

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MILTON CÉSAR SOTO RENDÓN

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MILTON CÉSAR SOTO RENDÓN

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

DIRECTOR:

Msc GERARDO GRANADOS ACUÑA

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

MEDELLÍN

2021

**NOTA DE ACEPTACIÓN**

---

---

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

MEDELLÍN, 20 de noviembre de 2021

## **AGRADECIMIENTOS**

Inicialmente agradezco a la Universidad por brindarme los pilares para fortalecerme como un gran profesional, como es el área de telecomunicaciones, agradezco a mi tutor Héctor Julián Parra quien fue el apoyo principal, para el desarrollo de este Diplomado de Profundización CCNP, y los demás tutores quienes fueron parte del proceso integral de formación. Por otra parte, a mi familia por el apoyo emocional e incondicional; son quienes me fortalecieron y me inculcaron valores personales, estableciendo en mi vida como estudiante y profesional. Igualmente, a mi esposa por ser parte de este proyecto, por el apoyo moral y entusiasta durante todo este tiempo.

## CONTENIDO

<b>AGRADECIMIENTOS</b>	<b>4</b>
<b>CONTENIDO</b>	<b>5</b>
<b>LISTA DE TABLAS</b>	<b>7</b>
<b>LISTA DE FIGURAS</b>	<b>8</b>
<b>GLOSARIO</b>	<b>9</b>
<b>RESUMEN</b>	<b>10</b>
<b>ABSTRACT</b>	<b>11</b>
<b>INTRODUCCIÓN</b>	<b>12</b>
<b>DESARROLLO DEL EJERCICIO PROPUESTO</b>	<b>13</b>
<b>Parte 1: Construya la red y configure los ajustes básicos del dispositivo y el direccionamiento de la interfaz</b>	<b>15</b>
<b>Paso 1: Cablear la red como se muestra en la topología.</b>	<b>15</b>
<b>Paso 2: Configurar los parámetros básicos para cada dispositivo.</b>	<b>15</b>
<b>Router R1: Configuración básica.</b>	<b>16</b>
<b>Router R2: Configuración básica.</b>	<b>18</b>
<b>Router R3: Configuración básica.</b>	<b>19</b>
<b>Switch D1: Configuración básica.</b>	<b>20</b>
<b>Switch A1: Configuración básica.</b>	<b>29</b>
<b>Parte 2: Configurar la capa 2 de la red y el soporte de Host</b>	<b>31</b>
<b>Switch D1: Configuración capa 2.</b>	<b>37</b>
<b>Switch D2: Configuración capa 2.</b>	<b>39</b>
<b>Switch A1: Configuración capa 2.</b>	<b>41</b>
<b>Parte 3: Configurar los protocolos de enrutamiento.</b>	<b>43</b>
<b>Router R1: Configuración OSPFv2, OSPFv3.</b>	<b>46</b>
<b>Router R2: Configuración OSPFv2, OSPFv3.</b>	<b>49</b>
<b>Router R3: Configuración OSPFv2, OSPFv3.</b>	<b>50</b>
<b>Switch D1: Configuración OSPFv2, OSPFv3.</b>	<b>51</b>
<b>Switch D2: Configuración OSPFv2, OSPFv3.</b>	<b>53</b>

<b>Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).</b>	<b>55</b>
Switch D1: Configuración IP SLAs, HSRPv2.	59
Switch D2: Configuración IP SLAs, HSRPv2.	62
<b>Parte 5: Seguridad.</b>	<b>65</b>
Route R1: Configuración SCRYPT, AAA.	66
Route R2: Configuración SCRYPT.	67
Route R3: Configuración SCRYPT, AAA.	67
Switch D1: Configuración SCRYPT, AAA.	68
Switch D2: Configuración SCRYPT, AAA.	69
Switch A1: Configuración SCRYPT, AAA.	70
<b>Parte 6: Configure las funciones de Administración de Red.</b>	<b>73</b>
Actualización: De reloj en todos los dispositivos.	74
Router R2: Configuración NTP Máster 3.	74
Router R1: Configuración NTP y SNMP.	75
Router R3: Configuración NTP y SNMP.	76
Switch D1: Configuración NTP y SNMP.	77
Switch D2: Configuración NTP y SNMP.	78
Switch A1: Configuración NTP y SNMP.	79
<b>CONCLUSIONES</b>	<b>55</b>
<b>BIBLIOGRAFÍA</b>	<b>56</b>
<b>ANEXOS</b>	<b>57</b>
Parte 1: revisar configuración de las interfaces	57
Parte 2: Revisar configuración de capa 2 y compatibilidad de host.	59
Parte 3: Revisar configuración de enrutamiento.	62
Parte 4: Revisar configuración de redundancia de primer salto.	69
Parte 5: Revisa configuración de seguridad.	71
Parte 6: Revisar configuración de función de administración de red.	72

## LISTA DE TABLAS

<b>Tabla 1: Tabla de direccionamiento</b>	<b>14</b>
<b>Tabla 2: Configuración a aplicar en Switches -Parte 2</b>	<b>32</b>
<b>Tabla 3: Configuración a aplicar en red - ISP - Parte 3</b>	<b>43</b>
<b>Tabla 4: Configurar la Redundancia del Primer Salto - Parte 4</b>	<b>56</b>
<b>Tabla 5: Seguridad – Parte 5</b>	<b>65</b>
<b>Tabla 6: Configure las funciones de Administración de Red – Parte 6</b>	<b>73</b>

## LISTA DE FIGURAS

<b>Figura 1: Escenario Propuesto</b>	13
<b>Figura 2: Topología de Red a Cablear</b>	15
<b>Figura 3: PC2 Cliente DHCP</b>	34
<b>Figura 4: PC3 Cliente DHCP</b>	34
<b>Figura 5: Conectividad PC1</b>	35
<b>Figura 6: Conectividad PC2</b>	36
<b>Figura 7: Conectividad PC3</b>	36
<b>Figura 8: Conectividad PC4</b>	37
<b>Figura 9: Solicitud de Autenticación R1.</b>	71
<b>Figura 10: Solicitud de Autenticación R3</b>	71
<b>Figura 11: Solicitud de Autenticación D1.</b>	72
<b>Figura 12: Solicitud de Autenticación D2.</b>	72
<b>Figura 13: Solicitud de Autenticación A1.</b>	73
<b>Figura 14: Sincronización del reloj.</b>	80



## GLOSARIO

**BGP:** (*Border Gateway Protocol*), Protocolo que facilita compartir información relacionada a enrutamiento en una red.

**CCNP:** Cisco Certified Network Professional.

**DHCP:** (*Dynamic Host Configuration Protocol*), facilita la asignación de IP de forma automática.

**LACP:** (*Link Aggregation Control Protocol*), permite la agrupación de puertos físicos y construir uno lógico.

**LOOPBACK:** Interfaz Virtual.

**OSPF:** (*Open Shortest Path First*), protocolo de direccionamiento facilita el recalculación de una ruta.

**RSTP:** (*Rapid Spanning Tree Protocol*), versión actualizada del STP.

**PORTFAST:** Es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto pasa del estado de bloqueo al de reenvío de inmediato.

**SWITCH:** Dispositivo de interconexión, este se encarga de conectar equipos de una misma red.

## RESUMEN

El desarrollo de esta actividad facilita el entendimiento del CCNP, uno de los varios certificados con los que cuenta CISCO. CCNP exige un entendimiento completo de los conceptos bases, en donde el dominio las redes y enrutamientos permite al profesional certificado dominar un mundo de conexiones constantes y cambiantes como es el área de Electrónica, dado que cada comunicación realizada se genera a causa de una necesidad, es decir; se enruta paquetes, datos e información de un origen hacia uno o varios destinos, según sea la necesidad.

Por medio del simulador GNS3 se desarrolla la red empresarial con los dispositivos R1, R3, D1, D2 y A1 configurado MP-BGP ASN 300, para R2 se encuentra en la red ISP configurado MP-BGP ASN 500, se aplica conceptos de redes, configuración de la red en capa 2 y compatibilidad con los hosts, el uso de protocolos de enrutamiento como lo es el OSPF en versiones IPv4 e IPv6, configuración de redundancia del primer salto con el protocolo HSRPv2 y v3, el uso de aplicación de seguridad con el servidor RADIUS y la aplicación de AAA, por último, la configuración de las funciones de administración en las redes LAN y WAN, permitiendo la conectividad de los dispositivos, se evidencia la amplia comprensión arquitectónica y profundización de habilidades requeridas por las redes empresariales como es la conmutación.

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

## **ABSTRACT**

The development of this activity facilitates the understanding of the CCNP, one of the several certificates that CISCO has. CCNP requires a complete understanding of the basic concepts, where the domain of networks and routing allows the certified professional to master a world of constant and changing connections such as the Electronics area, since each communication made is generated because of a need, that is to say; packets, data and information are routed from one source to one or more destinations, depending on the need..

Through the GNS3 simulator, the business network is developed with devices R1, R3, D1, D2 and A1 configured MP-BGP ASN 300, for R2 it is in the ISP network configured MP-BGP ASN 500, network concepts are applied, Layer 2 network configuration and host compatibility, the use of networking protocols such as OSPF in IPv4 and IPv6 versions, first-hop redundancy configuration with the HSRPv2 and v3 protocol, the use of security application with the RADIUS server and the AAA application, finally, the configuration of the management functions in the LAN and WAN networks, allowing the connectivity of the devices, the broad architectural understanding and deepening of skills required by business networks such as switching.

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

## INTRODUCCIÓN

CCNP no está orientada o enfocada en solo un área profesional, sino en todas aquellas que se forma directa o indirecta involucren temas como diseño de arquitectura, infraestructura, carreras profesionales como Sistemas, Electrónica, Telecomunicaciones, Informática, entre otras; tanto la certificación como CISCO tienen un enfoque muy específico en administración de redes principales, enrutamiento avanzado que se ven en todo lo que conocemos como internet.

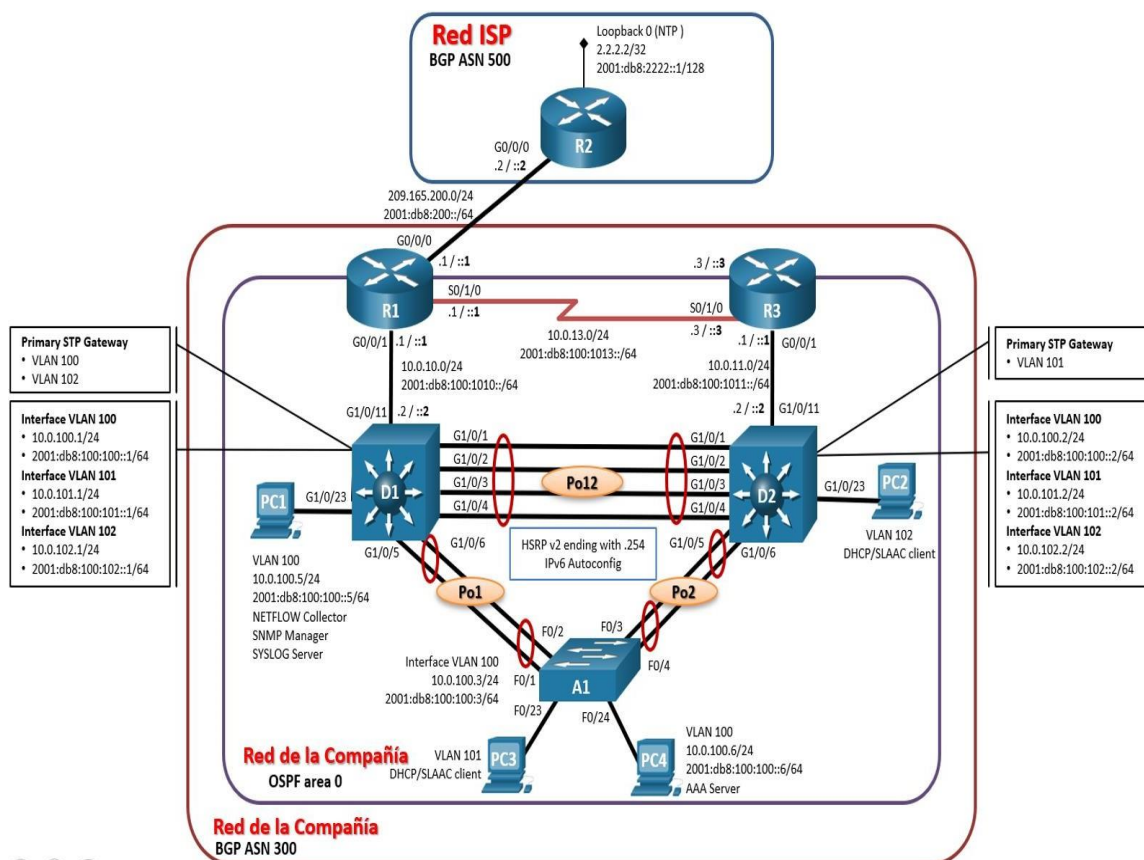
En la ejecución de este trabajo se desarrolla el resultado de las rúbrica de aprendizajes del Diplomado, y son la implementación de comandos IOS usados para la configuración de Routers y Switchs, los comandos son ejecutados en sus modos (Modo usuario, modo privilegio y modo global), los comando IOS permitieron en el desarrollo de la actividad identificar cuando se trabaja sobre un protocolo de enrutamiento, en qué modo y que parámetros se requiere para indicar al dispositivo sus rutas o acción; también se desarrolla la rúbrica del uso de plataforma para desarrollar el ejercicio propuesto.

Para el escenario propuesto del diplomado se realiza por medio de la topología conformada por la red empresarial, el cual está dividida por 6 partes; se construye la red en el simulador GNS3 configurando los dispositivos con comandos básicos asignándole direccionamiento a cada una de las interfaces, en la asignación de capa 2 cada host se obtiene compatibilidad entre ellos, por medio de protocolos de enrutamiento, asignación de redundancia del primer salto, asignación de seguridad a cada equipo, y con la configuración de las funciones de administración de red, se logra tener un red completa y con conectividad.

## DESARROLLO DEL EJERCICIO PROPUESTO

- a. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.
- b. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

**Figura 1: Escenario Propuesto**



**Tabla 1: Tabla de direccionamiento**

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S02/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64

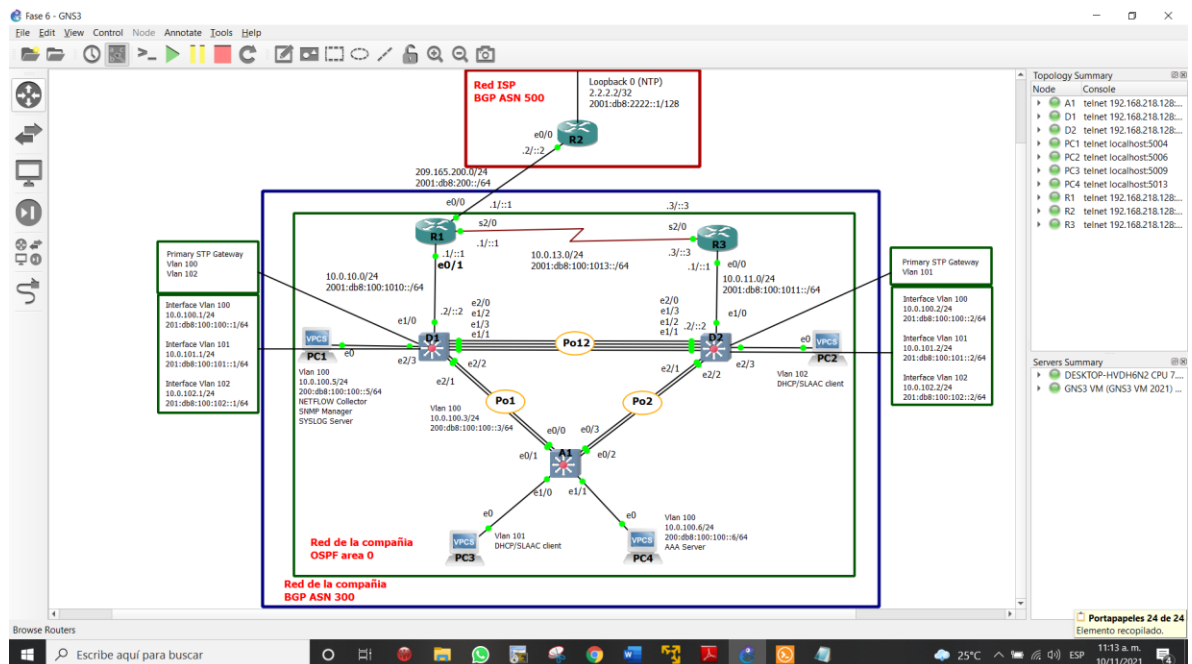
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

