

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RONNY SAVIER PAEZ PINILLA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RONNY SAVIER PAEZ PINILLA

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

ZIPAQUIRÁ, 29 de Noviembre de 2021

## AGRADECIMIENTOS

Agradezco a Dios primeramente, a mis compañeros y tutores del curso diplomado de profundización cisco CCNP por la entrega y el compromiso, lo cual me ayudo a desarrollar las actividades propuestas sobre todo en los trabajos colaborativos, al tutor por compartirnos sus experiencias y la información necesaria para el entendimiento de las temáticas del curso y los ejercicios, de igual manera por los espacios brindados a través de las webconferencias, herramienta fundamental para que nosotros los estudiantes pudiéramos despejar dudas importantes acerca de los temas y actividades a desarrollar para poder culminar de manera satisfactoria este proyecto final de grado.

En general a mi familia por el apoyo incondicional y entendimiento sobre en esta modalidad de estudio la cual requiere de un gran esfuerzo, dedicación y sacrificio sobre todo cuando se estudia y se trabaja al mismo tiempo.

## CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN .....	12
DESARROLLO .....	13
Paso 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.....	13
Paso 2: Configurar la capa 2 de la red y el soporte de Host.....	26
Paso 3: Configurar los protocolos de enrutamiento .....	44
Paso 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)...	65
Paso 5: Seguridad .....	71
Paso 6: Configure las funciones de Administración de Red .....	78
CONCLUSIONES .....	92
BIBLIOGRAFÍA.....	93

## LISTA DE TABLAS

Tabla 1 Direccionamiento de los Routers .....	14
Tabla 2 Enrutamiento de los Switches .....	17
Tabla 3 Enrutamiento de los PC's.....	24

## LISTA DE FIGURAS

Figura 1 Topología de red.....	13
Figura 2 Simulación Topología red en GNS3.....	14
Figura 3 Configuración PC1 .....	25
Figura 4 Configuración PC4.....	26
Figura 5 Configuración de interfaces troncales D1 .....	29
Figura 6 Configuración de interfaces troncales D2 .....	29
Figura 7 Configuración de interfaces troncales A1 .....	30
Figura 8 Configuración de los puentes raíz RSTP en D1.....	32
Figura 9 Configuración de los puentes raíz RSTP en D2.....	32
Figura 10 Configuración de los EtherChannels LACP en D1 .....	36
Figura 11 Configuración de los EtherChannels LACP en D2.....	37
Figura 12 Configuración de los EtherChannels LACP en A1 .....	37
Figura 13 Configuración dhcp PC2 .....	40
Figura 14 Configuración dhcp PC3 .....	41
Figura 15 Ping de PC1.....	42
Figura 16 Ping de PC2.....	43
Figura 17 Ping de PC3.....	43
Figura 18 Ping de PC4.....	44
Figura 19 Configuración ospf 4 en R1.....	46
Figura 20 Configuración Process ID 4 R3.....	46
Figura 21 Configuración Process ID 4 D1 .....	48
Figura 22 Configuración Process ID 4 D2.....	50
Figura 23 Configuración Process ID 6 R1 .....	54
Figura 24 Configuración Process ID 6 R3.....	55
Figura 25 Configuración Process ID 6 D1 .....	57
Figura 26 Configuración Process ID 6 D2.....	59
Figura 27 Configuración bgp ASN 500 en R2 .....	61
Figura 28 Configuración bgp relación vecino R2 .....	62
Figura 29 Configuración bgp ASN 300 en R1 .....	63
Figura 30 Configuración bgp relación vecino R1 .....	65

Figura 31 Configuración Redundancia del Primer Salto D1 .....	71
Figura 32 Configuración Redundancia del Primer Salto D2.....	71
Figura 33 Configuraciones de Seguridad en R1 .....	74
Figura 34 Configuraciones de Seguridad en R2 .....	74
Figura 35 Configuraciones de Seguridad en R3 .....	74
Figura 36 Configuraciones de Seguridad en D1 .....	75
Figura 37 Configuraciones de Seguridad en D2 .....	75
Figura 38 Configuraciones de Seguridad en A1 .....	75
Figura 39 Verificación el servicio AAA en R1 .....	76
Figura 40 Verificación el servicio AAA en R3.....	76
Figura 41 Verificación el servicio AAA en D1 .....	77
Figura 42 Verificación el servicio AAA en D2.....	77
Figura 43 Verificación el servicio AAA en A1 .....	78
Figura 44 Configuración reloj local hora UTC R1.....	79
Figura 45 Configuración reloj local hora UTC R2.....	79
Figura 46 Configuración reloj local hora UTC R3.....	80
Figura 47 Configuración reloj local hora UTC D1.....	81
Figura 48 Configuración reloj local hora UTC D2.....	81
Figura 49 Configuración reloj local hora UTC A1 .....	82
Figura 50 Configuración NTP maestro 3.....	82
Figura 51 Configuración NTP R1 .....	83
Figura 52 Configuración NTP R3.....	83
Figura 53 Configuración NTP D1 .....	84
Figura 54 Configuración NTP A1 .....	84
Figura 55 Configuración NTP D2 .....	84
Figura 56 Configuración SNMPv2c en R1 .....	86
Figura 57 Configuración SNMPv2c en R3 .....	87
Figura 58 Configuración SNMPv2c en D1 .....	88
Figura 59 Configuración SNMPv2c en D2 .....	89
Figura 60 Configuración SNMPv2c en A1.....	90

## GLOSARIO

**OSPF:** Open Shortest Path First, Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol

**RSTP:** Rapid Spanning Tree Protocol es un protocolo de red de la segunda capa OSI, que gestiona enlaces redundantes. Especificado en IEEE 802.1w.

**VLAN:** Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física.

**SLAAC:** Es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6.

**ENLACE TRONCAL:** Es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red.

## RESUMEN

En el presente trabajo del diplomado de profundización CCNP Cisco, se desarrolla el escenario propuesto en la prueba de habilidades, con el fin de aplicar los conocimientos aprendidos a lo largo del curso, configurando cada uno de los equipos dispuestos en la topología de la red, de acuerdo a los requerimientos solicitados, aplicando protocolos de enrutamiento OSPF, BGP e interfaz virtual Loopback 0, de igual manera protocolos de seguridad SNMP, Syslog, así como también protocolo NTP para tiempos de red, con el fin de hacer la red convergente y funcional.

La práctica se realiza en el software GNS3, el cual nos permite tener un entorno con equipos similares a los reales gracias a los complementos como los IOS de las imágenes Cisco y máquina virtual ayudando a solventar los recursos de equipo y memoria, se crea la red e interconectado cada uno de los equipos como Routers, Switches y PC, obteniendo simulaciones que permiten evidenciar el funcionamiento de los protocolos de enrutamiento previamente configurados en la topología de red, teniendo en cuenta cada uno de los pasos de la guía.

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

## ABSTRACT

In the present work of the Cisco CCNP in-depth diplomated, the scenario proposed in the skills test is developed, in order to apply the knowledge learned throughout the course, configuring each of the equipment arranged in the topology of the network of according to the requested requirements, applying protocols of routing OSPF, BGP and Loopback 0 virtual interface , as well as security protocols SNMP, Syslog, as well as NTP protocol for network times, in order to make the network convergent and functional.

The practice is carried out in the GNS3 software, which allows us to have an environment with equipment similar to the real ones thanks to accessories such as the IOS of the Cisco images and the virtual machine helping to manage the resources equipment and memory. The network is created by connecting each of the equipment such as Routers, Switches and PCs, obtaining simulations that allow to demonstrate the operation of the routing protocols previously configured in the network topology, taking into account each of the steps in the guide.

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

## INTRODUCCIÓN

En el siguiente documento se desarrolla la prueba de habilidades con base en un caso de estudio propuesto para culminar el diplomado de profundización Cisco CCNP proyecto final como opción de grado de Ingeniería electrónica, adoptando la estrategia ABE (Aprendizaje Basada en Entornos), la cual nos permite enriquecer los conocimientos en redes para el uso plataformas de comunicación equipadas con switches, routers, PC's, con protocolos de enrutamiento y configuraciones de VLANs, enlaces troncales, adquiriendo bases necesarias para la identificación y solución de posibles situaciones problemáticas en casos de conmutación y enrutamiento.

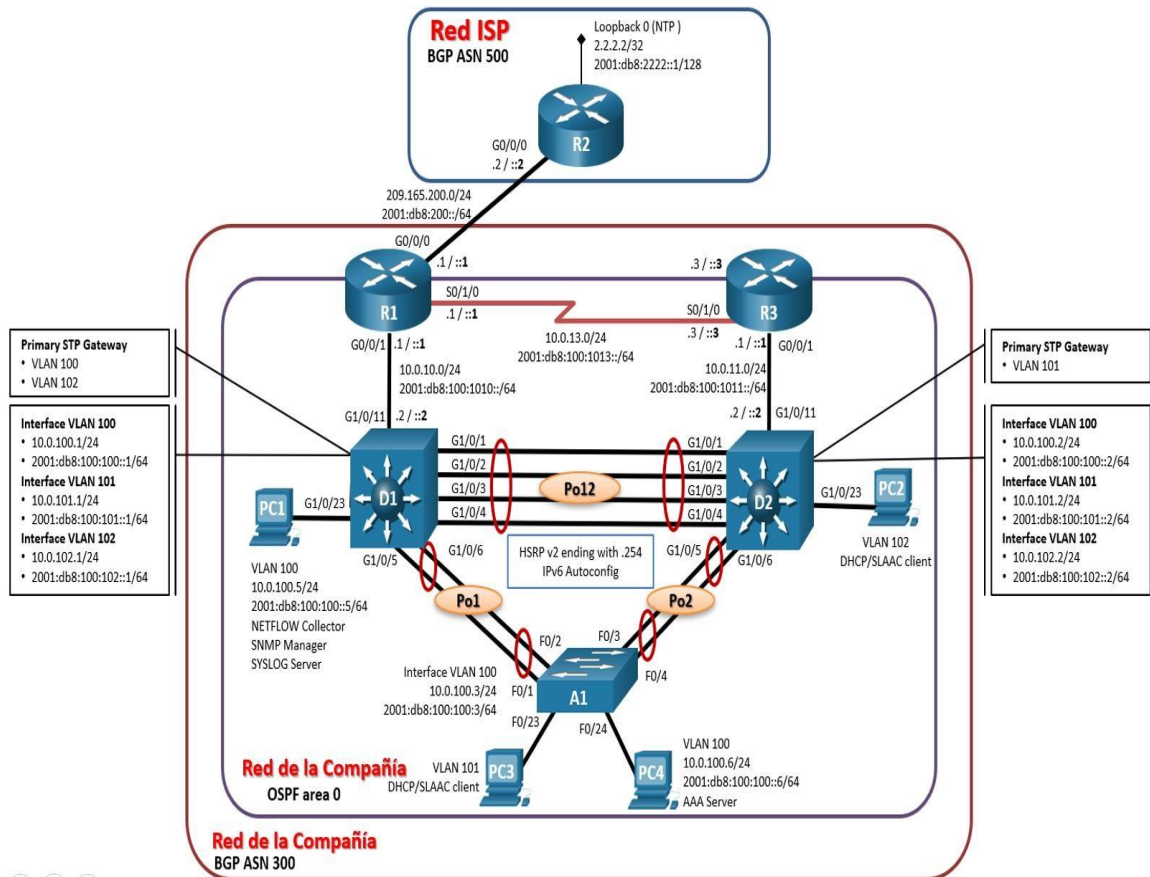
El documento está compuesto por seis partes la primera: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces, la segunda: Configurar la capa 2 de la red y el soporte de Host, la tercera: Configurar los protocolos de enrutamiento, la cuarta: Configurar la redundancia del primer salto, la quinta: Configurar la seguridad, sexta y última Configurar las características de administración de red; el desarrollo de esta prueba de habilidades tiene como fin que en la red haya accesibilidad completa de un extremo a otro, lo que quiere decir que los pings serán éxitos entre un equipo y otro.

Por último, el desarrollo de cada paso estará debidamente documentado y soportado por cada uno de las evidencias respectivas con imágenes de la ejecución de los comandos: `show interfaces trunk`, `show run | include spanning-tree`, `show etherchannel`, `show ip`, `show run | section ^router ospf`, `show run | section ^ipv6`, `router`, `show run | section router bgp`, `show run | include route`, `show standby brief`, `show run aaa | exclude !`; como los más relevantes de los procesos de enrutamiento y configuración.

## DESARROLLO

### ESCENARIO PROPUESTO

Figura 1 Topología de red

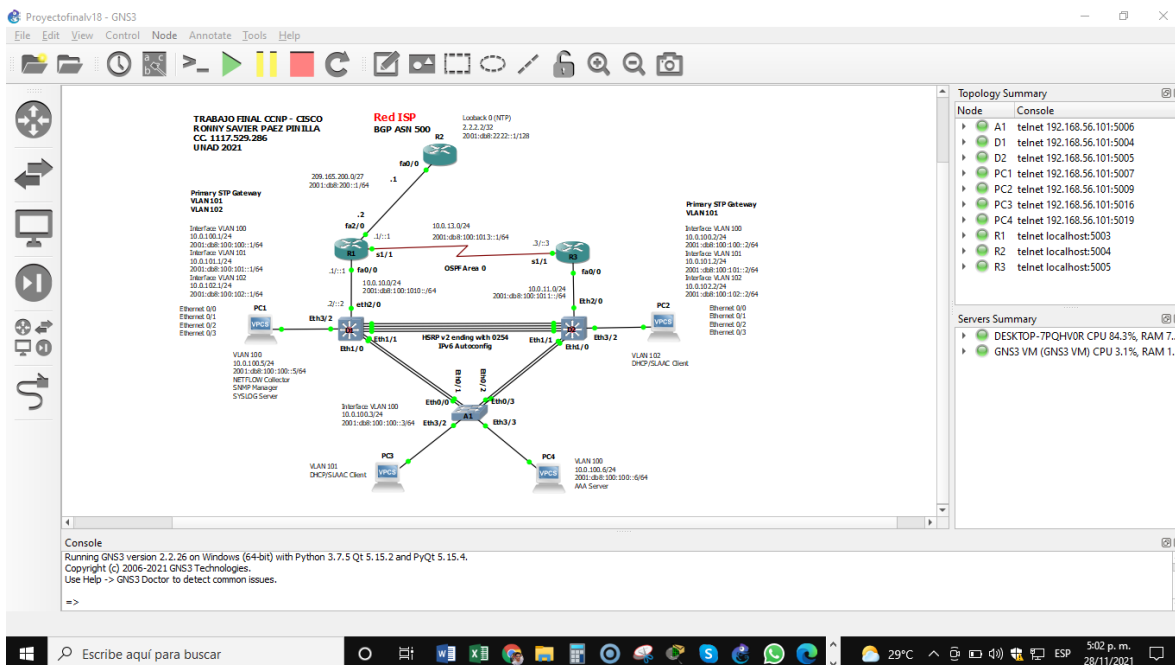


Paso 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

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 Simulación Topología red en GNS3



Configurar los parámetros básicos para cada dispositivo.

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

1.1 Se aplica las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2 y R3, switches D1, D2 y A1, PC1, PC2, PC3 y PC4; según el diagrama. No se asigna password en los routers. Se configuran las interfaces con las direcciones que se muestran en la topología de red.

Tabla 1 Direccionamiento de los Routers

Routers	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	Fa2/0	209.165.200.2/27	2001:db8:200::1/64	fe80::1:1
	Fa0/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S1/1	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3

R2	Fa0/0	209.165.200.1/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	Fa0/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S1/1	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3

**NOTA:** Cabe resaltar que la tabla de direccionamiento tuvo algunos cambios con respecto a la planteada en el escenario, por un lado, las interfaces de Gigabit propuestas en los routers R1, R2, R3 se cambiaron por Fastethernet y el puerto serial cambio, esto a razón de que los equipos no tienen las mismas características en los puertos de comunicación de la topología y las direcciones IPv4 en R1 y R2 también se cambian para tener una misma concordancia

### Router R1

```

R1(config)#hostname R1                               Asigno nombre al router
R1(config)#ipv6 unicast-routing                       Enrutamiento IPv6
R1(config)#no ip domain lookup                       Deshabilita la búsqueda DNS
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)# exec-timeout 0 0
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#interface fa2/0                            Ingreso a la interfaz fa2/0
R1(config-if)# ip address 209.165.200.2 255.255.255.224
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# ipv6 address 2001:db8:200::1/64
R1(config-if)# no shutdown                            Asignación de dirección ipv6
R1(config-if)# exit                                  Salida de la interfaz
R1(config)#interface fa0/0                            Ingreso a la interfaz fa0/0
R1(config-if)# ip address 10.0.10.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1:2 link-local
R1(config-if)# ipv6 address 2001:db8:100:1010::1/64

```

R1(config-if)# no shutdown	Enrutamiento IPv6
R1(config-if)# exit	Salida de la interfaz
R1(config)#interface s1/1	Ingreso a la interfaz s1/1
R1(config-if)# ip address 10.0.13.1 255.255.255.0	
R1(config-if)# ipv6 address fe80::1:3 link-local	
R1(config-if)# ipv6 address 2001:db8:100:1013::1/64	
R1(config-if)# no shutdown	Enrutamiento IPv6
R1(config-if)# exit	Salida de la interfaz

## Router R2

R2(config)#hostname R2	Asigno nombre al router
R2(config)#ipv6 unicast-routing	Enrutamiento IPv6
R2(config)#no ip domain lookup	Deshabilita la búsqueda DNS
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	
R2(config)#line con 0	
R2(config-line)# exec-timeout 0 0	
R2(config-line)# logging synchronous	
R2(config-line)# exit	
R2(config)#interface fa0/0	Ingreso a la interfaz fa2/0
R2(config-if)# ip address 209.165.200.1 255.255.255.224	
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	Asignación de dirección IPv6
R2(config-if)# exit	Salida de la interfaz
R2(config)#interface Loopback 0	Ingreso a la interfaz virtual
R2(config-if)# ip address 2.2.2.2 255.255.255.255	
R2(config-if)# ipv6 address fe80::2:3 link-local	
R2(config-if)# ipv6 address 2001:db8:2222::1/128	
R2(config-if)# no shutdown	Enrutamiento IPv6
R2(config-if)# exit	Salida de la interfaz

## Router R3

R3(config)#hostname R3	Asigno nombre al router
R3(config)#ipv6 unicast-routing	Enrutamiento IPv6
R3(config)#no ip domain lookup	Deshabilita la búsqueda DNS
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	
R3(config)#line con 0	
R3(config-line)# exec-timeout 0 0	
R3(config-line)# logging synchronous	
R3(config-line)# exit	
R3(config)#interface fa0/0	Ingreso a la interfaz fa0/0
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	Enrutamiento IPv6
R3(config-if)# exit	Salida de la interfaz
R3(config)#interface s1/1	Ingreso a la interfaz s1/1
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	Enrutamiento IPv6
R3(config-if)# exit	Salida de la interfaz

*Tabla 2 Enrutamiento de los Switches*

Switch	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
D1	Et2/0	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	Et2/0	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

**NOTA:** Cabe resaltar que la tabla de direccionamiento tuvo algunos cambios con respecto a la planteada en el escenario, por un lado, las interfaces de Gigabit propuestas en los switches D1, D2 y A1 se cambiaron por Ethernet respectivamente, debido a que los equipos no tienen las mismas características en los puertos de comunicación de la topología.

