

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDUARDO ANDRES SANTOS CONTRERAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI}
INGENIERIA ELECTRONICA
SINCELEJO, SUCRE
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDUARDO ANDRES SANTOS CONTRERAS

Diplomado en opción de grado presentado para optar por el título de INGENIERO
ELECTRONICO

DIRECTOR: GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI}
INGENIERIA ELECTRONICA
SINCELEJO, SUCRE
2021

NOTA DE ACEPTACION

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

AGRADECIMIENTOS

A mis padres quienes son una constante ayuda y recordatorio de la importancia de no rendirse ante los obstáculos y a tener paciencia para afrontar los problemas. A mi familia que siempre me ha acompañado en los logros y proyectos que he emprendido confiando siempre en que doy lo mejor de mí.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	11
INTRODUCCION.....	12
DESARROLLO	13
1. Escenario planteado	13
2. Construcción de la topología	14
2.2 Copia del archivo running-config al archivo startup-config	26
3. Configuración de la capa 2 de la red y el soporte de Host	28
3.1 Configuración de Red Capa 2 para Switch D1	29
3.2 Configuración de Red Capa 2 para D2.....	31
3.3 Configuración de Red Capa 2 para A1	34
4. Configuración de los Protocolos de Enrutamiento.....	36
4.1 Router R1	37
4.2 Router R2	40
4.3 Router R3	42
4.4 SWITCH D1.....	44
4.5 SWITCH D2.....	46
5. Configurar la redundancia del primer salto.....	48
5.1 Switch D1	50
5.2 Switch D2	53
6. Seguridad.....	55
6.1 Configuración de Seguridad para R1	56
6.2 Configuración de Seguridad para R2	57

6.3 Configuración de Seguridad para R3	58
6.4 Configuración de Seguridad para D1	59
6.5 Configuración de Seguridad para D2	60
7. Configure las funciones de Administración de Red	61
7.1 Configuración de Administración para Router R2:	62
7.2 Configuración de Administración para Router R1	62
7.3 Configuración de Administración para Router R3	65
7.4 Configuración de Administración para Switch D1	66
7.5 Configuración de Administración para Switch D2.....	68
7.6 Configuración de Administración para Switch A1	69
CONCLUSIONES	73
REFERENCIAS BIBLIOGRAFICAS.....	74

LISTA DE TABLAS

Tabla N°1 - Tabla de direcciones.....	17
Tabla N°2 - Configuración capa 2 y host	28
Tabla N°3. Configuración de protocolos de enrutamiento.....	36
Tabla N°4. Tareas Configuración de Redundancia.....	48
Tabla N°5. Configuraciones de Seguridad para dispositivos	55
Tabla N°6 - Configuraciones de Administración de Red para los dispositivos	61

LISTA DE FIGURAS

Figura 1 Topología a Diseñar.....	13
Figura 2 GNS3 web site.....	14
Figura 3. Máquina Virtual VMware.....	14
Figura 4. Simulación utilizando GSN3.....	15
Figura 5. Puertos de los dispositivos.....	16
Figura 6. Topología diseñada	16
Figura 7. Configuraciones R1 por consola	19
Figura 8. Configuraciones R2 por consola.....	20
Figura 9. Configuraciones R3 por consola.....	21
Figura 10. Configuraciones D1 por consola.....	23
Figura 11. Configuraciones D2 por consola.....	25
Figura 12. Configuraciones A1 por consola.....	26
Figura 13. Copy run start para R1.....	27
Figura 14. Copy run start para R2.....	27
Figura 15. Copy run start para R3.....	27
Figura 16. Copy run start para D1.....	27
Figura 17. Copy run start para D2.....	27
Figura 18. Copy run start para A1.....	27
Figura 19. Configuración de Red Capa 2 para Switch D1	30
Figura 20. show run include spanning-tree D1.....	30
Figura 21. show run interface en D1	31
Figura 22. Configuración de Red Capa 2 para D2	32
Figura 23. show interface trunk para D2	32
Figura 24. show run include spanning-tree D2.....	33
Figura 25. show run interface D2.....	33
Figura 26. Configuración de Red Capa 2 para A1.....	35
Figura 27. show run interface.....	35
Figura 28. Configuración de enrutamiento R1.....	38
Figura 29. show run section ^router ospf en R1	38
Figura 30. show run section ^ipv6 router en R1	38
Figura 31. show run section bgp en R1.....	39
Figura 32. show ip route include O B en R1.....	39
Figura 33. show ipv6 route en R1	40
Figura 34. Configuración de enrutamiento R2.....	41
Figura 35. show run section bgp en R2.....	41
Figura 36. show run include route en R2.....	42
Figura 37. Configuración de enrutamiento R3.....	43
Figura 38. show run section ^router ospf en R3	43
Figura 39. show ipv6 ospf interface brief en R3	43
Figura 40. show ip route ospf begin Gateway en R3	44
Figura 41. show ipv6 route ospf en R3.....	44
Figura 42. Configuración de enrutamiento D1.....	45
Figura 43. show run section ^router ospf en D1	46
Figura 44. Configuración de enrutamiento D2.....	47

Figura 45. show run section ^router ospf en D2	47
Figura 46. Configuración de Redundancia para D1	51
Figura 47. show run section ip sla para D1	52
Figura 48. show standby brief para D1	52
Figura 49. Configuración de Redundancia para D2	54
Figura 50. show run section ip sla para D2	54
Figura 51. show stanbdy brief para D2	55
Figura 52. Configuración de Seguridad para R1	56
Figura 53. show run include secret para R1	56
Figura 54. show run aaa exclude ! Para R1	57
Figura 55. Configuración de Seguridad para R2	57
Figura 56. show run include secret para R2.....	57
Figura 57. Configuración de Seguridad para R3	58
Figura 58. show run aaa exclude ! para R3.....	58
Figura 59. show run aaa exclude Para R3	58
Figura 60. Configuración de Seguridad para D1	59
Figura 61. show run include secret para D1	59
Figura 62. show run aaa exclude ! para D1.....	59
Figura 63. Configuración de Seguridad para D2	60
Figura 64. show run include secret para D2.....	60
Figura 65. show run aaa exclude ! para D2.....	60
Figura 66. Configuración de Administración para R2	62
Figura 67. show run include ntp para R2.....	62
Figura 68. Configuración de administración para R1	63
Figura 69. show ntp status include stratum para R1.....	63
Figura 70. show run include logging para R1	64
Figura 71. show run include snmp para R1	64
Figura 72. Configuración de Administración para R3	65
Figura 73. show run include snmp para R3.....	66
Figura 74. Configuración de Administración para D1	67
Figura 75. show ip access-list SNMP-NMS Para D1	67
Figura 76. Configuración de Administración para D2	68
Figura 77. show run include snmp para D2.....	69
Figura 78. Configuración de Administración para A1	70
Figura 79. show run include snmp Para A1.....	70
Figura 80. Ping en PC1.....	71
Figura 81. Comprobación Ping en PC2.....	71
Figura 82. Comprobación de Seguridad para R1	72

GLOSARIO

Trunk Interface: Trunk es una configuración de canal para puertos de switch que estén en una red Ethernet, que posibilita que se pueda pasar varias VLAN por un único link, o sea, un link de troncal es un canal que puede ser switch-switch o switch-router, por donde se pasan informaciones originadas y con destino a más de una VLAN.

VLAN: La red de área local virtual (VLAN) es una agrupación lógica de hosts. La agrupación permite a los hosts comunicarse como si estuvieran en la misma LAN, independientemente de la topología física de la red. Las VLAN pueden agrupar los ordenadores en grupos de trabajo lógicos. Conectar clientes a servidores dispersos geográficamente simplifica la gestión de la red. Normalmente, las VLAN constan de compañeros de trabajo en el mismo departamento que se encuentran en lugares diferentes.

OSPF (Open Shortest Path First): es considerado como un protocolo de estado de enlace que es capaz de detectar cambios en la topología dentro de un Sistema autónomo permitiendo una red de rutas sin bucles. OSPF traza un mapa completo de una interred y luego escoge el camino de menor coste basándose en dicho mapa. Con este protocolo cada enrutador posee un mapa completo de toda la red. Si un enlace falla, el protocolo OSPF puede localizar y resolver rápidamente un camino alternativo al destino basándose en el mapa sin que se forme un bucle de enrutamiento.

IPv4: IP significa Protocolo de Internet que se utiliza para entregar datagramas entre hosts en una red. Típicamente, es un método por el cual los datos serán enviados de un dispositivo de computadora a otro dispositivo de computadora a través de Internet. IPv4 es la cuarta versión del Protocolo de Internet que fue adaptado y ahora se utiliza ampliamente en la comunicación de datos a través de diferentes tipos de redes.

IPv6: IPv6 es la versión 6 del Protocolo de Internet, es la sexta versión del protocolo que hace posible conectar dispositivos en Internet, identificándolos con una dirección unívoca. La necesidad de diseñar una nueva versión del protocolo surge a raíz del agotamiento del espacio de direcciones disponibles en IPv4. Cada dirección IPv4 se compone de cuatro dígitos de ocho bits lo cual permite generar 2^{32} direcciones únicas, aproximadamente 4.300 millones.

RESUMEN

CCNP nos ayuda a tener una mejor comprensión sobre cómo funciona la arquitectura jerárquica de redes mucho más complejas, con temáticas como Switching, routing, security options, IPv4, IPv6, VLAN, etc. El propósito del curso desarrollado es lograr la implementación de tecnologías avanzadas para administrar una arquitectura de red, configurar redes empresariales, redes inalámbricas y profundizar en los conocimientos y competencias sobre virtualización y automatización de redes. En el presente documento se encuentra el desarrollo de un escenario propuesto, una topología donde se encuentran dispositivos como switches, routers, EthernetSwitchs y pc virtuales donde se propone hacer uso de los conocimientos adquiridos durante el desarrollo del curso de profundización.

En el desarrollo del documento se construye la red utilizando el software GNS3, se ejecutan los ajustes básicos de cada dispositivo, se configura la capa 2 de la red, se establecen protocolos de enrutamiento, trunk interfaces, OSPF, redundancia del primer salto, configuraciones de seguridad y características para administración de red. Se busca con esta actividad lograr una conectividad extremo a extremo de la topología.

Palabras Clave: Trunk interfaces, VLAN, OSPF, IPv4, IPv6.

ABSTRACT

CCNP helps us to have a better understanding of how the hierarchical architecture of much more complex networks works, with topics such as Switching, routing, security options, OSPF, IPv4, IPv6, trunk interfaces, VLAN, etc. the implementation of advanced technologies to manage a network architecture, configure business networks, wireless networks and deepen the knowledge and skills about network virtualization and automation. This document contains the development of a proposed scenario, a topology where there are devices such as switches, routers, Ethernet switches and virtual PCs where it is proposed to make use of the knowledge acquired during the development of the in-depth course.

In the development of the document, the network is built using the GNS3 software, the basic settings of each device are executed, layer 2 of the network is configured, the routing protocols, first-hop redundancy, security configurations and characteristics are used to red administration. This activity seeks to achieve end-to-end connectivity of the topology.

Keywords: Trunk interfaces, VLAN, OSPF, IPv4, IPv6.

INTRODUCCION

La prueba de habilidades del curso CCNP en su actividad final consiste en el desarrollo de una topología, en implementar su diseño, configuración, arreglos y ajustar su funcionamiento conforme los dispositivos que la conforman. Esta actividad es la culminación de las actividades realizadas durante el diplomado, en donde se pone en práctica lo aprendido y las habilidades de los estudiantes para resolver impedimentos y contratiempos a la hora de cumplir con lo planteado.

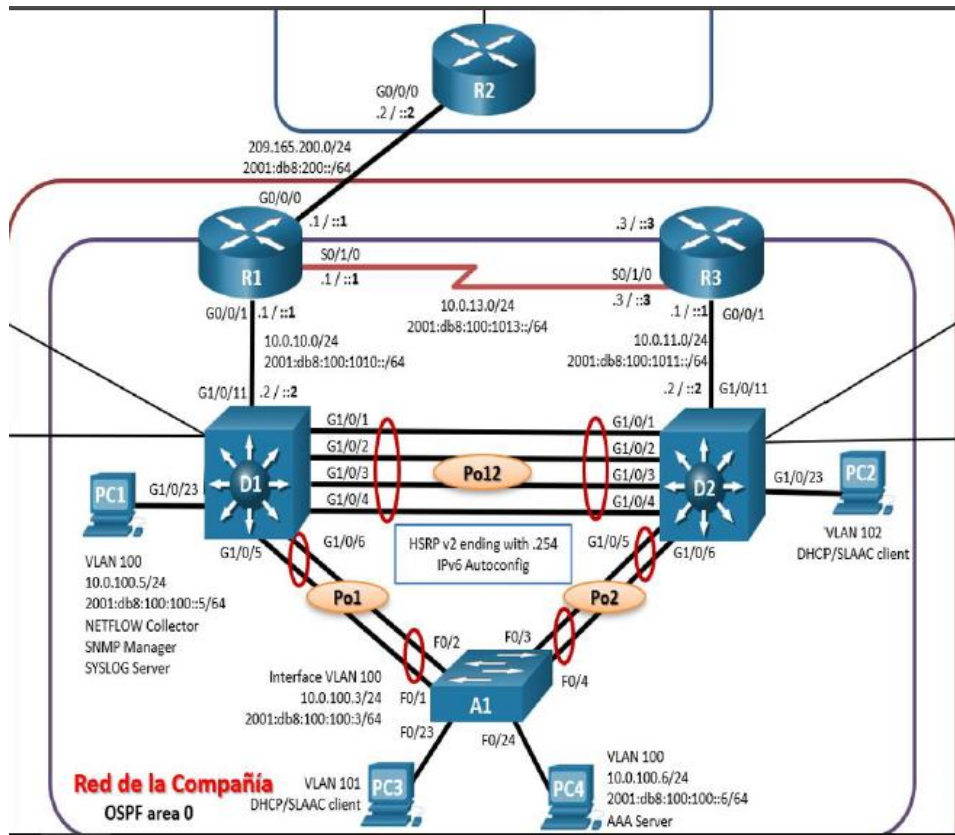
Aquellas personas que encaminen su perfil profesional a redes o que estudien ingeniería de sistemas conocen de primera mano futuros inconvenientes que tendrán que resolver en el manejo y administración de pequeñas y medianas redes de comunicación empresarial o comunitaria. Por ello la prueba busca recrear ciertas problemáticas en donde se busca despertar el sentido analítico y lógico para dar solución a fallas específicas.