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

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

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

**Figura 2: Topología de Red a Cablear**



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

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

**Router R1:** Configuración básica.

R2(config)#**hostname R1** *##Estando en modo configuración terminal con la instrucción hostname se procede a nombrar el equipo en este caso R1.*

R1(config)#**ipv6 unicast-routing** *## Se habilita el protocolo Ipv6 en el router.*

R1(config)#**no ip domain lookup** *## Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje que interrumpa el comando ingresado.*

R1(config)#**line con 0** *## Ingreso al modo de configuración línea de consola 0.*

R1(config-line)#**exec-timeout 0 0** *## Se indica que no habrá límite de tiempo por inactividad.*

R1(config-line)#**logging synchronous** *## Evita que algún mensaje interrumpa la línea o comando ingresado.*

R1(config-line)#**exit** *## Salir del modo consola.*

R1(config)#**interface e0/0** *## En modo configuración global, se ingresa a la Interface Ethernet 0/0.*

R1(config-if)#**ip address 209.165.200.225 255.255.255.224** *## Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la F0/0.*

R1(config-if)#**ipv6 address fe80::1:1 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

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

R1(config-if)#**no shutdown** *## Se sube o enciende la interface.*

R1(config-if)#**exit** *## Salir de la interface que se está configurando.*



R1(config)#**interface e0/1** *## Ingreso a la interface Ethernet 0/1, estando en el modo configuración global.*

R1(config-if)#**ip address 10.0.10.1 255.255.255.0** *## Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la F0/1.*

R1(config-if)#**ipv6 address fe80::1:2 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

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

R1(config-if)#**no shutdown** *## Se sube o enciende la interface.*

R1(config-if)#**exit** *## Salir de la interface que se está configurando.*

Las configuraciones realizadas en las interfaces E0/0 y el E0/1, se van a ingresar también para la Interfaz del S2/0, aplican los mismos comandos

R1(config)#**interface s2/0** *## Ingreso a la interfaz S2/0.*

R1(config-if)#**ip address 10.0.13.1 255.255.255.0** *## Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la S0/1.*

R1(config-if)#**ipv6 address fe80::1:3 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

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

R1(config-if)#**no shutdown** *## Se sube o enciende la interfaz S.*

R1(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

**Router R2:** Configuración básica.

R1(config)#**hostname R2** *## Asignación de nombre al Router como R2.*

R2(config)#**ipv6 unicast-routing** *## Se Habilita el protocolo Ipv6 en el router.*

R2(config)#**no ip domain lookup** *## Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje.*

R2(config)#**banner motd # R2, ENCOR Skills Assessment, Scenario 1 #**

R2(config)#**line con 0** *## Ingreso al modo de configuración línea de consola 0.*

R2(config-line)#**exec-timeout 0 0** *## Se indica que no habrá límite de tiempo por inactividad.*

R2(config-line)#**logging synchronous** *## Evita que algún mensaje interrumpa la línea o comando ingresado.*

R2(config-line)#**exit** *## Salir del modo consola..*

En el Router R2 se aplican las configuraciones aplicadas en las interfaces del R1, para la interfaz E0/0 del R2. (aplica la misma descripción indicada en las líneas anteriores).

R2(config)#**interface e0/0**

R2(config-if)#**ip address 209.165.200.226 255.255.255.224**

R2(config-if)#**ipv6 address fe80::2:1 link-local**

R2(config-if)#**ipv6 address 2001:db8:200::2/64**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

Se crea una interfaz Loopback, se asigna direccionamiento correspondiente, habilitación del IPV6 y de la interfaz.

R2(config)#**interface Loopback 0** *## se ingresa al interfaz Loopback 0.*

R2(config-if)#**ip address 2.2.2.2 255.255.255.255** *## Se asigna la Ip y Mascara que usará la Interface Loopback.*

R2(config-if)#**ipv6 address fe80::2:3 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

R2(config-if)#**ipv6 address 2001:db8:2222::1/128** *## Asignación de la red estática.*

R2(config-if)#**no shutdown** *## Se sube o enciende la interface Loopback*

R2(config-if)#**exit** *## Salir de la interface que se está configurando.*

**Router R3:** Configuración básica.

R3#**confi terminal** *## Ingreso al modo configuración global.*

R3(config)#**hostname R3** *##Asignación de nombre al Router.*

R3(config)#**ipv6 unicast-routing** *## Se Habilita el protocolo Ipv6 en el Router.*

R3(config)#**no ip domain lookup** *## Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje.*

R3(config)#**line con 0** *## Ingreso al modo de configuración línea de consola 0.*

R3(config-line)#**exec-timeout 0 0** *## Se indica que no habrá límite de tiempo por inactividad.*

R3(config-line)#**logging synchronous** *## Evita que algún mensaje interrumpa la*

*línea o comando ingresado.*

R3(config-line)#**exit** *## Salir del modo consola.*

Repetir comandos que se han aplicado en los Router **R1** y **R2** para la Interfaces **E0/0** y la **S2/0**, los cuales comprenden la asignación del direccionamiento a cada interfaz, habilitación del IPV6 y de la interfaz, asignación de la porción de red al prefijo FE80 del IPV6.

R3(config)#**interface e0/0**

R3(config-if)#**ip address 10.0.11.1 255.255.255.0**

R3(config-if)#**ipv6 address fe80::3:2 link-local**

R3(config-if)#**ipv6 address 2001:db8:100:1011::1/64**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

R3(config)#**interface s2/0**

R3(config-if)#**ip address 10.0.13.3 255.255.255.0**

R3(config-if)#**ipv6 address fe80::3:3 link-local**

R3(config-if)#**ipv6 address 2001:db8:100:1010::2/64**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

**Switch D1:** Configuración básica.

D1>**enable** *## Se ingresa a modo privilegiado.*

D1#**configure terminal** *## Se ingresa a modo configuración global.*

D1(config)#**ip routing** *## Habilitar enrutamiento IP en el Switch.*

D1(config)#**ipv6 unicast-routing** *## Se habilita el IPV6 sobre el Switch.*

D1(config)#**no ip domain lookup** *## Permite que el sistema indique que el comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje de error de ingreso del comando.*

D1(config)#**line con 0** *## Ingreso a la línea de consola 0.*

D1(config-line)#**exec-timeout 0 0** *## Configuración de las excepciones de tiempo.*

D1(config-line)#**logging synchronous** *## Evita que algún mensaje interrumpa la línea o comando ingresado.*

D1(config-line)#**exit** *## Salir del modo configuración.*

A continuación, se crean las VLAN 100, 101, 102, y 999 con sus respectivos nombres.

D1(config)#**vlan 100** *## Ingresar a la Vlan a crear.*

D1(config-vlan)#**name Management** *## Se nombra la Vlan Managment.*

D1(config-vlan)#**exit** *## Salir del modo configuración.*

D1(config)#**vlan 101** *## Ingresar a la Vlan a crear.*

D1(config-vlan)#**name UserGroupA** *## Se nombra la Vlan UserGroupA.*

D1(config-vlan)#**exit** *## Salir del modo configuración.*

D1(config)#**vlan 102** *## Ingresar a la Vlan a crear.*

D1(config-vlan)#**name UserGroupB** *## Se nombra la Vlan UserGroupB.*

D1(config-vlan)#**exit** *## Salir del modo configuración.*

D1(config)#**vlan 999** *## Ingresar a la Vlan a crear.*

D1(config-vlan)#**name NATIVE** *## Se nombra la Vlan NATIVE.*

D1(config-vlan)#**exit** *## Salir del modo configuración.*

Aplicación de los comandos ya usados en el **R1**, **R2** y **R3**, en este caso se aplica sobre la Ethernet 1/0

D1(config)#**interface e1/0** *## Ingreso a la Interfaz Ethernet 1/0.*

D1(config-if)#**no switchport** *## aporta a la interfaz capacidad de Capa 3. La dirección IP se encuentra en la misma subred que el Router predeterminado.*

D1(config-if)#**ip address 10.0.10.2 255.255.255.0** *## Asignación de direccionamiento a la Ethernet IPV4.*

D1(config-if)#**ipv6 address fe80::d1:1 link-local***## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D1(config-if)#**ipv6 address 2001:db8:100:1010::2/64** *## Asignación de direccionamiento a la Ethernet IPV6.*

D1(config-if)#**no shutdown** *## Se enciende la interfaz.*

D1(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

Asignación de direccionamiento, segmento de red al prefijo **FE80** para **IPV6**, se

habilita interfaz para cada Vlan creada antes (Vlan 100, 101, 102).

D1(config)#**interface vlan 100** *## Ingresar a la Vlan.*

D1(config-if)#**ip address 10.0.100.1 255.255.255.0** *## Asignación de direccionamiento a la Ethernet IPV4.*

D1(config-if)#**ipv6 address fe80::d1:2 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D1(config-if)#**ipv6 address 2001:db8:100:100::1/64** *## Asignación de direccionamiento a la Ethernet IPV6.*

D1(config-if)#**no shutdown** *## Se enciende la interfaz.*

D1(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

Se configura la interfaz Vlan 101 y 102, la descripción de cada una de las líneas es la misma del paso anterior Vlan 100.

D1(config)#**interface vlan 101**

D1(config-if)#**ip address 10.0.101.1 255.255.255.0** *## Asignación del direccionamiento IP con su respectiva mascara de subred a la Vlan.*

D1(config-if)#**ipv6 address fe80::d1:3 link-local** *## Activación de una porción de red estática al prefijo FE80 protocolo Ipv6.*

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

D1(config-if)#**no shutdown** *## Se enciende la interfaz.*

D1(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

```
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
```

### **Exclusión por DHCP de las siguientes direcciones IP en D1.**

```
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
```

### **Creación de pool de direccionamiento para cada VLAN y Default.**

```
D1(config)#ip dhcp pool VLAN-101  ## Ingreso a la Vlan-101 para asignación de
pool de dirección por DHCP.
D1(dhcp-config)#network 10.0.101.0 255.255.255.0  ## Asignación de IP.
D1(dhcp-config)#default-router 10.0.101.254  ## Gateway default.
D1(dhcp-config)#exit  ## Salir del modo configuración DHCP pool VLAN-101.

D1(config)#ip dhcp pool VLAN-102  ## Ingreso a la Vlan-102 para asignación de
```



*pool de dirección por DHCP.*

D1(dhcp-config)#**network 10.0.102.0 255.255.255.0** *## Asignación de IP al pool de la Vlan.*

D1(dhcp-config)#**default-router 10.0.102.254** *## Gateway default.*

D1(dhcp-config)#**exit** *## Salir del modo configuración DHCP pool VLAN-102.*

### **Se apagan el rango de interfaces Ethernet 0/0-3 y la 3/0-3**

D1(config)#**interface range e0/0-3, e3/0-3** *## Ingreso al rango de interfaces Ethernet o las Ethernet que se apagarán.*

D1(config-if-range)#**shutdown** *## Comando para apagar las interfaces.*

D1(config-if-range)#**exit** *## Salir de las interfaces Ethernet.*

D1(config)#

**Switch D2:** Configuración básica.

El mismo proceso realizado sobre el Switch D1 se aplica en el D2

Switch>**enable** *## Ingreso a modo privilegiado.*

Switch#**configure terminal** *## Ingreso a modo configuración global.*

Switch(config)#**hostname D2** *## darle nombre al Switch.*

D2(config)#**ip routing** *## Habilitar enrutamiento IP en el Switch.*

D2(config)#**ipv6 unicast-routing** *## Se habilita el IPV6 sobre el Switch.*

D2(config)#**no ip domain lookup** *## Permite que el sistema indique que el*

*comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje se error de ingreso del comando.*

*D2(config)#**line con 0** ## Ingreso a la línea de consola 0.*

*D2(config-line)#**exec-timeout 0 0** ## Configuración de las excepciones de tiempo.*

*D2(config-line)#**logging synchronous** ## Evita que algún mensaje interrumpa la línea o comando ingresado.*

*D2(config-line)#**exit** ## Salir del modo configuración line con 0.*

A continuación, se crean las VLAN 100, 101, 102, y 999 con sus respectivos nombres.

*D2(config)#**vlan 100** ## Ingreso de la Vlan a crear 100.*

*D2(config-vlan)#**name Management** ## Se nombra la Vlan Managment.*

*D2(config-vlan)#**exit** ## Salir de la configuración de la Vlan 100.*

*D2(config)#**vlan 101** ## Ingreso de la Vlan a crear 101.*

*D2(config-vlan)#**name UserGroupA** ## Se nombra la Vlan UserGroupA.*

*D2(config-vlan)#**exit** ## Salir de la configuración de la Vlan 101.*

*D2(config)#**vlan 102** ## Ingresar a la Vlan a crear 102.*

*D2(config-vlan)#**name UserGroupB** ## Se nombra la Vlan UserGroupB.*

*D2(config-vlan)#**exit** ## Salir de la configuración de la Vlan 102.*

*D2(config)#**vlan 999** ## Ingresar a la Vlan a crear 999.*

*D2(config-vlan)#**name NATIVE** ## Se nombra la Vlan NATIVE.*

D2(config-vlan)#**exit** *## Salir de la configuración de la Vlan 99.*

Aplicación las líneas de comandos ya usados en el R1, R2 y R3, en este caso se aplica sobre la Ethernet 1/0.

D2(config)#**interface e1/0** *## En modo configuración global, se ingresa a la Interface Ethernet 1/0.*

D2(config-if)#**no switchport** *## aporta a la interfaz capacidad de Capa 3. La dirección IP se encuentra en la misma subred que el Router predeterminado.*

D2(config-if)#**ip address 10.0.11.2 255.255.255.0** *## Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la E1/0.*

D2(config-if)#**ipv6 address fe80::d1:1 link-local***## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D2(config-if)#**ipv6 address 2001:db8:100:1011::2/64** *## Asignación de la red estática.*

D2(config-if)#**no shutdown** *## Se enciende la interfaz.*

D2(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

D2(config-if)#**ip address 10.0.100.2 255.255.255.0** *## Asignación de la red estática IPV4.*

D2(config-if)#**ipv6 address fe80::d2:2 link-local** *## Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D2(config-if)#**ipv6 address 2001:db8:100:100::2/64** *## Asignación de la red estática.*

D2(config-if)#**no shutdown** *## Se enciende la interfaz.*

D2(config-if)#**exit** *## Salir de la interfaz que se está configurando.*

Asignación de direccionamiento, segmento de red al prefijo **FE80** para **IPV6**, se habilita interfaces para cada Vlan creadas antes (**Vlan 101, 102**).