### Switch D1

```

D1(config)#hostname D1                               Asigno nombre al switch
D1(config)#ip routing
D1(config)#ipv6 unicast-routing                       Enrutamiento IPv6
D1(config)#no ip domain lookup                       Deshabilita la búsqueda DNS
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)# exec-timeout 0 0
D1(config-line)# logging synchronous
D1(config-line)# exit
D1(config)#vlan 100                                  Creación de vlan 100
D1(config-vlan)# name Management
D1(config-vlan)# exit
D1(config)#vlan 101                                  Creación de vlan 101
D1(config-vlan)# name UserGroupA
D1(config-vlan)# exit
D1(config)#vlan 102                                  Creación de vlan 102
D1(config-vlan)# name UserGroupB

```

```

D1(config-vlan)# exit
D1(config)#vlan 999                                Creación de vlan 999
D1(config-vlan)# name NATIVE                       Creación de vlan nativa
D1(config-vlan)# exit
D1(config)#interface e2/0                          Ingreso a la interfaz Eth2/0
D1(config-if)# no switchport                       Se enciende la interfaz
D1(config-if)# ip address 10.0.10.2 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:1 link-local
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64
D1(config-if)# no shutdown
D1(config-if)# exit
D1(config)#interface vlan 100                      Se asigna add ip a la vlan 100
D1(config-if)# ip address 10.0.100.1 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:2 link-local
D1(config-if)# ipv6 address 2001:db8:100:100::1/64
D1(config-if)# no shutdown
D1(config-if)# exit
D1(config)#interface vlan 101                      Se asigna add ip a la vlan 101
D1(config-if)# ip address 10.0.101.1 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:3 link-local
D1(config-if)# ipv6 address 2001:db8:100:101::1/64
D1(config-if)# no shutdown
D1(config-if)# exit
D1(config)#interface vlan 102                      Se asigna add ip a la 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
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109

```

```

D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)# network 10.0.101.0 255.255.255.0
D1(dhcp-config)# default-router 10.0.101.254
D1(dhcp-config)# exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)# network 10.0.102.0 255.255.255.0
D1(dhcp-config)# default-router 10.0.102.254
D1(dhcp-config)# exit
D1(config)#interface range e1/2-3, e2/1-3, e3/0-1, e3/3
D1(config-if-range)#shutdown                               Apaga las interfaces libres
D1(config-if-range)#exit

```

## Switche D2

```

D2(config)#hostname D2                                     Asigno nombre al switch
D2(config)#ip routing
D2(config)#ipv6 unicast-routing                           Enrutamiento IPv6
D2(config)#no ip domain lookup                            Deshabilita la búsqueda DNS
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)# exec-timeout 0 0
D2(config-line)# logging synchronous
D2(config-line)# exit
D2(config)#vlan 100                                       Creación de vlan 100
D2(config-vlan)# name Management
D2(config-vlan)# exit
D2(config)#vlan 101                                       Creación de vlan 101
D2(config-vlan)# name UserGroupA
D2(config-vlan)# exit
D2(config)#vlan 102                                       Creación de vlan 102
D2(config-vlan)# name UserGroupB

```

D2(config-vlan)# exit	
D2(config)#vlan 999	Creación de vlan 999
D2(config-vlan)# name NATIVE	Creación de vlan nativa
D2(config-vlan)# exit	
D2(config)#interface e2/0	Ingreso a la interfaz Eth2/0
D2(config-if)# no switchport	Se enciende la interfaz
D2(config-if)# ip address 10.0.11.2 255.255.255.0	
D2(config-if)# ipv6 address fe80::d1:1 link-local	
D2(config-if)# ipv6 address 2001:db8:100:1011::2/64	
D2(config-if)# no shutdown	
D2(config-if)# exit	
D2(config)#interface vlan 100	Asigna add ip a la vlan 100
D2(config-if)# ip address 10.0.100.2 255.255.255.0	
D2(config-if)# ipv6 address fe80::d2:2 link-local	
D2(config-if)# ipv6 address 2001:db8:100:100::2/64	
D2(config-if)# no shutdown	
D2(config-if)# exit	
D2(config)#interface vlan 101	Asigna add ip a la 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	Asigna add ip a la vlan 102
D2(config-if)# ip address 10.0.102.2 255.255.255.0	
D2(config-if)# ipv6 address fe80::d2:4 link-local	
D2(config-if)# ipv6 address 2001:db8:100:102::2/64	
D2(config-if)# no shutdown	
D2(config-if)# exit	
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209	
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254	
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209	

```

D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)# network 10.0.101.0 255.255.255.0
D2(dhcp-config)# default-router 10.0.101.254
D2(dhcp-config)# exit
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 e1/2-3, e2/1-3, e3/0-1, e3/3
D2(config-if-range)# shutdown                               Apaga las interfaces libres
D2(config-if-range)# exit

```

### Switch A1

```

A1(config)#hostname A1                                     Asigno nombre al switch
A1(config)#no ip domain lookup                            Deshabilita la búsqueda DNS
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)# exec-timeout 0 0
A1(config-line)# logging synchronous
A1(config-line)# exit
A1(config)#vlan 100                                       Creación de vlan 100
A1(config-vlan)# name Management
A1(config-vlan)# exit
A1(config)#vlan 101                                       Creación de vlan 101
A1(config-vlan)# name UserGroupA
A1(config-vlan)# exit
A1(config)#vlan 102                                       Creación de vlan 102
A1(config-vlan)# name UserGroupB
A1(config-vlan)# exit
A1(config)#vlan 999                                       Creación de vlan 999

```

```

A1(config-vlan)# name NATIVE
A1(config-vlan)# exit
A1(config)#interface vlan 100
A1(config-if)# ip address 10.0.100.3 255.255.255.0
A1(config-if)# ipv6 address fe80::a1:1 link-local
A1(config-if)# ipv6 address 2001:db8:100:100::3/64
A1(config-if)# no shutdown
A1(config-if)# exit
A1(config)#interface range e1/0-3, e2/0-3, e3/0-1
A1(config-if-range)# shutdown
A1(config-if-range)# exit

```

Creación de vlan nativa

Apagan las interfaces libres

b. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.

Se realiza la copia correspondiente en cada uno de los dispositivos por medio del comando **copy running-config startup-config**

**R1**

```

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Guarda la config en el equipo

**R2**

```

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Guarda la config en el equipo

**R3**

```

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Guarda la config en el equipo

**D1**

D1#copy running-config startup-config  
 Destination filename [startup-config]?  
 Building configuration...  
 [OK]

Guarda la config en el equipo

**D2**

D2#copy running-config startup-config  
 Destination filename [startup-config]?  
 Building configuration...  
 [OK]

Guarda la config en el equipo

**A1**

A1#copy running-config startup-config  
 Destination filename [startup-config]?  
 Building configuration...  
 [OK]

Guarda la config en el equipo

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

*Tabla 3 Enrutamiento de los PC's*

<b>PC</b>	<b>Interfaz</b>	<b>Dirección IPv4</b>	<b>Dirección IPv6</b>	<b>IPv6 Link-Local</b>
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

Se realiza el direccionamiento con la ip y puerta de enlace en los PC1 y PC2 con los siguientes comandos

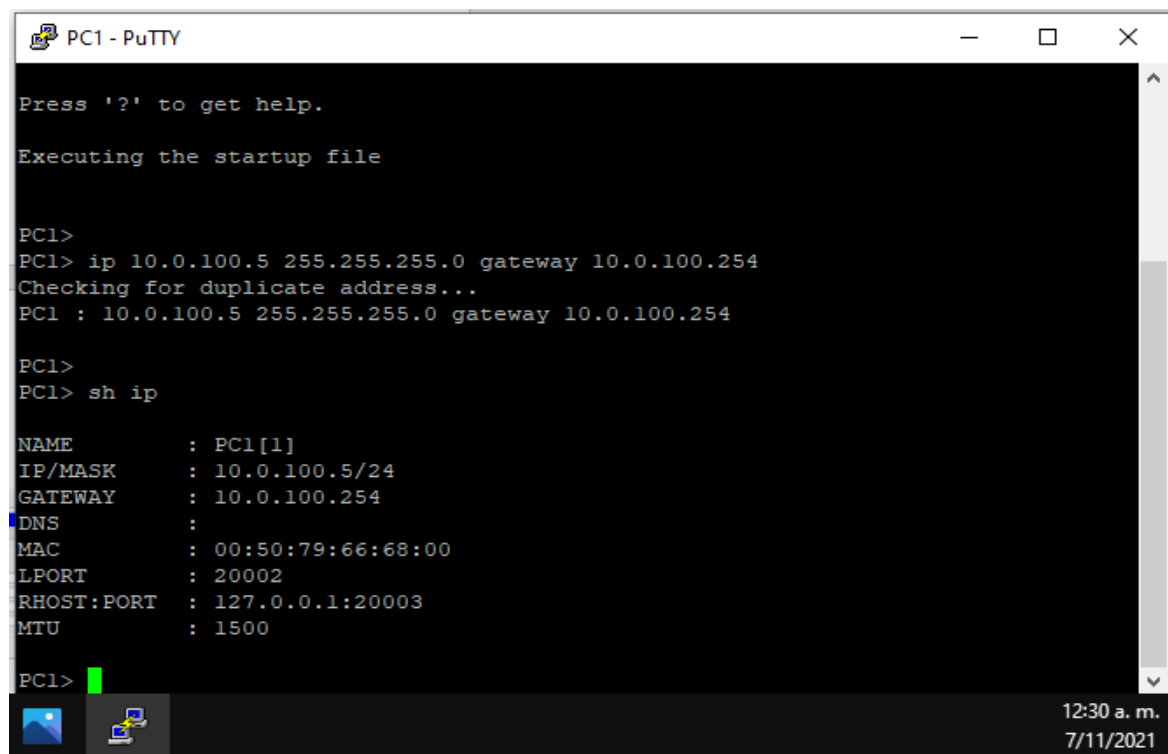
### PC1

```
PC1> ip 10.0.100.5 255.255.255.0 gateway 10.0.100.254   IP y puerta de enlace
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
```

PC1>show ip Muestra la configuración de la IP y el Gateway

En la siguiente imagen se puede ver la configuración del direccionamiento en la PC1

*Figura 3 Configuración PC1*



### PC4

```
PC4> ip 10.0.100.6 255.255.255.0 gateway 10.0.100.254
Checking for duplicate address...
```

PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4>show ip Muestra la configuración de la IP y el Gateway

En la siguiente imagen se puede ver la configuración del direccionamiento en la PC4

*Figura 4 Configuración PC4*

```
PC4 - PuTTY
PC4>
PC4>
PC4>
PC4> ip 10.0.100.6 255.255.255.0 gateway 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4>
PC4> sh ip

NAME       : PC4[1]
IP/MASK    : 10.0.100.6/24
GATEWAY    : 10.0.100.254
DNS        :
MAC        : 00:50:79:66:68:03
LPORT     : 20006
RHOST:PORT : 127.0.0.1:20007
MTU       : 1500

PC4>
```

### Paso 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 debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Habilite enlaces trunk 802.1Q entre:

- D1 and D2
- D1 and A1
- D2 and A1

En este paso se habilitan los enlaces troncales para cada uno de los enlaces de red entre los switches D1, D2 y A1 aplicando los siguientes comandos y mediante el comando rango se accede al modo de configuración global de las interfaces

### **Configuración interfaces troncales D1 y D2**

Con los siguientes comandos se configuran los enlaces troncales entre los switches D1 y D2

#### **Configuración en D1**

```
D1(config)#int range e0/0-3          Ingreso a las interfaces Eth0-3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk    Denomina las interfaces troncales
D1(config-if-range)#exite
D1(config)#exit
```

#### **Configuración en D2**

```
D2(config)#int range e0/0-3          Ingreso a las interfaces Eth0-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk    Denomina las interfaces troncales
D2(config-if-range)#exit
D2(config)#
```

### **Configuración interfaces troncales D1 y A1**

Con los siguientes comandos se configuran los enlaces troncales entre los switches D1 y A1

#### **Configuración en D1**

```
D1(config)#int range e1/0-1          Ingreso a las interfaces Eth0-1
D1(config-if-range)#switchport trunk encapsulation dot1q
```

D1(config-if-range)#switchport mode trunk      Denomina las interfaces troncales  
D1(config-if-range)#exite  
D1(config)#exit

### **Configuración en A1**

A1(config)#int range e0/0-1      Ingreso a las interfaces Eth0-1  
A1(config-if-range)#switchport trunk encapsulation dot1q  
A1(config-if-range)#switchport mode trunk      Denomina las interfaces troncales  
A1(config-if-range)#exit  
A1(config)#

### **Configuración interfaces troncales D2 y A1**

Con los siguientes comandos se configuran los enlaces troncales entre los switches D2 y A1

### **Configuración en D2**

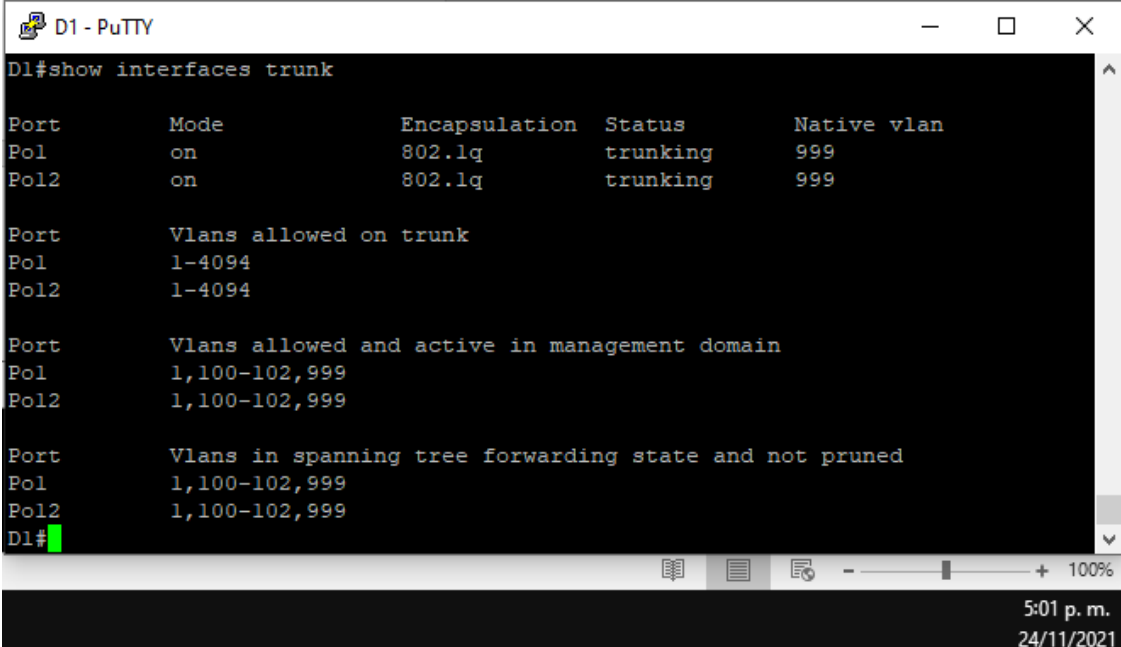
D2(config)#int range e1/0-1      Ingreso a las interfaces Eth0-1  
D2(config-if-range)#switchport trunk encapsulation dot1q  
D2(config-if-range)#switchport mode trunk      Denomina las interfaces troncales  
D2(config-if-range)#exit  
D2(config)#

### **Configuración en A1**

A1(config)#int range e0/2-3      Ingreso a las interfaces Eth0/2-0/3  
A1(config-if-range)#switchport trunk encapsulation dot1q  
A1(config-if-range)#switchport mode trunk      Denomina las interfaces troncales  
A1(config-if-range)#exit  
A1(config)#

Con el siguiente comando **show interfaces trunk** revisamos la configuración de interfaces troncales en D1, D2 y A1

Figura 5 Configuración de interfaces troncales D1



```
D1#show interfaces trunk

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

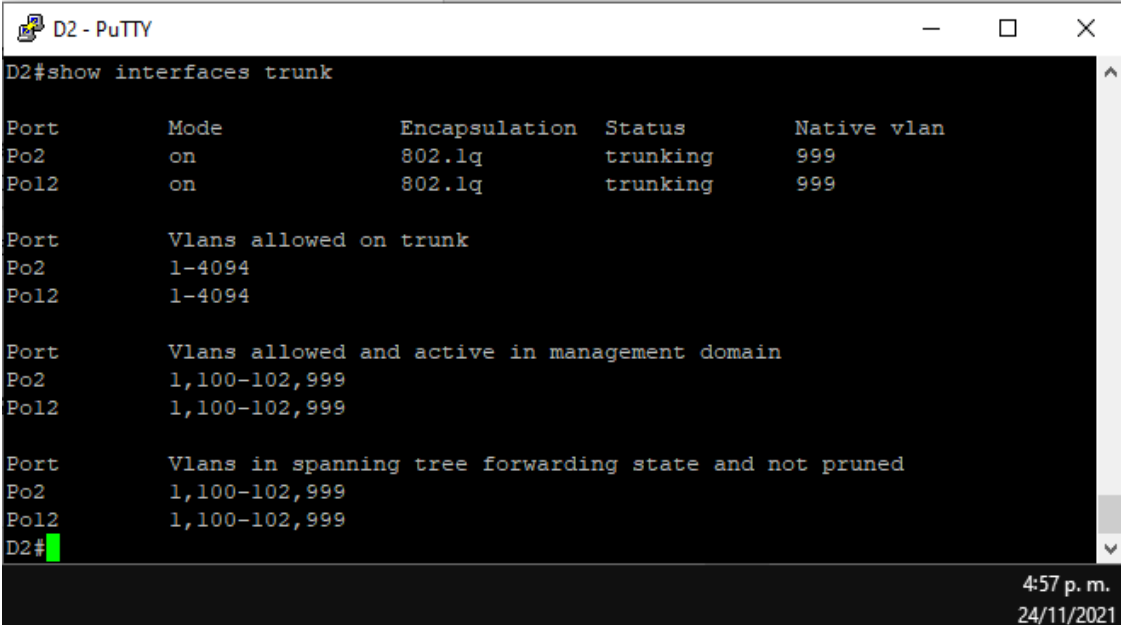
Port      Vlans allowed on trunk
-----
Po1       1-4094
Po12      1-4094

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

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

5:01 p. m.  
24/11/2021

Figura 6 Configuración de interfaces troncales D2



```
D2#show interfaces trunk

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

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

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

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

4:57 p. m.  
24/11/2021



```
A1(config)#int range e0/0-3          Ingreso a las interfaces Ethernet
A1(config-if-range)#switchport trunk native vlan 999      Establece la vlan 999
A1(config-if-range)#exit
```

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)  
- Use Rapid Spanning Tree (RSPT).

Se ingresa este comando con el fin de disminuir los tiempos de convergencia de la red cuando alguno de los enlaces falla se realiza este paso en D1, D2 Y A1

#### **D1**

```
D1(config)#spanning-tree mode?
mode
D1(config)#spanning-tree mode rapid-pvst          Habilita el protocolo RSTP
D1(config)#exit
D1#
```

#### **D2**

```
D2(config)#spanning-tree mode?
mode
D2(config)#spanning-tree mode rapid-pvst          Habilita el protocolo RSTP
D2(config)#exit
D2#
```

#### **A1**

```
A1(config)#spanning-tree mode?
mode
A1(config)#spanning-tree mode rapid-pvst          Habilita el protocolo RSTP
A1(config)#exit                                  Sale del modo configuración
A1#
```

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).

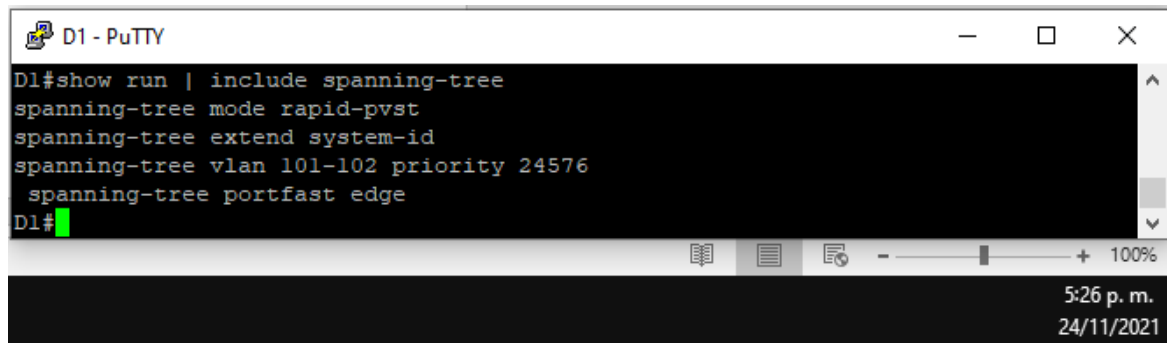
- Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch

Se configura D1 y D2 como raíz teniendo en cuenta las VLAN de la topología con la finalidad de obtener un respaldo entre estos dos dispositivos, se ingresa el siguiente comando en D1 y D2

#### **D1**

