

**DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

EDWIN LEONARDO RANGEL LUNA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
BARBOSA.
2021**

**DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

EDWIN LEONARDO RANGEL LUNA

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

**DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
BARBOSA.
2021**

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 29 de noviembre de 2021

AGRADECIMIENTOS

A Dios, al concederme la vida y salud, pilares fundamentales para el logro de cada meta, proyecto y sueño propuesto. A la institucionalidad, como lo fueron la Policía Nacional al permitirme el inicio de estudios superiores y capacitarme como técnico en Telemática y Electrónica durante el tiempo laborado; La Universidad Nacional Abierta y a Distancia y sus directivos quienes celebraron un convenio educativo con las Fuerzas Militares y de Policía, motivando con ello la continuidad en la profesionalización personal. A mi Familia, quienes son la razón por la cual me esfuerzo cada día por ser mejor.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	7
LISTA DE FIGURAS.....	8
GLOSARIO	10
RESUMEN.....	12
ABSTRACT.....	12
INTRODUCCIÓN.....	13
DESARROLLO	14
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	15
Router R1	15
Router R2	17
Router R3	19
Switch D1.....	20
Switch D2.....	24
Switch A1.....	27
Parte 2: Configurar la capa 2 de la red y el soporte de Host.	30
Switch D1.....	31
Switch D2.....	33
Switch A1	34
Evidencia parte 2. Resultados mediante comandos	36
Parte 3: Configurar los protocolos de enrutamiento.	41
Router R1	42
Router R2	45
Router R3	46
Switch D1.....	47
Switch D2.....	49
Evidencia parte 3. Resultados mediante comandos	51
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).....	56
Switch D1.....	59

Switch D2.....	63
Evidencia parte 4. Resultados mediante comandos	67
Parte 5: Seguridad.....	68
Router R1	69
Router R2	70
Router R3	70
Switch D1.....	71
Switch D2.....	72
Switch A1	73
Evidencia parte 5. Resultados mediante comandos	74
Parte 6: Configure las funciones de Administración de Red.....	75
Router R1	76
Router R2	77
Router R3	78
Switch D1.....	79
Switch D2.....	80
Switch A1	81
Evidencia parte 6. Resultados mediante comandos	83
CONCLUSIONES	86
BIBLIOGRAFIA.....	87

LISTA DE TABLAS

Tabla 1. Direccionamiento de los dispositivos	15
Tabla 2. Tareas de configuración parte 2.....	30
Tabla 3. Tareas de configuración parte 3.....	41
Tabla 4. Tareas de configuración parte 4.....	56
Tabla 5. Tareas de configuración parte 5.....	68
Tabla 6. Tareas de configuración parte 6.....	75

LISTA DE FIGURAS

Figura 1. Escenario Propuesto	14
Figura 2. Escenario Simulado (GNS3)	14
Figura 3. Comando show.	29
Figura 4. Comando show.	29
Figura 5. Verificación servicios DHCP IPv4 e IPv6 en PC2.	36
Figura 6. Verificación servicios DHCP IPv4 e IPv6 en PC3.	37
Figura 7. Ping con éxito desde PC1 a D1, D1 y PC4.	37
Figura 8. Ping con éxito desde PC2 A D1 y D2.	37
Figura 9. Ping con éxito desde PC3 A D1 y D2.	38
Figura 10. Ping con éxito desde PC4 A D1, D2 y PC1.	38
Figura 11. Comando show interfaces trunk.	38
Figura 12. Comando show interfaces trunk.	39
Figura 13. Comando show run include spanning-tree.	39
Figura 14. Comando show run include spanning-tree.	39
Figura 15. Comando show run interface.	40
Figura 16. Comando show run interface.	40
Figura 17. Comando show run interface.	40
Figura 18. Comando show run section ^router ospf.	51
Figura 19. Comando show run section ^router ospf.	51
Figura 20. Comando show run section ^router ospf.	52
Figura 21. Comando show run section ^router ospf	52
Figura 22. Show run section ^ipv6 router y show ipv6 ospf interface brief.	52
Figura 23. Show run section ^ipv6 router y show ipv6 ospf interface brief.	53
Figura 24. Show run section ^ipv6 router y show ipv6 ospf interface brief.	53
Figura 25. Show run section ^ipv6 router y show ipv6 ospf interface brief.	53
Figura 26. Comando show run section bgp y show run include route.	54
Figura 27. Comando show run section bgp y show run include route.	54
Figura 28. Show ip route include O B para la verificación de OSPF y BGP.	54
Figura 29. Show ipv6 route para la verificación de OSPFv3.	55
Figura 30. Comando show ip route ospf begin Gateway.	55
Figura 31. Comando show ipv6 route ospf.	56
Figura 32. Comando show run section ip sla.	67
Figura 33. Comando show run section ip sla.	67
Figura 34. Comando show standby brief.	67
Figura 35. Comando show run include secret	74
Figura 36. Comando show run aaa exclude !.	74
Figura 37. Conexión a través de TELNET.	75
Figura 38. Verificación de la hora actual en formato UTC.	83

Figura 39. Comando show run include ntp. _____	83
Figura 40. Comando show ntp status include stratum. _____	83
Figura 41. Comando show run include logging. _____	84
Figura 42. Comando show ip access-list SNMP-NMS. _____	84
Figura 43. Comando show run include snmp. _____	84

GLOSARIO

BGP: (Border Gateway Protocol) es un protocolo que permite crear enrutamiento entre dominios sin bucles entre sistemas autónomos (AS). Un AS es un conjunto de enrutadores bajo una única administración técnica. Los enrutadores en un AS pueden usar múltiples Protocolos de puerta de enlace interior (IGP) para intercambiar información de enrutamiento dentro del AS. Los enrutadores pueden usar un protocolo de puerta de enlace exterior para enrutar paquetes fuera del AS.

DHCP: (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de host. Protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.

IPv4: es un sistema de direccionamiento de 32 bits que se utiliza para identificar un dispositivo en una red. Es el sistema de direccionamiento utilizado en la mayoría de las redes informáticas, incluida Internet.

IPv6: es un sistema de direccionamiento de 128 bits que se utiliza para identificar un dispositivo en una red. Es el sucesor de IPv4 y la versión más reciente del sistema de direccionamiento utilizado en las redes informáticas. Actualmente, IPv6 se está implementando en todo el mundo. Una dirección IPv6 se representa en ocho campos de números hexadecimales, cada campo contiene 16 bits. Una dirección IPv6 se divide en dos partes, cada parte compuesta por 64 bits. La primera parte es la dirección de red y la segunda parte la dirección del host.

MSTP: (Multiple Spanning Tree Protocol) es un protocolo que crea múltiples árboles de expansión (instancias) para cada LAN virtual (VLAN) en una sola red física. Esto permite que cada VLAN tenga un puente raíz configurado y una topología de reenvío. Esto reduce el número de unidades de datos de protocolo puente (BPDU) en la red y reduce el estrés en las unidades centrales de procesamiento (CPU) de los dispositivos de red.

NAT: (Network Address Translation ó Traducción de Dirección de Red) es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

OSPF: (Open Shortest Path First) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF).

RSTP: (Rapid Spanning Tree Protocol) es una mejora de STP. RSTP proporciona una convergencia de árbol de expansión más rápida después de un cambio de topología. STP puede tardar de 30 a 50 segundos en responder a un cambio de topología, mientras que RSTP responde dentro de tres veces el

tiempo de saludo configurado. RSTP es compatible con versiones anteriores de STP.

SERVIDOR RADIUS: el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un mecanismo de autenticación para que los dispositivos se conecten y utilicen un servicio de red. Se utiliza con fines de autenticación, autorización y contabilidad centralizados. Un servidor RADIUS regula el acceso a la red verificando la identidad de los usuarios a través de las credenciales de inicio de sesión ingresadas. Por ejemplo, se instala una red Wi-Fi pública en un campus universitario. Solo aquellos estudiantes que tengan la contraseña pueden acceder a estas redes. El servidor RADIUS verifica las contraseñas ingresadas por los usuarios y otorga o deniega el acceso según corresponda.

TELNET: es un método inseguro para establecer una sesión CLI de manera remota a través de una interface virtual por medio de una red. A diferencia de SSH, Telnet no proporciona una conexión segura y encriptada y solo debe usarse en un entorno de laboratorio. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto simple. La mejor práctica es usar SSH en lugar de Telnet. Cisco IOS incluye un servidor Telnet y un cliente Telnet.

VLAN: (Virtual Local Area Network) es una red conmutada que está segmentada lógicamente por función, área o aplicación, sin tener en cuenta las ubicaciones físicas de los usuarios. Las VLAN son un grupo de hosts o puertos que pueden ubicarse en cualquier lugar de una red, pero se comunican como si estuvieran en el mismo segmento físico. Las VLAN ayudan a simplificar la administración de la red al permitirle mover un dispositivo a una nueva VLAN sin cambiar ninguna conexión física.

RESUMEN

En el presente documento, se llega a la solución de un escenario práctico, el busca la generación y construcción de conocimiento en aras de lograr que el participante cumpla con el contenido programático del Diplomado de Profundización CISCO y se certifique como profesional de redes CISCO (CCNP).

La actividad consta de la construcción de la red y configuración básica de los dispositivos y direccionamiento de las interfases, de la capa 2 de la red, usando protocolos DHCP, SLAAC, RSTP. También se usan de protocolos para el enrutamiento IPv4 e IPv6, mediante OSPF, MP-BGP, interface Loopback 0 y la relación de vecinos en ASN. Aunado a lo anterior, se realiza la configuración de la redundancia de primer salto, empleando el protocolo HSRP. La parte final del ejercicio práctico establece la seguridad y funciones de administración de la misma, donde se usan servidores como RADIUS y NTP.

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

ABSTRACT

In this document, the solution of a practical scenario is reached, it seeks the generation and construction of knowledge in order to ensure that the participant complies with the programmatic content of the CISCO Deepening Diploma and is certified as a CISCO network professional (CCNP).

The activity consists of the construction of the network and basic configuration of the devices and addressing of the interfaces, of layer 2 of the network, using DHCP, SLAAC, RSTP protocols. They are also used as protocols for IPv4 and IPv6 routing, through OSPF, MP-BGP, interface Loopback 0 and the relationship of neighbors in ASN. In addition to the above, the first-hop redundancy configuration is performed, using the HSRP protocol. The final part of the practical exercise establishes the security and administration functions of the same, where servers such as RADIUS and NTP are used.

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics.

INTRODUCCIÓN

Con el fin de interiorizar y afianzar las temáticas propias del Diplomado de Profundización CISCO, en el presente trabajo escrito, se da solución al escenario dispuesto, donde el participante a través de la práctica construye conocimiento y genera para lograr certificarse como profesional de redes CISCO (CCNP).

La práctica realizada consta de un escenario, desagregado en seis partes, las cuales se definen y se establecen así: Construcción de la Red y configuración básica de los dispositivos y direccionamiento de las interfases. Seguidamente, se configura la capa 2 de la red, donde se usan protocolos como DHCP, SLAAC, RSTP, entre otros; esto con el objetivo de lograr comunicación entre los switches y los terminales PC2 y PC3. Una tercera parte consistente en la configuración de protocolos de enrutamiento IPv4 e IPv6, para lo que se usan protocolos OSPF, MP-BGP, configuración de la interface Loopback 0 y la relación de vecinos en ASN.

Aunado a lo anterior, se realiza la configuración de la redundancia de primer salto, para ello se hace necesario el uso del protocolo HSRP, el cual permite que los Routers y/o switches multicapa de la red se vean como si tuvieran una única puerta de enlace (Gateway), comprobando su estado y evitando con esto puntos de fallos únicos garantizando una alta disponibilidad del servicio de red. Las partes finales se establecen para dar seguridad y configurar algunas funciones de administración de la red, donde se usan servidores como RADIUS y NTP.

Para el desarrollo del presente, se acataron las recomendaciones dadas en el uso de software especializado para la simulación de la red y configurarla con los parámetros ya descritos, mediante el uso de GNS3. No obstante, se deben concatenar con una máquina virtual que para el caso se trabaja VMware Workstation y las imágenes IOS para enrutadores 7200 y switches de capa 2 y 3.

Finalmente, con esta actividad práctica se da solución al escenario propuesto, se comprenden cada uno de las tareas, actividades y fases propuestas, así como la resolución de conflictos presentados durante la misma, partiendo desde el mismo momento de instalación de los programas usados y la interacción con ellos y el rendimiento de la maquina física al usar tantos dispositivos virtuales.

