linea de consola

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

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: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	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: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 D2 a A1 – Port channel 2

2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 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 chennel-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

2.6switchport access vlan 100

2.6spanning-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 raiz 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

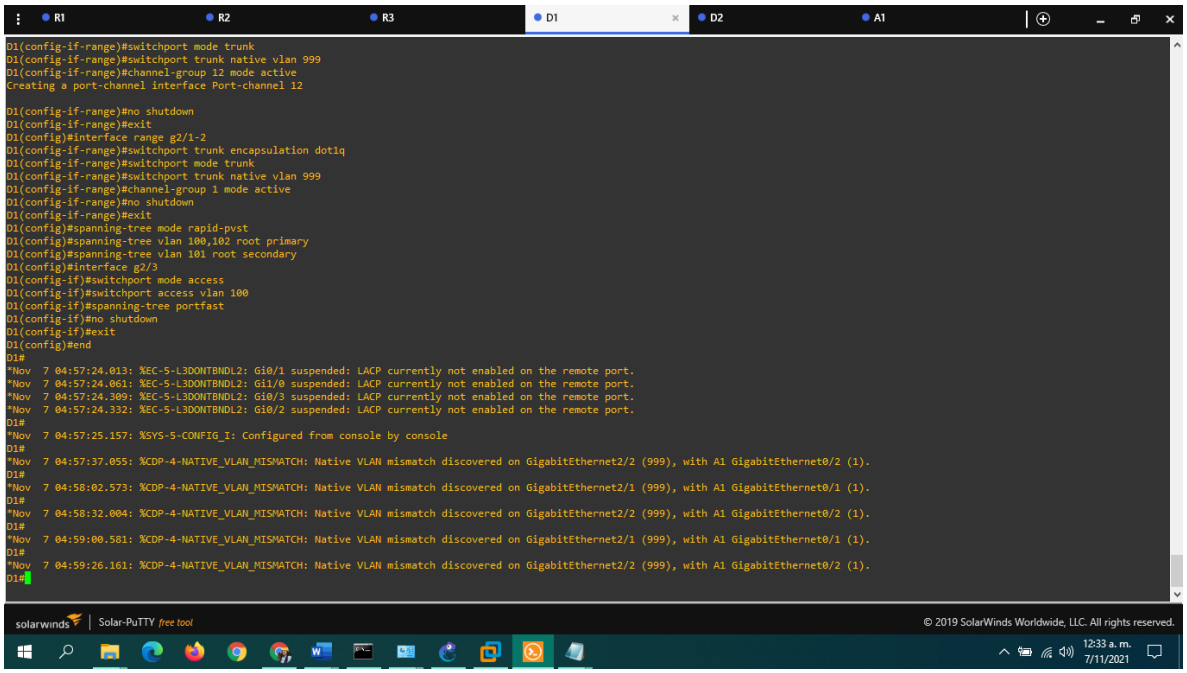
end

Código desarrollado D1

Tabla 9. Código desarrollado D1

Switch D1	
interface range g0/1-3,g1/0 switchport trunk encapsulation dot1q switchport mode trunk	enlace troncal 1 a 4 para que sea troncal
switchport trunk native vlan 999 channel-group 12 mode active active	configure los puertos de acceso de host
no shutdown exit	encender y asegurar que el rango de las interfaces este activado salida
interface range g2/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 999 channel-group 1 mode active	configuración de los puertos de acceso host
no shutdown exit	encender y asegurar que el rango de las interfaces este activado salida
spanning-tree mode rapid-pvst	ayuda a que la transición sea inmediata
no shutdown spanning-tree vlan 100,102 root primary	encender y asegurar que el rango de las interfaces este activado salida
spanning-tree vlan 101 root secondary interface g2/3 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end	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

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



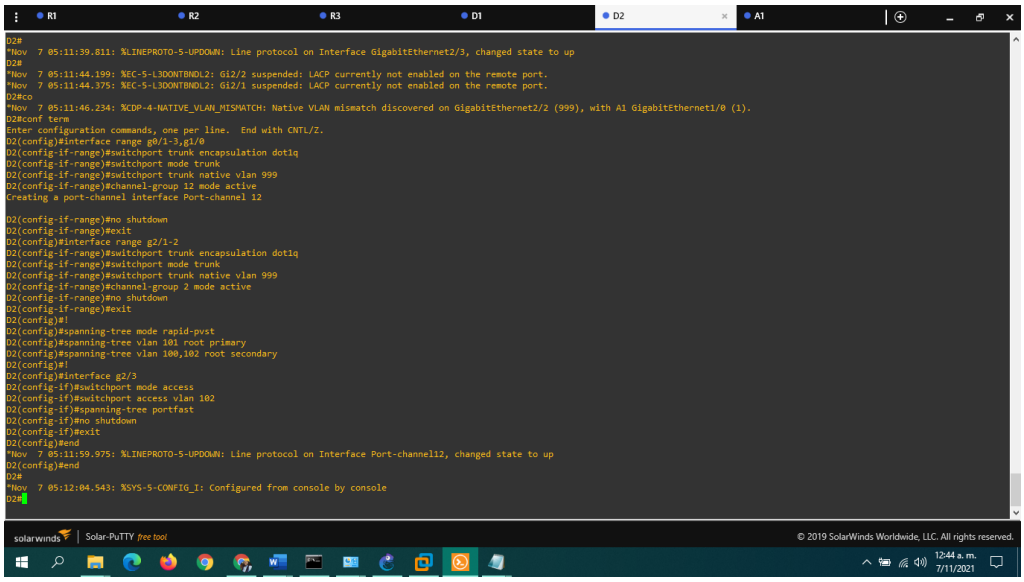
Código desarrollado D2

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	
	configure los puertos de acceso del host
	se activa el protocolo LACP de manera incondicional
no shutdown	

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	configure la terminal se activa el modo trunk se activa en modo trunk configure los puertos de acceso del host salida Se ejecuta en el modo de configuración global para configurar el conmutador para usar el protocolo compatible 802.1wy rápido por VLAN 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 enlace troncal modo de acceso ayuda a que la transición sea inmediata salida

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



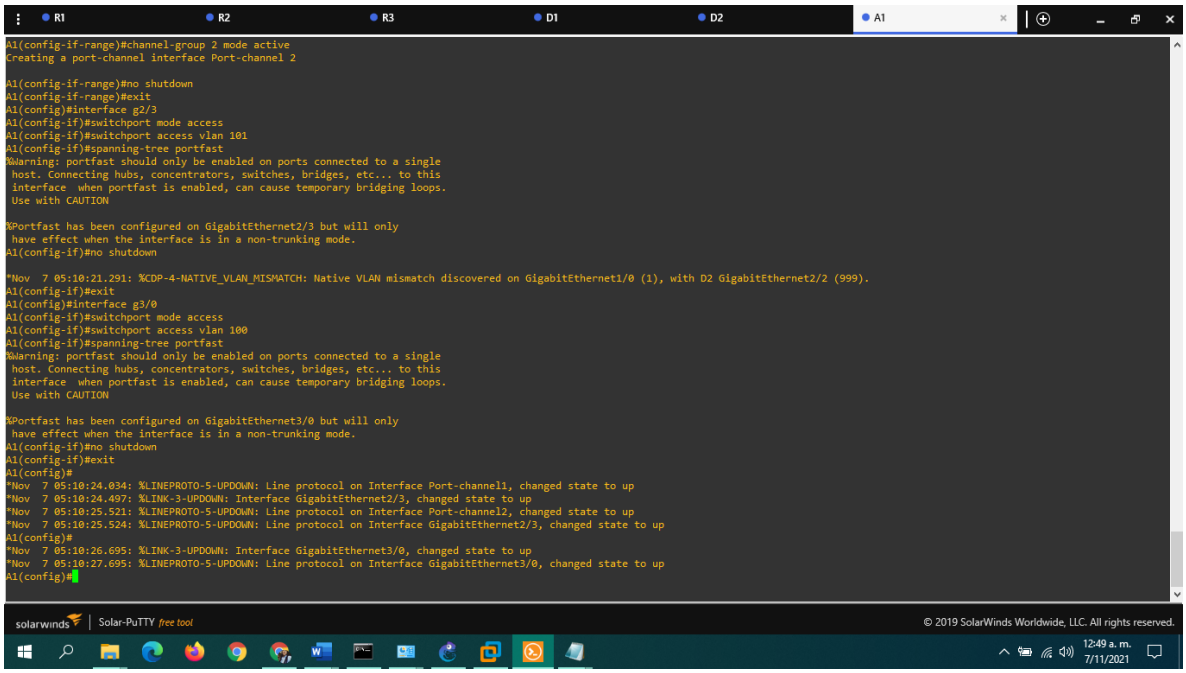
Código desarrollado A1

Tabla 11. Código desarrollado A1

Switch A1	
switch A1 spanning-tree mode rapid-pvst Spanning Tree. interface range g0/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 999 channel-group 1 mode active	 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 para que se troncal encender y asegurar que el rango de las interfaces este activado

no shutdown exit// salida	 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	 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