```
D1#conf t
D1(config)#spanning-tree vlan 101 root primary
D1(config)#spanning-tree vlan 102 root primary
D1(config)#exit
D1#show run | include spanning-tree
```

*Figura 8 Configuración de los puentes raíz RSTP en D1*

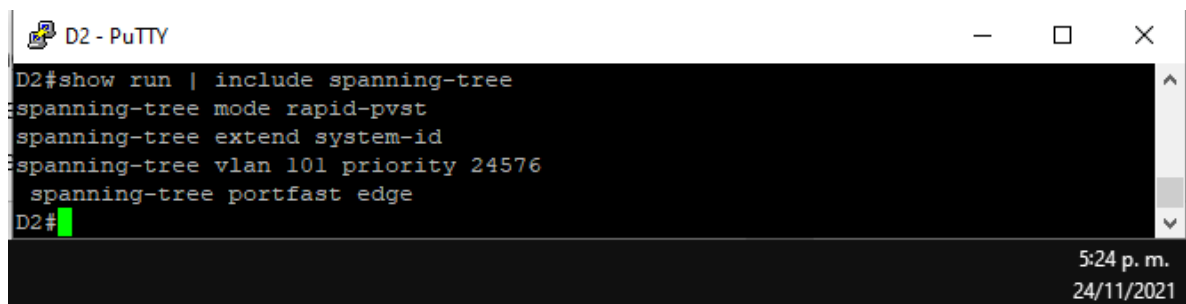


The screenshot shows a PuTTY terminal window titled "D1 - PuTTY". The terminal output displays the configuration for RSTP on switch D1. The commands entered are: `D1#show run | include spanning-tree`, `spanning-tree mode rapid-pvst`, `spanning-tree extend system-id`, `spanning-tree vlan 101-102 priority 24576`, and `spanning-tree portfast edge`. The prompt `D1#` is visible at the bottom left. The window's status bar at the bottom right shows the time `5:26 p. m.` and the date `24/11/2021`.

## D2

```
D2#conf t
D2(config)#spanning-tree vlan 101 root primary
D2(config)#exit
D2#show run | include spanning-tree
```

*Figura 9 Configuración de los puentes raíz RSTP en D2*



The screenshot shows a PuTTY terminal window titled "D2 - PuTTY". The terminal output displays the configuration for RSTP on switch D2. The commands entered are: `D2#show run | include spanning-tree`, `spanning-tree mode rapid-pvst`, `spanning-tree extend system-id`, `spanning-tree vlan 101 priority 24576`, and `spanning-tree portfast edge`. The prompt `D2#` is visible at the bottom left. The window's status bar at the bottom right shows the time `5:24 p. m.` and the date `24/11/2021`.

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

- Use los siguientes números de canales:

- D1 a D2 – Port channel 12
- D1 a A1 – Port channel 1
- D2 a A1 – Port channel 2

Teniendo en cuenta el diagrama de la topología se crean los EtherCannel entre los switches D1, D2 y A1

### **D1 a D2 – Port channel 12**

D1(config)#int range e0/0-3	Ingreso a las interfaces
D1(config-if-range)#shutdown	Se apagan las interfaces
D1(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
D1(config-if-range)#channel-group 12 mode active	Se crea el grupo port ch 12
Creating a port-channel interface Port-channel 12	
D1(config-if-range)#no shutdown	Se enciende las interfaces
D1(config-if)#exit	Se sale del modo config int
D1(config)#int Port-channel12	Se ingresa al port channel
D1(config-if)#switchport trunk encapsulation dot1q	
D1(config-if)#switchport mode trunk	Se declara modo troncal
D1(config-if)#switchport trunk native vlan 999	Se asocia el puerto a la vlan
D1(config-if)#switchport trunk allowed vlan all	
D1(config-if)#end	
D1#show etherchannel summary	Se verifica la configuración

### **D2 a D1 – Port channel 12**

D2(config)#int range e0/0-3	Ingreso a las interfaces
D2(config-if-range)#shutdown	Se apagan las interfaces
D2(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
D2(config-if-range)#channel-group 12 mode active	Se crea el grupo port ch 12
Creating a port-channel interface Port-channel 12	
D2(config-if-range)#no shutdown	Se enciende las interfaces
D2(config-if-range)#exit	
D2(config)#int Port-channel12	Se ingresa al port channel
D2(config-if)#switchport trunk encapsulation dot1q	

D2(config-if)#switchport mode trunk	Se declara modo troncal
D2(config-if)#switchport trunk native vlan 999	Se asocia el puerto a la vlan
D2(config-if)#switchport trunk allowed vlan all	
D2(config-if)#end	
D2#show etherchannel summary	Se verifica la configuración

### **D1 a A1 – Port channel 1**

D1(config)#int range e1/0-1	Ingreso a las interfaces
D1(config-if-range)#shutdown	Se apagan las interfaces
D1(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
D1(config-if-range)#channel-group 1 mode active	Se crea el grupo port ch 1
Creating a port-channel interface Port-channel 1	
D1(config-if-range)#no shutdown	Se enciende las interfaces
D1(config-if-range)#exit	
D1(config)#int Port-channel1	Se ingresa al port channel
D1(config-if)#switchport trunk encapsulation dot1q	
D1(config-if)#switchport mode trunk	Se declara modo troncal
D1(config-if)#switchport trunk native vlan 999	Se asocia el puerto a la vlan
D1(config-if)#switchport trunk allowed vlan all	
D1(config-if)#end	
D1#sh etherchannel summary	Se verifica la configuración

### **A1 a D1 – Port channel 1**

A1(config)#int range e0/0-1	Ingreso a las interfaces
A1(config-if-range)#shutdown	
A1(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
A1(config-if-range)#channel-group 1 mode active	Se crea el grupo port ch 1
Creating a port-channel interface Port-channel 1	
A1(config-if-range)#no shutdown	Se enciende las interfaces
A1(config-if-range)#exit	
A1(config)#int Port-channel1	Se ingresa al port channel
A1(config-if)#switchport trunk encapsulation dot1q	

A1(config-if)#switchport mode trunk	Se declara modo troncal
A1(config-if)#switchport trunk native vlan 999	Se asocia el puerto a la vlan
A1(config-if)#switchport trunk allowed vlan all	
A1(config-if)#end	
A1#sh etherchannel summary	Se verifica la configuración

### **D2 a A2 – Port channel 2**

D2(config)#int range e1/0-1	Ingreso a las interfaces
D2(config-if-range)#shutdown	
D2(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
D2(config-if-range)#channel-group 2 mode active	Se crea el grupo port ch 2
Creating a port-channel interface Port-channel 2	
D2(config-if-range)#no shutdown	Se enciende las interfaces
D2(config-if-range)#exit	
D2(config)#int Port-channel2	Se ingresa al port channel
D2(config-if)#switchport trunk encapsulation dot1q	
D2(config-if)#switchport mode trunk	Se declara modo troncal
D2(config-if)#switchport trunk native vlan 999	Se asocia el puerto a la vlan
D2(config-if)#switchport trunk allowed vlan all	
D2(config-if)#end	
D2#sh etherchannel summary	Se verifica la configuración

### **A2 a D2 – Port channel 2**

A1(config)#int range e0/2-3	Ingreso a las interfaces
A1(config-if-range)#shutdown	
A1(config-if-range)#channel-protocol lacp	Se ingresa el protocolo lacp
A1(config-if-range)#channel-group 2 mode active	Se crea el grupo port ch 12
Creating a port-channel interface Port-channel 2	
A1(config-if-range)#no shutdown	Se enciende las interfaces
A1(config-if-range)#exit	
A1(config)#int Port-channel2	Se ingresa al port channel
A1(config-if)#switchport trunk encapsulation dot1q	

A1(config-if)#switchport mode trunk Se declara modo troncal  
A1(config-if)#switchport trunk native vlan 999 Se asocia el puerto a la vlan  
A1(config-if)#switchport trunk allowed vlan all  
A1(config-if)#exit  
A1 (config-if)#end  
A1#sh etherchannel summary Se verifica la configuración

Con el comando **show etherchannel summary** visualizamos la configuración en D1, D2 y A1

*Figura 10 Configuración de los EtherChannels LACP en D1*

```

D1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----+-----+-----
 1     Po1(SU)        LACP        Et1/0(P)  Et1/1(P)
12     Po12(SU)       LACP        Et0/0(P)  Et0/1(P)  Et0/2(P)
                                     Et0/3(P)
D1#

```

Figura 11 Configuración de los EtherChannels LACP en D2

```

D2#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----+-----+-----
 2     Po2 (SU)      LACP       Et1/0 (P)  Et1/1 (P)
12     Po12 (SU)     LACP       Et0/0 (P)  Et0/1 (P)  Et0/2 (P)
                                         Et0/3 (P)
D2#

```

5:41 p. m.  
24/11/2021

Figura 12 Configuración de los EtherChannels LACP en A1

```

A1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----+-----+-----
 1     Po1 (SU)      LACP       Et0/0 (P)  Et0/1 (P)
 2     Po2 (SU)     LACP       Et0/2 (P)  Et0/3 (P)
A1#

```

5:41 p. m.  
24/11/2021

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).

### **PC1**

#### **Se ingresa a al switch D1 y se configura los puertos de acceso**

D1(config)#interface e3/2

D1(config-if)#switchport mode access                      Se declara la interfaz a modo acceso

D1(config-if)#switchport access vlan 100                      Se declara la vlan a modo acceso

D1(config-if)#spanning-tree portfast                      Se establece como protocolo STP

D1(config-if)#no shutdown

D1(config-if)#exit

### **PC2**

#### **Se ingresa a al switch D1 y se configura los puertos de acceso**

D2(config)#interface e3/2

D2(config-if)#switchport mode access                      Se declara la interfaz a modo acceso

D2(config-if)#switchport access vlan 102                      Se declara la vlan a modo acceso

D2(config-if)#spanning-tree portfast                      Se establece como protocolo STP

D2(config-if)#no shutdown

D2(config-if)#exit

### **PC3**

#### **Se ingresa a al switch D1 y se configura los puertos de acceso**

A1(config)#interface e3/2

A1(config-if)#switchport mode access	Se declara la interfaz a modo acceso
A1(config-if)#switchport access vlan 101	Se declara la vlan a modo acceso
A1(config-if)#spanning-tree portfast	Se establece como protocolo STP
A1(config-if)#no shutdown	
A1(config-if)#exit	

#### PC4

##### Se ingresa a al switch D1 y se configura los puertos de acceso

A1(config)#interface e3/3	
A1(config-if)#switchport mode access	Se declara la interfaz a modo acceso
A1(config-if)#switchport access vlan 100	Se declara la vlan a modo acceso
A1(config-if)#spanning-tree portfast	Se establece como protocolo STP
A1(config-if)#no shutdown	
A1(config-if)#exit	

#### 2.7 Verifique los servicios DHCP IPv4.

- PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

#### PC2

Se ingresa el siguiente comando **ip dhcp** para configurar dhcp en el PC2

PC2> ip dhcp	Configura direccionamiento dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254	

PC2> show ip	Permite visualizar la configuración
--------------	-------------------------------------

```

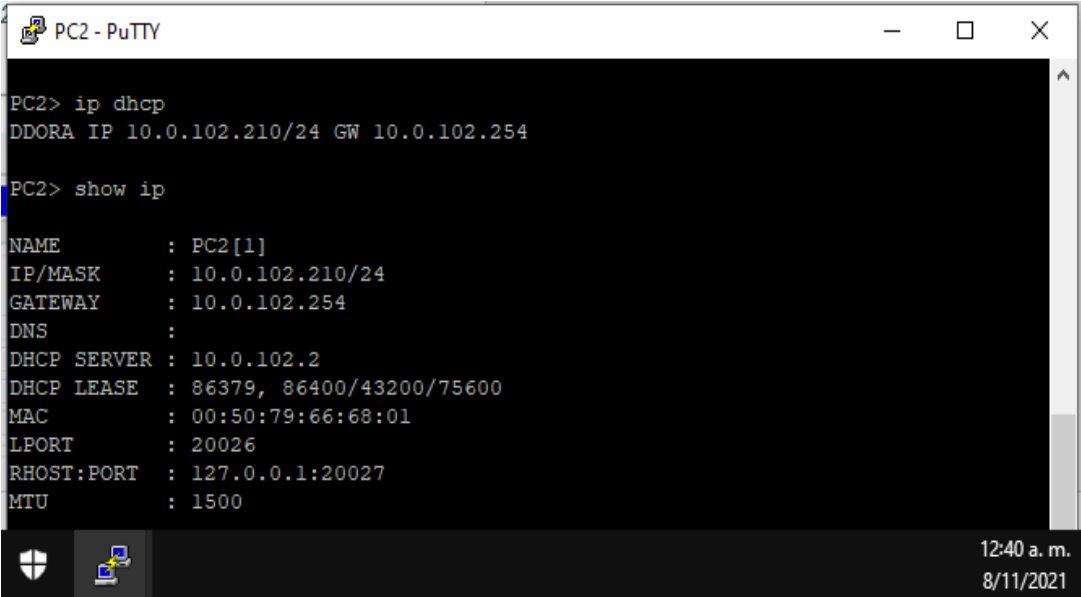
NAME      : PC2[1]
IP/MASK   : 10.0.102.210/24
GATEWAY   : 10.0.102.254
DNS       :
DHCP SERVER : 10.0.102.2
DHCP LEASE : 86379, 86400/43200/75600

```

```
MAC      : 00:50:79:66:68:01
LPORT    : 20026
RHOST:PORT : 127.0.0.1:20027
MTU      : 1500
PC2>
```

Con el comando **show ip** podemos verificar el direccionamiento dhcp en la PC2

*Figura 13 Configuración dhcp PC2*



```
PC2 - PuTTY
PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> show ip

NAME      : PC2[1]
IP/MASK   : 10.0.102.210/24
GATEWAY   : 10.0.102.254
DNS       :
DHCP SERVER : 10.0.102.2
DHCP LEASE : 86379, 86400/43200/75600
MAC       : 00:50:79:66:68:01
LPORT     : 20026
RHOST:PORT : 127.0.0.1:20027
MTU       : 1500

12:40 a.m.
8/11/2021
```

### PC3

Se ingresa el siguiente comando **ip dhcp** para configurar dhcp en el PC3

```
PC3> ip dhcp                                Configura direccionamiento dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254
```

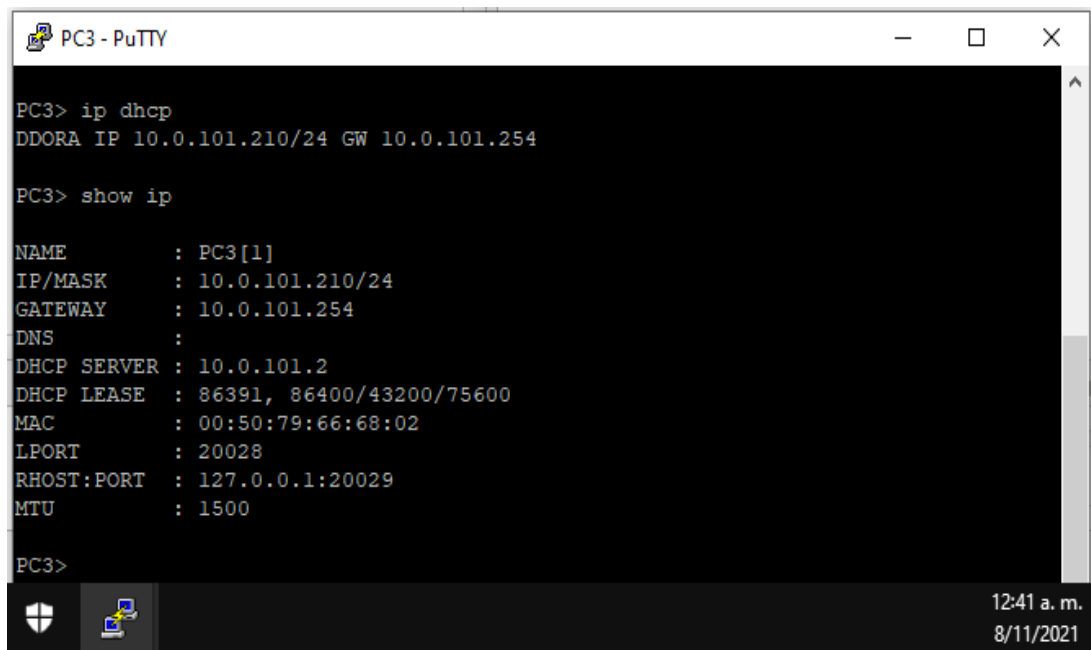
```
PC3> show ip                                Permite visualizar la configuración
```

```
NAME      : PC3[1]
IP/MASK   : 10.0.101.210/24
```

```
GATEWAY : 10.0.101.254
DNS :
DHCP SERVER : 10.0.101.2
DHCP LEASE : 86391, 86400/43200/75600
MAC : 00:50:79:66:68:02
LPORT : 20028
RHOST:PORT : 127.0.0.1:20029
MTU : 1500
PC3>
```

Con el comando **show ip** podemos verificar el direccionamiento dhcp en la PC3

*Figura 14 Configuración dhcp PC3*



```
PC3 - PuTTY
PC3> ip dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254

PC3> show ip

NAME : PC3[1]
IP/MASK : 10.0.101.210/24
GATEWAY : 10.0.101.254
DNS :
DHCP SERVER : 10.0.101.2
DHCP LEASE : 86391, 86400/43200/75600
MAC : 00:50:79:66:68:02
LPORT : 20028
RHOST:PORT : 127.0.0.1:20029
MTU : 1500

PC3>
```

## 2.8 Verifique la conectividad de la LAN local

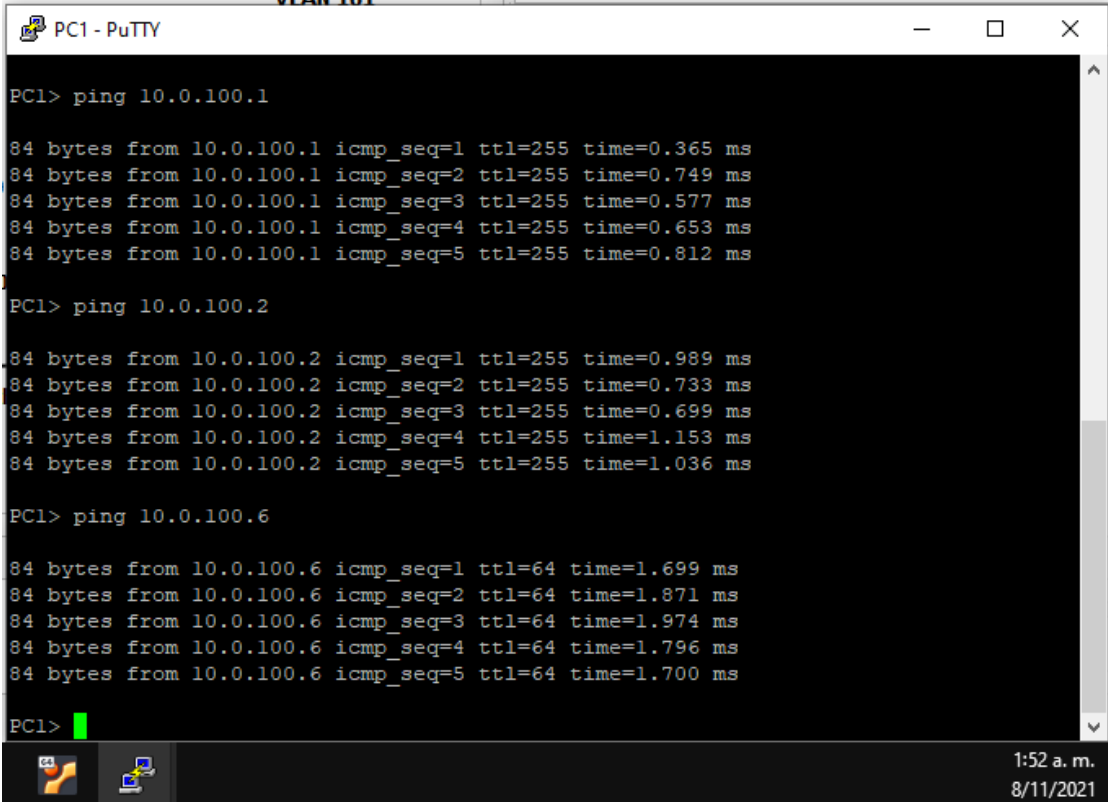
- PC1 debería hacer ping con éxito a:

- **D1: 10.0.100.1**

- **D2: 10.0.100.2**
- **PC4: 10.0.100.6**

En la siguiente imagen se puede visualizar los pings exitosos de PC1 entre D1, D2 y PC4 permitiendo el alcance de los dispositivos, lo que quiere decir que la conectividad de la red funciona correctamente

*Figura 15 Ping de PC1*



```
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.365 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.749 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.577 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.653 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.812 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.989 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.733 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.699 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.153 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.036 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.699 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.871 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.974 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.796 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.700 ms