DESARROLLO

Figura 1. Escenario Propuesto

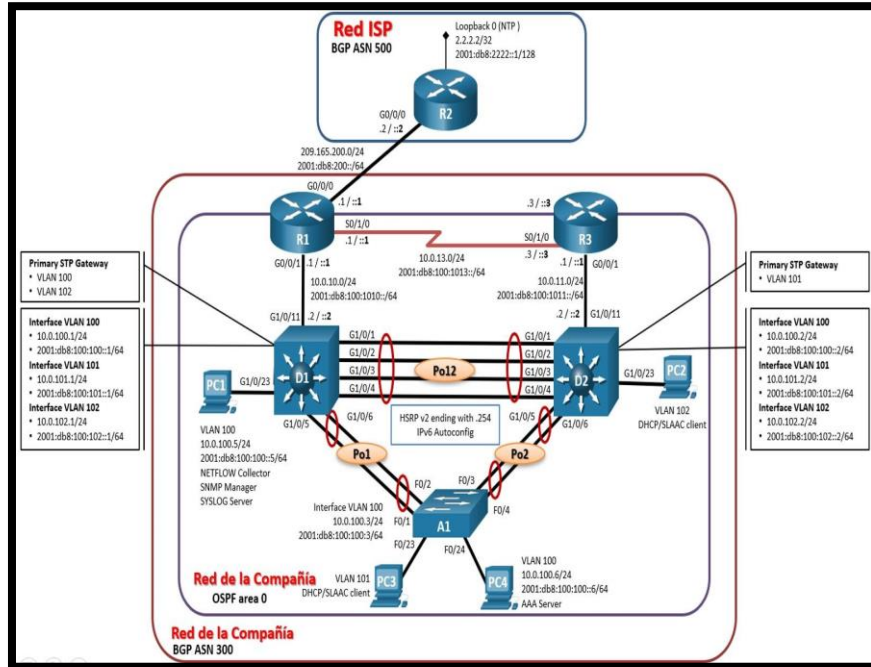


Figura 2. Escenario Simulado (GNS3)

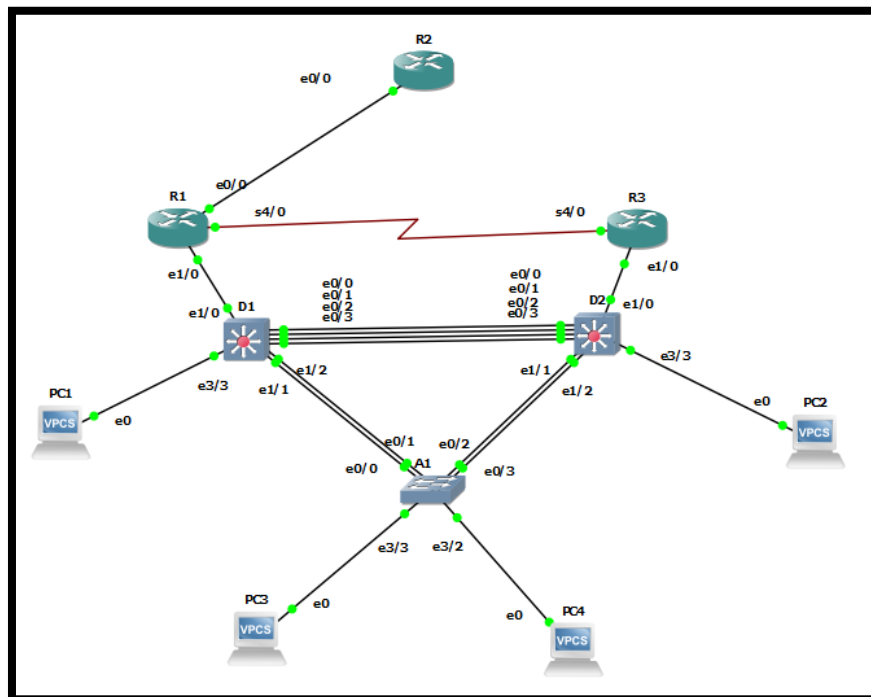


Tabla 1. Direccionamiento de los dispositivos

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

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

En esta primera etapa se construye la red en el software GNS3, se tiene en cuenta el cambio y/o uso de las interfaces toda vez que las IOS usadas en el programa así lo requiere. Posteriormente se realiza la configuración básica de los dispositivos como lo es asignación de nombres, habilitación de servicios como IPv6, entre otras.

Router R1

R1#configure terminal

- Ingreso a modo de configuración.

R1(config)#hostname R1

- Se asigna nombre del host.

R1(config)#ipv6 unicast-routing	• Se habilita el routing IPv6 en el host
R1(config)#no ip domain lookup	• Desactivo la traducción de nombres a dirección del dispositivo.
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	• Se establece mensaje de aviso o de inicio.
R1(config)#line con 0	• Se ingresa al modo de configuración de línea de la consola.
R1(config-line)#exec-timeout 0 0	• Se establece el tiempo de espera inactivo de la sesión remota.
R1(config-line)#logging synchronous	• evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento.
R1(config-line)#exit	• Sale de la configuración de línea
R1(config)#interface ether 0/0	• Selección de interface ethernet
R1(config-if)#ip address 209.165.200.225 255.255.255.224	• Se asigna dirección IP y máscara en IPv4.
R1(config-if)#ipv6 address fe80::1:1 link-local	• Se habilita direccionamiento IPv6.
R1(config-if)#ipv6 address 2001:db8:200::1/64	• Se asigna dirección IP y máscara en IPv6.
R1(config-if)#no shutdown	• Se enciende o activa la interface.
R1(config-if)#exit	• Sale de la configuración de interface
R1(config)#interface ether 1/0	• Selección de interface ethernet
R1(config-if)#ip address 10.0.10.1 255.255.255.0	• Se asigna dirección IP y máscara en IPv4.
R1(config-if)#ipv6 address fe80::1:2 link-local	• Se habilita direccionamiento IPv6.
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64	• Se asigna dirección IP y máscara en IPv6.
R1(config-if)#no shutdown	• Se enciende o activa la interface.

R1(config-if)#exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
R1(config)#interface s4/0	<ul style="list-style-type: none"> • Selección de interface serial
R1(config-if)#ip address 10.0.13.1 255.255.255.0	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv4.
R1(config-if)#ipv6 address fe80::1:3 link-local	<ul style="list-style-type: none"> • Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv6.
R1(config-if)#no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
R1(config-if)#exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
R1(config)#clock timezone UTC -5	<ul style="list-style-type: none"> • Se establece formato de hora UTC
R1(config)#end	<ul style="list-style-type: none"> • Se regresa al modo EXEC privilegiado
R1#copy running-config startup-config	<ul style="list-style-type: none"> • Se guarda la configuración realiza.

Router R2

R2#configure terminal	<ul style="list-style-type: none"> • Ingreso a modo de configuración.
R2(config)#hostname R2	<ul style="list-style-type: none"> • Se asigna nombre del host.
R2(config)#ipv6 unicast-routing	<ul style="list-style-type: none"> • Se habilita el routing IPv6 en el host
R2(config)#no ip domain lookup	<ul style="list-style-type: none"> • Desactivo la traducción de nombres a dirección del dispositivo.
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	<ul style="list-style-type: none"> • Se establece mensaje de aviso o de inicio.
R2(config)#line con 0	<ul style="list-style-type: none"> • Se ingresa al modo de configuración de línea de la consola.
R2(config-line)#exec-timeout 0 0	<ul style="list-style-type: none"> • Se establece el tiempo de espera inactivo de la sesión remota.

R2(config-line)#logging synchronous	<ul style="list-style-type: none"> • evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento.
R2(config-line)#exit	<ul style="list-style-type: none"> • Sale de la configuración de línea
R2(config)#interface ether 0/0	<ul style="list-style-type: none"> • Selección de interface ethernet
R2(config-if)#ip address 209.165.200.226 255.255.255.224	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv4.
R2(config-if)#ipv6 address fe80::2:1 link-local	<ul style="list-style-type: none"> • Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
R2(config-if)#ipv6 address 2001:db8:200::2/64	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv6.
R2(config-if)#no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
R2(config-if)#exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
R2(config)#interface Loopback 0	<ul style="list-style-type: none"> • Se ingresa y/o crea interface.
R2(config-if)#ip address 2.2.2.2 255.255.255.255	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv4.
R2(config-if)#ipv6 address fe80::2:3 link-local	<ul style="list-style-type: none"> • Se habilita direccionamiento IPv6.
R2(config-if)#ipv6 address 2001:db8:2222::1/128	<ul style="list-style-type: none"> • Se asigna dirección IP y máscara en IPv6.
R2(config-if)#no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
R2(config-if)#exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
R2(config)#clock timezone UTC -5	<ul style="list-style-type: none"> • Se establece formato de hora UTC
R2(config)#end	<ul style="list-style-type: none"> • Se regresa al modo EXEC privilegiado
R2#copy running-config startup-config	<ul style="list-style-type: none"> • Se guarda la configuración realiza.

Router R3

```
R3#configure terminal

R3(config)#hostname R3
R3(config)#ipv6 unicast-routing

R3(config)#no ip domain lookup

R3(config)#banner motd # R3, ENCOR
Skills Assessment, Scenario 1 #
R3(config)#line con 0

R3(config-line)#exec-timeout 0 0

R3(config-line)#logging synchronous

R3(config-line)#exit

R3(config)#interface ether 1/0

R3(config-if)#ip address 10.0.11.1
255.255.255.0
R3(config-if)#ipv6 address fe80::3:2
link-local

R3(config-if)#ipv6 address
2001:db8:100:1011::1/64
R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface s4/0
R3(config-if)#ip address 10.0.13.3
255.255.255.0
```

- Ingreso a modo de configuración.
- Se asigna nombre del host.
- Habilito el routing IPv6 en el host
- Desactivo la traducción de nombres a dirección del dispositivo.
- Se establece mensaje de aviso o de inicio.
- Se ingresa al modo de configuración de línea de la consola.
- Se establece el tiempo de espera inactivo de la sesión remota.
- evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento.
- Sale de la configuración de línea
- Selección de interface ethernet
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de interface serial
- Se asigna dirección IP y máscara en IPv4.

R3(config-if)#ipv6 address fe80::3:3 link-local	• Se habilita direccionamiento IPv6.
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64	• Se asigna dirección IP y máscara en IPv6.
R3(config-if)#no shutdown	• Se enciende o activa la interface.
R3(config-if)#exit	• Sale de la configuración de interface
R3(config)#clock timezone UTC -5	• Se establece formato de hora UTC
R3(config)#end	• Se regresa al modo EXEC privilegiado
R3#copy running-config startup-config	• Se guarda la configuración realiza.

Switch D1

Sw_L21#conf ter	• Ingreso a modo de configuración.
Sw_L21(config)#hostname D1	• Se asigna nombre del host.
D1(config)#ip routing	• Se habilita la enrutamiento en el Switch.
D1(config)#ipv6 unicast-routing	• Habilito el routing IPv6 en el host.
D1(config)#no ip domain lookup	• Se desactiva la traducción de nombres a dirección del dispositivo.
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	• Se establece mensaje de aviso o de inicio.
D1(config)#line con 0	• Se ingresa al modo de configuración de línea de la consola.
D1(config-line)#exec-timeout 0 0	• Se establece el tiempo de espera inactivo de la sesión remota.
D1(config-line)#logging synchronous	• evita que los mensajes inesperados que aparecen en pantalla, nos

```

D1(config-line)#exit

D1(config)#vlan 100
D1(config-vlan)#name Management

D1(config-vlan)#exit

D1(config)#vlan 101
D1(config-vlan)#name UserGroupA

D1(config-vlan)#exit

D1(config)#vlan 102
D1(config-vlan)#name UserGroupB

D1(config-vlan)#exit

D1(config)#vlan 999
D1(config-vlan)#name NATIVE

D1(config-vlan)#exit

D1(config)#interface ethe 1/0

D1(config-if)#no switchport

D1(config-if)#ip address 10.0.10.2
255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1
link-local

D1(config-if)#ipv6 address
2001:db8:100:1010::2/64
D1(config-if)#no shutdown

```

desplacen los comandos que estamos escribiendo en el momento.

- Sale de la configuración de línea
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Selección de interface ethernet
- Se cambio el caracter de la interface, el cual aporta a esta capacidad de Capa 3.
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.

D1(config-if)#exit

D1(config)#interface vlan 100

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)#ipv6 address
2001:db8:100:100::1/64

D1(config-if)#no shutdown

D1(config-if)#exit

D1(config)#interface vlan 101

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
2001:db8:100:101::1/64

D1(config-if)#no shutdown

D1(config-if)#exit

D1(config)#interface vlan 102

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

D1(config-if)#exit

- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface

```

D1(config)#ip dhcp excluded-address
10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address
10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address
10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address
10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101

```

```

D1(dhcp-config)#network 10.0.101.0
255.255.255.0
D1(dhcp-config)#default-router
10.0.101.254

```

```

D1(dhcp-config)#exit

```

```

D1(config)#ip dhcp pool VLAN-102

```

```

D1(dhcp-config)#network 10.0.102.0
255.255.255.0
D1(dhcp-config)#default-router
10.0.102.254

```

```

D1(dhcp-config)#exit

```

```

D1(config)#interface range ethe 0/0-3,
ethe 1/1-2, ethe 3/3
D1(config-if-range)#shutdown

```

```

D1(config-if-range)#exit

```

```

D1(config)#clock timezone UTC -5

```

- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se da un nombre al ámbito de direccionamiento y provoca que el router entre en el modo de configuración de DHCP.
- Se le dice el ámbito de la red.
- Se señala la IP para indicarle a los host cual es la puerta de enlace.
- Sale de la configuración de interface
- Se da un nombre al ámbito de direccionamiento y provoca que el router entre en el modo de configuración de DHCP.
- Se le dice el ámbito de la red.
- Se señala la IP para indicarle a los host cual es la puerta de enlace.
- Sale de la configuración de interface.
- Selección rango de interfaces ethernet.
- Se desactivan o apagan las interfaces.
- Sale de la configuración de interfaces.
- Se establece formato de hora UTC.

D1(config)#end

D1#copy running-config startup-config

- Se regresa al modo EXEC privilegiado.
- Se guarda la configuración realiza.