La topología es desarrollada y configurada desde la capa 2 hasta la capa 3. Los dispositivos utilizados son switches, routers, Ethernet switch y ordenadores virtuales, ejecutados en GSN3 y utilizando softwares alternativos para contar con una máquina virtual.

DESARROLLO

1. Escenario planteado

Figura 1 Topología a Diseñar



La topología que se acaba de mostrar es la base sobre la cual se trabaja en el siguiente desarrollo, inicialmente se tenía previsto que se desarrollara en CISCO PACKET TRACER que fue la herramienta que se ha manejado durante el desarrollo del curso y manejada en otras asignaturas como CCNA 1 y CCNA2.

Sin embargo algunas características y funciones de la topología no son soportadas para las versiones de CISCO PACKET TRACER 8.0.1 y 7.2.2, por ello fue necesario realizar la implementación en el software GNS3 de versión 2.2.27. Software que es capaz de emular las tarjetas de red reales y switches utilizando una máquina virtual.

2. Construcción de la topología

Para lograr el desarrollo de la topología solicitada fue necesario hacer uso del programa GNS3 que al igual que la herramienta CISCO PACKET TRACER, utilizada a lo largo del curso, es un simulador gráfico de redes de telecomunicaciones donde se pueden mezclar dispositivos reales y virtuales.

Para lograr la utilización del software GNS3 es necesario descargar el software desde la página web: <https://www.gns3.com/software/download>. Allí mismo podemos encontrar también la maquina virtual requerida por el software para poder correr nuestros dispositivos. El software VMware Workstation es un software de virtualización para computadores compatibles con X86 con lo cual recreamos dispositivos.

Figura 2 GNS3 web site

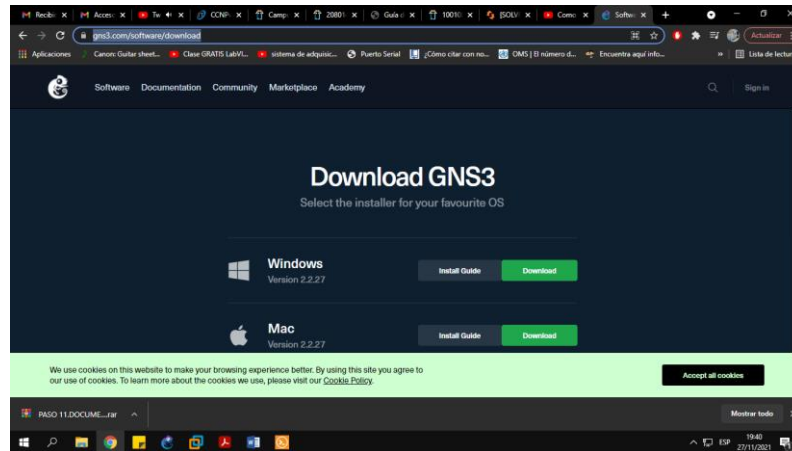
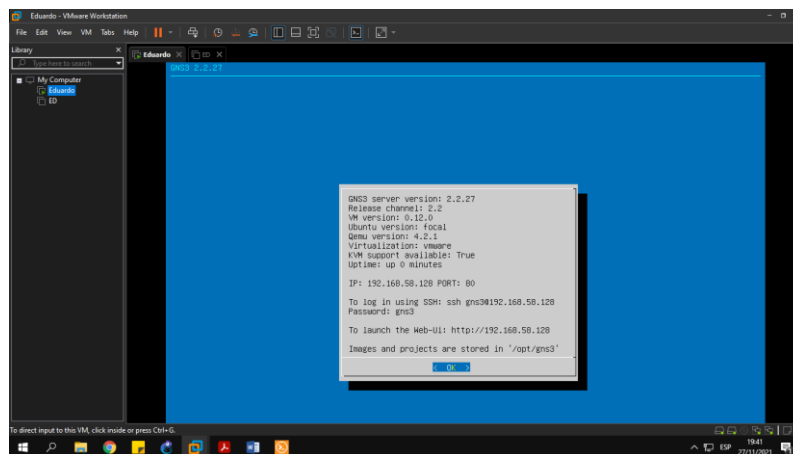
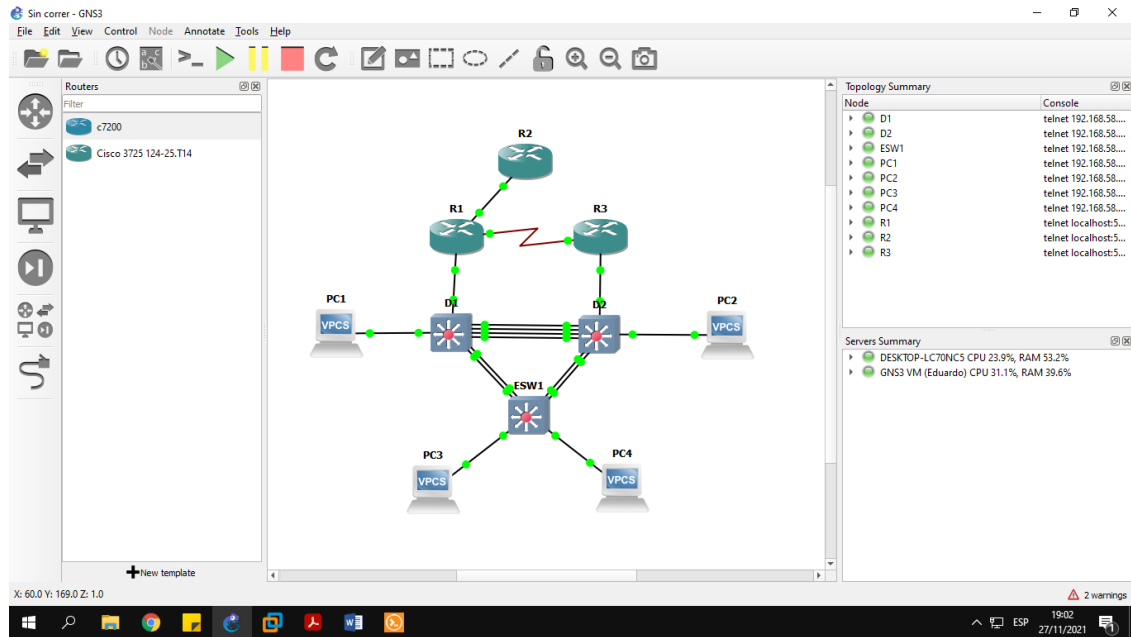


Figura 3. Máquina Virtual VMware



A continuación se denota la simulación del software GNS3 donde se desarrolló la topología propuesta utilizando:

Figura 4. Simulación utilizando GSN3



A continuación vamos a observar un detallado sobre los puertos utilizados en el desarrollo de la topología, como se puede observar son distintos a los puertos estipulados en la guía y mucho menos puertos de los que tienen los dispositivos cuando se utiliza el software Cisco Packet Tracer. Lo anterior tiene varios motivos, el primero es que la memoria RAM del ordenador utilizado se vió afectada por alguna razón que no se pudo determinar.

Adicionalmente existen problemas para guardar el nombre de las interfaces. Por ejemplo, si se renombra un adaptador como "g1/0/11" al momento de ejecutarlo a través de la consola no acepta modificaciones, en cambio sí se resetean los nombres a los que trae por defecto el software (gi1/0, gi1/1, etc) no existen problemas de identificación en la consola del dispositivo y permite su configuración.

Teniendo en cuenta lo anterior se decide utilizar los puertos estrictamente necesarios y dejar algunos libres en el caso de los Switches.

Figura 5. Puertos de los dispositivos

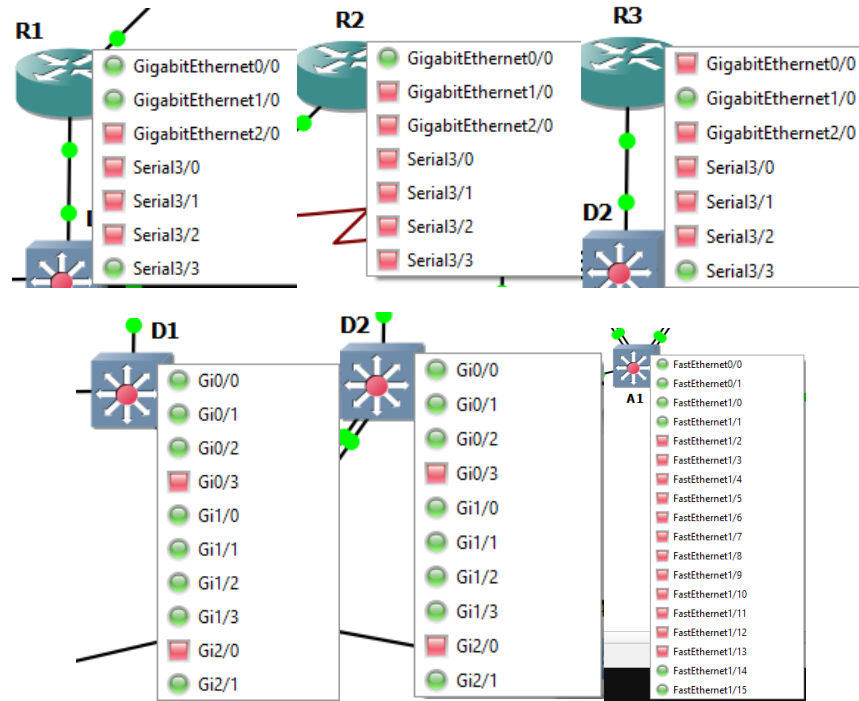


Figura 6. Topología diseñada

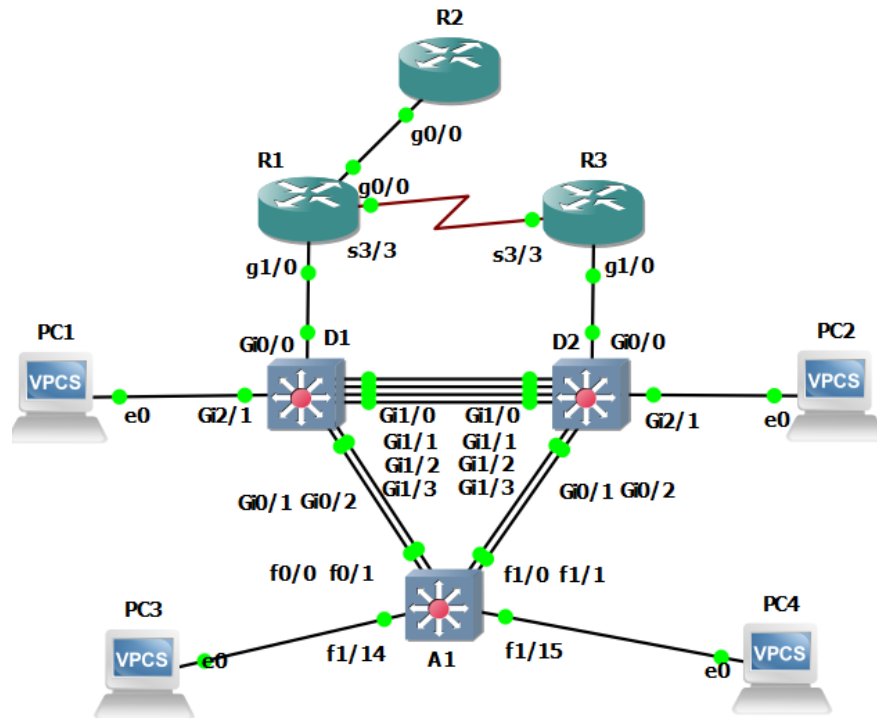


Tabla N°1 - Tabla de direcciones

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.162.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S3/3	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S3/3	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G0/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G0/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

2.1 Configuración Básica de los dispositivos

Aquí se encuentran las configuraciones iniciales dadas para el router R1, a continuación se describe que función cumplen las líneas de comandos que son utilizadas también para R2 y R3, al igual que D1, D2 y A1.