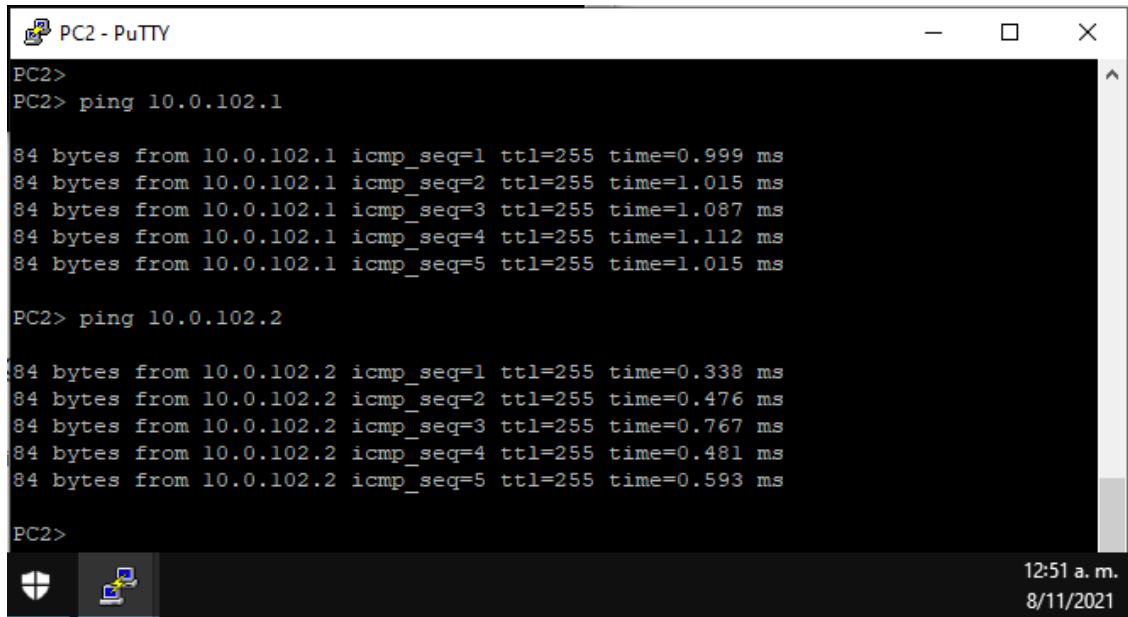
PC1>
```

PC2 debería hacer ping con éxito a:

- **D1: 10.0.102.1**
- **D2: 10.0.102.2**

En la siguiente imagen se puede visualizar los pings exitosos de PC2 entre D1 y D2 permitiendo el alcance de los dispositivos, lo que quiere decir que la conectividad de la red funciona correctamente

Figura 16 Ping de PC2



```
PC2>
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.999 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.015 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=1.087 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.112 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.015 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.338 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.476 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.767 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.481 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.593 ms

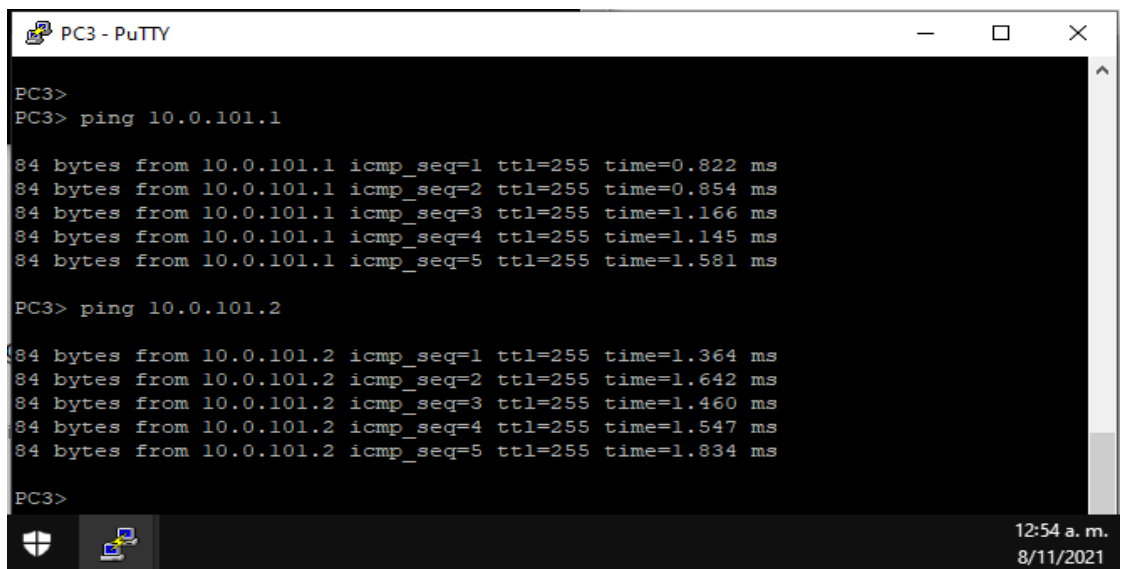
PC2>
```

PC3 debería hacer ping con éxito a:

- **D1: 10.0.101.1**
- **D2: 10.0.101.2**

En la siguiente imagen se puede visualizar los pings exitosos de PC3 entre D1 y D2 permitiendo el alcance de los dispositivos, lo que quiere decir que la conectividad de la red funciona correctamente

Figura 17 Ping de PC3



```
PC3>
PC3> ping 10.0.101.1

84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.822 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.854 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.166 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.145 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=1.581 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=1.364 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=1.642 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=1.460 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=1.547 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=1.834 ms

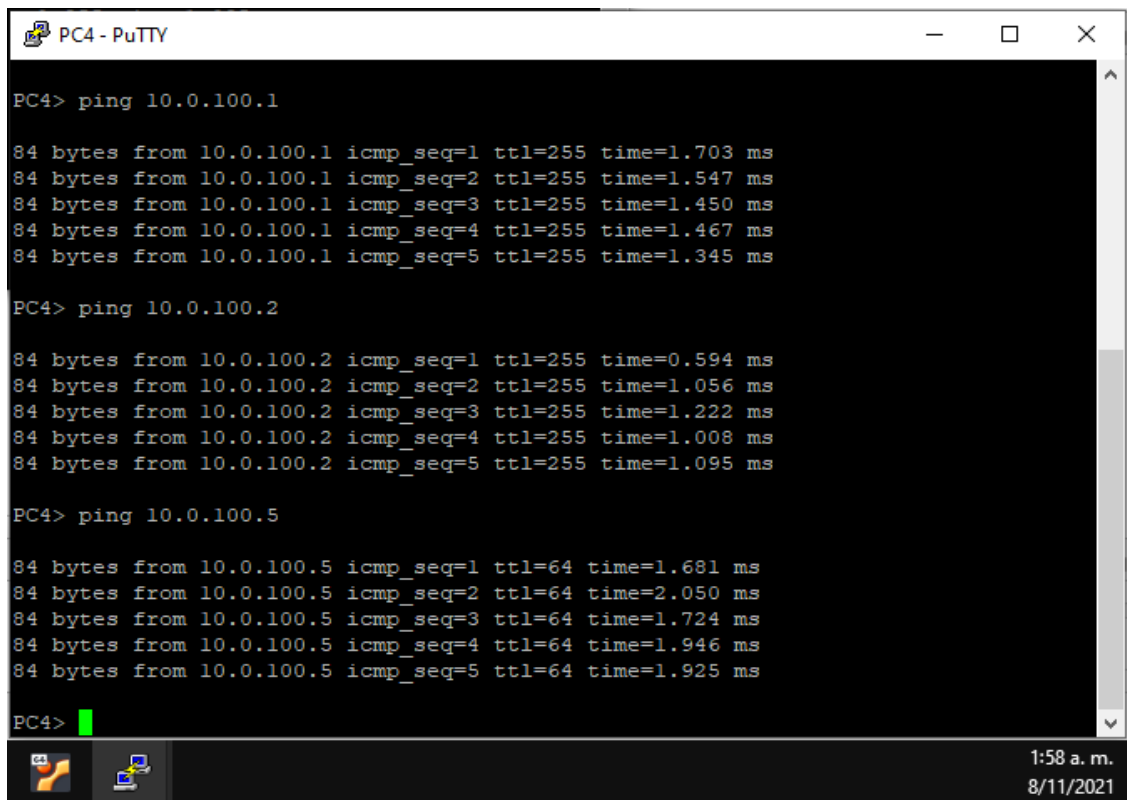
PC3>
```

PC4 debería hacer ping con éxito a:

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

En la siguiente imagen se puede visualizar los pings exitosos de PC4 entre D1, D2 y PC1 permitiendo el alcance de los dispositivos, lo que quiere decir que la conectividad de la red funciona correctamente

*Figura 18 Ping de PC4*



```
PC4 - PuTTY
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=1.703 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.547 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.450 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.467 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.345 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.594 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.056 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.222 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.008 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.095 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=1.681 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=2.050 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.724 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.946 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.925 ms

PC4> █
```

1:58 a. m.  
8/11/2021

### Paso 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:

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.

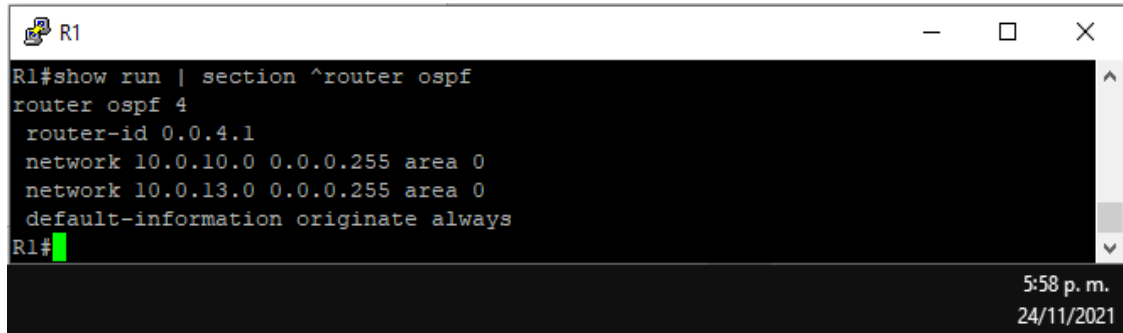
- Use OSPF Process ID **4** y asigne los siguientes routerIDs:

- **R1: 0.0.4.1**

```
R1(config)#router ospf 4                               Accedemos al modo config ospf del
router
R1(config-router)#router-id 0.0.4.1                   Asignamos el ID del
router
R1(config-router)#do show ip route connected          Permite ver las redes
directamente conectadas
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C    10.0.10.0/24 is directly connected, FastEthernet0/0
L    10.0.10.1/32 is directly connected, FastEthernet0/0
C    10.0.13.0/24 is directly connected, Serial1/1
L    10.0.13.1/32 is directly connected, Serial1/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/27 is directly connected, FastEthernet2/0
L    209.165.200.2/32 is directly connected, FastEthernet2/0
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate always
R1(config-router)#exit
R1(config)#do wr                                       Guarda la configuración
Building configuration...
[OK]
R1(config)#
```

**NOTA:** Es de aclarar que en este paso no se anunció la red entre R1 y R2 en ospf  
Con el siguiente comando **show run | section ^router ospf** podemos ver la configuración ospf 4 en el router R1

*Figura 19 Configuración ospf 4 en R1*



```
R1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate always
R1#
```

5:58 p. m.  
24/11/2021

• **R3: 0.0.4.3**

```
R3(config)#router ospf 4          Accedemos al modo config ospf del router
R3(config-router)#router-id 0.0.4.3      Asignamos el ID del router
R3(config-router)#do show ip route connected      Permite ver las redes
directamente conectadas
    10.0.0.0/24 is subnetted, 2 subnets
C    10.0.11.0 is directly connected, FastEthernet0/0
C    10.0.13.0 is directly connected, Serial1/1
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#
*Nov 9 00:56:22.159: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial1/1 from
LOADING to FULL, Loading Done
R3(config-router)#exit
R3(config)#do wr          Guarda la configuración en el router
Building configuration...
[OK]
R3(config)#
```

Con el siguiente comando **show run | section ^router ospf** podemos ver la configuración ospf 4 en el router R3

*Figura 20 Configuración Process ID 4 R3*

```

R3
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
R3#

```

6:03 p. m.  
24/11/2021

- **D1: 0.0.4.131**

D1(config)#router ospf 4                    Accedemos al modo config ospf del switch  
D1(config-router)#router-id 0.0.4.131        Asignamos el ID del switch  
D1(config-router)#do show ip route connected    Permite ver las redes directamente conectadas

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter área  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, H - NHRP, I – LISP  
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

C    10.0.10.0/24 is directly connected, Ethernet2/0  
L    10.0.10.2/32 is directly connected, Ethernet2/0  
C    10.0.100.0/24 is directly connected, Vlan100  
L    10.0.100.1/32 is directly connected, Vlan100  
C    10.0.101.0/24 is directly connected, Vlan101  
L    10.0.101.1/32 is directly connected, Vlan101  
C    10.0.102.0/24 is directly connected, Vlan102  
L    10.0.102.1/32 is directly connected, Vlan102

```

D1(config-router)#$rotocol on Interface Vlan102, changed state to up
46: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed
state to up^
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#
*Nov 9 06:11:03.623: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on
Ethernet2/0 from LOADING to FULL, Loading Done
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#exit
D1(config)#do wr                               Guarda la configuración en el switch
Building configuration...
Compressed configuration from 3951 bytes to 1954 bytes[OK]
D1(config)#

```

Con el siguiente comando **show run | section ^router ospf** podemos ver la configuración ospf 4 en el switch D1

*Figura 21 Configuración Process ID 4 D1*

```

D1-PuTTY
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  passive-interface Ethernet0/0
  passive-interface Ethernet0/1
  passive-interface Ethernet0/2
  passive-interface Ethernet0/3
  passive-interface Ethernet1/0
  passive-interface Ethernet1/1
  passive-interface Vlan100
  passive-interface Vlan101
  passive-interface Vlan102
  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
D1#

```

6:05 p. m.  
24/11/2021

• **D2: 0.0.4.132**

D2(config)#router ospf 4                    Accedemos al modo config ospf del switch  
D2(config-router)#router-id 0.0.4.132        Asignamos el ID del switch  
D2(config-router)#do show ip route connected    Permite ver las redes  
directamente conectadas

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP  
+ - replicated route, % - next hop override

Gateway of last resort is not set

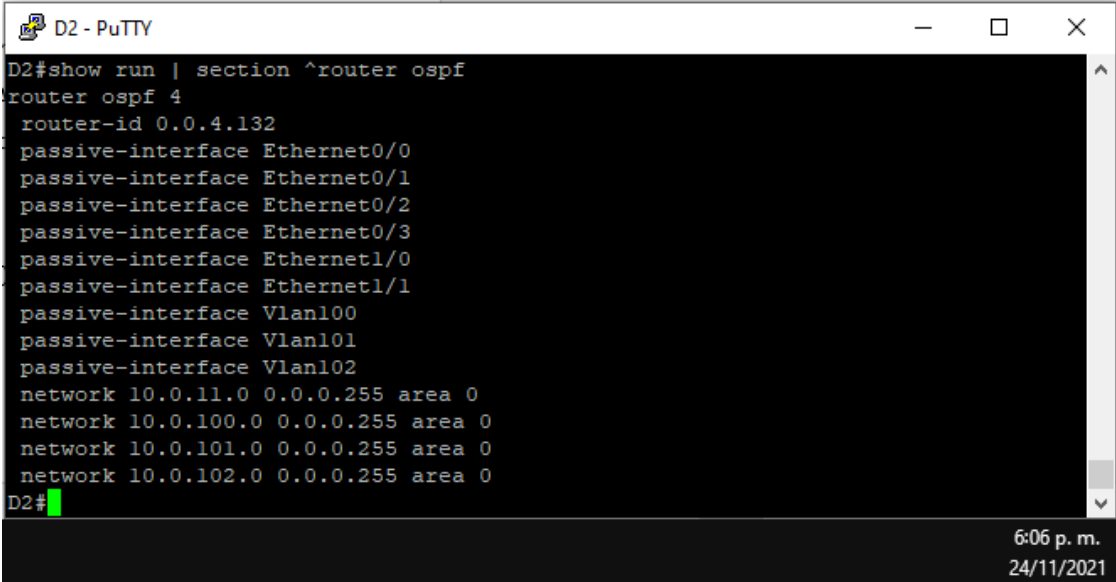
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks  
C    10.0.11.0/24 is directly connected, Ethernet2/0  
L    10.0.11.2/32 is directly connected, Ethernet2/0  
C    10.0.100.0/24 is directly connected, Vlan100  
L    10.0.100.2/32 is directly connected, Vlan100  
C    10.0.101.0/24 is directly connected, Vlan101  
L    10.0.101.2/32 is directly connected, Vlan101  
C    10.0.102.0/24 is directly connected, Vlan102  
L    10.0.102.2/32 is directly connected, Vlan102  
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0  
D2(config-router)#  
\*Nov 9 06:20:19.185: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on  
Ethernet2/0 from LOADING to FULL, Loading Done  
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0  
D2(config-router)#  
\*Nov 9 06:21:12.991: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Vlan100  
from LOADING to FULL, Loading Done

```

D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.10 0.0.0.255 area 0
*Nov 9 06:22:33.758: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Vlan101
from LOADING to FULL, Loading Done
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#
*Nov 9 06:22:48.197: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Vlan102
from LOADING to FULL, Loading Done
D2(config-router)#exit
D2(config)#do wr                               Guarda la configuración en el switch
Building configuration...
Compressed configuration from 3951 bytes to 1949 bytes[OK]
D2(config)#
Con el siguiente comando show run | section ^router ospf podemos ver la
configuración ospf 4 en el switch D2

```

*Figura 22 Configuración Process ID 4 D2*



```

D2 - PuTTY
D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface Ethernet0/0
passive-interface Ethernet0/1
passive-interface Ethernet0/2
passive-interface Ethernet0/3
passive-interface Ethernet1/0
passive-interface Ethernet1/1
passive-interface Vlan100
passive-interface Vlan101
passive-interface Vlan102
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
D2#
6:06 p. m.
24/11/2021

```

**En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.**

**R1:**

```
R1(config-router)#router bgp 300          Accedemos al modo config bgp del router
R1(config-router)#bgp router-id 1.1.1.1  Asignamos el ID del router
R1(config-router)#do sh ip route connected  Permite ver las redes
directamente conectadas
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C    10.0.10.0/24 is directly connected, FastEthernet0/0
L    10.0.10.1/32 is directly connected, FastEthernet0/0
C    10.0.13.0/24 is directly connected, Serial1/1
L    10.0.13.1/32 is directly connected, Serial1/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/27 is directly connected, FastEthernet2/0
L    209.165.200.2/32 is directly connected, FastEthernet2/0
R1(config-router)#no bgp default ipv4-unicast
R1(config-router)#neighbor 209.165.200.1 remote-as 500
R1(config-router)#neighbor 2001:DB8:200::2 remote-as 500
R1(config-router)#network 209.165.200.0 mask 255.255.255.224
R1(config-router)#exit
R1(config)#do wr                          Guarda la configuración en el router
Building configuration...
[OK]
R1(config)#
```

**R2:**

```
R2(config)#router bgp 500                  Accedemos al modo config ospf del router
R2(config-router)#bgp router-id 2.2.2.2  Asignamos el ID del router
R2(config-router)#no bgp default ipv4-unicast
R2(config-router)#do sh ip route connected  Permite ver las redes
directamente conectadas
2.0.0.0/32 is subnetted, 1 subnets
```

```

C    2.2.2.2 is directly connected, Loopback0
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/27 is directly connected, FastEthernet0/0
L    209.165.200.1/32 is directly connected, FastEthernet0/0
R2(config-router)#neighbor 209.165.200.2 remote-as 300
R2(config-router)#network 209.165.200.0 mask 255.255.255.224
R2(config-router)#exit
R2(config)#do wr                                Guarda la configuración en el router
Building configuration...
[OK]
R2(config)#

```

**Deshabilite las publicaciones OSPFv2 en:**

**• D1: todas las interfaces excepto e2/0**

```

D1(config)#router ospf 4                        Accedemos al modo config ospf del switch
D1(config-router)#passive-interface vlan 100    Deshabilita OSPF de la vlan 100
D1(config-router)#
*Nov  9 06:54:48.032: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.132 on  Vlan100
from FULL to DOWN , Neighbor Down: Interface down or detached
D1(config-router)#passive-interface vlan 101
D1(config-router)#
*Nov  9 06:55:25.120: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.132 on  Vlan101
from FULL to DOWN , Neighbor Down: Interface down or detached
D1(config-router)#passive-interface vlan 102    Deshabilita OSPF de la vlan 100
D1(config-router)#
*Nov  9 06:55:49.921: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.132 on  Vlan102
from FULL to DOWN , Neighbor Down: Interface down or detached
D1(config-router)#passive-interface e0/0
D1(config-router)#passive-interface e0/1
D1(config-router)#passive-interface e0/2
D1(config-router)#passive-interface e0/3
D1(config-router)#passive-interface e1/0
D1(config-router)#passive-interface e1/0

```