Switch D2

Sw_L22#conf ter

Sw_L22(config)#hostname D2

D2(config)#ip routing

D2(config)#ipv6 unicast-routing

D2(config)#no ip domain lookup

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

D2(config)#line con 0

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

D2(config-line)#logging synchronous

D2(config-line)#exit

D2(config)#vlan 100

D2(config-vlan)#name Management

D2(config-vlan)#exit

D2(config)#vlan 101

D2(config-vlan)#name UserGroupA

D2(config-vlan)#exit

- Ingreso a modo de configuración.
- Se asigna nombre del host.
- Se habilita la enrutamiento en el Switch.
- Habilito el routing IPv6 en el host.
- Se desactiva la traducción de nombres a dirección del dispositivo.
- Se establece mensaje de aviso o de inicio.
- Se ingresa al modo de configuración de línea de la consola.
- Se establece el tiempo de espera inactivo de la sesión remota.
- evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento.
- Sale de la configuración de línea
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan


```
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
```

```
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
```

```
D2(config)#interface ethe 1/0
```

```
D2(config-if)#no switchport
```

```
D2(config-if)#ip address 10.0.11.2
255.255.255.0
```

```
D2(config-if)#ipv6 address fe80::d1:1
link-local
```

```
D2(config-if)#ipv6 address
2001:db8:100:1011::2/64
```

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

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

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

```
D2(config-if)#ip address 10.0.100.2
255.255.255.0
```

```
D2(config-if)#ipv6 address fe80::d2:2
link-local
```

```
D2(config-if)#ipv6 address
2001:db8:100:100::2/64
```

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

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

```
D2(config)#interface vlan 101
```

```
D2(config-if)#ip address 10.0.101.2
255.255.255.0
```

- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Selección de interface ethernet
- Se cambio el caracter de la interface, el cual aporta a esta capacidad de Capa 3.
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.

```
D2(config-if)#ipv6 address fe80::d2:3  
link-local
```

```
D2(config-if)#ipv6 address  
2001:db8:100:101::2/64  
D2(config-if)#no shutdown
```

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

```
D2(config)#interface vlan 102  
D2(config-if)#ip address 10.0.102.2  
255.255.255.0  
D2(config-if)#ipv6 address fe80::d2:4  
link-local
```

```
D2(config-if)#ipv6 address  
2001:db8:100:102::2/64  
D2(config-if)#no shutdown
```

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

```
D2(config)#ip dhcp excluded-address  
10.0.101.1 10.0.101.209  
D2(config)#ip dhcp excluded-address  
10.0.101.241 10.0.101.254  
D2(config)#ip dhcp excluded-address  
10.0.102.1 10.0.102.209  
D2(config)#ip dhcp excluded-address  
10.0.102.241 10.0.102.254  
D2(config)#ip dhcp pool VLAN-101
```

```
D2(dhcp-config)#network 10.0.101.0  
255.255.255.0  
D2(dhcp-config)#default-router  
10.0.101.254
```

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

- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección de Vlan
- Se asigna dirección IP y máscara en IPv4.
- Se utiliza para que sea posible reconocer fácilmente que pertenece al host.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se excluyen rango de direcciones específicas.
- Se da un nombre al ámbito de direccionamiento y provoca que el router entre en el modo de configuración de DHCP.
- Se le dice el ámbito de la red.
- Se señala la IP para indicarle a los host cual es la puerta de enlace.
- Sale de la configuración de interface

D2(config)#ip dhcp pool VLAN-102

D2(dhcp-config)#network 10.0.102.0
255.255.255.0

D2(dhcp-config)#default-router
10.0.102.254

D2(dhcp-config)#exit

D2(config)#interface range ethe 0/0-3,
ethe 1/1-2, ethe 3/3

D2(config-if-range)#shutdown

D2(config-if-range)#exit

D2(config)#clock timezone UTC -5

D2(config)#end

D2#copy running-config startup-config

- Se da un nombre al ámbito de direccionamiento y provoca que el router entre en el modo de configuración de DHCP.
- Se le dice el ámbito de la red.
- Se señala la IP para indicarle a los host cual es la puerta de enlace.
- Sale de la configuración de interface.
- Selección rango de interfaces ethernet.
- Se desactivan o apagan las interfaces.
- Sale de la configuración de interfaces.
- Se establece formato de hora UTC.
- Se regresa al modo EXEC privilegiado.
- Se guarda la configuración realiza.

Switch A1

Sw_L23#conf ter

Sw_L23(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)#exec-timeout 0 0

- Ingreso a modo de configuración.
- Se asigna nombre del host.
- Se desactiva la traducción de nombres a dirección del dispositivo.
- Se establece mensaje de aviso o de inicio.
- Se ingresa al modo de configuración de línea de la consola.
- Se establece el tiempo de espera inactivo de la sesión remota.

A1(config-line)#logging synchronous

A1(config-line)#exit

A1(config)#vlan 100

A1(config-vlan)#name Management

A1(config-vlan)#exit

A1(config)#vlan 101

A1(config-vlan)#name UserGroupA

A1(config-vlan)#exit

A1(config)#vlan 102

A1(config-vlan)#name UserGroupB

A1(config-vlan)#exit

A1(config)#vlan 999

A1(config-vlan)#name NATIVE

A1(config-vlan)#exit

A1(config)#interface vlan 100

A1(config-if)#ip address 10.0.100.3
255.255.255.0

A1(config-if)#ipv6 address fe80::a1:1
link-local

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

A1(config-if)#no shutdown

A1(config-if)#exit

A1(config)#interface range ethe 1/1-3,
ethe 2/0, ethe 3/2-3

A1(config-if-range)#shutdown

A1(config-if-range)#exit

- evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento.
- Sale de la configuración de línea
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se crea Vlan
- Se asigna nombre a la Vlan
- Sale de la configuración de Vlan
- Se ingresa a la interface de Vlan.
- Se asigna dirección IP y máscara en IPv4.
- Se habilita direccionamiento IPv6.
- Se asigna dirección IP y máscara en IPv6.
- Se enciende o activa la interface.
- Sale de la configuración de interface
- Selección rango de interfaces ethernet.
- Se desactivan o apagan las interfaces.
- Sale de la configuración de interfaces.

- A1(config)#clock timezone UTC -5
 - Se establece formato de hora UTC.
- A1(config)#end
 - Se regresa al modo EXEC privilegiado.
- A1#copy running-config startup-config
 - Se guarda la configuración realiza.

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

Figura 3. Comando show.

```

C1> ip 10.0.100.5/24 10.0.100.254
checking for duplicate address...
C1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

C1> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
C1       10.0.100.5/24  10.0.100.254 00:50:79:66:68:00 20044  127.0.0.1:20045
          fe80::250:79ff:fe66:6800/64
          2001:db8:100:1010:2050:79ff:fe66:6800/64 eui-64

C1>
  
```

Configuración manual IP en PC1 y comando show para verificar el direccionamiento obtenido

Figura 4. Comando show.

```

PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4       10.0.100.6/24  10.0.100.254 00:50:79:66:68:03 20050  127.0.0.1:20051
          fe80::250:79ff:fe66:6803/64
          2001:db8:100:1010:2050:79ff:fe66:6803/64 eui-64

PC4>
  
```

Configuración manual IP en PC4 y comando show para verificar el direccionamiento obtenido.

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

Se inicia la configuración de la capa 2 de la red y se establece el soporte básico de host, en esta etapa todos los switches deben comunicarse. PC2 y PC3 reciben direccionamiento de DHCP y SLAAC.

Tabla 2. Tareas de configuración parte 2.

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: D1 and D2 D1 and A1 D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
Tarea#	Tarea	Especificación
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: D1 a D2 – Port channel 12 D1 a A1 – Port channel 1 D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: D1: 10.0.102.1 D2: 10.0.102.2 PC3 debería hacer ping con éxito a: D1: 10.0.101.1 D2: 10.0.101.2 PC4 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC1: 10.0.100.5
-----	---	--

Switch D1

D1#conf ter

D1(config)#interface range ethe 0/0-3

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

D1(config-if-range)# switchport trunk native vlan 999

D1(config-if-range)# channel-group 12 mode active

D1(config-if-range)# no shutdown

D1(config-if-range)# exit

D1(config)#interface range ethe 1/1-2

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

- Ingreso a modo configuración
- Ingreso a un rango de interfaces ethernet
- Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.
- Se establece la VLAN que será nativa o de administración.
- Se crea un port-channel
- Se enciende o activa la interface.
- Sale de la configuración del rango interfaces.
- Ingreso a un rango de interfaces ethernet
- Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.

D1(config-if-range)# switchport trunk native vlan 999	<ul style="list-style-type: none"> • Se establece la VLAN que será nativa o de administración.
D1(config-if-range)# channel-group 1 mode active	<ul style="list-style-type: none"> • Se crea un port-channel
D1(config-if-range)# no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
D1(config-if-range)# exit	<ul style="list-style-type: none"> • Sale de la configuración del rango interfaces.
D1(config)#spanning-tree mode rapid-pvst	<ul style="list-style-type: none"> • Se activa el modo de arbol de expansión rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary	<ul style="list-style-type: none"> • Se establece la prioridad primaria a las Vlan enunciadas.
D1(config)#spanning-tree vlan 101 root secondary	<ul style="list-style-type: none"> • Se establece la prioridad secundaria a las Vlan enunciadas.
D1(config)#interface ethe 3/3	<ul style="list-style-type: none"> • Selección de interface ethernet
D1(config-if)# switchport mode access	<ul style="list-style-type: none"> • Se establece la interface como modo de acceso permanente
D1(config-if)# switchport access vlan 100	<ul style="list-style-type: none"> • Se establece la Vlan que usara la interface
D1(config-if)# spanning-tree portfast	<ul style="list-style-type: none"> • Se establece para obtener acceso inmediato a la red por las terminales de usuarios finales.
D1(config-if)# no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
D1(config-if)# exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
D1(config)#interface Port-channel1	<ul style="list-style-type: none"> • Se ingresa a la interface del Port-channel
D1(config-if)#Switchport Mode trunk	<ul style="list-style-type: none"> • Se establece las interfaces en modo troncal.
D1(config-if)#Switchport acces vlan 102	<ul style="list-style-type: none"> • Se permite el acceso de la Vlan enunciada en la interface.
D1(config-if)#exit	<ul style="list-style-type: none"> • Sale de la configuración de interface

Switch D2

D2#conf ter

D2(config)#interface range ethe 0/0-3

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

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

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

D2(config-if-range)# no shutdown

D2(config-if-range)#exit

D2(config)#interface range ethe 1/1-2

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

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

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

D2(config-if-range)# no shutdown

D2(config-if-range)# exit

D2(config)#spanning-tree mode
rapid-pvst

D2(config)#spanning-tree vlan 101
root primary

D2(config)#spanning-tree vlan
100,102 root secondary

- Ingreso a modo configuración
- Ingreso a un rango de interfaces ethernet
- Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.
- Se establece la VLAN que será nativa o de administración.
- Se crea un port-channel
- Se enciende o activa la interface.
- Sale de la configuración del rango interfaces.
- Ingreso a un rango de interfaces ethernet
- Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.
- Se establece la VLAN que será nativa o de administración.
- Se crea un port-channel
- Se enciende o activa la interface.
- Sale de la configuración del rango interfaces.
- Se activa el modo de arbol de expansión rapid-pvst
- Se establece la prioridad primaria a las Vlan enunciadas.
- Se establece la prioridad secundaria a las Vlan enunciadas.

D2(config)#interface ethe 3/3	• Selección de interface ethernet
D2(config-if)# switchport mode access	• Se establece la interface como modo de acceso permanente
D2(config-if)# switchport access vlan 102	• Se establece la Vlan que usara la interface
D2(config-if)# spanning-tree portfast	• Se establece para obtener acceso inmediato a la red por las terminales de usuarios finales.
D2(config-if)# no shutdown	• Se enciende o activa la interface.
D2(config-if)# exit	• Sale de la configuración de interface
D2(config)#interface Port-channel2	• Se ingresa a la interface del Port-channel
D2(config-if)#Switchport Mode trunk	• Se establece las interfaces en modo troncal.
D2(config-if)#Switchport acces vlan 101	• Se permite el acceso de la Vlan enunciada en la interface.
D2(config-if)#exit	• Sale de la configuración de interface
D2(config)#end	• Se regresa al modo EXEC privilegiado.

Switch A1

A1#conf ter	• Ingreso a modo configuración
A1(config)#spanning-tree mode rapid-pvst	• Se activa el modo de arbol de expansión rapid-pvst
A1(config)#interface range ethe 0/0-1	• Selección de interface ethernet
A1(config-if-range)# switchport trunk encapsulation dot1q	• Ingreso a un rango de interfaces ethernet
A1(config-if-range)# switchport trunk native vlan 999	• Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.