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

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

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

```
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
```

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

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

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

```
D2(config-if)#ip address 10.0.102.2 255.255.255.0
```

```
D2(config-if)#ipv6 address fe80::d2:4 link-local
```

```
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
```

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

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

#### **Exclusión por DHCP de las siguientes direcciones IP en D2**

```
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
```

### Creación de pool de direccionamiento para cada VLAN y Default

```
D2(config)#ip dhcp pool VLAN-101
```

```
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
```

```
D2(dhcp-config)#default-router 10.0.101.254
```

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

```
D2(config)#ip dhcp pool VLAN-102
```

```
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
```

```
D2(dhcp-config)#default-router 10.0.102.254
```

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

```
D2(config)#interface range e0/0-3, e3/0-3
```

```
D2(config-if-range)#shutdown
```

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

**Switch A1:** Configuración básica.

```
Router(config)#hostname A1  ## Se nombra al Swicth como A1.
```

```
A1(config)#no ip domain lookup  ## Permite que el sistema indique que el comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje se error de ingreso del comando.
```

```
A1(config)#line con 0  ## Ingreso al modo de configuración línea de consola 0.
```

```
A1(config-line)#exec-timeout 0 0  ## Se indica que no habrá límite de tiempo por
```

*inactividad.*

A1(config-line)#**logging synchronous** *## Evita que algún mensaje interrumpa la línea o comando ingresado.*

A1(config-line)#**exit** *## Salir del modo consola.*

### **Creación de las VLAN 100, 101, 102, 999 y asignación de nombre**

A1(config)#**vlan 100** *## Ingresar a la Vlan a crear.*

A1(config-vlan)#**name Management** *## Se nombra la Vlan Managment.*

A1(config-vlan)#**exit** *## Salir del modo configuración.*

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**

**Asignación de direccionamiento prefijo FE80 para IPV6, se sube la interfaz Vlan 100.**

```
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 e1/2-3, e2/0-3, e3/0-3
A1(config)#shutdown
A1(config)#exit
```

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

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

**Tabla 2: Configuración a aplicar en Switches -Parte 2**

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> <li>• D1 and D2</li> <li>• D1 and A1</li> <li>• D2 and A1</li> </ul>
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.  D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> <li>• D1 a D2 – Port channel 12</li> <li>• D1 a A1 – Port channel 1</li> <li>• D2 a A1 – Port channel 2</li> </ul>
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.  Los puertos de host deben pasar



		inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC4: 10.0.100.6</li> </ul> <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC1: 10.0.100.5</li> </ul>

Verifique los servicios DHCP IPv4: PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

**Figura 3: PC2 Cliente DHCP**

```
PC2> show ip
NAME       : PC2[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:01
LPORT     : 10006
RHOST:PORT : 127.0.0.1:10007
MTU        : 1500

PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> ip dhcp
DORA IP 10.0.102.110/24 GW 10.0.102.254

PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> █
```

**Figura 4: PC3 Cliente DHCP**

```
PC3> show ip
NAME       : PC3[1]
IP/MASK    : 10.0.101.110/24
GATEWAY    : 10.0.101.254
DNS        :
DHCP SERVER : 10.0.101.1
DHCP LEASE  : 86232, 86400/43200/75600
MAC        : 00:50:79:66:68:02
LPORT     : 10008
RHOST:PORT : 127.0.0.1:10009
MTU        : 1500

PC3> ip dhcp
DORA IP 10.0.101.110/24 GW 10.0.101.254

PC3> █
```

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

**Figura 5: Conectividad PC1**

```
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=24.845 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=12.074 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=6.254 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=7.956 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=8.706 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=26.202 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=17.401 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=18.798 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=20.259 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=23.045 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=21.384 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=13.139 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=16.456 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=27.771 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=18.756 ms

PC1> █
```

16°C Lluvia ligera 10:24 p. m. 27/09/2021

**PC2** debería hacer ping con éxito a:

- D1: 10.0.102.1
- D2: 10.0.102.2

**Figura 6: Conectividad PC2**

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

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

PC2> █
```

16°C Lluvia ligera 10:25 p. m. 27/09/2021

**PC3** debería hacer ping con éxito a:

- D1: 10.0.101.1
- D2: 10.0.101.2

**Figura 7: Conectividad PC3**

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

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

PC3> █
```

16°C Lluvia ligera 10:26 p. m. 27/09/2021

**PC4** debería hacer ping con éxito a:

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC1: 10.0.100.5

Figura 8: Conectividad PC4

```

PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=31.689 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=11.354 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=9.665 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=21.305 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=13.305 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=33.461 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=24.236 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=20.612 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=33.631 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=28.375 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=17.713 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=25.824 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=30.061 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=24.452 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=16.208 ms

PC4>

```

Los siguientes comandos son aplicados a los 3 Switch, configurando las interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches -> D1, D2 y A1. D1 y D2 se configura los puentes raíz RSTP (root bridges) para proporcionar respaldo en caso de falla del puente raíz (root bridge).

**Switch D1:** Configuración capa 2.

D1(config)#**interface range e1/1-3, e2/0##** *Ingresar al rango de interfaces Ethernet.*

D1(config-if-range)#**switchport trunk encapsulation dot1q**## Se genera el enlace troncal sobre el SW con encapsulación dot1q.

D1(config-if-range)#**switchport mode trunk**## Enlace troncal del SW D1 para interfaces Ethernet.

D1(config-if-range)#**switchport trunk native vlan 999**## Como se habilito la encapsulación con protocolo dot1q se debe indicar la Vlan nativa 999.

D1(config-if-range)#**channel-group 12 mode active**##En modo configuración se activa el grupo de canal 12.

D1(config-if-range)#**no shutdown**## Subir interfaz.

D1(config-if-range)#**exit** ## Salir de la interfaz.

D1(config)#

Los comandos anteriores se aplican en las interfaces Ethernet 2/1-2

D1(config)#**interface range e2/1-2**## Ingresar al rango de interfaces Ethernet.

D1(config-if-range)#**switchport trunk encapsulation dot1q**## encapsulación troncal de la interfaz el estándar IEEE 802.1Q.

D1(config-if-range)#**switchport mode trunk**## configuración modo troncal IEEE 802.1Q.

D1(config-if-range)#**switchport trunk native vlan 999**## Vlan nativa.

D1(config-if-range)#**channel-group 1 mode active**## En modo configuración se activa el grupo de canal 1, de D1 a A1.

D1(config-if-range)#**no shutdown**## activar configuración.

D1(config-if-range)#**exit** ## salir del interfaz.

D1(config)#**spanning-tree mode rapid-pvst**## *Configuración más rápida el PVST.*

D1(config)#**spanning-tree vlan 100,102 root primary**## *Asignación de prioridad en el Sw para el puente raíz que se designa como primario.*

D1(config)#**spanning-tree vlan 101 root secondary**## *Asignación de prioridad en el Sw para un segundo puente raíz.*

D1(config)#**interface e2/3**## *Ingresar al rango de interfaz Ethernet2/3.*

D1(config-if)#**switchport mode access** ## *puerto interface g2/3 de acceso.*

D1(config-if)#**switchport access vlan 100**## *Fuerza la creación de una VLAN si es que aún no existe en el switch.*

D1(config-if)#**spanning-tree portfast** ## *Habilitación del PortFast global se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.*

D1(config-if)#**no shutdown** ## *Se sube la Vlan.*

D1(config-if)#**exit** ## *salir del interfaz.*

D1(config)#**end**## *salir de modo configuración.*

## **Switch D2:** Configuración capa 2.

Se aplican los comandos ejecutados en el SW D1 pero ahora sobre el D2 rango e1/1-3, e2/0, e2/1-2, e2/3.

D2(config)#**interface range e1/1-3, e2/0**## *rango de interfaces Ethernet.*

D2(config-if-range)#**switchport trunk encapsulation dot1q**## *encapsulación troncal de la interfaz el estándar IEEE 802.1Q.*

D2(config-if-range)#**switchport mode trunk**## configuración modo troncal IEEE 802.1Q.

D2(config-if-range)#**switchport trunk native vlan 999**## Vlan nativa.

D2(config-if-range)#**channel-group 12 mode active**##En modo configuración se activa el grupo de canal 12, para D1 a D2.

D2(config-if-range)#**no shutdown**## se sube interfaces modo troncal con Vlan nativa.

D2(config-if-range)#**exit** ## salir de las interfaces.

D2(config)#**interface range e2/1-2**## rango de interfaces Ethernet 2/1-2.

D2(config-if-range)#**switchport trunk encapsulation dot1q**## encapsulación troncal de la interfaz el estándar IEEE 802.1Q.

D2(config-if-range)#**switchport mode trunk**## configuración modo troncal IEEE 802.1Q.

D2(config-if-range)#**switchport trunk native vlan 999**## configuración Vlan nativa.

D2(config-if-range)#**channel-group 2 mode active**##En modo configuración se activa el grupo de canal 2, para D1 a A1.

D2(config-if-range)#**no shutdown** ##Se sube la configuración realizada.

D2(config-if-range)#**exit** ## salir del interfaz.

D2(config)#**spanning-tree mode rapid-pvst** ## Configuración más rápida el PVST.

D2(config)#**spanning-tree vlan 101 root primary** ## Asignación de prioridad en el Sw para el puente raíz que se designa como primario.

D2(config)#**spanning-tree vlan 100,102 root secondary**## Asignación de prioridad en el Sw para un segundo puente raíz.

D2(config)#**interface e2/3** ## ingreso a la interfaz Ethernet2/3.



D2(config-if)#**switchport mode access**##puerto interfaz Ethernet2/3 de modo de acceso.

D2(config-if)#**switchport access vlan 102**##Puerto de acceso Vlan102, por lo que otro dispositivo se conecte a este puerto debe tener esta misma Vlan..

D2(config-if)#**spanning-tree portfast**## se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.

D2(config-if)#**no shutdown**## Se sube el puerto en acceso con Vlan 102.

D2(config-if)#**exit** ## salir del interfaz.

D2(config)#**end** ## salir de modo configuración.

### **Switch A1:** Configuración capa 2.

Se aplican los comandos ejecutados en el SW D1 pero ahora sobre el A1 rangeo Ethernet0/0-1, Ethernet0/2-3, Ethernet1/0 Y Ethernet1/1,

A1(config)#**spanning-tree mode rapid-pvst**## Configuración más rápida el PVST.

A1(config)#**interface range e0/0-1**## ingreso al rango de las interfaces Ethernet0/0-1.

A1(config-if-range)#**switchport mode trunk**## configuración modo troncal IEEE 802.1Q.

A1(config-if-range)#**switchport trunk native vlan 999**## configuración Vlan nativa.

A1(config-if-range)#**channel-group 1 mode active**##En modo configuración se activa el grupo de canal 1.

A1(config-if-range)#**no shutdown** ##Se sube la configuración realizada.

A1(config-if-range)#**exit**## salgo de la interfaces Etherne0/0-1.

A1(config)#**interface range e0/2-3**## ingreso al rango de interfaces Ethernet0/2-3.

A1(config-if-range)#**switchport mode trunk**##puertos de interfaces Etherne0/2-3 de modo de troncal.

A1(config-if-range)#**switchport trunk native vlan 999**##Puerto troncal con la Vlan 999.

A1(config-if-range)#**channel-group 2 mode active**##En modo configuración se activa el grupo de canal 2.

A1(config-if-range)#**no shutdown**##Se sube la configuración realizada.

A1(config-if-range)#**exit**## salgo de las interfaces Etherne0/2-3.

A1(config)#**interface e1/0**## ingreso al interfaz Ethernet1/0.

A1(config-if)#**switchport mode access**##puerto de interfaz E1/0 de modo de acceso.

A1(config-if)#**switchport access vlan 101**##Puerto acceso con la Vlan 101.

A1(config-if)#**spanning-tree portfast**## se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.

A1(config-if)#**no shutdown**##Se sube la configuración realizada.

A1(config-if)#**exit**## salgo de la interfaz Etherne1/0.

A1(config)#**interface e1/1**## ingreso al interfaz Ethernet1/1.

A1(config-if)#**switchport mode access**##puerto de interfaz E1/1 de modo de acceso.

A1(config-if)#**switchport access vlan 100**##Puerto acceso con la Vlan 100.

A1(config-if)#**spanning-tree portfast**## se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.

A1(config-if)#**no shutdown**##Se sube la configuración realizada.

A1(config-if)#**exit**## salgo de la interfaz Etherne1/1.

A1(config)#end## salgo del modo configuración.

A1#

### Parte 3: Configurar los protocolos de enrutamiento.

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

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

Las tareas de configuración son las siguientes:

**Tabla 3: Configuración a aplicar en red - ISP - Parte 3**

Tarea#	Tarea	Especificación
--------	-------	----------------

3.1	<p>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-área OSPFv2 en área 0.</p>	<p>Use OSPF Process ID <b>4</b> y asigne los siguientes router- IDs:</p> <p>R1: 0.0.4.1</p> <p>R3: 0.0.4.3</p> <p>D1: 0.0.4.131</p> <p>D2: 0.0.4.132</p> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <p>En R1, no publique la red R1 – R2.</p> <p>En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</p> <p>Deshabilite las publicaciones OSPFv2 en:</p> <p>D1: todas las interfaces excepto G1/0/11</p> <p>D2: todas las interfaces excepto G1/0/11</p>
3.2	<p>En la “Red de la compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.</p>	<p>Use OSPF Process ID <b>6</b> y asigne los siguientes router- IDs:</p> <p>R1: 0.0.6.1</p> <p>R3: 0.0.6.3</p> <p>D1: 0.0.6.131</p> <p>D2: 0.0.6.132</p> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <p>En R1, no publique la red R1 – R2.</p> <p>On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser</p>

		<p>provista por BGP.</p> <p>Deshabilite las publicaciones OSPFv3 en:</p> <p>D1: todas las interfaces excepto G1/0/11</p> <p>D2: todas las interfaces excepto G1/0/11</p>
3.3	<p>En R2 en la "Red ISP", configure MP- BGP</p>	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <p>Una ruta estática predeterminada IPv4.</p> <p>Una ruta estática predeterminada IPv6.</p> <p>Configure R2 en BGP ASN <b>500</b> y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <p>La red Loopback 0 IPv4 (/32).</p> <p>La ruta por defecto (0.0.0.0/0).</p> <p>En IPv6 address family, anuncie:</p> <p>La red Loopback 0 ipv4 (/128).</p> <p>La ruta por defecto (::/0).</p>
3.4	<p>En R1 en la "Red ISP", configure MP- BGP.</p>	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <p>Una ruta resumen IPv4 para 10.0.0.0/8.</p> <ul style="list-style-type: none"> <li>• Una ruta resumen IPv6 para</li> </ul>

		<p>2001:db8:100::/48. Configure R1 en BGP ASN <b>300</b> 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:</p> <p>Deshabilite la relación de vecino IPv6.</p> <p>Habilite la relación de vecino IPv4.</p> <ul style="list-style-type: none"> <li>• Anuncie la red 10.0.0.0/8. En IPv6 address family:</li> </ul> <p>Deshabilite la relación de vecino IPv4.</p> <p>Habilite la relación de vecino IPv6.</p> <p>Anuncie la red 2001:db8:100::/48.</p>
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Router R1:** Configuración OSPFv2, OSPFv3.

Se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.1

R1#**conf terminal** *## configuración global.*

R1(config)#**router ospf 4** *## Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

R1(config-router)#**router-id 0.0.4.1** *## Marcación o identificación del router ID OSPF.*

R1(config-router)#**network 10.0.10.0 0.0.0.255 area 0** *## Asignación de la red que*

*será ruta del área 0.*

R1(config-router)#**network 10.0.13.0 0.0.0.255 area 0** *## Asignación de la red que será ruta del área 0.*

R1(config-router)#**default-information originate** *## Informar una ruta predeterminada en el área.*

R1(config-router)#**exit** *## Salir de la configuración del router-id 0.0.4.1.*

R1(config)#**ipv6 router ospf 6** *## Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

R1(config-rtr)#**router-id 0.0.6.1** *## Marcación o identificación del router ID OSPF.*

R1(config-rtr)#**default-information originate** *## Informar una ruta predeterminada en el área.*

R1(config-rtr)#**exit** *## Salir de la configuración del router-id 0.0.6.1.*

R1(config)#**interface e0/1** *## En modo configuración global se ingresa en la interface Ethernet0/1.*

R1(config-if)#**ipv6 ospf 6 area 0** *## Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R1(config-if)#**exit** *## Salir de la interfaz E0/1.*

R1(config)#**interface s2/0** *## En modo configuración global se ingresa en la interfaz S2/0.*

R1(config-if)#**ipv6 ospf 6 area 0** *## Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R1(config-if)#**exit** *## Salir de la interfaz S2/0.*

R1(config)#**ip route 10.0.0.0 255.0.0.0 null0** *## Se configura la tabla de rutas en la que se indica que la Ip Route 10.0.0.0 con Submask 255.0.0.0 apunta a la interfaz null0 que es una interfaz virtual.*

R1(config)#**ipv6 route 2001:db8:100::/48 null0** ## Configuración ruta estática a la interfaz Null 0 para IPv6.

R1(config)#**router bgp 300** ## se usa BGP ASN 300.

R1(config-router)#**bgp router-id 1.1.1.1** ## Se configura el ID del router en bgp.

R1(config-router)#**neighbor 209.165.200.226 remote-as 500** ## Se habilita una relación de vecino IPv4 con R2 en ASN 500.

R1(config-router)#**neighbor 2001:db8:200::2 remote-as 500**## Se habilita una relación de vecino IPv6 con R2 en ASN 500.

R1(config-router)#**address-family ipv4 unicast** ## Especifica la familia de direcciones, evita intercambio de direcciones IPv4 unicast de forma predeterminada.

R1(config-router-af)#**neighbor 209.165.200.226 activate**## Activación de la dirección de vecino en IPv4.

R1(config-router-af)#**no neighbor 2001:db8:200::2 activate**## Excluye la dirección de vecino de IPv6 en IPv4.

R1(config-router-af)#**network 10.0.0.0 mask 255.0.0.0** ## Anunciado de la red 10.0.0.0/8. En IPv6 address family.

R1(config-router-af)#**exit-address-family**## Se sale de la sub interfaz de direcciones vecino IPv4.

R1(config-router)#**address-family ipv6 unicast**## Se ingresa de la sub interfaz de direcciones vecino IPv6.

R1(config-router-af)#**no neighbor 209.165.200.226 activate**## Excluye la dirección de vecino de IPv4 en IPv6.

R1(config-router-af)#**neighbor 2001:db8:200::2 activate**## Activación de la dirección de vecino en IPv6.

