DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NARCISO MANUEL MEJIA REYES

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NARCISO MANUEL MEJIA REYES

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

DIRECTOR: MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Barranquilla, 29 de noviembre del 2021

1. AGRADECIMIENTOS

Primeramente, doy gracias a Dios por la vida, a mi familia a mi esposa a mi hija, a mis padres y hermanos, ellos son mi motor, todos me apoyaron en este proceso y a pesar de las adversidades, siempre mantuvieron la confianza y la esperanza de superación tanto en lo personal como en lo profesional, aspectos que me ayudaron a formarme como ingeniero de telecomunicaciones.

CONTENIDO

2. LISTA DE FIGURAS

3. GLOSARIO

ENRUTAMIENTO: Es el proceso el cual permite que los paquetes entre redes y a la vez buscando la mejor ruta para que esos paquetes lleguen a su destino.

WAN: (Wide Área Network, o WAN) es una red privada y amplia consiste en varias redes locales unidad.

LAN: (Local Área Network): son un conjunto de dispositivos electrónicos conectados entre sí.

VLAN: (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

INTERFAZ: Es el elemento que sirve para indicar el enlace que se da de manera física.

GATEWAY: También llamado puerta de enlace puerta es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, ingresar a otra red.

DNS: Domain Name System” (Sistema de Nombre de Dominio). DNS es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.

COMANDO: Es una instrucción que se le da a un programa para que realice una tarea especifica.

4. RESUMEN

Las nuevas tecnologías de la información se han convertido en una revolución a nivel mundial, estas se adoptaron con gran auge porque ayudan al desarrollo de diferentes sectores como: Económico, social, político, etc. Hecho que ha generado una competitividad positiva en todos los ámbitos, de esta forma el hombre busca a diario una optimización en esta rama, la cual logra desarrollo a gran escala en la electrónica y las telecomunicaciones.

El diplomado de profundización de CISCO CCNP permite escalar y profundizar los diferentes temas, logrando habilidades y destreza a través de la investigación y la practica en cuanto a las redes LAN Y WAN. Apoyándome en los diferentes recursos y simuladores como los son GNS3 y Packet Tracert, se realizaron procesos de enrutamiento, Conmutación y comprobación de cada uno de los pasos en el desarrollo del trabajo.

Palabras claves: CISCO, CCNP DNS, LAN, WAN, VLAN, PING, EIGRP, IP, enrutamiento, Conmutación, Redes y electrónica.

ABSTRACT

The new information technologies have become a revolution worldwide, they were adopted with great boom because they help the development of different sectors such as: Economic, social, political, etc. Fact that has generated positive competitiveness in all areas, in this way man seeks daily optimization in this branch, which achieves large-scale development in electronics and telecommunications.

The CISCO CCNP in-depth diploma allows to scale and deepen the different topics, achieving skills and dexterity through research and practice regarding LAN and WAN networks. Relying on the different resources and simulators such as GNS3 and Packet Tracert, routing, switching and checking processes were carried out for each of the steps in the development of the work.

Keywords: CISCO, CCNP DNS, LAN, WAN, VLAN, PING, EIGRP, IP, routing, Switching, Networks and electronics.

5. INTRODUCCION

Este documento es el desarrollo del Diplomado de Profundización CCNP, aquí se ha plasmado lo investigado y aprendido con las competencias dadas en cada guía de estudio a raíz de la solución expuesta, la cual se puso en práctica en el simulador Gns3, tomando como estrategia el enrutamiento y cada una de las configuraciones de los diferentes dispositivos que componen la topología dada.

Los ingenieros de telecomunicaciones muestran habilidades con las que pueden otorgar soluciones a diferentes problemas, por tal razón se puso en práctica los conocimientos obtenidos en el diplomado de profundización CCNP, enfocándonos en la realidad con respecto a las tecnologías de la información.

Se implementó una red de datos que podría presentarse en la vida diaria de cualquier persona o empresa, para ello nos presentan un escenario en cual se realizaran interconexiones y configuraciones de redes adaptándonos en cada paso e identificando los problemas propios del escenario ejecutado en el simulador GNS3 y una máquina virtual.

6. DESARROLLO

Escenario Propuesto

Topología de la Red:

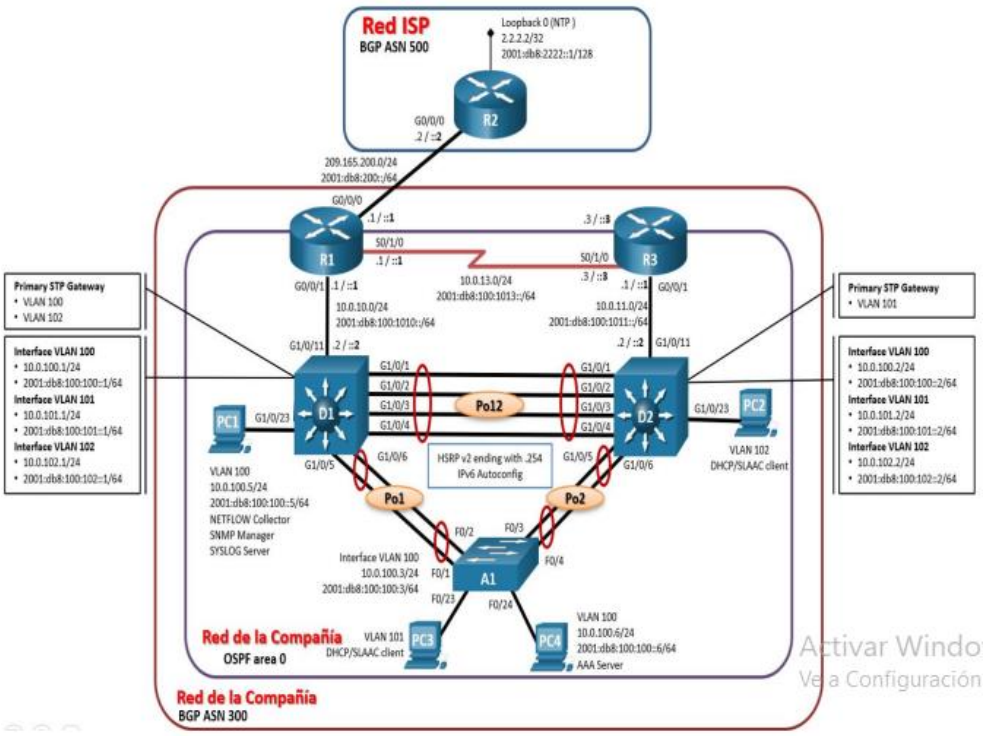

Figura 1. Escenario

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

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

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

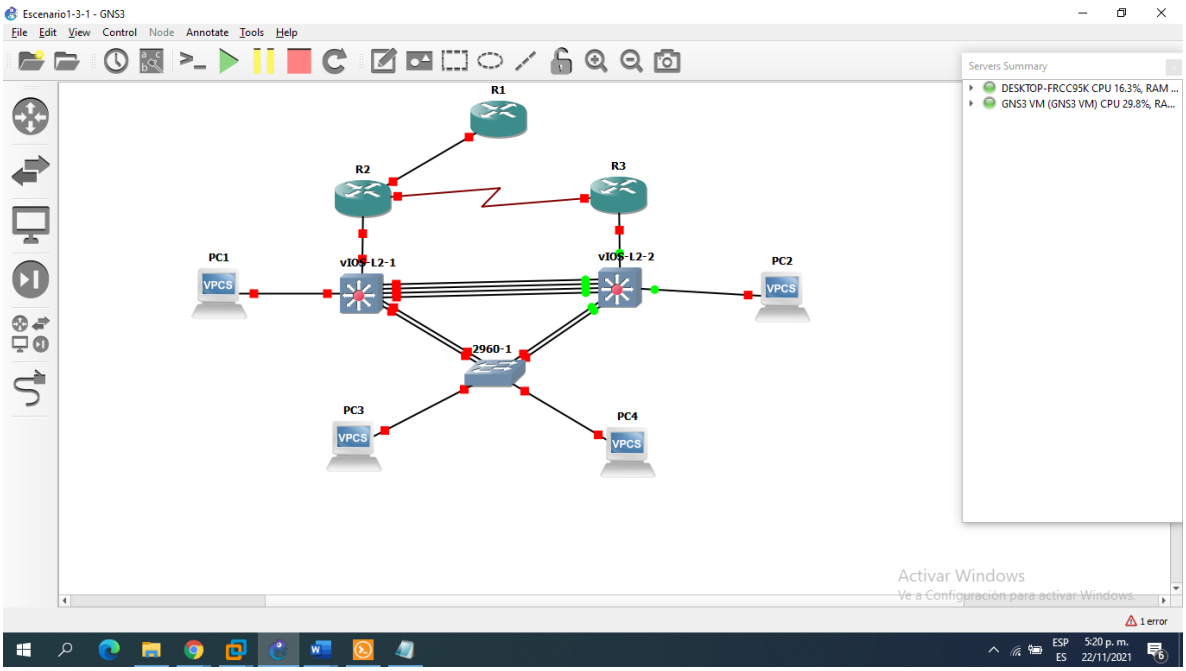

Figura 2. Simulación del escenario

Paso 2: Configurar los parámetros básicos para cada dispositivo.