A1(config-if-range)# channel-group 1 mode active	<ul style="list-style-type: none"> • Se establece la VLAN que será nativa o de administración.
A1(config-if-range)# no shutdown A1(config-if-range)# exit	<ul style="list-style-type: none"> • Se crea un port-channel • Se enciende o activa la interface.
A1(config)#interface range ethe 0/2-3	<ul style="list-style-type: none"> • Ingreso a un rango de interfaces ethernet
A1(config-if-range)# switchport trunk encapsulation dot1q	<ul style="list-style-type: none"> • Se establecen las interfaces en modo de enlace permanente o troncal utilizando IEEE 802.1Q.
A1(config-if-range)# switchport trunk native vlan 999	<ul style="list-style-type: none"> • Se establece la VLAN que será nativa o de administración.
A1(config-if-range)# channel-group 2 mode active A1(config-if-range)# no shutdown	<ul style="list-style-type: none"> • Se crea un port-channel • Se enciende o activa la interface.
A1(config-if-range)# exit	<ul style="list-style-type: none"> • Sale de la configuración del rango interfaces.
A1(config)#interface ethe 3/3	<ul style="list-style-type: none"> • Selección de interface ethernet
A1(config-if)# switchport mode access	<ul style="list-style-type: none"> • Se establece la interface como modo de acceso permanente
A1(config-if)# switchport access vlan 101	<ul style="list-style-type: none"> • Se establece la Vlan que usara la interface
A1(config-if)# spanning-tree portfast	<ul style="list-style-type: none"> • Se establece para obtener acceso inmediato a la red por las terminales de usuarios finales.
A1(config-if)# no shutdown	<ul style="list-style-type: none"> • Se enciende o activa la interface.
A1(config-if)# exit	<ul style="list-style-type: none"> • Sale de la configuración de interface
A1(config)#interface ethe 3/2	<ul style="list-style-type: none"> • Selección de interface ethernet
A1(config-if)# switchport mode access	<ul style="list-style-type: none"> • Se establece la interface como modo de acceso permanente
A1(config-if)# switchport access vlan 100	<ul style="list-style-type: none"> • Se establece la Vlan que usara la interface

- | | |
|---|---|
| <p>A1(config-if)# spanning-tree portfast</p> <p>A1(config-if)# no shutdown</p> <p>A1(config-if)# exit</p> <p>A1(config)#interface Port-channel1</p> <p>A1(config-if)#Switchport Mode trunk</p> <p>A1(config-if)#Switchport acces vlan 102</p> <p>A1(config-if)#exit</p> <p>A1(config)#interface Port-channel2</p> <p>A1(config-if)#Switchport Mode trunk</p> <p>A1(config-if)#Switchport acces vlan 101</p> <p>A1(config-if)#exit</p> <p>A1(config)#end</p> | <ul style="list-style-type: none"> • Se establece para obtener acceso inmediato a la red por las terminales de usuarios finales. • Se enciende o activa la interface. • Sale de la configuración de interface • Se ingresa a la interface del Port-channel • Se establece las interfaces en modo troncal. • Se permite el acceso de la Vlan enunciada en la interface. • Sale de la configuración de interface • Se ingresa a la interface del Port-channel • Se establece las interfaces en modo troncal. • Se permite el acceso de la Vlan enunciada en la interface. • Sale de la configuración de interface • Se regresa al modo EXEC privilegiado. |
|---|---|

Evidencia parte 2. Resultados mediante comandos

Figura 5. Verificación servicios DHCP IPv4 e IPv6 en PC2.

```

PC2> dhcp
DORA IP 10.0.102.211/24 GW 10.0.102.254

PC2> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.102.211/24 10.0.102.254 00:50:79:66:68:01 20046 127.0.0.1:20047
fe80::250:79ff:fe66:6801/64
2001:db8:100:1010:2050:79ff:fe66:6801/64 eui-64

PC2>

```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved
12°C Lluvia ligera 8:21 p. m. 16/11/2021

Figura 6. Verificación servicios DHCP IPv4 e IPv6 en PC3.

```
PC3> dhcp
DORA IP 10.0.101.210/24 GW 10.0.101.254

PC3> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.210/24 10.0.101.254 00:50:79:66:68:02 20048 127.0.0.1:20049
fe80::250:79ff:fe66:6802/64
2001:db8:100:1010:2050:79ff:fe66:6802/64 eui-64

PC3>
```

solarwinds Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved 12°C Lluvia ligera 8:22 p. m. 16/11/2021

Figura 7. Ping con éxito desde PC1 a D1, D1 y PC4.

```
PC1> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.100.5/24 10.0.100.254 00:50:79:66:68:00 20044 127.0.0.1:20045
fe80::250:79ff:fe66:6800/64
2001:db8:100:1010:2050:79ff:fe66:6800/64 eui-64

PC1> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=1.060 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.756 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.605 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.434 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.476 ms

PC1> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.630 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.303 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.134 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.952 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.198 ms

PC1> ping 10.0.100.6

84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.316 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.270 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.073 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.119 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.088 ms

PC1>
```

solarwinds Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved 12°C Lluvia ligera 8:22 p. m. 16/11/2021

Figura 8. Ping con éxito desde PC2 A D1 y D2.

```
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.771 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.922 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.959 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.821 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.941 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.273 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.360 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.359 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.435 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.670 ms

PC2> dhcp
DORA IP 10.0.102.211/24 GW 10.0.102.254
```

Figura 9. Ping con éxito desde PC3 A D1 y D2.

```

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.417 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.714 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=1.362 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.773 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.735 ms

PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.992 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.712 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=0.787 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=0.833 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.729 ms

PC3> dhcp
DORA IP 10.0.101.218/24 GW 10.0.101.254

PC3> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.218/24 10.0.101.254 00:50:79:66:68:02 20048 127.0.0.1:20049
fe80::250:79ff:fe66:6802/64
2001:db8:100:1010:2050:79ff:fe66:6802/64 eui-64

PC3>
    
```

Figura 10. Ping con éxito desde PC4 A D1, D2 y PC1.

```

PC4> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.100.6/24 10.0.100.254 00:50:79:66:68:03 20050 127.0.0.1:20051
fe80::250:79ff:fe66:6803/64
2001:db8:100:100:2050:79ff:fe66:6803/64 eui-64

PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.424 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.648 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.719 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.732 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.665 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.031 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.830 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.889 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.702 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.700 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.724 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.769 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.048 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.838 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.727 ms

PC4>
    
```

Figura 11. Comando show interfaces trunk.

```

#Nov 23 22:45:24.675: %SYS-5-CONFIG_I: Configured from console by console
D1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999

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

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

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100-102,999
Po12      1,100-102,999
D1#
    
```

para verificar actividades 2.1, 2.2 y 2.5 sobre Switch D1

Figura 12. Comando show interfaces trunk.

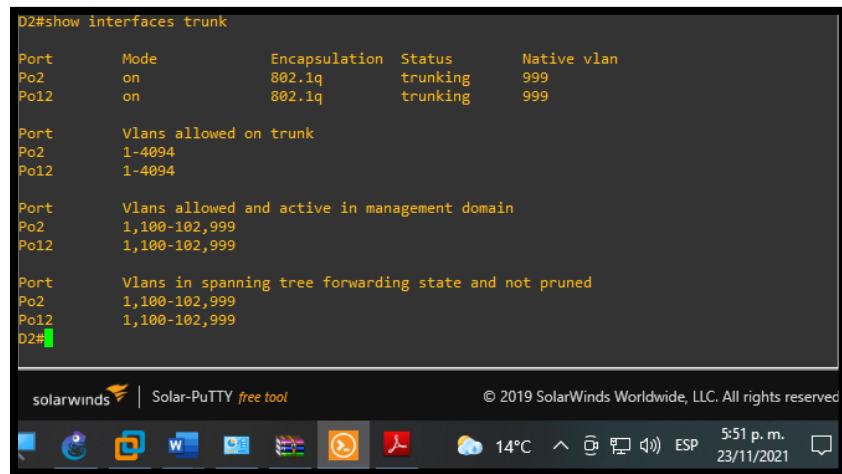
```
D2#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Po2       on        802.1q         trunking      999
Po12      on        802.1q         trunking      999

Port      Vlans allowed on trunk
Po2       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po12      1,100-102,999

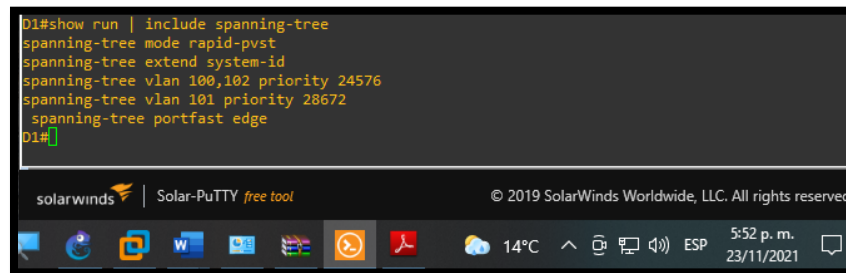
Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,100-102,999
Po12      1,100-102,999
D2#
```



para verificar actividades 2.5 sobre Switch D2.

Figura 13. Comando show run | include spanning-tree.

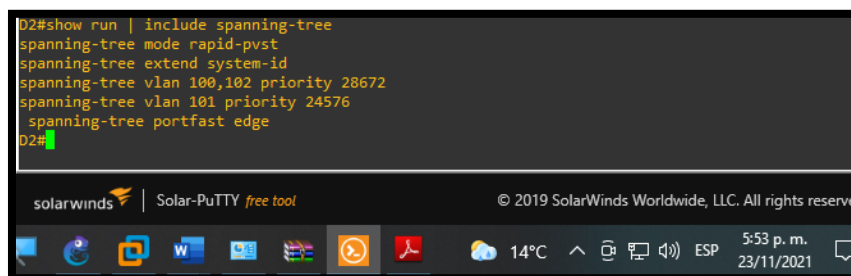
```
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast edge
D1#
```



para verificar actividades 2.3 y 2.4 sobre Switch D1.

Figura 14. Comando show run | include spanning-tree.

```
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#
```

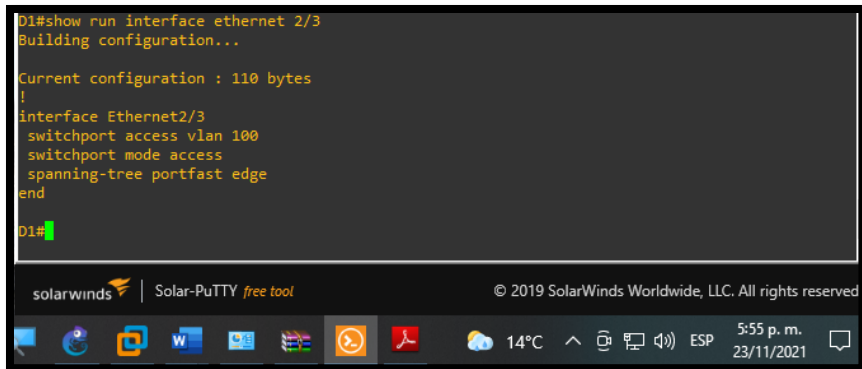


para verificar actividades 2.3 y 2.4 sobre Switch D2.

Figura 15. Comando show run interface.

```
D1#show run interface ethernet 2/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/3
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
D1#
```

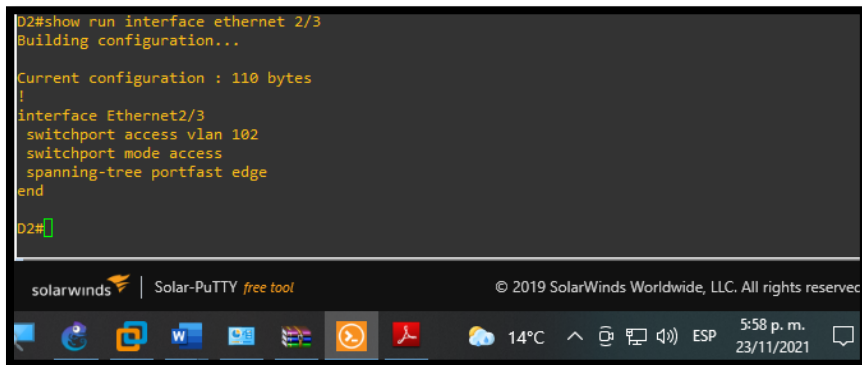


para verificar actividades 2.6 sobre Switch D1.

Figura 16. Comando show run interface.

```
D2#show run interface ethernet 2/3
Building configuration...

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



para verificar actividades 2.6 sobre Switch D2.

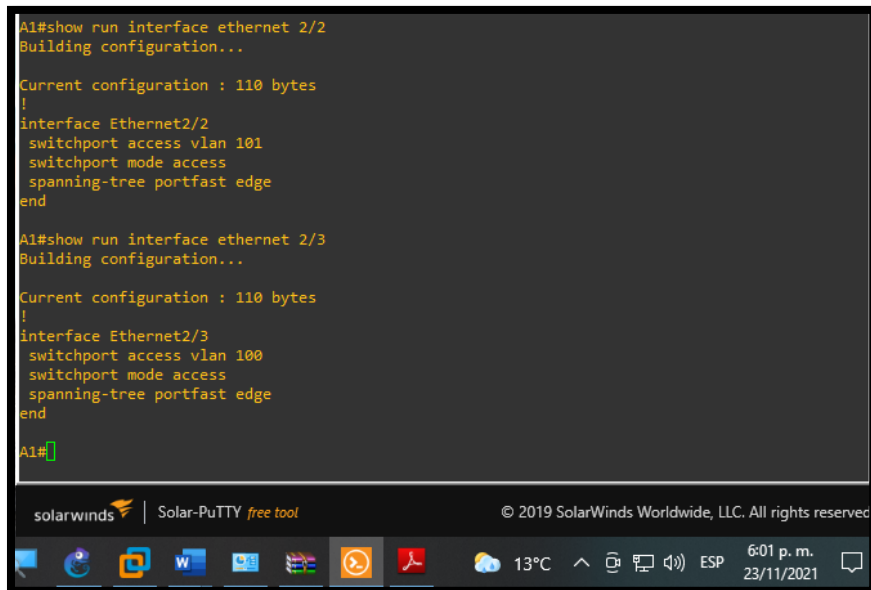
Figura 17. Comando show run interface.