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



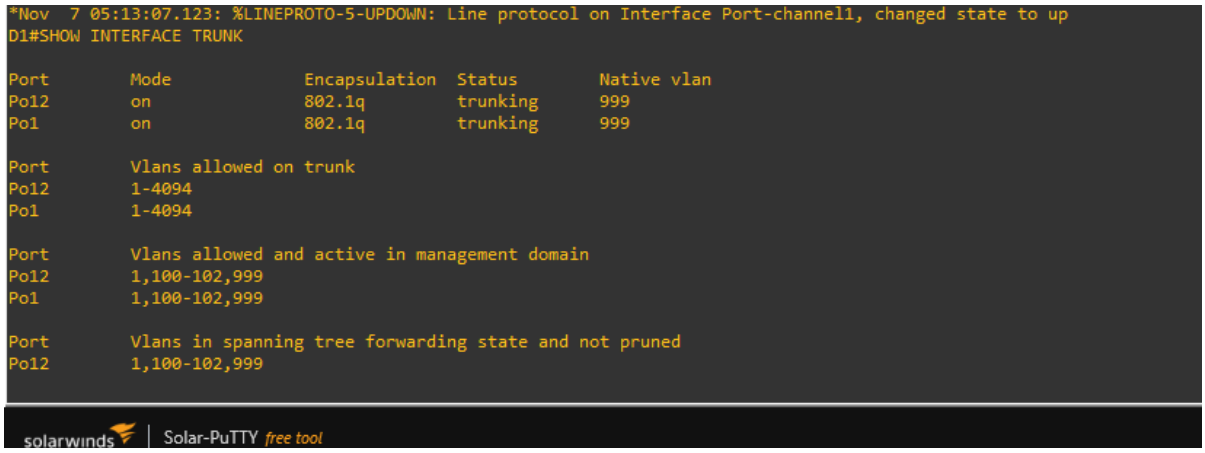
-2.7 y 2.8

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

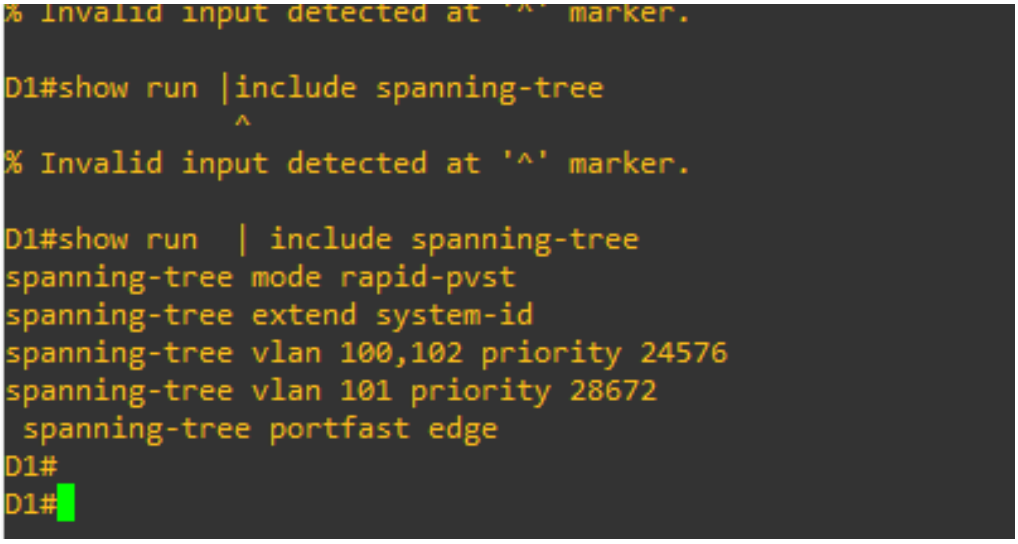
Figura 17. verificación con el comando show interface trunk



SHOW RUN | INCLUDE SPANNING-TREE

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

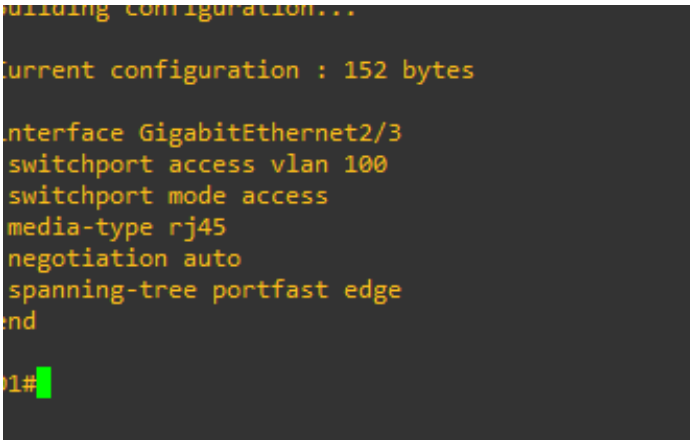
Figura 18. Verificación con el comando Show run | include spanning-tree



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.

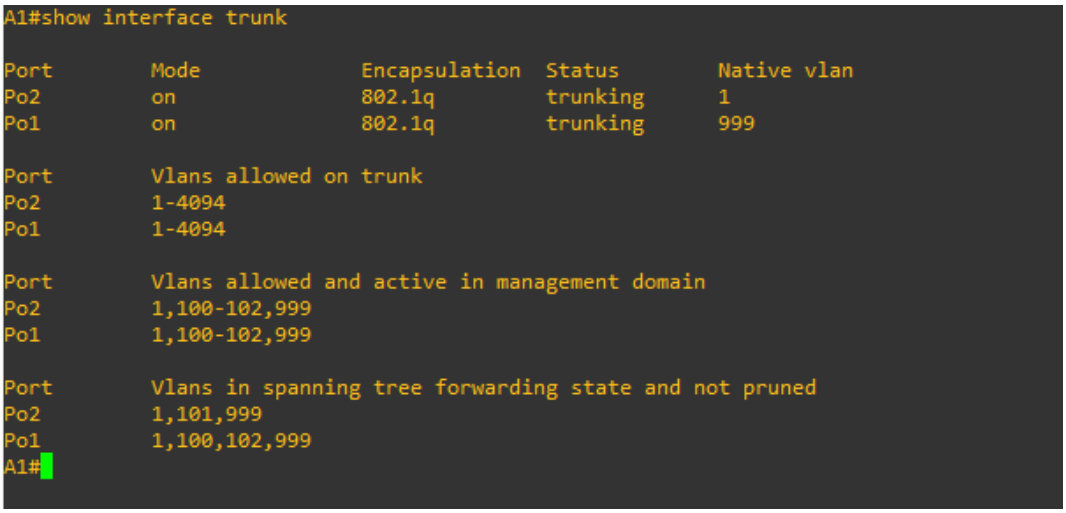
Figura 19. verificación con el comando show run int g2/3



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

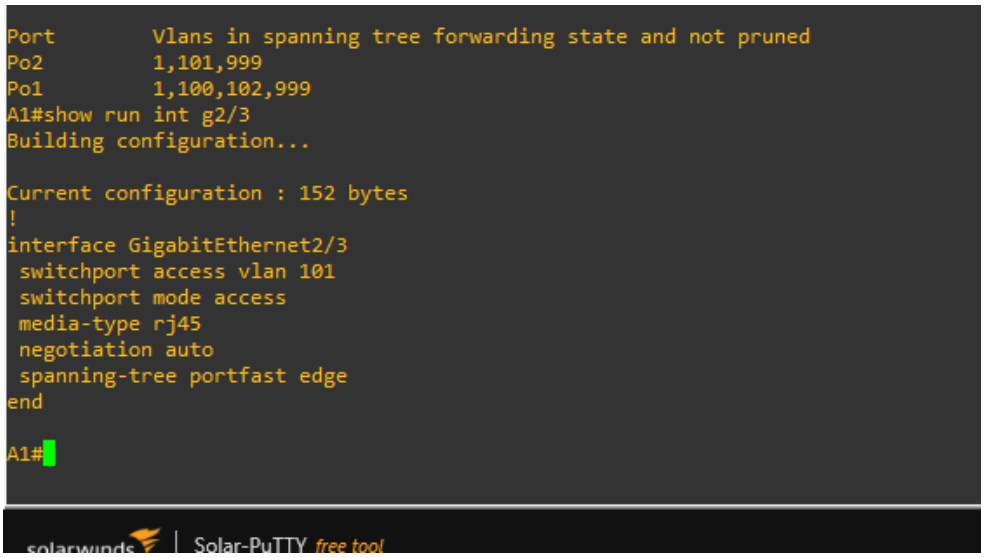


PO2 CONEXIÓN D2
PO1 CONEXIÓN D1
Nativa vlan

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.