R1(config-router-af)#**network 2001:db8:100::/48**## Dirección de la red Loopback (/48).



R1(config-router-af)#**exit-address-family**## *Se sale de la sub interfaz de direcciones vecino IPv6.*

R1(config-router)#**fin** ## *Salir del modo configuración.*

**Router R2:** Configuración OSPFv2, OSPFv3.

En el R2 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con router-id 2.2.2.2

R2#**conf terminal** ## *Configuración global.*

R2(config)#**ip route 0.0.0.0 0.0.0.0 loopback 0** ## *Configuración rutas estáticas de la interfaz Loopback 0 para IPV4 con ruta por defecto (0.0.0.0/0).*

R2(config)#**ipv6 route ::/0 loopback 0**## *Configuración rutas estáticas de la interfaz Loopback 0 para IPV6 con ruta por defecto (::/0).*

R2(config)#**router bgp 500** ## *Se usa BGP ASN 500.*

R2(config-router)#**bgp router-id 2.2.2.2**## *Se usa BGP ASN 500 router-id 2.2.2.2.*

R2(config-router)#**neighbor 209.165.200.225 remote-as 300**## *Se habilita una relación de vecino IPv4 con R1 en ASN 300.*

R2(config-router)#**neighbor 2001:db8:200::1 remote-as 300**## *Se habilita una relación de vecino IPv6 con R1 en ASN 300.*

R2(config-router)#**address-family ipv4**## *Se habilita una relación de vecino IPv4 con R1 en ASN 300 con dirección de familia.*

R2(config-router-af)#**neighbor 209.165.200.225 activate**## *Activación de la dirección de vecino en IPv4.*

R2(config-router-af)#**no neighbor 2001:db8:200::1 activate**## *Excluye la dirección de vecino de IPv6 en IPv4.*

R2(config-router-af)#**network 2.2.2.2 mask 255.255.255.255** ## Router-id 2.2.2.2.

R2(config-router-af)#**network 0.0.0.0** ## Ruta por defecto (0.0.0.0/0).

R2(config-router-af)#**exit-address-family**## Se sale de la sub interfaz de direcciones vecino IPv4.

R2(config-router)#**address-family ipv6**## Ingreso de la sub interfaz de direcciones vecino IPv6.

R2(config-router-af)#**no neighbor 209.165.200.225 activate**## Excluye la dirección de vecino de IPv4 en IPv6.

R2(config-router-af)#**neighbor 2001:db8:200::1 activate**## Activación de la dirección de vecino en IPv6.

R2(config-router-af)#**network 2001:db8:2222::/128** ## Dirección de la red Loopback (/128).

R2(config-router-af)#**network ::/0** ## Ruta por defecto (::/0).

R2(config-router-af)#**exit-address-family**## Se sale de la sub interfaz de direcciones vecino IPv6.

R2(config-router)#**end** ## Salir de modo configuración.

### **Router R3:** Configuración OSPFv2, OSPFv3.

En el R3 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.3

R3#**confi terminal**## Configuración global.

R3(config)#**router ospf 4**## Habilitación del enrutamiento por medio del OSPF en el proceso 4.

R3(config-router)#**router-id 0.0.4.3**## *Marcación o identificación del Router ID OSPF.*

R3(config-router)#**network 10.0.11.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

R3(config-router)#**network 10.0.13.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

R3(config-router)#**exit**## *Salir de la configuración Router-id 0.0.4.3.*

R3(config)#**ipv6 router ospf 6**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

R3(config-rtr)#**router-id 0.0.6.3**## *Marcación o identificación del Router ID OSPF*

R3(config-rtr)#**exit**## *Salir de la configuración Router-id 0.0.6.3*

R3(config)#**interface e0/0**## *En modo configuración global se ingresa en la interfaz Ethernet0/0.*

R3(config-if)#**ipv6 ospf 6 area 0**## *Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R3(config-if)#**exit**## *Salir de la interfaz Ethernet0/0.*

R3(config)#**interface s2/0**## *En modo configuración global se ingresa en la interfaz S2/0.*

R3(config-if)#**ipv6 ospf 6 area 0**## *Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R3(config-if)#**exit**## *Salir de la interfaz S2/0.*

R3(config)#**end**## *Salir de la configuración.*

**Switch D1:** Configuración OSPFv2, OSPFv3.

En el D1 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.131.

D1#**conf terminal** *## Configuración global.*

D1(config)#**router ospf 4***## Habilidadación del enrutamiento por medio del OSPF en el proceso 4.*

D1(config-router)#**router-id 0.0.4.131***## Habilidadación del enrutamiento por medio del OSPF en el proceso 4.*

D1(config-router)#**network 10.0.100.0 0.0.0.255 area 0***## Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.101.0 0.0.0.255 area 0***## Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.102.0 0.0.0.255 area 0***## Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.10.0 0.0.0.255 area 0***## Asignación de la red que será ruta del área 0.*

D1(config-router)#**passive-interface default** *## Deshabilito las publicaciones OSPFv2, todas las interfaces.*

D1(config-router)#**no passive-interface e1/0***## No deshabilito las publicaciones de la interfaz Etherne1/0.*

D1(config-router)#**exit** *## Salgo de la configuración Router OSPF 4.*

D1(config)#**ipv6 router ospf 6** *## Habilidadación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-rtr)#**router-id 0.0.6.131** *## Habilidadación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-rtr)#**passive-interface default** ## *Deshabilito las publicaciones OSPFv3, todas las interfaces.*

D1(config-rtr)#**no passive-interface e1/0** ## *No deshabilito las publicaciones de la interfaz Ethernet 1/0.*

D1(config-rtr)#**exit** ## *Salgo de la configuración de router OSPF 6.*

D1(config)#**interface e1/0** ## *Ingreso al interfaz Ethernet 1/0.*

D1(config-if)#**ipv6 ospf 6 area 0** ## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit** ## *Salgo de la configuración de router.*

D1(config)#**interface vlan 100** ## *Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0** ## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit**## *Salir de la configuración vlan 100.*

D1(config)#**interface vlan 101** ## *Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit**## *Salir de la configuración vlan 101.*

D1(config)#**interface vlan 102**## *Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit**## *Salir de la configuración vlan 102.*

D1(config)#**end**## *Salir del modo configuración.*

D1#

**Switch D2:** Configuración OSPFv2, OSPFv3.

En el D2 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.132.

D2#**conf terminal** ## Configuración global.

D2(config)#**router ospf 4**## *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D2(config-router)#**router-id 0.0.4.132**## *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D2(config-router)#**network 10.0.100.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.101.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.102.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.11.0 0.0.0.255 area 0**## *Asignación de la red que será ruta del área 0.*

D2(config-router)#**passive-interface default**## *Deshabilito las publicaciones OSPFv2, todas las interfaces.*

D2(config-router)#**no passive-interface e1/0**## *No deshabilito las publicaciones de la interfaz Ethernet1/0.*

D2(config-router)#**exit**## *Salgo de la configuración.*

D2(config)#**ipv6 router ospf 6**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-router)#**router-id 0.0.6.132**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-router)#**passive-interface default**## *Deshabilito las publicaciones OSPFv3, todas las interfaces.*

D2(config-router)#**no passive-interface e1/0**## *No deshabilito las publicaciones de la interfaz Ethernet 1/0.*

D2(config-router)#**exit** ## *Salgo de la configuración de router.*

D2(config)#**interface e1/0** ## *Ingreso al interfaz Ethernet 1/0.*

D2(config-if)#**ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-if)#**exit**## *Salgo de la interfaz Ethernet 1/0.*

D2(config)#**interface vlan 100** ## *Ingresando a la Vlan.*

**D2(config-if)#ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-if)#**exit** ## *Salir de la configuración vlan 100.*

D2(config)#**interface vlan 101**## *Ingresando a la Vlan.*

D2(config)#**ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config)#**exit**## *Salir de la configuración vlan 101.*

D2(config)#**interface vlan 102**## *Ingresando a la Vlan.*

D2(config)#**ipv6 ospf 6 area 0**## *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config)#**exit** ## *Salir de la configuración vlan 102.*

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de

primer salto para los host en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

**Tabla 4: Configurar la Redundancia del Primer Salto - Parte 4**

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 F0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use la SLA número <b>4</b> para IPv4.</li> <li>• Use la SLA número <b>6</b> para Ipv6.</li> </ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 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 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> <li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li> <li>• Use el número de rastreo <b>6</b> para la IP SLA 6.</li> </ul> <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 F0/0.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use la SLA número <b>4</b> para Ipv4.</li> <li>• Use la SLA número <b>6</b> para Ipv6.</li> </ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 F0/0 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> <ul style="list-style-type: none"> <li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li> <li>• Use el número de rastreo <b>6</b> para la SLA 6.</li> </ul> <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15</p>



		segundos.
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 versión 2.</p> <p>Configure IPv4 HSRP grupo <b>104</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.100.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>114</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.101.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.102.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>106</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>116</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Registre el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>126</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> </ul>

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

		Rastree el objeto 6 para disminuir en 60.
--	--	-------------------------------------------

**Switch D1:** Configuración IP SLAs, HSRPv2.

Se crean las dos IP SLAs, número 4 para IPv4 y número 6 para Ipv6:

D1#**configure terminal** ## Se ingresa al modo configuración.

D1(config)#**ip sla 4** ## Se crea SLA número 4 para IPv4.

D1(config-ip-sla)#**icmp-echo 10.0.10.1**## Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV4.

D1(config-ip-sla-echo)#**frequency 5**## IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.

D1(config-ip-sla-echo)#**exit**## Salir de la configuración ip sla 4.

D1(config)#**ip sla 6** ## Se crea SLA número 4 para IPv6.

D1(config-ip-sla)#**icmp-echo 2001:db8:100:1010::1** ## Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV6.

D1(config-ip-sla-echo)#**frequency 5** ## IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.

D1(config-ip-sla-echo)#**exit** ## Salir de la configuración IP sla 6.

D1(config)#**ip sla schedule 4 life forever start-time now** ## Es la IP SLA objeto para la IP SLA 4.

D1(config)#**ip sla schedule 6 life forever start-time now** ## Es la IP SLA objeto para la IP SLA 6.

D1(config)#**track 4 ip sla 4** ## El número 4 es de rastreo para la IP SLA 4.

D1(config-track)#**delay down 10 up 15** ## IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV4.

D1(config-track)#**exit** ## Salir de la configuración IP sla 4.

D1(config)#**track 6 ip sla 6** ## El número 6 es de rastreo para la IP SLA 4.

D1(config-track)#**delay down 10 up 15** ## IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV6.

D1(config-track)#**exit** ## Salir de la configuración ip sla 6.

D1 es el Router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150, se Configura HSRP versión 2 en el grupo 104, 114 y 124 para IPV4, los grupos 106, 116 y 126 para IPV6:

D1(config)#**interface vlan 100** ## Ingreso a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106.

D1(config-if)#**standby version 2** ## Configuración de HSRP versión 2.

D1(config-if)#**standby 104 ip 10.0.100.254** ## Se asigna dirección IP virtual (10.0.100.254) en IPv4 HSRP grupo 104.

D1(config-if)#**standby 104 priority 150** ## Se establece la prioridad del grupo en 150.

D1(config-if)#**standby 104 preempt** ## Se habilita la preferencia.

D1(config-if)#**standby 104 track 4 decrement 60** ## Rastrea el objeto 4 y decremente en 60.

D1(config-if)#**standby 106 ipv6 autoconfig** ## La dirección IP virtual como automática.

D1(config-if)#**standby 106 priority 150** ## Prioridad del grupo en 150.

D1(config-if)#**standby 106 preempt** ## Se habilita la preferencia.

D1(config-if)#**standby 106 track 6 decrement 60** ## Rastrea el objeto 6 y

*decremente en 60.*

D1(config-if)#**exit** ## *Salir de la configuración Vlan 100.*

D1(config)#**interface vlan 101** ## *Ingreso a la interfaz Vlan 101, para luego configurar IPv4 HSRP grupo 114 e IPV6 HSRP grupo 116.*

D1(config-if)#**standby version 2** ## *Configuración de HSRP versión 2.*

D1(config-if)#**standby 114 ip 10.0.101.254** ## *Se asigna dirección IP virtual (10.0.101.254) en IPv4 HSRP grupo 114.*

D1(config-if)#**standby 114 preempt** ## *Se habilita la preferencia.*

D1(config-if)#**standby 114 track 4 decrement 60** ## *Rastrea el objeto 4 y decremente en 60.*

D1(config-if)#**standby 116 ipv6 autoconfig** ## *La dirección IP virtual como automática.*

D1(config-if)#**standby 116 preempt** ## *Se habilita la preferencia.*

D1(config-if)#**standby 116 track 6 decrement 60** ## *Rastrea el objeto 6 y decremente en 60.*

D1(config-if)#**exit** ## *Salir de la configuración Vlan 101.*

D1(config)#**interface vlan 102** ## *Ingreso a la interfaz Vlan 102, para luego configurar IPv4 HSRP grupo 124 e IPV6 HSRP grupo 126.*

D1(config-if)#**standby version 2** ## *Configuración de HSRP versión 2.*

D1(config-if)#**standby 124 ip 10.0.102.254** ## *Se asigna dirección IP virtual (10.0.102.254) en IPv4 HSRP grupo 124.*

D1(config-if)#**standby 124 priority 150** ## *Se establece la prioridad del grupo en 150.*

D1(config-if)#**standby 124 preempt** ## Se habilita la preferencia.

D1(config-if)#**standby 124 track 4 decrement 60** ## Rastrea el objeto 4 y decremente en 60.

D1(config-if)#**standby 126 ipv6 autoconfig** ## La dirección IP virtual como automática.

D1(config-if)#**standby 126 priority 150** ## Se establece la prioridad del grupo en 150.

D1(config-if)#**standby 126 preempt** ## Se habilita la preferencia

D1(config-if)#**standby 126 track 6 decrement 60** ## Rastrea el objeto 6 y decremente en 60.

D1(config-if)#**exit** ## Salir de la configuración Vlan 102.

D1(config)#**end** ## Salir del modo configuración.

D1#

**Switch D2:** Configuración IP SLAs, HSRPv2.

Se crean las dos IP SLAs, número 4 para IPv4 y número 6 para Ipv6:

D2#**configure terminal** ## Ingresa a modo configuración.

D2(config)#**ip sla 4** ## Se crea SLA número 4 para IPv4.

D2(config-ip-sla)#**icmp-echo 10.0.11.1** ## Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV4.

D2(config-ip-sla-echo)#**frequency 5** ## IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.

D2(config-ip-sla-echo)#**exit** ## Salir de la configuración ip sla 4.

D2(config)#**ip sla 6** ## Se crea SLA número 4 para IPv6.

D2(config-ip-sla)#**icmp-echo 2001:db8:100:1011::1** ## Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV6.

D2(config-ip-sla-echo)#**frequency 5** ## IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.

D2(config-ip-sla-echo)#**exit** ## Salir de la configuración IP sla 6.

D2(config)#**ip sla schedule 4 life forever start-time now** ## Es la IP SLA objeto para la IP SLA.

D2(config)#**ip sla schedule 6 life forever start-time now** ## Es la IP SLA objeto para la IP SLA.

D2(config)#**track 4 ip sla 4** ## El número 4 es de rastreo para la IP SLA 4.

D2(config-track)#**delay down 10 up 15** ## IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV4.

D2(config-track)#**exit** ##Salir de la configuración IP SLA 4.

D2(config)#**interface vlan 100** ## Ingreso a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106.

D2(config-if)#**standby version 2** ## Configuración de HSRP versión 2.

D2(config-if)#**standby 104 ip 10.0.100.254** ## Se establece la prioridad del grupo en 150.

D2(config-if)#**standby 104 preempt** ## Se habilita la preferencia.

D2(config-if)#**standby 104 track 4 decrement 60** ## Rastrea el objeto 4 y decremente en 60.

D2(config-if)#**standby 106 ipv6 autoconfig** ## La dirección IP virtual como automática.

D2(config-if)#**standby 106 preempt** ## Se habilita la preferencia.

D2(config-if)#**standby 106 track 6 decrement 60** ## Rastrea el objeto 6 y decremente en 60.

D2(config-if)#**exit** ## Salir de la configuración Vlan 100.

D2(config)#**interface vlan 101** ## Ingreso a la interfaz Vlan 101, para luego configurar IPv4 HSRP grupo 114 e IPV6 HSRP grupo 116.

D2(config-if)#**standby version 2** ## Configuración de HSRP versión 2

D2(config-if)#**standby 114 ip 10.0.101.254** ## Se asigna dirección IP virtual (10.0.101.254) en IPv4 HSRP grupo 114.

D2(config-if)#**standby 114 priority 150** ## Prioridad del grupo en 150.