a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:
b. Copie el archivo running-config al archivo startup-config en todos los dispositivos.
c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne
una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP
utilizada en la Parte 4.

```
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
interface g0/0
 ip address 209.165.200.225 255.255.255.224
 ipv6 address fe80::1:1 link-local
 ipv6 address 2001:db8:200::1/64
 no shutdown
 exit
```

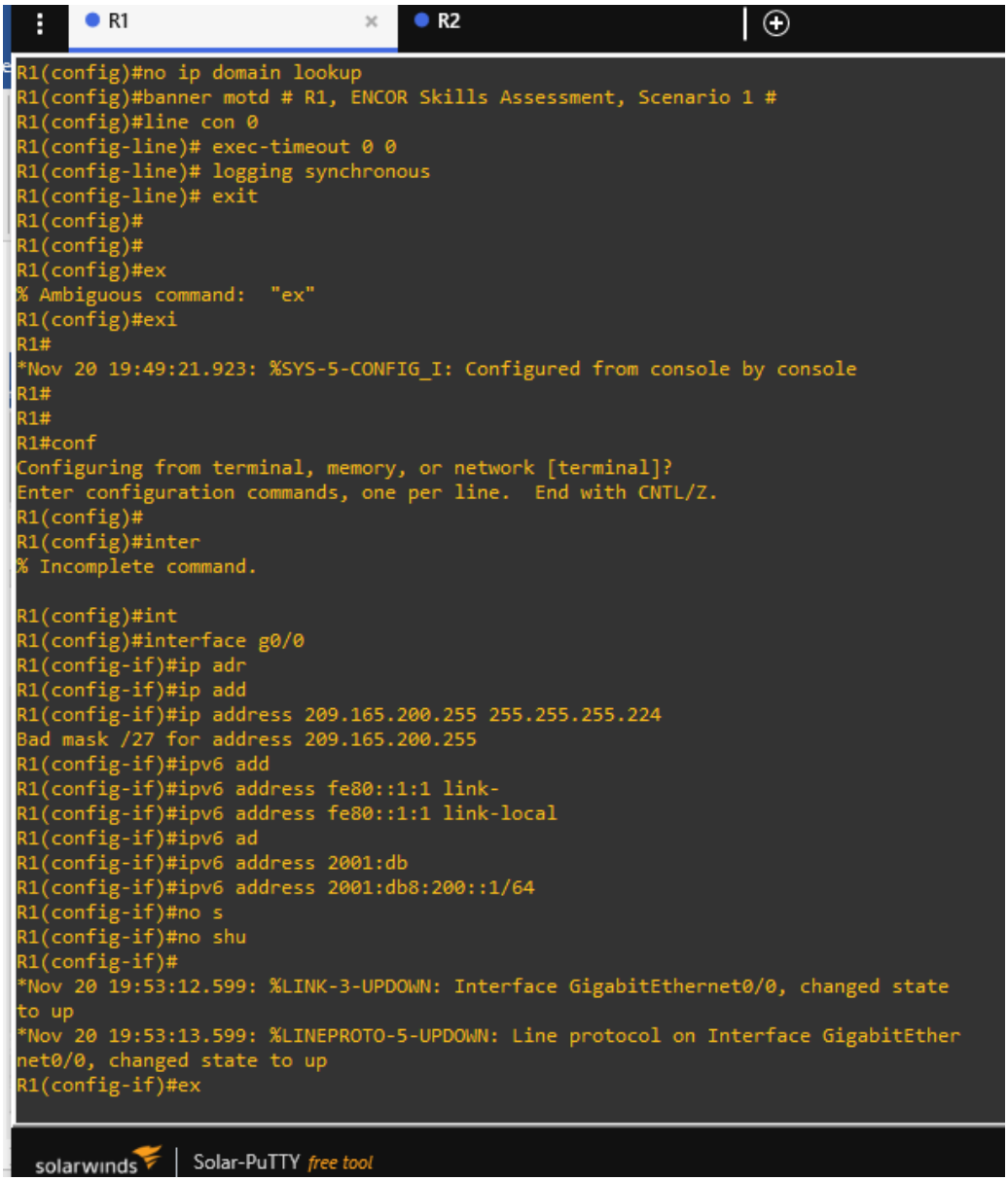

Figura 3. Aplicando código R1

Router R2
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface g0/0

ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit

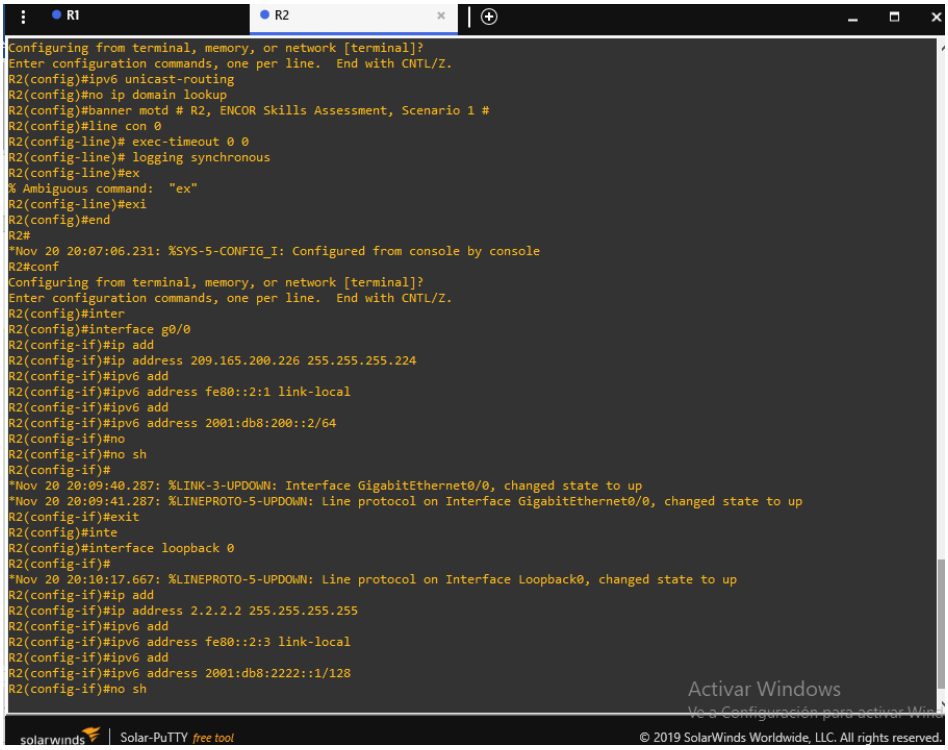

Figura 4. Aplicando código R2

Router R3
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 g2/0

ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s1/0
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
no shutdown
exit