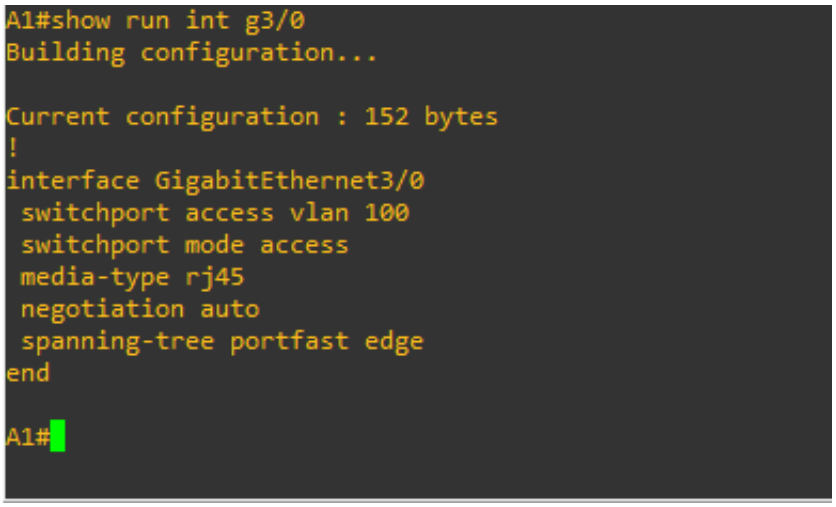
Figura 21. Verificación con el comando show INT G2/3



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. Verificacion con el comando show int g3/0



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 Compañia” (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: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

3.2	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID **6** y asigne los siguientes router- IDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la “Red ISP”, configure MP- BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). La ruta por defecto (::/0).

3.4	En R1 en la “Red ISP”, configure MP- BGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. Anuncie la red 2001:db8:100::/48.

Desarrollo de la tarea 3.1.

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

Configuración en R1

Tabla 13. Configuración en R1

R1# show run | section ^router ospf router ospf 4 router-id 0.0.4.1 network 10.0.10.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0 default-information originate	 id de proceso id del router 1 notificación de red 10.0 notificación de red 13.0 propague la ruta por defecto

Configuración en R3

Tabla 14. Configuración en R3

R3# show run | section ^router ospf router ospf 4 router-id 0.0.4.3	 id de proceso id del router 3

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 red11.0
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

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

// 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
Vl102	6	0	41	1	DR	0/0
Vl101	6	0	40	1	DR	0/0
Vl100	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 exepto la 11

Interface	PID	Area	Intf ID	Cost	State	Nbrs F/C
Vl102	6	0	41	1	DR	0/0 // vlan 102
Vl101	6	0	40	1	DR	0/0 // vlan 101
Vl100	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

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 //	lconfigure la ruta estatica loopback0 interfaz de salida

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

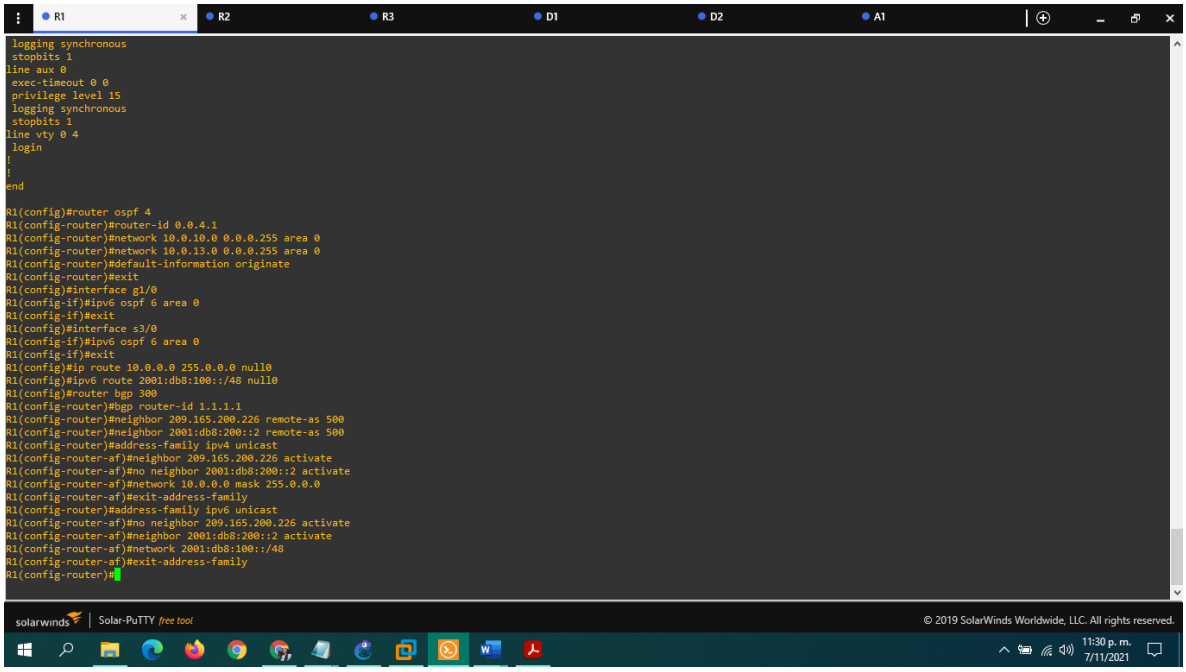
!

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

Simulaciones

R1

Figura 23. Simulación BGP en R1



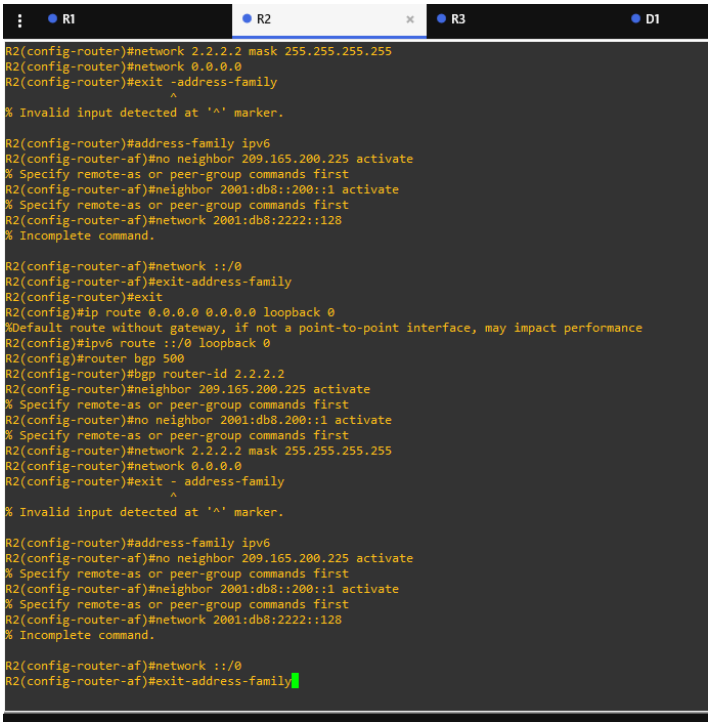
Código demostración del problema | sección BGP en R1

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

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	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 actívate salida actívate actívate notifique la red salida