2.1.1 Configuraciones para R1

hostname R1	<i>Nombre del dispositivo</i>
ipv6 unicast-routing	<i>Se habilita IPV6</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	
line con 0	<i>Modo de Configuración de línea</i>
exec-timeout 0 0	<i>Sin interrupción por inactividad</i>
logging synchronous	<i>Sincroniza mensajes con tecla Enter</i>
exit	
interface g0/0	<i>Configuración de la interface</i>
ip address 209.165.200.225 255.255.255.224	<i>Configuración de ip y submask</i>
ipv6 address fe80::1:1 link-local	<i>Configuración de pertenencia a R1</i>
ipv6 address 2001:db8:200::1/64	<i>Configuración de pertenencia a R1</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface g1/0	<i>Configuración de la interface</i>
ip address 10.0.10.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::1:2 link-local	<i>Configuración de pertenencia a R1</i>
ipv6 address 2001:db8:100:1010::1/64	<i>Configuración de pertenencia a R1</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface s3/3	<i>Configuración de la interface</i>
ip address 10.0.13.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::1:3 link-local	<i>Configuración de pertenencia a R1</i>
ipv6 address 2001:db8:100:1013::1/64	<i>Configuración de pertenencia a R1</i>
no shutdown	<i>No apagar terminal</i>
exit	

Figura 7. Configuraciones R1 por consola

```
RI (config)#interface g0/1
% Invalid input detected at '^' marker.
RI (config)#interface g1/0
RI (config-if)#exit
RI (config)#interface g0/0
RI (config-if)#ip address 209.165.200.226 255.255.255.224
RI (config-if)#ipv6 address fe80::1:1 link-local
RI (config-if)#ipv6 address 2001:db8:200::1/64
RI (config-if)#no shutdown
RI (config-if)#exit
RI (config)#
*Nov 28 14:26:56.091: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Nov 28 14:26:57.001: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
RI (config)#interface g1/0
RI (config-if)#ip address 10.0.10.1 255.255.255.0
RI (config-if)#ipv6 address fe80::1:2 link-local
RI (config-if)#ipv6 address fe80::1:2 link-local
RI (config-if)#ipv6 address 2001:db8:100::1/64
RI (config-if)#ipv6 address 2001:db8:100::1/64
RI (config-if)#no shutdown
RI (config-if)#exit
RI (config)#
*Nov 28 14:27:37.399: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Nov 28 14:27:38.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
RI (config)#interface s3/3
RI (config-if)#ip address 10.0.13.1 255.255.255.0
RI (config-if)#ipv6 address fe80::1:3 link-local
RI (config-if)#ipv6 address 2001:db8:100::1/64
RI (config-if)#no shutdown
RI (config-if)#exit
RI (config)#
*Nov 28 14:27:59.531: %LINK-3-UPDOWN: Interface Serial3/3, changed state to up
RI (config)#
*Nov 28 14:28:00.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/3, changed state to up
RI (config)#
```

2.1.2 Configuraciones para R2

hostname R2	<i>Nombre del dispositivo</i>
ipv6 unicast-routing	<i>Se habilita IPV6</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	<i>Modo de Configuración de línea</i>
line con 0	<i>Sin interrupción por inactividad</i>
exec-timeout 0 0	<i>Sincroniza mensajes con tecla Enter</i>
logging synchronous	
exit	

interface g0/0	<i>Configuración de la interface</i>
ip address 209.165.200.226 255.255.255.224	<i>Configuración de ip y submask</i>
ipv6 address fe80::2:1 link-local	<i>Configuración de pertenencia a R2</i>
ipv6 address 2001:db8:200::2/64	<i>Configuración de pertenencia a R2</i>
no shutdown	<i>No apagar terminal</i>
exit	

interface Loopback 0	<i>Interfaz lógica del router (UP)</i>
ip address 2.2.2.2 255.255.255.255	<i>Configuración de ip y submask</i>
ipv6 address fe80::2:3 link-local	<i>Configuración de pertenencia a R2</i>
ipv6 address 2001:db8:2222::1/128	<i>Configuración de pertenencia a R2</i>
no shutdown	<i>No apagar terminal</i>
exit	

Figura 8. Configuraciones R2 por consola

2.1.3 Configuraciones para R3

hostname R3	<i>Nombre del dispositivo</i>
ipv6 unicast-routing	<i>Se habilita IPV6</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	<i>Modo de Configuración de línea</i>
line con 0	<i>Sin interrupción por inactividad</i>
exec-timeout 0 0	<i>Sincroniza mensajes con tecla Enter</i>
logging synchronous	
exit	
interface g1/0	<i>Configuración de la interface</i>
ip address 10.0.11.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::3:2 link-local	<i>Configuración de pertenencia a R3</i>
ipv6 address 2001:db8:100:1011::1/64	<i>Configuración de pertenencia a R3</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface s3/3	<i>Configuración de la interface</i>
ip address 10.0.13.3 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::3:3 link-local	<i>Configuración de pertenencia a R3</i>
ipv6 address 2001:db8:100:1010::2/64	<i>Configuración de pertenencia a R3</i>
no shutdown	<i>No apagar terminal</i>
exit	

Figura 9. Configuraciones R3 por consola

2.1.4 Configuraciones para D1

hostname D1	<i>Nombre del dispositivo</i>
ip routing	<i>Habilita enrutamiento IPV4 capa 3</i>
ipv6 unicast-routing	<i>Habilita IPV6</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	<i>Modo de Configuración de Línea</i>
line con 0	<i>Sin interrupción por inactividad</i>
exec-timeout 0 0	<i>Sincroniza mensajes con tecla Enter</i>
logging synchronous	
exit	
vlan 100	<i>Crea LAN virtual 100</i>
name Management	<i>Se nombra VLAN 100</i>
exit	
vlan 101	<i>Crea LAN virtual 101</i>
name UserGroupA	<i>Se nombra VLAN 101</i>
exit	
vlan 102	<i>Crea LAN virtual 102</i>
name UserGroupB	<i>Se nombra VLAN 102</i>
exit	
vlan 999	<i>Crea LAN virtual 999</i>
name NATIVE	<i>Se nombra VLAN 999</i>

exit	
interface g0/0	<i>Configuración de la interface</i>
no switchport	<i>Convierte puerto capa 2 en 3</i>
ip address 10.0.10.2 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d1:1 link-local	<i>Configuración de pertenencia a D1</i>
ipv6 address 2001:db8:100:1010::2/64	<i>Configuración de pertenencia a D1</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 100	<i>Configuración VLAN</i>
ip address 10.0.100.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d1:2 link-local	<i>Configuración de pertenencia a D1</i>
ipv6 address 2001:db8:100:100::1/64	<i>Configuración de pertenencia a D1</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 101	<i>Configuración VLAN</i>
ip address 10.0.101.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d1:3 link-local	<i>Configuración de pertenencia a D1</i>
ipv6 address 2001:db8:100:101::1/64	<i>Configuración de pertenencia a D1</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 102	<i>Configuración VLAN</i>
ip address 10.0.102.1 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d1:4 link-local	<i>Configuración de pertenencia a D1</i>
ipv6 address 2001:db8:100:102::1/64	<i>Configuración de pertenencia a D1</i>
no shutdown	<i>No apagar terminal</i>
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.101.141 10.0.101.254	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.102.1 10.0.102.109	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.102.141 10.0.102.254	<i>Reserva de direcciones IP</i>
ip dhcp pool VLAN-101	<i>Nombra grupo direcciones DHCP</i>
network 10.0.101.0 255.255.255.0	<i>Configura direcciones DHCP</i>
default-router 10.0.101.254	<i>Configura IP del enrutador</i>
exit	
ip dhcp pool VLAN-102	<i>Nombra grupo direcciones DHCP</i>
network 10.0.102.0 255.255.255.0	<i>Configura direcciones DHCP</i>
default-router 10.0.102.254	<i>Configura IP del enrutador</i>
exit	
interface range g0/1-3, g1/0-3, g2/0-1	<i>Configurar rango de Interfaces</i>
shutdown	<i>Apaga interfaces</i>
exit	

Figura 10. Configuraciones D1 por consola

```

D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#
*Nov 28 19:36:03.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to down
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80:d1:2 link-local
D1(config-if)#
Translating "www.cisco.com"...domain server (255.255.255.255)
D1(config-if)#
D1(config-if)#ip address 2001:db8:100:100::1/64
D1(config-if)#
Translating "www.cisco.com"...domain server (255.255.255.255)
D1(config-if)#no shutdown
D1(config-if)#
*
*Nov 28 19:36:39.000: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#
*Nov 28 19:36:47.762: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to down
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80:d1:3 link-local
D1(config-if)#ipv6 address fe80:d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#
*Nov 28 19:37:08.861: %LINK-3-UPDOWN: Interface Vlan101, changed state to down
D1(config)#interface vlan 102
D1(config-if)#
*Nov 28 19:37:13.493: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to down
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80:d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
  
```

2.1.5 Configuraciones para D2

hostname D2	<i>Nombre del dispositivo</i>
ip routing	<i>Habilita enrutamiento IPV4 capa 3</i>
ipv6 unicast-routing	<i>Habilita IPV6</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	<i>Modo de Configuración de Línea</i>
line con 0	<i>Sin interrupción por inactividad</i>
exec-timeout 0 0	<i>Sincroniza mensajes con tecla Enter</i>
logging synchronous	
exit	
vlan 100	<i>Crea LAN virtual 100</i>
name Management	<i>Se nombra VLAN 100</i>
exit	
vlan 101	<i>Crea LAN virtual 101</i>
name UserGroupA	<i>Se nombra VLAN 101</i>
exit	
vlan 102	<i>Crea LAN virtual 102</i>
name UserGroupB	<i>Se nombra VLAN 102</i>
exit	
vlan 999	<i>Crea LAN virtual 999</i>
name NATIVE	<i>Se nombra VLAN 999</i>

exit	
interface g0/0	<i>Configuración de la interface</i>
no switchport	<i>Convierte puerto capa 2 en 3</i>
ip address 10.0.11.2 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d2:1 link-local	<i>Configuración de pertenencia a D2</i>
ipv6 address 2001:db8:100:1011::2/64	<i>Configuración de pertenencia a D2</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 100	<i>Configuración VLAN</i>
ip address 10.0.100.2 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d2:2 link-local	<i>Configuración de pertenencia a D2</i>
ipv6 address 2001:db8:100:100::2/64	<i>Configuración de pertenencia a D2</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 101	<i>Configuración VLAN</i>
ip address 10.0.101.2 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d2:3 link-local	<i>Configuración de pertenencia a D2</i>
ipv6 address 2001:db8:100:101::2/64	<i>Configuración de pertenencia a D2</i>
no shutdown	<i>No apagar terminal</i>
exit	
interface vlan 102	<i>Configuración VLAN</i>
ip address 10.0.102.2 255.255.255.0	<i>Configuración de ip y submask</i>
ipv6 address fe80::d2:4 link-local	<i>Configuración de pertenencia a D2</i>
ipv6 address 2001:db8:100:102::2/64	<i>Configuración de pertenencia a D2</i>
no shutdown	<i>No apagar terminal</i>
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.209	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.101.241 10.0.101.254	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.102.1 10.0.102.209	<i>Reserva de direcciones IP</i>
ip dhcp excluded-address 10.0.102.241 10.0.102.254	<i>Reserva de direcciones IP</i>
ip dhcp pool VLAN-101	<i>Nombra grupo direcciones DHCP</i>
network 10.0.101.0 255.255.255.0	<i>Configura direcciones DHCP</i>
default-router 10.0.101.254	<i>Configura IP del enrutador</i>
exit	
ip dhcp pool VLAN-102	<i>Nombra grupo direcciones DHCP</i>
network 10.0.102.0 255.255.255.0	<i>Configura direcciones DHCP</i>
default-router 10.0.102.254	<i>Configura IP del enrutador</i>
exit	
interface range g0/1-3, g1/0-3, g2/0-1	<i>Configurar rango de Interfaces</i>
shutdown	<i>Apaga rango de interfaces</i>
exit	

Figura 11. Configuraciones D2 por consola

```

D2(config-vlan)#exit
D2(config)#interface g0/0
D2(config)#interface g0/0
D2(config-if)#no switchport
D2(config-if)#
*Nov 28 19:41:09.838: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state
to up
D2(config-if)#
*Nov 28 19:41:18.837: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
er0/0, changed state to up
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#
*Nov 28 19:41:34.366: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, cha
nged state to down
D2(config-if)#
D2(config-if)#
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
*Nov 28 19:41:58.982: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
D2(config)#interface vlan 101
D2(config-if)#
*Nov 28 19:42:07.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, cha
nged state to down
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d3:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
*Nov 28 19:42:25.203: %LINK-3-UPDOWN: Interface Vlan101, changed state to down
D2(config)#interface vlan 102
D2(config-if)#

```

2.1.6 Configuraciones para A1

hostname A1	<i>Nombre del dispositivo</i>
no ip domain lookup	<i>No se ejecutan comandos errados</i>
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	
line con 0	<i>Modo de Configuración de línea</i>
exec-timeout 0 0	<i>Sin interrupción por inactividad</i>
logging synchronous	<i>Sincroniza mensajes con tecla Enter</i>
exit	
vlan 100	<i>Crea LAN virtual 100</i>
name Management	<i>Se nombra VLAN 100</i>
exit	
vlan 101	<i>Crea LAN virtual 101</i>
name UserGroupA	<i>Se nombra VLAN 101</i>
exit	
vlan 102	<i>Crea LAN virtual 102</i>
name UserGroupB	<i>Se nombra VLAN 102</i>
exit	
vlan 999	<i>Crea LAN virtual 999</i>
name NATIVE	<i>Se nombra VLAN 999</i>
exit	
interface vlan 100	<i>Configuración VLAN</i>
ip address 10.0.100.3 255.255.255.0	<i>Configuración de ip y submask</i>

```
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/0-1, f1/0-13
shutdown
exit
```

Configuración de pertenencia a A1
Configuración de pertenencia a A1
No apaga terminal

Selección Rango de interfaces
Apaga rango de interfaces

Figura 12. Configuraciones A1 por consola



```
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#
A1(config)#
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#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)#
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:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range f0/0-1, f1/0-13
% Invalid input detected at '^' marker.
A1(config)#interface f0/0
A1(config-if)#shutdown
A1(config-if)#interface f0/1
A1(config-if)#shutdown
A1(config-if)#interface range f1/0-13
```

2.2 Copia del archivo running-config al archivo startup-config

Abreviado se escribe **copy run start**, es un comando que se utiliza para hacer una copia de seguridad en la VRAM de las líneas de comandos ejecutadas o modificadas, de esta forma cuando se reinicie el dispositivo no se perderán las configuraciones.

2.2.1 Para dispositivo R1

Figura 13. Copy run start para R1

```
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

2.2.2 Para dispositivo R2

Figura 14. Copy run start para R2

```
R2#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

2.2.3 Para dispositivo R3

Figura 15. Copy run start para R3

```
R3#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

2.2.4 Para dispositivo D1

Figura 16. Copy run start para D1

```
copy run start
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3957 bytes to 1932 bytes[OK]
D1#
*Nov 27 21:27:42.533: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 27 21:27:43.210: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
```

2.2.5 Para dispositivo D2

Figura 17. Copy run start para D2

```
copy run start
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 4045 bytes to 1972 bytes[OK]
*Nov 27 21:27:34.599: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 27 21:27:35.270: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
```

2.2.6 Para dispositivo A1

Figura 18. Copy run start para A1

```
A1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

3. Configuración de la capa 2 de la red y el soporte de Host

Tabla 2 - Configuración capa 2 y host

Tareas	Especificaciones
En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa
En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
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
En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
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).
Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Teniendo en cuenta los requerimientos de la tabla N° 2, se realizan las configuraciones necesarias para los dispositivos involucrados y se ejecutan los comandos de verificación luego de la configuración.