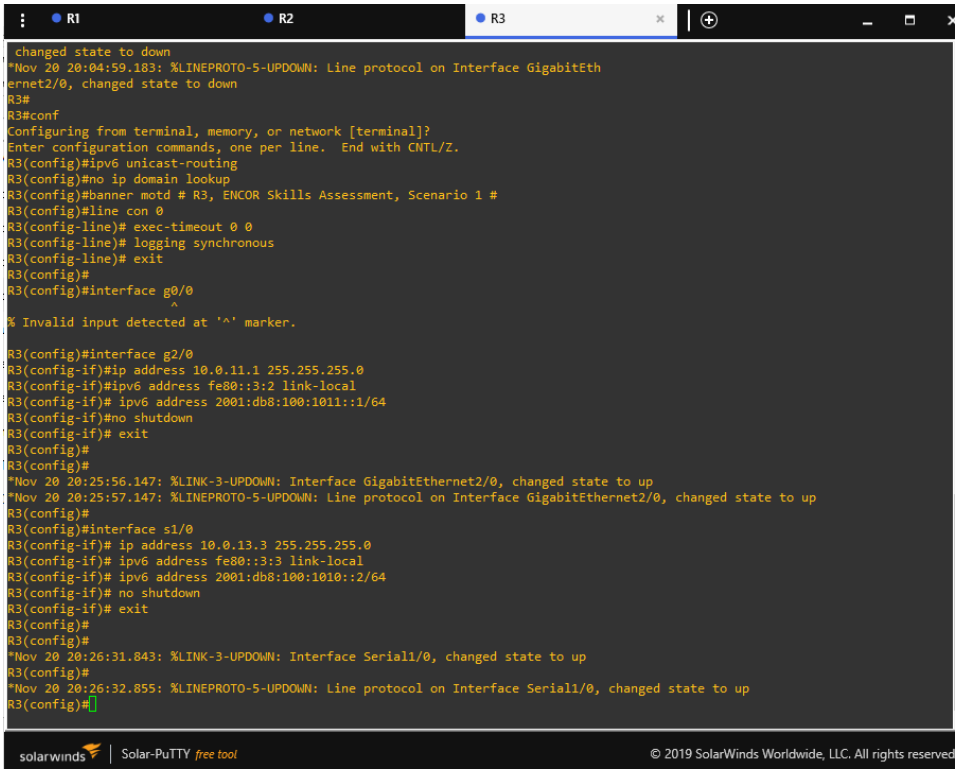

Figura 5. Aplicando código R3

Switch D1

hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous

exit

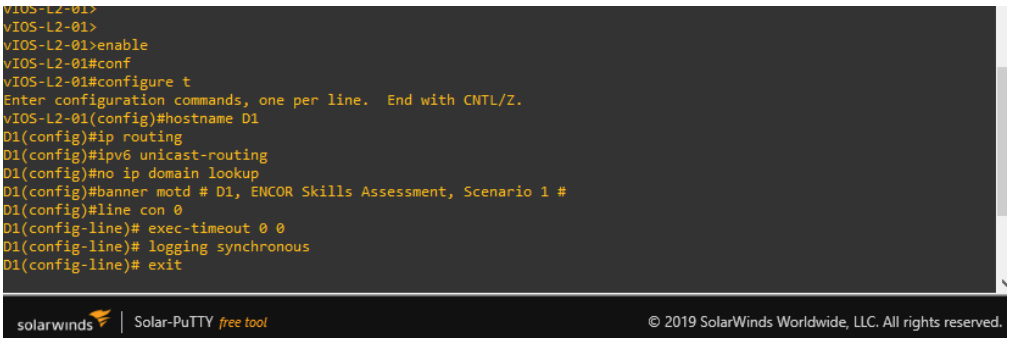

Figura 6. Aplicando código_1 Switch D1

```
vlan 100
 name Management
 exit
vlan 101
 name UserGroupA
 exit
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
interface g0/0
 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
 no shutdown
 exit
interface vlan 100
 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
 no shutdown
 exit
interface vlan 101
 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
 no shutdown
```

```
 exit
interface vlan 102
 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
 no shutdown
 exit
```

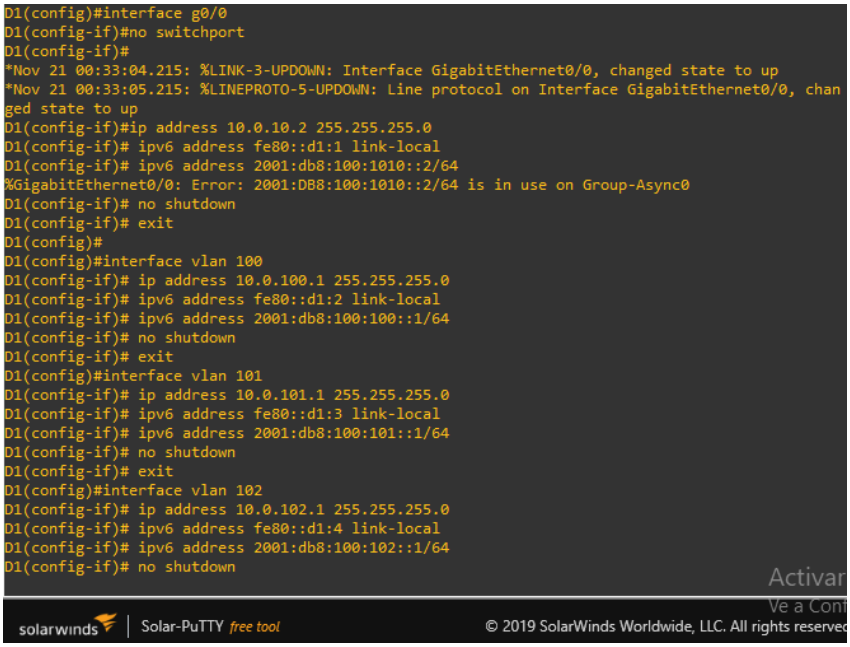

Figura 7. Aplicando código_2 Switch D1

```
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
ip dhcp pool VLAN-101
 network 10.0.101.0 255.255.255.0
 default-router 10.0.101.254
 exit
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
 exit
```

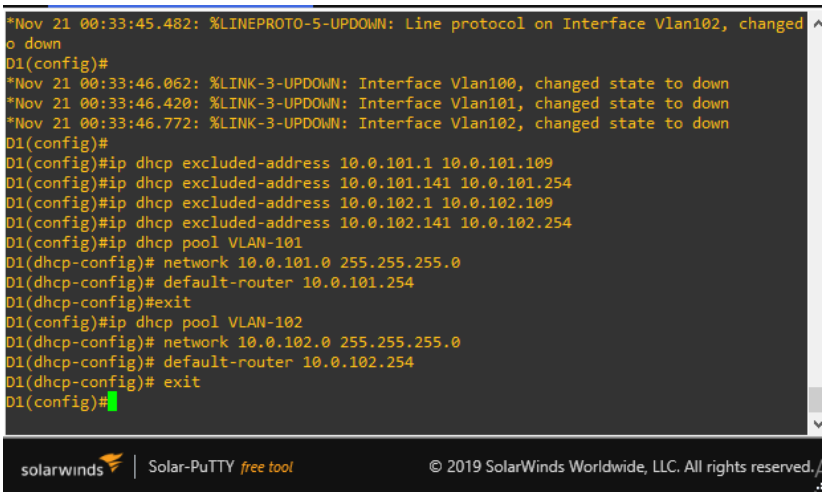

Figura 8. Aplicando código_3 Switch D1

```
interface g0/0
 shutdown
interface g0/1
shutdown
interface g0/2
shutdown
interface g0/3
shutdown
interface g0/4
shutdown
interface g0/5
shutdown
interface g6
shutdown
interface g7
shutdown
interface g8
shutdown
 exit
```

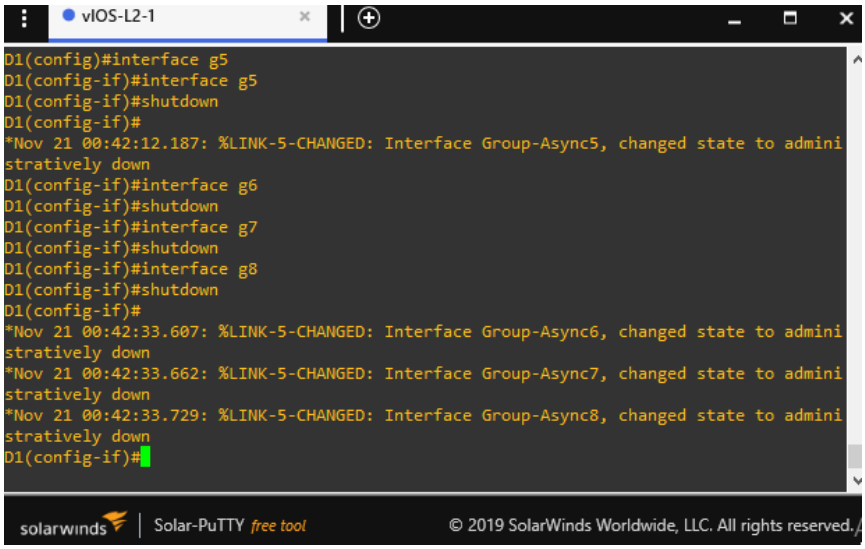

Figura 9. Código Encender interfaces Switch D1

Switch D2

```
hostname D2
ip routing
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
 exit
vlan 101
 name UserGroupA
 exit
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
```

