

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**OSCAR ANDRÉS RAMIREZ SERNA**

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**OSCAR ANDRÉS RAMIREZ SERNA**

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

\_\_\_\_\_  
Firma del Presidente del Jurado

\_\_\_\_\_  
Firma del Jurado

\_\_\_\_\_  
Firma del Jurado

MEDELLÍN, 29 de noviembre de 2021

## **AGRADECIMIENTOS**

Este trabajo realizado se lo dedico a mi hija Julieta Ramírez Sosa, por ser el motivo principal por el que emprendí el camino de estudiar ingeniería de telecomunicaciones, a mi instructor Juan David Londoño del SENA quién me inspiró y transmitió la pasión por el mundo de las tecnologías de la información, redes y seguridad. Por otro lado también me dirijo a los señores tutores de la universidad UNAD, a quienes expreso mi más profunda gratitud, por brindarme el apoyo en cada una de áreas que intervinieron con su supervisión.

## CONTENIDO

AGRADECIMIENTOS .....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	11
RESUMEN .....	12
ABSTRACT .....	13
INTRODUCCIÓN.....	14
DESARROLLO .....	16
1. Parte 1: Construir la red y configurar los parámetros básicos .....	16
2. Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	26
3. Parte 3: Configurar los protocolos de enrutamiento .....	46
4. Parte 4: Configurar la Redundancia del Primer Salto .....	56
5. Parte 5: Seguridad .....	69
6. Parte 6: Configure las funciones de Administración de Red .....	72
CONCLUSIONES .....	78
BIBLIOGRAFÍA.....	79

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	15
--	----

## LISTA DE FIGURAS

Figura 1. Escenario 1 .....	15
Figura 2. Simulación de escenario 1 .....	16
Figura 3. Direccionamiento interfaces R1 .....	17
Figura 4. Direccionamiento interfaces R2 .....	18
Figura 5. Direccionamiento interfaces R3 .....	19
Figura 6. Direccionamiento interfaces D1 .....	22
Figura 6. Direccionamiento interfaces D2 .....	24
Figura 7. Direccionamiento interfaces A1 .....	25
Figura 8. Direccionamiento estático PC1 .....	25
Figura 9. Direccionamiento estático PC4 .....	26
Figura 10. Interfaces troncales D1 .....	28
Figura 11. Interfaces troncales D2 .....	30
Figura 12. Interfaces troncales A1 .....	32
Figura 13. RSTP habilitado en D1 .....	34
Figura 14. RSTP habilitado en D2 .....	35
Figura 15. RSTP habilitado en A1 .....	35
Figura 16. Prioridad puente raíz en D1 .....	36
Figura 17. Prioridad puente raíz en D2 .....	37
Figura 18. Port-channel en D1 .....	38
Figura 19. Port-channel en D2 .....	39
Figura 20. Port-channel en A1 .....	40
Figura 21. Verificación servicio DHCP PC2 .....	41

Figura 22. Verificación servicio DHCP PC3 .....	42
Figura 23. Verificación conectividad PC1-D1 .....	42
Figura 24. Verificación conectividad PC1-D2 .....	42
Figura 25. Verificación conectividad PC1-PC4 .....	43
Figura 26. Verificación conectividad PC2-D1 .....	43
Figura 27. Verificación conectividad PC2-D1 .....	43
Figura 28. Verificación conectividad PC3-D1 .....	44
Figura 29. Verificación conectividad PC3-D2 .....	44
Figura 30. Verificación conectividad PC4-D1 .....	44
Figura 31. Verificación conectividad PC4-D2 .....	45
Figura 32. Verificación conectividad PC4-PC1 .....	45
Figura 33. Verificación OSPF v2 en R1 .....	46
Figura 34. Verificación OSPF v2 en R3 .....	47
Figura 35. Verificación OSPF v2 en D1 .....	48
Figura 36. Verificación OSPF v2 en D2 .....	49
Figura 37. Verificación OSPF v3 en R1 .....	50
Figura 38. Verificación OSPF v3 en R3 .....	51
Figura 39. Verificación OSPF v3 en D1 .....	52
Figura 40. Verificación OSPF v3 en D2 .....	53
Figura 41. Verificación BGP en R2.....	54
Figura 42. Verificación BGP en R1.....	55
Figura 43. Verificación IP SLA 4 en D1 .....	57
Figura 44. Verificación IP SLA 6 en D1 .....	57
Figura 45. Evento interfaz G1/0 de R1 indisponible .....	57



Figura 46. Evento interfaz G1/0 de R1 disponible .....	58
Figura 47. Verificación IP SLA 4 en D2 .....	59
Figura 48. Verificación IP SLA 6 en D2 .....	59
Figura 49. Evento interfaz G0/0 de R3 indisponible .....	59
Figura 50. Evento interfaz G0/0 de R3 disponible .....	60
Figura 51. Verificación HSRP VLAN 100 en D1 .....	60
Figura 52. Verificación HSRP VLAN 101 en D1 .....	61
Figura 53. Verificación HSRP VLAN 101 en D1 .....	62
Figura 54. Verificación HSRP VLAN 100 IPV6 en D1 .....	62
Figura 55. Verificación HSRP VLAN 101 IPV6 en D1 .....	63
Figura 56. Verificación HSRP VLAN 102 IPV6 en D1 .....	64
Figura 57. Verificación HSRP VLAN 100 IPV4 en D2 .....	65
Figura 58. Verificación HSRP VLAN 101 IPV4 en D2 .....	65
Figura 59. Verificación HSRP VLAN 102 IPV4 en D2 .....	66
Figura 60. Verificación HSRP VLAN 100 IPV6 en D2 .....	67
Figura 61. Verificación HSRP VLAN 101 IPV6 en D2 .....	67
Figura 62. Verificación HSRP VLAN 102 IPV6 en D2 .....	68
Figura 63. Configuración servidor radius en R1 .....	70
Figura 64. Configuración servidor radius en R3 .....	70
Figura 65. Configuración servidor radius en D1 .....	70
Figura 66. Configuración servidor radius en D2 .....	71
Figura 67. Configuración servidor radius en A1 .....	71
Figura 68. Verificación hora en R1 .....	72
Figura 69. Verificación hora en R2 .....	72

Figura 70. Verificación hora en R3 .....	72
Figura 71. Verificación hora en D1 .....	72
Figura 72. Verificación hora en D2 .....	73
Figura 73. Verificación hora en A1 .....	73
Figura 74. Verificación NTP en R2 .....	73
Figura 75. Verificación asociaciones NTP en R1 .....	74
Figura 76. Verificación asociaciones NTP en R3 .....	74
Figura 77. Verificación asociaciones NTP en D1 .....	75
Figura 78. Verificación asociaciones NTP en D2 .....	75
Figura 79. Configuración syslog R1 .....	76
Figura 80. Configuración syslog R3 .....	76
Figura 81. Configuración syslog D1 .....	76
Figura 82. Configuración syslog D2 .....	76

## GLOSARIO

**VTP:** son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

**OSPF:** Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos, OSPF funciona formando adyacencias con los dispositivos vecinos que estén ejecutando la misma versión de OSPF. Este protocolo crea y mantiene tres bases de datos base de datos de adyacencia: crea la tabla de vecinos, base de datos de estado de enlace (LSDB): crea la tabla de topología y base de datos de reenvío: crea la tabla de enrutamiento.

**IPv6:** en inglés, Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet. Con la transición de IPv4 a IPv6 se conseguirán un montón de mejoras que influyen en bastantes aspectos como seguridad, facilidad de unirse a una red, etc. El aporte de una cantidad enorme de direcciones, hará posible que internet crezca y permitirá por ejemplo, el desarrollo de la industria 4.0 y del internet de las cosas.

**EtherChannel:** es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet.[cita requerida] Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad. Además proporcionar enlaces de alta velocidad y también tiene la característica de redundancia a nivel de puerto.

**HSRP:** es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos (single point of failure) en la red mediante técnicas de redundancia y comprobación del estado de los routers. Evitar puntos únicos de fallo en la red es muy importante para dotar de alta disponibilidad al servicio de red.

## RESUMEN

En el siguiente Informe, se desarrolla escenario propuesto en seis partes con el propósito de aplicar todos los conocimientos y habilidades prácticas obtenidas en el estudio de diplomado de profundización Cisco CCNP, en el documento encontramos una descripción detallada de las configuraciones realizadas en el desarrollo del laboratorio con la respectiva evidencia de su correcto funcionamiento.

El escenario completo se desarrolla sobre la plataforma de simulación GNS3 que proporciona un completo set de características que permiten simular lo más real posible el escenario implementado, para las primeras tres partes del proyecto que abarcan la conmutación y enrutamiento, se configuraron protocolos como BGP, OSPF, HSRP, IPv4, IPv6, VTP, VLAN y DHCP. Las partes 4, 5 y 6 se enfocan en implementar seguridad para las redes a nivel de confidencialidad y disponibilidad, se configuran protocolos como HSRP, AAA, SNMP y NTP.

En el escenario encontraremos 3 dispositivos enrutadores, dos conmutadores capa 3 y un conmutador capa 2. El cual busca desarrollar en el estudiante competencias y habilidades en el manejo de configuración y administración de dispositivos de electrónica como enrutadores y conmutadores en un entorno basado en solución de problemas que permitan incorporar habilidades para posteriores encuentros con dispositivos e infraestructuras reales.

Palabras Clave: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

## **ABSTRACT**

In the following Report, a proposed scenario is developed in six parts with the purpose of applying all the knowledge and practical skills obtained in the study of the Cisco CCNP in-depth diploma, in the document we find a detailed description of the configurations made in the development of the laboratory with the respective evidence of its correct operation.

The complete scenario is developed on the GNS3 simulation platform that provides a complete set of characteristics that allow to simulate the implemented scenario as real as possible, for the first three project parts that cover switching and routing protocols such as BGP, OSPF, HSRP were configured, IPV4, IPV6, VTP, VLAN and DHCP. Parts 4, 5 and 6 focus on implementing networking security at the level of confidentiality and availability, protocols such as HSRP, AAA, SNMP and NTP are configured.

In the scenario we will find 3 router devices, two layer 3 switches and one layer two switch. Which seeks to develop in the student skills and abilities in managing the configuration and administration of electronics devices such as routers and switches in an environment based on problem solving that incorporates skills for subsequent encounters with real devices and infrastructures.

Keywords: CISCO, CCNP, ROUTING, SWICTHING, NETWORKING, ELECTRONICS.

## INTRODUCCIÓN

El presente trabajo se desarrolla para abordar de manera práctica los conceptos aprendidos en el diplomado de profundización CCNP. Para llevar a cabo la actividad se planteó un escenario en el que se abarca todos los conceptos divididos en 6 partes aplicativas, En las cuales se pretende simular la operación de los protocolos de conmutación, enrutamiento y alta disponibilidad.

En el escenario propuesto se implementa 3 dispositivos enrutadores, R2 simulará la red ISP, R1 y R3 simularan los enrutadores de la red de la compañía en los que se configuran protocolos de enrutamiento como OSPF y BGP, además se establecerá direccionamiento IPV4 e IPV6, y el protocolo de redundancia de Gateway HSRP el cual tiene por propósito mantener la disponibilidad a nivel puerta de enlace para garantizar conectividad con redes externas.

Para la parte conmutación se construye una arquitectura contraída en la que se utilizan dos conmutadores D1 y D2 como conmutadores de núcleo y distribución a la vez, en los que se implementa segmentación, STP, VTP, port-channel, direccionamiento IPV6 e IPV4, enrutamiento dinámico y servidores DHCP. Para la red de acceso se utiliza un conmutador capa dos que se denominó A1.

Figura 1. Escenario 1

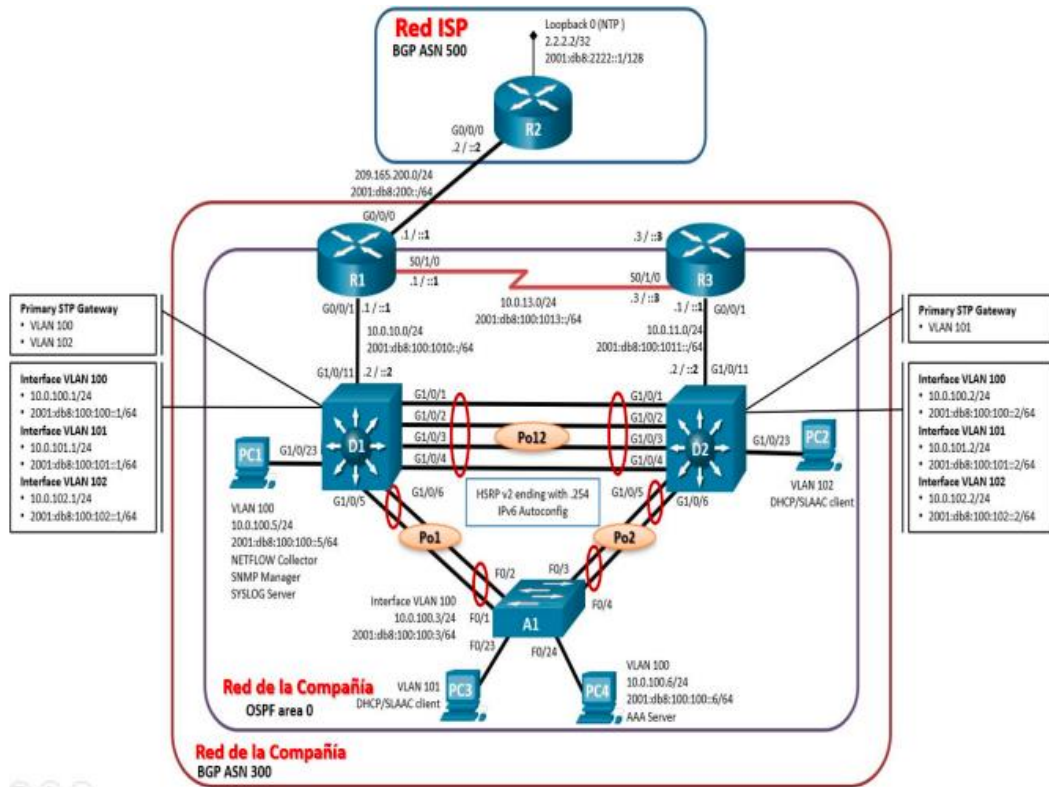


Tabla 1. Tabla de direccionamiento

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



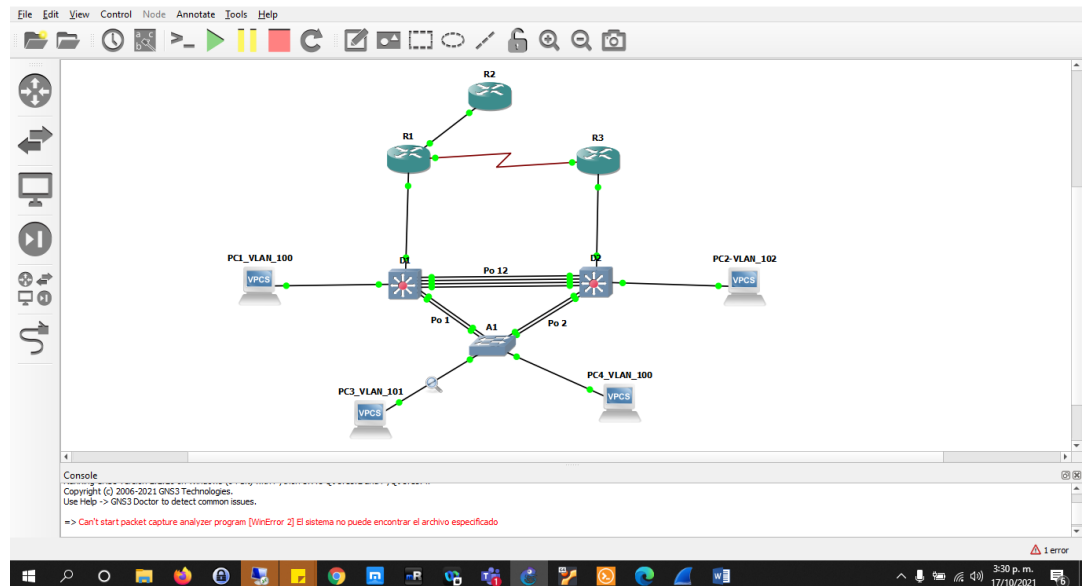
## DESARROLLO

### 1. Parte 1: Construir la red y configurar los parámetros básicos

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

Se construye la topología en el simulador GNS3 según el diseño propuesto en el documento oficial, se agregan los dispositivos enrutadores R1, R2 y R3, se agregan dos conmutadores capa 3 y un conmutador capa 2 y los respectivos equipos finales.