R2

Figura 24. Simulación BGP en R2



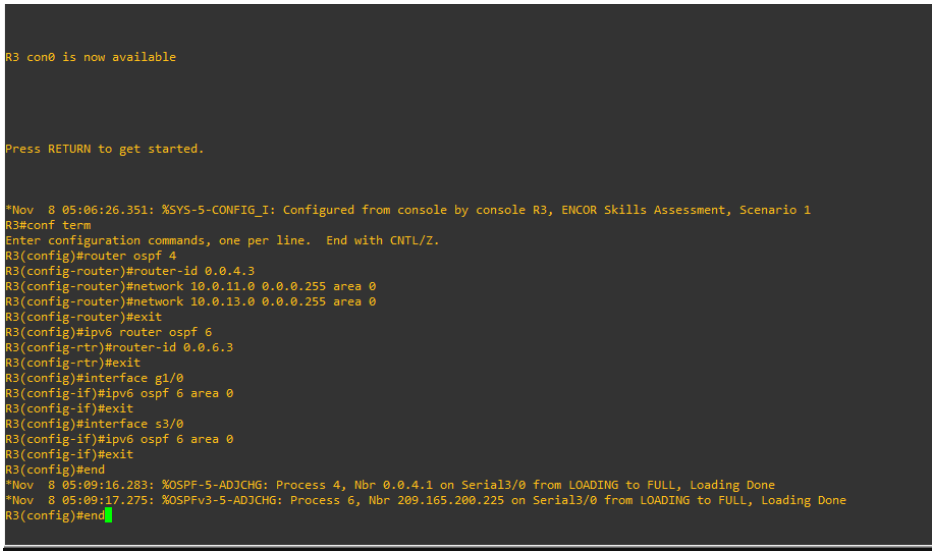
Código

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



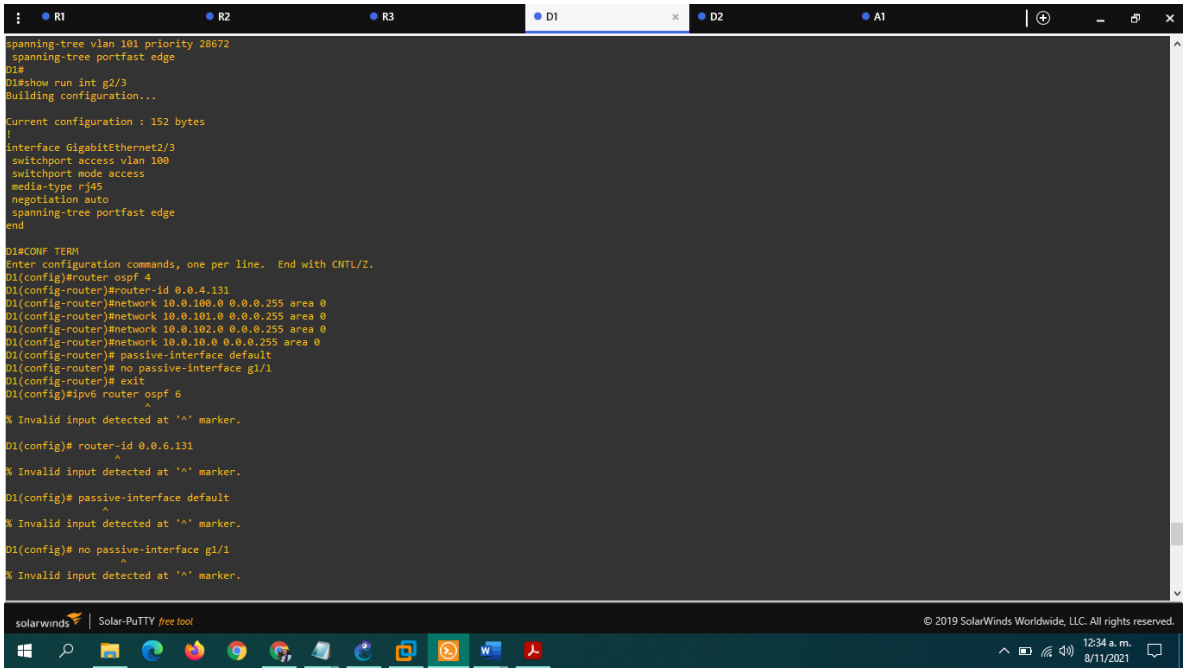
Código

Tabla 24. Código en R3

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

ipv6 ospf 6 area 0 exit interface s3/0 ipv6 ospf 6 area 0 // ipv6 exit // salida end	conexión al serial ipv6 Salida

Figura 26. Simulación BGP en D1



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

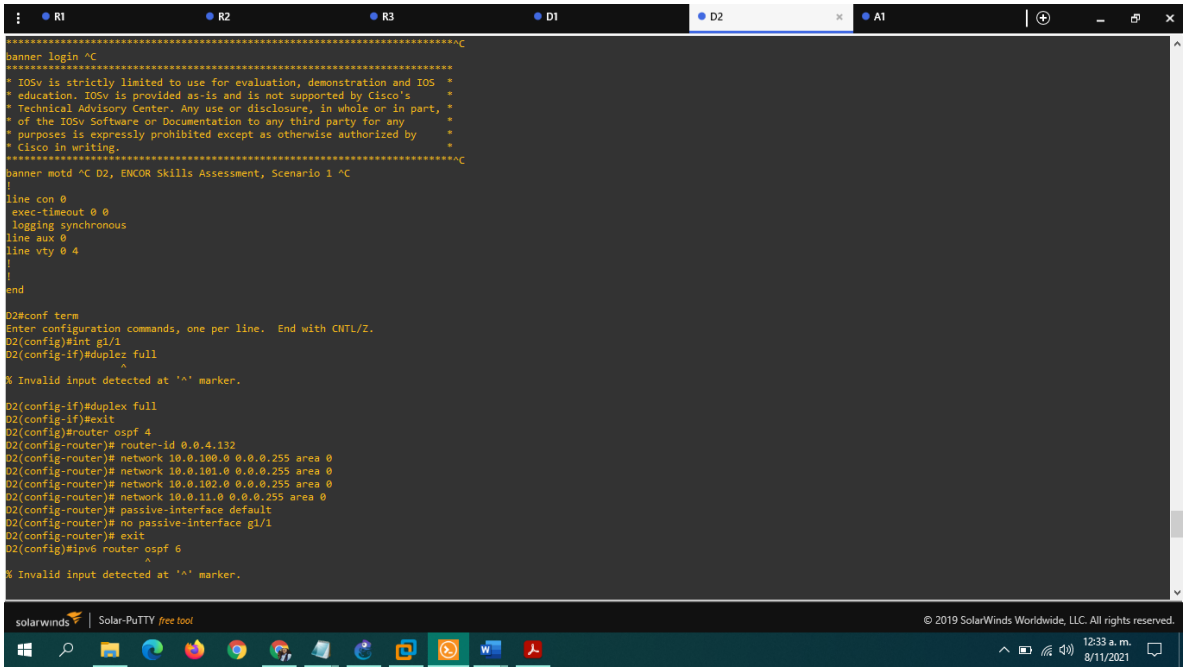
network 10.0.101.0 0.0.0.255 area 0 notificación de red 101.0

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

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	para no anunciar las rutas al vecino, pero el siguiente salto si ve la ruta salida todas las interfaces pasivas excepto la 1 todas las interfaces pasivas exceto la 1 todas las interfaces pasivas excepto la 1 todas las interfaces pasivas excepto la 1 todas las interfaces pasivas excepto la 1 Salida

Figura 27. Simulación BGO en D2



Código

Tabla 26. Código en D2

router ospf 4 router-id 0.0.4.132 network 10.0.100.0 0.0.0.255 area 0 network 10.0.101.0 0.0.0.255 area 0 network 10.0.102.0 0.0.0.255 area 0 network 10.0.11.0 0.0.0.255 area 0 passive-interface default no passive-interface g1/1 exit ipv6 router ospf 6 router-id 0.0.6.132 passive-interface default no passive-interface g1/1 exit interface g1/ 1	id de proceso id del router 132 notificación de 4 redes notificación de red 100.0 notificación de red 101.0 notificación de red 102.0 notificación de red11.0 //desactive todas las interfaces excepto 1 Salida Interface g1/1 salida

ipv6 ospf 6 area 0 exit interface vlan 100 ipv6 ospf 6 area 0 exit// salida interface vlan 101 ipv6 ospf 6 area 0 exit// salida interface vlan 102 ipv6 ospf 6 area 0 exit//salida end	Ipv6 en área 0 Vlan 100 Vlan 102 Salida

Parte 4: Configurar la redundancia del primer salto (first hop redundancy)

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

Tabla 27. Las tareas de configuración

Las tareas de configuración son las siguientes: **Tarea4**	**Tarea**	**Especificación**
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • • Use la SLA número **4** para IPv4. • • Use la SLA número **6** para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

		• • Use el número de rastreo **4** para la IP SLA 4. • • Use el número de rastreo **6** para la IP SLA 6. 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.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • • Use la SLA número **4** para IPv4. • • Use la SLA número **6** para IPv6. 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. • • Use el número de rastreo **4** para la IP SLA 4. • • Use el número de rastreo **6** para la SLA 6. 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.