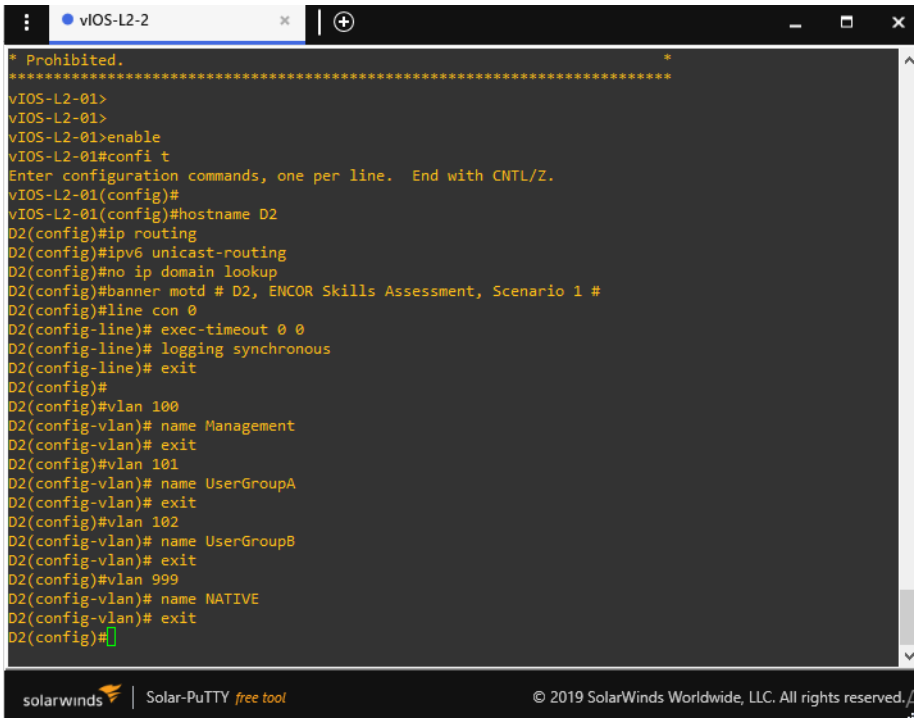

Figura 10. Aplicando código_1 Switch D2

```
interface g0/0
 no switchport
 ip address 10.0.11.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1011::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.0.100.2 255.255.255.0
 ipv6 address fe80::d2:2 link-local
 ipv6 address 2001:db8:100:100::2/64
 no shutdown
 exit
interface vlan 101
 ip address 10.0.101.2 255.255.255.0
 ipv6 address fe80::d2:3 link-local
 ipv6 address 2001:db8:100:101::2/64
 no shutdown
 exit
interface vlan 102
 ip address 10.0.102.2 255.255.255.0
 ipv6 address fe80::d2:4 link-local
```

```
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
```

Figura 11. Aplicando código_2 Switch D2

```
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
 network 10.0.101.0 255.255.255.0
 default-router 10.0.101.254
 exit
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
 exit
interface g0/0
 shutdown
interface g0/1
shutdown
interface g0/2
shutdown
```

interface g0/3
shutdown
interface g0/4
shutdown
interface g0/5
shutdown
interface g6
shutdown
interface g7
shutdown
interface g8
shutdown
exit