```
A1#show run interface ethernet 2/2
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/2
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end

A1#show run interface ethernet 2/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/3
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
A1#
```



para verificar actividad 2.6 sobre Switch A1.

Parte 3: Configurar los protocolos de enrutamiento.

Se realiza la configuración de los protocolos de enrutamiento IPv4 e IPv6, para ello se usan protocolos OSPF, Vlan's en áreas, entre otros. Con esto la red queda completamente convergente. Para ello, se realizan pruebas de conectividad mediante pings exitosos desde D1 y D2 hasta la interface Loopback 0.

Tabla 3. Tareas de configuración parte 3.

Tarea#	Tarea	Especificación
3.1	En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.	Use OSPF Process ID 4 y asigne los siguientes routerIDs: R1: 0.0.4.1 R3: 0.0.4.3 D1: 0.0.4.131 D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. En R1, no publique la red R1 – R2. En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: D1: todas las interfaces excepto G1/0/11 D2: todas las interfaces excepto G1/0/11
3.2	En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID 6 y asigne los siguientes routerIDs: 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
Tarea#	Tarea	Especificación

3.3	En R2 en la "Red ISP", configure MPBGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interface Loopback 0: Una ruta estática predeterminada IPv4. Una ruta estática predeterminada IPv6.</p> <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie: La red Loopback 0 IPv4 (/32). La ruta por defecto (0.0.0.0/0).</p> <p>En IPv6 address family, anuncie: La red Loopback 0 IPv4 (/128). La ruta por defecto (::/0).</p>
3.4	En R1 en la "Red ISP", configure MPBGP.	<p>Configure dos rutas resumen estáticas a la interface 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.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family: Deshabilite la relación de vecino IPv6. Habilite la relación de vecino IPv4. Anuncie la red 10.0.0.0/8.</p> <p>En IPv6 address family: Deshabilite la relación de vecino IPv4. Habilite la relación de vecino IPv6. Anuncie la red 2001:db8:100::/48.</p>

Router R1

R1#configure terminal

R1(config)#router ospf 4

R1(config-router)# router-id 0.0.4.1

- Ingreso a modo configuración
- Se ingresa y habilita el enrutamiento OSPF 4.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número

```
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 g1/0
```

```
R1(config-if)# ipv6 ospf 6 area 0
```

```
R1(config-if)# exit
```

```
R1(config)#interface s4/0
```

```
R1(config-if)# ipv6 ospf 6 area 0
```

que se utiliza para identificar dicho proceso.

- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se establece y propaga una ruta predeterminada y las actualizaciones OSPF donde el origen de la información es R2.
- Sale de la configuración OSPF 4.
- Se ingresa y habilita el enrutamiento OSPF 6.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se establece y propaga una ruta predeterminada y las actualizaciones OSPF donde el origen de la información es R2.
- Sale de la configuración OSPF 6.
- Selección de interface ethernet.
- Se asigna a esta interface el protocolo y área enunciado.
- Sale de la configuración de interface.
- Selección de interface serial
- Se asigna a esta interface el protocolo y área enunciado.

R1(config-if)# exit

R1(config)#ip route 10.0.0.0 255.0.0.0
null0

R1(config)#ipv6 route
2001:db8:100::/48 null0

R1(config)#router bgp 300

R1(config-router)# bgp router-id 1.1.1.1

R1(config-router)# neighbor
209.165.200.226 remote-as 500

R1(config-router)# neighbor
2001:db8:200::2 remote-as 500

R1(config-router)#address-family ipv4
unicast

R1(config-router-af)# neighbor
209.165.200.226 activate

R1(config-router-af)# no neighbor
2001:db8:200::2 activate

R1(config-router-af)# network 10.0.0.0
mask 255.0.0.0

R1(config-router-af)# exit-address-
family

R1(config-router)# address-family ipv6
unicast

R1(config-router-af)# no neighbor
209.165.200.226 activate

R1(config-router-af)# neighbor
2001:db8:200::2 activate

- Sale de la configuración de interface.
- Se asigna una ruta o dirección estática a IPv4.
- Se asigna una ruta o dirección estática a IPv6.
- Se añade a la tabla de enrutamiento del Router, para lo cual se utiliza el comando estático.
- Se establece el enrutamiento BGP a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se define un vecino BGP con dirección IPv4 específica y como miembro de ASN remoto.
- Se define un vecino BGP con dirección IPv6 específica y como miembro de ASN remoto.
- Se ingresa a la interface para configuración de familia en IPv4.
- Se activa la red de vecino IPv4
- Se desactiva la red de vecino IPv6.
- Se establece la red por la cual se envían mensajes de actualización de rutas.
- Sale de la configuración de familia.
- Se ingresa a la interface para configuración de familia en IPv6.
- Se desactiva la red de vecino IPv4.
- Se activa la red de vecino IPv6.

```
R1(config-router-af)# network
2001:db8:100::/48
```

```
R1(config-router-af)# exit-address-
family
R1(config-router)#end
```

- Se establece la red por la cual se envían mensajes de actualización de rutas.
- Sale de la configuración de familia.
- Se regresa al modo EXEC privilegiado.

Router R2

```
R2#configure terminal
```

```
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
```

- Ingreso a modo configuración
- Configura el router IPV6 con loopback 0.
- Se añade a la tabla de enrutamiento del Router, para lo cual se utiliza el comando estático.
- Se establece el enrutamiento BGP a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se define un vecino BGP con dirección IPv4 específica y como miembro de ASN remoto.
- Se define un vecino BGP con dirección IPv6 específica y como miembro de ASN remoto.
- Se ingresa a la interface para configuración de familia en IPv4.
- Se activa la red de vecino IPv4.
- Se desactiva la red de vecino IPv6.
- Se establece la red por la cual se envían mensajes de actualización de rutas.

R2(config-router-af)# network 0.0.0.0	<ul style="list-style-type: none"> • Se enuncia red estatica IPv4.
R2(config-router-af)# exit-address-family	<ul style="list-style-type: none"> • Sale de la configuración de familia.
R2(config-router)# address-family ipv6	<ul style="list-style-type: none"> • Se ingresa a la interface para configuración de familia en IPv6.
R2(config-router-af)# no neighbor 209.165.200.225 activate	<ul style="list-style-type: none"> • Se desactiva la red de vecino IPv4.
R2(config-router-af)# neighbor 2001:db8:200::1 activate	<ul style="list-style-type: none"> • Se activa la red de vecino IPv6.
R2(config-router-af)# network 2001:db8:2222::/128	<ul style="list-style-type: none"> • Se establece la red por la cual se envian mensajes de actualización de rutas.
R2(config-router-af)# network ::/0	<ul style="list-style-type: none"> • Se enuncia red estatica IPv6.
R2(config-router-af)# exit-address-family	<ul style="list-style-type: none"> • Sale de la configuración de familia.
R2(config-router)#end	<ul style="list-style-type: none"> • Se regresa al modo EXEC privilegiado.

Router R3

R3#configure terminal	<ul style="list-style-type: none"> • Ingreso a modo configuración
R3(config)#router ospf 4	<ul style="list-style-type: none"> • Se ingresa y habilita el enrutamiento OSPF 4.
R3(config-router)# router-id 0.0.4.3	<ul style="list-style-type: none"> • Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
R3(config-router)# network 10.0.11.0 0.0.0.255 area 0	<ul style="list-style-type: none"> • Se establece la red por la cual se envian mensajes de actualización de rutas, con una máscara wildcard y un area de pertenencia.
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0	<ul style="list-style-type: none"> • Se establece la red por la cual se envian mensajes de actualización de rutas, con

R3(config-router)# exit

R3(config)#ipv6 router ospf 6

R3(config-rtr)# router-id 0.0.6.3

R3(config-rtr)# exit

R3(config)#interface g1/0

R3(config-if)# ipv6 ospf 6 area 0

R3(config-if)# exit

R3(config)#interface s4/0

R3(config-if)# ipv6 ospf 6 area 0

R3(config-if)# exit

R3(config)#end

una máscara wildcard y un area de pertenencia.

- Sale de la configuración OSPF 4.
- Se ingresa y habilita el enrutamiento OSPF 6.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Sale de la configuración OSPF 6
- Selección de interface ethernet.
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface
- Selección de interface serial.
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface.
- Se regresa al modo EXEC privilegiado.

Switch D1

D1#configure terminal

D1(config)#router ospf 4

D1(config-router)# router-id 0.0.4.131

D1(config-router)# network 10.0.100.0
0.0.0.255 area 0

- Ingreso a modo configuración.
- Se ingresa y habilita el enrutamiento OSPF 4.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se establece la red por la cual se envían mensajes de

```
D1(config-router)# network 10.0.101.0  
0.0.0.255 area 0
```

```
D1(config-router)# network 10.0.102.0  
0.0.0.255 area 0
```

```
D1(config-router)# network 10.0.10.0  
0.0.0.255 area 0
```

```
D1(config-router)# passive-interface  
default
```

```
D1(config-router)# no passive-interface  
ethe 2/0
```

```
D1(config-router)# exit
```

```
D1(config)#router ospf 6
```

```
D1(config-router)#router-id 0.0.6.131
```

```
D1(config-router)# passive-interface  
default
```

```
D1(config-router)# no passive-interface  
ethe 2/0
```

```
D1(config-router)# exit
```

```
D1(config)#interface ethe 2/0
```

```
D1(config-if)# ipv6 ospf 6 area 0
```

actualización de rutas, con una máscara wildcard y un área de pertenencia.

- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se configura la interfaz como pasiva.
- Se configura la interfaz ether2/0 como no pasiva para OSPF4
- Sale de la configuración OSPF 4.
- Se ingresa y habilita el enrutamiento OSPF 6.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se configura la interfaz como pasiva.
- Se configura la interfaz ether2/0 como no pasiva para OSPF 6.
- Sale de la configuración OSPF 6.
- Selección de interfaz ethernet
- Se asigna a esta interfaz el protocolo y área enunciado.

D1(config-if)# exit

D1(config)#interface vlan 100
D1(config-if)# ipv6 ospf 6 area 0

D1(config-if)# exit

D1(config)#interface vlan 101
D1(config-if)# ipv6 ospf 6 area 0

D1(config-if)# exit

D1(config)#interface vlan 102
D1(config-if)# ipv6 ospf 6 area 0

D1(config-if)# exit

D1(config)#end

- Sale de la configuración de interface
- Selección de interface Vlan
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface
- Selección de interface Vlan
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface
- Selección de interface Vlan
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface
- Se regresa al modo EXEC privilegiado.

Switch D2

D2#configure terminal

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

- Ingreso a modo configuración.
- Se ingresa y habilita el enrutamiento OSPF 4.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un área de pertenencia.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con

```
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  
ethe 2/0
```

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

```
D2(config)#ipv6 router ospf 6
```

```
D2(config-rtr)# router-id 0.0.6.132
```

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

```
D2(config-rtr)# no passive-interface  
ethe 2/0
```

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

```
D2(config)#interface ethe 2/0
```

```
D2(config-if)# ipv6 ospf 6 area 0
```

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

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

```
D2(config-if)# ipv6 ospf 6 area 0
```

una máscara wildcard y un area de pertenencia.

- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un area de pertenencia.
- Se establece la red por la cual se envían mensajes de actualización de rutas, con una máscara wildcard y un area de pertenencia.
- Se configura la interface como pasiva.
- Se configura la interface ether2/0 como no pasiva para OSPF4
- Sale de la configuración OSPF 4.
- Se ingresa y habilita el enrutamiento OSPF 6.
- Se establece el enrutamiento OSPF a través del ID, el cual es un número que se utiliza para identificar dicho proceso.
- Se configura la interface como pasiva.
- Se configura la interface ether2/0 como no pasiva para OSPF 6.
- Sale de la configuración OSPF 6.
- Selección de interface ethernet
- Se asigna a esta interface el protocolo y area enunciado.
- Sale de la configuración de interface
- Selección de interface Vlan
- Se asigna a esta interface el protocolo y area enunciado.

- | | |
|-----------------------------------|---|
| D2(config-if)# exit | • Sale de la configuración de interface |
| D2(config)#interface vlan 101 | • Selección de interface Vlan |
| D2(config-if)# ipv6 ospf 6 area 0 | • Se asigna a esta interface el protocolo y area enunciado. |
| D2(config-if)# exit | • Sale de la configuración de interface |
| D2(config)#interface vlan 102 | • Selección de interface Vlan |
| D2(config-if)# ipv6 ospf 6 area 0 | • Se asigna a esta interface el protocolo y area enunciado. |
| D2(config-if)# exit | • Sale de la configuración de interface |
| D2(config)#end | • Se regresa al modo EXEC privilegiado. |

Evidencia parte 3. Resultados mediante comandos

Figura 18. Comando show run | section ^router ospf.

```

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#
  
```

para verificar la actividad 3.1 sobre dispositivos de red R1.

Figura 19. Comando show run | section ^router ospf.

```

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#
  
```

para verificar la actividad 3.1 sobre dispositivos de red R3.

Figura 20. Comando show run | section ^router ospf.