```

D1(config-router)#passive-interface e1/1           Deshabilita OSPF en cada una
de la interfaces del switch
D1(config-router)#exit
D1(config)#do wr                                  Guarda la configuración en el switch
Building configuration...
Compressed configuration from 4279 bytes to 2092 bytes[OK]
D1(config)#

```

• **D2: todas las interfaces excepto e2/0**

```

D2(config)#router ospf 4                         Accedemos al modo config ospf del switch
D2(config-router)#passive-interface vlan 100
D2(config-router)#passive-interface vlan 101
D2(config-router)#passive-interface vlan 102
D2(config-router)#passive-interface e0/0
D2(config-router)#passive-interface e0/1
D2(config-router)#passive-interface e0/2
D2(config-router)#passive-interface e0/3
D2(config-router)#passive-interface e1/0
D2(config-router)#passive-interface e1/1         Deshabilita OSPF en cada una
de la interfaces del switch y la vlan
D2(config-router)#exit
D2(config)#do wr                                  Guarda la configuración en el switch
Building configuration...
Compressed configuration from 4279 bytes to 2089 bytes[OK]
D2(config)#

```

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

Use OSPF Process ID 6 y asigne los siguientes routerIDs:

- R1: 0.0.6.1
- R3: 0.0.6.3
- D1: 0.0.6.131

- D2: 0.0.6.132
- En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.
- **R1: 0.0.6.1**

Se configura el Process ID 6 y se asigna los siguientes routerIDs

**R1: Se anuncian todas las redes directamente conectadas en Area 0. excepto FastEthernet2/0**

R1(config)#ipv6 router ospf 6	Accedemos al modo config ospf del router
R1(config-rtr)#router-id 0.0.6.1	Asignamos el ID del router
R1(config-rtr)#do show ip route connected	Permite ver las redes directamente conectadas
209.165.200.0/27 is subnetted, 1 subnets	
C 209.165.200.224	is directly connected, FastEthernet2/0
10.0.0.0/24 is subnetted, 6 subnets	
C 10.0.10.0	is directly connected, FastEthernet0/0
C 10.0.13.0	is directly connected, Serial1/1
R1(config-rtr)#interface fa0/0	Ingresamos a la interfaz fa0/0
R1(config-if)#ipv6 ospf 6 area 0	Config ospf 6 en área 0 a la interfaz
R1(config-if)#interface s1/1	Ingresamos a la interfaz s1/1
R1(config-if)#ipv6 ospf 6 area 0	Config ospf 6 en área 0 a la interfaz
R1(config-if)#exit	Salimos de la configuración interfaz
R1(config)#do wr	Guarda la configuración en el router

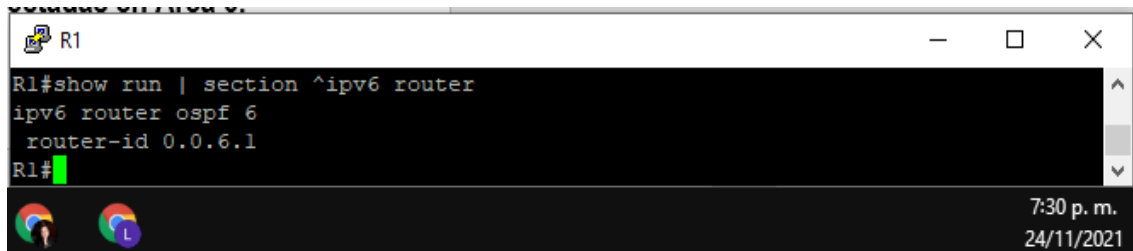
Building configuration...

[OK]

R1(config)#ig#router ospf 6

Con el siguiente comando **show run | section ^ipv6 router** podemos ver la configuración ospf 6 en R1

*Figura 23 Configuración Process ID 6 R1*



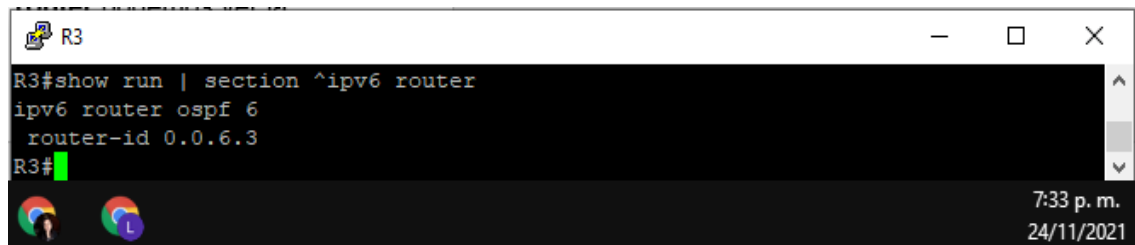
- **R3: 0.0.6.3**

**R3: Se anuncian todas las redes directamente conectadas en Area 0.**

```
R3(config)#ipv6 router ospf 6          Accedemos al modo config ospf del router
R3(config-rtr)#router-id 0.0.6.3      Asignamos el ID del router
R3(config-rtr)#do sh ip route connected  Permite ver las redes
directamente conectadas
    10.0.0.0/24 is subnetted, 6 subnets
C    10.0.11.0 is directly connected, FastEthernet0/0
C    10.0.13.0 is directly connected, Serial1/1
R3(config-rtr)#interface fa0/0
R3(config-if)#ipv6 ospf 6 area 0      Config ospf 6 en área 0 a la interfaz
R3(config-if)#interface s1/1
R3(config-if)#ipv6 ospf 6 area 0      Config ospf 6 en área 0 a la interfaz
R3(config-if)#
*Nov 9 12:23:11.855: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial1/1
fro LOADING to FULL, Loading Done
R3(config-if)#exit
R3(config)#do wr                       Guarda la configuración en el router
Building configuration...
[OK]
```

Con el siguiente comando **show run | section ^ipv6 router** podemos ver la configuración ospf 6 en R3

*Figura 24 Configuración Process ID 6 R3*



- **D1: 0.0.6.131**

• **D1: Se anuncian todas las redes directamente conectadas / VLANs en Area 0.**

```
D1(config)#ipv6 router ospf 6          Accedemos al modo config ospf del router
D1(config-rtr)#router-id 0.0.6.131    Asignamos el ID del switch
```

D1(config-rtr)#do sh ip route connected  
directamente conectadas

Permite ver las redes

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B – BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter área

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, I – LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks

C 10.0.10.0/24 is directly connected, Ethernet2/0

L 10.0.10.2/32 is directly connected, Ethernet2/0

C 10.0.100.0/24 is directly connected, Vlan100

L 10.0.100.1/32 is directly connected, Vlan100

C 10.0.101.0/24 is directly connected, Vlan101

L 10.0.101.1/32 is directly connected, Vlan101

C 10.0.102.0/24 is directly connected, Vlan102

L 10.0.102.1/32 is directly connected, Vlan102

```

D1(config)#interface e2/0                               Ingresamos a la interfaz e2/0
D1(config-if)#ipv6 ospf 6 area 0                       Config ospf 6 en área 0 a la interfaz
D1(config-if)#
*Nov  9 08:37:28.465: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on
Ethernet2/0 from LOADING to FULL, Loading Done
D1(config-if)#interface vlan100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface vlan101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface vlan102
D1(config-if)#ipv6 ospf 6 area 0                       Se anuncian todas las redes conectadas
al switch
D1(config-if)#exit
D1(config)#do wr                                       Guarda la configuración en el switch
Building configuration...
Compressed configuration from 4340 bytes to 2096 bytes[OK]
Con el siguiente comando show run | section ^ipv6 router podemos ver la
configuración ospf 6 en D1

```

*Figura 25 Configuración Process ID 6 D1*

```

D1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
D1#

```

- **D2: 0.0.6.132**
  - **D1: Se anuncian todas las redes directamente conectadas / VLANs en Area 0.**

```

D2(config)#ipv6 router ospf 6                          Accedemos al modo config ospf del switch
D2(config-rtr)#router-id 0.0.6.132                    Asignamos el ID del switch
D2(config-rtr)#do sh ip route connected               Permite ver las redes
directamente conectadas

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2  
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
 ia - IS-IS inter area, \* - candidate default, U - per-user static route  
 o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP  
 + - replicated route, % - next hop override

Gateway of last resort is not set

```

10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C   10.0.11.0/24 is directly connected, Ethernet2/0
L   10.0.11.2/32 is directly connected, Ethernet2/0
C   10.0.100.0/24 is directly connected, Vlan100
L   10.0.100.2/32 is directly connected, Vlan100
C   10.0.101.0/24 is directly connected, Vlan101
L   10.0.101.2/32 is directly connected, Vlan101
C   10.0.102.0/24 is directly connected, Vlan102
L   10.0.102.2/32 is directly connected, Vlan102
D2(config-rtr)#interface e2/0                               Ingresamos a la interfaz e2/0
D2(config-if)#ipv6 ospf 6 area 0                           Config ospf 6 en área 0 a la interfaz
D2(config-if)#
*Nov  9 08:45:41.452: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.3 on Ethernet2/0
fr   om LOADING to FULL, Loading Done
D2(config-if)#interface vlan100                             Ingresamos a la interfaz vlan 100
D2(config-if)#ipv6 ospf 6 area 0                           Config ospf 6 en área 0 a la interfaz
D2(config-if)#
*Nov  9 08:46:26.732: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.131 on Vlan100
from   LOADING to FULL, Loading Done
D2(config)#interface vlan101                                Ingresamos a la interfaz vlan 101
D2(config-if)#ipv6 ospf 6 area 0                           Config ospf 6 en área 0 a la interfaz
D2(config-if)#

```

\*Nov 9 08:47:13.363: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.131 on Vlan101 from LOADING to FULL, Loading Done

D2(config-if)#interface vlan102 Ingresamos a la interfaz vlan 102

D2(config-if)#ipv6 ospf 6 area 0 Config ospf 6 en área 0 a la interfaz

D2(config-if)#

\*Nov 9 08:48:05.725: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.131 on Vlan102 from LOADING to FULL, Loading Done

D2(config-if)#exit

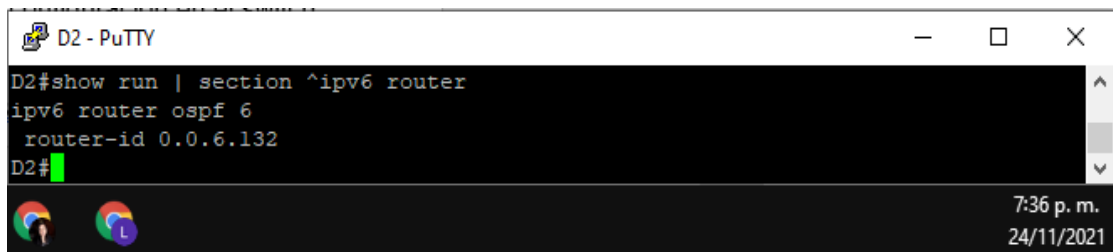
D2(config)#do wr Guarda la configuración en el switch

Building configuration...

Compressed configuration from 4340 bytes to 2093 bytes[OK]

Con el siguiente comando **show run | section ^ipv6 router** podemos ver la configuración ospf 6 en D2

*Figura 26 Configuración Process ID 6 D2*



```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.132
D2#
```

Deshabilite las publicaciones OSPFv3 en:

- **D1: todas las interfaces excepto e2/0**

D1(config)#ipv6 router ospf 6 Accedemos al modo config ospf del switch

D1(config-rtr)#passive-interface e0/0

D1(config-rtr)#passive-interface e0/1

D1(config-rtr)#passive-interface e0/2

D1(config-rtr)#passive-interface e0/3

D1(config-rtr)#passive-interface e1/0

D1(config-rtr)#passive-interface e1/1 Deshabilita todas interfaces excepto e2/0

D1(config-rtr)#do wr Guarda la configuración en el switch

Building configuration...

Compressed configuration from 4401 bytes to 2143 bytes[OK]

D1(config-rtr)#

- **D2: todas las interfaces excepto e2/0**

```
D2(config)#ipv6 router ospf 6          Accedemos al modo config ospf del switch
D2(config-rtr)#passive-interface e0/0
D2(config-rtr)#passive-interface e0/1
D2(config-rtr)#passive-interface e0/2
D2(config-rtr)#passive-interface e0/3
D2(config-rtr)#passive-interface e1/0
D2(config-rtr)#passive-interface e1/1  Deshabilitan todas interfaces excepto e2/0
D2(config-rtr)#do wr                  Guarda la configuración en el switch
Building configuration...
Compressed configuration from 4401 bytes to 2135 bytes[OK]
D2(config-rtr)#
```

### 3.3 En R2 en la “Red ISP”, configure MPBGP.

- Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- **Una ruta estática predeterminada IPv4.**

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback0          Asigna ruta IPv4
R2(config)#do wr                                       Guarda la configuración en el router
Building configuration...
[OK]
```

- **Una ruta estática predeterminada IPv6.**

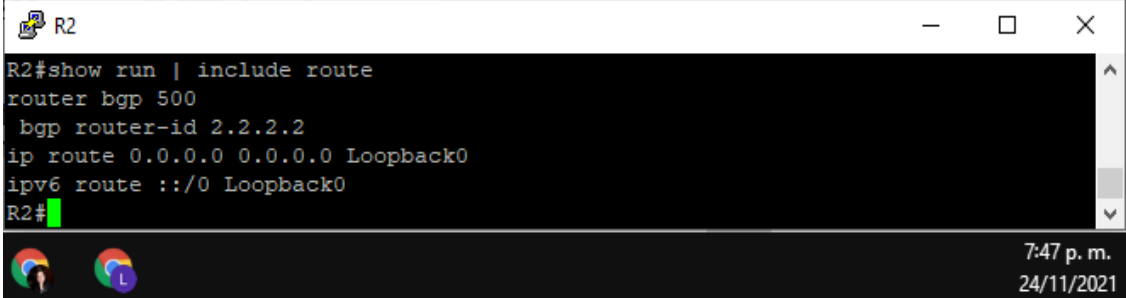
```
R2(config)#ipv6 route ::/0 loopback0                  Asigna ruta IPv6
R2(config)#do wr                                       Guarda la configuración en el router
Building configuration...
[OK]
```

- Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2.

```
R2(config)#router bgp 500                             Accedemos al modo config bgp del router
R2(config-router)#bgp router-id 2.2.2.2              Asignamos el ID del router
R2(config-router)#
```

Con el siguiente comando **show run | include route** podemos ver la configuración bgp y la interfaz Loopback0 por defecto en R2

*Figura 27 Configuración bgp ASN 500 en R2*



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

**Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.**

**En IPv4 address family, anuncie:**

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0).

```
R2(config)#router bgp 500           Accede al modo config bgp del router
R2(config-router)#address-family ipv4 unicast   Accede a config add family IPv4
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255   Habilita la red
R2(config-router-af)#neighbor 209.165.200.2 activate           Relación de vecino
R2(config-router-af)#redistribute ospf 4 match internal external 1 external 2   Con
este comando le decimos al router que redistribuya interna o externamente ospf 4
R2(config-router-af)#do wr           Guarda la configuración en el router
Building configuration...
[OK]
```

**En IPv6 address family, anuncie:**

- La red Loopback 0 IPv4 (/128).
- La ruta por defecto (::/0).

```
R2(config)#router bgp 500           Accede al modo config bgp del router
R2(config-router)#address-family ipv6 unicast   Accede a la config add family
R2(config-router-af)#network 2001:db8:2222::1/128   Anuncia la red
```

```
R2(config-router-af)#exit
```

```
R2(config-router)#do wr
```

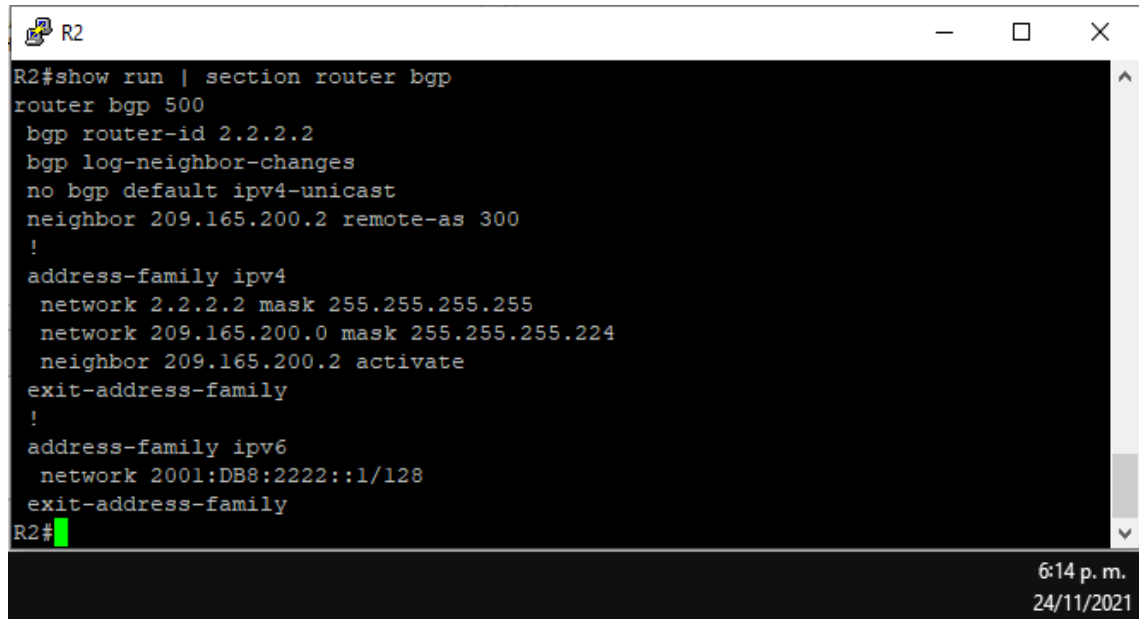
Guarda la configuración en el router

```
Building configuration...
```

```
[OK]
```

En la siguiente imagen se puede ver la configuración en R2 de bgp, address family IPv4 e IPv6 usando el comando **show run | section router bgp**

*Figura 28 Configuración bgp relación vecino R2*



```
R2
R2#show run | section router bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 209.165.200.2 remote-as 300
  !
  address-family ipv4
    network 2.2.2.2 mask 255.255.255.255
    network 209.165.200.0 mask 255.255.255.224
    neighbor 209.165.200.2 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:2222::1/128
  exit-address-family
R2#
```

6:14 p. m.  
24/11/2021

3.4 En R1 en la “Red ISP”, configure MPBGP.

Configure dos rutas resumen estáticas a la interfaz Null 0:

- **Una ruta resumen IPv4 para 10.0.0/8.**

Mediante el siguiente comando se configura la interfaz Null 0 con la ip route 10.0.0.0 con máscara red 255.0.0.0 para IPv4

```
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
```

- **Una ruta resumen IPv6 para 2001:db8:100::/48.**

Con el siguiente comando se configura la ruta estática a la interfaz Null 0 para la IPv6

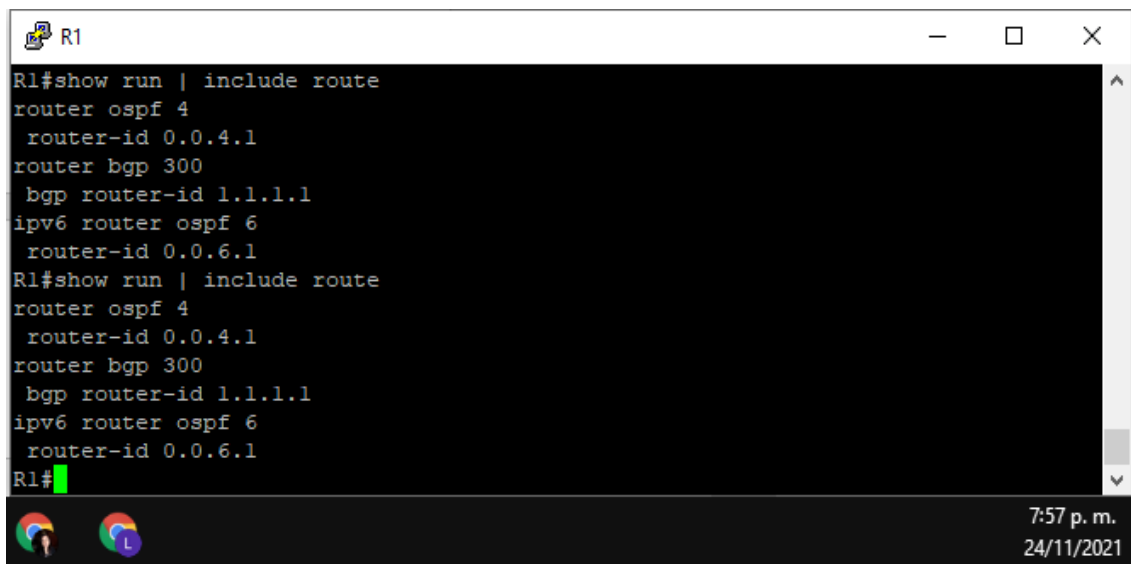
```
R1(config)#ipv6 route 2001:db8:100::/48 null0
```

### Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

```
R1(config)#router bgp 300           Accede al modo config bgp del router
R1(config-router)#bgp router-id 1.1.1.1       Asigna el ID del router
R1(config-router)#
```

Con el siguiente comando **show run | include route** podemos ver la configuración bgp 300, ospf 4 y ospf 6 en R1

*Figura 29 Configuración bgp ASN 300 en R1*



```
R1#show run | include route
router ospf 4
  router-id 0.0.4.1
router bgp 300
  bgp router-id 1.1.1.1
ipv6 router ospf 6
  router-id 0.0.6.1
R1#show run | include route
router ospf 4
  router-id 0.0.4.1
router bgp 300
  bgp router-id 1.1.1.1
ipv6 router ospf 6
  router-id 0.0.6.1
R1#
```

### Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

- Deshabilite la relación de vecino IPv6.