Figura 2. Simulación de escenario 1



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

Se procede a configurar los parámetros básicos para los dispositivos R1, R2, R3, D1, D2 y A1, tales como nombres, líneas VTY, interfaces direccionamiento, banner de ingreso, VLANs entre otros.

#### Router R1

##### Comando

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR
Skills Assessment, Scenario 1 #
line con 0 exec-timeout 0 0
logging synchronous
exit
```

##### Explicación

*Establece el nombre del dispositivo*  
*Habilita el enrutamiento IPV6*  
*Deshabilita la traducción de nombres*  
*Establece un mensaje para cuando se inicia en el modo privilegiado*  
*Establece para línea de consola el time out de 0 minutos y 0 segundos.*

```

interface GigabitEthernet1/0
ip address 10.0.10.1
255.255.255.0
negotiation auto
ipv6 address FE80::1:2 link-
local
ipv6 address
2001:DB8:100:1010::1/64
ospfv3 6 ipv6 area 0

```

*Configuración de la interface con su correspondiente direccionamiento IPV4 e IPV6 y publicación OSPF versión 3.*

```

interface GigabitEthernet2/0
ip address 209.165.200.225
255.255.255.224
negotiation auto
ipv6 address FE80::1:1 link-
local
ipv6 address
2001:DB8:200::1/64
ospfv3 6 ipv6 area 0

```

*Configuración de la interface con su correspondiente direccionamiento IPV4 e IPV6 y publicación OSPF versión 3.*

```

interface Serial4/1
ip address 10.0.13.1
255.255.255.0
ipv6 address FE80::1:3 link-
local
ipv6 address
2001:DB8:100:1013::1/64
serial restart-delay 0

```

*Configuración de la interface con su correspondiente direccionamiento IPV4 e IPV6*

Figura 3. Direccionamiento interfaces R1

```

R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          unassigned      YES NVRAM    administratively down  down
GigabitEthernet1/0       10.0.10.1       YES NVRAM    up          up
GigabitEthernet2/0       209.165.200.225 YES NVRAM    up          up
Serial4/0                 unassigned      YES NVRAM    administratively down  down
Serial4/1                 10.0.13.1       YES NVRAM    up          up
Serial4/2                 unassigned      YES NVRAM    administratively down  down
Serial4/3                 unassigned      YES NVRAM    administratively down  down
R1#

```

The screenshot shows a terminal window with the Solar-PuTTY logo and version information. The system tray at the bottom indicates the time is 12:48 p. m. on 27/11/2021.

## Router R2

Comando	Explicación
hostname R2	<i>Establece el nombre del dispositivo</i>
ipv6 unicast-routing	<i>Habilita el enrutamiento IPV6</i>
no ip domain lookup	<i>Deshabilita la traducción de nombres</i>
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	<i>Establece un mensaje para cuando se inicia en el modo privilegiado</i>
line con 0 exec-timeout 0 0 logging synchronous exit	<i>Establece para línea de consola el time out de 0 minutos y 0 segundos.</i>
interface Loopback0 ip address 2.2.2.2 255.255.255.255 ipv6 address FE80::2:3 link- local ipv6 address 2001:DB8:2222::1/128	<i>Configuración de interface loopback con su correspondiente direccionamiento IPV4 e IPV6</i>
interface GigabitEthernet0/0 ip address 209.165.200.226 255.255.255.224 duplex full speed 1000 media-type gbic negotiation auto ipv6 address FE80::2:1 link- local ipv6 address 2001:DB8:200::2/64	<i>Configuración de interface GigabitEthernet con su correspondiente direccionamiento IPV4 e IPV6</i>

Figura 4. Direccionamiento interfaces R2

```
R2(config)#end
R2#
Nov 25 17:17:19.731: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
Ethernet0/0              unassigned     YES NVRAM   administratively down  down
GigabitEthernet0/0      209.165.200.226 YES NVRAM   up          up
Loopback0                2.2.2.2       YES NVRAM   up          up
R2#
```

## Router R3

### Comando

```
hostname R3
ipv6 unicast-routing
no ip domain lookup

banner motd # R3, ENCOR Skills
Assessment, Scenario 1 #

line con 0 exec-timeout 0 0
logging synchronous
exit

interface GigabitEthernet0/0
ip address 10.0.11.1
255.255.255.0
duplex full
speed 1000
media-type gbic
negotiation auto
ipv6 address FE80::3:2 link-local
ipv6 address
2001:DB8:100:1011::1/64
ospfv3 6 ipv6 area 0

interface Serial1/0
ip address 10.0.13.3
255.255.255.0
ipv6 address FE80::3:3 link-local
ipv6 address
2001:DB8:100:1010::2/64
serial restart-delay 0
```

### Explicación

*Establece el nombre del dispositivo*  
*Habilita el enrutamiento IPV6*

*Deshabilita la traducción de nombres*

*Establece un mensaje para cuando se inicia en el modo privilegiado*

*Establece para línea de consola el time out de 0 minutos y 0 segundos.*

*Se configura la interface GigabitEthernet0/0 con su respectivo direccionamiento IPV4 e IPV6, adicional se habilita la interface en ospfv3 para el área 0.*

*Se configura la interface Serial1/0 con su respectivo direccionamiento IPV4 e IPV6.*

Figura 5. Direccionamiento interfaces R3

```
R3#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        unassigned      YES NVRAM    administratively down  down
GigabitEthernet0/0 10.0.11.1       YES NVRAM    up          up
Serial1/0          10.0.13.3       YES NVRAM    up          up
Serial1/1          unassigned      YES NVRAM    administratively down  down
Serial1/2          unassigned      YES NVRAM    administratively down  down
Serial1/3          unassigned      YES NVRAM    administratively down  down
R3#
```

## Switch D1

<b>Comando</b>	<b>Explicación</b>
hostname D1	<i>Establece el nombre del dispositivo</i>
ipv6 unicast-routing	<i>Habilita el enrutamiento IPV6</i>
no ip domain lookup	<i>Deshabilita la traducción de nombres</i>
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	<i>Establece un mensaje para cuando se inicia en el modo privilegiado</i>
line con 0 exec-timeout 0 0 logging synchronous exit	<i>Establece para línea de consola el time-out de 0 minutos y 0 segundos.</i>
vlan 100 name Management	<i>Crea la VLAN 100 con su respectivo nombre</i>
vlan 101 name UserGroupA	<i>Crea la VLAN 101 con su respectivo nombre</i>
vlan 102 name UserGroupB	<i>Crea la VLAN 102 con su respectivo nombre</i>
vlan 999 name NATIVE	<i>Crea la VLAN 999 con su respectivo nombre</i>
interface Ethernet1/1 no switchport ip address 10.0.10.2 255.255.255.0 ipv6 address FE80::D1:1 link- local ipv6 address 2001:DB8:100:1010::2/64	<i>Configuración Ethernet1/1 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6.</i>
interface Vlan100 ip address 10.0.100.1 255.255.255.0 ipv6 address FE80::D1:2 link- local ipv6 address 2001:DB8:100:100::1/64 ospfv3 6 ipv6 area 0	<i>Configuración interface VLAN 100 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.</i>

```
interface Vlan101
 ip address 10.0.101.1
 255.255.255.0
 ipv6 address FE80::D1:3 link-
 local
 ipv6 address
 2001:DB8:100:101::1/64
 ospfv3 6 ipv6 area 0
```

*Configuración interface VLAN 101 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.*

```
interface Vlan102
 ip address 10.0.102.1
 255.255.255.0
 ipv6 address FE80::D1:4 link-
 local
 ipv6 address
 2001:DB8:100:102::1/64
 ospfv3 6 ipv6 area 0
```

*Configuración interface VLAN 102 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.*

```
ip dhcp pool VLAN-102
 network 10.0.102.0
 255.255.255.0
 default-router 10.0.102.254
```

*Se configuran los pools de direccionamiento para las VLANs 101 y 102 con su respectiva mascara y puerta de enlace predeterminada.*

```
ip dhcp pool VLAN-101
 network 10.0.101.0
 255.255.255.0
 default-router 10.0.101.254
```

```
ip dhcp excluded-address
 10.0.101.1 10.0.101.109
 ip dhcp excluded-address
 10.0.101.141 10.0.101.254
 ip dhcp excluded-address
 10.0.102.1 10.0.102.109
 ip dhcp excluded-address
 10.0.102.141 10.0.102.254
```

*Se excluyen los rangos de direcciones que no van a ser entregados por el servidor DHCP.*

Figura 6. Direccinamiento interfaces D1

```
D1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/0    unassigned      YES unset  up         up
Ethernet0/1    unassigned      YES unset  up         up
Ethernet0/2    unassigned      YES unset  up         up
Ethernet0/3    unassigned      YES unset  up         up
Ethernet1/0    unassigned      YES unset  up         up
Ethernet1/1    10.0.10.2       YES NVRAM  up         up
Ethernet1/2    unassigned      YES unset  up         up
Ethernet1/3    unassigned      YES unset  up         up
Port-channel12 unassigned      YES unset  up         up
Port-channel11 unassigned      YES unset  up         up
Vlan100        10.0.100.1      YES NVRAM  up         up
Vlan101        10.0.101.1      YES NVRAM  up         up
Vlan102        10.0.102.1      YES NVRAM  up         up
D1#
```

## Switch D2

### Comando

```
hostname D2
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills
Assessment, Scenario 1 #
line con 0 exec-timeout 0 0
logging synchronous
exit

vlan 100
name Management

vlan 101
name UserGroupA

vlan 102
name UserGroupB

vlan 999
name NATIVE
```

### Explicación

*Establece el nombre del dispositivo*

*Habilita el enrutamiento IPV6*

*Deshabilita la traducción de nombres*

*Establece un mensaje para cuando se inicia en el modo privilegiado*

*Establece para línea de consola el time-out de 0 minutos y 0 segundos.*

*Crea la VLAN 100 con su respectivo nombre*

*Crea la VLAN 101 con su respectivo nombre*

*Crea la VLAN 102 con su respectivo nombre*

*Crea la VLAN 999 con su respectivo nombre*

```
interface Vlan100
 ip address 10.0.100.1
 255.255.255.0
 ipv6 address FE80::D1:2 link-local
 ipv6 address
 2001:DB8:100:100::1/64
 ospfv3 6 ipv6 area 0
```

*Configuración interface VLAN 100 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.*

```
interface Vlan101
 ip address 10.0.101.1
 255.255.255.0
 ipv6 address FE80::D1:3 link-local
 ipv6 address
 2001:DB8:100:101::1/64
 ospfv3 6 ipv6 area 0
```

*Configuración interface VLAN 101 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.*

```
interface Vlan102
 ip address 10.0.102.1
 255.255.255.0
 ipv6 address FE80::D1:4 link-local
 ipv6 address
 2001:DB8:100:102::1/64
 ospfv3 6 ipv6 area 0
```

*Configuración interface VLAN 102 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6. Adicional se anuncia la interface en OSPF versión 3 para el área 0.*

```
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
```

*Se configuran los pools de direccionamiento para las VLANs 101 y 102 con su respectiva mascara y puerta de enlace predeterminada.*

```
ip dhcp pool VLAN-101
 network 10.0.101.0 255.255.255.0
 default-router 10.0.101.254
```

```
ip dhcp excluded-address
 10.0.101.1 10.0.101.109
 ip dhcp excluded-address
 10.0.101.141 10.0.101.254
 ip dhcp excluded-address
 10.0.102.1 10.0.102.109
 ip dhcp excluded-address
 10.0.102.141 10.0.102.254
```

*Se excluyen los rangos de direcciones que no van a ser entregados por el servidor DHCP.*



Figura 6. Direccionamiento interfaces D2

```
D2#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        unassigned      YES unset  up          up
Ethernet0/1        unassigned      YES unset  up          up
Ethernet0/2        unassigned      YES unset  up          up
Ethernet0/3        unassigned      YES unset  up          up
Ethernet1/0        unassigned      YES unset  up          up
Ethernet1/1        10.0.11.2       YES NVRAM  up          up
Ethernet1/2        unassigned      YES unset  up          up
Ethernet1/3        unassigned      YES unset  up          up
Port-channel12    unassigned      YES unset  up          up
Port-channel2     unassigned      YES unset  up          up
Vlan100           10.0.100.2      YES NVRAM  up          up
Vlan101           10.0.101.2      YES NVRAM  up          up
Vlan102           10.0.102.2      YES NVRAM  up          up
D2#
```

### Switch A1

#### Comando

```
hostname D2
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0 exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
vlan 101
name UserGroupA
vlan 102
name UserGroupB
vlan 999
name NATIVE
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
```

#### Explicación

*Establece el nombre del dispositivo*

*Habilita el enrutamiento IPV6*

*Deshabilita la traducción de nombres*

*Establece un mensaje para cuando se inicia en el modo privilegiado*

*Establece para línea de consola el time out de 0 minutos y 0 segundos.*

*Crea la VLAN 100 con su respectivo nombre*

*Crea la VLAN 101 con su respectivo nombre*

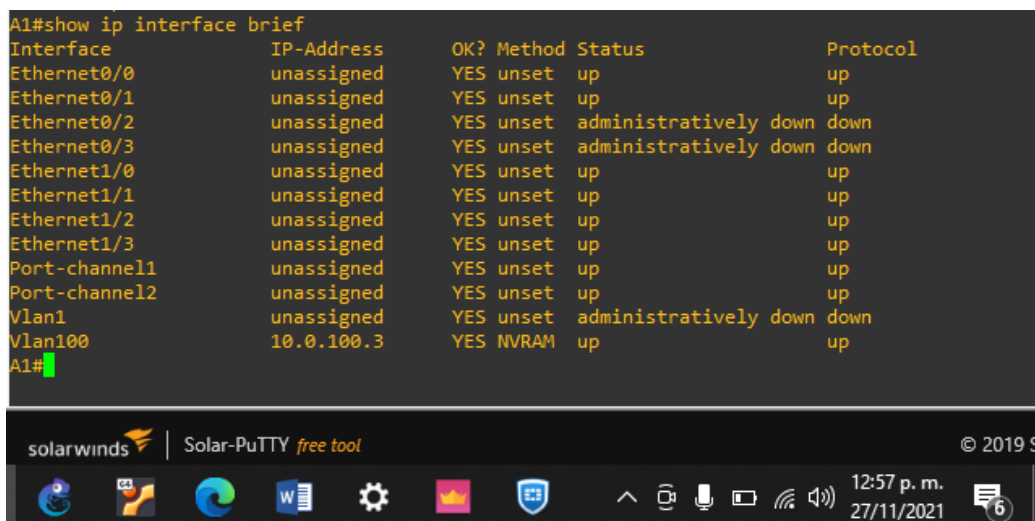
*Crea la VLAN 102 con su respectivo nombre*

*Crea la VLAN 999 con su respectivo nombre*

*Configuración interface VLAN 100 en modo capa 3 con su respectivo direccionamiento IPV4 e IPV6.*

Figura 7. Direccionamiento interfaces A1

```
A1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
Ethernet0/0        unassigned      YES unset  up              up
Ethernet0/1        unassigned      YES unset  up              up
Ethernet0/2        unassigned      YES unset  administratively down down
Ethernet0/3        unassigned      YES unset  administratively down down
Ethernet1/0        unassigned      YES unset  up              up
Ethernet1/1        unassigned      YES unset  up              up
Ethernet1/2        unassigned      YES unset  up              up
Ethernet1/3        unassigned      YES unset  up              up
Port-channel1     unassigned      YES unset  up              up
Port-channel2     unassigned      YES unset  up              up
Vlan1              unassigned      YES unset  administratively down down
Vlan100            10.0.100.3     YES NVRAM  up              up
A1#
```



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

Figura 8. Direccionamiento estático PC1