```
D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet2/0
network 10.0.10.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet2/0
D1#
```

para verificar la actividad 3.1 sobre dispositivos de red D1.

Figura 21. Comando show run | section ^router ospf

```
D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet2/0
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#
```

para verificar la actividad 3.1 sobre dispositivos de red D2.

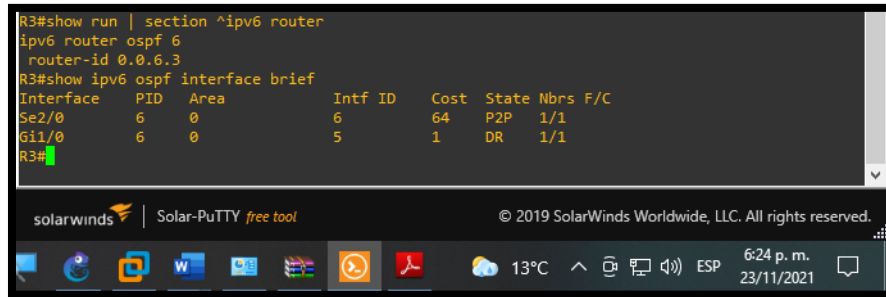
Figura 22. Show run | section ^ipv6 router y show ipv6 ospf interface brief.

```
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
Se2/0      6   0             6        64   P2P    1/1
Gi1/0      6   0             5         1   DR     1/1
R1#
```

Comando para verificar la actividad 3.2 sobre dispositivos de red R1.

Figura 23. Show run | section ^ipv6 router y show ipv6 ospf interface brief.

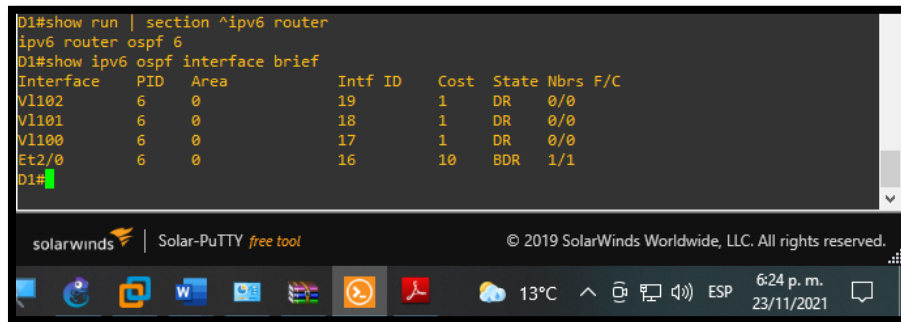
```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Se2/0     6   0         6        64   P2P   1/1
Gi1/0     6   0         5         1    DR    1/1
R3#
```



Comando para verificar la actividad 3.2 sobre dispositivos de red R3.

Figura 24. Show run | section ^ipv6 router y show ipv6 ospf interface brief.

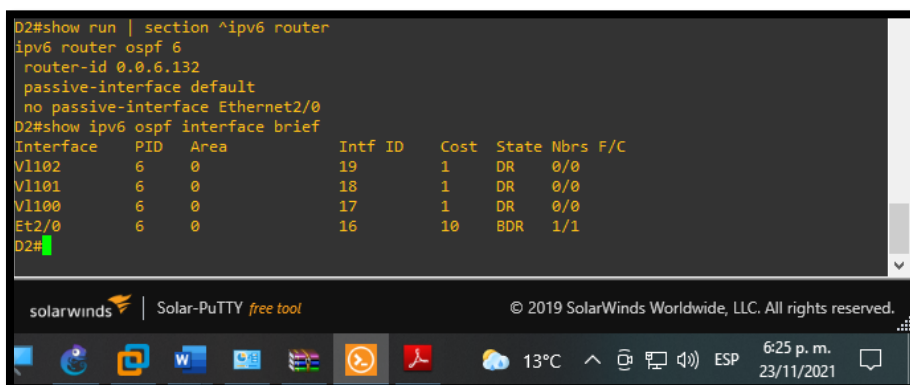
```
D1#show run | section ^ipv6 router
ipv6 router ospf 6
D1#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Vl102     6   0         19         1    DR    0/0
Vl101     6   0         18         1    DR    0/0
Vl100     6   0         17         1    DR    0/0
Et2/0     6   0         16        10   BDR   1/1
D1#
```



Comando para verificar la actividad 3.2 sobre dispositivos de red D1.

Figura 25. Show run | section ^ipv6 router y show ipv6 ospf interface brief.

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet2/0
D2#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Vl102     6   0         19         1    DR    0/0
Vl101     6   0         18         1    DR    0/0
Vl100     6   0         17         1    DR    0/0
Et2/0     6   0         16        10   BDR   1/1
D2#
```



Comando para verificar la actividad 3.2 sobre dispositivos de red D2.

Figura 26. Comando show run | section bgp y show run | include route.

```
R2#show run | section 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#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#
```

para verificar la actividad 3.3 sobre Router R2.

Figura 27. Comando show run | section bgp y show run | include route.

```
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#
```

para verificar la actividad 3.4 sobre Router R1.

Figura 28. Show ip route | include O|B para la verificación de OSPF y BGP.

```
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
B* 0.0.0.0/0 [20/0] via 209.165.200.226, 00:19:14
B  2.2.2.2 [20/0] via 209.165.200.226, 00:19:14
O  10.0.11.0/24 [110/65] via 10.0.13.3, 00:18:56, Serial2/0
O  10.0.100.0/24 [110/2] via 10.0.10.2, 00:18:01, GigabitEthernet1/0
O  10.0.101.0/24 [110/2] via 10.0.10.2, 00:18:01, GigabitEthernet1/0
O  10.0.102.0/24 [110/2] via 10.0.10.2, 00:18:01, GigabitEthernet1/0
R1#
```

Comando para constatar tablas de enrutamiento para IPv4 configurada y funcionando sobre R1.

Figura 29. Show ipv6 route para la verificación de OSPFv3.

```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
B ::0 [20/0]
  via FE80::2:1, GigabitEthernet0/0
S 2001:DB8:100::/48 [1/0]
  via Null0, directly connected
O 2001:DB8:100:100::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
O 2001:DB8:100:101::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
O 2001:DB8:100:102::/64 [110/2]
  via FE80::D1:1, GigabitEthernet1/0
C 2001:DB8:100:1010::/64 [0/0]
  via GigabitEthernet1/0, directly connected
L 2001:DB8:100:1010::1/128 [0/0]
  via GigabitEthernet1/0, receive
O 2001:DB8:100:1011::/64 [110/65]
  via FE80::3:3, Serial2/0
C 2001:DB8:100:1013::/64 [0/0]
  via Serial2/0, directly connected
L 2001:DB8:100:1013::1/128 [0/0]
  via Serial2/0, receive
C 2001:DB8:200::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:200::1/128 [0/0]
  via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
R1#
```

Comando para constatar tablas de enrutamiento IPv6 configurada y funcionando sobre R1.

Figura 30. Comando show ip route ospf | begin Gateway.

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

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 00:25:10, Serial2/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O      10.0.10.0/24 [110/65] via 10.0.13.1, 00:25:10, Serial2/0
O      10.0.100.0/24 [110/2] via 10.0.11.2, 00:23:44, GigabitEthernet1/0
O      10.0.101.0/24 [110/2] via 10.0.11.2, 00:23:44, GigabitEthernet1/0
O      10.0.102.0/24 [110/2] via 10.0.11.2, 00:23:44, GigabitEthernet1/0
R3#
```

para la verificación de OSPF constatando que IPv4 este configurada y funcionando sobre R3.

Figura 31. Comando show ipv6 route ospf.

```

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

para la verificación de OSPFv3 constatando que IPv6 este configurada y funcionando sobre R3.

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

Se realiza la configuración HSRP versión 2 para proveer redundancia de primer salto para los hosts que hacen parte de la red.

Tabla 4. Tareas de configuración parte 4.

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interface R1 G0/0/1.	<p>Cree dos IP SLAs. Use la SLA número 4 para IPv4. Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interface R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. Use el número de rastreo 4 para la IP SLA 4. Use el número de rastreo 6 para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interface R3 G0/0/1.	<p>Cree IP SLAs.</p> <p>Use la SLA número 4 para IPv4.</p> <p>Use la SLA número 6 para IPv6.</p> <p>Las IP SLAs probarán la disponibilidad de la interface R3 G0/0/1 cada 5 segundos.</p> <p>Programa la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <p>Use el número de rastreo 4 para la IP SLA 4.</p> <p>Use el número de rastreo 6 para la SLA 6.</p> <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
-----	---	---

Tarea#	Tarea	Especificación
4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <p>Asigne la dirección IP virtual 10.0.100.254.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 y decremente en 60.</p> <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <p>Asigne la dirección IP virtual 10.0.101.254.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 para disminuir en 60.</p> <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <p>Asigne la dirección IP virtual 10.0.102.254.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 para disminuir en 60.</p> <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 6 y decremente en 60.</p> <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p>

		<p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Habilite la preferencia (preemption).</p> <p>Registre el objeto 6 y decremente en 60.</p> <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 6 y decremente en 60.</p>
Tarea#	Tarea	Especificación
	En D2, configure HSRPv2.	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <p>Asigne la dirección IP virtual 10.0.100.254.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 y decremente en 60.</p> <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <p>Asigne la dirección IP virtual 10.0.101.254.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 para disminuir en 60.</p> <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <p>Asigne la dirección IP virtual 10.0.102.254.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 4 para disminuir en 60.</p> <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 6 para disminuir en 60.</p> <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Establezca la prioridad del grupo en 150.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 6 para disminuir en 60.</p> <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <p>Asigne la dirección IP virtual usando ipv6 autoconfig.</p> <p>Habilite la preferencia (preemption).</p> <p>Rastree el objeto 6 para disminuir en 60.</p>

Switch D1

D1#configure terminal	• Ingreso a modo configuración.
D1(config)#ip sla 4	• para definir el # de la "sesión" del SLA.
D1(config-ip-sla)# icmp-echo 10.0.10.1	• Establece el tipo de mensaje que se va a enviar y a que dirección IP.
D1(config-ip-sla-echo)# frequency 5	• Se indica cada cuanto tiempo se va a enviar el mensaje.
D1(config-ip-sla-echo)# exit	• Sale de la función SLA 4
D1(config)#ip sla 6	• para definir el # de la "sesión" del SLA.
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1	• Establece el tipo de mensaje que se va a enviar y a que dirección IP.
D1(config-ip-sla-echo)# frequency 5	• Se indica cada cuanto tiempo se va a enviar el mensaje.
D1(config-ip-sla-echo)# exit	• Sale de la función SLA 6
D1(config)#ip sla schedule 4 life forever start-time now	• Se habilita el IP SLA, indica cuando y por cuanto tiempo estará activo
D1(config)#ip sla schedule 6 life forever start-time now	• Se habilita el IP SLA, indica cuando y por cuanto tiempo estará activo.
D1(config)#track 4 ip sla 4	• Se crea un tracker, cuya función es saber si el IP SLA está respondiendo correctamente.
D1(config-track)# delay down 10 up 15	• Se establece un tiempo de retraso.
D1(config-track)# exit	• Sale de la función.
D1(config)#track 6 ip sla 6	• Se crea un tracker, cuya función es saber si el IP SLA está respondiendo correctamente.
D1(config-track)# delay down 10 up 15	• Se establece un tiempo de retraso.
D1(config-track)# exit	• Sale de la función.

D1(config)#interface vlan 100

D1(config-if)# standby version 2

D1(config-if)# standby 104 ip
10.0.100.254

D1(config-if)# standby 104 priority 150

D1(config-if)# standby 104 preempt

D1(config-if)# standby 104 track 4
decrement 60

D1(config-if)# standby 106 ipv6
autoconfig

D1(config-if)# standby 106 priority 150

D1(config-if)# standby 106 preempt

- Ingresar a la interface de Vlan
- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura el router activo deseado con una prioridad más alta que la prioridad predeterminada de 100. El rango es de 0 a 255. Si no se configura ninguna prioridad o si la prioridad es igual, tiene prioridad el router con la dirección IP más alta.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Se establece la prioridad que este switch va a tener, la cual ayudará a la elección del router Activo.
- Configura un router para sustituir al router activo.

D1(config-if)# standby 106 track 6
decrement 60

D1(config-if)# exit
D1(config)#interface vlan 101

D1(config-if)# standby version 2

D1(config-if)# standby 114 ip
10.0.101.254

D1(config-if)# standby 114 preempt

D1(config-if)# standby 114 track 4
decrement 60

D1(config-if)# standby 116 ipv6
autoconfig

D1(config-if)# standby 116 preempt

D1(config-if)# standby 116 track 6
decrement 60

D1(config-if)# exit

- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Sale de la función.
- Ingresar a la interface de Vlan
- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Sale de la función.

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

- Ingresar a la interface de Vlan
- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Se establece la prioridad que este switch va a tener, la cual ayudará a la elección del router Activo.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Se establece la prioridad que este switch va a tener, la cual ayudará a la elección del router Activo.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado

```
D1(config-if)# exit
D1(config)#end
```

y un decremento establecido.

- Sale de la función.
- Se regresa al modo EXEC privilegiado.

Switch D2

```
D2#configure terminal
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
```

- Ingreso a modo configuración.
- para definir el # de la "sesión" del SLA.
- Establece el tipo de mensaje que se va a enviar y a que dirección IP.
- Se indica cada cuanto tiempo se va a enviar el mensaje.
- Sale de la función SLA 4
- para definir el # de la "sesión" del SLA.
- Establece el tipo de mensaje que se va a enviar y a que dirección IP.
- Se indica cada cuanto tiempo se va a enviar el mensaje.
- Sale de la función SLA 6
- Se habilita el IP SLA, indica cuando y por cuanto tiempo estará activo
- Se habilita el IP SLA, indica cuando y por cuanto tiempo estará activo.
- Se crea un tracker, cuya función es saber si el IP SLA está respondiendo correctamente.
- Se establece un tiempo de retraso.
- Sale de la función.