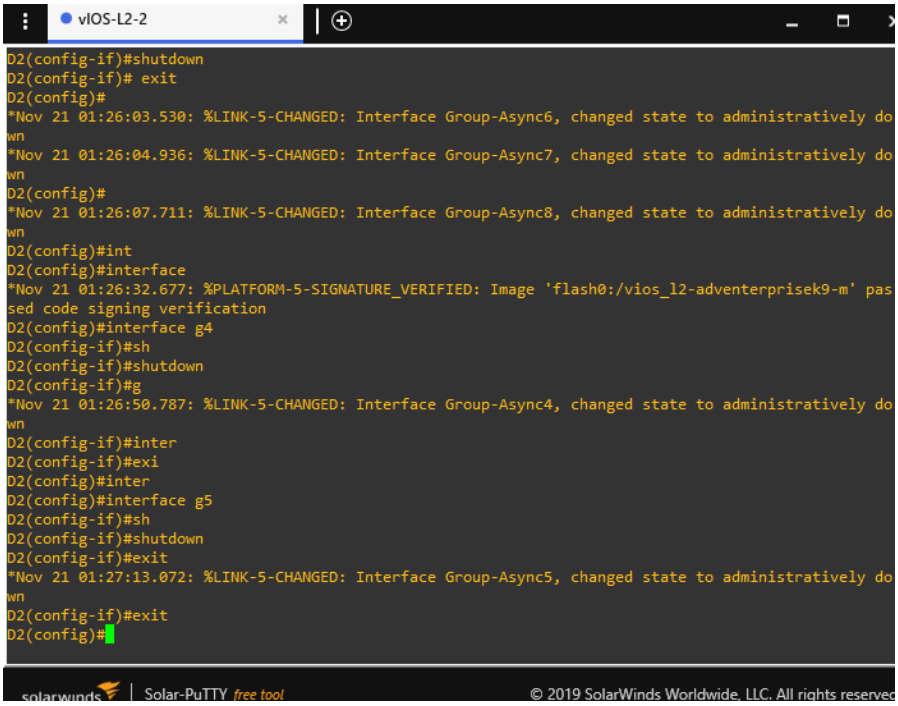

Figura 12. Aplicando código_3 Switch D2

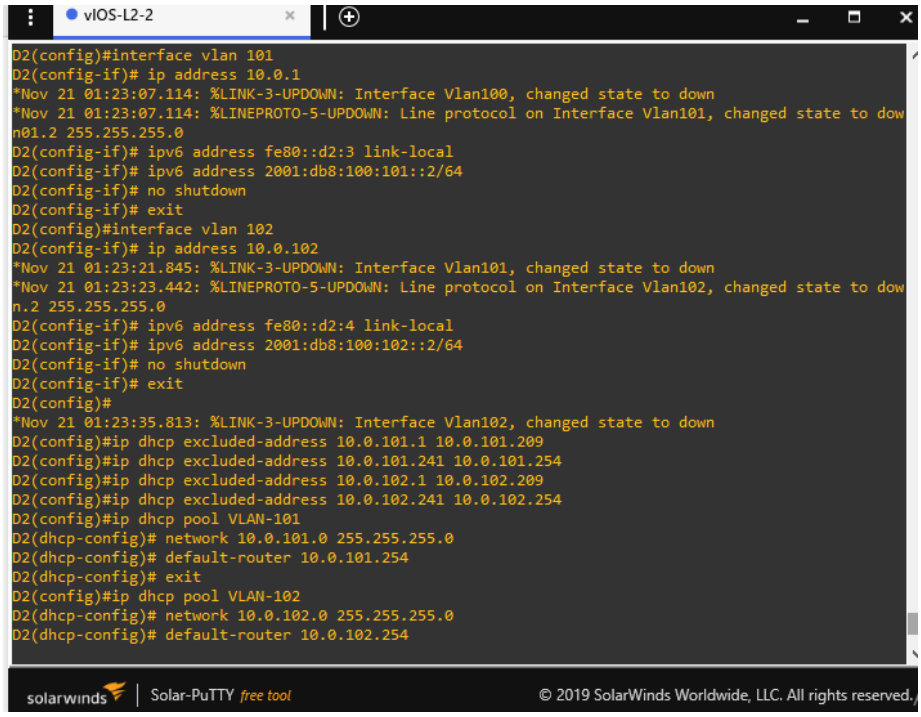

Figura 13. Código Encender interfaces Switch D2

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
vlan 100
 name Management
 exit
vlan 101
 name UserGroupA
 exit
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
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
 exit
interface g0
 shutdown
 exit
interface g1
 shutdown
 exit
interface g2
 shutdown
 exit
interface g3
 shutdown
 exit
interface g4
 shutdown
 exit
interface g5
 shutdown
 exit
```

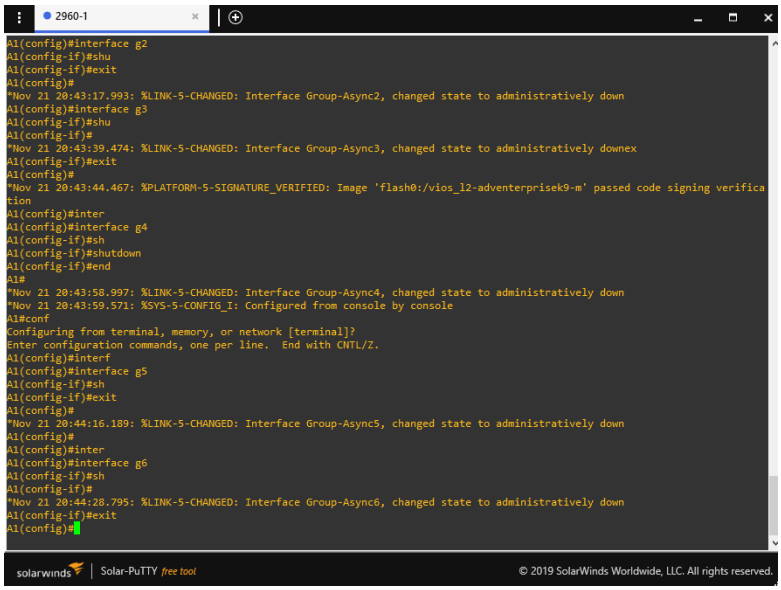

Figura 14. Aplicando código_1 Switch A1

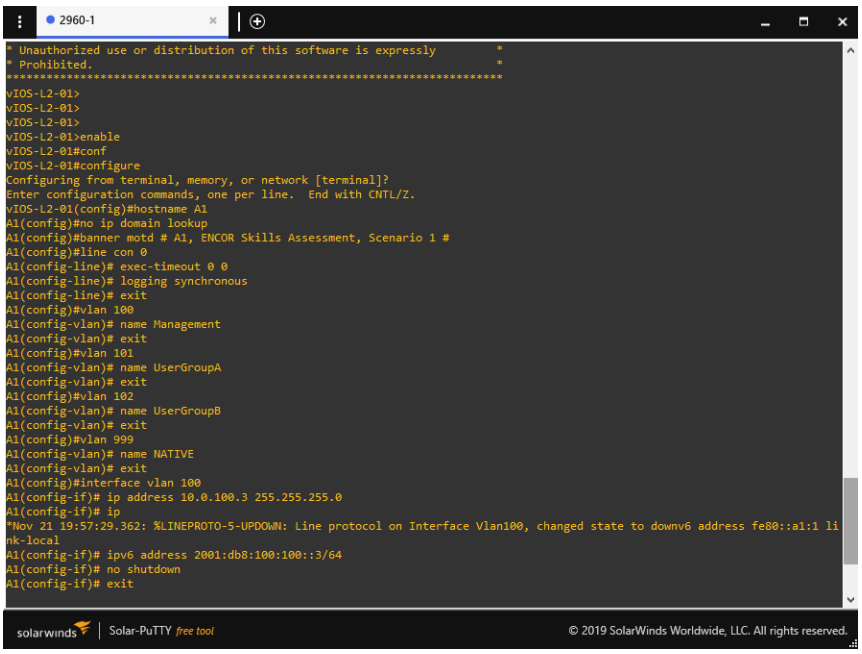

Figura 15. Aplicando código_2 Switch A

5.2 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.

Las tareas de configuración son las siguientes:

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

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

D1#

interf g1/0

switchport trunk encapsulation dot1q

switchport trunk native vlan 999

switchport mode trunk

Figura 16. aplicando codigo show interface trunk D1

D2#
interf g1/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk

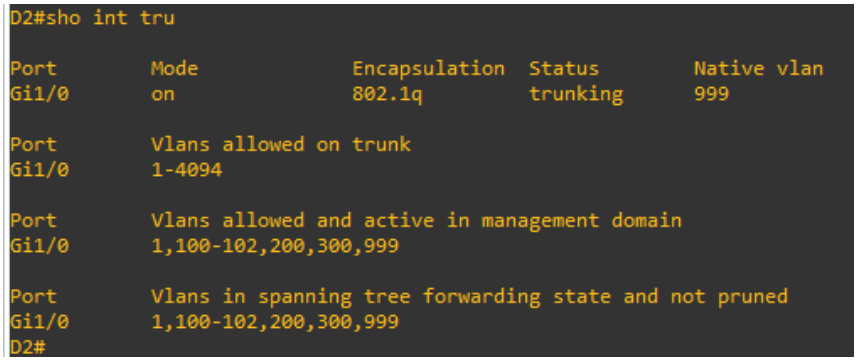

Figura 17. Aplicando codigo show interface trunk D2

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

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

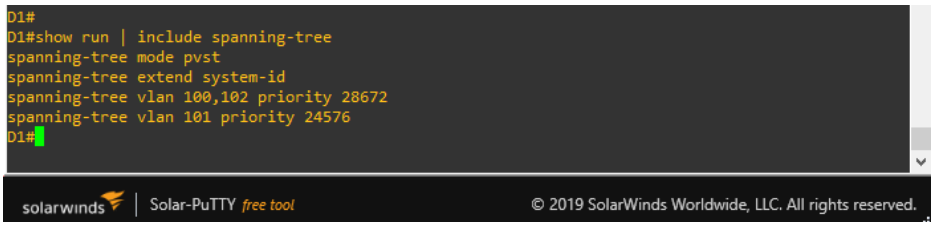

Figura 18. Show run | include spanning-tree D1

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

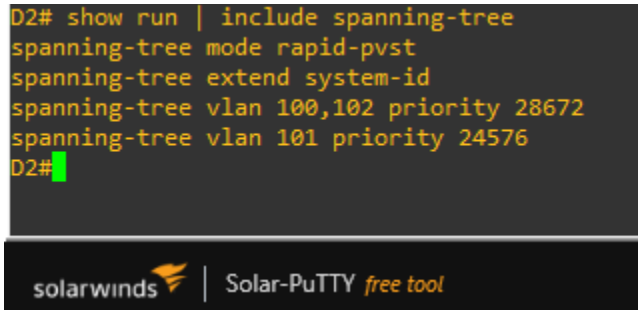

Figura 19. show run | include spanning-tree D2

A1# show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576

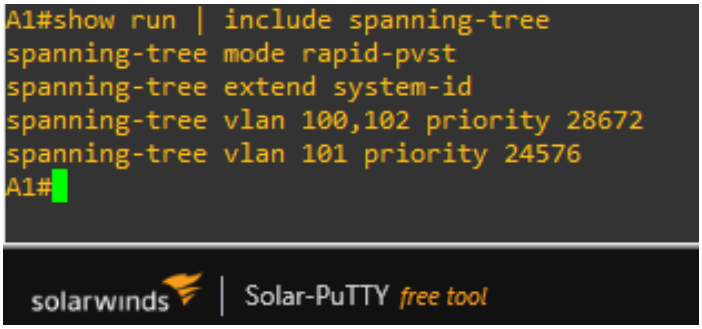

Figura 20. show run | include spanning-tree A1

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

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

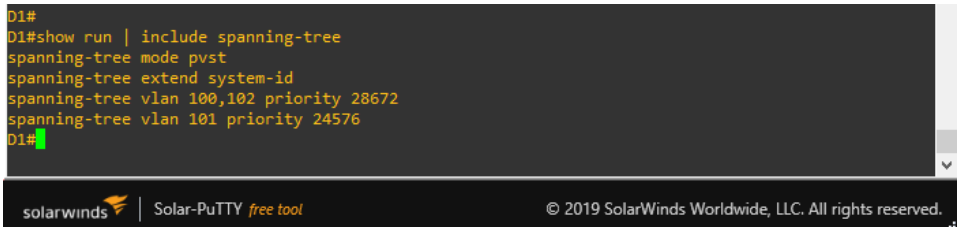

Figura 21. show run | include spanning-tree D1

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

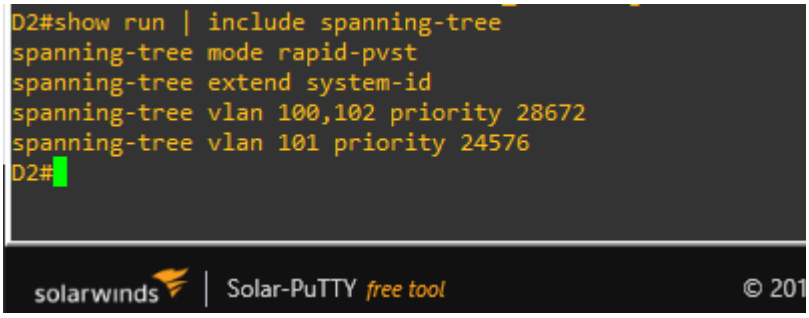

Figura 22. show run | include spanning-tree D2

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

int g0/1
no switchport
channel-group 12 mode active
channel-protocol LACP
no shutdown
exit

int g0/2
no switchport
channel-group 12 mode active
channel-protocol LACP
no shutdown
exit
int g0/3
no switchport
channel-group 12 mode active
channel-protocol LACP
no shutdown
exit
int g0/0
no switchport
channel-group 12 mode active
channel-protocol LACP
no shutdown
exit

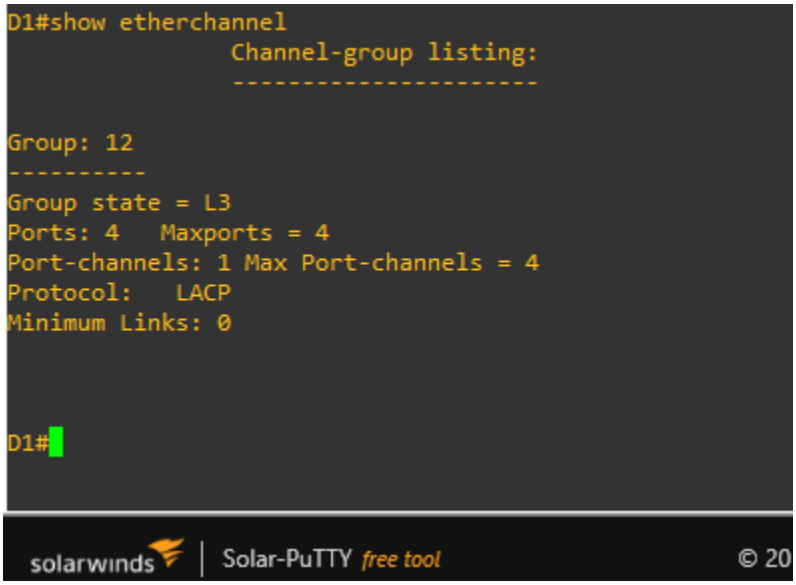

Figura 23. Show etherchannel D1

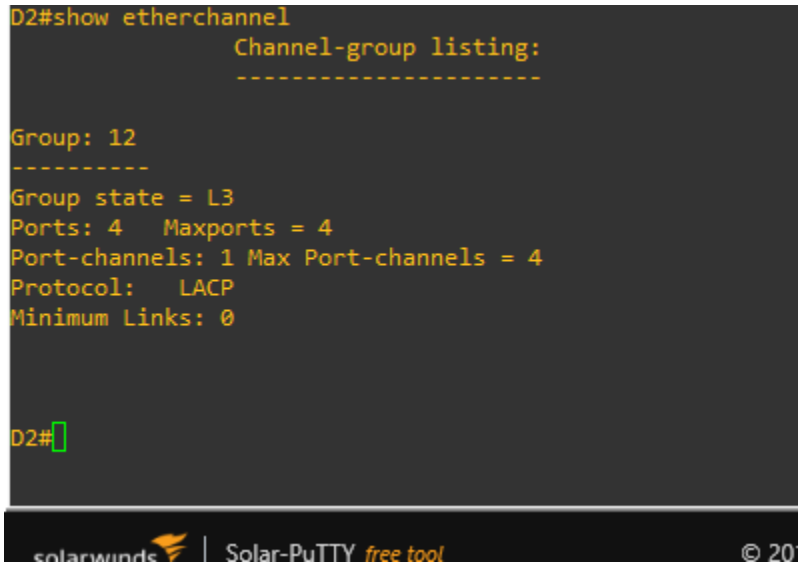

Figura 24. Show etherchannel D2

2.6 En todos los switches, configure los de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

Inter g/1/1
Switchport mode acces
Switchpor Access vlan 100
Exit

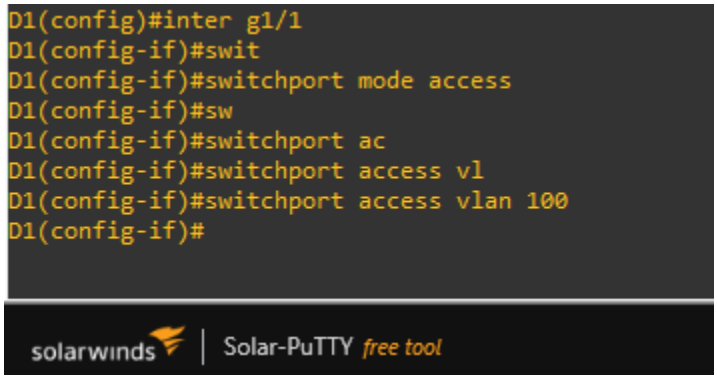

Figura 25. Host acces port D1

Inter g/1/1
Switchport mode acces
Switchpor Access vlan 102
Exit

Figura 26. Host acces port D2

Inter g/1/1
Switchport mode acces
Switchpor Access vlan 101
Exit

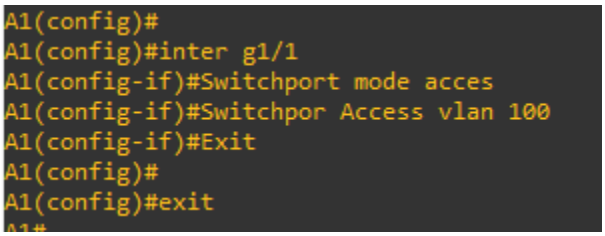

Figura 27. Host acces port A1

Inter g/1/0
Switchport mode acces
Switchpor Access vlan 101
Exit

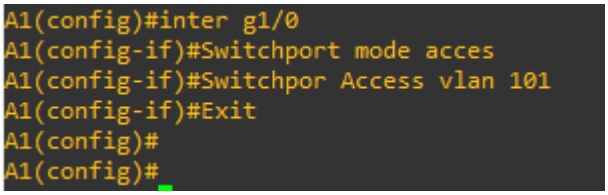

Figura 28. Host acces port A1

2.7 Verifique los servicios DHCP IPv4. Puertos

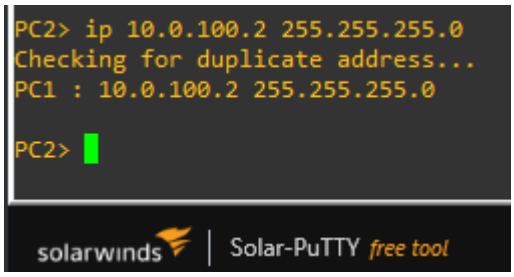

Figura 29. Ip pc2

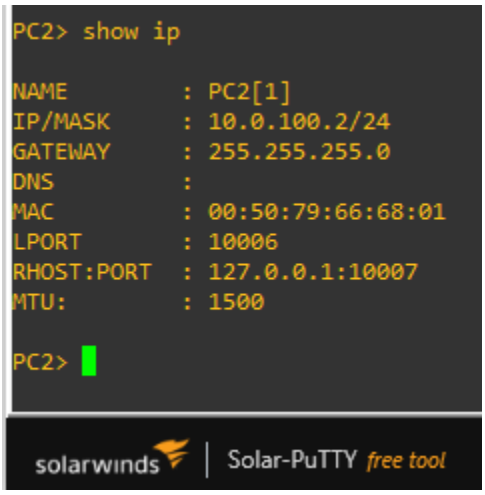

Figura 30. Show ip Pc2

2.8 Verifique la conectividad de la LAN local

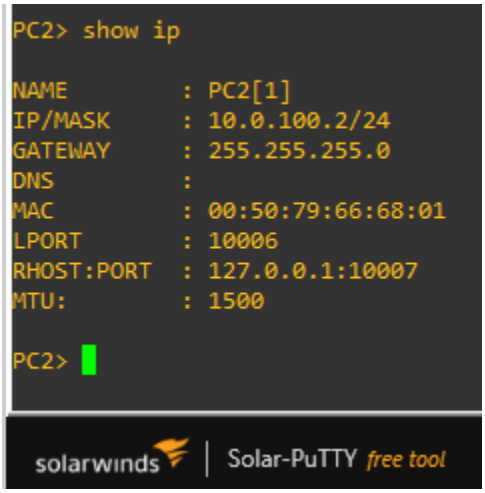

Figura 31.Conectividad pc2

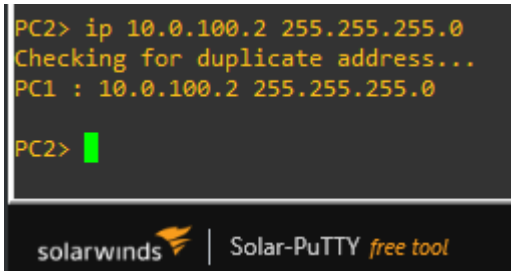

Figura 32. ip Pc2

5.2 Parte 3: Configurar los protocolos de enrutamiento

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

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

3.1 En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure single area OSPFv2 en area 0.

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

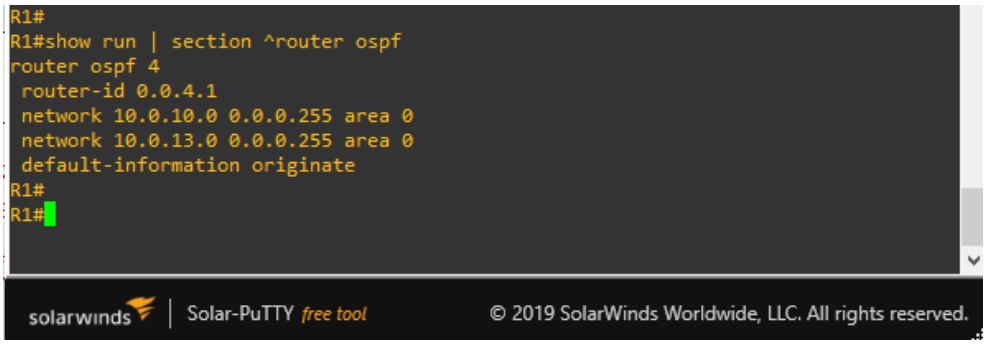

Figura 33. show run | section ^router ospf R1

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

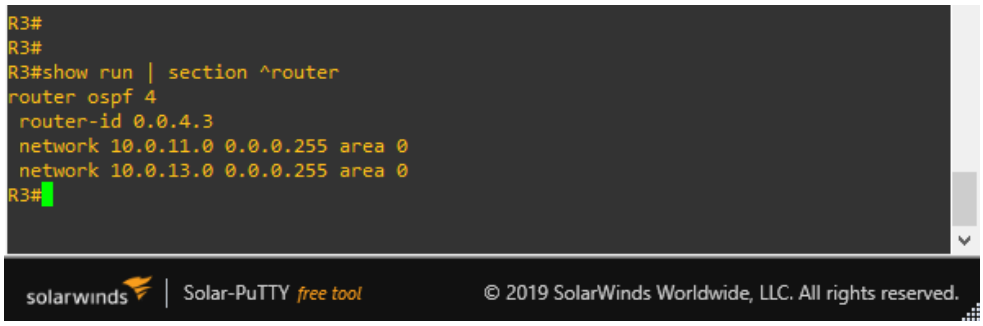

Figura 34. show run | section ^router R3