```
PC1_VLAN_100> show ip
NAME                : PC1_VLAN_100[1]
IP/MASK              : 10.0.100.5/24
GATEWAY              : 10.0.100.254
DNS                  :
MAC                  : 00:50:79:66:68:00
LPORT                : 10022
RHOST:PORT           : 127.0.0.1:10023
MTU                  : 1500
PC1_VLAN_100>
```

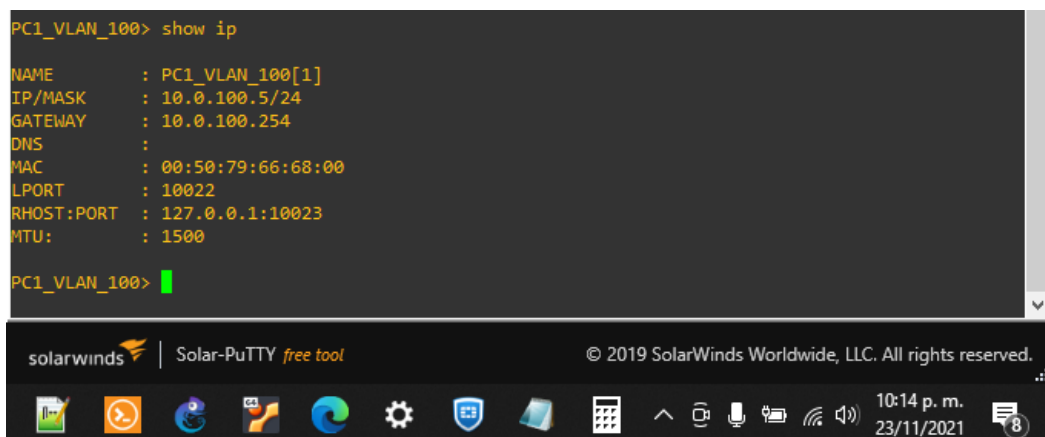
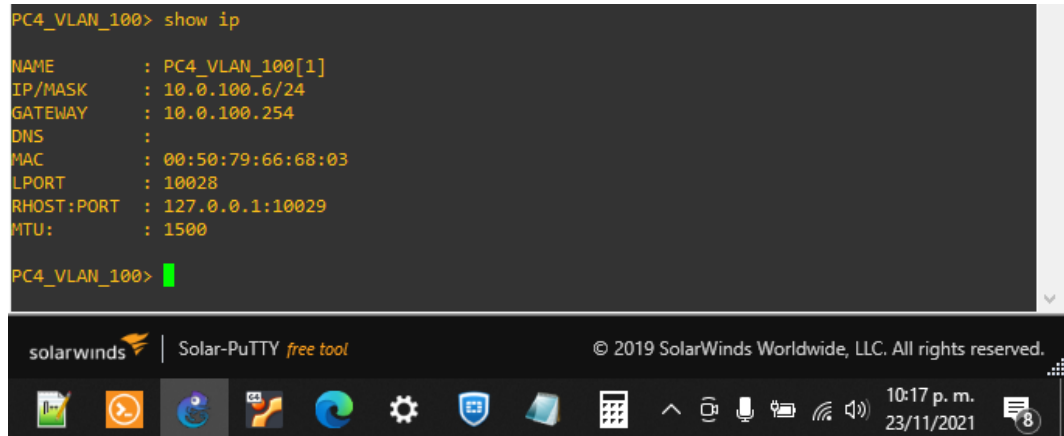


Figura 9. Direccionamiento estático PC4

```
PC4_VLAN_100> show ip
NAME      : PC4_VLAN_100[1]
IP/MASK   : 10.0.100.6/24
GATEWAY   : 10.0.100.254
DNS       :
MAC       : 00:50:79:66:68:03
LPORT     : 10028
RHOST:PORT : 127.0.0.1:10029
MTU       : 1500

PC4_VLAN_100> █
```



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

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

En esta parte dos se configuró a nivel de capa 2 en los switches D1, D2 y A1 enlaces troncales 802.1Q, VLAN nativa sobre enlaces troncales, protocolo de árbol de expansión y etherchannels.

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

### Switch D1

#### Comando

```
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 12 mode active
```

#### Explicación

*Configuración Ethernet0/0 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 12 mode active
```

*Configuración Ethernet0/1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 12 mode active
```

*Configuración Ethernet0/2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 12 mode active
```

*Configuración Ethernet0/3 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```

interface Ethernet1/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 1 mode active

```

*Configuración Ethernet1/2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 1*

```

interface Ethernet1/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-
102, 999
switchport mode trunk
duplex auto
channel-group 1 mode active

```

*Configuración Ethernet1/3 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 1*

Figura 10. Interfaces troncales D1

```

D1#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Et1/2     on             802.1q         trunking      999
Et1/3     on             802.1q         trunking      999
Po12     on             802.1q         trunking      999

Port      Vlans allowed on trunk
Et1/2     none
Et1/3     none
Po12     100-102,999

Port      Vlans allowed and active in management domain
Et1/2     none
Et1/3     none
Po12     100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Et1/2     none
Et1/3     none
Po12     100-102,999
D1#

```

solarwinds | Solar-PuTTY free tool © 2019 S

1:23 p. m. 27/11/2021

## Switch D2

### Comando

```
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,
 999
 switchport mode trunk
 duplex auto
 channel-group 12 mode active
```

### Explicación

*Configuración Ethernet0/0 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,
 999
 switchport mode trunk
 duplex auto
 channel-group 12 mode active
```

*Configuración Ethernet0/1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,
 999
 switchport mode trunk
 duplex auto
 channel-group 12 mode active
```

*Configuración Ethernet0/2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-102,
 999
 switchport mode trunk
 duplex auto
 channel-group 12 mode active
```

*Configuración Ethernet0/3 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 12*

```
interface Ethernet1/0
 switchport access vlan 102
 switchport mode access
 duplex auto
 spanning-tree portfast
```

*Configuración Ethernet1/0 en modo acceso en vlan 102 y con el comando spanning-tree portfast que hace que el puerto pase a estado de reenvío inmediatamente.*

<pre>interface Ethernet1/2 switchport trunk encapsulation dot1q switchport trunk native vlan 999 switchport trunk allowed vlan 100-102, 999 switchport mode trunk duplex auto channel-group 2 mode active</pre>	<p><i>Configuración Ethernet1/2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 2</i></p>
<pre>interface Ethernet1/3 switchport trunk encapsulation dot1q switchport trunk native vlan 999 switchport trunk allowed vlan 100-102, 999 switchport mode trunk duplex auto channel-group 2 mode active</pre>	<p><i>Configuración Ethernet1/3 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 2</i></p>

Figura 11. Interfaces troncales D2

```
D2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Po12     on        802.1q         trunking    999
Po2      on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po12     100-102,999
Po2      100-102,999

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

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

## Switch A1

### Comando

```
interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100-
  102,999
  switchport mode trunk
  duplex auto
  channel-group 2 mode active
```

### Explicación

*Configuración Ethernet0/0 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 2*

```
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100-
  102,999
  switchport mode trunk
  duplex auto
  channel-group 2 mode active
```

*Configuración Ethernet0/1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 2*

```
interface Ethernet0/2
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100-
  102,999
  switchport mode trunk
  shutdown
  duplex auto
  channel-group 1 mode active
```

*Configuración Ethernet0/2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 1*

```
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 999
  switchport trunk allowed vlan 100-
  102,999
  switchport mode trunk
  shutdown
  duplex auto
  channel-group 1 mode active
```

*Configuración Ethernet0/3 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999, adicional agregada al port-channel 2*



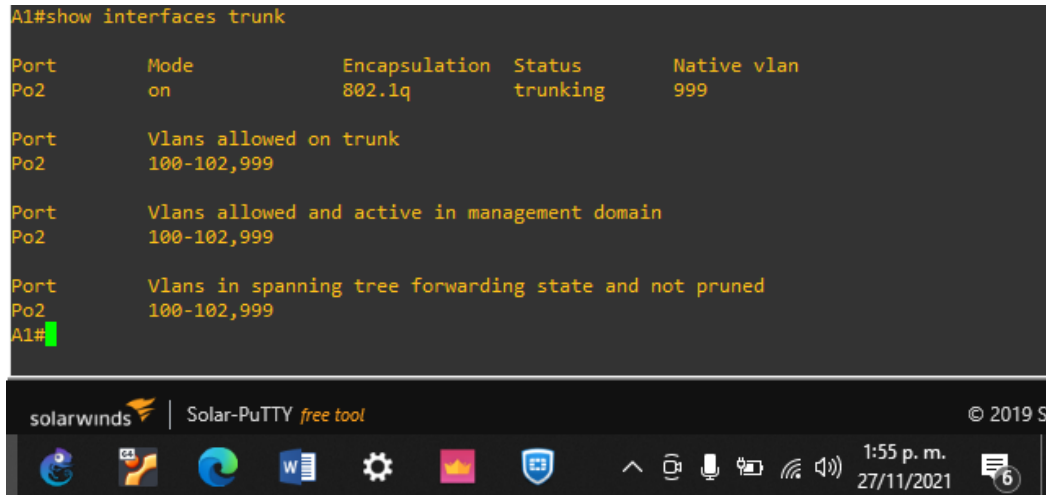
Figura 12. Interfaces troncales A1

```
A1#show interfaces trunk
Port      Mode           Encapsulation  Status        Native vlan
Po2       on             802.1q         trunking      999

Port      Vlans allowed on trunk
Po2       100-102,999

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

Port      Vlans in spanning tree forwarding state and not pruned
Po2       100-102,999
A1#
```



2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

### Switch D1

Comando	Explicación
interface Ethernet0/0 switchport trunk native vlan 999	Configuración Ethernet0/0 en modo troncal con vlan nativa 999.
interface Ethernet0/1 switchport trunk native vlan 999	Configuración Ethernet0/1 en modo troncal con vlan nativa 999.
interface Ethernet0/2 switchport trunk native vlan 999	Configuración Ethernet0/2 en modo troncal con vlan nativa 999
interface Ethernet0/3 switchport trunk native vlan 999	Configuración Ethernet0/3 en modo troncal con vlan nativa 999.
interface Ethernet1/2 switchport trunk native vlan 999	Configuración Ethernet1/2 en modo troncal con vlan nativa 999.
interface Ethernet1/3 switchport trunk native vlan 999	Configuración Ethernet1/3 en modo troncal con vlan nativa 999.

## Switch D2

### Comando

```
interface Ethernet0/0  
switchport trunk native vlan 999
```

```
interface Ethernet0/1  
switchport trunk native vlan 999
```

```
interface Ethernet0/2  
switchport trunk native vlan 999
```

```
interface Ethernet0/3  
switchport trunk native vlan 999
```

```
interface Ethernet1/2  
switchport trunk native vlan 999
```

```
interface Ethernet1/3  
switchport trunk native vlan 999
```

### Explicación

*Configuración Ethernet0/0 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/1 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/2 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/3 en modo troncal con vlan nativa 999.*

*Configuración Ethernet1/2 en modo troncal con vlan nativa 999.*

*Configuración Ethernet1/3 en modo troncal con vlan nativa 999.*

## Switch A1

### Comando

```
interface Ethernet0/0  
switchport trunk native vlan 999
```

```
interface Ethernet0/1  
switchport trunk native vlan 999
```

```
interface Ethernet0/2  
switchport trunk native vlan 999
```

```
interface Ethernet0/3  
switchport trunk native vlan 999
```

### Explicación

*Configuración Ethernet0/0 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/1 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/2 en modo troncal con vlan nativa 999.*

*Configuración Ethernet0/3 en modo troncal con vlan nativa 999.*

### 2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

En esta tarea se habilita el protocolo de árbol de expansión en su versión rápida en los switches D1, D2 y A1.

#### Comando

spanning-tree mode rapid-pvst

#### Explicación

Se *habilita STP en modo rápido*

Figura 13. RSTP habilitado en D1

```
D1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0100, VLAN0102, VLAN0999
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is enabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast              is disabled
BackboneFast            is disabled
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0100	0	0	0	2	2
VLAN0101	0	0	0	1	1
VLAN0102	0	0	0	1	1
VLAN0999	0	0	0	1	1
4 vlans	0	0	0	5	5

D1#

solarwinds | Solar-PuTTY free tool © 2019 S  
2:03 p. m. 27/11/2021

Figura 14. RSTP habilitado en D2

```
D2#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0101
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is enabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast              is disabled
BackboneFast            is disabled
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0100	0	0	0	2	2
VLAN0101	0	0	0	2	2
VLAN0102	0	0	0	3	3
VLAN0999	0	0	0	2	2
4 vlans	0	0	0	9	9

D2#

Figura 15. RSTP habilitado en A1

```
A1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID      is enabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is enabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast              is disabled
BackboneFast            is disabled
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
VLAN0100	0	0	0	2	2
VLAN0101	0	0	0	2	2
VLAN0102	0	0	0	1	1
VLAN0999	0	0	0	1	1
5 vlans	0	0	0	8	8

A1#

2.4 En D1 y D2, configure los puentes raízRSTP (root bridges) según la información del diagrama de topología.

### Switch D1

#### Comando

spanning-tree vlan 100,102  
priority 24576

spanning-tree vlan 101 priority  
28672

#### Explicación

*Se habilita D1 como root bridge primario para las VLANs 100 y 102*

*Se habilita D1 como root bridge secundario para la VLAN 101*

Figura 16. Prioridad puente raíz en D1

```
D1#show spanning-tree bridge
```

Vlan	Bridge ID	Hello Time	Max Age	Fwd Dly	Protocol
VLAN0100	24676 (24576, 100) aabb.cc00.0100	2	20	15	rstp
VLAN0101	28773 (28672, 101) aabb.cc00.0100	2	20	15	rstp
VLAN0102	24678 (24576, 102) aabb.cc00.0100	2	20	15	rstp
VLAN0999	33767 (32768, 999) aabb.cc00.0100	2	20	15	rstp

D1#

### Switch D2

#### Comando

spanning-tree vlan 100,102  
priority 28672

spanning-tree vlan 101 priority  
24576

#### Explicación

*Se habilita D1 como root bridge secundario para las VLANs 100 y 102*

*Se habilita D1 como root bridge primario para la VLAN 101*

Figura 17. Prioridad puente raíz en D2

```
D2#show spanning-tree bridge
```

Vlan	Bridge ID	Hello Time	Max Age	Fwd Dly	Protocol
VLAN0100	28772 (28672, 100) aabb.cc00.0200	2	20	15	rstp
VLAN0101	24677 (24576, 101) aabb.cc00.0200	2	20	15	rstp
VLAN0102	28774 (28672, 102) aabb.cc00.0200	2	20	15	rstp
VLAN0999	33767 (32768, 999) aabb.cc00.0200	2	20	15	rstp

D2#

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

### Switch D1

#### Comando

```
interface Port-channel12
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan
 100-102,999
 switchport mode trunk
```

#### Explicación

*Configuración port-channel 12 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*

```
interface Port-channel1
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan
 100-102, 999
 switchport mode trunk
```

*Configuración port-channel 1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*

Figura 18. Port-channel 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       f - failed to allocate aggregator

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

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

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

D1#
```

## Switch D2

### Comando

```
interface Port-channel12
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan
 100-102,999
 switchport mode trunk
```

```
interface Port-channel2
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan
 100-102, 999
 switchport mode trunk
```

### Explicación

*Configuración port-channel 12 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*

*Configuración port-channel 1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*

Figura 19. Port-channel 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       f - failed to allocate aggregator

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

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

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

D2#

## Switch A1

### Comando

```
interface Port-channel1
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-
 102,999
 switchport mode trunk
```

```
interface Port-channel2
 switchport
 switchport trunk encapsulation
 dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100-
 102,999
 switchport mode trunk
```

### Explicación

*Configuración port-channel 1 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*

*Configuración port-channel 2 en modo troncal con vlan nativa 999 y vlans permitidas para atravesar el troncal 100, 101, 102 y 999*



Figura 20. Port-channel 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       f - failed to allocate aggregator

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

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

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

A1#
```

solarwinds | Solar-PuTTY free tool © 2019 S

2:21 p. m. 27/11/2021 6

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.