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

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

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

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

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

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

```
D2(config-if)# standby 104 preempt
```

```
D2(config-if)# standby 104 track 4  
decrement 60
```

```
D2(config-if)# standby 106 ipv6  
autoconfig
```

```
D2(config-if)# standby 106 preempt
```

```
D2(config-if)# standby 106 track 6  
decrement 60
```

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

```
D2(config)#interface vlan 101
```

- Se crea un tracker, cuya función es saber si el IP SLA está respondiendo correctamente.
- Se establece un tiempo de retraso.
- Sale de la función.
- Ingresar a la interface de Vlan
- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Sale de la función.
- Ingresar a la interface de Vlan

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

- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Se establece la prioridad que este switch va a tener, la cual ayudará a la elección del router Activo.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Se establece la prioridad que este switch va a tener, la cual ayudará a la elección del router Activo.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Sale de la función.

```
D2(config)#interface vlan 102
```

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

```
D2(config-if)# standby 124 ip  
10.0.102.254
```

```
D2(config-if)# standby 124 preempt
```

```
D2(config-if)# standby 124 track 4  
decrement 60
```

```
D2(config-if)# standby 126 ipv6  
autoconfig
```

```
D2(config-if)# standby 126 preempt
```

```
D2(config-if)# standby 126 track 6  
decrement 60
```

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

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

- Ingresar a la interface de Vlan
- Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
- Configura un router para sustituir al router activo.
- Se establece un monitoreo del ID del grupo de HSRP, a través del track programado y un decremento establecido.
- Sale de la función.
- Se regresa al modo EXEC privilegiado.

Evidencia parte 4. Resultados mediante comandos

Figura 32. Comando show run | section ip sla.

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

para verificar la actividad 4.1 y el punto 3 de la actividad 4.3 sobre D1.

Figura 33. Comando show run | section ip sla.

```
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#
```

para verificar la actividad 4.1 y el punto 3 de la actividad 4.3 sobre D2.

Figura 34. Comando show standby brief.

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

Parte 5: Seguridad.

Se realiza la configuración de varios mecanismos de seguridad en los dispositivos de la topología.

Tabla 5. Tareas de configuración parte 5.

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: Nombre de usuario Local: sadmin Nivel de privilegio 15 Contraseña: cisco12345cisco
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: Dirección IP del servidor RADIUS es 10.0.100.6. Puertos UDP del servidor RADIUS son 1812 y 1813. Contraseña: \$strongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: Use la lista de métodos por defecto Valide contra el grupo de servidores RADIUS De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123 .

Se ejecuta en los dispositivos R1, R2, R3, D1, D2 y A1, lo siguiente:

Router R1

```
R1#configure terminal
```

```
R1(config)#enable          algorithm-type  
SCRYPT secret cisco12345cisco
```

```
R1(config)#$admin        privilege    15  
algorithm-type          SCRYPT      secret  
cisco12345cisco
```

```
R1(config)#end
```

```
R1#configure terminal
```

```
R1(config)#aaa new-model
```

```
R1(config)#radius server RADIUS
```

```
R1(config-radius-server)#$v4  
10.0.100.6 auth-port 1812 acct-port  
1813
```

```
R1(config-radius-server)#          key  
$trongPass
```

```
R1(config-radius-server)# exit
```

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

```
R1(config)#end
```

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de funcion hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.

- Ingreso a modo configuración.
- Se habilita un nuevo modelo de autenticación AAA.
- Ingreso a la configuración de radius server como grupo
- Se establece la dirección IP del servidor RADIUS, así como los puertos UDP.
- Se asigna contraseña
- Sale de la configuración Radius server
- Se ingresa los métodos por los cuales se va a autenticar el usuario, ya sea group radius
- Se regresa al modo EXEC privilegiado.

Router R2

```
R2#configure terminal

R2(config)#enable          algorithm-type
SCRYPT secret cisco12345cisco

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

R2(config)#end
```

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de funcion hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.

Router R3

```
R3#configure terminal

R3(config)#enable          algorithm-type
SCRYPT secret cisco12345cisco

R3(config)#$dmin          privilege    15
algorithm-type            SCRYPT      secret
cisco12345cisco

R3(config)#end
```

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de funcion hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.

```

R3#configure terminal

R3(config)#aaa new-model

R3(config)#radius server RADIUS

R3(config-radius-server)#$v4
10.0.100.6 auth-port 1812 acct-port
1813
R3(config-radius-server)# key
$strongPass
R3(config-radius-server)# exit

R3(config)#aaa authentication login
default group radius local

R3(config)#end

```

- Ingreso a modo configuración.
- Se habilita un nuevo modelo de autenticación AAA.
- Ingreso a la configuración de radius server como grupo
- Se establece la dirección IP del servidor RADIUS, así como los puertos UDP.
- Se asigna contraseña
- Sale de la configuración Radius server
- Se ingresa los métodos por los cuales se va a autenticar el usuario, ya sea group radius
- Se regresa al modo EXEC privilegiado.

Switch D1

```

D1#configure terminal

D1(config)#enable algorithm-type
SCRYPT secret cisco12345cisco

D1(config)#$dmin privilege 15
algorithm-type SCRYPT secret
cisco12345cisco

D1(config)#end

```

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de función hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.

```

D1#configure terminal

D1(config)#aaa new-model

D1(config)#radius server RADIUS

D1(config-radius-server)#$v4
10.0.100.6 auth-port 1812 acct-port
1813
D1(config-radius-server)#          key
$strongPass
D1(config-radius-server)# exit

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

D1(config)#end

```

- Ingreso a modo configuración.
- Se habilita un nuevo modelo de autenticación AAA.
- Ingreso a la configuración de radius server como grupo
- Se establece la dirección IP del servidor RADIUS, así como los puertos UDP.
- Se asigna contraseña
- Sale de la configuración Radius server
- Se ingresa los métodos por los cuales se va a autenticar el usuario, ya sea group radius
- Se regresa al modo EXEC privilegiado.

Switch D2

```

D2#configure terminal

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

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

D2(config)#end

D2#configure terminal

```

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de función hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.
- Ingreso a modo configuración.

D2(config)#aaa new-model

D2(config)#radius server RADIUS

D2(config-radius-server)#\$v4
10.0.100.6 auth-port 1812 acct-port
1813

D2(config-radius-server)# key
\$trongPass

D2(config-radius-server)# exit

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

D2(config)#end

Switch A1

A1#configure terminal

A1(config)#enable algorithm-type
SCRYPT secret cisco12345cisco

A1(config)#\$dmin privilege 15
algorithm-type SCRYPT secret
cisco12345cisco

A1(config)#end

A1#configure terminal

- Se habilita un nuevo modelo de autenticación AAA.
- Ingreso a la configuración de radius server como grupo
- Se establece la dirección IP del servidor RADIUS, así como los puertos UDP.
- Se asigna contraseña
- Sale de la configuración Radius server
- Se ingresa los métodos por los cuales se va a autenticar el usuario, ya sea group radius
- Se regresa al modo EXEC privilegiado.

- Ingreso a modo configuración.
- Se habilita configuración de la contraseña, esta será encriptada cuando el enrutador la almacene en Ejecutar / Iniciar archivos usando el cifrado scrypt como el algoritmo hash.
- Se configura usuario admin con nivel de privilegio 15, y contraseña secreta de función hash tipo Scrypt, el cual garantiza mayor nivel de seguridad
- Se regresa al modo EXEC privilegiado.
- Ingreso a modo configuración.

A1(config)#aaa new-model

A1(config)#radius server RADIUS

A1(config-radius-server)#\$v4
10.0.100.6 auth-port 1812 acct-port
1813

A1(config-radius-server)# key
\$trongPass

A1(config-radius-server)# exit

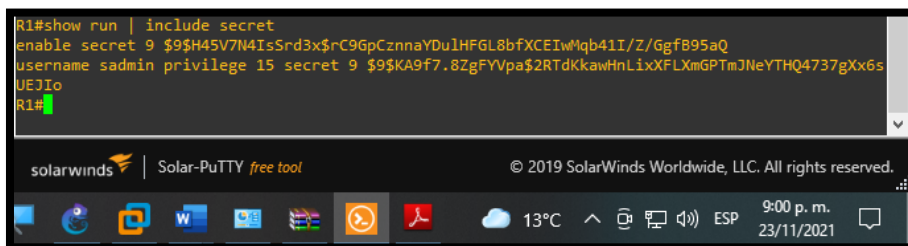
A1(config)#aaa authentication login
default group radius local

A1(config)#end

- Se habilita un nuevo modelo de autenticación AAA.
- Ingreso a la configuración de radius server como grupo
- Se establece la dirección IP del servidor RADIUS, así como los puertos UDP.
- Se asigna contraseña
- Sale de la configuración Radius server
- Se ingresa los métodos por los cuales se va a autenticar el usuario, ya sea group radius
- Se regresa al modo EXEC privilegiado.

Evidencia parte 5. Resultados mediante comandos

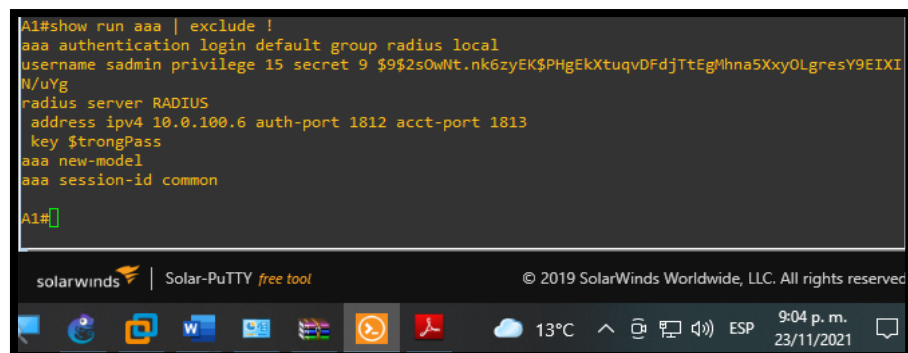
Figura 35. Comando show run | include secret



```
R1#show run | include secret
enable secret 9 $9$H45V7M4IsSrd3x$rC9GpCzannaYDulHFGL8bfXCEIwMqb41I/Z/GgfB95aQ
username sadmin privilege 15 secret 9 $9$KA9f7.8ZgFVvpa$2RTdKkawHnLixFLLXmGPTmJNeYTHQ4737gXx6s
UEJIo
R1#
```

para verificar aleatoriamente la actividad 5.1 y 5.2, constatando que quedaron debidamente configurados la totalidad de los dispositivos de red.

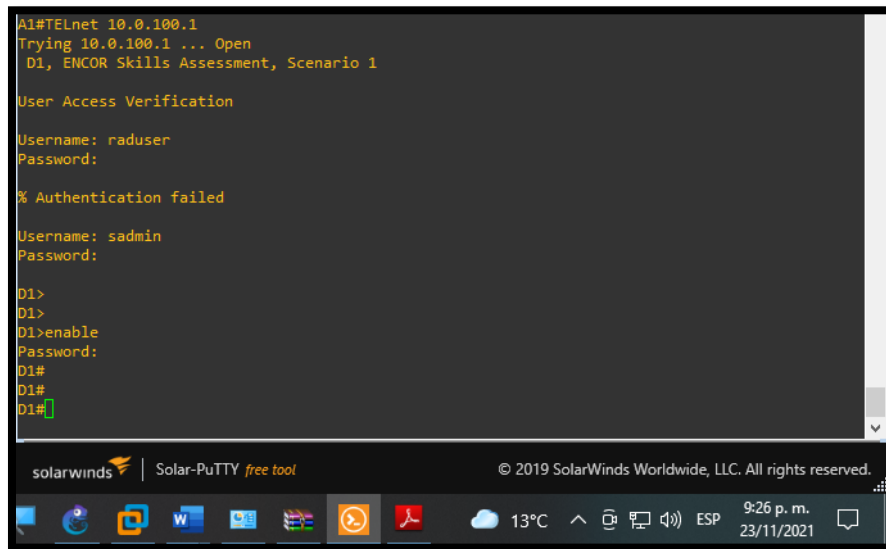
Figura 36. Comando show run aaa | exclude !



```
A1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$2s0wNt.nk6zyEK$PHgEkXtuqvDFdjTtEgMhna5XxyOLgresY9EIXI
N/uYg
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
aaa new-model
aaa session-id common
A1#
```

para verificar aleatoriamente la actividad 5.3, 5.4 y 5.5, constatando que quedaron debidamente configurados la totalidad de los dispositivos de red, exceptuando R2

Figura 37. Conexión a través de TELNET.



desde A1 a D1 mediante la dirección de la VLAN 10.0.100.1, donde solicita usuario y contraseña para ingresar.

Parte 6: Configure las funciones de Administración de Red.

Finalmente, se realizan configuraciones de varias funciones de administración de red.

Tabla 6. Tareas de configuración parte 6.

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

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

Router R1

R1#configure terminal	• Ingreso a modo configuración.
R1(config)#ntp server 2.2.2.2	• Permite que el servidor horario NTP sincronice el reloj del software.
R1(config)# logging trap warning	• Establece nivel 4 de control sobre los mensajes que se envían al servidor de syslog.
R1(config)# logging host 10.0.100.5	• Se establece para registrar mensajes en un host del servidor syslog.