D2(config-if)#**standby 114 preempt** ## Se habilita la preferencia.

D2(config-if)#**standby 114 track 4 decrement 60** ## Rastrea el objeto 6 y decremente en 60.

D2(config-if)#**standby 116 ipv6 autoconfig** ## La dirección IP virtual como automática.

D2(config-if)#**standby 116 priority 150** ## Prioridad del grupo en 150.

D2(config-if)#**standby 116 preempt** ## Se habilita la preferencia.

D2(config-if)#**standby 116 track 6 decrement 60** ## Rastrea el objeto 6 y decremente en 60.

D2(config-if)#**exit** ## Salir de la configuración Vlan 101.

D2(config)#**interface vlan 102** ## Ingreso a la interfaz Vlan 102, para luego configurar IPv4 HSRP grupo 124 e IPV6 HSRP grupo 126.

D2(config-if)#**standby version 2** ## Configuración de HSRP versión 2.

D2(config-if)#**standby 124 ip 10.0.102.254** ## Se asigna dirección IP virtual (10.0.102.254) en IPv4 HSRP grupo 124.

D2(config-if)#**standby 124 preempt** ## Se habilita la preferencia.



D2(config-if)#**standby 124 track 4 decrement 60** ## Rastrea el objeto 4 y decremente en 60.

D2(config-if)#**standby 126 ipv6 autoconfig** ## La dirección IP virtual como automática.

D2(config-if)#**standby 126 preempt** ## Se habilita la preferencia

D2(config-if)#**standby 126 track 6 decrement 60** ## Rastrea el objeto 6 y decremente en 60.

D2(config-if)#**exit** ## Salir de la configuración Vlan 102.

D2(config)#**end** ## Salir del modo configuración.

D2#

## Parte 5: Seguridad.

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

**Tabla 5: Seguridad – Parte 5**

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"><li>• Nombre de usuario Local: <b>admin</b></li><li>• Nivel de privilegio <b>15</b></li><li>• Contraseña: <b>cisco12345cisco</b></li></ul>
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.

5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"> <li>• Dirección IP del servidor RADIUS es 10.0.100.6.</li> <li>• Puertos UDP del servidor RADIUS son 1812 y 1813.</li> <li>• Contraseña: <b>\$trongPass</b></li> </ul>
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> <li>• Use la lista de métodos por defecto</li> <li>• Valide contra el grupo de servidores RADIUS</li> <li>• De lo contrario, utilice la base de datos local.</li> </ul>
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: <b>raduser</b> y la contraseña: <b>upass123</b> .

En todos los dispositivos, se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT, adicional se crea un usuario local con la misma encriptación, con usuario **sadmin** y contraseña **cisco12345cisco**. Para habilita Autenticación, autorización, contabilidad se realiza en R1, R3, D1, D2 y A1.

**Route R1:** Configuración SCRYPT, AAA.

R1# **configure terminal** ## *Ingresar a modo configuración.*

R1(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** ## *Se hace uso del algoritmo de encriptación SCRYPT.*

R1(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** ## *Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

R1(config)#**aaa new-model** *## Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

R1(config)#**radius server RADIUS** *## Se ingresa al interfaz del servidor Radius.*

R1(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *## Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

R1(config-radius-server)#**key \$strongPass** *## Asignación de la contraseña.*

R1(config-radius-server)#**exit** *## Salir de la interfaz del servidor Radius.*

R1(config)#**aaa authentication login default group radius local** *## Se realiza autenticación por defecto.*

R1(config)#**end** *## Salir del modo configuración.*

R1#

**Route R2:** Configuración SCRYPT.

R2#**configure terminal** *## Ingresa a modo configuración.*

R2(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *## Se hace uso del algoritmo de encriptación SCRYPT.*

R2(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *## Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

R2(config)#**end** *## Salir del modo configuración.*

R2#

**Route R3:** Configuración SCRYPT, AAA.

**R3#configure terminal** *## Ingresa a modo configuración.*

**R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco** *## Se hace uso del algoritmo de encriptación SCRYPT.*

**R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *## Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

**R3(config)#aaa new-model** *## Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

**R3(config)#radius server RADIUS** *## Se ingresa al interfaz del servidor Radius.*

**R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *## Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

**R3(config-radius-server)# key \$strongPass** *## Asignación de la contraseña.*

**R3(config-radius-server)#exit** *## Salir de la interfaz del servidor Radius.*

**R3(config)#aaa authentication login default group radius local** *## Se realiza autenticación por defecto.*

**R3(config)#end** *## Salir del modo configuración.*

**R3#**

**Switch D1:** Configuración SCRYPT, AAA.

**D1#configure terminal** *## Ingresa a modo configuración.*

**D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco** *## Se hace uso del algoritmo de encriptación SCRYPT.*

**D1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret**

**cisco12345cisco** *## Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

D1(config)#**aaa new-model** *## Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

D1(config)#**radius server RADIUS** *## Se ingresa al interfaz del servidor Radius.*

D1(config-radius-server)# **address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *## Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

D1(config-radius-server)#**key \$strongPass** *## Asignación de la contraseña.*

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

D1(config)#**aaa authentication login default group radius local** *## Se realiza autenticación por defecto.*

D1(config)#**end** *## Salir del modo configuración.*

D1#

**Switch D2:** Configuración SCRYPT, AAA.

D2#**configure terminal** *## Ingresa a modo configuración.*

D2(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *## Se hace uso del algoritmo de encriptación SCRYPT.*

D2(config)# **username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *## Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

D2(config)#**aaa new-model** *## Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

D2(config)#**radius server RADIUS** *## Se ingresa al interfaz del servidor Radius.*

D2(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813**  
*## Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

D2(config-radius-server)#**key \$strongPass** *## Asignación de la contraseña.*

D2(config-radius-server)#**exit** *## Salir de la interfaz del servidor Radius.*

D2(config)#**aaa authentication login default group radius local** *## Se realiza autenticación por defecto.*

D2(config)#**end** *## Salir del modo configuración.*

D2#

**Switch A1:** Configuración SCRYPT, AAA.

A1#**configure terminal** *## Ingresa a modo configuración.*

A1(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *## Se hace uso del algoritmo de encriptación SCRYPT.*

A1(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *## Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

A1(config)#**aaa new-model** *## Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

A1(config)#**radius server RADIUS** *## Se ingresa al interfaz del servidor Radius.*

A1(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813**  
*## Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

A1(config-radius-server)#**key \$strongPass** *## Asignación de la contraseña.*

A1(config-radius-server)#**exit** *## Salir de la interfaz del servidor Radius.*

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

autenticación por defecto.

A1(config)#end ## Salir del modo configuración.

A1#

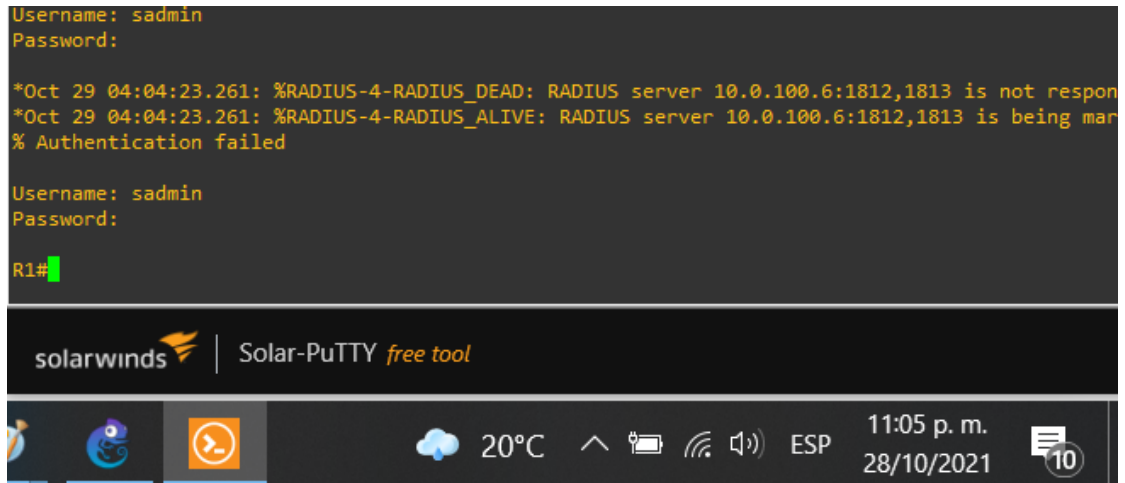
**Figura 9: Solicitud de Autenticación R1.**

```
Username: sadmin
Password:

*Oct 29 04:04:23.261: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.0.100.6:1812,1813 is not respon
*Oct 29 04:04:23.261: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.0.100.6:1812,1813 is being mar
% Authentication failed

Username: sadmin
Password:

R1#
```



**Figura 10: Solicitud de Autenticación R3**

```
Username: sadmin
Password:

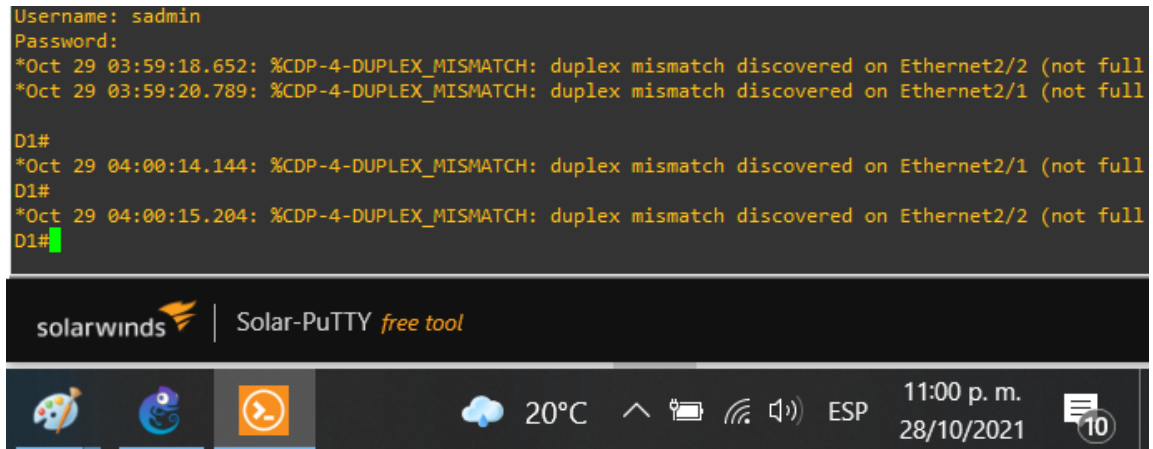
*Oct 29 03:58:36.554: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.0.100.6:1812,1813 is not responding
*Oct 29 03:58:36.554: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.0.100.6:1812,1813 is being marked
R3#
R3#
```



**Figura 11: Solicitud de Autenticación D1.**

```
Username: sadmin
Password:
*Oct 29 03:59:18.652: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not full
*Oct 29 03:59:20.789: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/1 (not full

D1#
*Oct 29 04:00:14.144: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/1 (not full
D1#
*Oct 29 04:00:15.204: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not full
D1#
```

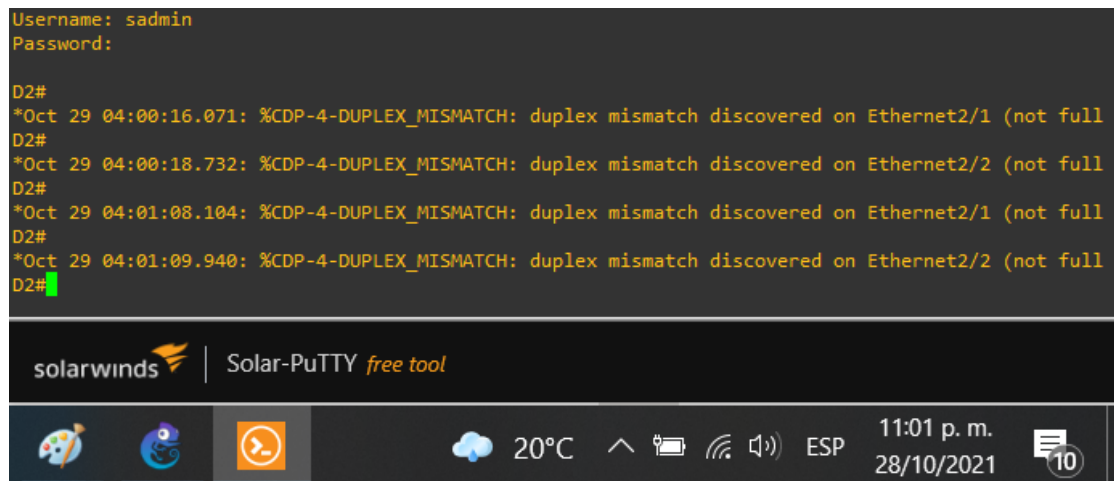


The screenshot shows a terminal window titled "Solar-PuTTY free tool" with the SolarWinds logo. The terminal output displays a login prompt for "sadmin", followed by two CDP error messages regarding duplex mismatches on Ethernet2/2 and Ethernet2/1. The user then enters "D1#" and receives another CDP error message on Ethernet2/1, followed by a third CDP error message on Ethernet2/2. A green cursor is visible at the end of the final "D1#" prompt. The Windows taskbar at the bottom shows the time as 11:00 p.m. on 28/10/2021, along with system icons for weather (20°C), network, and volume.

**Figura 12: Solicitud de Autenticación D2.**

```
Username: sadmin
Password:

D2#
*Oct 29 04:00:16.071: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/1 (not full
D2#
*Oct 29 04:00:18.732: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not full
D2#
*Oct 29 04:01:08.104: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/1 (not full
D2#
*Oct 29 04:01:09.940: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not full
D2#
```



The screenshot shows a terminal window titled "Solar-PuTTY free tool" with the SolarWinds logo. The terminal output displays a login prompt for "sadmin", followed by four CDP error messages regarding duplex mismatches on Ethernet2/1 and Ethernet2/2. The user then enters "D2#" and receives a series of CDP error messages. A green cursor is visible at the end of the final "D2#" prompt. The Windows taskbar at the bottom shows the time as 11:01 p.m. on 28/10/2021, along with system icons for weather (20°C), network, and volume.



**Figura 13: Solicitud de Autenticación A1.**

```

Username: admin
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

A1>
*Oct 29 04:02:41.988: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet0/3 (not half duplex)
A1>
*Oct 29 04:02:47.882: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet0/2 (not half duplex)
A1>

```

**Parte 6: Configure las funciones de Administración de Red.**

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

**Tabla 6: Configure las funciones de Administración de Red – 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.
6.3	Configure NTP en R1, R3, D1, D2, y A1	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> <li>R1 debe sincronizar con R2.</li> <li>R3, D1 y A1 para sincronizar la hora con R1.</li> <li>D2 para sincronizar la hora con R3.</li> </ul>

6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	<p>Especificaciones de SNMPv2:</p> <ul style="list-style-type: none"> <li>• Únicamente se usará SNMP en modo lectura (Read-Only).</li> <li>• Límite el acceso SNMP a la dirección IP de la PC1.</li> <li>• Configure el valor de contacto SNMP con su nombre.</li> <li>• Establezca el <i>community string</i> en <b>ENCORSA</b>.</li> <li>• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.</li> <li>• En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>.</li> </ul> <p>En A1, habilite el envío de <i>traps config</i>.</p>

En todos los dispositivos se configura el reloj local UTC, para el R2 se configura el NTP maestro en estrato 3.

**Actualización:** De reloj en todos los dispositivos.

clock timezone UTC -5

**Router R2:** Configuración NTP Máster 3.

R2(config)#**ntp master 3** ## Se configura el NTP maestro en estrato 3.

R2(config)#**end** ## Salir del modo configuración.

Se realiza configuración de NTP y SNMPv2 en R1, R3, D1, D2 y A1.

## **Router R1: Configuración NTP y SNMP.**

**R1#configure terminal** *## Ingresa a modo configuración*

**R1(config)#ntp server 2.2.2.2** *## Se configura NTP para sincronizar con R2 por medio de Loopback 0.*

**R1(config)#logging trap warning** *## Se configura Syslog en nivel WARNING.*

**R1(config)#logging host 10.0.100.5** *## Se configura Syslog a la PC1 10.0.100.5.*

**R1(config)#logging on** *## Se enciende configuración Syslog.*

**R1(config)#ip access-list standard SNMP-NMS** *## Configuración de SNMPv2c en modo estándar (lectura).*

**R1(config-std-nacl)#permit host 10.0.100.5** *## Límite de acceso SNMP a la PC1.*

**R1(config-std-nacl)#exit** *## Salir de la configuración SNMPv2c.*

**R1(config)#snmp-server contact Cisco Milton** *## Se configura el valor de contacto SNMP con mi nombre.*

**R1(config)#snmp-server community ENCORSA ro SNMP-NMS** *## Se establece community string en ENCORSA.*

**R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA** *## Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

**R1(config)#snmp-server ifindex persist** *## Identifica cada interfaz para la identificación SNMP de esta interfaz.*

**R1(config)#snmp-server enable traps bgp** *## Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

**R1(config)#snmp-server enable traps config** *## Envía notificaciones de configuración.*

**R1(config)#snmp-server enable traps ospf** *## Envía notificaciones de OSPF.*

R1(config)#**end** ## Salir del modo configuración.