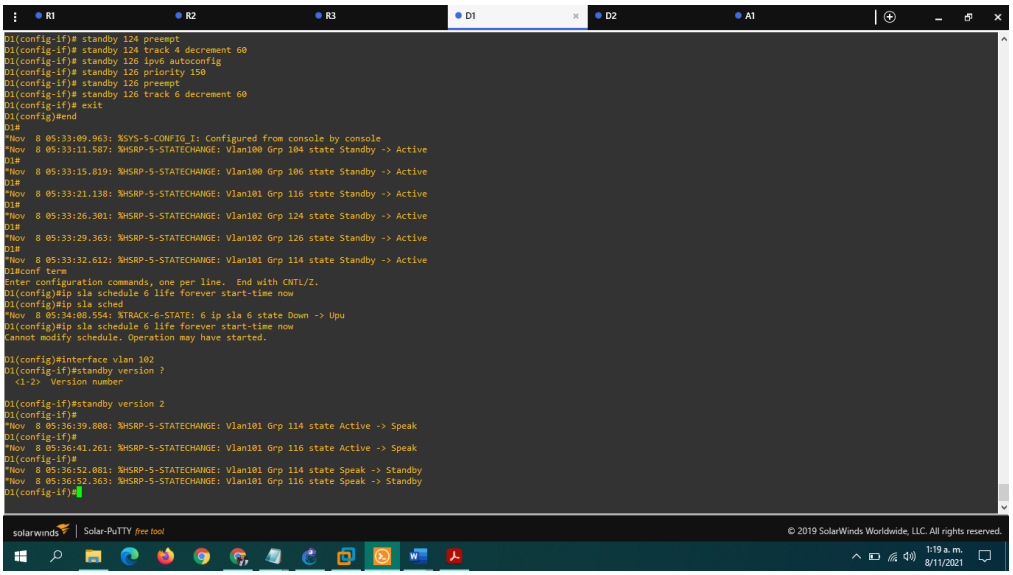
Desarrollo de la tarea 4.1

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



Código

Tabla 28. Código en D1

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	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

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	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

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

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	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

track 4 ip sla 4	numero track 4
delay down 10 up 15 exit	retardo de caido 10 a levantado 15 salida
track 6 ip sla 6 delay down 10 up 15 exit	numero track 6 retardo de caido 10 a levantado 15 salida
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 100 grupo 104 asigne ip virtual decrementar prioridad 60 grupo 106 vlan 100 // autoconfiguración 60 // drecrementar la prioridad a 60

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
	salida
	configure ipv6 HSRP grupo 116
	ip virtual asigne
	// prioridad 150
	
	drecrementar a 60
	// autoconfiguración
	// prioridad 150
	
	decrementar prioridad 60
	salida

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	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

Desarrollo de la tarea 4.3

Tabla 30. Desarrollo de la tarea 4.3

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	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.

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: **Tarea#**	**Tarea**	**Especificación**
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio 15 • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6.

		• Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y la contraseña: **upass123**.

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 , cifranos 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