3.1 Configuración de Red Capa 2 para Switch D1

```
interface range g1/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g0/1-2
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
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
interface g2/1
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end
```

Configuración de Interfaces
Corrige el estándar de la interface
Convierte link de interfaces en trunk
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal

Configuración de Interfaces
Corrige el estándar de la interface
Convierte link de interface en trunk
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal

Topología de árbol de expansión
Configura Vlans como raiz primaria
Configura Vlan como secundaria
Configuración de Interfaces
Configura el puerto como troncal
Configura puerto de acceso
Permite acceso a red capa 2
No apagar terminal

Figura 19. Configuración de Red Capa 2 para Switch D1

```
*Nov 28 19:53:29.708: %EC-5-L3DONTBNL2: Gi1/3 suspended: LACP currently not enabled on the remote port.
*Nov 28 19:53:30.014: %EC-5-L3DONTBNL2: Gi1/2 suspended: LACP currently not enabled on the remote port.
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

D1(config-if-range)#no shutdown
D1(config-if-range)#
*Nov 28 19:54:04.233: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Nov 28 19:54:04.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
D1(config-if-range)#exit
D1(config)#
*Nov 28 19:54:13.553: %EC-5-L3DONTBNL2: Gi0/1 suspended: LACP currently not enabled on the remote port.
*Nov 28 19:54:14.033: %EC-5-L3DONTBNL2: Gi0/2 suspended: LACP currently not enabled on the remote port.
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface g2/1
D1(config-if)#switchport mode access
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#no shutdown
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#end
D1#
*Nov 28 19:54:43.631: %LINK-3-UPDOWN: Interface GigabitEthernet2/1, changed state to up
D1#
*Nov 28 19:54:44.630: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/1, changed state to up
*Nov 28 19:54:44.977: %SYS-5-CONFIG_I: Configured from console by console
D1#
D1#
```

Comprobación utilizando el comando “show run | include spanning-tree”, se deja registro de la hora y fecha

Figura 20. show run | include spanning-tree D1

```
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast edge
D1#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
```

Comprobación utilizando el comando “show run interface”, se deja registro de la hora y fecha

Figura 21. show run interface en D1

```
D1#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 16:45 27/11/2021

3.2 Configuración de Red Capa 2 para D2

```
interface range g1/0-3
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g0/1-2
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
interface g2/1
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
```

*Configuración de Interfaces
Convierte link de interfaces en trunk
Corrige el estándar de la interface
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal*

*Configuración de Interfaces
Convierte link de interface en trunk
Corrige el estándar de la interface
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal*

*Topología de árbol de expansión
Configura Vlans como raiz primaria
Configura Vlan como secundaria
Configuración de Interfaces
Configura el puerto como troncal
Configura puerto de acceso
Permite acceso a red capa 2
No apagar terminal*

Figura 22. Configuración de Red Capa 2 para D2

```

Nov 27 21:52:43.119: %SYS-5-CONFIG_I: Configured from console by console
D2#
D2#spanning-tree mode rapid-pvst
^
% Invalid input detected at '^' marker.

D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
^
% Invalid input detected at '^' marker.

D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#
D2(config)#interface g1/3
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(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

Spanning-tree has been configured on GigabitEthernet1/3 but will only
have effect when the interface is in a non-trunking mode.
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
Nov 27 21:54:50.394: %LINK-3-UPDOWN: Interface GigabitEthernet1/3, changed state
to up
Nov 27 21:54:50.558: %LINK-3-UPDOWN: Interface Vlan102, changed state to up
Nov 27 21:54:51.394: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthe
rnet1/3, changed state to up
D2(config)#en
Nov 27 21:54:51.568: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, cha
nged state to up
D2(config)#end
D2#
Nov 27 21:54:54.928: %SYS-5-CONFIG_I: Configured from console by console
D2#

```

Se comprueba la configuración utilizando el comando “show interface trunk”, se registra hora y fecha.

Figura 23. show interface trunk para D2

```

Nov 28 20:37:46.482: %SYS-5-CONFIG_I: Configured from console by console
D2#show interface trunk

Port      Mode           Encapsulation  Status        Native vlan
-----
Po12     auto           802.1q         trunking      999

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

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

Port      Vlans in spanning tree forwarding state and not pruned
-----
Po12     1,100-102,999
D2#

```

Se comprueba la configuración utilizando el comando “show run | include spanning-tree”, se registra hora y fecha.

Figura 24. show run | include spanning-tree D2

```
% Unknown command or computer name, or unable to find computer address
D2#enable
D2#show interface trunk
D2#
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
spanning-tree portfast edge
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All r

ESP 16:57 27/11/2021

Se comprueba la configuración utilizando el comando “show run interface g1/3”, se registra hora y fecha.

Figura 25. show run interface D2

```
spanning-tree portfast edge
D2#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/3
 switchport access vlan 102
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All r

ESP 16:58 27/11/2021

3.3 Configuración de Red Capa 2 para A1

```
spanning-tree mode rapid-pvst
interface range f0/0-1
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range f1/0-1
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface f1/14
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface f1/15
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
```

Topología de árbol de expansión
Configuración de Interfaces
Convierte link de interfaces en trunk
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal

Configuración de Interfaces
Convierte link de interfaces en trunk
Convierte Vlan en enlace troncal
Crea EthernetChannel y lo activa
No apagar terminal

Configuración de Interface
Configura el puerto como troncal
Configura puerto de acceso
Permite acceso a red capa 2
No apagar terminal

Configuración de Interface
Configura el puerto como troncal
Configura puerto de acceso
Permite acceso a red capa 2
No apagar terminal

Figura 26. Configuración de Red Capa 2 para A1

```
A1(config-if)#switchport mode trunk
A1(config-if)#switch
*Mar 1 00:43:52.583: %DTP-5-TRUNKPORTON: Port Fa1/1 has become dot1q trunk
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#channel-group 1 mode active
^
% Invalid input detected at '^' marker.

A1(config-if)#no shutdown
A1(config-if)#
A1(config-if)#
A1(config-if)#
A1(config-if)#
A1(config-if)#
A1(config-if)#interface f1/15
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(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 spanning tree loops.
Use with CAUTION

*Portfast has been configured on FastEthernet1/15 but will only
have effect when the interface is in a non-trunking mode.
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface f1/14
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(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 spanning tree loops.
Use with CAUTION

*Portfast has been configured on FastEthernet1/14 but will only
have effect when the interface is in a non-trunking mode.
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#
```

Se comprueba la configuración utilizando el comando “show run interface”, se registra hora y fecha

Figura 27. show run interface

```
*Mar 1 00:47:36.659: %SYS-5-CONFIG_I: Configured from console by console
A1#show run interface f1/15
Building configuration...

Current configuration : 86 bytes
!
interface FastEthernet1/15
 switchport access vlan 101
 spanning-tree portfast
end

A1#show run interface f1/14
Building configuration...

Current configuration : 86 bytes
!
interface FastEthernet1/14
 switchport access vlan 100
 spanning-tree portfast
end

A1#
```

4. Configuración de los Protocolos de Enrutamiento

Tabla N°3. Configuración de protocolos de enrutamiento

TAREA	ESPECIFICACIONES
<p>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.</p>	<p>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</p>
<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 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</p>
<p>En R2 en la “Red ISP”, configure MP-BGP.</p>	<p>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).</p>
<p>En R1 en la “Red ISP”, configure MP-BGP.</p>	<p>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.</p>

4.1 Router R1

```
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
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface g1/0
ipv6 ospf 6 area 0
exit
interface s3/3
ipv6 ospf 6 area 0
exit
!
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
!
router bgp 300
bgp router-id 1.1.1.1
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
```

*Configuración de IPV4 en OSPF
Asignación de Id al router
Configuración de área
Configuración de área
Información predeterminada*

*Configuración de IPV6 en OSPF
Se establece Id
Información predeterminada*

*Interface para configuración
Designación de área 0 en IPV6*

*Interface para configuración
Designación de área 0 en IPV6*

*Interfaz para null en IPv4
Interfaz para null en IPv6*

*Intercambio de Información
Se asigna id para el router
Relación vecina para IPv4
Relación vecina para IPv6
Configuración para IPv4*

*Configura red y mascara
Cierra configuración de la familia
Configuración para IPv6*

*Configuración del area
Cierra configuración de la familia*

Figura 28. Configuración de enrutamiento R1

```
R1#
R1#
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface s3/3
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#!
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#!
R1(config)#router bgp 200
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)#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)#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)#exit
R1(config)#
```

Verificamos la configuración con el comando “show run | section ^router ospf”, se deja registro de fecha y hora.

Figura 29. show run | section ^router ospf en R1

```
*Nov 27 17:33:54.639: %SYS-5-CONFIG_I: Configured from console by console
R1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
R1#
```

Verificamos la configuración con el comando “show run | section ^ipv6 router”, se deja registro de fecha y hora.

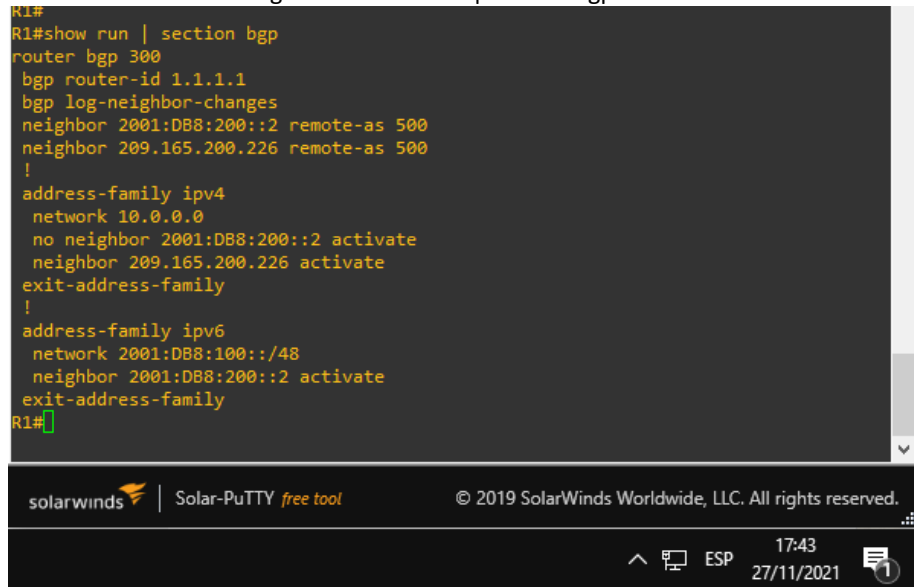
Figura 30. show run | section ^ipv6 router en R1

```
default-information originate
R1#show run | section ^ipv6 router
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
Se3/3 6 0 10 64 P2P 0/0
G11/0 6 0 5 1 DR 0/0
R1#
```

Verificamos la configuración con el comando “show run | section bgp”, se deja registro de fecha y hora.

Figura 31. show run | section bgp en R1

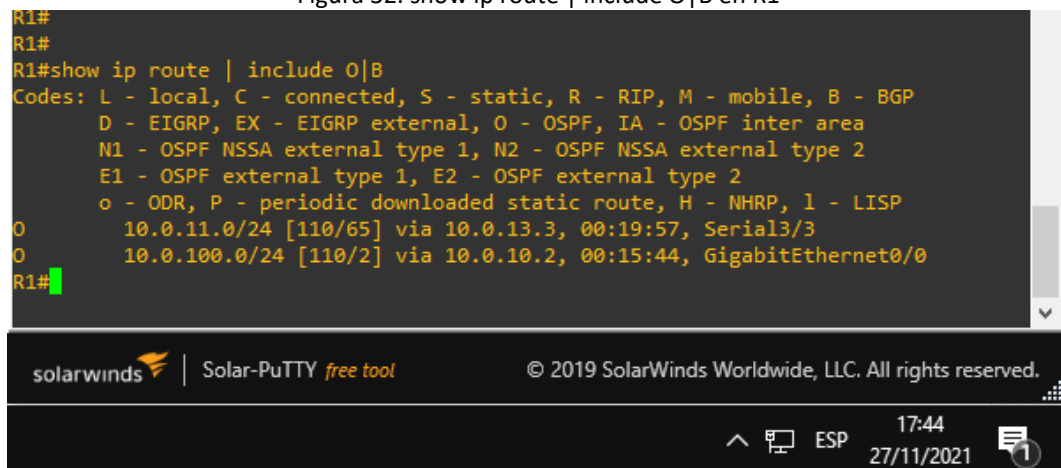
```
R1#
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate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



Verificamos la configuración con el comando “show ip route | include O|B”, se deja registro de fecha y hora.

Figura 32. show ip route | include O|B en R1

```
R1#
R1#
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
O      10.0.11.0/24 [110/65] via 10.0.13.3, 00:19:57, Serial3/3
O      10.0.100.0/24 [110/2] via 10.0.10.2, 00:15:44, GigabitEthernet0/0
R1#
```



Verificamos la configuración con el comando “show ipv6 route”, se deja registro de fecha y hora.