R1#

**Router R3:** Configuración NTP y SNMP.

R3#**configure terminal** ## Ingresa a modo configuración

R3(config)#**ntp server 10.0.10.1** ## Se configura NTP para sincronizar hora con R1.

R3(config)#**logging trap warning** ## Se configura Syslog en nivel WARNING.

R3(config)#**logging host 10.0.100.5** ## Se configura Syslog a la PC1 10.0.100.5.

R3(config)#**logging on** ## Se enciende configuración Syslog.

R3(config)#**ip access-list standard SNMP-NMS** ## Configuración de SNMPv2c en modo estándar (lectura).

R3(config-std-nacl)#**permit host 10.0.100.5** ## Límite de acceso SNMP a la PC1.

R3(config-std-nacl)#**exit** ## Salir de la configuración SNMPv2c.

R3(config)#**snmp-server contact Cisco Milton** ## Se configura el valor de contacto SNMP con mi nombre.

R3(config)#**snmp-server community ENCORSA ro SNMP-NMS** ## Se establece community string en ENCORSA.

R3(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** ## Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.

R3(config)#**snmp-server ifindex persist** ## Identifica cada interfaz para la identificación SNMP de esta interfaz.

R3(config)#**snmp-server enable traps config** ## Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).

R3(config)#**snmp-server enable traps ospf** ## Envía notificaciones de

*configuración.*

R3(config)#**end** *## Salir del modo configuración.*

R3#

**Switch D1:** Configuración NTP y SNMP.

D1(config)#**ntp server 10.0.10.1** *## Se configura NTP para sincronizar hora con R1.*

D1(config)#**logging trap warning** *## Se configura Syslog en nivel WARNING.*

D1(config)#**logging host 10.0.100.5** *## Se configura Syslog a la PC1 10.0.100.5.*

D1(config)#**logging on** *## Se enciende configuración Syslog.*

D1(config)#**ip access-list standard SNMP-NMS** *## Configuración de SNMPv2c en modo estándar (lectura).*

D1(config-std-nacl)#**permit host 10.0.100.5** *## Límite de acceso SNMP a la PC1.*

D1(config-std-nacl)#**exit** *## Salir de la configuración SNMPv2c.*

D1(config)#**snmp-server contact Cisco Student** *## Se configura el valor de contacto SNMP con mi nombre.*

D1(config)#**snmp-server community ENCORSA ro SNMP-NMS** *## Se establece community string en ENCORSA.*

D1(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** *## Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

D1(config)#**snmp-server ifindex persist** *## Identifica cada interfaz para la identificación SNMP de esta interfaz.*

D1(config)#**snmp-server enable traps** *## Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

D1(config)#**snmp-server enable traps config** ## Envía notificaciones de configuración.

D1(config)#**snmp-server enable traps ospf** ## Envía notificaciones de OSPF

D1(config)#**end** ## Salir del modo configuración.

D1#

**Switch D2:** Configuración NTP y SNMP.

D2(config)#**ntp server 10.0.10.1** ## Se configura NTP para sincronizar hora con R1.

D2(config)#**logging trap warning** ## Se configura Syslog en nivel WARNING.

D2(config)#**logging host 10.0.100.5** ## Se configura Syslog a la PC1 10.0.100.5.

D2(config)#**logging on** ## Se enciende configuración Syslog.

D2(config)#**ip access-list standard SNMP-NMS** ## Configuración de SNMPv2c en modo estándar (lectura).

D2(config-std-nacl)#**permit host 10.0.100.5** ## Límite de acceso SNMP a la PC1.

D2(config-std-nacl)#**exit** ## Salir de la configuración SNMPv2c.

D2(config)#**snmp-server contact Cisco Milton** ## Se configura el valor de contacto SNMP con mi nombre.

D2(config)#**snmp-server community ENCORSA ro SNMP-NMS** ## Se establece community string en ENCORSA.

D2(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** ## Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.

D2(config)#**snmp-server enable traps config** ## Envía notificaciones de configuración.

D2(config)#**snmp-server enable traps ospf** ## Envía notificaciones de OSPF.

D2(config)#**end** ## salir del modo configuración.

**Switch A1:** Configuración NTP y SNMP.

A1(config)#**ntp server 10.0.10.1** ## Se configura NTP para sincronizar hora con R1.

A1(config)#**logging trap warning** ## Se configura Syslog en nivel WARNING.

A1(config)#**logging host 10.0.100.5** ## Se configura Syslog a la PC1 10.0.100.5.

A1(config)#**logging on** ## Se enciende configuración Syslog.

A1(config)#**ip access-list standard SNMP-NMS** ## Configuración de SNMPv2c en modo estándar (lectura).

A1(config-std-nacl)#**permit host 10.0.100.5** ## Límite de acceso SNMP a la PC1.

A1(config-std-nacl)#**exit** ## Salir de la configuración SNMPv2c.

A1(config)#**snmp-server contact Cisco Milton** ## Se configura el valor de contacto SNMP con mi nombre.

A1(config)#**snmp-server community ENCORSA ro SNMP-NMS** ## Se establece community string en ENCORSA.

A1(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** ## Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.

A1(config)#**snmp-server ifindex persist** ## Identifica cada interfaz para la identificación SNMP de esta interfaz.

A1(config)#**snmp-server enable traps** ## Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).

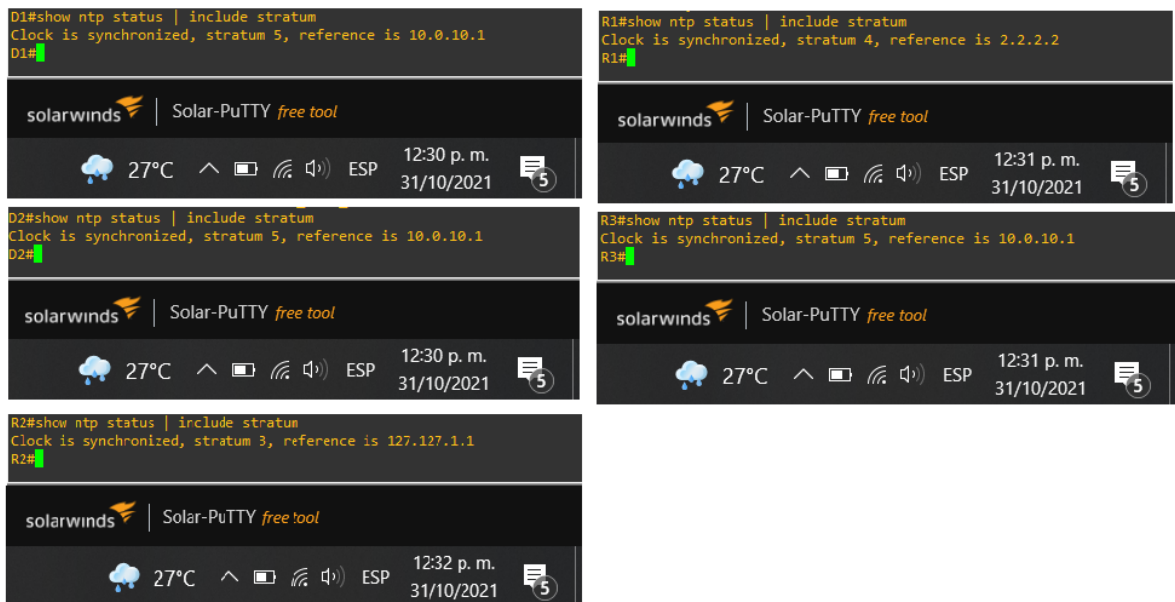
A1(config)#**snmp-server enable traps ospf** ## Envía notificaciones de

configuración.

A1(config)#end ## Salir del modo configuración.

A1#

Figura 14: Sincronización del reloj.





## CONCLUSIONES

Con la creciente evolución de las tecnologías, las redes se vuelven cada vez más importante e imprescindible, la evolución y mejoras continuas que se deben realizar sobre estas tanto en su parte técnica como en la seguridad apunta a que quien tenga una certificación CCNP abre sus puertas y gana una falibilidad en su trabajo.

El simulador GNS3 fue muy importante para el desarrollo de la actividad, siempre y cuando se presentó falencias al momento de configurar los Switchs, no soportaba la capa 3 del modelo OSI; inicialmente se instaló la imagen IOU L2 Versión 15.1a, como alternativa se instala la imagen IOU L2 versión 15.2d, logrando que los Switchs contara con características de capa 2 y capa 3.

Para el protocolo OSPFv2 y v3, durante la simulación presentó inconveniente de no tomar los comandos de configuración, para la solución, se anticipa con el comando `ipv6 unicast-routing`, logrando así la actualización de las tablas de enrutamiento.

Al momento de configurar las interfaces de los dispositivos en modo troncal, se evidencio la importancia del comando `switchport trunk encapsulation dot1q`, sin esta línea de comando, los dispositivos no permitían conectividad.

Para el escenario realizado muestra la importancia del protocolo de autenticación, autorización y auditoría (AAA), proporciona el marco de trabajo necesario para habilitar la seguridad de acceso, como la política de seguridad de red logra la implementación de un sistema de auditoría que registre quién inició sesión y cuándo, y qué hizo mientras permaneció conectado. Es de gran importancia los protocolos Remote Authentication Dial-In User Service (RADIUS) porque permite el acceso solo a personas autorizados.

## BIBLIOGRAFÍA

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

MARCO, Maria. "Escaneando la Informática". {En línea}. {16 septiembre de 2021} disponible en: (<https://books.google.com.co/books?id=svpzjkMpdUC&lpg=PA99&dq=importancia%20del%20ccnp%20cisco&pg=PP1#v=onepage&q=importancia%20del%20ccnp%20cisco&f=false>).

RICO, Alberto. "CCNA, la certificación de Cisco (cómo conseguirla)". {En línea}. {16 septiembre de 2021} disponible en: (<https://www.ambit-bst.com/blog/ccna-la-certificaci%C3%B3n-de-cisco-c%C3%B3mo-conseguirla>).

ROMERO, Christian. "Establecer IOU L2 e IOU L3 en GNS3". {En línea}. {16 Octubre de 2021} disponible en: ([www.youtube.com/watch?v=ZXfseiLKlgl](http://www.youtube.com/watch?v=ZXfseiLKlgl)).

ROMERO, Christian. "Setup IOU L2 and IOU L3 on GNS3 VM 2.2.14". {En línea}. {16 septiembre de 2021} disponible en: (<https://www.youtube.com/watch?v=ivxMfrcMuAk>).

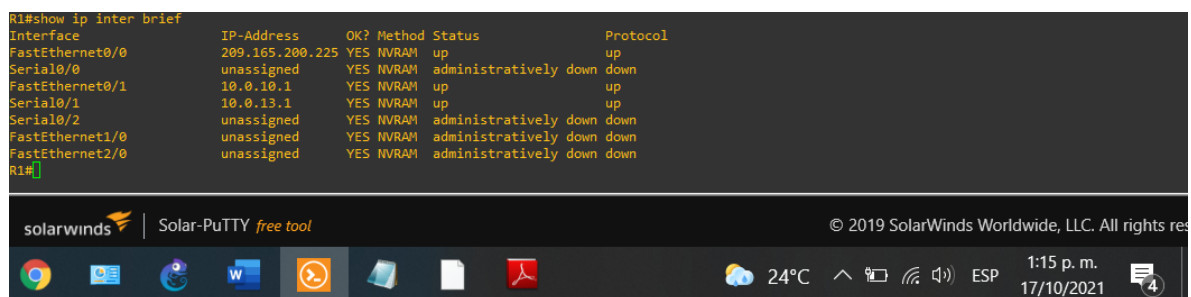
## ANEXOS

### Evidencias Del Desarrollo:

#### Parte 1: revisar configuración de las interfaces

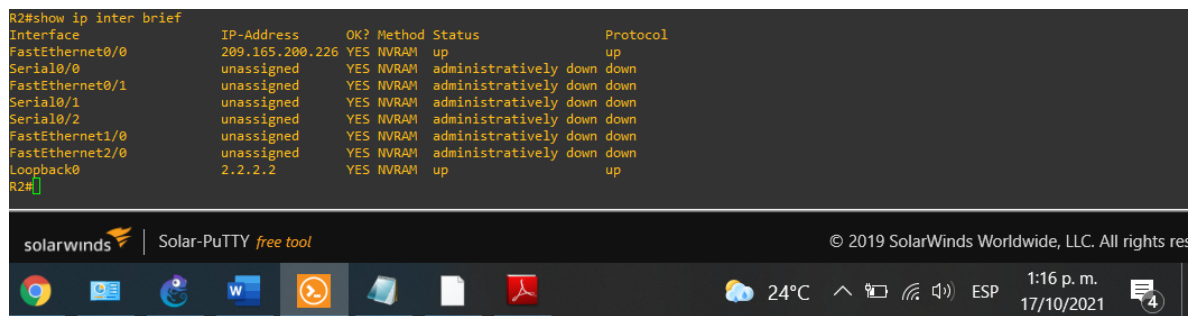
##### R1:

```
R1#show ip inter brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    209.165.200.225 YES NVRAM    up          up
Serial0/0          unassigned     YES NVRAM    administratively down down
FastEthernet0/1    10.0.10.1      YES NVRAM    up          up
Serial0/1          10.0.13.1     YES NVRAM    up          up
Serial0/2          unassigned     YES NVRAM    administratively down down
FastEthernet1/0    unassigned     YES NVRAM    administratively down down
FastEthernet2/0    unassigned     YES NVRAM    administratively down down
R1#
```



##### R2:

```
R2#show ip inter brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    209.165.200.226 YES NVRAM    up          up
Serial0/0          unassigned     YES NVRAM    administratively down down
FastEthernet0/1    unassigned     YES NVRAM    administratively down down
Serial0/1          unassigned     YES NVRAM    administratively down down
Serial0/2          unassigned     YES NVRAM    administratively down down
FastEthernet1/0    unassigned     YES NVRAM    administratively down down
FastEthernet2/0    unassigned     YES NVRAM    administratively down down
Loopback0          2.2.2.2        YES NVRAM    up          up
R2#
```



##### R3:

```
R3#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 10.0.11.1       YES NVRAM   up          up
Serial0/0       unassigned      YES NVRAM   administratively down down
FastEthernet0/1 unassigned      YES NVRAM   administratively down down
Serial0/1       10.0.13.3       YES NVRAM   up          up
Serial0/2       unassigned      YES NVRAM   administratively down down
FastEthernet1/0 unassigned      YES NVRAM   administratively down down
FastEthernet2/0 unassigned      YES NVRAM   administratively down down
R3#
```

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

24°C ESP 1:16 p. m. 17/10/2021

**D1:**

```
D1#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/1 unassigned      YES unset  administratively down down
GigabitEthernet0/2 unassigned      YES unset  administratively down down
GigabitEthernet0/3 unassigned      YES unset  administratively down down
GigabitEthernet1/0 10.0.10.2       YES NVRAM   up          up
GigabitEthernet1/1 unassigned      YES unset  up          up
GigabitEthernet1/2 unassigned      YES unset  up          up
GigabitEthernet1/3 unassigned      YES unset  up          up
GigabitEthernet2/0 unassigned      YES unset  up          up
GigabitEthernet2/1 unassigned      YES unset  up          up
GigabitEthernet2/2 unassigned      YES unset  up          up
GigabitEthernet2/3 unassigned      YES unset  up          up
GigabitEthernet3/0 unassigned      YES unset  administratively down down
GigabitEthernet3/1 unassigned      YES unset  administratively down down
GigabitEthernet3/2 unassigned      YES unset  administratively down down
GigabitEthernet3/3 unassigned      YES unset  administratively down down
Port-channel11 unassigned      YES unset  up          up
Port-channel12 unassigned      YES unset  up          up
Vlan100         10.0.100.1      YES NVRAM   up          up
Vlan101         10.0.101.1      YES NVRAM   up          up
Vlan102         10.0.102.1      YES NVRAM   up          up
D1#
```

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

24°C ESP 1:17 p. m. 17/10/2021

**D2:**

```

D2#show ip inter brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  unassigned     YES unset  administratively down  down
GigabitEthernet0/1  unassigned     YES unset  down        down
GigabitEthernet0/2  unassigned     YES unset  down        down
GigabitEthernet0/3  unassigned     YES unset  down        down
GigabitEthernet1/0  10.0.11.2      YES NVRAM  up          up
GigabitEthernet1/1  unassigned     YES unset  up          up
GigabitEthernet1/2  unassigned     YES unset  up          up
GigabitEthernet1/3  unassigned     YES unset  up          up
GigabitEthernet2/0  unassigned     YES unset  up          up
GigabitEthernet2/1  unassigned     YES unset  up          up
GigabitEthernet2/2  unassigned     YES unset  up          up
GigabitEthernet2/3  unassigned     YES unset  up          up
GigabitEthernet3/0  unassigned     YES unset  down        down
GigabitEthernet3/1  unassigned     YES unset  down        down
GigabitEthernet3/2  unassigned     YES unset  down        down
GigabitEthernet3/3  unassigned     YES unset  down        down
Port-channel2      unassigned     YES unset  up          up
Port-channel12     unassigned     YES unset  up          up
Vlan100            10.0.100.2     YES NVRAM  up          up
Vlan101            10.0.101.2     YES NVRAM  up          up
Vlan102            10.0.102.2     YES NVRAM  up          up
D2#
*Oct 17 18:14:06.785: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/0 (not half duplex), with R3 FastEthernet0/0 (half duplex)
D2#

```

**Parte 2:** Revisar configuración de capa 2 y compatibilidad de host.

**D1:**

**Mostrar configuración troncal**

```

D1#show inter 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#

```

**Revisar 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#
```

## Show run interface G2/3, configuración del interfaz del PC1

```
D1#Show run interface G2/3
Building configuration...