```
R1(config)#router bgp 300           Accede al modo config bgp del router
R1(config-router)#address-family ipv4 unicast   Accede a la config add family
```

R1(config-router-af)#no neighbor 2001:db8:200::2 activate  
R1(config-router-af)#neighbor 209.165.200.30 activate   Deshabilita la relación de vecino

- Habilite la relación de vecino IPv4.

- **Anuncie la red 10.0.0.0/8.**

R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0                    Se anuncia la red  
R1(config-router-af)#

En IPv6 address family:

- **Deshabilite la relación de vecino IPv4.**

R1(config)#router bgp 300    Accede al modo config bgp del router  
R1(config-router)#address-family ipv6 unicast                    Accede a la config add family  
R1(config-router-af)#no neighbor 209.165.200.226 activate       Deshabilita la relación vecino

- **Habilite la relación de vecino IPv6.**

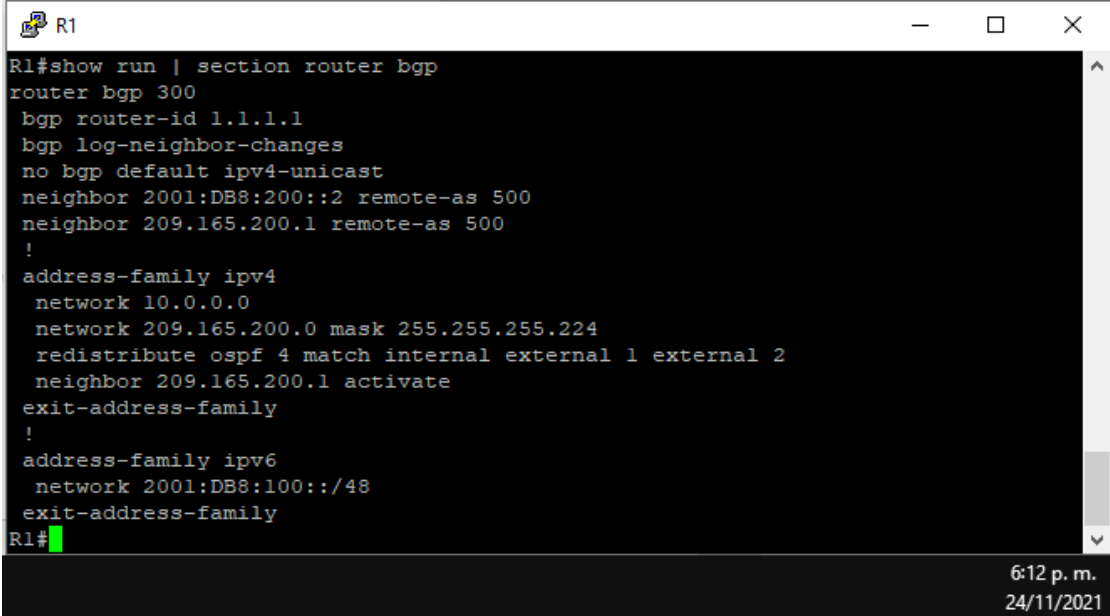
R1(config-router-af)#neighbor 2001:db8:200::2 activate        Habilita relación vecino

- **Anuncie la red 2001:db8:100::/48.**

R1(config-router-af)#network 2001:db8:100::/48                    Anuncia la red IPv6

En la siguiente imagen se puede ver la configuración en R1 de bgp, address family IPv4 e IPv6 usando el comando **show run | section router bgp**

Figura 30 Configuración bgp relación vecino R1



```
R1#show run | section router bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.1 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    network 209.165.200.0 mask 255.255.255.224
    redistribute ospf 4 match internal external 1 external 2
    neighbor 209.165.200.1 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
  exit-address-family
R1#
```

6:12 p. m.  
24/11/2021

Paso 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:

### 4.3 En D1 configure HSRPv2.

D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

#### Configure HSRP versión 2.

##### Configure IPv4 HSRP grupo 104 para la VLAN 100:

- En D1 Asigne la dirección IP virtual 10.0.100.254.

Con los siguientes comandos se asigna la IP virtual en la vlan 100

```
D1(config)#interface vlan 100
D1(config)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#standby 104 ip 10.0.100.254
```

- **Establezca la prioridad del grupo en 150.**

D1(config-if)#standby 104 priority 150 Se establece la prioridad

- **Habilite la preferencia (preemption).**

D1(config-if)# standby 104 preempt Habilita la preferencia grupo 104

- **Rastree el objeto 4 y decremente en 60.**

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

**Configure IPv4 HSRP grupo 114 para la VLAN 101:**

- **Asigne la dirección IP virtual 10.0.101.254.**

Con los siguientes comandos se asigna la IP virtual en la vlan 101

D1(config)#interface vlan 101

D1(config)#ip address 10.0.101.1 255.255.255.0

D1(config-if)#standby 114 ip 10.0.101.254

- **Establezca la prioridad del grupo en 150.**

D1(config-if)#standby 114 priority 150 Se establece la prioridad

- **Habilite la preferencia (preemption).**

D1(config-if)# standby 114 preempt Habilita la preferencia grupo 114

- **Rastree el objeto 4 para disminuir en 60.**

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

**Configure IPv4 HSRP grupo 124 para la VLAN 102:**

- **Asigne la dirección IP virtual 10.0.102.254.**

Con los siguientes comandos se asigna la IP virtual en la vlan 102

D1(config)#interface vlan 102

D1(config)#ip address 10.0.102.1 255.255.255.0

D1(config-if)#standby 124 ip 10.0.102.254

- **Establezca la prioridad del grupo en 150.**

D1(config)#standby 114 priority 150 Se establece la prioridad

- **Habilite la preferencia (preemption).**

D1(config-if)# standby 114 preempt Habilita la preferencia grupo 114

- **Rastree el objeto 4 para disminuir en 60.**

```
D1(config-if)# standby 124 track 4 decrement 60
```

### **Configure IPv6 HSRP grupo 106 para la VLAN 100:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 100

```
D1(config)#interface vlan 100
```

```
D1(config-if)#standby version 2
```

```
D1(config-if)#standby 106 ipv6 autoconfig
```

- **Establezca la prioridad del grupo en 150.**

```
D1(config-if)#standby 106 priority 150
```

Se establece la prioridad

- **Habilite la preferencia (preemption).**

```
D1(config-if)#standby 106 preempt
```

Habilita la preferencia grupo 106

- **Rastree el objeto 6 y decremente en 60.**

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

### **Configure IPv6 HSRP grupo 116 para la VLAN 101:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 101

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

```
D1(config-if)#standby version 2
```

```
D1(config-if)#standby 116 ipv6 autoconfig
```

- **Habilite la preferencia (preemption).**

```
D1(config-if)#standby 116 preempt
```

Habilita la preferencia grupo 116

- **Registre el objeto 6 y decremente en 60.**

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

### **Configure IPv6 HSRP grupo 126 para la VLAN 102:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 102

```
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 126 ipv6 autoconfig
```

- **Establezca la prioridad del grupo en 150.**

```
D1(config-if)#standby 126 priority 150
```

Se establece la prioridad

- **Habilite la preferencia (preemption).**

```
D1(config-if)#standby 126 preempt
```

Habilita la preferencia grupo 126

- **Rastree el objeto 6 y decremente en 60**

```
D1(config-if)#standby 126 track 6 decrement 60
```

### **En D2, configure HSRPv2.**

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.

### **Configure HSRP versión 2.**

#### **Configure IPv4 HSRP grupo 104 para la VLAN 100:**

- **Asigne la dirección IP virtual 10.0.100.254.**

Con los siguientes comandos se asigna la IP virtual en la vlan 100

```
D2(config)#interface vlan 100
D2(config)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#standby 104 ip 10.0.100.254
```

- **Habilite la preferencia (preemption).**

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

Habilita la preferencia grupo 104

- **Rastree el objeto 4 y decremente en 60.**

```
D2(config-if)#standby 104 track 6 decrement 60
```

#### **Configure IPv4 HSRP grupo 114 para la VLAN 101:**

- **Asigne la dirección IP virtual 10.0.101.254.**

Con los siguientes comandos se asigna la IP virtual en la vlan 101

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

D2(config)#ip address 10.0.101.2 255.255.255.0

D2(config-if)#standby 114 ip 10.0.101.254

- **Establezca la prioridad del grupo en 150.**

D2(config-if)#standby 114 priority 150

Se establece la prioridad

- **Habilite la preferencia (preemption).**

D2(config-if)#standby 114 preempt

Habilita la preferencia grupo 114

- **Rastree el objeto 4 para disminuir en 60.**

D2(config-if)#standby 114 track 4 decrement 60

### **Configure IPv4 HSRP grupo 124 para la VLAN 102:**

- **Asigne la dirección IP virtual 10.0.102.254.**

Con los siguientes comandos se asigna la IP virtual en la vlan 102

D2(config)#interface vlan 102

D2(config)#ip address 10.0.102.2 255.255.255.0

D2(config-if)#standby 124 ip 10.0.102.254

- **Habilite la preferencia (preemption).**

D2(config-if)#standby 124 preempt

Habilita la preferencia grupo 124

- **Rastree el objeto 4 para disminuir en 60.**

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

### **Configure IPv6 HSRP grupo 106 para la VLAN 100:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 100

D2(config)#interface vlan 100

D2(config-if)#standby version 2

D2(config-if)#standby 106 ipv6 autoconfig

- **Habilite la preferencia (preemption).**

D2(config-if)#standby 106 preempt

Habilita la preferencia grupo 106

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

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

### **Configure IPv6 HSRP grupo 116 para la VLAN 101:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 101

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

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

```
D2(config-if)#standby 116 ipv6 autoconfig
```

- **Establezca la prioridad del grupo en 150.**

```
D2(config-if)#standby 116 priority 150
```

Se establece la prioridad

- **Habilite la preferencia (preemption).**

```
D2(config-if)#standby 116 preempt
```

Habilita la preferencia grupo 116

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

```
D2(config-if)#standby 116 track 6 decrement 60
```

### **Configure IPv6 HSRP grupo 126 para la VLAN 102:**

- **Asigne la dirección IP virtual usando ipv6 autoconfig.**

Con los siguientes comandos se asigna la IP virtual en la vlan 102

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

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

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

- **Habilite la preferencia (preemption).**

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

Habilita la preferencia grupo 126

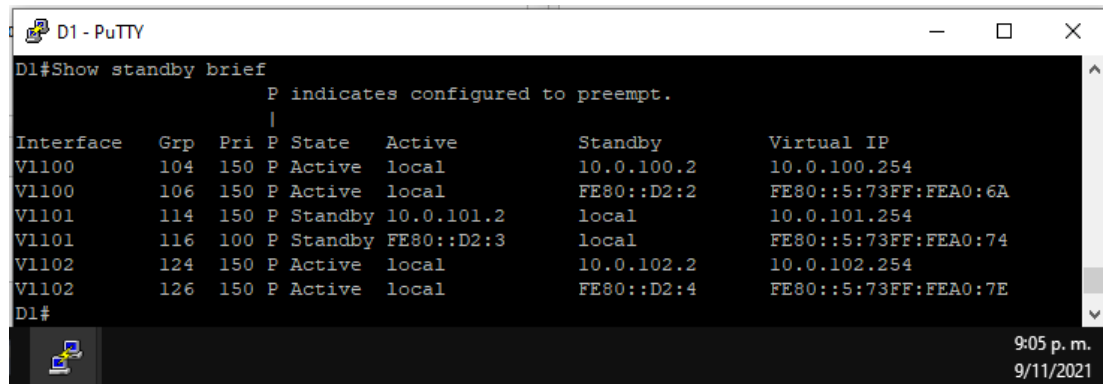
- **Rastree el objeto 6 para disminuir en 60.**

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

Se verifica las configuraciones realizadas con el comando **show standby brief** en D1 y D2

**D1:**

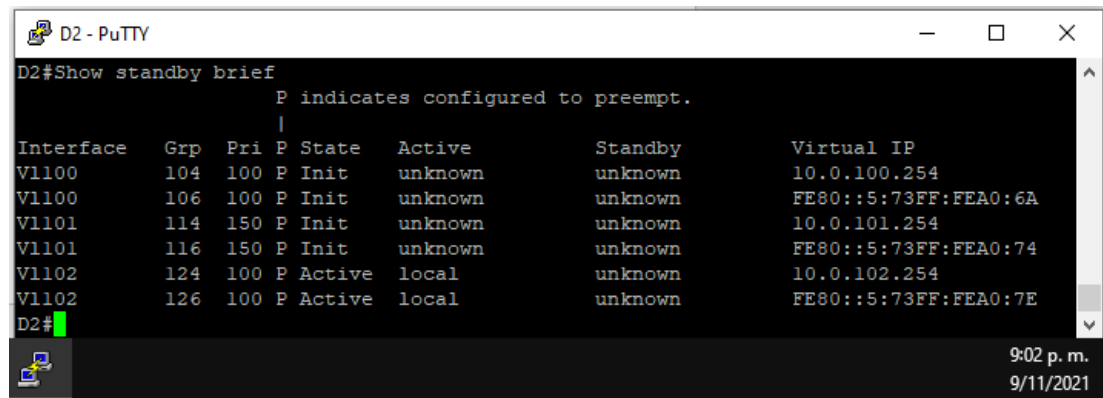
Figura 31 Configuración Redundancia del Primer Salto D1



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

D2:

Figura 32 Configuración Redundancia del Primer Salto D2



```
D2#Show standby brief
          P indicates configured to preempt.
          |
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 Active local           unknown           10.0.102.254
Vl102     126 100 P Active local           unknown           FE80::5:73FF:FEA0:7E
D2#
```

### Paso 5: Seguridad

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

Las tareas de configuración son las siguientes:

#### 5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

Contraseña: **cisco12345cisco**

Con el siguiente comando desde el modo de configuración global se habilita el EXEC privilegiado en cada uno de los dispositivos R1, R2, R3, D1, D2 y A1

R1(config)# enable algorithm-type scrypt secret cisco12345cisco

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

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

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

```
D2(config)# enable algorithm-type scrypt secret cisco12345cisco
```

```
A1(config)# enable algorithm-type scrypt secret cisco12345cisco
```

## **5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.**

Detalles de la cuenta encriptada SCRYPT:

- Nombre de usuario Local: **sadmin**
- Nivel de privilegio **15**
- Contraseña: **cisco12345cisco**

Con el siguiente comando desde el modo de configuración global se encripta las contraseñas configuradas en el anterior paso en cada uno de los dispositivos R1, R2, R3, D1, D2 y A1

```
R1(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

```
R2(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

```
R3(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

```
D1(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

```
D2(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

```
A1(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

## **5.3 En todos los dispositivos (excepto R2), habilite AAA.**

Habilite AAA.

Con el siguiente comando desde el modo de configuración global se habilita AAA en los dispositivos R1, R3, D1, D2 y A1

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

```
R3(config)# aaa new-model
```

```
D1(config)# aaa new-model
```

```
D2(config)# aaa new-model
```

```
A1(config)# aaa new-model
```

## **5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.**

Especificaciones del servidor RADIUS.:

- Dirección IP del servidor RADIUS es 10.0.100.6.
- Puertos UDP del servidor RADIUS son 1812 y 1813.
- Contraseña: **\$strongPass**

Con el siguiente comando desde el modo de configuración global se configure las especificaciones del servidor RADIUS en los dispositivos R1, R3, D1, D2 y A1

Es de resaltar que antes de hacer este paso es necesario configurar el full dúplex encada una de la interfaces donde se conectan con otros equipos con el comando **R#(config-if)#duplex full**

```
R1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
R1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
R3(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
R3(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
D1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
D1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
D2(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
D2(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
A1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
A1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

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

Especificaciones de autenticación AAA:

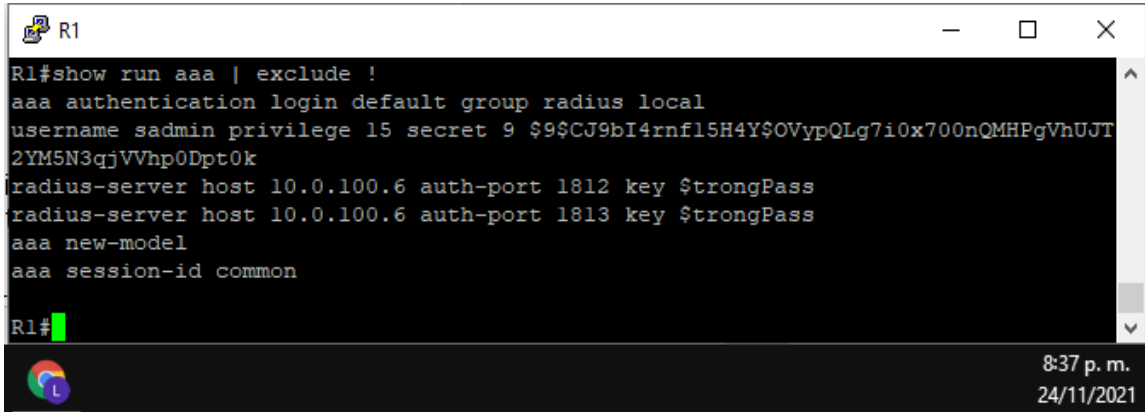
- Use la lista de métodos por defecto
- Valide contra el grupo de servidores RADIUS
- De lo contrario, utilice la base de datos local.