Figura 33. show ipv6 route en R1

```

R1#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - IISP
B ::/0 [20/0]
   via FE80::12:1, GigabitEthernet1/0
S 2001:DB8:100::/48 [1/0]
   via Null0, directly connected
C 2001:DB8:100:1010::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001:DB8:100:1010::1/128 [0/0]
   via GigabitEthernet0/0, receive
O 2001:DB8:100:1011::/64 [110/65]
   via FE80::3:3, Serial3/3
C 2001:DB8:100:1013::/64 [0/0]
   via Serial3/3, directly connected
L 2001:DB8:100:1013::1/128 [0/0]
   via Serial3/3, receive
C 2001:DB8:200::/64 [0/0]
   via GigabitEthernet1/0, directly connected
L 2001:DB8:200::1/128 [0/0]
   via GigabitEthernet1/0, receive
L FF00::/8 [0/0]
   via Null0, receive
R1#
R1#

```

4.2 Router R2

```

ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family

```

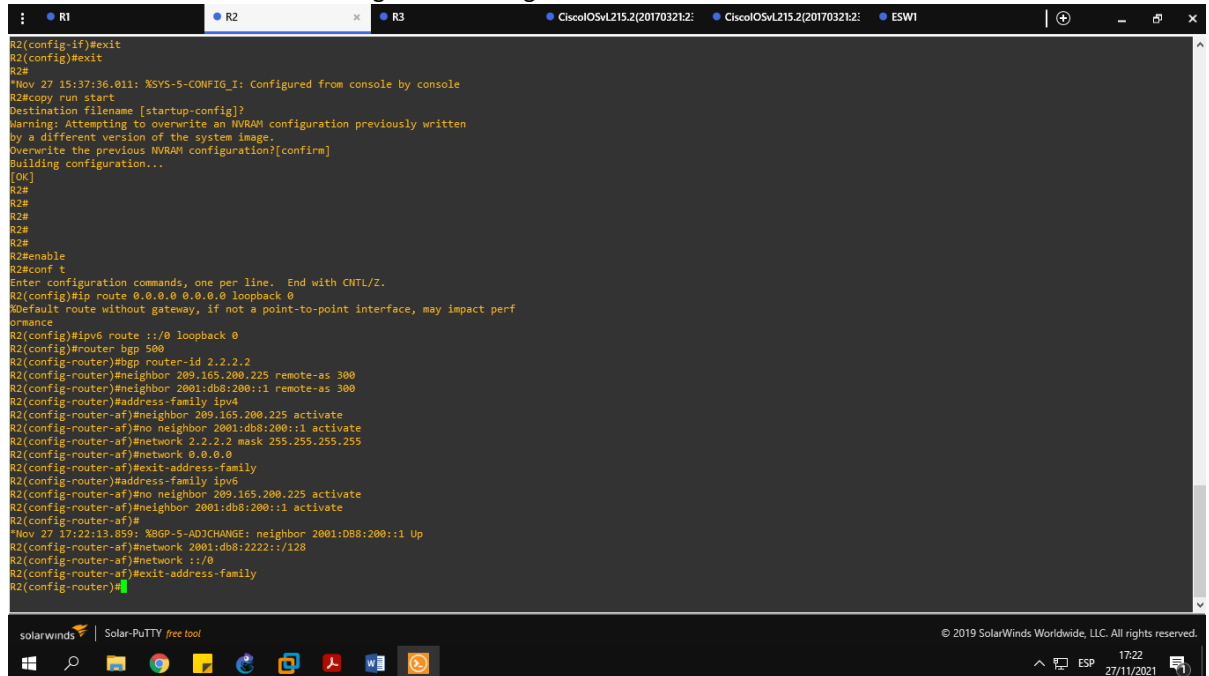
*Se declara la IP para Loopback
Configuración de IPv6 en OSPF
Intercambio de Información
Define id del router
Relación vecina para IPv4
Relación vecina para IPv6
Configuración para IPv4*

Configura red y mascara

*Salir del grupo familiar
Configuración para IPv6*

Salir del grupo familiar

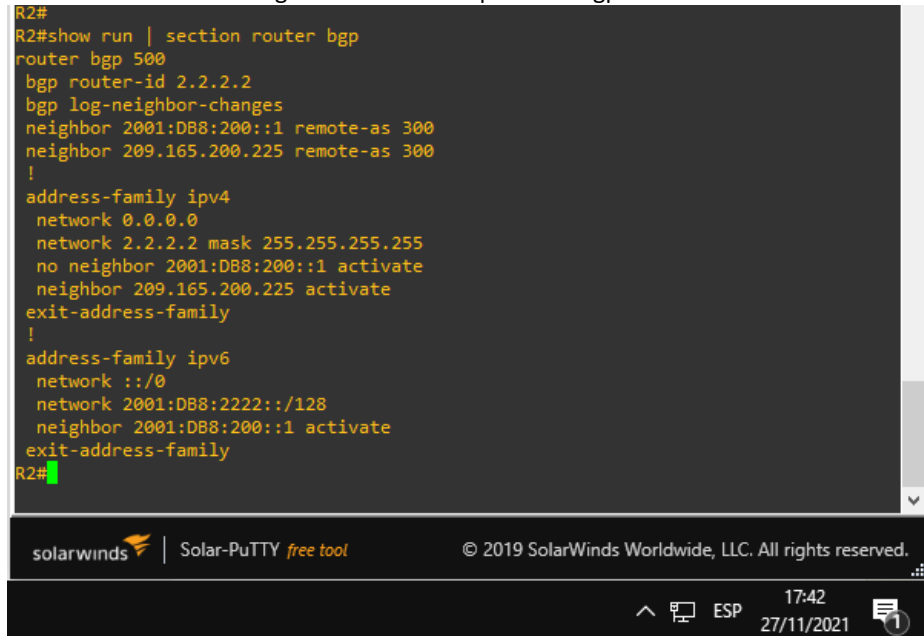
Figura 34. Configuración de enrutamiento R2



```
R2(config-if)#exit
R2(config)#exit
R2#
*Nov 27 15:37:36.011: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
R2#
R2#
R2#
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
!Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#
*Nov 27 17:22:13.859: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#
```

Verificamos la configuración con el comando “show run | section bgp”, se deja registro de fecha y hora.

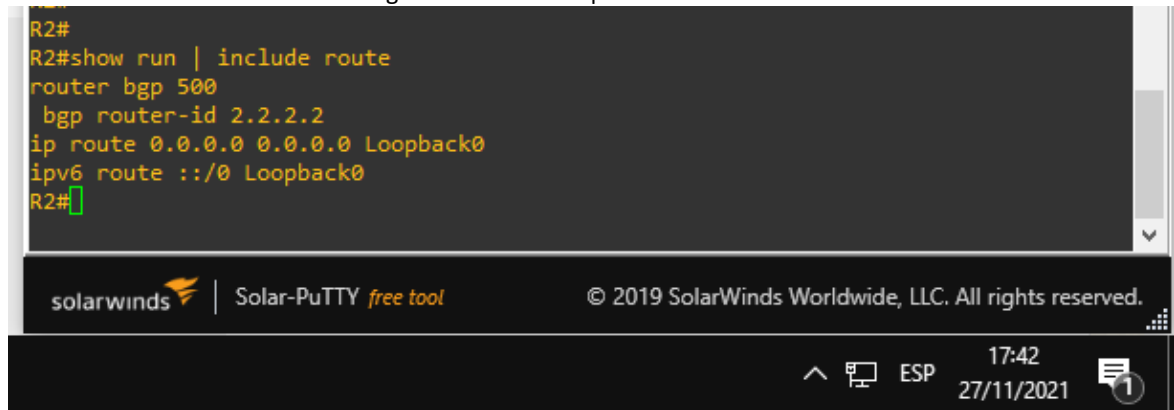
Figura 35. show run | section bgp en R2



```
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
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network ::/0
    network 2001:DB8:2222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#
```

Verificamos la configuración con el comando “show run | include route”, se deja registro de fecha y hora.

Figura 36. show run | include route en R2



```
R2#
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
R2#
```

4.3 Router R3

```
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface g1/0
ipv6 ospf 6 area 0
exit
interface s3/3
ipv6 ospf 6 area 0
exit
end
```

Configuración de IPv4 en OSPF
Se define Id del router
Configuración de área
Configuración de área

Configuración de IPv6 en OSPF
Se define Id del router

Interface a configurar
Designación de área 0 en IPV6

Interface a configurar
Designación de área 0 en IPV6

Figura 37. Configuración de enrutamiento R3

```
R3(config)#exit
R3#
*Nov 27 15:42:29.479: %SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
Destination filename [startup-config]:
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
R3#
R3#
R3#enable
R3#conf t
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)#
*Nov 27 17:23:54.638: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial13/3 from LOA
ADING to FULL, Loading Done
R3(config-router)#exit
R3(config)#ipw router ospf 6
R3(config-mtr)#router-id 0.0.6.3
R3(config-mtr)#exit
R3(config)#interface g0/0
R3(config-if)#ipw ospf 6 area 0
R3(config-if)#exit
R3(config)#interface s3/3
R3(config-if)#ipw ospf 6 area 0
R3(config-if)#exit
R3(config)#e
*Nov 27 17:23:59.471: %OSPF-3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial13/3 from L
OADING to FULL, Loading Done
R3(config)#end
R3#
*Nov 27 17:26:01.247: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

Verificamos la configuración con el comando “show run | section ^router ospf”, se deja registro de fecha y hora.

Figura 38. show run | section ^router ospf en R3

```
R3#
*Nov 27 17:26:01.247: %SYS-5-CONFIG_I: Configured from console by console
R3#
R3#
R3#show run | section ^router ospf
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
R3#
```

Verificamos la configuración con el comando “show ipv6 ospf interface brief”, se deja registro de fecha y hora.

Figura 39. show ipv6 ospf interface brief en R3

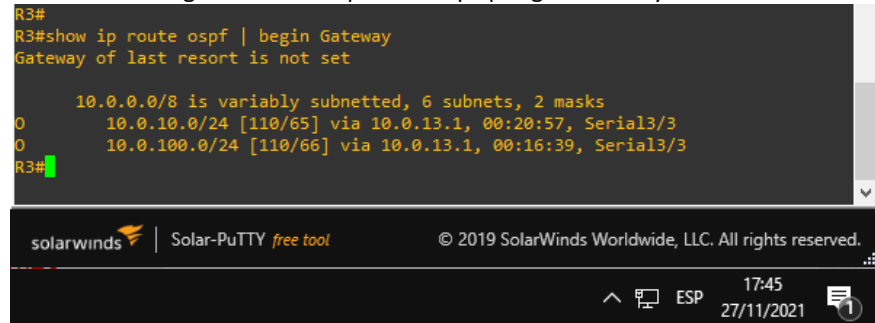
```
R3#show ipv6 ospf interface brief
Interface PID Area Intf ID Cost State Nbrs F/C
Se3/3 6 0 10 64 P2P 1/1
Gi0/0 6 0 4 1 DR 0/0
R3#
```

Verificamos la configuración con el comando “show ip route ospf | begin Gateway”, se deja registro de fecha y hora.

Figura 40. show ip route ospf | begin Gateway en R3

```
R3#
R3#show ip route ospf | begin Gateway
Gateway of last resort is not set

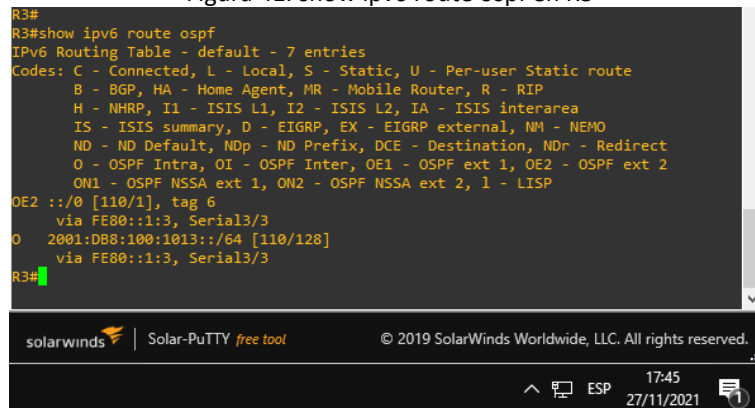
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.0.10.0/24 [110/65] via 10.0.13.1, 00:20:57, Serial3/3
O       10.0.100.0/24 [110/66] via 10.0.13.1, 00:16:39, Serial3/3
R3#
```



Verificamos la configuración con el comando “show ipv6 route ospf”, se deja registro de fecha y hora.

Figura 41. show ipv6 route ospf en R3

```
R3#
R3#show ipv6 route ospf
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, L - LISP
OE2 ::/0 [110/1], tag 6
    via FE80::1:3, Serial3/3
O    2001:DB8:100:1013::/64 [110/128]
    via FE80::1:3, Serial3/3
R3#
```



4.4 SWITCH D1

```
router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/0
exit
ipv6 router ospf 6
router-id 0.0.6.131
```

Configuración de IPv4 en OSPF

Se define id del router

Configuración de área

Configuración de área

Configuración de área

Configuración de área

Interface sin actualizaciones

Interface sin envío de datos

Configuración de IPv6 en OSPF

Se define id del router

```

passive-interface default
no passive-interface g0/0
exit
interface g0/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit

```

*Interface sin actualizaciones
Interface sin envío de datos*

*Interface a configurar
Designación de área 0 en IPv6*

*Interface a configurar VLAN
Designación de área 0 en IPv6*

*Interface a configurar VLAN
Designación de área 0 en IPv6*

*Interface a configurar VLAN
Designación de área 0 en IPv6*

Figura 42. Configuración de enrutamiento D1

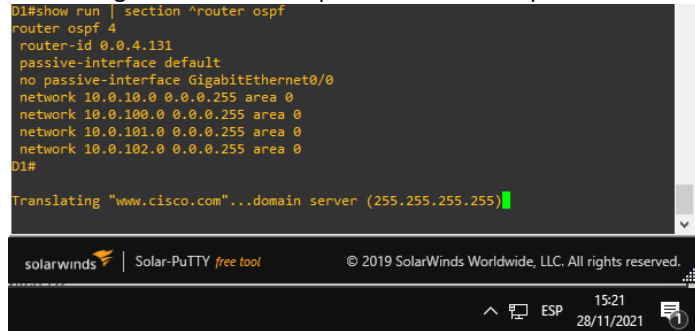
```

D1#
D1#
D1#
D1#enable
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 6
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 g1/2
D1(config-router)#
*Nov 27 22:27:41.125: %OSPF-5-ADJCHG: Process 6, Nbr 0.0.4.1 on GigabitEthernet1/2
from LOADING to FULL, Loading Done
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
D1(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.
D1(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.
D1(config)#interface g1/2
D1(config-if)#ipv6 ospf 6 area 0
^
% Invalid input detected at '^' marker.
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
^
% Invalid input detected at '^' marker.
D1(config-if)#exit
D1(config)#exit
D1#
*Nov 27 22:29:38.738: %SYS-5-CONFIG_I: Configured from console by console
D1#

```

Verificamos la configuración con el comando “show run | section ^router ospf”, se deja registro de fecha y hora.

Figura 43. show run | section ^router ospf en D1



```
D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface GigabitEthernet0/0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
D1#
Translating "www.cisco.com"...domain server (255.255.255.255)
```

4.5 SWITCH D2

```
router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/0
exit
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g0/0
exit
interface g0/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