### Switch D1

#### Comando

```
interface Ethernet1/0
switchport access vlan 100
switchport mode access
duplex auto
spanning-tree portfast
```

#### Explicación

*Configuración Ethernet1/0 en modo acceso en vlan 100 y con el comando spanning-tree portfast que hace que el puerto pase a estado de reenvío inmediatamente.*

## Switch D2

### Comando

```
interface Ethernet1/0
switchport access vlan 102
switchport mode access
duplex auto
spanning-tree portfast
```

### Explicación

*Configuración Ethernet1/0 en modo acceso en vlan 102 y con el comando spanning-tree portfast que hace que el puerto pase a estado de reenvío inmediatamente.*

## Switch A1

### Comando

```
interface Ethernet1/0
switchport access vlan 101
switchport mode access
duplex auto
spanning-tree portfast
```

### Explicación

*Configuración Ethernet1/0 en modo acceso con vlan 101 y el comando spanning-tree portfast que establece la niterface en modo reenvío inmediatamente*

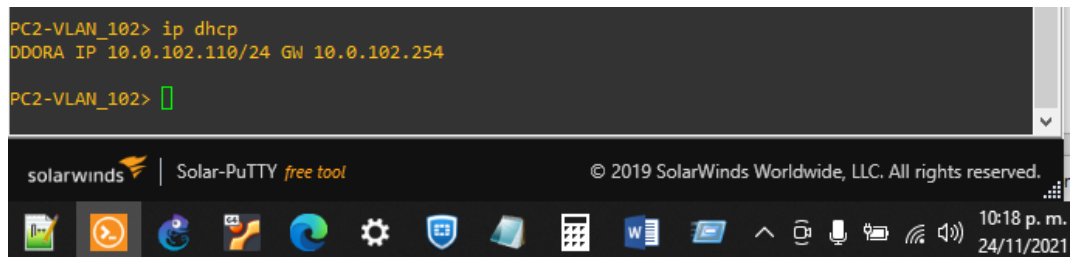
```
interface Ethernet1/1
switchport access vlan 100
switchport mode access
duplex auto
spanning-tree portfast
```

*Configuración Ethernet1/1 en modo acceso con vlan 100 y el comando spanning-tree portfast que establece la interface en modo reenvío inmediatamente*

## 2.7 Verifique los servicios DHCP IPv4.

Se ejecuta el comando IP DHCP en host PC2 y vemos como le entrega la dirección IP 10.0.102.110.

Figura 21. Verificación servicio DHCP PC2



```
PC2-VLAN_102> ip dhcp
DDORA IP 10.0.102.110/24 GW 10.0.102.254
PC2-VLAN_102> 
```

Se ejecuta el comando IP DHCP en host PC3 y vemos como le entrega la dirección IP 10.0.101.210.

Figura 22. Verificación servicio DHCP PC3

```
PC3_VLAN_101> ip dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254

PC3_VLAN_101> █
```

2.8 Verifique la conectividad de la LAN local.

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1

Figura 23. Verificación conectividad PC1-D1

```
PC1_VLAN_100> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.531 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.704 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.254 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.393 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.009 ms

PC1_VLAN_100> █
```

D2: 10.0.100.2

Figura 24. Verificación conectividad PC1-D2

```
PC1_VLAN_100> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.774 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.890 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.531 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=2.961 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.812 ms

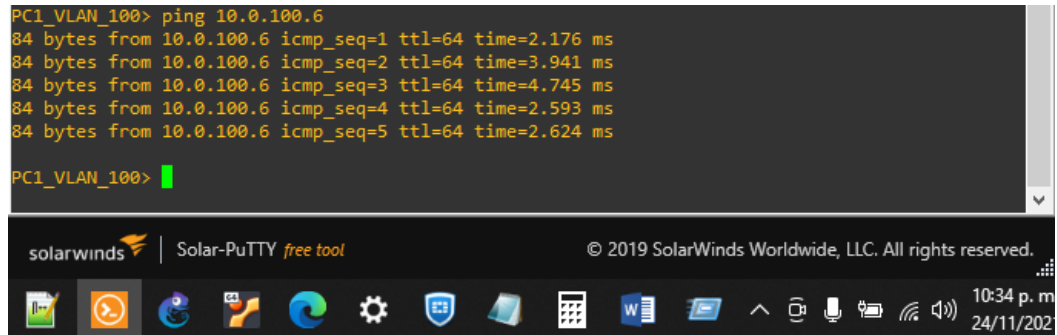
PC1_VLAN_100> █
```

PC4: 10.0.100.6

Figura 25. Verificación conectividad PC1-PC4

```
PC1_VLAN_100> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=2.176 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=3.941 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=4.745 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=2.593 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=2.624 ms

PC1_VLAN_100> █
```



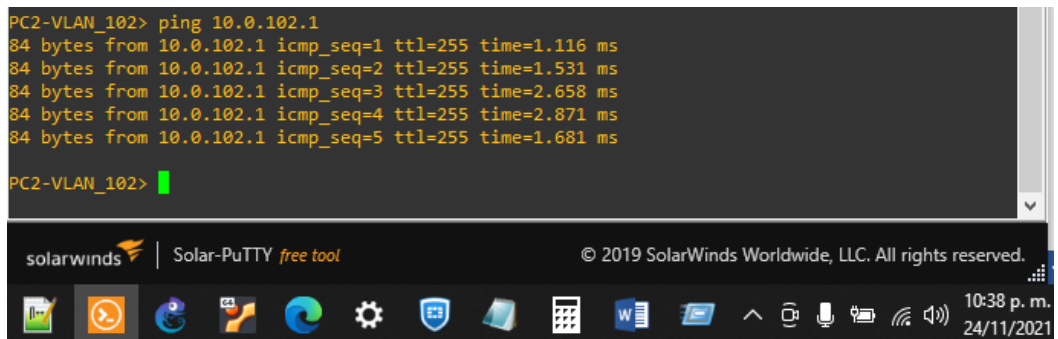
PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

Figura 26. Verificación conectividad PC2-D1

```
PC2-VLAN_102> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.116 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.531 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=2.658 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=2.871 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.681 ms

PC2-VLAN_102> █
```

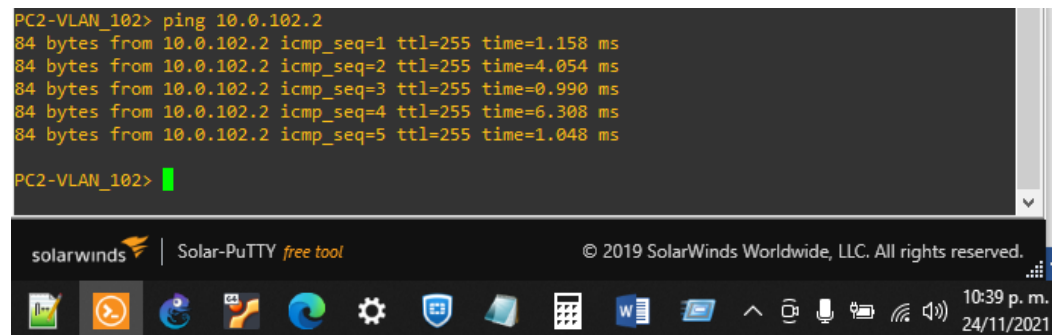


D2: 10.0.102.2

Figura 27. Verificación conectividad PC2-D1

```
PC2-VLAN_102> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=1.158 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=4.054 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.990 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=6.308 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=1.048 ms

PC2-VLAN_102> █
```



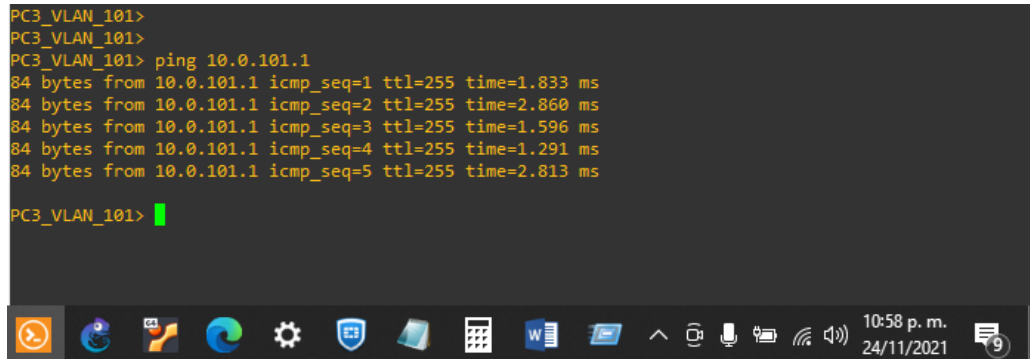
PC3 debería hacer ping con éxito a:

D1: 10.0.101.1

Figura 28. Verificación conectividad PC3-D1

```
PC3_VLAN_101>
PC3_VLAN_101>
PC3_VLAN_101> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=1.833 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=2.860 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.596 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.291 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=2.813 ms

PC3_VLAN_101> █
```

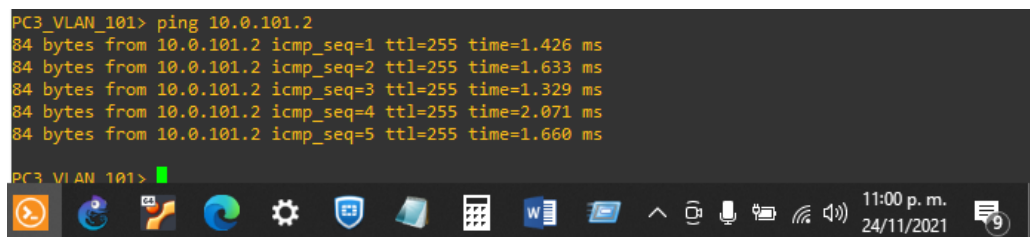


D2: 10.0.101.2

Figura 29. Verificación conectividad PC3-D2

```
PC3_VLAN_101> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=1.426 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=1.633 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=1.329 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=2.071 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=1.660 ms

PC3_VLAN_101> █
```



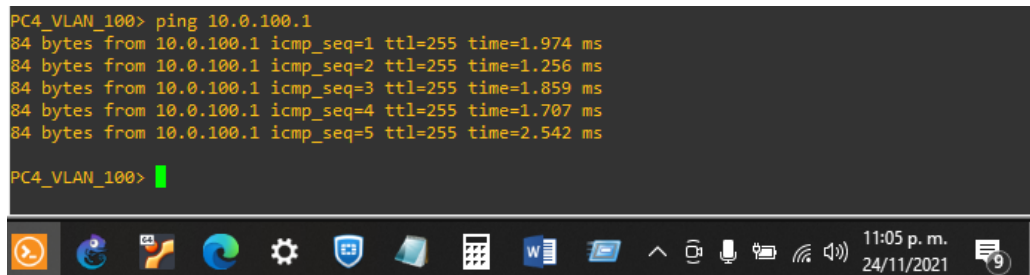
PC4 debería hacer ping con éxito a:

D1: 10.0.100.1

Figura 30. Verificación conectividad PC4-D1

```
PC4_VLAN_100> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=1.974 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.256 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.859 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.707 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=2.542 ms

PC4_VLAN_100> █
```

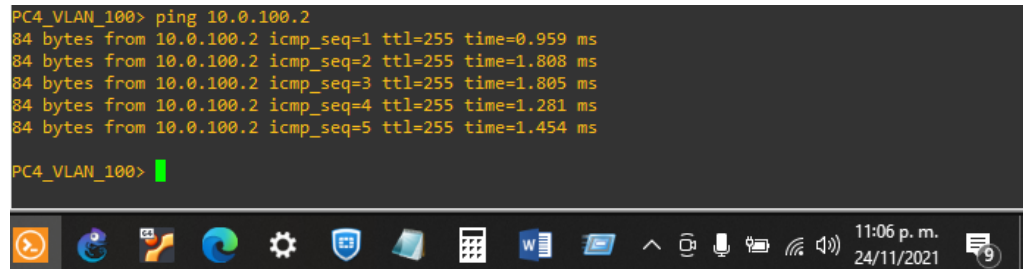


D2: 10.0.100.2

Figura 31. Verificación conectividad PC4-D2

```
PC4_VLAN_100> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.959 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.808 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.805 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.281 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.454 ms

PC4_VLAN_100> █
```

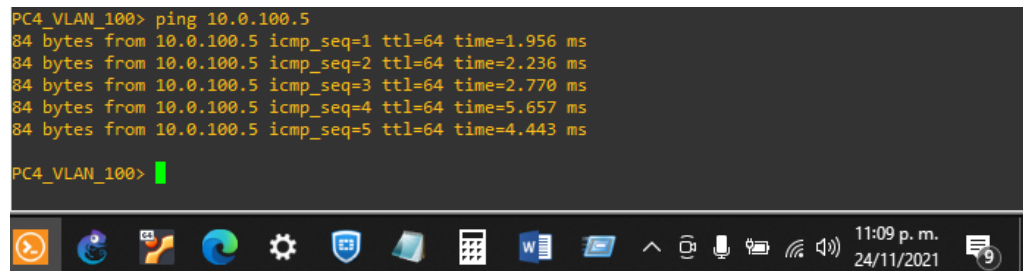


PC1: 10.0.100.5

Figura 32. Verificación conectividad PC4-PC1

```
PC4_VLAN_100> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=1.956 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=2.236 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=2.770 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=5.657 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=4.443 ms

PC4_VLAN_100> █
```



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

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

LA parte 3 se básicamente se configura OSPF versión 2, OSPF versión 3, BGP, se anuncian rutas y se deshabilitan interfaces para formen adyacencias.

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

#### Router R1

Comando	Explicación
router ospf 4	Habilita el protocolo OSPF con el ID 4
router-id 0.0.4.1	Se establece el identificador de router para el proceso 4
network 10.0.10.0 0.0.0.255 area 0	Se publica la red en el área cero
network 10.1.11.0 0.0.0.255 area 0	Se publica la red en el área cero
network 209.165.200.224 0.0.0.31 area 0	Se publica la red en el área cero
default-information originate	Propaga ruta por defecto a los router adyacentes.

Figura 33. Verificación OSPF v2 en R1

```
R1# show ip ospf 4
Routing Process "ospf 4" with ID 0.0.4.1
Start time: 00:00:34.752, Time elapsed: 2d19h
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 1. Checksum Sum 0x005902
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

## Router R3

### Comando

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

### Explicación

*Habilita OSPF versión 2 con el ID de proceso 4*

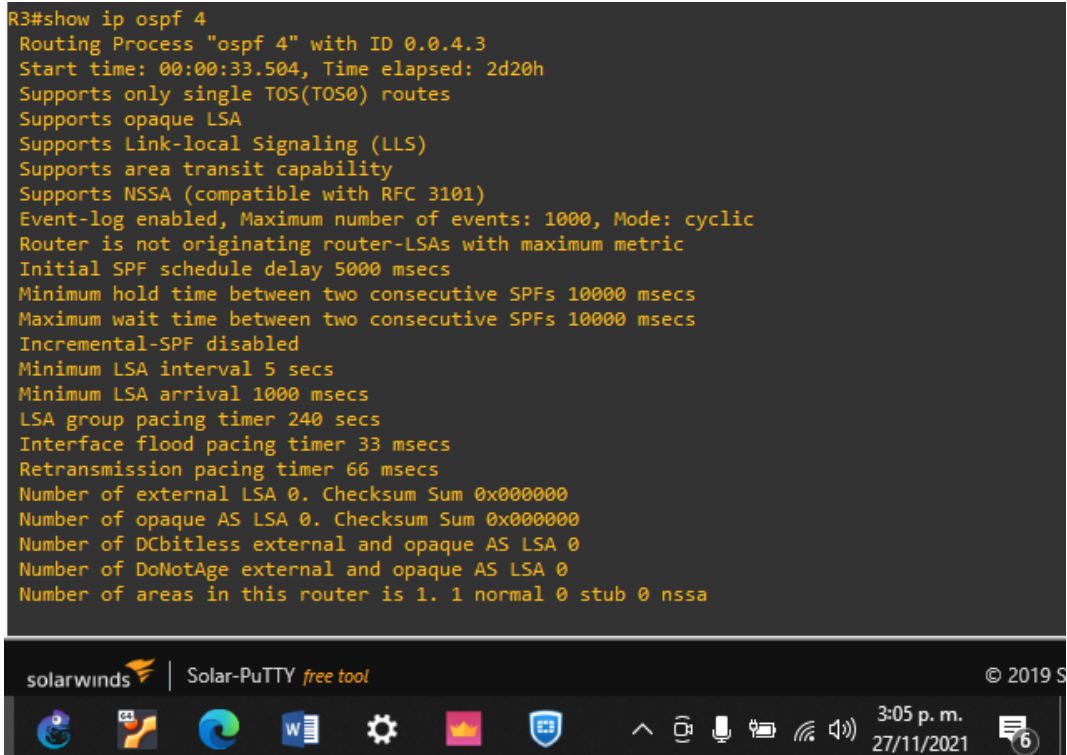
*Asigna identificador de router para ospf con ID de proceso 4*

*Anuncia la ruta 10.0.11.0/24 al área 0*

*Anuncia la ruta 10.0.13.0/24 al área 0*

Figura 34. Verificación OSPF v2 en R3

```
R3#show ip ospf 4
Routing Process "ospf 4" with ID 0.0.4.3
Start time: 00:00:33.504, Time elapsed: 2d20h
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```