```
D1# show run | section ^router ospf
router ospf 4
 router-id 0.0.4.131
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.0.10.0 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
```

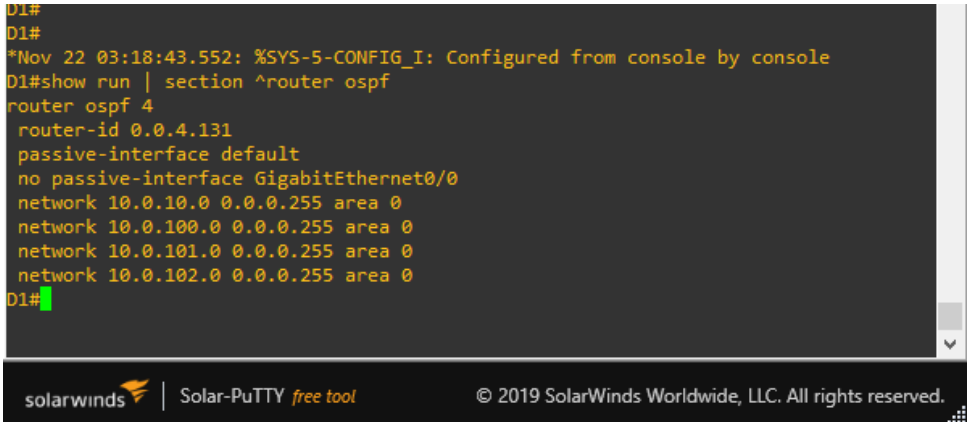

Figura 35. show run | section ^router ospf D1