*Configuración de IPv4 en OSPF
Designación de ID para swiytch*

Configuración de área

Configuración de área

Configuración de área

Configuración de área

Interface sin actualizaciones

Interface sin envío de datos

Configuración de IPv6 en OSPF

Interface sin actualizaciones

Interface sin envío de datos

Interface a configurar

Designación de área 0 en IPv6

Interface a configurar

Designación de área 0 en IPv6

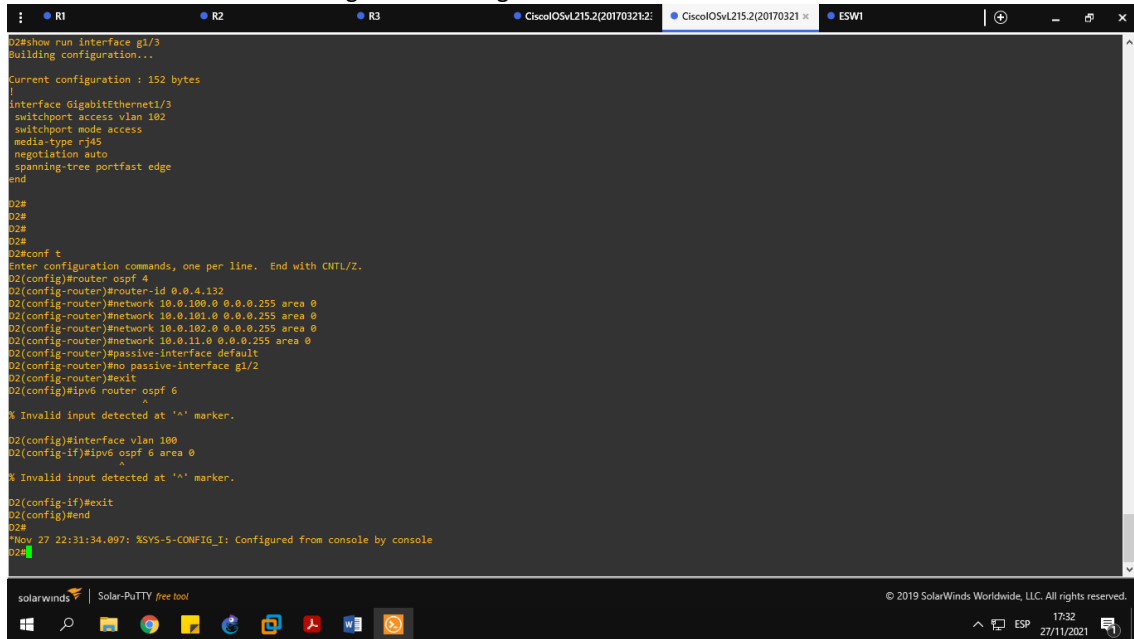
Interface a configurar

Designación de área 0 en IPv6

Interface a configurar

Designación de área 0 en IPv6

Figura 44. Configuración de enrutamiento D2

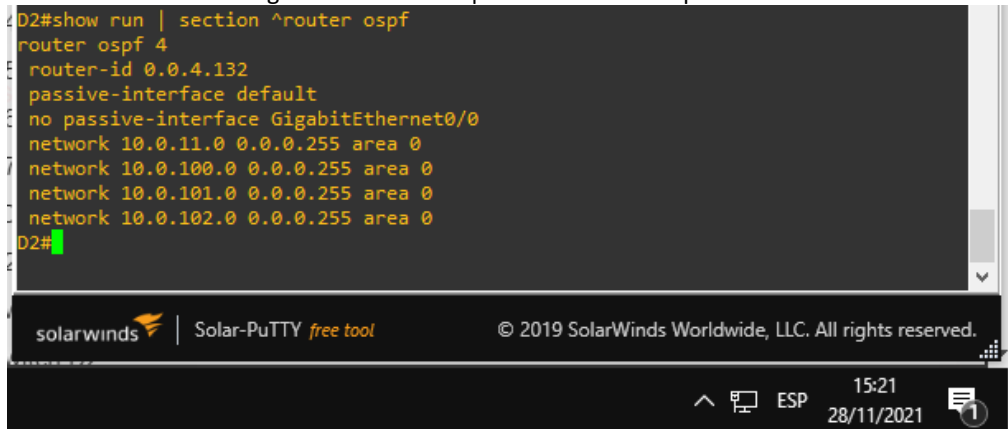


```
D2#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/3
 switchport access vlan 102
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
!
D2#
D2#
D2#
D2#
D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/2
D2(config-router)#exit
D2(config)#ip v6 router ospf 6
!
% Invalid input detected at '^' marker.
D2(config)#interface vlan 100
D2(config-if)#ip v6 ospf 6 area 0
!
% Invalid input detected at '^' marker.
D2(config-if)#exit
D2(config)#end
!
*Nov 27 22:31:34.097: %SYS-5-CONF1G_I: Configured from console by console
D2#
```

Verificamos la configuración con el comando “show run | section ^router ospf”, se deja registro de fecha y hora

Figura 45. show run | section ^router ospf en D2



```
D2#show run | section ^router ospf
router ospf 4
 router-id 0.0.4.132
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.101.0 0.0.0.255 area 0
 network 10.0.102.0 0.0.0.255 area 0
D2#
```

5. Configurar la redundancia del primer salto

Tabla N°4. Tareas Configuración de Redundancia

TAREA	ESPECIFICACIONES
<p>En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.</p>	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
<p>En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.</p>	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
<p>En D1 configure HSRPv2</p>	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p>

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

5.1 Switch D1

ip sla 4	<i>Servidor a configurar IPV4</i>
icmp-echo 10.0.10.1	<i>IP a configurar</i>
frequency 5	<i>Chequeo Disponibilidad de interface cada 5 s</i>
exit	
ip sla 6	<i>Servidor a configurar IPV6</i>
icmp-echo 2001:db8:100:1010::1	<i>IP a configurar</i>
frequency 5	<i>Chequeo Disponibilidad de interface cada 5 s</i>
exit	
ip sla schedule 4 life forever start-time now	<i>Se deja habilitada la IP</i>
ip sla schedule 6 life forever start-time now	<i>Se deja habilitada la IP</i>
track 4 ip sla 4	<i>Actualiza estatus de conexión IPV4</i>
delay down 10 up 15	<i>Tiempo de notificación</i>
exit	
track 6 ip sla 6	<i>Actualiza estatus de conexión IPV6</i>
delay down 10 up 15	<i>Tiempo de notificación</i>
exit	
interface vlan 100	<i>Configuración VLAN100</i>
standby version 2	<i>Configuración HSRP</i>
standby 104 ip 10.0.100.254	<i>IP Virtual</i>
standby 104 priority 150	<i>Prioridad 150</i>
standby 104 preempt	<i>Configuración de preferencia</i>
standby 104 track 4 decrement 60	<i>Rastreo y decremento</i>
standby 106 ipv6 autoconfig	<i>Asigna dirección automática</i>
standby 106 priority 150	<i>Prioridad 150</i>
standby 106 preempt	<i>Configuración de preferencia</i>
standby 106 track 6 decrement 60	<i>Rastreo y decremento</i>
exit	
interface vlan 101	<i>Configuración VLAN101</i>
standby version 2	<i>Configuración HSRP</i>
standby 114 ip 10.0.101.254	<i>IP Virtual</i>
standby 114 preempt	<i>Configuración de preferencia</i>
standby 114 track 4 decrement 60	<i>Rastreo y decremento</i>
standby 116 ipv6 autoconfig	<i>Asigna dirección automática</i>
standby 116 preempt	<i>Configuración de preferencia</i>
standby 116 track 6 decrement 60	<i>Rastreo y decremento</i>
exit	
interface vlan 102	<i>Configuración VLAN102</i>
standby version 2	<i>Configuración HSRP</i>
standby 124 ip 10.0.102.254	<i>IP Virtual</i>

```
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
```

Prioridad 150
Configuración de preferencia
Rastreo y decremento
Asigna dirección automática
Prioridad 150
Configuración de preferencia
Rastreo y decremento

Figura 46. Configuración de Redundancia para D1



```
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#
*Nov 27 22:49:30.538: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
*Nov 27 22:49:55.307: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
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 27 22:51:18.019: %SYS-5-CONFIG_I: Configured from console by console
D1#
```

Figura 47. show run | section ip sla para D1

```
D1#show run | section ip sla
*Nov 28 20:22:01.084: %TRACK-6-STATE: 6 ip sla 6 state Down -> Uptrack 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
*Nov 28 20:22:03.885: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
*Nov 28 20:22:04.238: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Standby -> Active
*Nov 28 20:22:04.652: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
*Nov 28 20:22:04.864: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby -> Active
D1#
*Nov 28 20:22:04.958: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Active
*Nov 28 20:22:05.055: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
D1#
```

Verificamos la configuración con el comando “show standby brief”, se deja registro de fecha y hora

Figura 48. show standby brief para D1

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

5.2 Switch D2

ip sla 4	<i>Servidor a configurar IPV4</i>
icmp-echo 10.0.11.1	<i>IP a configurar</i>
frequency 5	<i>Chequeo Disponibilidad de interface cada 5 s</i>
exit	
ip sla 6	<i>Servidor a configurar IPV6</i>
icmp-echo 2001:db8:100:1011::1	<i>IP a configurar</i>
frequency 5	<i>Chequeo Disponibilidad de interface cada 5 s</i>
exit	
ip sla schedule 4 life forever start-time now	<i>Se deja habilitada la IP</i>
ip sla schedule 6 life forever start-time now	<i>Se deja habilitada la IP</i>
track 4 ip sla 4	<i>Actualiza estatus de conexión IPV4</i>
delay down 10 up 15	<i>Tiempo de notificación</i>
exit	
track 6 ip sla 6	<i>Actualiza estatus de conexión IPV6</i>
delay down 10 up 15	<i>Tiempo de notificación</i>
exit	
interface vlan 100	<i>Configuración VLAN100</i>
standby version 2	<i>Configuración HSRP</i>
standby 104 ip 10.0.100.254	<i>IP Virtual</i>
standby 104 preempt	<i>Configuración de preferencia</i>
standby 104 track 4 decrement 60	<i>Rastreo y decremento</i>
standby 106 ipv6 autoconfig	<i>Asigna dirección automática</i>
standby 106 preempt	<i>Configuración de preferencia</i>
standby 106 track 6 decrement 60	
exit	
interface vlan 101	<i>Configuración VLAN101</i>
standby version 2	<i>Configuración HSRP</i>
standby 114 ip 10.0.101.254	<i>IP Virtual</i>
standby 114 priority 150	<i>Prioridad 150</i>
standby 114 preempt	<i>Configuración de preferencia</i>
standby 114 track 4 decrement 60	<i>Rastreo y decremento</i>
standby 116 ipv6 autoconfig	<i>Asigna dirección automática</i>
standby 116 priority 150	<i>Prioridad 150</i>
standby 116 preempt	<i>Configuración de preferencia</i>
standby 116 track 6 decrement 60	<i>Rastreo y decremento</i>
exit	
interface vlan 102	<i>Configuración VLAN102</i>
standby version 2	<i>Configuración HSRP</i>
standby 124 ip 10.0.102.254	<i>IP Virtual</i>

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

*Configuración de preferencia
Rastreo y decremento
Asigna dirección automática
Configuración de preferencia
Rastreo y decremento*

Figura 49. Configuración de Redundancia para D2

```
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#interface vian 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vian 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vian 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#e
*Nov 27 22:55:46.463: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby -> Active
K
D2(config-if)#exit
D2(config)#end
D2#
*Nov 27 22:55:51.652: %SYS-5-CONFIG_I: Configured from console by console
D2#
```

Verificamos la configuración con el comando “show run | section ip sla”, se deja registro de fecha y hora

Figura 50. show run | section ip sla para D2

```
D2#show run | section ip sla
track 4 ip sla 4
delay down 10 up 15
track 6 ip sla 6
delay down 10 up 15
ip sla 4
icmp-echo 10.0.11.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001::DB8:100:1011:1
frequency 5
ip sla schedule 6 life forever start-time now
D2#
*Nov 28 20:23:35.458: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Speak -> Standby
*Nov 28 20:23:36.039: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby
D2#
*Nov 28 20:23:37.216: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby
*Nov 28 20:23:37.701: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Speak -> Standby
D2#
```

Verificamos la configuración con el comando “show standby brief”, se deja registro de fecha y hora

Figura 51. show standby brief para D2

```

D2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State   Active        Standby        Virtual IP
Vl100     104 100  P Standby 10.0.100.1   local          10.0.100.254
Vl100     106 100  P Standby FE80::D1:2   local          FE80::5:73FF:FEA0:6A
Vl101     114 150  P Active  local        10.0.101.1    10.0.101.254
Vl101     116 150  P Active  local        FE80::D1:3    FE80::5:73FF:FEA0:74
Vl102     124 100  P Standby 10.0.102.1   local          10.0.102.254
Vl102     126 100  P Standby FE80::D1:4   local          FE80::5:73FF:FEA0:7E
D2#
  
```

6. Seguridad

Tabla N°5. Configuraciones de Seguridad para dispositivos

TAREA	ESPECIFICACIONES
En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"> Nombre de usuario Local: sadmin Nivel de privilegio 15 Contraseña: cisco12345cisco
En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"> Dirección IP del servidor RADIUS es 10.0.100.6. Puertos UDP del servidor RADIUS son 1812 y 1813. Contraseña: \$trongPass
En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> Use la lista de métodos por defecto Valide contra el grupo de servidores RADIUS De lo contrario, utilice la base de datos local.
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 .