## Switch D1

### Comando

```
router ospf 4
router-id 0.0.4.131

passive-interface Port-channel12
passive-interface Port-channel1

network 10.0.10.0.0.0.255 area 0
network 10.0.100.0.0.0.255 area 0
network 10.0.101.0.0.0.255 area 0
network 10.0.102.0.0.0.255 area 0
```

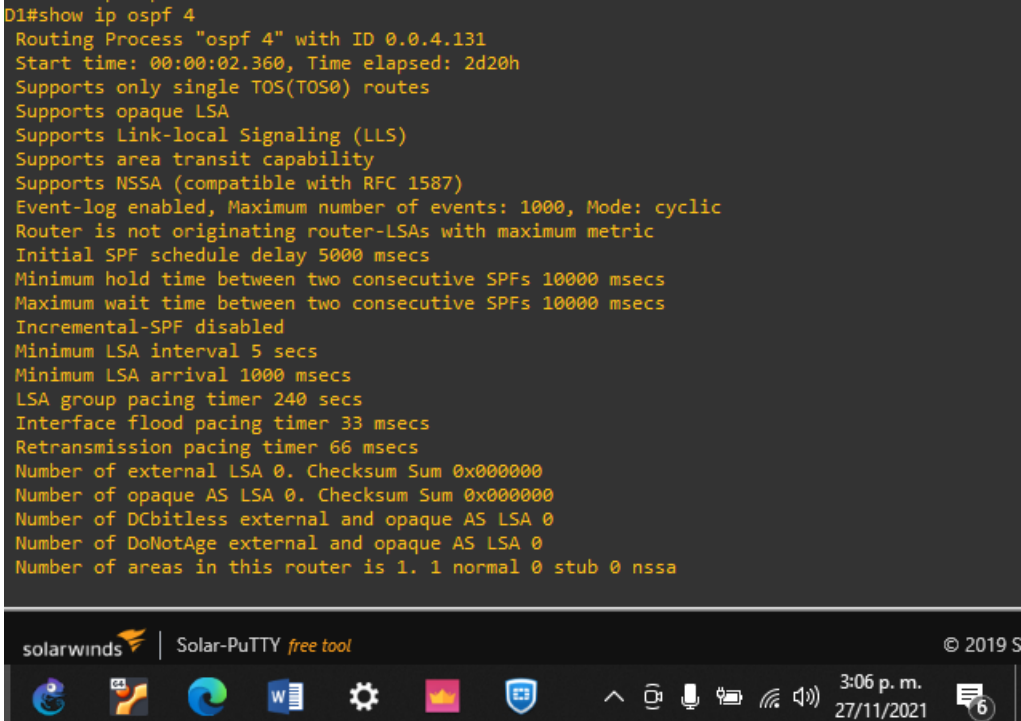
### Explicación

*Habilita OSPF con el ID de proceso 4 y se asigna el identificador de router.*

*Se deshabilitan las interfaces agregadas a los port-channel 1 y 12 para que no envíen paquetes hello de OSPF y no establezcan adyacencias.*

*Se anuncian en el area cero las redes 10.0.10.0/24, 10.0.100.0/24, 10.0.101.0/24 y 10.0.102.0/24*

Figura 35. Verificación OSPF v2 en D1



```
D1#show ip ospf 4
Routing Process "ospf 4" with ID 0.0.4.131
Start time: 00:00:02.360, Time elapsed: 2d20h
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

solarwinds | Solar-PuTTY free tool © 2019 S

3:06 p. m. 27/11/2021

## Switch D2

### Comando

```
router ospf 4
router-id 0.0.4.132

passive-interface Port-channel12
passive-interface Port-channel2

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
```

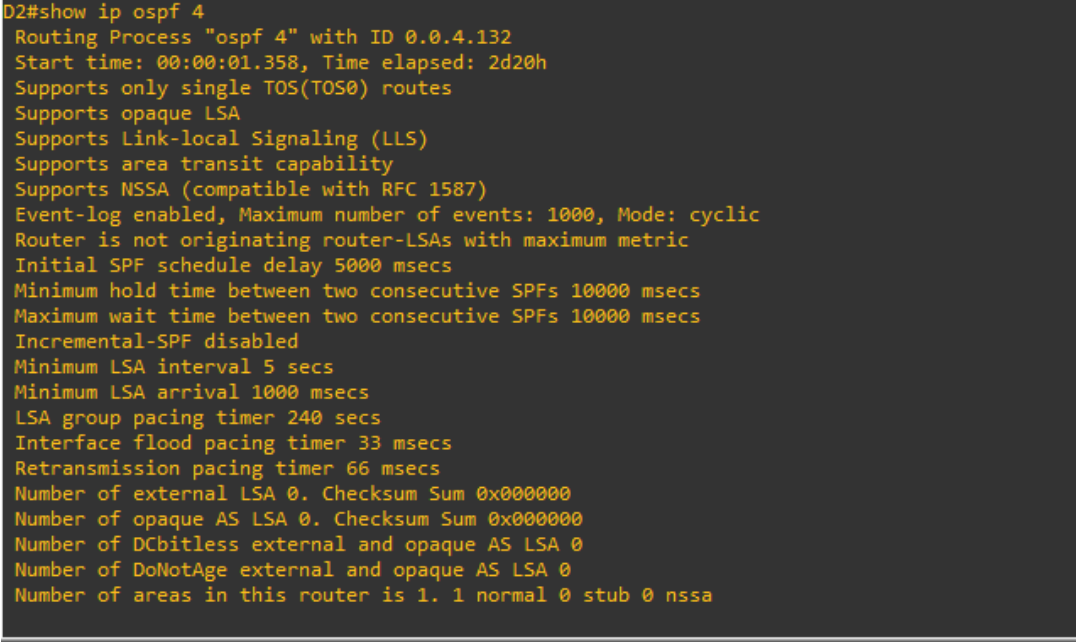
### Explicación

*Habilita OSPF con el ID de proceso 4 y se asigna el identificador de router.*

*Se deshabilitan las interfaces agregadas a los port-channel 2 y 12 para que no envíen paquetes hello de OSPF y no establezcan adyacencias.*

*Se anuncian las redes 10.0.10.0/24, 10.0.100.0/24, 10.0.101.0/24 y 10.0.102.0/24*

Figura 36. Verificación OSPF v2 en D2



```
D2#show ip ospf 4
Routing Process "ospf 4" with ID 0.0.4.132
Start time: 00:00:01.358, Time elapsed: 2d20h
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

solarwinds | Solar-PuTTY free tool © 2019 S

3:08 p. m. 27/11/2021 6

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

## Router R1

### Comando

```
router ospfv3 6
router-id 0.0.6.1

address-family ipv6 unicast

interface GigabitEthernet1/0
ospfv3 6 ipv6 area 0

interface Serial4/1
ospfv3 6 ipv6 area 0

default-information originate
```

### Explicación

*Habilita OSPF versión 3 con ID 6*  
*Se establece el identificador de router para el proceso 6*

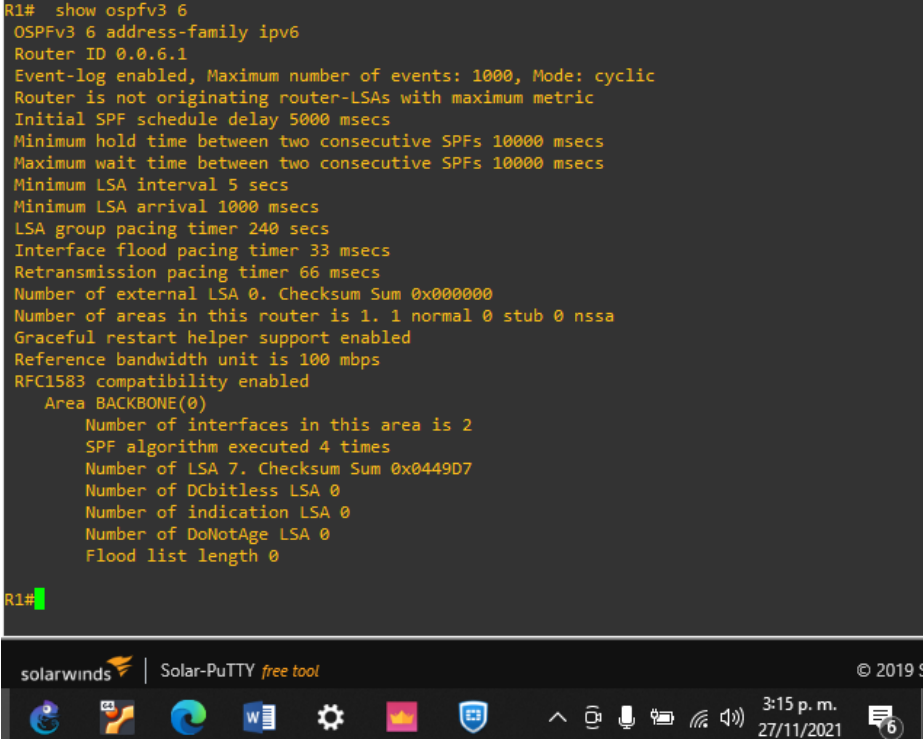
*Habilita la ejecución de direccionamiento IPV6 en OSPF versión 3*

*Se anuncia la interface GigabitEthernet1/0 para participar de OSPF versión 3 ID 6.*

*Se anuncia la interface Serial4/1 para participar de OSPF versión 3 ID 6.*

*Propaga ruta por defecto a los routers adyacentes.*

Figura 37. Verificación OSPF v3 en R1



```
R1# show ospfv3 6
OSPFv3 6 address-family ipv6
Router ID 0.0.6.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
Area BACKBONE(0)
Number of interfaces in this area is 2
SPF algorithm executed 4 times
Number of LSA 7. Checksum Sum 0x0449D7
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#
```

### Router R3

#### Comando

```
router ospfv3 6  
  
router-id 0.0.6.3  
  
address-family ipv6 unicast  
  
interface GigabitEthernet0/0  
ospfv3 6 ipv6 area 0  
  
interface Serial1/0  
ospfv3 6 ipv6 area 0
```

#### Explicación

*Habilita OSPF versión 3 con el ID proceso 6*

*Se asigna identificador de router*

*Habilita la familia de direcciones IPV6 para OSPF versión 3*

*Se anuncia la interface GigabitEthernet0/0 para participar de OSPF versión 3 ID 6.*

*Se anuncia la interface Serial1/0 para participar de OSPF versión 3 ID 6.*

Figura 38. Verificación OSPF v3 en R3

```
R3#show ospfv3 6  
OSPFv3 6 address-family ipv6  
Router ID 0.0.6.3  
Event-log enabled, Maximum number of events: 1000, Mode: cyclic  
Router is not originating router-LSAs with maximum metric  
Initial SPF schedule delay 5000 msec  
Minimum hold time between two consecutive SPFs 10000 msec  
Maximum wait time between two consecutive SPFs 10000 msec  
Minimum LSA interval 5 secs  
Minimum LSA arrival 1000 msec  
LSA group pacing timer 240 secs  
Interface flood pacing timer 33 msec  
Retransmission pacing timer 66 msec  
Number of external LSA 0. Checksum Sum 0x000000  
Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
Graceful restart helper support enabled  
Reference bandwidth unit is 100 mbps  
RFC1583 compatibility enabled  
Area BACKBONE(0)  
Number of interfaces in this area is 2  
SPF algorithm executed 4 times  
Number of LSA 7. Checksum Sum 0x048C8F  
Number of DCbitless LSA 0
```

## Switch D1

Comando	Explicación
router ospfv3 6	Se habilita el OSPF versión 3 con el proceso 6.
router-id 0.0.6.131	Se asigna identificador de router.
address-family ipv6 unicast	se habilita la familia de direcciones IPV6
passive-interface Port-channel12 passive-interface Port-channel2	Se deshabilitan las interfaces agregadas a los port-channel 1 y 12 para que no envíen paquetes hello de OSPF y no establezcan adyacencias.
interface Ethernet1/1 ospfv3 6 ipv6 area 0	Se anuncia la interface Ethernet1/1 para participar de OSPF versión 3 ID 6.
interface Vlan100 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 100 para participar de OSPF versión 3 ID 6.
interface Vlan101 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 101 para participar de OSPF versión 3 ID 6.
interface Vlan102 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 102 para participar de OSPF versión 3 ID 6.

Figura 39. Verificación OSPF v3 en D1

```
D1#show ospfv3 6
OSPFv3 6 address-family ipv6
Router ID 0.0.6.131
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Retransmission limit dc 24 non-dc 24
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 4
    SPF algorithm executed 7 times
    Number of LSA 16. Checksum Sum 0x09A2F3
    Number of DCbitless LSA 0
```

## Switch D2

Comando	Explicación
router ospfv3 6	Se habilita el OSPF versión 3 con el proceso 6.
router-id 0.0.6.132	Se asigna identificador de router.
address-family ipv6 unicast	se habilita la familia de direcciones IPV6
passive-interface Port-channel12 passive-interface Port-channel2	Se deshabilitan las interfaces agregadas a los port-channel 2 y 12 para que no envíen paquetes hello de OSPF y no establezcan adyacencias.
interface Ethernet1/1 ospfv3 6 ipv6 area 0	Se anuncia la interface Ethernet1/1 para participar de OSPF versión 3 ID 6.
interface Vlan100 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 100 para participar de OSPF versión 3 ID 6.
interface Vlan101 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 101 para participar de OSPF versión 3 ID 6.
interface Vlan102 ospfv3 6 ipv6 area 0	Se anuncia la interface vlan 102 para participar de OSPF versión 3 ID 6.

Figura 40. Verificación OSPF v3 en D2

```
D2#show ospfv3 6
OSPFv3 6 address-family ipv6
Router ID 0.0.6.132
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Retransmission limit dc 24 non-dc 24
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
Area BACKBONE(0)
  Number of interfaces in this area is 3
  SPF algorithm executed 6 times
  Number of LSA 15. Checksum Sum 0x08CA26
  Number of DCbitless LSA 0
```

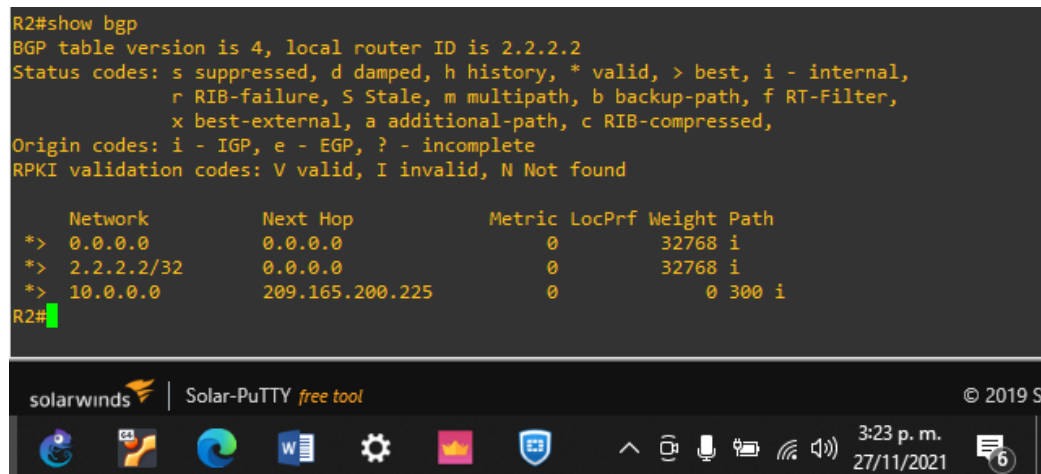
### 3.3 En R2 en la “Red ISP”, configure MP-BGP.