Current configuration : 152 bytes
|
interface GigabitEthernet2/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
D1#
```

En D2:

## Show run interface trunk

```
D2#show inter trunk

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

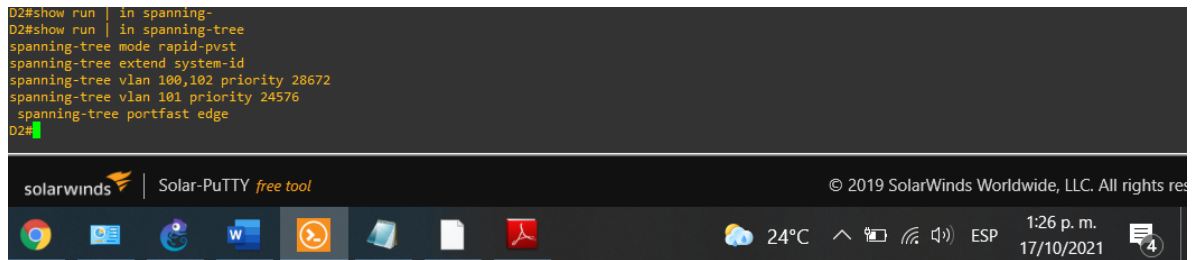
Port      Vlans allowed on trunk
Po2       1-4094
Po12      1-4094

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      100-102
D2#
```

show run | include spanning-tree

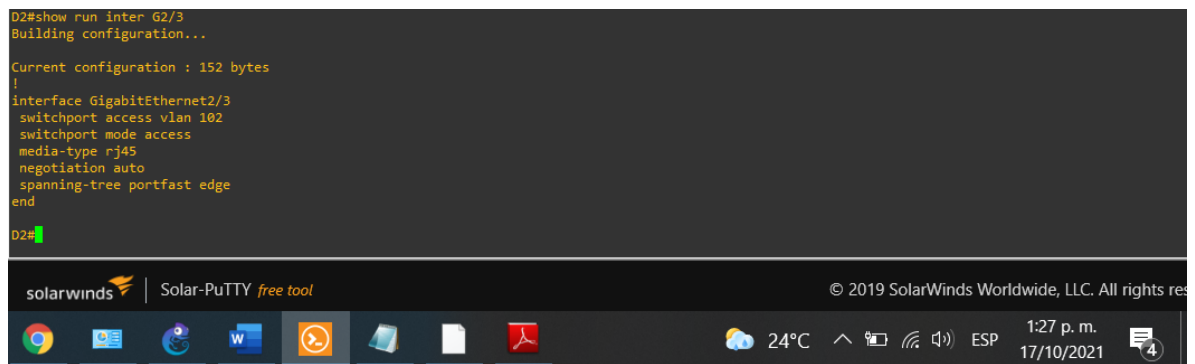
```
D2#show run | in spanning-
D2#show run | in spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
spanning-tree portfast edge
D2#
```



**Show run interface G2/3, es revisar configuración de la interfaz del PC2**

```
D2#show run inter G2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 102
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
D2#
```

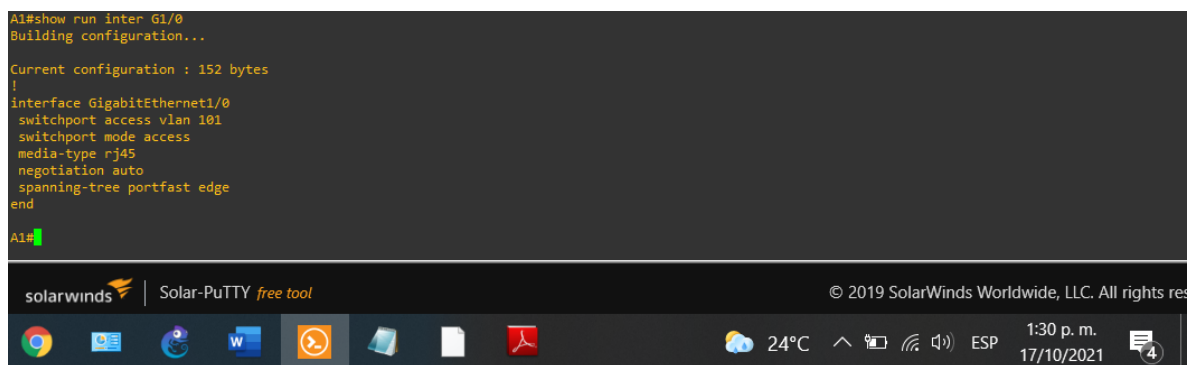


**A1:**

**show run interface G1/0, para revisar la configuración en el interfaz donde esta el PC3**

```
A1#show run inter G1/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/0
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```



**show run interface G1/1, para revisar la configuración en el interfaz donde esta el PC4**

```
A1#show run inter G1/1
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/1
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```

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

24°C 1:30 p. m. 17/10/2021

**Parte 3:** Revisar configuración de enrutamiento.

**R1:** show run | section ^router ospf

```
R1#show run | section ^router ospf

*Mar 1 00:52:00.247: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not full duplex),
ter ospf 4
 router-id 0.0.4.1
 log-adjacency-changes
 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#
```

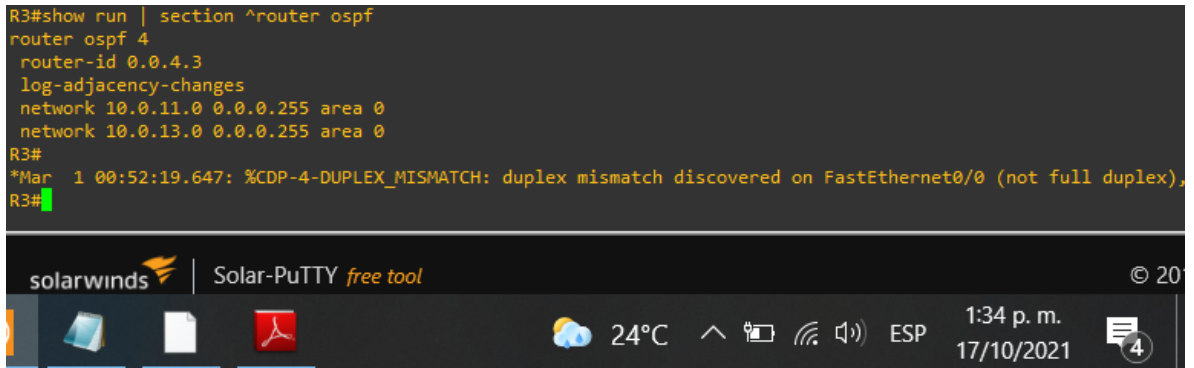
solarwinds | Solar-PuTTY free tool © 20

24°C 1:33 p. m. 17/10/2021

**R3:** show run | section ^router ospf

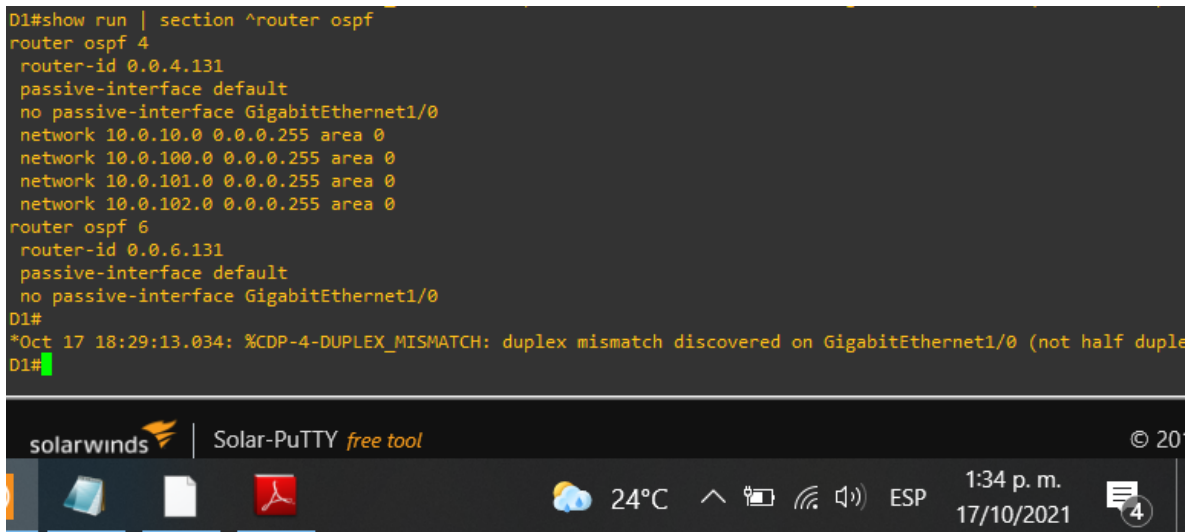


```
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  log-adjacency-changes
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
R3#
*Mar 1 00:52:19.647: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/0 (not full duplex),
R3#
```



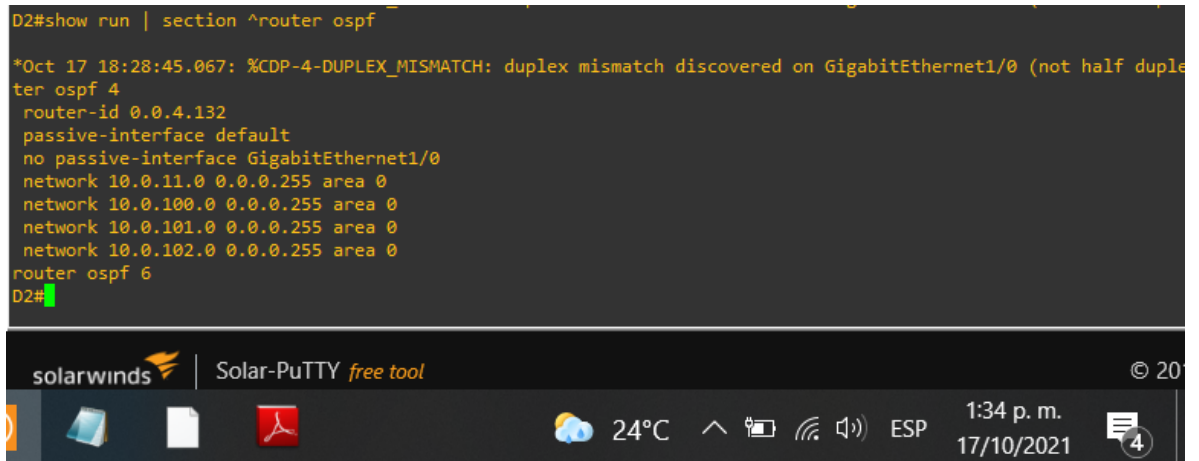
**D1: show run | section ^router ospf**

```
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  passive-interface default
  no passive-interface GigabitEthernet1/0
  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 GigabitEthernet1/0
D1#
*Oct 17 18:29:13.034: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/0 (not half duplex),
D1#
```



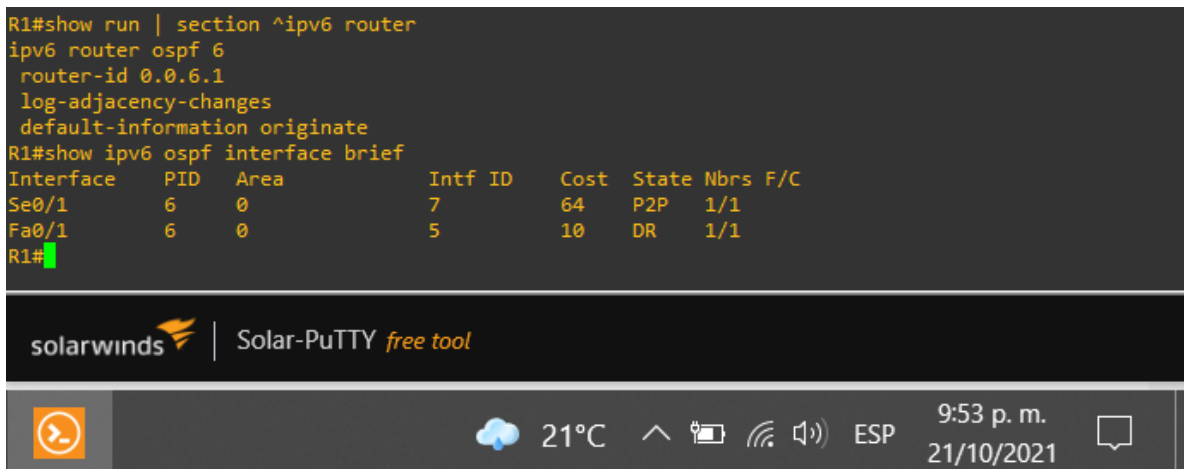
**D2: show run | section ^router ospf**

```
D2#show run | section ^router ospf
*Oct 17 18:28:45.067: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/0 (not half duplex)
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface GigabitEthernet1/0
  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
router ospf 6
D2#
```



**R1: *show run | section ^ipv6 router - show ipv6 ospf interface brief*, verificar sección y OSPF de IPV6.**

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  log-adjacency-changes
  default-information originate
R1#show ipv6 ospf interface brief
Interface    PID  Area    Intf ID    Cost  State Nbrs F/C
Se0/1        6    0        7           64   P2P   1/1
Fa0/1        6    0        5           10   DR    1/1
R1#
```



**R3: *show run | section ^ipv6 router - show ipv6 ospf interface brief*, verificar sección y OSPF de IPV6.**

```

R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
  log-adjacency-changes
R3#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Se0/1     6    0         7        64   P2P   1/1
Fa0/0     6    0         4        10   DR    0/0
R3#

```

**D1: *show run | section ^ipv6 router - show ipv6 ospf interface brief*, verificar sección y OSPF de IPV6.**

```

D1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/0
D1#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Vl102     6    0         23        1   WAIT  0/0
Vl101     6    0         22        1   WAIT  0/0
Vl100     6    0         21        1   WAIT  0/0
Et1/0     6    0         20        10   BDR   1/1
D1#
*Oct 22 03:03:50.751: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not fu
D1#

```

**D2: *show run | section ^ipv6 router - show ipv6 ospf interface brief*, verificar sección y OSPF de IPV6.**

```

D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet1/0
D2#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Vl102     6   0         23       1    DR    0/0
Vl101     6   0         22       1    DR    0/0
Vl100     6   0         21       1    DR    0/0
Et1/0     6   0         20       10   BDR   1/1
D2#
*Oct 22 02:57:54.536: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/2 (not full)
D2#

```

solarwinds | Solar-PuTTY free tool

21°C 9:57 p.m. 21/10/2021

**R2: show run | section bgp - show run | include route, Verifico secciones de BGP.**

```

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
  no neighbor 2001:DB8:200::1 activate
  neighbor 209.165.200.225 activate
  no auto-summary
  no synchronization
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  exit-address-family
  !
  address-family ipv6
  neighbor 2001:DB8:200::1 activate
  network ::/0
  network 2001:DB8:2222::/128
  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#