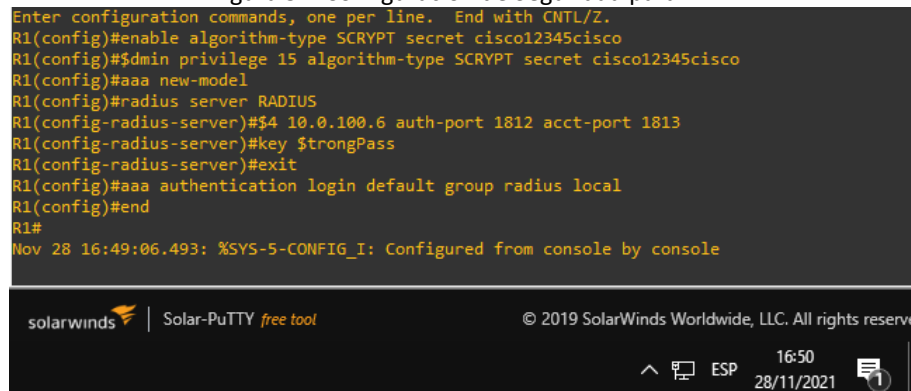
Teniendo en cuenta la tabla de tareas se genera entonces para todos los dispositivos el siguiente código:

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

Se declara modelo AAA
Servidor a Configurar
Ip y puertos
Asignación de Contraseña

6.1 Configuración de Seguridad para R1

Figura 52. Configuración de Seguridad para R1



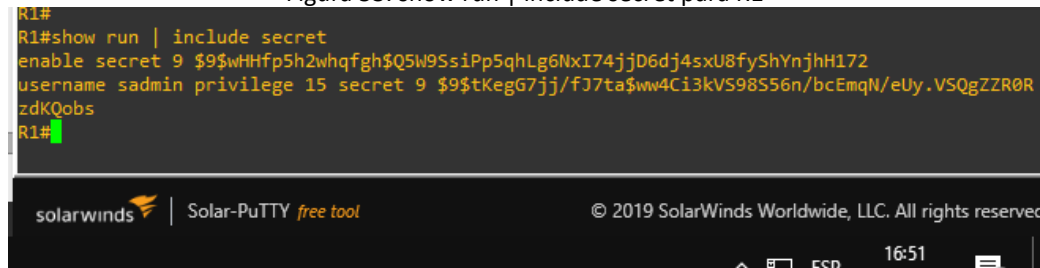
```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)#key $trongPass
R1(config-radius-server)#exit
R1(config)#aaa authentication login default group radius local
R1(config)#end
R1#
Nov 28 16:49:06.493: %SYS-5-CONFIG_I: Configured from console by console
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved

16:50 28/11/2021

Verificamos la configuración con el comando “show run | include secret”, se deja registro de fecha y hora

Figura 53. show run | include secret para R1



```
R1#
R1#show run | include secret
enable secret 9 $9$wHHfp5h2whqfgh$Q5w9SsiPp5qhlG6NxI74jjD6dj4sxU8fyShYnjhH172
username sadmin privilege 15 secret 9 $9$tKegG7jj/fJ7ta$ww4Ci3kVS98S56n/bcEmqN/eUy.VSQgZZR0R
zdKQobs
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved

16:51

Verificamos la configuración con el comando “show run aaa | exclude !”, se deja registro de fecha y hora

Figura 54. show run aaa | exclude ! Para R1

```
R1#
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$aQ3v4HSQBnA3Y4$EgtHs3RcjKDCOuovj6m2Ll0j.M0GDbA/o7jhPd21eE
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $strongPass
aaa new-model
aaa session-id common
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:27 27/11/2021

6.2 Configuración de Seguridad para R2

Figura 55. Configuración de Seguridad para R2

```
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R2(config)#$admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R2(config)#
R2(config)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 16:52 28/11/2021

Verificamos la configuración con el comando “show run | include secret”, se deja registro de fecha y hora

Figura 56. show run | include secret para R2

```
R2#A
*Nov 27 18:17:53.235: %SYS-5-CONFIG_I: Configured from console by console
R2#show run | include secret
enable secret 9 $9$ORimRjVGzG2BeB$ctWZ2uJWZZooQU4hyfGQhRGOynFFw.magLNN8TLrJ46
username sadmin privilege 15 secret 9 $9$sXr1vbIX7UsuxK$gj1w/wiMKZwf90DZHD93I9A2QjNuLN17ZJBW26
URP3o
R2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:24 27/11/2021

6.3 Configuración de Seguridad para R3

Figura 57. Configuración de Seguridad para R3

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)#$admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)#key $strongPass
R3(config-radius-server)#exit
R3(config)#aaa authentication login default group radius local
R3(config)#end
R3#
Nov 28 16:53:58.620: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 16:53 28/11/2021

Verificamos la configuración con el comando “show run aaa | exclude !”, se deja registro de fecha y hora

Figura 58. show run aaa | exclude ! para R3

```
R3#
R3#show run | include secret
enable secret 9 $9$femvD5uFgeHEiR$6kVctaRE6qcKJ8M1kE21Y62yAKswM1KzCFin.PIEyZA
username sadmin privilege 15 secret 9 $9$24RRy1NiEZ1b9K$6mKhCddoX0V7nLuPk9Q5XBRzidHMW6LkKb1HH9
XzAOA
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:25 27/11/2021

Verificamos la configuración con el comando “show run aaa | exclude”, se deja registro de fecha y hora

Figura 59. show run aaa | exclude Para R3

```
R3#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$24RRy1NiEZ1b9K$6mKhCddoX0V7nLuPk9Q5XBRzidHMW6LkKb1HH9
XzAOA
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $strongPass
aaa new-model
aaa session-id common
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:28 27/11/2021

6.4 Configuración de Seguridad para D1

Figura 60. Configuración de Seguridad para D1

```
D1#conf t
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)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)#key $strongPass
D1(config-radius-server)#exit
D1(config)#aaa authentication login default group radius local
D1(config)#end
D1#
Nov 28 16:54:37.226: %SYS-5-CONFIG_I: Configured from console by console
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 16:54 28/11/2021

Verificamos la configuración con el comando “show run | include secret”, se deja registro de fecha y hora

Figura 61. show run | include secret para D1

```
D1#
D1#
D1#show run | include secret
enable secret 9 $9$ruZ1Gv5Nhxl6A2$7EXABtL4y53YTX6/GXwn47H/KQLf9XHvggLfR7EAW2o
username sadmin privilege 15 secret 9 $9$djxkTygQ/UwmIo$Cr5j58QGhVzXpQVNAH.0x3dTkuaFnTkN//EGQc
b9CqM
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:25 27/11/2021

Verificamos la configuración con el comando “show run aaa | exclude !”, se deja registro de fecha y hora

Figura 62. show run aaa | exclude ! para D1

```
D1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$djxkTygQ/UwmIo$Cr5j58QGhVzXpQVNAH.0x3dTkuaFnTkN//EGQc
b9CqM
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $strongPass
aaa new-model
aaa session-id common
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:28 27/11/2021

6.5 Configuración de Seguridad para D2

Figura 63. Configuración de Seguridad para D2

```
D2#conf t
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)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $strongPass
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local
D2(config)#end
D2#
D2#
Nov 28 16:53:28.246: %SYS-5-CONFIG_I: Configured from console by console
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 16:54 28/11/2021

Verificamos la configuración con el comando “show run | include secret”, se deja registro de fecha y hora

Figura 64. show run | include secret para D2

```
D2#
*Nov 27 23:20:43.390: %SYS-5-CONFIG_I: Configured from console by console
D2#show run | include secret
enable secret 9 $9$HRoLLD/RIkINm2$KO.rDNRHsueLB9oKD3up305d/dddGIL8qRFF/dECrV.
username sadmin privilege 15 secret 9 $9$9eA/JpMPhISqM2$XRJ.W1aeb/92HV3JA1ZeQLBk5K5VTXZFfw1YQZ
2hGX.
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:26 27/11/2021

Verificamos la configuración con el comando “show run aaa | exclude !”, se deja registro de fecha y hora

Figura 65. show run aaa | exclude ! para D2

```
D2#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$9eA/JpMPhISqM2$XRJ.W1aeb/92HV3JA1ZeQLBk5K5VTXZFfw1YQZ
2hGX.
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $strongPass
aaa new-model
aaa session-id common
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 18:28 27/11/2021

7. Configure las funciones de Administración de Red

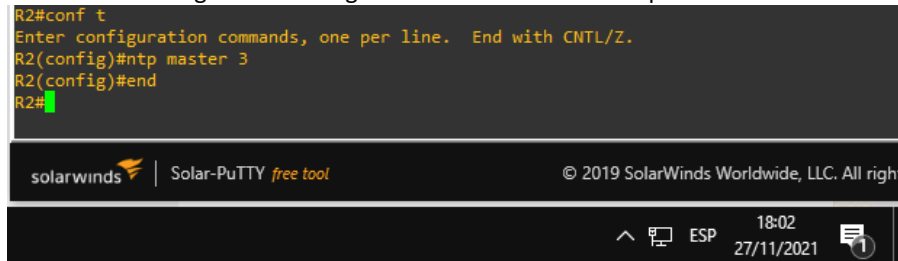
Tabla N°6 - Configuraciones de Administración de Red para los dispositivos

TAREA	ESPECIFICACIONES
En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none">• R1 debe sincronizar con R2.• R3, D1 y A1 para sincronizar la hora con R1.• D2 para sincronizar la hora con R3.
Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: <ul style="list-style-type: none">• Únicamente se usará SNMP en modo lectura (Read-Only).• Limite el acceso SNMP a la dirección IP de la PC1.• Configure el valor de contacto SNMP con su nombre.• Establezca el <i>community string</i> en ENCORSA.• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.• En R1, habilite el envío de <i>traps bgp, config, y ospf</i>.• En A1, habilite el envío de <i>traps config</i>.

7.1 Configuración de Administración para Router R2:

```
ntp master 3  
end
```

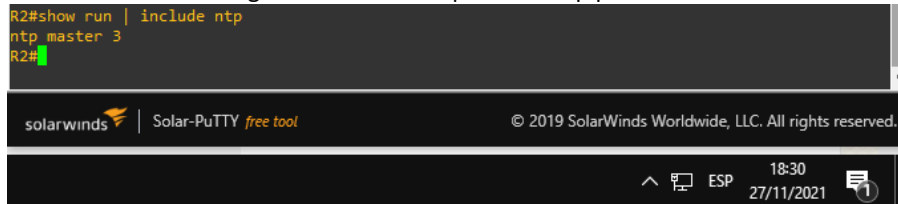
Figura 66. Configuración de Administración para R2



```
R2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#ntp master 3  
R2(config)#end  
R2#
```

Verificamos la configuración con el comando “show run | include ntp”, se deja registro de fecha y hora.

Figura 67. show run | include ntp para R2



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

7.2 Configuración de Administración para 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
```

```
snmp-server enable traps ospf
```

```
end
```

Configuración de NTP

Syslogs level warning

Configura dirección de host

Configuración de estado ON

SNMP se setea para lectura

Asignación de limite

Configuración de contacto

Declaración de Host

Habilita envío de bgp

Habilita envío de traps

Habilita envío de ospf traps

Figura 68. Configuración de administración para R1

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

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#!enable and enter password
R1(config)#ntp server 2.2.2.2
R1(config)#logging trap warning
R1(config)#logging host 10.0.100.5
R1(config)#logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#permit host 10.0.100.5
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Cisco Student
R1(config)#snmp-server community ENCORSA ro SNMP-NMS
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)#snmp-server ifindex persist
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#end
R1#
*Nov 27 18:05:06.183: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:05 27/11/2021

Verificamos la configuración con el comando “show ntp status | include stratum”, se deja registro de fecha y hora.

Figura 69. show ntp status | include stratum para R1

```
R1#
Nov 27 18:33:29.607: %SYS-5-CONFIG_I: Configured from console by console
R1#show ntp status | include stratum
Clock is unsynchronized, stratum 3, reference is 127.127.1.1
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:35 27/11/2021

Verificamos la configuración con el comando “show run | include logging”, se deja registro de fecha y hora.

Figura 70. show run | include logging para R1

```
R1#show run | include logging
logging trap warnings
logging host 10.0.100.5
  logging synchronous
logging synchronous
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

ESP 18:37 27/11/2021

Verificamos la configuración con el comando “show run | include snmp”, se deja registro de fecha y hora.

Figura 71. show run | include snmp para R1

```
logging synchronous
R1#
R1#
R1#
R1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

ESP 18:39 27/11/2021

7.3 Configuración de Administración para Router R3

ntp server 10.0.10.1	<i>Configuración de NTP</i>
logging trap warning	<i>Syslogs level warning</i>
logging host 10.0.100.5	<i>Configura dirección de host</i>
logging on	<i>Configuración de estado ON</i>
ip access-list standard SNMP-NMS	<i>SNMP se setea para lectura</i>
permit host 10.0.100.5	<i>Asignación de limite</i>
exit	
snmp-server contact Cisco Student	<i>Configuración de contacto</i>
snmp-server community ENCORSA ro SNMP-NMS	
snmp-server host 10.0.100.5 version 2c ENCORSA	<i>Declaración de Host</i>
snmp-server ifindex persist	<i>Habilita envío de bgp</i>
snmp-server enable traps config	<i>Habilita envío de traps</i>
snmp-server enable traps ospf	<i>Habilita envío de ospf traps</i>
end	

Figura 72. Configuración de Administración para R3

```
R3#
R3#enable
R3#conf t
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
R3#
*Nov 27 18:07:36.327: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:07 27/11/2021

Verificamos la configuración con el comando “show run | include snmp”, se deja registro de fecha y hora.

Figura 73. show run | include snmp para R3

```
R3#
R3#
R3#
R3#
R3#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:39
27/11/2021

7.4 Configuración de Administración para Switch D1

ntp server 10.0.10.1	<i>Configuración de NTP</i>
logging trap warning	<i>Syslogs level warning</i>
logging host 10.0.100.5	<i>Configura dirección de host</i>
logging on	<i>Configuración de estado ON</i>
ip access-list standard SNMP-NMS	<i>SNMP se setea para lectura</i>
permit host 10.0.100.5	<i>Asignación de limite</i>
exit	
snmp-server contact Cisco Student	<i>Configuración de contacto</i>
snmp-server community ENCORSA ro SNMP-NMS	
snmp-server host 10.0.100.5 version 2c ENCORSA	<i>Declaración de Host</i>
snmp-server ifindex persist	<i>Habilita envío de bgp</i>
snmp-server enable traps config	<i>Habilita envío de traps</i>
snmp-server enable traps ospf	<i>Habilita envío de ospf traps</i>
end	

Figura 74. Configuración de Administración para D1

```
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ntp server 10.0.10.1
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco Student
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.
D1(config)#snmp-server enable traps ospf
D1(config)#snmp-server enable traps conf
^
% Invalid input detected at '^' marker.
D1(config)#end
D1#
*Nov 27 23:08:55.337: %SYS-5-CONFIG_I: Configured from console by console
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:09 27/11/2021

Verificamos la configuración con el comando “show ip access-list SNMP-NMS”, se deja registro de fecha y hora.