Comando	Explicación
ip route 0.0.0.0 0.0.0.0 Loopback0	Configura ruta predeterminada ipv4 vía la interfaz loopback 0
ipv6 route ::/0 Loopback0	Configura ruta predeterminada ipv6 vía la interfaz loopback 0
router bgp 500	Habilita BGP con número de sistema autónomo 500
bgp router-id 2.2.2.2	Asigna identificador de router para BGP 500
bgp log-neighbor-changes	Habilita el log de cambios en los routers vecinos
neighbor 209.165.200.225 remote-as 300	Establece relación de vecino con R1
address-family ipv4 network 0.0.0.0 network 2.2.2.2 mask 255.255.255.255 neighbor 209.165.200.225 activate	Habilita la familia de direcciones IPV4, anuncia ruta predeterminada y red 2.2.2.2/32, adicional activa el vecino R1
address-family ipv6 network ::/0 network 2001:DB8:2222::1/128	Habilita la familia de direcciones IPV6, anuncia ruta predeterminada y la red 2001:DB8:2222::1/128

Figura 41. Verificación BGP en R2

```
R2#show bgp
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*>  0.0.0.0         0.0.0.0           0         32768 i
*>  2.2.2.2/32      0.0.0.0           0         32768 i
*>  10.0.0.0        209.165.200.225  0         0 300 i
R2#
```



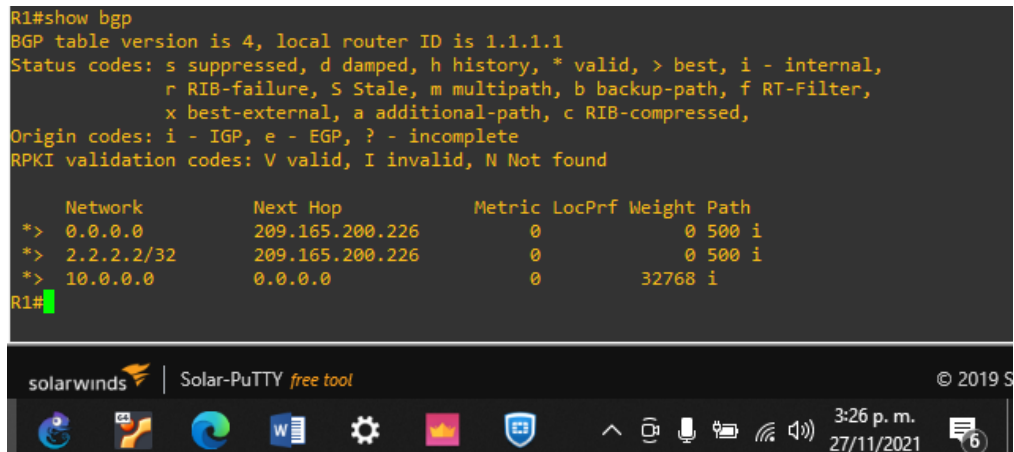
### 3.4 En R1 en la “Red ISP”, configure MP-BGP.

Comando	Explicación
ip route 10.0.0.0 255.0.0.0 Null0	Configura ruta estática en IPV4 con puerta de enlace Null0
ipv6 route 2001:DB8:100::/48 Null0	Configura ruta estática en IPV6 con puerta de enlace Null0
router bgp 300	Habilita BGP con el número de sistema autónomo 300
bgp router-id 1.1.1.1	Se asigna el identificador de router
bgp log-neighbor-changes	Se activa logs para cambios en los vecinos BGP
neighbor 209.165.200.226 remote-as 500	Se establece relación de vecino con R2
address-family ipv4 network 10.0.0.0 neighbor 209.165.200.226 activate	Para la familia de direcciones IPV4 se declara la red 10.0.0.0/8 y se activa el vecino R2
address-family ipv6 network 2001:DB8:100::/48	Para la familia de direcciones IPV6 se declara la red 2001:DB8:100::/48

Figura 42. Verificación BGP en R1

```
R1#show bgp
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
  *> 0.0.0.0         209.165.200.226      0           0 500 i
  *> 2.2.2.2/32      209.165.200.226      0           0 500 i
  *> 10.0.0.0        0.0.0.0              0           0 32768 i
R1#
```





#### 4. Parte 4: Configurar la Redundancia del Primer Salto

En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los host en la "Red de la Compañía". Adicional se configura IP SLA para monitoreas interfaces de los routers R1 y R3 con el fin de poder hacer seguimiento de la disponibilidad a la las interfaces que lindan con los switches D1 y D1.

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 GigabitEthernet1/0.

<b>Comando</b>	<b>Explicación</b>
ip sla 4	<i>Crea un SLA con ID 4.</i>
icmp-echo 10.0.10.1	<i>Prueba la disponibilidad de la interfaz G1/0 en R1.</i>
frequency 5	<i>Frecuencia de la prueba de disponibilidad cada 5 segundos.</i>
ip sla schedule 4 start-time now life forever	<i>Establece para que la SLA 4 inicie de inmediato y se ejecute por siempre.</i>
track 4 ip sla 4 reachability	<i>Configura objeto de seguimiento para el SLA 4.</i>
delay up 10 down 15	<i>notifica a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos</i>
ip sla 6	<i>Crea un SLA con ID 6.</i>
icmp-echo 2001:DB8:100:1010::1	<i>Prueba la disponibilidad de la interfaz G1/0 en R1.</i>
frequency 5	<i>Frecuencia de la prueba de disponibilidad cada 5 segundos.</i>
ip sla schedule 6 start-time now life forever	<i>Establece para que la SLA 6 inicie de inmediato y se ejecute por siempre.</i>
track 6 ip sla 6 reachability	<i>Configura objeto de seguimiento para el SLA 4.</i>
delay up 10 down 15	<i>notifica a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos</i>

Figura 43. Verificación IP SLA 4 en D1

```
D1#show ip sla statistics 4
IPSLAs Latest Operation Statistics

IPSLA operation id: 4
  Latest RTT: 8 milliseconds
Latest operation start time: 05:36:17 UTC Thu Nov 18 2021
Latest operation return code: OK
Number of successes: 130
Number of failures: 4
Operation time to live: Forever

D1#
```

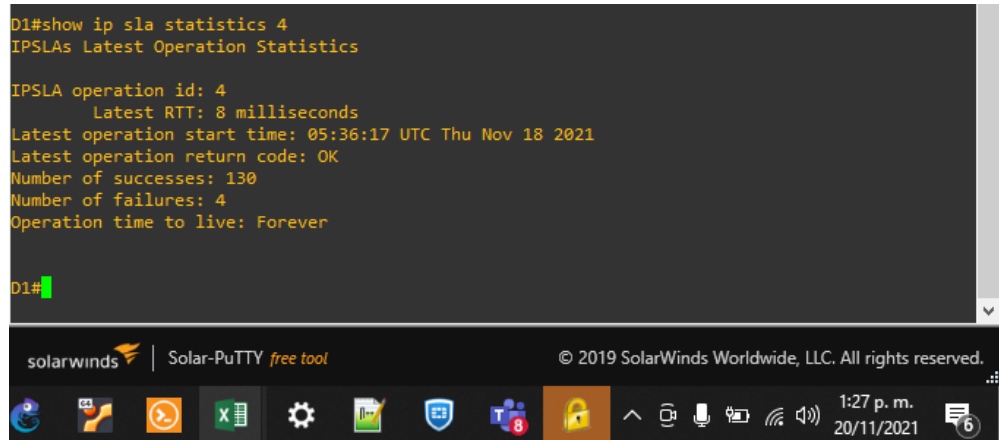


Figura 44. Verificación IP SLA 6 en D1

```
D1#show ip sla statistics 6
IPSLAs Latest Operation Statistics

IPSLA operation id: 6
  Latest RTT: 6 milliseconds
Latest operation start time: 05:37:12 UTC Thu Nov 18 2021
Latest operation return code: OK
Number of successes: 142
Number of failures: 5
Operation time to live: Forever

D1#
```

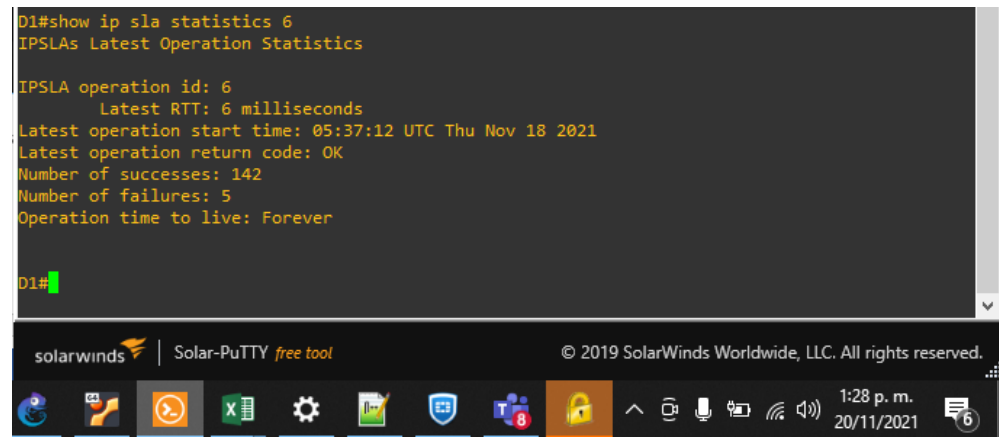


Figura 45. Evento interfaz G1/0 de R1 indisponible

```
D1#
*Nov 18 05:44:43.613: %TRACKING-5-STATE: 4 ip sla 4 reachability Up->Down
*Nov 18 05:44:43.613: %TRACKING-5-STATE: 6 ip sla 6 reachability Up->Down
D1#
```

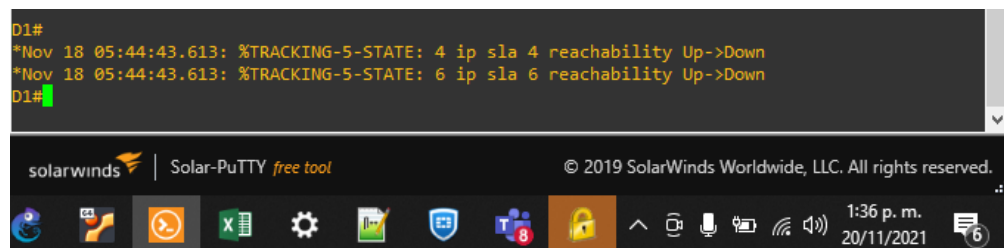
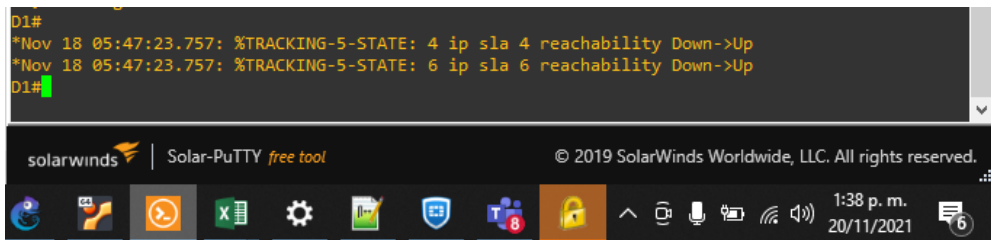


Figura 46. Evento interfaz G1/0 de R1 disponible



**4.2** En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 GigabitEthernet0/0.

<b>Comando</b>	<b>Explicación</b>
ip sla 4	<i>Crea un SLA con ID 4.</i>
icmp-echo 10.0.11.1	<i>Prueba la disponibilidad de la interfaz G0/0 en R3.</i>
frequency 5	<i>Frecuencia de la prueba de disponibilidad cada 5 segundos.</i>
ip sla schedule 4 start-time now life forever	<i>Establece para que la SLA 4 inicie de inmediato y se ejecute por siempre.</i>
track 4 ip sla 4 reachability	<i>Configura objeto de seguimiento para el SLA 4.</i>
delay up 10 down 15	<i>notifica a D2 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos</i>
ip sla 6	<i>Crea un SLA con ID 6.</i>
icmp-echo 2001:DB8:100:1011::1	<i>Prueba la disponibilidad de la interfaz G0/0 en R3.</i>
frequency 5	<i>Frecuencia de la prueba de disponibilidad cada 5 segundos.</i>
ip sla schedule 6 start-time now life forever	<i>Establece para que la SLA 6 inicie de inmediato y se ejecute por siempre.</i>
track 6 ip sla 4 reachability	<i>Configura objeto de seguimiento para el SLA 4.</i>
delay up 10 down 15	<i>notifica a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos</i>

Figura 47. Verificación IP SLA 4 en D2

```
D2#show ip sla statistics 4
IPSLAs Latest Operation Statistics

IPSLA operation id: 4
  Latest RTT: 12 milliseconds
Latest operation start time: 05:34:42 UTC Thu Nov 18 2021
Latest operation return code: OK
Number of successes: 111
Number of failures: 4
Operation time to live: Forever

D2#
```

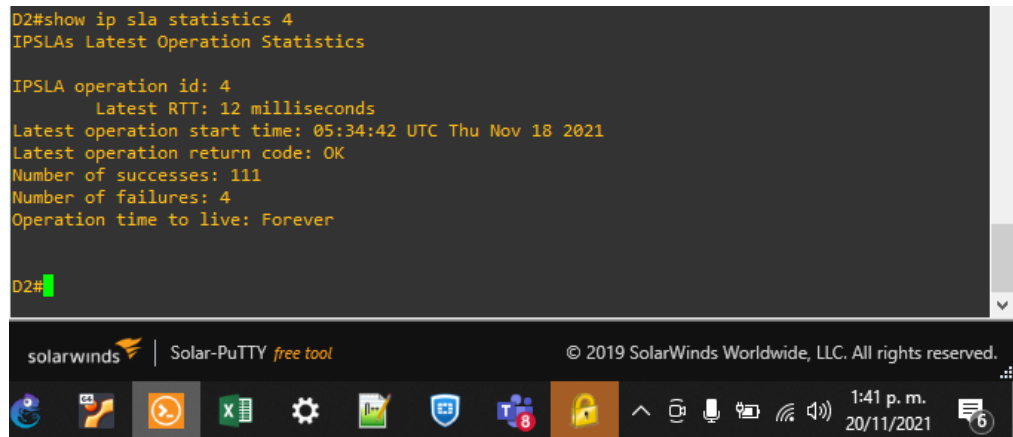


Figura 48. Verificación IP SLA 6 en D2

```
D2#show ip sla statistics 6
IPSLAs Latest Operation Statistics

IPSLA operation id: 6
  Latest RTT: 10 milliseconds
Latest operation start time: 05:50:52 UTC Thu Nov 18 2021
Latest operation return code: OK
Number of successes: 306
Number of failures: 5
Operation time to live: Forever

D2#
```

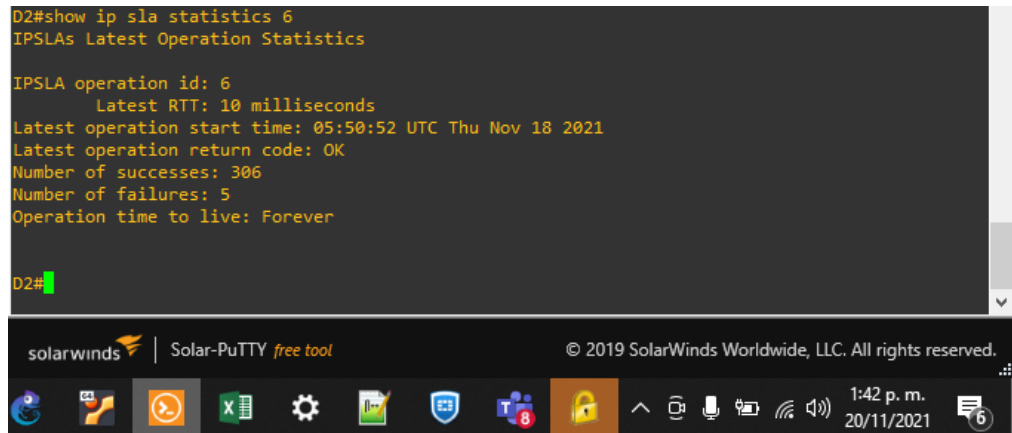


Figura 49. Evento interfaz G0/0 de R3 indisponible

```
D2#
*Nov 18 05:52:54.066: %TRACKING-5-STATE: 4 ip sla 4 reachability Up->Down
*Nov 18 05:52:54.066: %TRACKING-5-STATE: 6 ip sla 4 reachability Up->Down
D2#
```

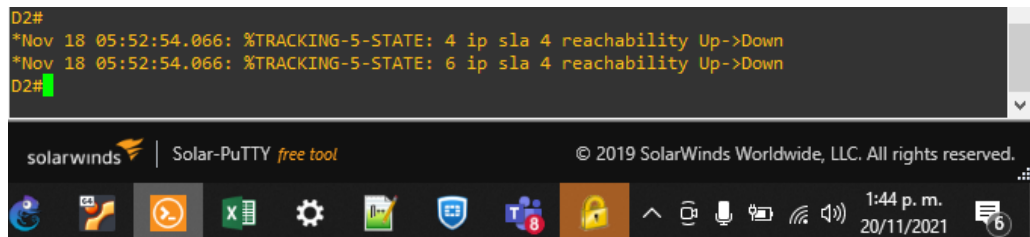


Figura 50. Evento interfaz G0/0 de R3 disponible

```
D2#
*Nov 18 05:53:44.110: %TRACKING-5-STATE: 4 ip sla 4 reachability Down->Up
*Nov 18 05:53:44.110: %TRACKING-5-STATE: 6 ip sla 4 reachability Down->Up
D2#
```