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

Figura 29. Asignación Scripypt Secret D1

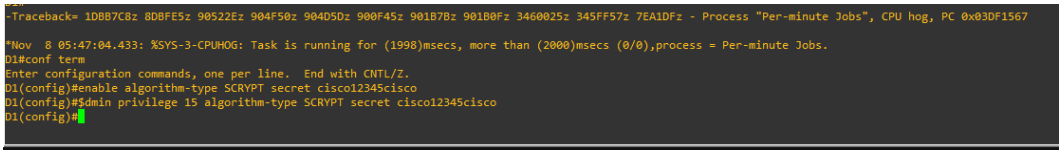


Figura 30. Asignación Scriptypt Secret D2

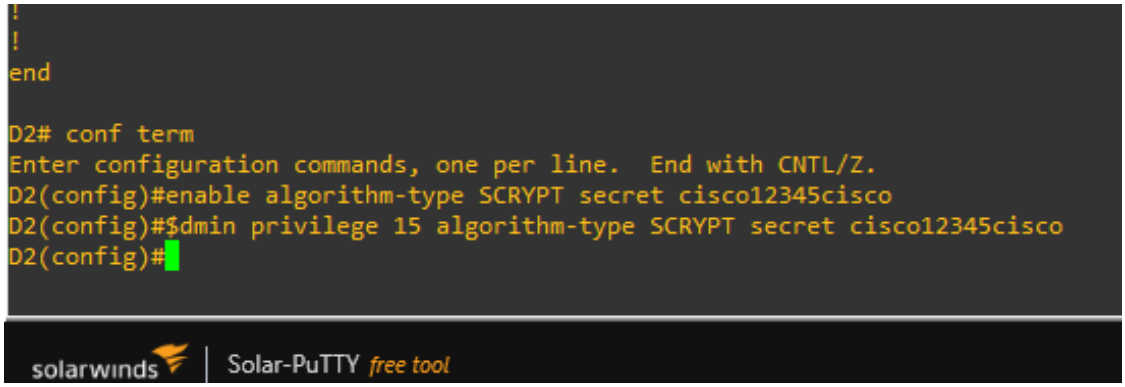


Figura 31. Asignación Scriptypt secret A1

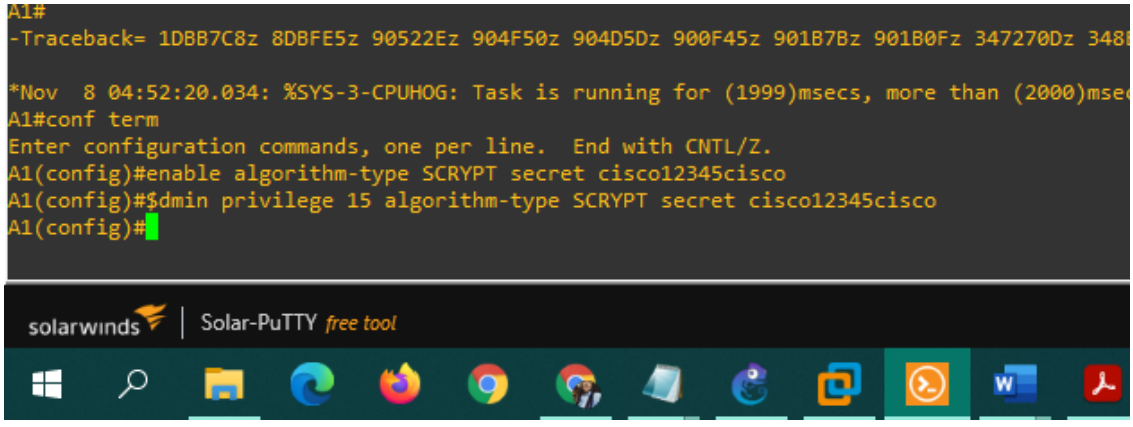


Figura 32. Asignación alternativa Scripypt secret R1

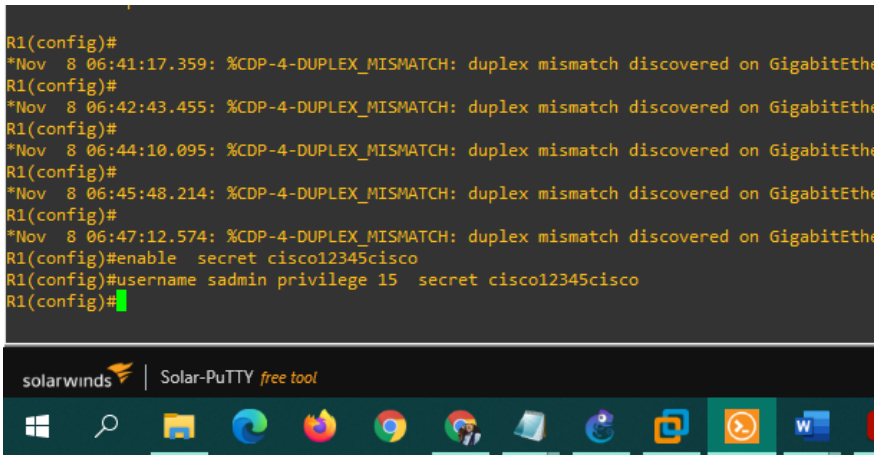


Figura 33. Asignación Scripypt Secret R2

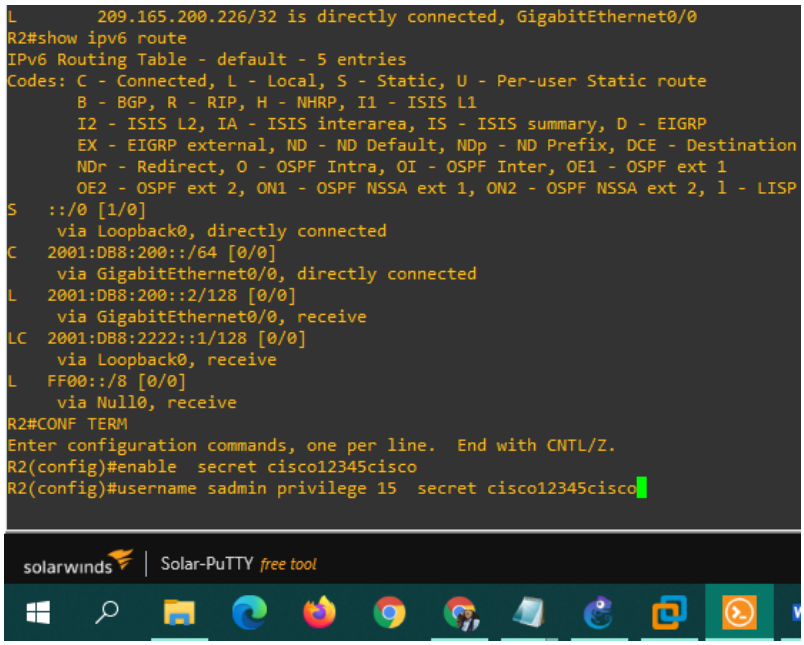
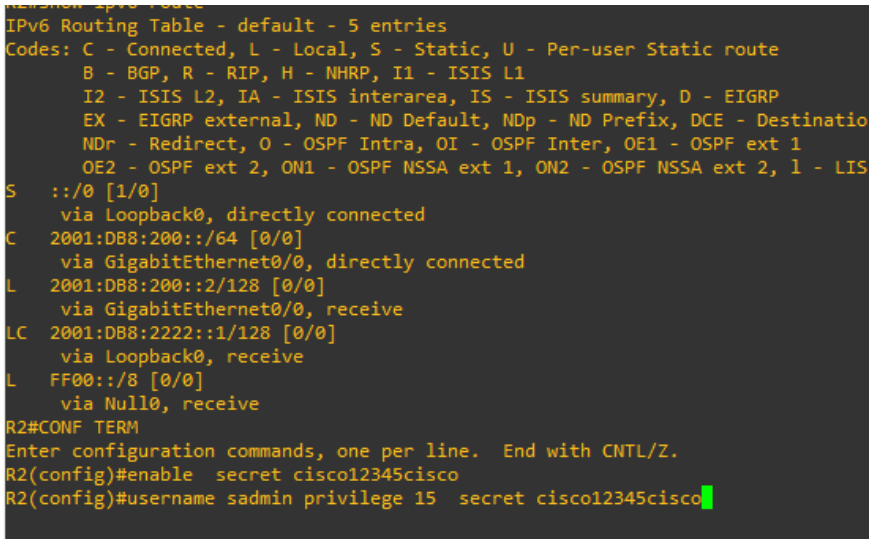


Figura 34. Asignación Scripypt Secret D1



Desarrollo de la tarea 5.5 y 5.6

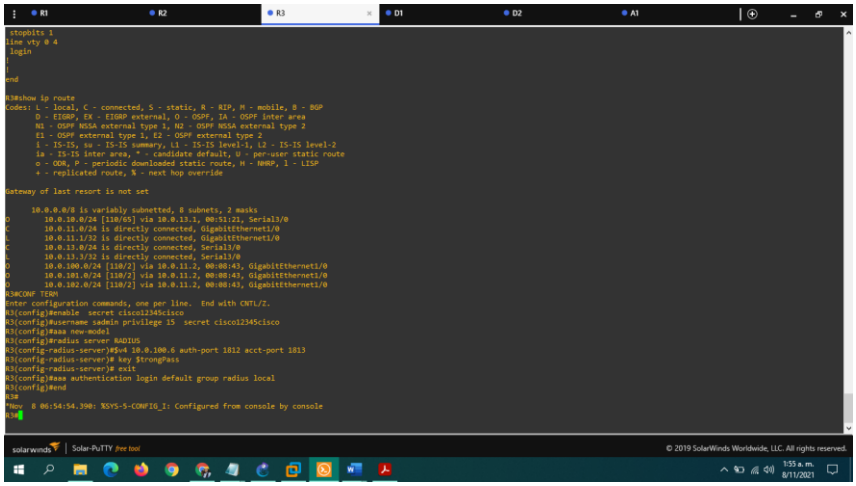
En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

Tabla 33. Tareas 5.5 y 5.6

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

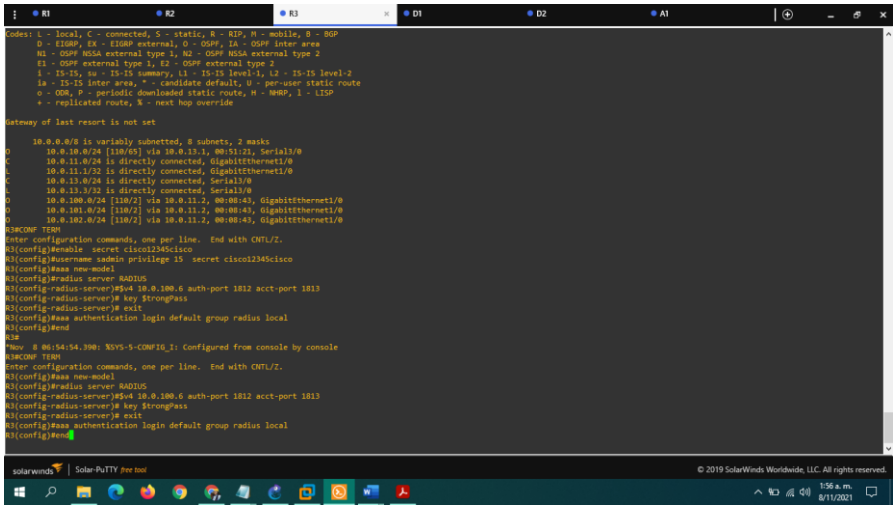
R1

Figura 35. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA



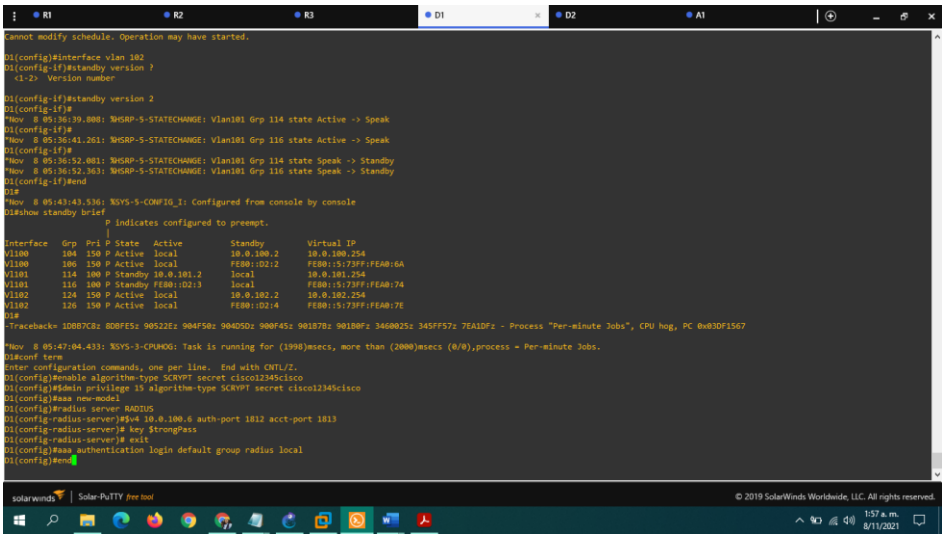
R3

Figura 36. Se habilitó AAA, se configuraron las especificaciones del servidor radius y se configuró la lista de métodos de autenticación AAA.