```
D2# show run | section ^router ospf
router ospf 4
 router-id 0.0.4.131
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.0.10.0 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
```

```
D2(config-router)#exit
D2(config)#exit
D2#show run | sect
*Nov 22 03:25:30.292: %SYS-5-CONFIG_I: Configured from console by consoleion ^rout
er ospf
D2#show run | section ^router ospf
router ospf 4
 router-id 0.0.4.132
 passive-interface default
 no passive-interface GigabitEthernet0/0
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.101.0 0.0.0.255 area 0
 network 10.0.102.0 0.0.0.255 area 0
D2#
```

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

Figura 36. show run | section ^router ospf D2

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

R1# show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate

```
R1#
R1#
R1#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
R1#
```

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

Figura 37. show run | section ^ipv6 router R1

R3# show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.1

```
R3#
R3#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
R3#
```

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

Figura 38. show run | section ^ipv6 router R3

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

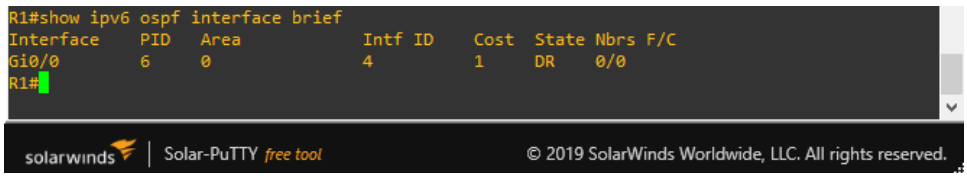

Figura 39. show ipv6 ospf interface brief R1

D2#
router ospf 6
router-id 0.0.4.131
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/0

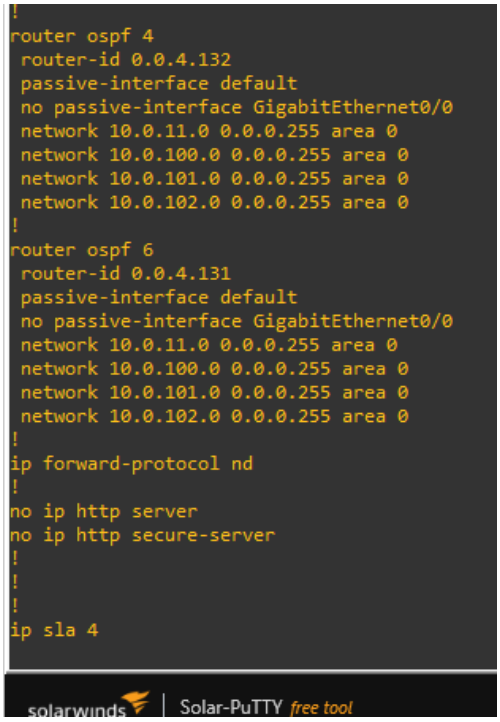

Figura 40. show ipv6 ospf interface D2

D1#
router ospf 6
router-id 0.0.4.131
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
passive-interface default
no passive- g0/0

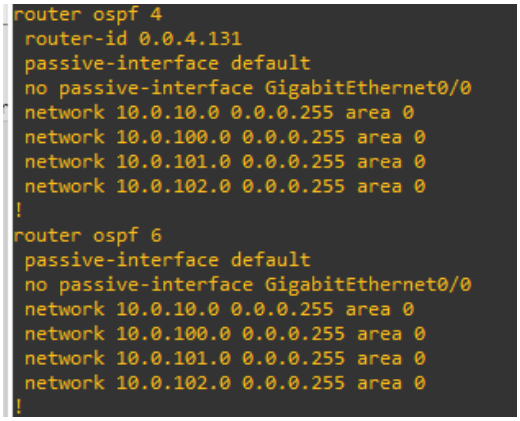

Figura 41. show ipv6 ospf interface D1

3.3 En R2 en la "Red ISP", configure MPBGP

R2# show run | section router bgp
router bgp 500
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2001:DB8:200::1 remote-as 300
 neighbor 209.165.200.225 remote-as 300
 !
 address-family ipv4
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  no neighbor 2001:DB8:200::1 activate
  neighbor 209.165.200.225 activate
 exit-address-family
 !
 address-family ipv6
  network ::/0
  network 2001:DB8:2222::/128
  neighbor 2001:DB8:200::1 activate
 exit-address-family

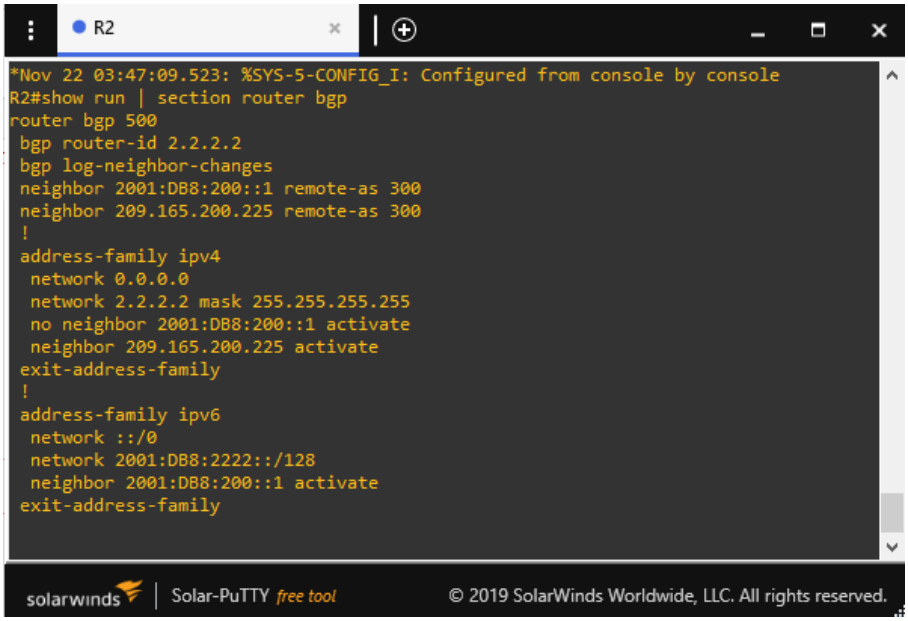

Figura 42. show run | section router bgp R2

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

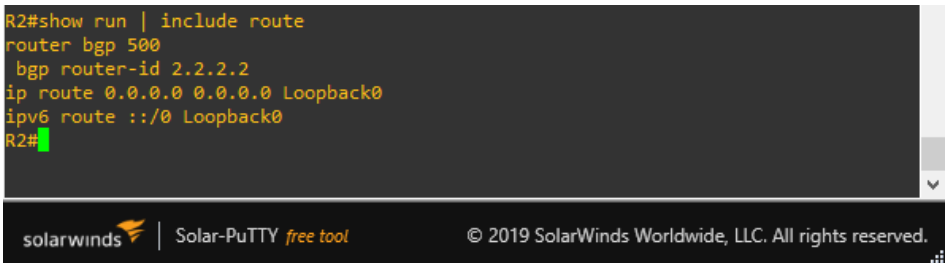

Figura 43. show run | include route R2

3.4 En R1 en la "Red ISP", configure MPBGP.

R1# show run | section bgp
router bgp 300
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 2001:DB8:200::2 remote-as 500
 neighbor 209.165.200.226 remote-as 500
 !
 address-family ipv4