### 4.3 En D1 configure HSRPv2.

Comando	Explicación
interface vlan 100	Configura interface virtual para la VLAN 100
standby version 2	Establece la versión 2 de HSRP
standby 104 ip 10.0.100.254	Configura la dirección virtual para grupo 104
standby 104 priority 150	Establece la prioridad del grupo 104 en 150
standby 104 preempt	Habilita la preferencia
standby 104 track 4 decrement 60	Rastree el objeto 4 para disminuir en 60

Figura 51. Verificación HSRP VLAN 100 en D1

```
D1#show standby vlan 100
Vlan100 - Group 104 (version 2)
  State is Active
    2 state changes, last state change 00:19:35
  Virtual IP address is 10.0.100.254
  Active virtual MAC address is 0000.0c9f.f068 (MAC In Use)
  Local virtual MAC address is 0000.0c9f.f068 (v2 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.920 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
  Track object 4 state Up decrement 60
  Group name is "hsrp-V1100-104" (default)
D1#
```

<b>Comando</b>	<b>Explicación</b>
interface vlan 101	Configura interface virtual para la VLAN 101
standby version 2	Establece la versión 2 de HSRP
standby 114 ip 10.0.101.254	Configura la dirección virtual para grupo 114
standby 114 preempt	Habilita la preferencia
standby 114 track 4 decrement 60	Rastree el objeto 4 para disminuir en 60

Figura 52. Verificación HSRP VLAN 101 en D1

```

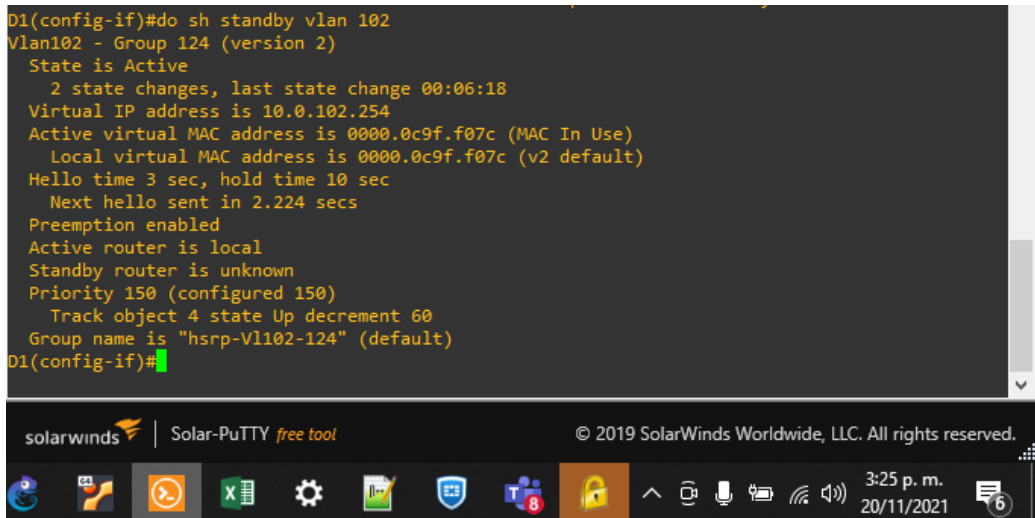
D1(config)#do sh standby vlan 101
Vlan101 - Group 114 (version 2)
  State is Active
    2 state changes, last state change 00:00:08
  Virtual IP address is 10.0.101.254
  Active virtual MAC address is 0000.0c9f.f072 (MAC In Use)
  Local virtual MAC address is 0000.0c9f.f072 (v2 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.640 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Track object 4 state Up decrement 60
  Group name is "hsrp-Vl101-114" (default)
D1(config)#

```

<b>Comando</b>	<b>Explicación</b>
interface vlan 102	<i>Configura interface virtual para la VLAN 102</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 124 ip 10.0.102.254	<i>Configura la dirección virtual para grupo 124</i>
standby 124 priority 150	<i>Establece la prioridad del grupo 124 en 150</i>
standby 124 preempt	<i>Habilita la preferencia</i>
standby 124 track 4 decrement 60	<i>Rastree el objeto 4 para disminuir en 60</i>

Figura 53. Verificación HSRP VLAN 101 en D1

```
D1(config-if)#do sh standby vlan 102
Vlan102 - Group 124 (version 2)
  State is Active
    2 state changes, last state change 00:06:18
  Virtual IP address is 10.0.102.254
  Active virtual MAC address is 0000.0c9f.f07c (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f07c (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.224 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
    Track object 4 state Up decrement 60
  Group name is "hsrp-V1102-124" (default)
D1(config-if)#
```



**Comando**

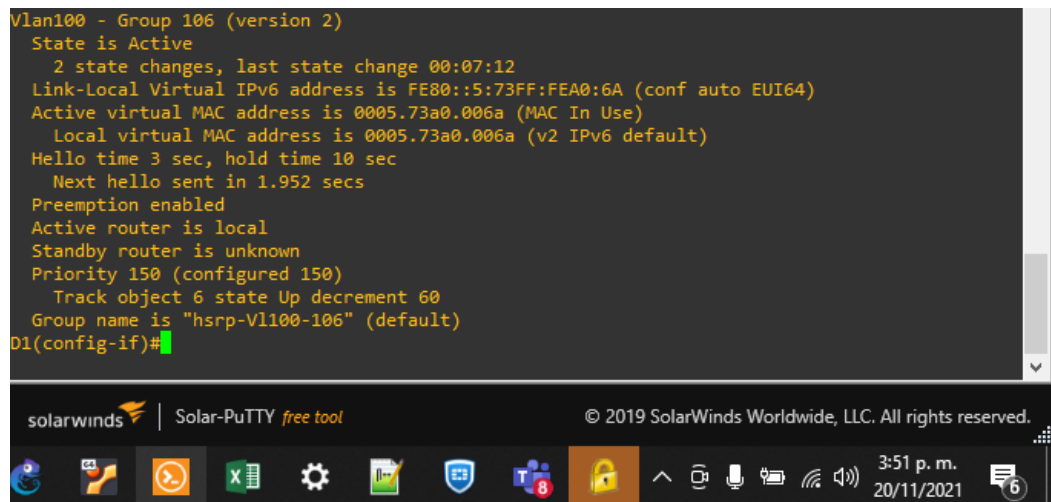
interface vlan 100  
standby version 2  
standby 106 ipv6 autoconfig  
standby 106 priority 150  
standby 106 preempt  
standby 106 track 6 decrement 60

**Explicación**

*Configura interface virtual para la VLAN 100*  
*Establece la versión 2 de HSRP*  
*Configura la dirección virtual para grupo 106*  
*Establece la prioridad del grupo 106 en 150*  
*Habilita la preferencia*  
*Rastree el objeto 6 para disminuir en 60*

Figura 54. Verificación HSRP VLAN 100 IPV6 en D1

```
Vlan100 - Group 106 (version 2)
  State is Active
    2 state changes, last state change 00:07:12
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:6A (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.006a (MAC In Use)
    Local virtual MAC address is 0005.73a0.006a (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.952 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
    Track object 6 state Up decrement 60
  Group name is "hsrp-V1100-106" (default)
D1(config-if)#
```



<b>Comando</b>	<b>Explicación</b>
interface vlan 101	Configura interface virtual para la VLAN 101
standby version 2	Establece la versión 2 de HSRP
standby 116 ipv6 autoconfig	Configura la dirección virtual para grupo 116
standby 116 preempt	Habilita la preferencia
standby 116 track 6 decrement 60	Rastree el objeto 6 para disminuir en 60

Figura 55. Verificación HSRP VLAN 101 IPV6 en D1

```

Vlan101 - Group 116 (version 2)
State is Active
  2 state changes, last state change 00:00:50
Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:74 (conf auto EUI64)
Active virtual MAC address is 0005.73a0.0074 (MAC In Use)
Local virtual MAC address is 0005.73a0.0074 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.384 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
Track object 6 state Up decrement 60
Group name is "hsrp-V101-116" (default)
D1(config-if)#

```

<b>Comando</b>	<b>Explicación</b>
interface vlan 102	Configura interface virtual para la VLAN 102
standby version 2	Establece la versión 2 de HSRP
standby 126 ipv6 autoconfig	Configura la dirección virtual para grupo 126
standby 126 priority 150	Establece la prioridad del grupo 126 en 150
standby 126 preempt	Habilita la preferencia
standby 126 track 6 decrement 60	Rastree el objeto 6 para disminuir en 60



Figura 56. Verificación HSRP VLAN 102 IPV6 en D1

```

Group Name is "hsrp-Vl102-126" (default)
Vlan102 - Group 126 (version 2)
  State is Active
    2 state changes, last state change 00:01:07
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:7E (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.007e (MAC In Use)
  Local virtual MAC address is 0005.73a0.007e (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.672 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
  Track object 6 state Up decrement 60
  Group name is "hsrp-Vl102-126" (default)
D1(config-if)#

```

#### 4.4 En D2 configure HSRPv2.

Comando	Explicación
interface vlan 100	Configura interface virtual para la VLAN 100
standby version 2	Establece la versión 2 de HSRP
standby 104 ip 10.0.100.254	Configura la dirección virtual para grupo 104
standby 104 preempt	Habilita la preferencia
standby 104 track 4 decrement 60	Rastree el objeto 4 para disminuir en 60

Figura 57. Verificación HSRP VLAN 100 IPV4 en D2

```
D2#show standby vlan 100
Vlan100 - Group 104 (version 2)
  State is Active
    2 state changes, last state change 00:06:13
  Virtual IP address is 10.0.100.254
  Active virtual MAC address is 0000.0c9f.f068 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f068 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.728 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
    Track object 4 state Up decrement 60
  Group name is "hsrp-Vl100-104" (default)
D2#
```

<b>Comando</b>	<b>Explicación</b>
interface vlan 101	<i>Configura interface virtual para la VLAN 101</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 114 ip 10.0.101.254	<i>Configura la dirección virtual para grupo 114</i>
standby 114 priority 150	<i>Establece la prioridad del grupo 114 en 150</i>
standby 114 preempt	<i>Habilita la preferencia</i>
standby 114 track 4 decrement 60	<i>Rastree el objeto 4 para disminuir en 60</i>

Figura 58. Verificación HSRP VLAN 101 IPV4 en D2

```
D2#show standby vlan 101
Vlan101 - Group 114 (version 2)
  State is Active
    2 state changes, last state change 00:06:08
  Virtual IP address is 10.0.101.254
  Active virtual MAC address is 0000.0c9f.f072 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f072 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.056 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
    Track object 4 state Up decrement 60
  Group name is "hsrp-Vl101-114" (default)
```

<b>Comando</b>	<b>Explicación</b>
interface vlan 102	<i>Configura interface virtual para la VLAN 102</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 124 ip 10.0.102.254	<i>Configura la dirección virtual para grupo 124</i>
standby 124 preempt	<i>Habilita la preferencia</i>
standby 124 track 4 decrement 60	<i>Rastree el objeto 4 para disminuir en 60</i>

Figura 59. Verificación HSRP VLAN 102 IPV4 en D2

```

D2#show standby vlan 102
Vlan102 - Group 124 (version 2)
  State is Active
    2 state changes, last state change 00:01:31
  Virtual IP address is 10.0.102.254
  Active virtual MAC address is 0000.0c9f.f07c (MAC In Use)
  Local virtual MAC address is 0000.0c9f.f07c (v2 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.160 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Track object 4 state Up decrement 60
  Group name is "hsrp-V1102-124" (default)
D2#

```

<b>Comando</b>	<b>Explicación</b>
interface vlan 100	<i>Configura interface virtual para la VLAN 100</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 106 ipv6 autoconfig	<i>Configura la dirección virtual para grupo 106</i>
standby 106 priority 150	<i>Establece la prioridad del grupo 106 en 150</i>
standby 106 preempt	<i>Habilita la preferencia</i>
standby 106 track 6 decrement 60	<i>Rastree el objeto 6 para disminuir en 60</i>

Figura 60. Verificación HSRP VLAN 100 IPV6 en D2

```
Vlan100 - Group 106 (version 2)
State is Active
  2 state changes, last state change 00:01:44
Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:6A (conf auto EUI64)
Active virtual MAC address is 0005.73a0.006a (MAC In Use)
  Local virtual MAC address is 0005.73a0.006a (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.296 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 150 (configured 150)
  Track object 6 state Up decrement 60
Group name is "hsrp-Vl100-106" (default)
```

<b>Comando</b>	<b>Explicación</b>
interface vlan 101	<i>Configura interface virtual para la VLAN 101</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 116 ipv6 autoconfig	<i>Configura la dirección virtual para grupo 116</i>
standby 116 preempt	<i>Habilita la preferencia</i>
standby 116 track 6 decrement 60	<i>Rastree el objeto 6 para disminuir en 60</i>

Figura 61. Verificación HSRP VLAN 101 IPV6 en D2

```
Vlan101 - Group 116 (version 2)
State is Active
  2 state changes, last state change 00:02:06
Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:74 (conf auto EUI64)
Active virtual MAC address is 0005.73a0.0074 (MAC In Use)
  Local virtual MAC address is 0005.73a0.0074 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.432 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 100 (default 100)
  Track object 6 state Up decrement 60
Group name is "hsrp-Vl101-116" (default)
```

<b>Comando</b>	<b>Explicación</b>
interface vlan 102	<i>Configura interface virtual para la VLAN 102</i>
standby version 2	<i>Establece la versión 2 de HSRP</i>
standby 126 ipv6 autoconfig	<i>Configura la dirección virtual para grupo 126</i>
standby 126 priority 150	<i>Establece la prioridad del grupo 126 en 150</i>
standby 126 preempt	<i>Habilita la preferencia</i>
standby 126 track 6 decrement 60	<i>Rastree el objeto 6 para disminuir en 60</i>

Figura 62. Verificación HSRP VLAN 102 IPV6 en D2

```
Vlan102 - Group 126 (version 2)
  State is Active
    2 state changes, last state change 00:02:19
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:7E (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.007e (MAC In Use)
    Local virtual MAC address is 0005.73a0.007e (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.408 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
    Track object 6 state Up decrement 60
  Group name is "hsrp-Vl102-126" (default)
```

## 5. Parte 5: Seguridad

**5.1** En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de cifrado SCRYPT.

Se ejecuta el siguiente comando en los dispositivos R1, R2, R3, D1, D2 y A1 para proteger el modo privilegiado.

<b>Comando</b>	<b>Explicación</b>
<code>enable secret cisco12345cisco</code>	<i>Habilita la contraseña cifrada para el modo exec privilegiado.</i>

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

Se ejecuta el siguiente comando en los dispositivos R1, R2, R3, D1, D2 y A1 para crear un usuario local con privilegios de administrador, adicional se cifra la contraseña con el algoritmo SCRYPT.

<b>Comando</b>	<b>Explicación</b>
<code>username sadmin privilege 15 secret cisco12345cisco</code>	<i>Crea un usuario con privilegios de administrador y contraseña cifrada</i>

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

Se ejecuta el siguiente comando en los dispositivos R1, R3, D1, D2 y A1 para habilitar el modelo de seguridad triple A.

<b>Comando</b>	<b>Explicación</b>
<code>aaa new-model</code>	<i>Habilita el modelo de seguridad triple a</i>

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

Se ejecutan los siguientes comandos en los dispositivos R1, R3, D1, D2 y A1 para configurar direcciones IP y puertos del servidor radius, adicional se establece la contraseña para autenticarse ante él.

Comando	Explicación
radius server radius-aaa	Nombra la configuración del servidor radius.
address ipv4 10.0.100.6 auth-port 1812	Configura la dirección IP del servidor y puerto de autenticación.
address ipv4 10.0.100.6 acct-port 1813	Establece el puerto de registro.
key \$strongPass	Configura la contraseña de conexión.