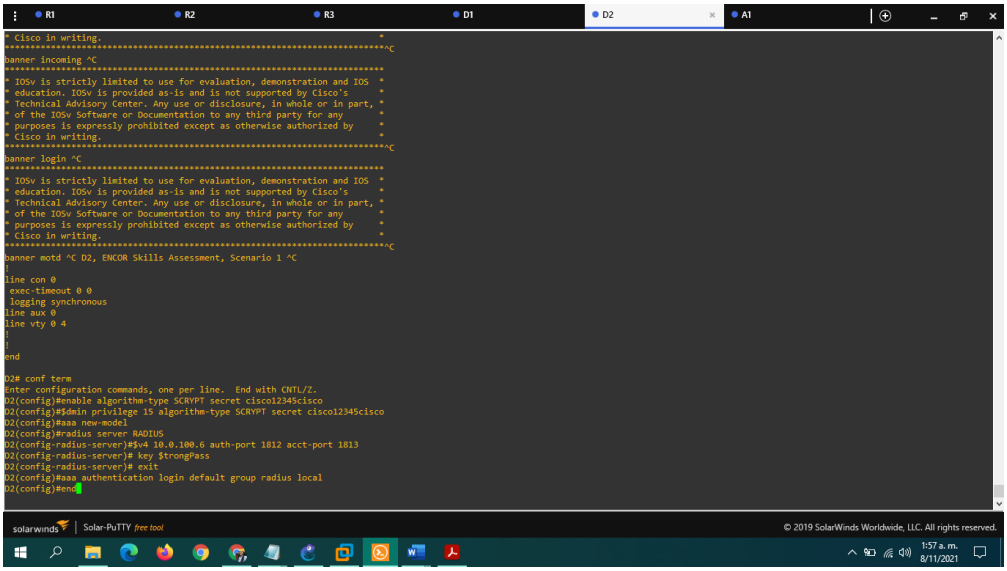
D1

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



D2

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



D3

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

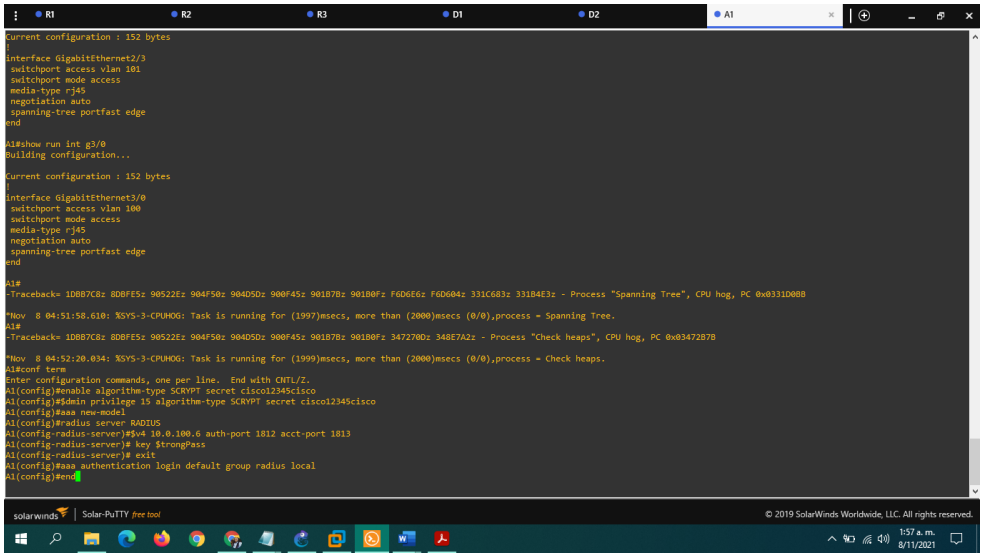
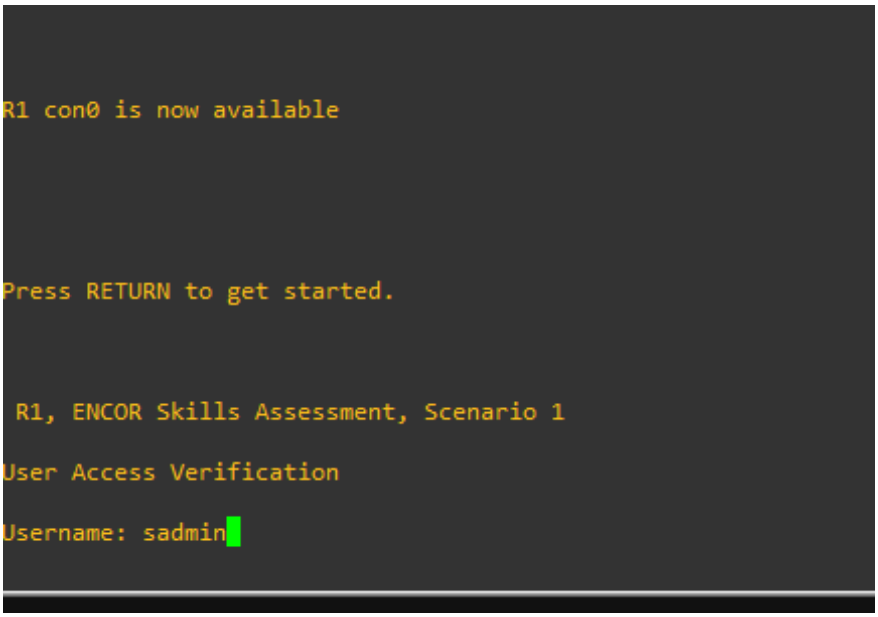


Figura 40. Verificación de acceso en R1



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: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

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

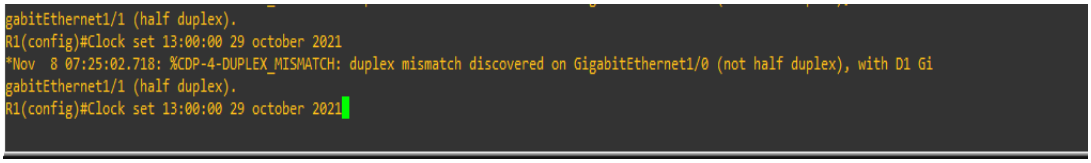


Tabla 35. Código configuración Router R2 y Router R1

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

Tabla 36. Código Router R3

ntp server 10.0.10.1 logging trap warning logging host 10.0.100.5 logging on ip access-list standard SNMP-NMS permit host 10.0.100.5 exit // 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	sincroniza con r1 Configure Syslog active login lista de acceso permitir solo a la pc 1 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 se habilita el envío de traps: config, y ospf

Figura 42. Verificación de la configuración R3

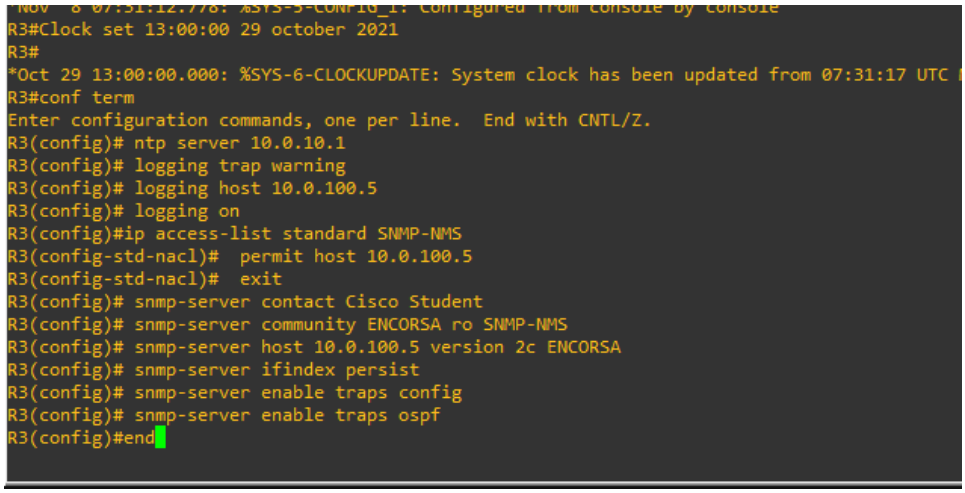


Tabla 37. Switch D1

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
	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