Figura 75. show ip access-list SNMP-NMS Para D1

```
D1#
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:38 27/11/2021

7.5 Configuración de Administración para Switch D2

ntp server 10.0.10.1	<i>Configuración de NTP</i>
logging trap warning	<i>Syslogs level warning</i>
logging host 10.0.100.5	<i>Configura dirección de host</i>
logging on	<i>Configuración de estado ON</i>
ip access-list standard SNMP-NMS	<i>SNMP se setea para lectura</i>
permit host 10.0.100.5	<i>Asignación de limite</i>
exit	
snmp-server contact Cisco Student	<i>Configuración de contacto</i>
snmp-server community ENCORSA ro SNMP-NMS	
snmp-server host 10.0.100.5 version 2c ENCORSA	<i>Declaración de Host</i>
snmp-server enable traps config	<i>Habilita envío de traps</i>
snmp-server enable traps ospf	<i>Habilita envío de ospf traps</i>
end	

Figura 76. Configuración de Administración para D2

```
D2#
D2#conf t
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
D2(config)#end
D2#
*Nov 27 23:10:57.535: %SYS-5-CONFIG_I: Configured from console by console
D2#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:11 27/11/2021

Verificamos la configuración con el comando “show run | include snmp”, se deja registro de fecha y hora.

Figura 77. show run | include snmp para D2

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

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:40
27/11/2021

7.6 Configuración de Administración para Switch A1

ntp server 10.0.10.1	<i>Configuración de NTP</i>
logging trap warning	<i>Syslogs level warning</i>
logging host 10.0.100.5	<i>Configura dirección de host</i>
logging on	<i>Configuración de estado ON</i>
ip access-list standard SNMP-NMS	<i>SNMP se setea para lectura</i>
permit host 10.0.100.5	<i>Asignación de limite</i>
exit	
snmp-server contact Cisco Student	<i>Configuración de contacto</i>
snmp-server community ENCORSA ro SNMP-NMS	
snmp-server host 10.0.100.5 version 2c ENCORSA	<i>Declaración de Host</i>
snmp-server ifindex persist	<i>Habilita envío de bgp</i>
snmp-server enable traps config	<i>Habilita envío de traps</i>
snmp-server enable traps ospf	<i>Habilita envío de ospf traps</i>
end	

Figura 78. Configuración de Administración para A1

```
A1#
A1#
A1#conf t
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
A1(config)#snmp-server enable traps ospf
% Cannot enable both sham-link state-change interface traps.
% New sham link interface trap not enabled.
A1(config)#end
A1#
*Mar 1 01:50:11.639: %SYS-5-CONFIG_I: Configured from console by console
A1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:13 27/11/2021

Verificamos la configuración con el comando “show run | include snmp”, se deja registro de fecha y hora.

Figura 79. show run | include snmp Para A1

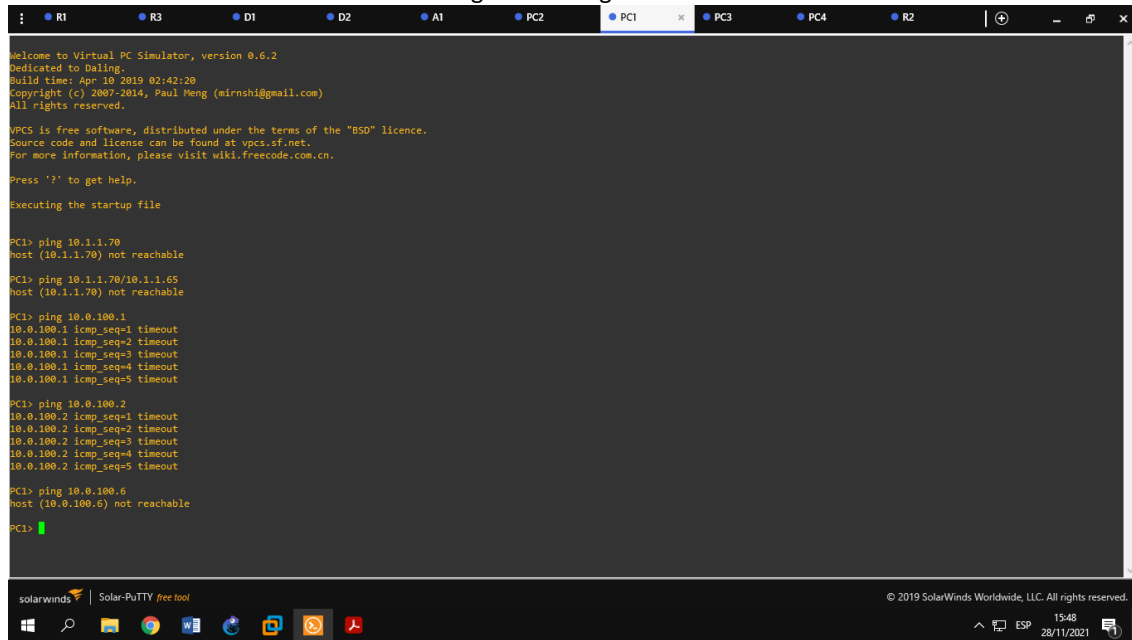
```
A1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps config
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
A1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

18:41 27/11/2021

Se comprueba la conexión entre PCS, como se muestra a continuación:

Figura 80. Ping en PC1



```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ping 10.1.1.70
10.0.100.1 icmp_seq=1 timeout
10.0.100.1 icmp_seq=2 timeout
10.0.100.1 icmp_seq=3 timeout
10.0.100.1 icmp_seq=4 timeout
10.0.100.1 icmp_seq=5 timeout
host (10.1.1.70) not reachable

PC1> ping 10.1.1.70/10.1.1.65
10.0.100.1 icmp_seq=1 timeout
10.0.100.1 icmp_seq=2 timeout
10.0.100.1 icmp_seq=3 timeout
10.0.100.1 icmp_seq=4 timeout
10.0.100.1 icmp_seq=5 timeout
host (10.1.1.70) not reachable

PC1> ping 10.0.100.1
10.0.100.1 icmp_seq=1 timeout
10.0.100.1 icmp_seq=2 timeout
10.0.100.1 icmp_seq=3 timeout
10.0.100.1 icmp_seq=4 timeout
10.0.100.1 icmp_seq=5 timeout

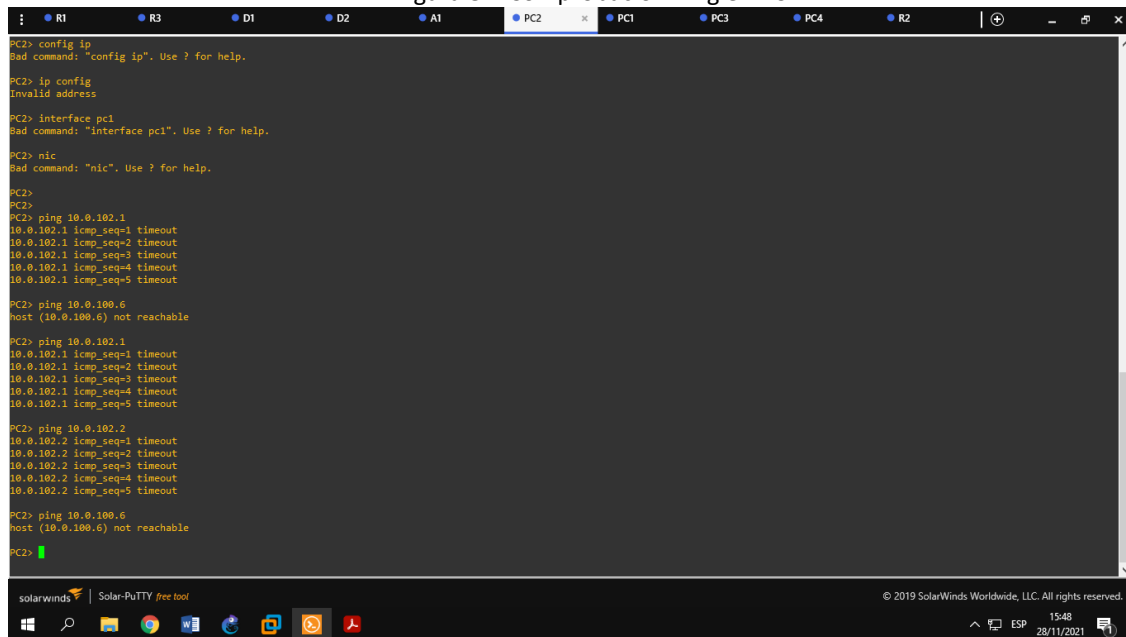
PC1> ping 10.0.100.2
10.0.100.2 icmp_seq=1 timeout
10.0.100.2 icmp_seq=2 timeout
10.0.100.2 icmp_seq=3 timeout
10.0.100.2 icmp_seq=4 timeout
10.0.100.2 icmp_seq=5 timeout

PC1> ping 10.0.100.6
10.0.100.6 icmp_seq=1 timeout
10.0.100.6 icmp_seq=2 timeout
10.0.100.6 icmp_seq=3 timeout
10.0.100.6 icmp_seq=4 timeout
10.0.100.6 icmp_seq=5 timeout
host (10.0.100.6) not reachable

PC1>

```

Figura 81. Comprobación Ping en PC2



```

PC2> config ip
Bad command: "config ip". Use ? for help.

PC2> ip config
Invalid address

PC2> interface pc1
Bad command: "interface pc1". Use ? for help.

PC2> nic
Bad command: "nic". Use ? for help.

PC2>
PC2> ping 10.0.102.1
10.0.102.1 icmp_seq=1 timeout
10.0.102.1 icmp_seq=2 timeout
10.0.102.1 icmp_seq=3 timeout
10.0.102.1 icmp_seq=4 timeout
10.0.102.1 icmp_seq=5 timeout

PC2> ping 10.0.100.6
10.0.100.6 icmp_seq=1 timeout
10.0.100.6 icmp_seq=2 timeout
10.0.100.6 icmp_seq=3 timeout
10.0.100.6 icmp_seq=4 timeout
10.0.100.6 icmp_seq=5 timeout
host (10.0.100.6) not reachable

PC2> ping 10.0.102.1
10.0.102.1 icmp_seq=1 timeout
10.0.102.1 icmp_seq=2 timeout
10.0.102.1 icmp_seq=3 timeout
10.0.102.1 icmp_seq=4 timeout
10.0.102.1 icmp_seq=5 timeout

PC2> ping 10.0.102.2
10.0.102.2 icmp_seq=1 timeout
10.0.102.2 icmp_seq=2 timeout
10.0.102.2 icmp_seq=3 timeout
10.0.102.2 icmp_seq=4 timeout
10.0.102.2 icmp_seq=5 timeout

PC2> ping 10.0.100.6
10.0.100.6 icmp_seq=1 timeout
10.0.100.6 icmp_seq=2 timeout
10.0.100.6 icmp_seq=3 timeout
10.0.100.6 icmp_seq=4 timeout
10.0.100.6 icmp_seq=5 timeout
host (10.0.100.6) not reachable

PC2>

```

Figura 82. Comprobación de Seguridad para R1

```
own R1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username:
*Nov 29 22:13:13.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/3, changed state to up
Username:
*Nov 29 22:13:33.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/3, changed state to do
wn
Username:
% Username: timeout expired!
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

22:14
29/11/2021

CONCLUSIONES

Este diplomado, basado en CCNP, busca probar nuestras capacidades y competencias en orden de generar y formar profesionales capaces de planificar, implementar, verificar y resolver problemas de redes locales.

De acuerdo a la norma de la OSI (modelo de interconexión de sistemas abiertos) hemos trabajado con dispositivos de capa 2 como lo son los switches, en esta capa encontramos el direccionamiento físico y la distribución de la trama de datos; de igual forma en la capa 3 encontramos protocolos como OSPF y BGP que se encargan de identificar el enrutamiento existente entre los dispositivos de la topología, para esto utilizamos los Routers.

El protocolo OSPF es una herramienta de direccionamiento de tipo enlace-estado muy importante para el desarrollo de la topología ya que nos permite escoger la ruta más corta utilizando sus algoritmos en la topología de red escogida que a su vez está basada en un sistema STP (spanning-tree protocol) donde los enlaces redundantes juegan un papel importante para garantizar las activaciones y desactivaciones de los enlaces de conexión que van a ser usados y no respectivamente eliminando la posibilidad de crear bucles de conexión que impidan que la información llegue a destino.

Muy importante también el protocolo BGP, Border Gateway Protocol, para compartir la información de enrutamiento volviendo cualquier topología en eficiente y estable.

REFERENCIAS BIBLIOGRAFICAS

- Bayardo, M. (2021, April 10). *¿Qué es un trunk en red? ¿qué es un trunk en red?* Retrieved November 29, 2021, from <https://aleph.org.mx/que-es-un-trunk-en-red>.
- Michely, Jtx, KaiserFdo, lucian2003, Jfriash, Ginash, Luishr, & EicheS. (2020, January 15). *Que Es y Cómo funciona OSPF (open shortest Pacth first) parte 1*. Comunidad Huawei Enterprise. Retrieved November 29, 2021, from <https://forum.huawei.com/enterprise/es/que-es-y-c%C3%B3mo-funciona-ospf-open-shortest-pacth-first-parte-1/thread/595568-100235>.
- Techopedia. (2017, December 12). *What is internet protocol version 4 (ipv4)? - definition from Techopedia*. Techopedia.com. Retrieved November 29, 2021, from <https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4>.
- Techopedia. (2017, December 12). *What is internet protocol version 4 (ipv4)? - definition from Techopedia*. Techopedia.com. Retrieved November 29, 2021, from <https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4>.
- Vlan de Servicios Avanzados de Red intel®*. Intel. (n.d.). Retrieved November 29, 2021, from <https://www.intel.la/content/www/xl/es/support/articles/000005677/network-and-i-o/ethernet-products.html>.