Figura 63. Configuración servidor radius en R1

```
R1#show running-config | section radius
radius server radius-aaa
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
R1#
```

Figura 64. Configuración servidor radius en R3

```
R3#show running-config | section radius
radius server radius-aaa
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
R3#
```

Figura 65. Configuración servidor radius en D1

```
D1#show running-config | section radius
radius server radius-aaa
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
D1#
```

Figura 66. Configuración servidor radius en D2

```
D2#show running-config | section radius
radius server radius-aaa
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
D2#
```

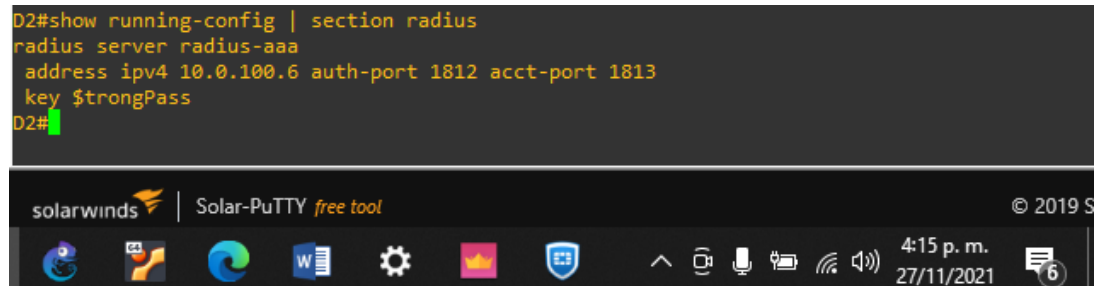
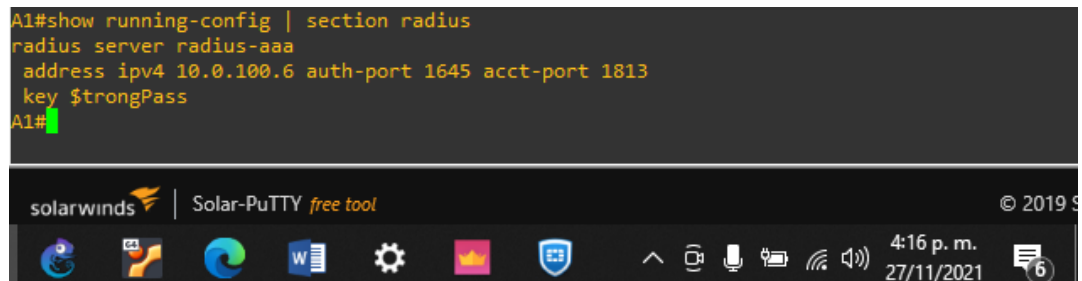


Figura 67. Configuración servidor radius en A1

```
A1#show running-config | section radius
radius server radius-aaa
  address ipv4 10.0.100.6 auth-port 1645 acct-port 1813
  key $strongPass
A1#
```



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

Se ejecutan los siguientes comandos en los dispositivos R1, R3, D1, D2 y A1 para configurar las listas de autenticación del modelo triple A.

**Comando**

aaa authentication login default  
group radius local

**Explicación**

*Configura la lista predeterminada para el modelo triple a, validando los usuario primero en servidor radius y luego localmente.*



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

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

Se ejecutan los siguientes comandos en los dispositivos R1, R2, R3, D1, D2 y A1 para configurar la zona horaria local y la hora actual.

Comando	Explicación
clock timezone UTC -5	Configura la zona horaria UTC
clock set 15:13:10 21 nov 2021	Establece la hora y fecha actual.

Figura 68. Verificación hora en R1

```
R1#show clock detail
15:49:57.527 UTC Thu Nov 25 2021
Time source is NTP
R1#
```

Figura 69. Verificación hora en R2

```
R2#show running-config | section radius
R2#show clock detail
15:53:14.374 UTC Thu Nov 25 2021
Time source is NTP
R2#
```

Figura 70. Verificación hora en R3

```
R3#show clock detail
15:53:01.313 UTC Thu Nov 25 2021
Time source is NTP
R3#
```

Figura 71. Verificación hora en D1

```
D1#show clock detail
*21:09:19.557 UTC Thu Nov 25 2021
Time source is NTP
D1#
```

Figura 72. Verificación hora en D2

```
D2#show clock detail
*21:10:30.381 UTC Thu Nov 25 2021
Time source is NTP
D2#
```

Figura 73. Verificación hora en A1

```
A1#show clock detail
*21:11:25.549 UTC Thu Nov 25 2021
Time source is hardware calendar
A1#
```

## 6.2 Configure R2 como un NTP maestro.

Se ejecutan los siguientes comandos en los dispositivos R1, R2, R3, D1, D2 y A1 para configurar el router R2 como servidor NTP maestro.

Comando	Explicación
ntp master 3	Configura R2 como NTP maestro stratum 3

Figura 74. Verificación NTP en R2

```
R2#show ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**16
ntp uptime is 25085000 (1/100 of seconds), resolution is 4000
reference time is E54A7A73.921ED318 (16:11:15.570 UTC Thu Nov 25 2021)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.41 msec, peer dispersion is 0.24 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.00000000 s/s
system poll interval is 16, last update was 11 sec ago.
R2#
```

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

Se ejecutan los siguientes comandos en los dispositivos R1, R3, D1, D2 y A1 para configurar los compañeros NTP de acuerdo a las especificaciones.

<b>Comando</b>	<b>Explicación</b>
ntp peer 2.2.2.2	Configura a R2 como peer NTP para R1
ntp peer 10.0.13.1	Configura a R1 como peer NTP para R2, D1 y A1
ntp peer 10.0.10.1	Configura a R1 como peer NTP para D1 y A1
ntp peer 10.0.11.1	Configura a R3 como peer NTP para D2

Figura 75. Verificación asociaciones NTP en R1

```
R1#show ntp associations
address          ref clock      st  when  poll reach  delay  offset  disp
*~2.2.2.2        127.127.1.1   3   56   1024  377  8.232  -1.127  3.205
 10.0.13.3       10.0.13.1    5   64   1024  377  4.124  -28.261  3.685
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
R1#
```

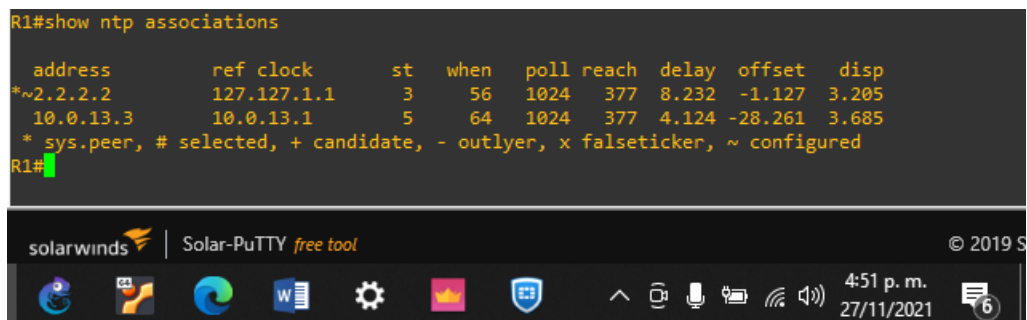


Figura 76. Verificación asociaciones NTP en R3

```
R3#show ntp associations
address          ref clock      st  when  poll reach  delay  offset  disp
*~10.0.13.1      2.2.2.2       4   68   128   375  8.056  13.663  5.563
 10.0.11.2       .INIT.        16  837  1024  0   0.000  0.000  15937.
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
R3#
```

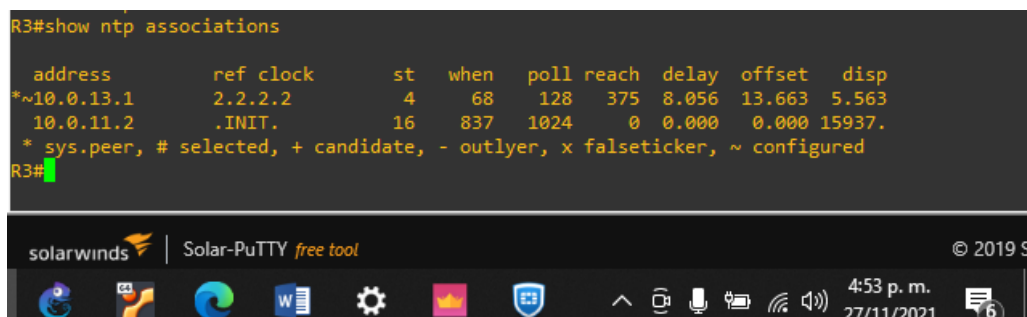


Figura 77. Verificación asociaciones NTP en D1

```
D1#show ntp associations
address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.13.1   .STEP.         16   -    1024   0  0.000  0.000 15937.
~10.0.10.1   .INIT.         16 247113 1024   0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
D1#
```

Figura 78. Verificación asociaciones NTP en D2

```
D2#show ntp associations
address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.11.1   .INIT.         16 187769 1024   0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
D2#
```

#### 6.4 Configure Syslog en todos los dispositivos excepto R2.

Se ejecutan los siguientes comandos en los dispositivos R1, R3, D1, D2 y A1 para configurar el servidor que recibirá los registros de eventos, adicional se establece el nivel 4.

##### Comando

Logging 10.0.100.5

Logging trap warning

##### Explicación

*Configura el servidor destino donde se envían los mensajes syslog.*

*Configura el nivel de mensajes que serán enviados.*

Figura 79. Configuración syslog R1

```
R1#sho running-config | include logging
logging trap warnings
logging host 10.0.100.5
  logging synchronous
  logging synchronous
R1#
```

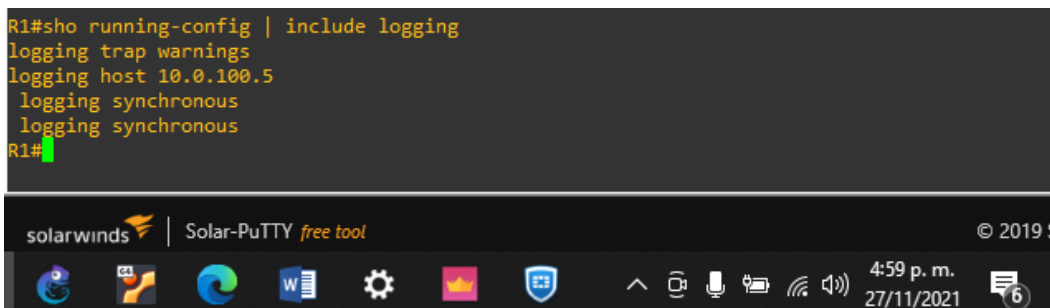


Figura 80. Configuración syslog R3

```
R3#sho running-config | include logging
logging trap warnings
logging host 10.0.100.5
  logging synchronous
  logging synchronous
R3#
```

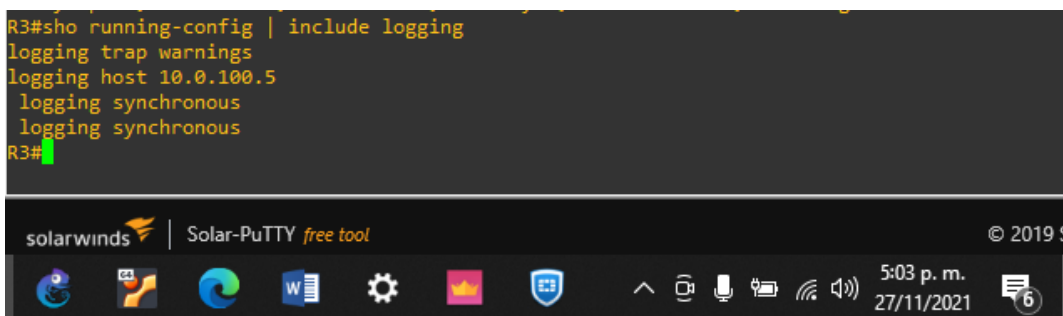


Figura 81. Configuración syslog D1

```
D1#sho running-config | include logging
logging trap warnings
logging host 10.0.100.5
  logging synchronous
  logging synchronous
D1#
```

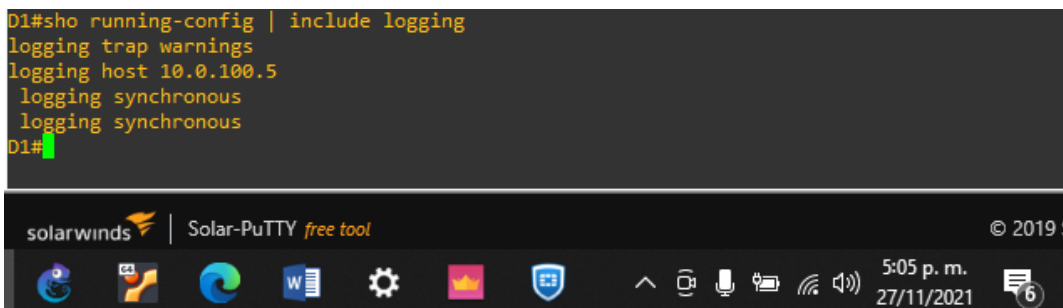
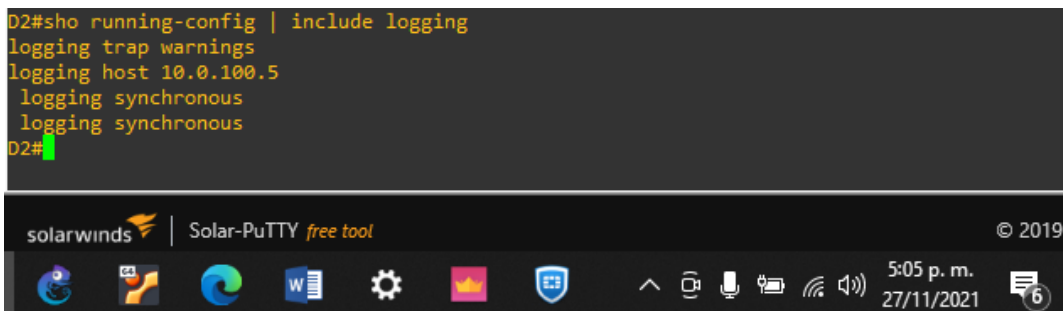


Figura 82. Configuración syslog D2

```
D2#sho running-config | include logging
logging trap warnings
logging host 10.0.100.5
  logging synchronous
  logging synchronous
D2#
```



## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Se ejecutan los siguientes comandos en los dispositivos R1, R3, D1, D2 y A1 para configurar el servicio SNMP

<b>Comando</b>	<b>Explicación</b>
snmp-server community ENCORSA ro 60	<i>Establece el nombre de la comunidad en modo solo lectura y especifica la lista de acceso 60 que solo permite acceso a la IP de la PC 1.</i>
snmp-server contact Oscar.ramirez@CCNP.com	<i>Configura el nivel de mensajes que serán enviados</i>
access-list 60 permit host 10.0.100.5 log	<i>Configura la lista de control de acceso solo para permitir la PC 1.</i>
snmp-server enable traps config	<i>Comando para enviar traps de configuración en R1, R3, D1, D2 y A1</i>
snmp-server enable traps bgp	<i>Comando para enviar traps de BGP en R1</i>
snmp-server enable traps ospf	<i>Comando para enviar traps de OSPF en R1</i>

## **CONCLUSIONES**

Segmentar la red es muy importante porque aísla el tráfico y evita que pueda ser escuchado por equipos que no pertenecen al mismo departamento, adicional reduce la congestión de los enlaces e incrementa los niveles de seguridad.

Se concluye que para garantizar la disponibilidad de la infraestructura de red , es vital construirla de manera redundante, de tal modo que si hay un punto de falla en la red se vea afectado la menor cantidad posible de usuarios o equipos terminales.

Habilitar STP cuando se tiene un diseño de red jerárquico y redundante es vital, porque este garantiza el óptimo funcionamiento de la capa de conmutación, ya que controla y evita que se formen loops de tráfico sobre enlaces redundantes.

Los equipos administrados deben ser configurados con parámetros de seguridad que garanticen control de accesos no autorizados, adicional , protocolos como syslog y SNMP pueden ayudar a monitorear la salubridad de los equipos.

## BIBLIOGRAFÍA

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Advanced OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGq5JUgUBthk8>

EDGEWORTH, B., GARZA RIOS, B., GOOLEY, J., HUCABY, D. (2020). CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGq5JUgUBthk8>

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!AAIGq5JUgUBthk8>

FROOM, R., FRAHIM, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmJYei-NT1lnWR0hoMxgBNv1CJ>

TEARE, D., VACHON B., GRAZIANI, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmJYei-NT1lnMfy2rhPZHwEoWx>