Con el siguiente comando desde el modo de configuración global se configure la lista de métodos de autenticación AAA en los dispositivos R1, R3, D1, D2 y A1

```
R1 (config)# aaa authentication login default group radius local
R3 (config)# aaa authentication login default group radius local
D1 (config)# aaa authentication login default group radius local
D2 (config)# aaa authentication login default group radius local
A1 (config)# aaa authentication login default group radius local
```

Ejecutando el siguiente comando **show run aaa | exclude !** se puede ver las configuraciones de seguridad en cada uno de los dispositivos R1, R2, R3, D1, D2 y A1 teniendo en cuenta que en R2 solo se crea usuario y se encripta

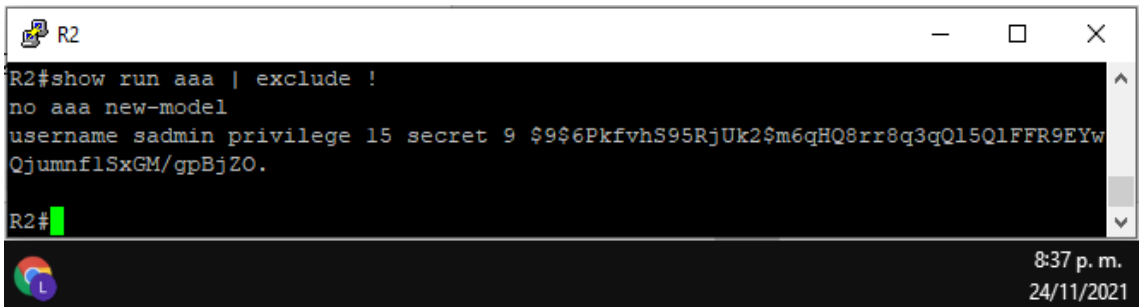
*Figura 33 Configuraciones de Seguridad en R1*

A screenshot of a terminal window titled 'R1'. The terminal shows the output of the command 'show run aaa | exclude !'. The output lists several configuration lines: 'aaa authentication login default group radius local', a username 'sadmin' with privilege 15 and a secret key, 'radius-server host 10.0.100.6 auth-port 1812 key \$strongPass', 'radius-server host 10.0.100.6 auth-port 1813 key \$strongPass', 'aaa new-model', and 'aaa session-id common'. The prompt 'R1#' is visible at the bottom left. The system tray at the bottom right shows the time '8:37 p. m.' and the date '24/11/2021'.

```
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$CJ9bI4rnf15H4Y$OVypQLg7i0x700nQMHPgVhUJT
2YM5N3qjVVhp0Dpt0k
radius-server host 10.0.100.6 auth-port 1812 key $strongPass
radius-server host 10.0.100.6 auth-port 1813 key $strongPass
aaa new-model
aaa session-id common

R1#
```

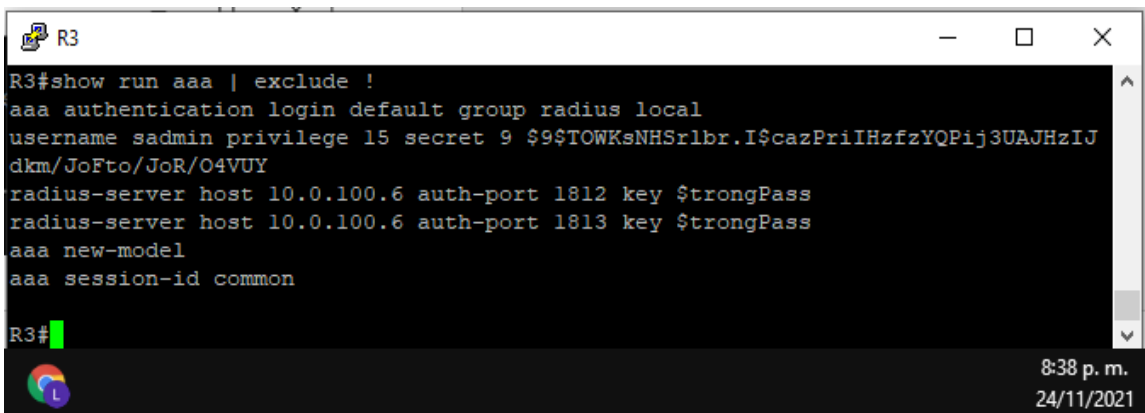
*Figura 34 Configuraciones de Seguridad en R2*

A screenshot of a terminal window titled 'R2'. The terminal shows the output of the command 'show run aaa | exclude !'. The output lists: 'no aaa new-model', a username 'sadmin' with privilege 15 and a secret key, and 'QjumnflSxGM/gpBjZO.'. The prompt 'R2#' is visible at the bottom left. The system tray at the bottom right shows the time '8:37 p. m.' and the date '24/11/2021'.

```
R2#show run aaa | exclude !
no aaa new-model
username sadmin privilege 15 secret 9 $9$6PkfvhS95RjUk2$m6qHQ8rr8q3qQ15Q1FFR9EYw
QjumnflSxGM/gpBjZO.

R2#
```

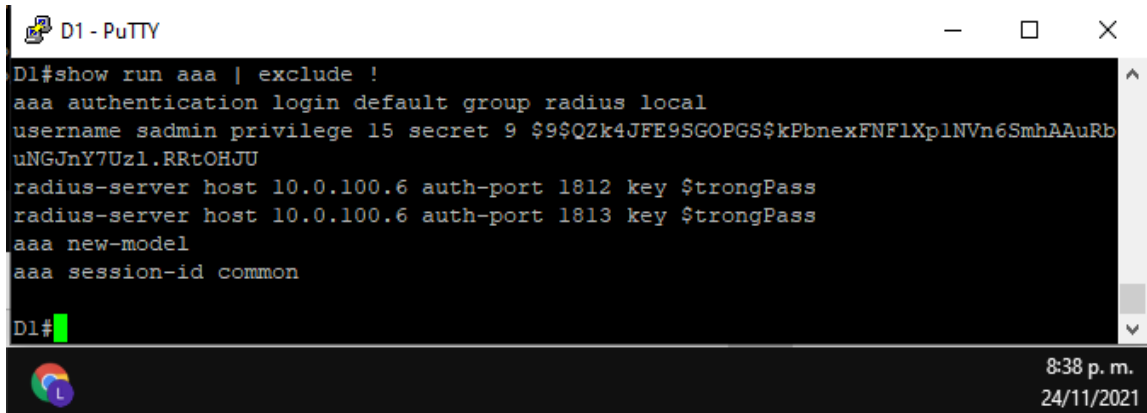
*Figura 35 Configuraciones de Seguridad en R3*

A screenshot of a terminal window titled 'R3'. The terminal shows the output of the command 'show run aaa | exclude !'. The output lists: 'aaa authentication login default group radius local', a username 'sadmin' with privilege 15 and a secret key, 'radius-server host 10.0.100.6 auth-port 1812 key \$strongPass', 'radius-server host 10.0.100.6 auth-port 1813 key \$strongPass', 'aaa new-model', and 'aaa session-id common'. The prompt 'R3#' is visible at the bottom left. The system tray at the bottom right shows the time '8:38 p. m.' and the date '24/11/2021'.

```
R3#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$TOWKsNHSrlbr.I$cazPriIHzfzYQPij3UAJHzIJ
dkm/JoFto/JoR/O4VUY
radius-server host 10.0.100.6 auth-port 1812 key $strongPass
radius-server host 10.0.100.6 auth-port 1813 key $strongPass
aaa new-model
aaa session-id common

R3#
```

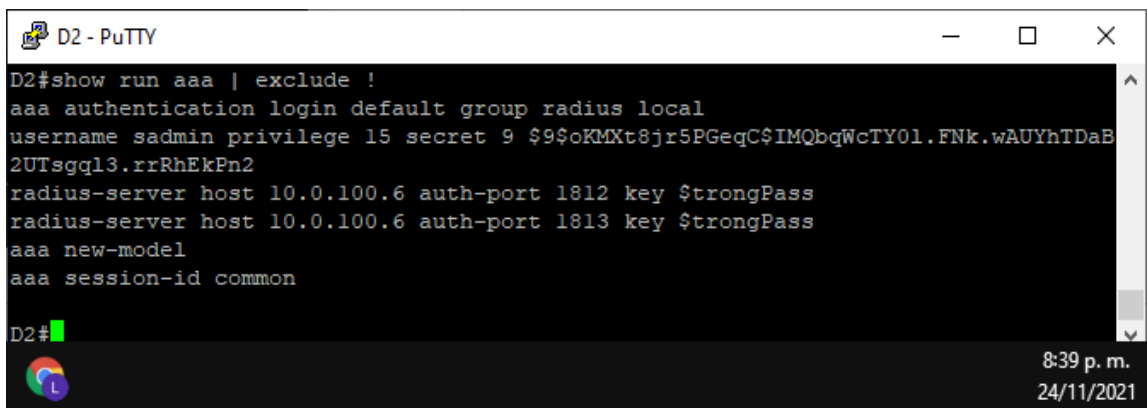
Figura 36 Configuraciones de Seguridad en D1



```
D1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$QZk4JFE9SGOPGS$kPbnexFNFlXplNVn6SmhAAuRb
uNGJnY7Uz1.RRtOHJU
radius-server host 10.0.100.6 auth-port 1812 key $strongPass
radius-server host 10.0.100.6 auth-port 1813 key $strongPass
aaa new-model
aaa session-id common
D1#
```

8:38 p. m.  
24/11/2021

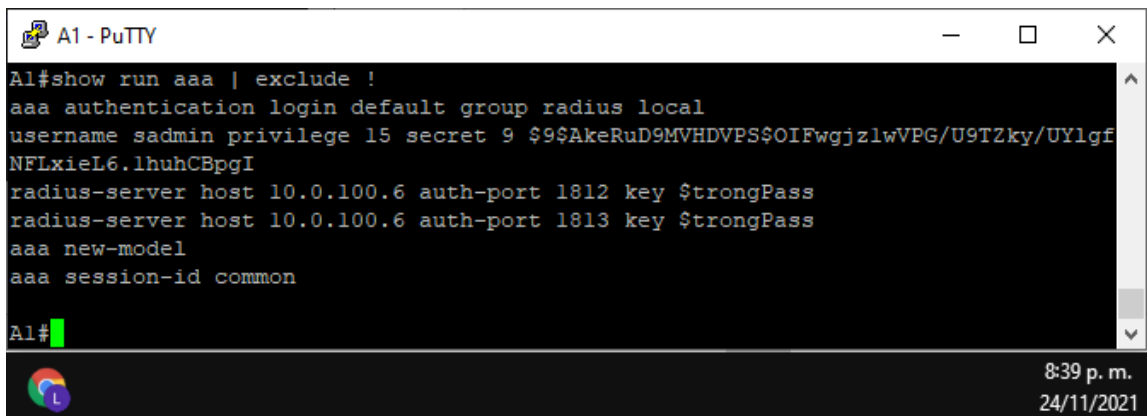
Figura 37 Configuraciones de Seguridad en D2



```
D2#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$oKMXt8jr5PGeqC$IMQbqWcTY01.FNk.wAUYhTDaB
2UTsgql3.rrRhEkPn2
radius-server host 10.0.100.6 auth-port 1812 key $strongPass
radius-server host 10.0.100.6 auth-port 1813 key $strongPass
aaa new-model
aaa session-id common
D2#
```

8:39 p. m.  
24/11/2021

Figura 38 Configuraciones de Seguridad en A1



```
A1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$AkeRuD9MVHDVPS$OIFwgjzlwVPG/U9TZky/Uylgf
NFLxieL6.lhuhCBpgI
radius-server host 10.0.100.6 auth-port 1812 key $strongPass
radius-server host 10.0.100.6 auth-port 1813 key $strongPass
aaa new-model
aaa session-id common
A1#
```

8:39 p. m.  
24/11/2021

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: sadmin y la contraseña: **cisco12345cisco**.

En el siguiente paso se verifica que los pasos anteriores estén bien configurados para ello todos los dispositivos excepto R2 deben pedir usuario y contraseña para acceder al modo de privilegiado

R1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: sadmin

Password:

R1#

*Figura 39 Verificación el servicio AAA en R1*



R3, ENCOR Skills Assessment, Scenario 1

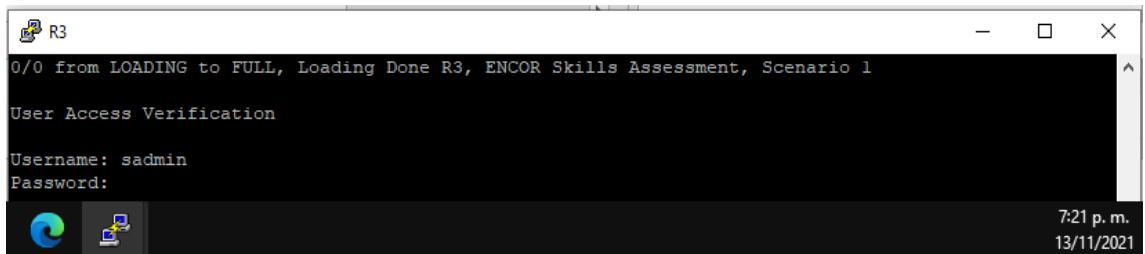
User Access Verification

Username: sadmin

Password:

R3#

*Figura 40 Verificación el servicio AAA en R3*



D1, ENCOR Skills Assessment, Scenario 1

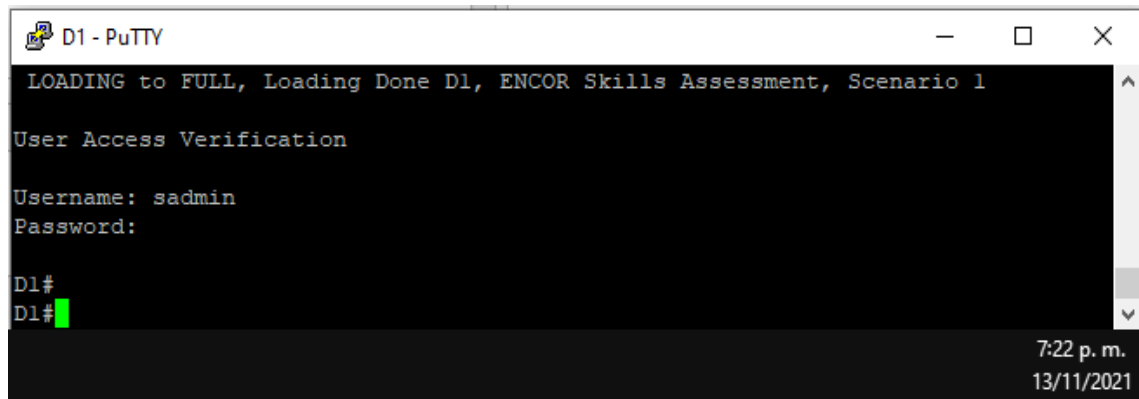
User Access Verification

Username: sadmin

Password:

D1#

*Figura 41 Verificación el servicio AAA en D1*



```
D1 - PuTTY
LOADING to FULL, Loading Done D1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
D1#
D1#
```

7:22 p. m.  
13/11/2021

D2, ENCOR Skills Assessment, Scenario 1

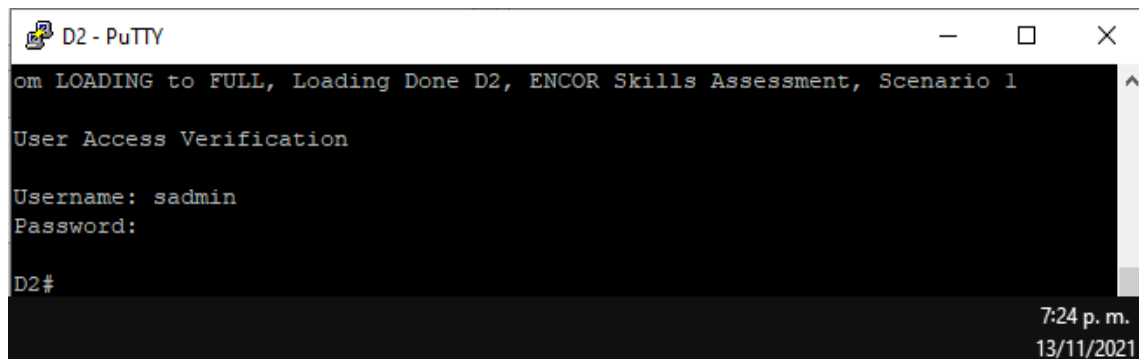
User Access Verification

Username: sadmin

Password:

D2#

*Figura 42 Verificación el servicio AAA en D2*



```
D2 - PuTTY
om LOADING to FULL, Loading Done D2, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
D2#
```

7:24 p. m.  
13/11/2021

A1, ENCOR Skills Assessment, Scenario 1

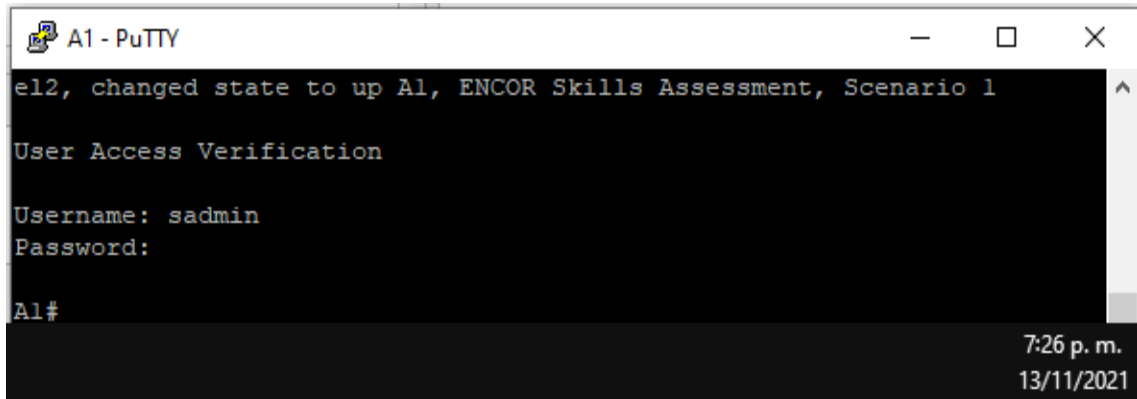
User Access Verification

Username: sadmin

Password:

A1#

Figura 43 Verificación el servicio AAA en A1



```
A1 - PuTTY
e12, changed state to up A1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
A1#
7:26 p. m.
13/11/2021
```

### Paso 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:

#### 6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.

Configure el reloj local a la hora UTC actual.

```
R1(config)#clock timezone UTC -5          Configuración hora local UTC
```

```
*Nov 13 19:40:09.575: %SYS-6-CLOCKUPDATE: System clock has been
updated from 19:40:09 UTC Sat Nov 13 2021 to 14:40:09 UTC Sat Nov 13 2021,
configured from console by sadmin on console.
```

```
R1#
```

```
*Nov 13 19:41:06.251: %SYS-5-CONFIG_I: Configured from console by sadmin
on console
```

```
R1#show clock detail
```

```
*14:41:09.331 UTC Sat Nov 13 2021
```

```
Time source is hardware calendar
```

```
R1#
```

Con el comando **show clock detail** se puede visualizar la configuración de la hora como se ve en la siguiente imagen



```
R3(config)#
```

```
*Nov 13 19:50:31.415: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:50:31 UTC Sat Nov 13 2021 to 14:50:31 UTC Sat Nov 13 2021, configured from console by sadmin on console.
```

```
R3(config)#exit
```

```
R3#
```

```
*Nov 13 19:50:35.399: %SYS-5-CONFIG_I: Configured from console by sadmin on console
```

```
R3#show clock detail
```

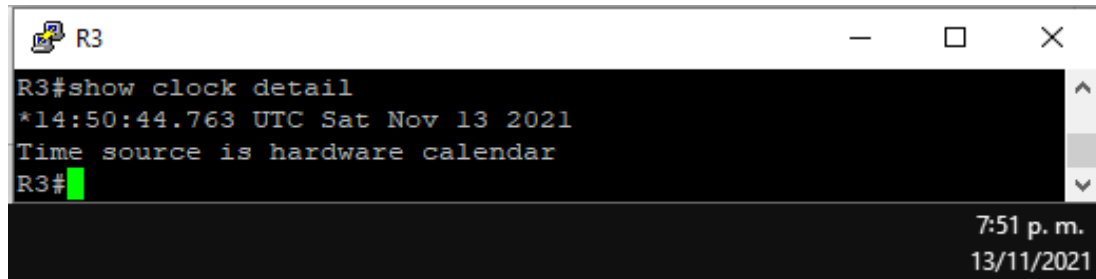
```
*14:50:44.763 UTC Sat Nov 13 2021
```

```
Time source is hardware calendar
```

```
R3#
```

Con el comando **show clock detail** se puede visualizar la configuración de la hora como se ve en la siguiente imagen

*Figura 46 Configuración reloj local hora UTC R3*



```
R3#show clock detail
*14:50:44.763 UTC Sat Nov 13 2021
Time source is hardware calendar
R3#
```

```
D1(config)#clock timezone UTC -5
```

Configuración hora local UTC

```
D1(config)#exit
```

```
D1#
```

```
*Nov 14 00:52:53.845: %SYS-5-CONFIG_I: Configured from console by sadminsole
```

```
D1#show clock detail
```

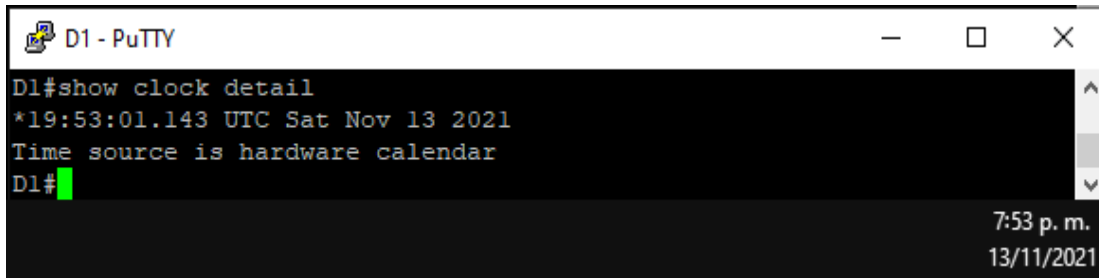
```
*19:53:01.143 UTC Sat Nov 13 2021
```

```
Time source is hardware calendar
```

```
D1#
```

Con el comando **show clock detail** se puede visualizar la configuración de la hora como se ve en la siguiente imagen