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

Router R2

R2#configure terminal

- Solicita autenticación al iniciar sesión.
 - Se ingresa a la lista SNMP-NMS, con el fin de limitar los host que pueden acceder al Switch a través de dicho protocolo.
 - Se establece la IP que puede conectarse a través de SNMP-NMS
 - Sale de la Interface de configuración SNMP-NMS
 - Se habilita el contacto del sistema.
 - Configura la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura)
 - Especifica el destinatario de las operaciones de trap de SNMP.
 - Permite una mayor precisión cuando recopila y procesa datos de administración de red mediante la identificación única de las interfaces de entrada y salida para los flujos de tráfico y las estadísticas SNMP
 - Se habilita el traps BGP en el agente SNMP.
 - Se habilita el traps CONFIG en el agente SNMP.
 - Se habilita el traps OSPF en el agente SNMP.
 - Se regresa al modo EXEC privilegiado.
-
- Ingreso a modo configuración.

R2(config)#ntp master 3

R2(config)#end

Router R3

R3#configure terminal

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

- Se establece el router como servidor maestro NTP en el estrato indicado, que permite sincronizar los dispositivos que funcionan en una red.
- Se regresa al modo EXEC privilegiado.

- Ingreso a modo configuración.
- Permite que el servidor horario NTP sincronice el reloj del software.
- Establece nivel 4 de control sobre los mensajes que se envían al servidor de syslog.
- Se establece para registrar mensajes en un host del servidor syslog.
- Solicita autenticación al iniciar sesión.
- Se ingresa a la lista SNMP-NMS, con el fin de limitar los host que pueden acceder al Switch a través de dicho protocolo.
- Se establece la IP que puede conectarse a través de SNMP-NMS
- Sale de la Interface de configuración SNMP-NMS
- Se habilita el contacto del sistema.
- Configura la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura)

```
R3(config)# snmp-server host
10.0.100.5 version 2c ENCORSAS
```

```
R3(config)# snmp-server ifindex persist
```

```
R3(config)# snmp-server enable traps
config
```

```
R3(config)# snmp-server enable traps
ospf
```

```
R3(config)#end
```

- Especifica el destinatario de las operaciones de trap de SNMP.
- Se habilita el traps CONFIG en el agente SNMP.
- Se habilita el traps OSPF en el agente SNMP.
- Se regresa al modo EXEC privilegiado.
- Se habilita el traps CONFIG en el agente SNMP.

Switch D1

```
D1#configure terminal
```

```
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
ENCORSAS ro SNMP-NMS
```

- Ingreso a modo configuración.
- Permite que el servidor horario NTP sincronice el reloj del software.
- Establece nivel 4 de control sobre los mensajes que se envían al servidor de syslog.
- Se establece para registrar mensajes en un host del servidor syslog.
- Solicita autenticación al iniciar sesión.
- Se ingresa a la lista SNMP-NMS, con el fin de limitar los host que pueden acceder al Switch a través de dicho protocolo.
- Se establece la IP que puede conectarse a través de SNMP-NMS
- Sale de la Interface de configuración SNMP-NMS
- Se habilita el contacto del sistema.
- Configura la cadena de comunidad y el nivel de

```
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
```

```
D1(config)# snmp-server enable traps  
ospf
```

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

Switch D2

```
D2#configure terminal
```

```
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
```

acceso (solo lectura o lectura y escritura)

- Especifica el destinatario de las operaciones de trap de SNMP.
- Permite una mayor precisión cuando recopila y procesa datos de administración de red mediante la identificación única de las interfaces de entrada y salida para los flujos de tráfico y las estadísticas SNMP
- Se habilita el traps CONFIG en el agente SNMP.
- Se habilita el traps OSPF en el agente SNMP.
- Se regresa al modo EXEC privilegiado.

- Ingreso a modo configuración.
- Permite que el servidor horario NTP sincronice el reloj del software.
- Establece nivel 4 de control sobre los mensajes que se envían al servidor de syslog.
- Se establece para registrar mensajes en un host del servidor syslog.
- Solicita autenticación al iniciar sesión.
- Se ingresa a la lista SNMP-NMS, con el fin de limitar los host que pueden acceder al Switch a través de dicho protocolo.

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 ifindex persist

D2(config)# snmp-server enable traps
config

D2(config)# snmp-server enable traps
ospf

D2(config)#end

- Se establece la IP que puede conectarse a través de SNMP-NMS
- Sale de la Interface de configuración SNMP-NMS
- Se habilita el contacto del sistema.
- Configura la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura)
- Especifica el destinatario de las operaciones de trap de SNMP.
- Permite una mayor precisión cuando recopila y procesa datos de administración de red mediante la identificación única de las interfaces de entrada y salida para los flujos de tráfico y las estadísticas SNMP
- Se habilita el traps CONFIG en el agente SNMP.
- Se habilita el traps OSPF en el agente SNMP.
- Se regresa al modo EXEC privilegiado.

Switch A1

A1#configure terminal

A1(config)#ntp server 10.0.10.1

A1(config)# logging trap warning

- Ingreso a modo configuración.
- Permite que el servidor horario NTP sincronice el reloj del software.
- Establece nivel 4 de control sobre los mensajes que se envían al servidor de syslog.

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

A1(config)#end

- Se establece para registrar mensajes en un host del servidor syslog.
- Solicita autenticación al iniciar sesión.
- Se ingresa a la lista SNMP-NMS, con el fin de limitar los host que pueden acceder al Switch a través de dicho protocolo.
- Se establece la IP que puede conectarse a través de SNMP-NMS
- Sale de la Interface de configuración SNMP-NMS
- Se habilita el contacto del sistema.
- Configura la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura)
- Especifica el destinatario de las operaciones de trap de SNMP.
- Permite una mayor precisión cuando recopila y procesa datos de administración de red mediante la identificación única de las interfaces de entrada y salida para los flujos de tráfico y las estadísticas SNMP
- Se habilita el traps CONFIG en el agente SNMP.
- Se habilita el traps OSPF en el agente SNMP.
- Se regresa al modo EXEC privilegiado.

Evidencia parte 6. Resultados mediante comandos

Figura 38. Verificación de la hora actual en formato UTC.

```
R2#show clock
*21:56:09.286 UTC Tue Nov 23 2021
R2#
```

verificando la actividad 6.1 sobre R2.

Figura 39. Comando show run | include ntp.

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

para verificar la actividad 6.2 sobre R2.

Figura 40. Comando show ntp status | include stratum.

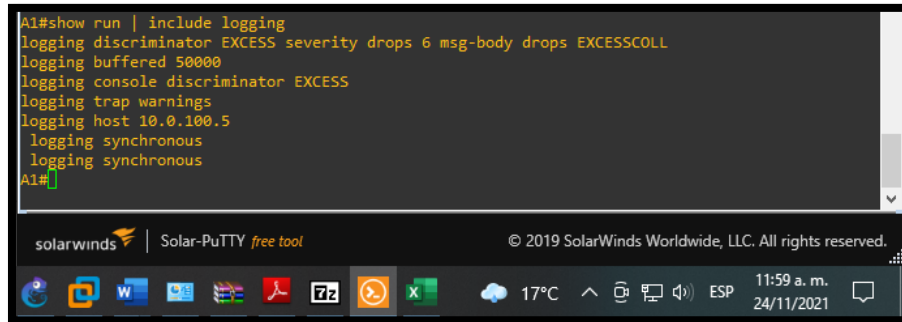
```
R3#show ntp status | include stratum
Clock is synchronized, stratum 13, reference is 2.2.2.2
R3#
```

```
D2#show ntp status | include stratum
Clock is synchronized, stratum 5, reference is 10.0.10.1
D2#
```

para verificar la actividad 6.3 sobre R1 y en todos los demás dispositivos.

Figura 41. Comando show run | include logging.

```
A1#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
A1#
```

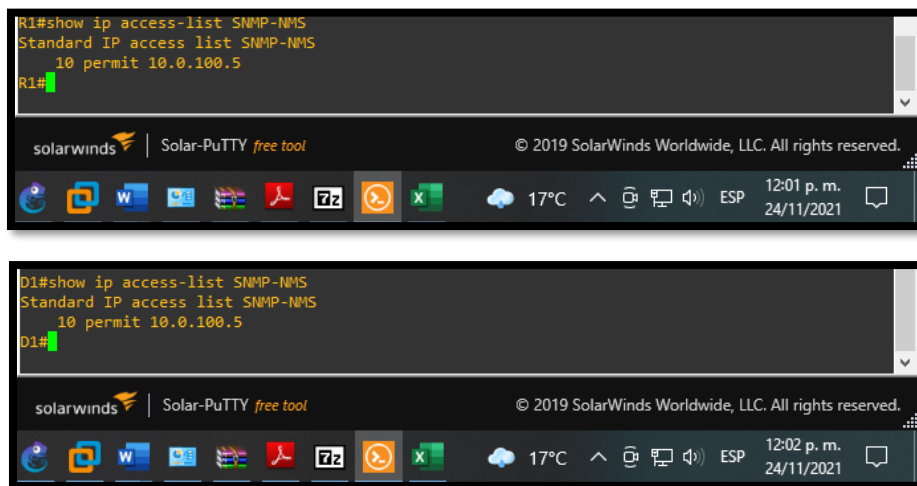


para verificar la actividad 6.4 sobre todos los dispositivos, excluyendo R2.

Figura 42. Comando show ip access-list SNMP-NMS.

```
R1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
R1#
```

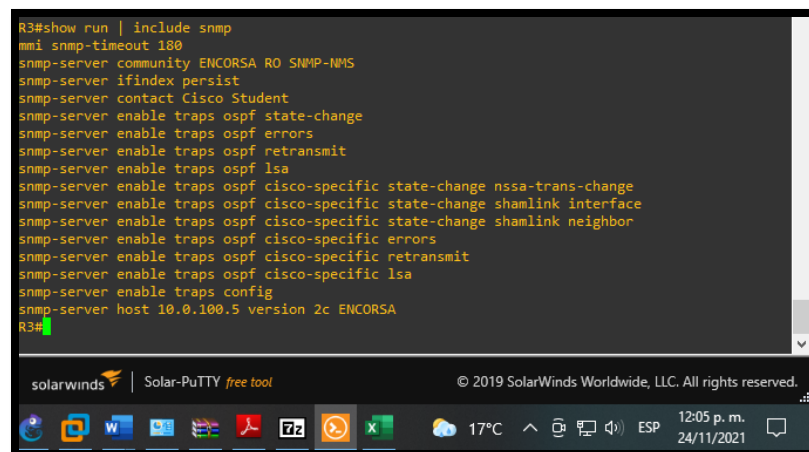
```
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D1#
```



para verificar la actividad 6.5 sobre todos los dispositivos, excluyendo R2.

Figura 43. Comando show run | include snmp.

```
R3#show run | include snmp
nmi snmp-timeout 180
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 config
snmp-server host 10.0.100.5 version 2c ENCORSA
R3#
```



```
A1#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
A1#
```

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

17°C 12:05 p. m. 24/11/2021

para verificar el punto 2 de la actividad 6.5 sobre todos los dispositivos, excluyendo R2.

CONCLUSIONES

Mediante el uso de herramientas tecnológicas las cuales simulan gráficamente los escenarios propuestos y cada uno de los dispositivos usados en el desarrollo del presente curso de profundización, se logró una mayor y mejor comprensión de las temáticas propuestas. No obstante, se presentaron una serie de inconvenientes con las versiones del software, la configuración y uso de las IOS necesarias.

Este aprendizaje por escenarios virtuales, garantizan que el participante logre comprender conceptos vistos durante la capacitación y desarrollo del mismo, logrando un conocimiento eficaz en temas como enrutamiento, aplicación de protocolos, interpretación de tablas de enrutamiento y entendimiento de cómo funcionan las redes a partir de la construcción de sus topologías.

Resulta interesante poder llevar a la practica en dispositivos reales todos los conocimientos vistos, toda vez que en las IOS usadas se encontraron dispositivos que no soportan ciertos protocolos para su configuración. Estar en este punto es saber cómo solucionar y brindar la mejor solución al requerimiento que se tiene por el usuario o dueño de la red.

Se requiere de mucha práctica y práctica y más práctica, hasta llegar a comprender e interiorizar todos los conceptos teóricos estudiados desde CCNA, pasando por CCNP hasta llegar a los demás cursos brindados por CISCO.

Se comprende la idea de la segmentación, configuración y enrutamiento de una red, ya que se hace con este escenario un paso a paso por conceptos básicos, los cuales van aumentando su complejidad para lograr usar protocolos como OSPF, Vlan, BGP, Spanning-tree, entro otros ya referenciados en el glosario del presente documento.

La red configurada, corresponde a algunas topologías usadas por empresas donde buscan que esta sea cien por ciento confiable; lo cual, mediante la adquisición de dispositivos y la asignación de algunos recursos económicos, tienen redes con redundancias de salto, donde se establecen servidores no solo NTP, sino de Dominio, DHCP, servidores de archivos, entre otros. Y corresponde al ingeniero administrador de red garantizar la disponibilidad y conectividad de la empresa 7/24

BIBLIOGRAFIA

Escuela de redes. (2019 febrero 18). First Steps with GNS3 - Network School Tutorial. <https://www.youtube.com/watch?v=O2WXI1kxwnk>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Pag 97 – 108. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Pag 193 – 225. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Pag 308 – 331. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>