Tabla 38. Switch D2

ntp server 10.0.10.1
 logging trap warning
 	
 logging host 10.0.100.5
 logging on
ip access-list standard SNMP-NMS
 permit host 10.0.100.5
 exit// 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
	// 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

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

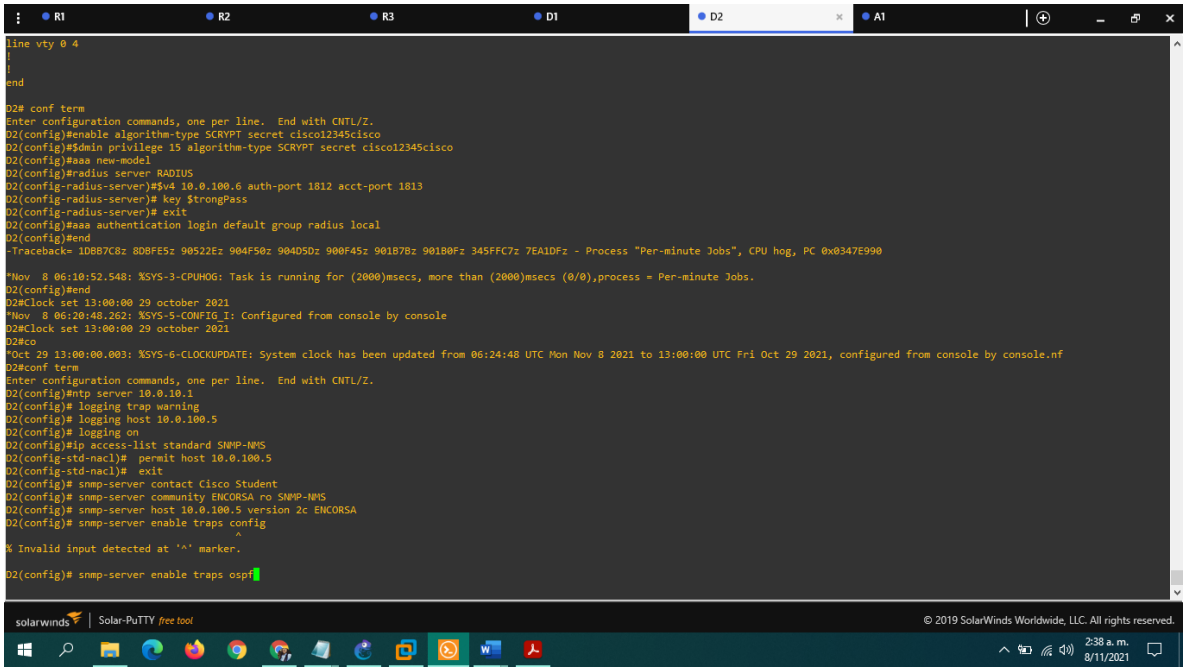
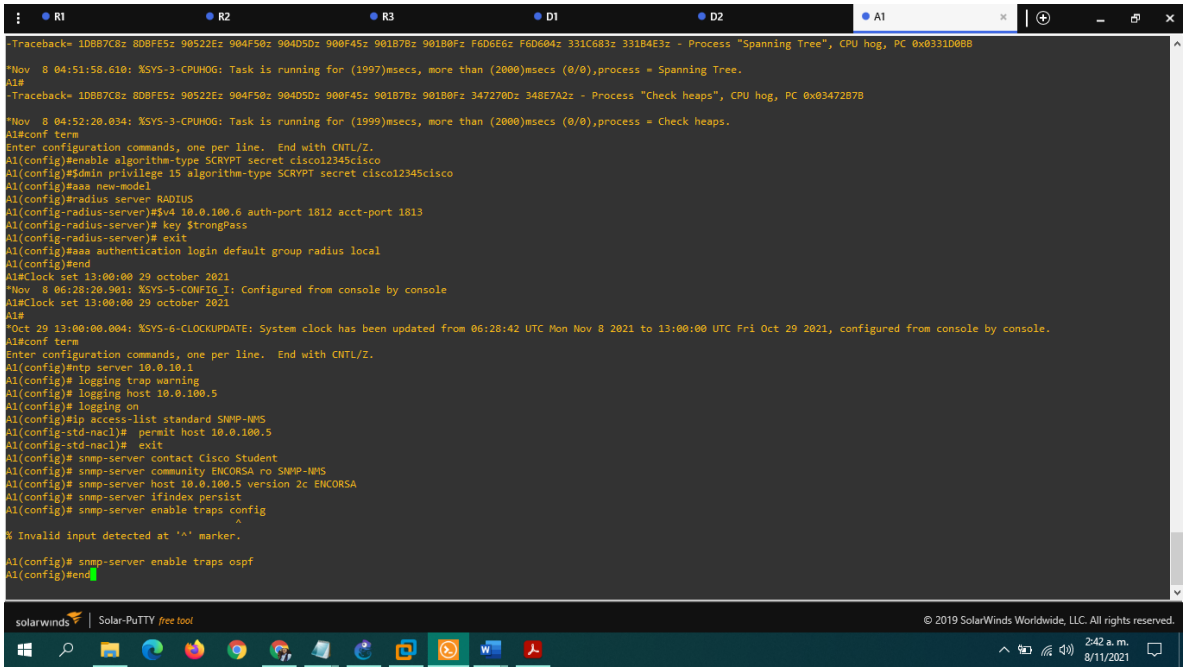


Tabla 39. Switch A1

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

snmp-server enable traps config snmp-server enable traps ospf end	En A1, habilite el envío de *traps config*.

Figura 44. Verificación de la configuración en A1

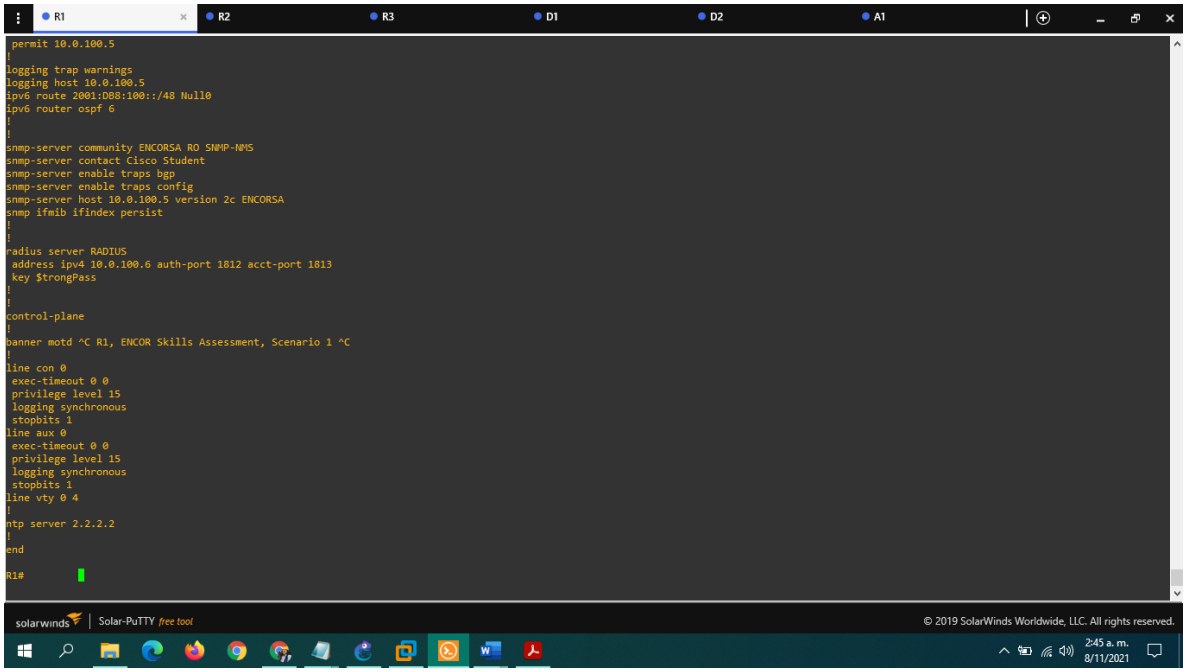


Verificaciones

Router R1

R1# show run

Figura 45. Verificación en R1 #show run



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 loopes. 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 arrojo 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 ENCOR 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 ENCOR 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 ENCOR 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 ENCOR 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 ENCOR 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 ENCOR 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!AAIGg5JUgUBthk8