Figura 47 Configuración reloj local hora UTC D1



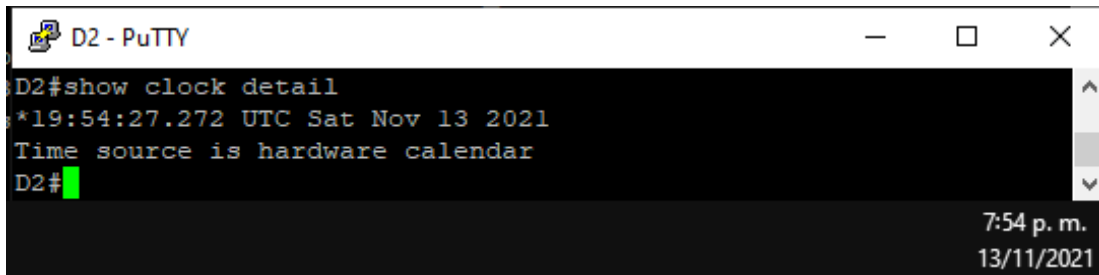
```
D1#show clock detail
*19:53:01.143 UTC Sat Nov 13 2021
Time source is hardware calendar
D1#
```

```
D2(config)#clock timezone UTC -5          Configuración hora local UTC
*Nov 14 00:54:24.031: %SYS-5-CONFIG_I: Configured from console by sadmin
on con                                     sole
```

```
D2#show clock detail
*19:54:27.272 UTC Sat Nov 13 2021
Time source is hardware calendar
D2#
```

Con el comando **show clock detail** se puede visualizar la configuración de la hora como se ve en la siguiente imagen

Figura 48 Configuración reloj local hora UTC D2



```
D2#show clock detail
*19:54:27.272 UTC Sat Nov 13 2021
Time source is hardware calendar
D2#
```

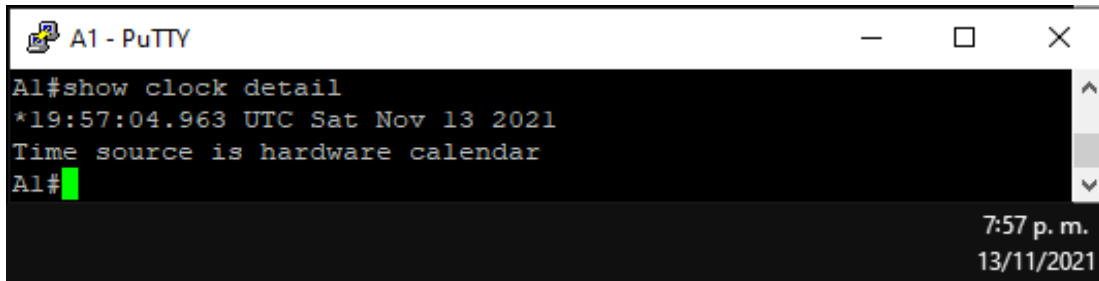
```
A1(config)#clock timezone UTC -5          Configuración hora local UTC
A1(config)#exit
```

```
A1#
*Nov 14 00:56:56.019: %SYS-5-CONFIG_I: Configured from console by sadmi
n on console
A1#show clock detail
*19:57:04.963 UTC Sat Nov 13 2021
Time source is hardware calendar
```

A1#

Con el comando **show clock detail** se puede visualizar la configuración de la hora como se ve en la siguiente imagen

*Figura 49 Configuración reloj local hora UTC A1*



```
A1 - PuTTY
A1#show clock detail
*19:57:04.963 UTC Sat Nov 13 2021
Time source is hardware calendar
A1#
```

## 6.2 Configure R2 como un NTP maestro.

Configurar R2 como NTP maestro en el nivel de estrato 3

Se aplica el siguiente **ntp master 3** comando en la configuración global del router R2 para configurarlo como NTP maestro

El número es el que le corresponda en base a la jerarquía de NTP que hemos establecido en el diseño de la red.

R2(config)#ntp master 3	Configuración NTP maestro
R2(config)#do wr	Guarda la configuración
show run   i ntp	Muestra la configuración

En la siguiente imagen se puede ver la configuración realizada NTP maestro 3 ejecutando el siguiente comando **show run | i ntp**

*Figura 50 Configuración NTP maestro 3*



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

Con el protocolo NTP se logra un sincronismo de la hora a través de redes de comunicaciones, lo que se espera entonces que la siguiente capa de sincronismo por debajo, sea ntp master 3.

## 6.3 Configure NTP en R1, R3, D1, D2, y A1

Configure NTP de la siguiente manera:

- **R1 debe sincronizar con R2.**

R1(config)#ntp server 209.165.30 Con este comando sincronizamos R1 con R2

R1(config)#do wr Guardamos la configuración

R1#show run | i ntp Muestra la configuración

*Figura 51 Configuración NTP R1*



```
R1#show run | i ntp
ntp server 209.165.30
R1#
```

8:13 p. m.  
13/11/2021

- **R3, D1 y A1 para sincronizar la hora con R1.**

R3(config)#ntp server 10.0.13.1 Con este comando sincronizamos R3 con R1

R3(config)#do wr Guardamos la configuración

R3#show run | i ntp Muestra la configuración

*Figura 52 Configuración NTP R3*



```
R3#show run | i ntp
ntp server 10.0.13.1
R3#
```

8:18 p. m.  
13/11/2021

D1(config)#ntp server 10.0.10.1 Con este comando sincronizamos D1 con R1

D1(config)#do wr Guardamos la configuración

D1#show run | i ntp Muestra la configuración

Figura 53 Configuración NTP D1



```
D1#show run | i ntp
ntp server 10.0.10.1
D1#
```

A1(config)#ntp server 10.0.10.1    Con este comando sincronizamos A1 con R1  
A1(config)#do wr    Guardamos la configuración  
A1#show run | i ntp    Muestra la configuración

Figura 54 Configuración NTP A1

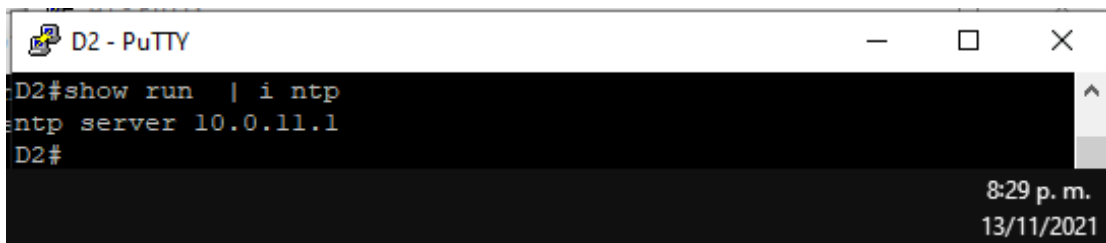


```
A1#show run | i ntp
ntp server 10.0.10.1
A1#
```

• **D2 para sincronizar la hora con R3.**

D2(config)#ntp server 10.0.11.1    Con este comando sincronizamos D2 con R3  
D2(config)#do wr    Guardamos la configuración  
D2#show run | i ntp    Muestra la configuración

Figura 55 Configuración NTP D2



```
D2#show run | i ntp
ntp server 10.0.11.1
D2#
```

**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.

R1(config)#logging 10.0.100.5	Configura syslog en R1 con la PC1
R1(config)#logging trap warning	Configura la trampa en nivel Warning
R1#show logging	Muestra la configuración

R3(config)#logging 10.0.100.5	Configura syslog en R3 con la PC1
R3(config)#logging trap warning	Configura la trampa en nivel Warning
R3#show logging	Muestra la configuración

D1(config)#logging 10.0.100.5	Configura syslog en R1 con la PC1
D1(config)#logging trap warning	Configura la trampa en nivel Warning
D1#show logging	Muestra la configuración

D2(config)#logging 10.0.100.5	Configura syslog en R1 con la PC1
D2(config)#logging trap warning	Configura la trampa en nivel Warning
D2#show logging	

A1(config)#logging 10.0.100.5	Configura syslog en R1 con la PC1
A1(config)#logging trap warning	Configura la trampa en nivel Warning
A1#show logging	Muestra la configuración

## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

**R1:**

• **Únicamente se usará SNMP en modo lectura (Read-Only).**

R1(config)#snmp-server community ENCORSA ro ACL_SNMP	Solo lectura
--	--------------

• **Limite el acceso SNMP a la dirección IP de la PC1.**

R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	
---	--

R1(config)# snmp-server location NETFLOW Collector	
--	--

R1(config)#ip access-list standard ACL_SNMP	
---	--

R1(config-std-nacl)#permit 10.0.100.5	Otorga permisos a PC1
---------------------------------------	-----------------------

• **Configure el valor de contacto SNMP con su nombre.**

R1(config-std-nacl)#snmp-server contact SNMP Manager	Asigna nombre
--	---------------

- Establezca el community string en **ENCORSA**.

R1(config)#do wr

Guardamos la configuración

R1#show snmp

Muestra la configuración

*Figura 56 Configuración SNMPv2c en R1*

```

R1#sh snmp
Chassis: 4279256517
Contact: SNMP Manager
Location: NETFLOW Collector
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP Dispatcher:
  queue 0/75 (current/max), 0 dropped
SNMP Engine:
  queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
  Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
R1#
  
```

**R3:**

R3(config)#snmp-server community ENCORSA ro ACL\_SNMP

Solo lectura

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

R3(config)#snmp-server location NETFLOW Collector

R3(config)#ip access-list standard ACL\_SNMP

R3(config-std-nacl)#permit 10.0.100.5

Otorga permisos a PC1

R3(config-std-nacl)#snmp-server contact SNMP Manager

Asigna nombre

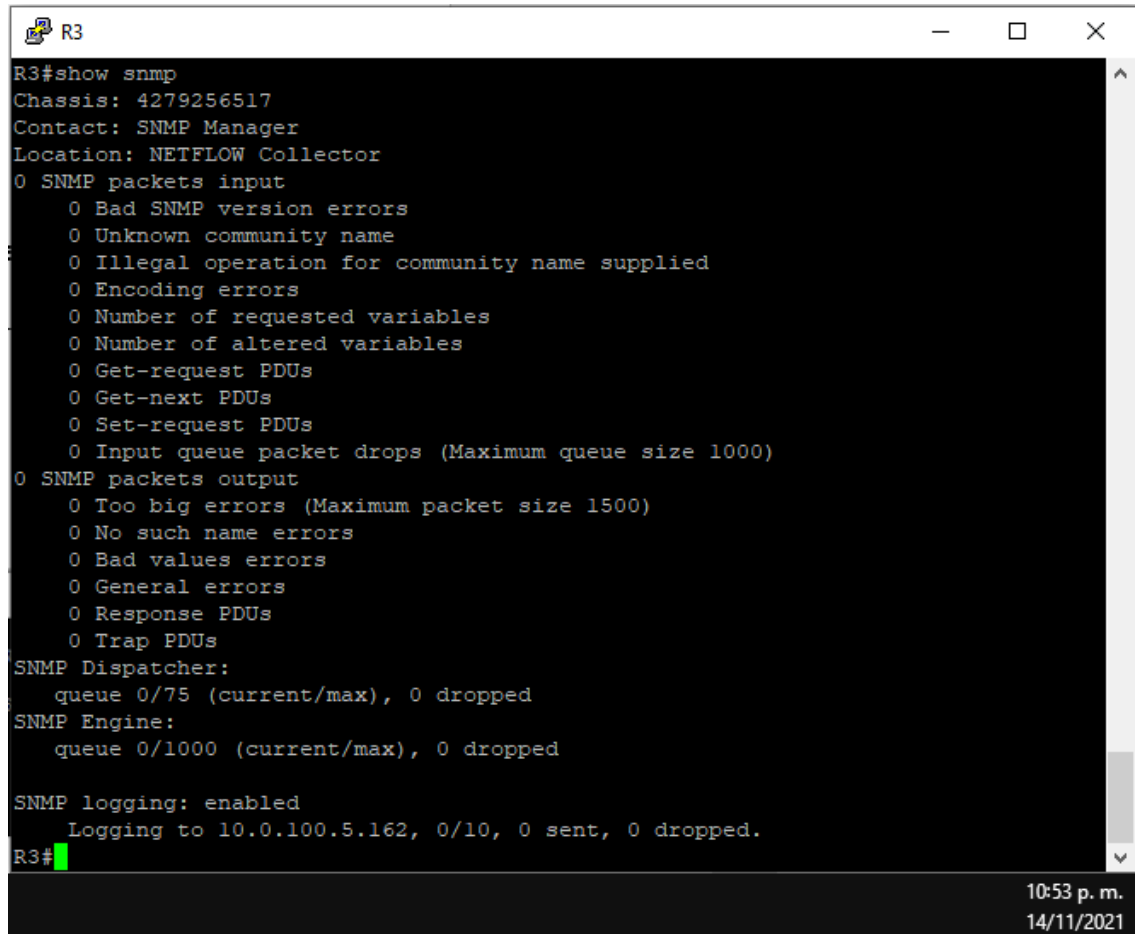
R3(config)#do wr

Guardamos la configuración

R3#show snmp

Muestra la configuración

Figura 57 Configuración SNMPv2c en R3



```
R3#show snmp
Chassis: 4279256517
Contact: SNMP Manager
Location: NETFLOW Collector
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP Dispatcher:
  queue 0/75 (current/max), 0 dropped
SNMP Engine:
  queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
  Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
R3#
```

**D1:**

D1(config)#snmp-server community ENCORSA ro ACL\_SNMP Solo lectura

D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA

D1(config)#snmp-server location NETFLOW Collector

D1(config)#ip access-list standard ACL\_SNMP

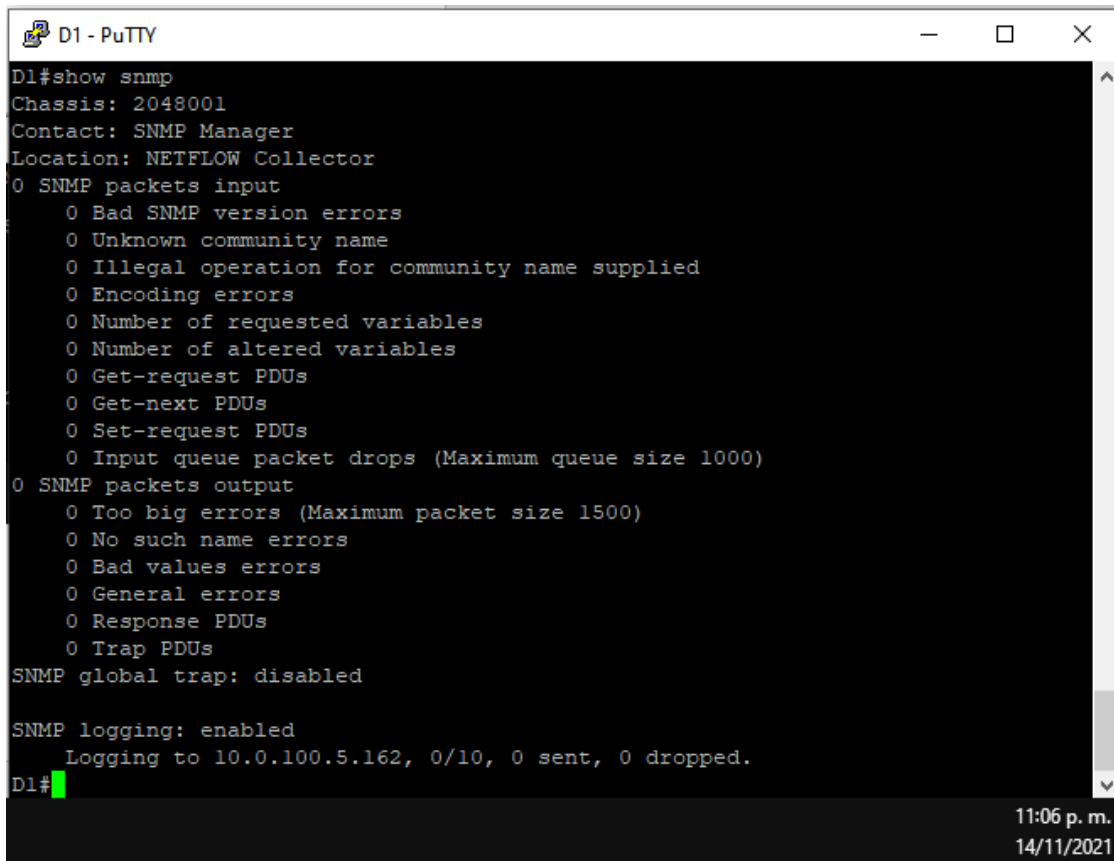
D1(config-std-nacl)#permit 10.0.100.5 Otorga permisos a PC1

D1(config-std-nacl)#snmp-server contact SNMP Manager Asigna nombre

D1(config)#do wr Guardamos la configuración

D1#show snmp Muestra la configuración

Figura 58 Configuración SNMPv2c en D1



```
D1 - PuTTY
D1#show snmp
Chassis: 2048001
Contact: SNMP Manager
Location: NETFLOW Collector
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled

SNMP logging: enabled
  Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
D1#
```

11:06 p. m.  
14/11/2021

**D2:**

D2(config)#snmp-server community ENCORSA ro ACL\_SNMP      Solo lectura  
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA  
D2(config)#snmp-server location NETFLOW Collector  
D2(config)#ip access-list standard ACL\_SNMP  
D2(config-std-nacl)#permit 10.0.100.5      Otorga permisos a PC1  
D2(config-std-nacl)#snmp-server contact SNMP Manager      Asigna nombre  
D2(config)#do wr      Guardamos la configuración  
D2#show snmp      Muestra la configuración

Figura 59 Configuración SNMPv2c en D2

```
D2 - PuTTY
D2#show snmp
Chassis: 2048002
Contact: SNMP Manager
Location: NETFLOW Collector
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled

SNMP logging: enabled
  Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
D2#
```

11:09 p. m.  
14/11/2021

**A1:**

- A1(config)#snmp-server community ENCORSAS ro ACL\_SNMP Solo lectura
- A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSAS
- A1(config)#snmp-server location NETFLOW Collector
- A1(config)#ip access-list standard ACL\_SNMP
- A1(config-std-nacl)#permit 10.0.100.5 Otorga permisos a PC1
- A1(config-std-nacl)#snmp-server contact SNMP Manager Asigna nombre
- A1(config)#do wr Guardamos la configuración
- A1#show snmp Muestra la configuración

Figura 60 Configuración SNMPv2c en A1

```
A1-PuTTY
A1#show snmp
Chassis: 2048003
Contact: SNMP Manager
Location: NETFLOW Collector
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled

SNMP logging: enabled
Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
A1#
```

11:12 p. m.  
14/11/2021

• En R3, D1, y D2, habilite el envío de traps config y ospf.

R3(config)#snmp-server enable traps config      Habilita trampas de configuración  
R3(config)#snmp-server enable traps ospf              Habilita trampas de ospf  
R3(config)#do wr

D1(config)#snmp-server enable traps config      Habilita trampas de configuración  
D1(config)#snmp-server enable traps ospf              Habilita trampas de ospf  
D1(config)#do wr

D2(config)#snmp-server enable traps config      Habilita trampas de configuración  
A1(config)#snmp-server enable traps ospf              Habilita trampas de ospf  
D2(config)#do wr



## CONCLUSIONES

Por medio de la practica realizada se logra entender mejor la funcionalidad de cada uno de los comandos usados en las configuraciones e interiorizando los conceptos más importantes en los procesos enrutamiento estáticos y dinámicos optimizando la red y tiempos de convergencia.

El uso de las VLAN ayuda a establecer una mejor comunicación y envío de información entre varias subredes independientes dentro de la misma red física con la ayuda del direccionamiento de los switches a través de sus direcciones IP.

Los enlaces troncales permiten crear rutas alternas de comunicación para los dispositivos que transportan más de una VLAN y así extenderlas a través de toda la red

En la práctica desarrollada se puede evidenciar que los protocolos de enrutamiento como OSPF y BGP son muy importantes ya que permiten diferentes alternativas de comunicación, estableciendo direccionamiento IPv4 e IPv6 con máscaras de red; además de esto puede establecer configuraciones relación de vecinos y address-family

Cuando se emplea el protocolo DHCP en la red este permite que los equipos como los PCs obtengan direccionamiento automático a través del comando ip dhcp.

El uso del software GNS3 proporciona muchas alternativas en la creación de topologías de redes permitiendo el uso de equipos con características muy similares a los reales, sin embargo, también hay decir que al momento de configurarlos genera bastantes inconvenientes con las versiones de IOS ya que algunos no admiten comandos más avanzados y es un poco tedioso conseguirlos

## BIBLIOGRAFÍA

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1>

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#5>

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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