```

solarwinds | Solar-PuTTY free tool © 20

25°C 1:42 p.m. 17/10/2021 4

**R1: show run | section bgp - show run | include route, Verifico secciones de BGP.**

```
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
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
    no auto-summary
    no synchronization
    network 10.0.0.0
  exit-address-family
  !
  address-family ipv6
    neighbor 2001:DB8:200::2 activate
    network 2001:DB8:100::/48
  exit-address-family
R1#show run | include route
router ospf 4
  router-id 0.0.4.1
router bgp 300
  bgp router-id 1.1.1.1
ip route 10.0.0.0 255.0.0.0 Null0
ipv6 route 2001:DB8:100::/48 Null0
ipv6 router ospf 6
  router-id 0.0.6.1
R1#
```

**Tablas de enrutamiento:**

**R1: show ip route | include O/B, se verifica tablas de enrutamiento del R1.**

```

R1#show ip route | include O|B
Codes: 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
B      2.2.2.2 [20/0] via 209.165.200.226, 01:01:52
O      10.0.11.0/24 [110/74] via 10.0.13.3, 01:02:32, Serial0/1
O      10.0.102.0/24 [110/11] via 10.0.10.2, 00:47:21, FastEthernet0/1
O      10.0.100.0/24 [110/11] via 10.0.10.2, 00:47:31, FastEthernet0/1
O      10.0.101.0/24 [110/11] via 10.0.10.2, 00:47:21, FastEthernet0/1
B*    0.0.0.0/0 [20/0] via 209.165.200.226, 01:01:52
R1#

```

También se usa el comando *show ipv6 route* para verificar el enrutamiento

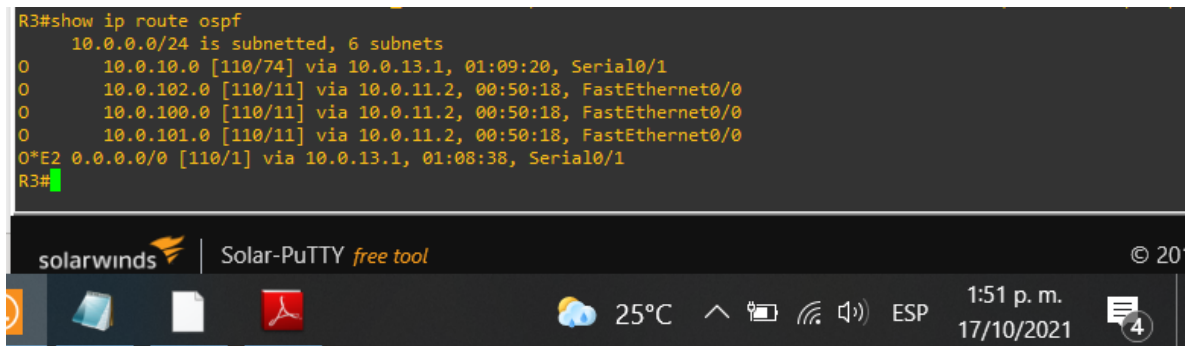
```

R1#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
B     ::/0 [20/0]
      via FE80::2:1, FastEthernet0/0
S     2001:DB8:100::/48 [1/0]
      via ::, Null0
C     2001:DB8:100:1010::/64 [0/0]
      via ::, FastEthernet0/1
L     2001:DB8:100:1010::1/128 [0/0]
      via ::, FastEthernet0/1
O     2001:DB8:100:1011::/64 [110/74]
      via FE80::3:3, Serial0/1
C     2001:DB8:100:1013::/64 [0/0]
      via ::, Serial0/1
L     2001:DB8:100:1013::1/128 [0/0]
      via ::, Serial0/1
C     2001:DB8:200::/64 [0/0]
      via ::, FastEthernet0/0
L     2001:DB8:200::1/128 [0/0]
      via ::, FastEthernet0/0
L     FF00::/8 [0/0]
      via ::, Null0
R1#

```

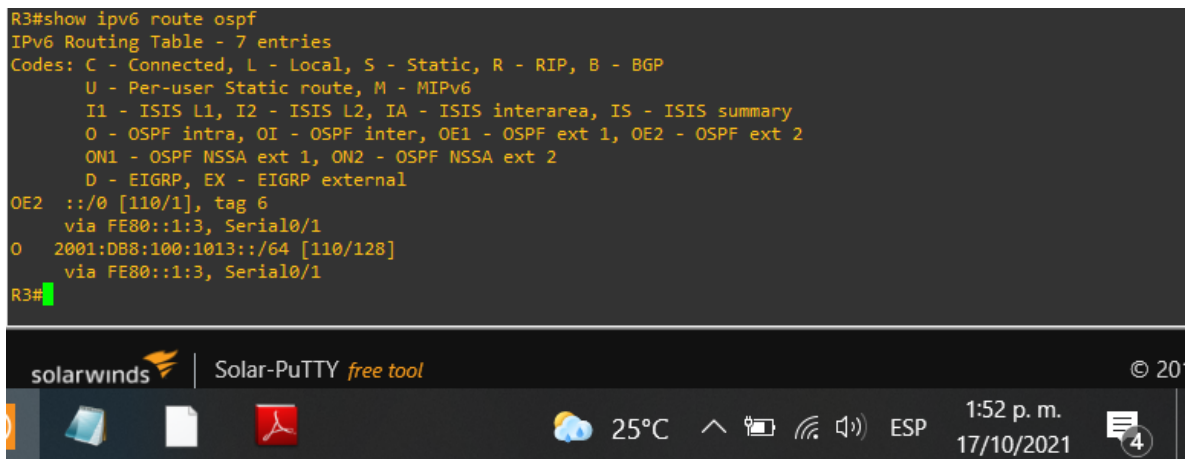
R3: *show ip route ospf*, para verificar que OSPF en IPV4 su funcionamiento.

```
R3#show ip route ospf
 10.0.0.0/24 is subnetted, 6 subnets
O    10.0.10.0 [110/74] via 10.0.13.1, 01:09:20, Serial0/1
O    10.0.102.0 [110/11] via 10.0.11.2, 00:50:18, FastEthernet0/0
O    10.0.100.0 [110/11] via 10.0.11.2, 00:50:18, FastEthernet0/0
O    10.0.101.0 [110/11] via 10.0.11.2, 00:50:18, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 01:08:38, Serial0/1
R3#
```



**R3: *show ipv6 route ospf*, para verificar que OSPF en IPV6 su funcionamiento.**

```
R3#show ipv6 route ospf
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
OE2  ::/0 [110/1], tag 6
    via FE80::1:3, Serial0/1
O   2001:DB8:100:1013::/64 [110/128]
    via FE80::1:3, Serial0/1
R3#
```



**Parte 4: Revisar configuración de redundancia de primer salto.**

## D1: Verificación de la sesión de 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#
```

solarwinds | Solar-PuTTY *free tool*

9:06 a. m. 10/11/2021

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

solarwinds | Solar-PuTTY *free tool*

9:12 a. m. 10/11/2021

## D2: Verificación de la sesión de 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#
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl100	104	100	P	Init	unknown	unknown	10.0.100.254
Vl100	106	100	P	Init	unknown	unknown	FE80::5:73FF:FEA0:6A
Vl101	114	150	P	Init	unknown	unknown	10.0.101.254
Vl101	116	150	P	Init	unknown	unknown	FE80::5:73FF:FEA0:74
Vl102	124	100	P	Standby	10.0.102.1	local	10.0.102.254
Vl102	126	100	P	Standby	FE80::D1:4	local	FE80::5:73FF:FEA0:7E

```
D2#
```

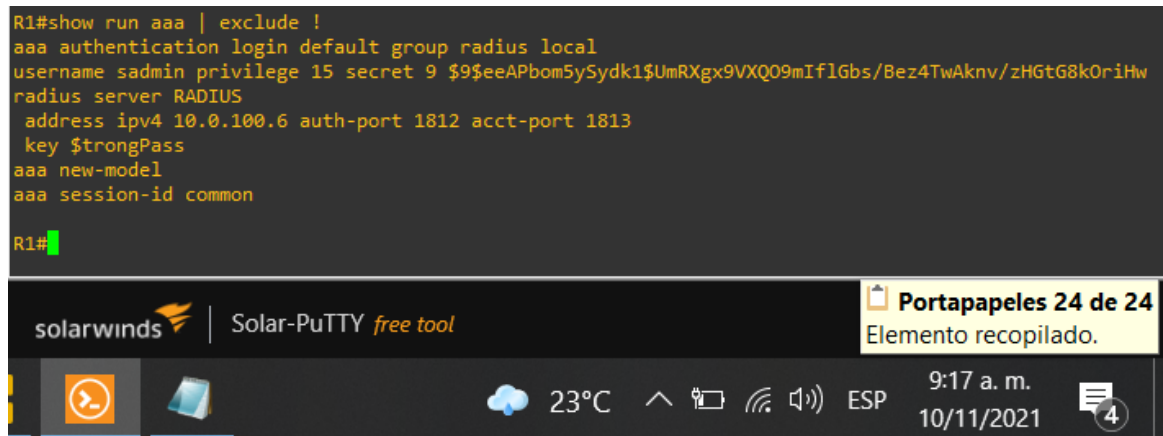
**Parte 5:** Revisa configuración de seguridad.

**En R1:** Verificación de seguridad en SCRYPT.

```
R1#show run | include secret
enable secret 9 $9$aPvg16Wqd9I9Cn$QwMN5sk.dDIJ01eJ2qIe7XYrdRMeqmIyK1PFKra5Edk
username sadmin privilege 15 secret 9 $9$eeAPbom5ySydk1$UmRXgx9VXQ09mIf1Gbs/Bez4TwAknv/zHGtG8kOriHw
R1#
```

## En R1: Verificación de seguridad en Radius y AAA.

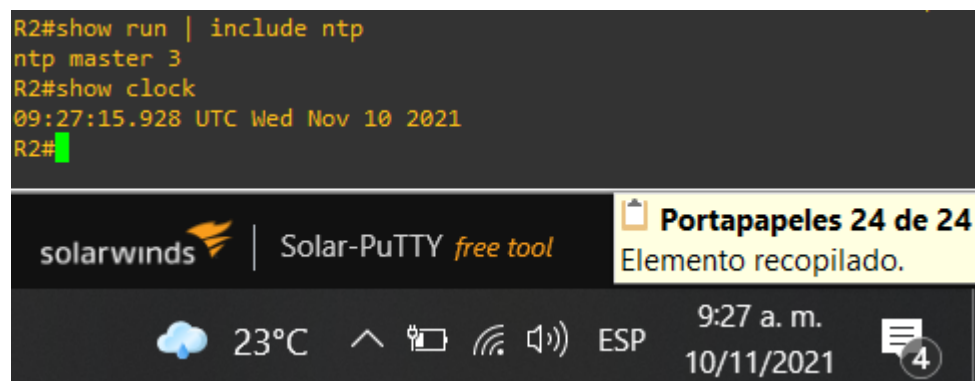
```
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$eeAPbom5ySydk1$UmRXgx9VXQ09mIf1Gbs/Bez4TwAknv/zHGtG8k0riHw
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
R1#
```



## Parte 6: Revisar configuración de función de administración de red.

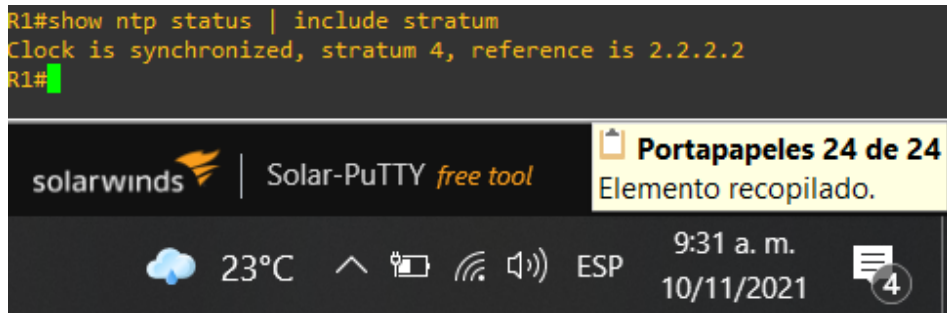
### R2: Verificación de NTP Máster.

```
R2#show run | include ntp
ntp master 3
R2#show clock
09:27:15.928 UTC Wed Nov 10 2021
R2#
```



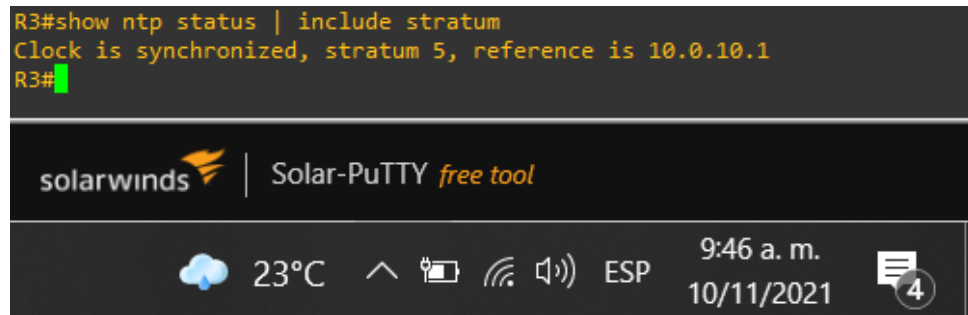
### R1: Verificación de sincronización de reloj con R2.

```
R1#show ntp status | include stratum
Clock is synchronized, stratum 4, reference is 2.2.2.2
R1#
```

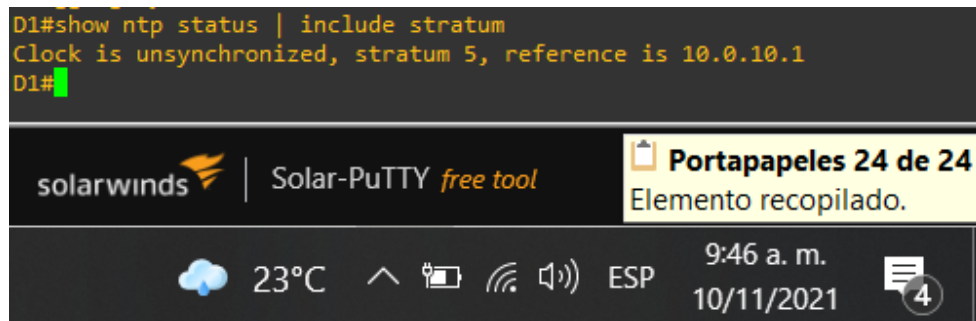


**R3, D1,: Verificación de sincronización de reloj R1.**

```
R3#show ntp status | include stratum
Clock is synchronized, stratum 5, reference is 10.0.10.1
R3#
```



```
D1#show ntp status | include stratum
Clock is unsynchronized, stratum 5, reference is 10.0.10.1
D1#
```



**D2: Verificación de sincronización de reloj R3.**

```
D2#show ntp status | include stratum
Clock is synchronized, stratum 6, reference is 10.0.11.1
D2#
```

solarwinds | Solar-PuTTY *free tool* **Portapapeles 24 de 24**  
Elemento recopilado.

25°C ^ [wifi] [speaker] ESP 11:08 a. m.  
10/11/2021 [4]

R1, R3, D1, D2 y A1: Verificación Syslogs enviado al PC1.

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

solarwinds | Solar-PuTTY *free tool* **Portapapeles 24 de 24**  
Elemento recopilado.

23°C ^ [wifi] [speaker] ESP 9:33 a. m.  
10/11/2021 [4]

```
R3#show run | include logging
cts logging verbose
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
R3#
```

solarwinds | Solar-PuTTY *free tool* **Portapapeles 24 de 24**  
Elemento recopilado.

23°C ^ [wifi] [speaker] ESP 9:36 a. m.  
10/11/2021 [4]

```
D1#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
D1#
```

solarwinds | Solar-PuTTY *free tool*

Portapapeles 24 de 24  
Elemento recopilado.

23°C ^ [Battery] [Wi-Fi] [Speaker] ESP 9:39 a. m.  
10/11/2021 [Messages] 4

```
D2#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
D2#
```

solarwinds | Solar-PuTTY *free tool*

23°C ^ [Battery] [Wi-Fi] [Speaker] ESP 9:41 a. m.  
10/11/2021 [Messages] 4

```
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 host 10.0.100.2
logging synchronous
logging synchronous
A1#
```

solarwinds | Solar-PuTTY *free tool*

23°C ^ [Battery] [Wi-Fi] [Speaker] ESP 9:42 a. m.  
10/11/2021 [Messages] 4