```
 network 10.0.0.0
 no neighbor 2001:DB8:200::2 activate
 neighbor 209.165.200.226 activate
exit-address-family
!
address-family ipv6
 network 2001:DB8:100::/48
 neighbor 2001:DB8:200::2 activate
exit-address-family
```

Figura 44. show run | section bgp R1

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)
En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los host en la "Red de la Compañia". Las tareas de configuración son las siguientes:
4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz G 0/0

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

frequency 5
ip sla schedule 6 life forever start-time now

Figura 45. show run | section ip sla D1

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

D2# show run | section ip sla
track 4 ip sla 4
 delay down 10 up 15
track 6 ip sla 6
 delay down 10 up 15
ip sla 4
 icmp-echo 10.0.11.1
 frequency 5
ip sla schedule 4 life forever start-time now

ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5
ip sla schedule 6 life forever start-time now

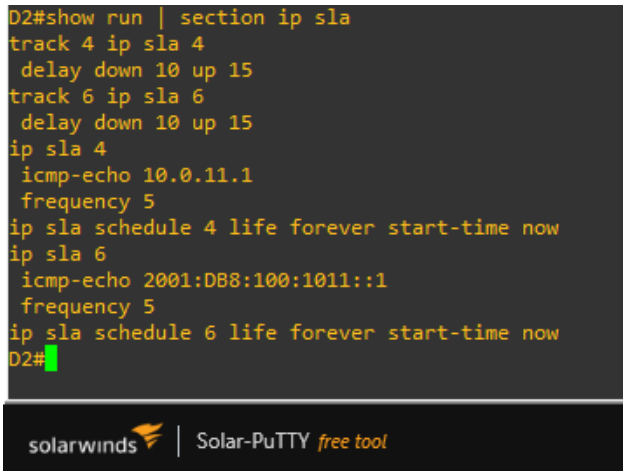

Figura 46. show run | section ip sla D2

4.3 En D1 configure HSRPv2. En D2, configure HSRPv2

D1# show standby brief

```
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       100  140 P Active FE80::5:73FF:FEA0:6A
Vl100       104  90 P Active  10.0.102.254
Vl100       106  90 P Active FE80::5:73FF:FEA0:6A
Vl101       114  40 P Active 10.0.102.254
Vl101       116  40 P Active  FE80::5:73FF:FEA0:74
Vl102       124  90 P Active 10.0.102.254
Vl102       126  90 P Active FE80::5:73FF:FEA0:7E
Vl110       114  110 P Active     FE80::5:73FF:FEA0:72
```

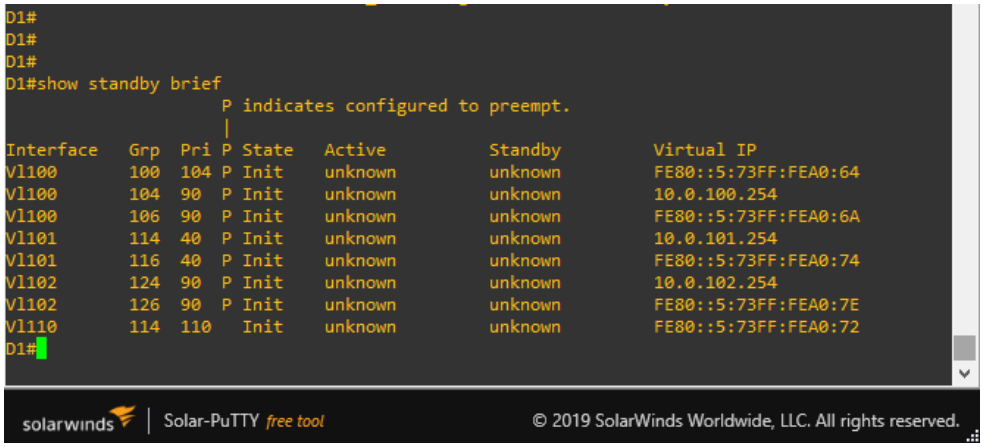

Figura 47. show standby brief D1

P indicates configured to preempt.

```
                |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       104  40 P Active  10.0.102.254
Vl100       106  40 P Active FE80::5:73FF:FEA0:6A
Vl101       114  90 P Active 10.0.102.254
Vl101       116  90 P Active  FE80::5:73FF:FEA0:74
Vl102       124  40 P Active 10.0.102.254
Vl102       126  40 P Active FE80::5:73FF:FEA0:7E
```

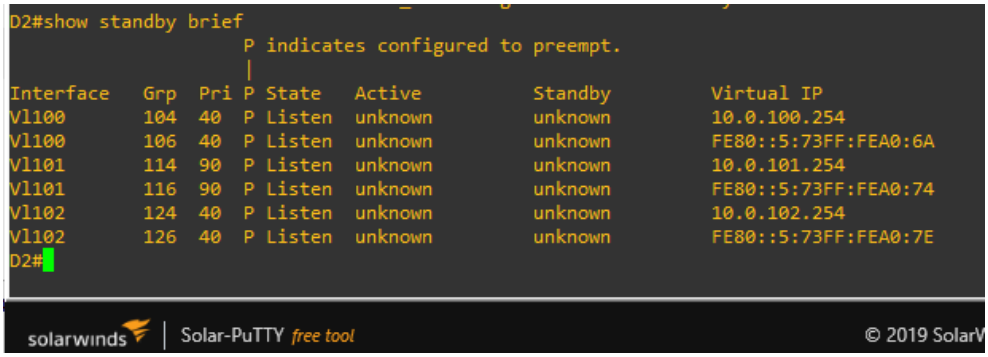

Figura 48. show standby brief D2

Parte 5: Seguridad En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

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

Usuario: sadmin
Contraseña: cisco12345cisco
Enable
Contraseña: cisco12345cisco
R1# show run | include secret
enable secret 9 $9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9 9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

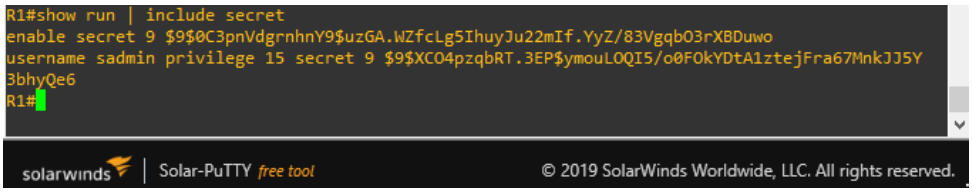

Figura 49. show run | include secret R1

R2# show run | include secret
enable secret 9
$9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

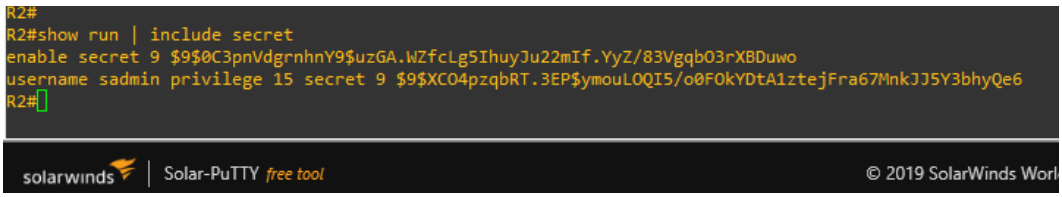

Figura 50. show run | include secret D1

R3# show run | include secret
enable secret 9
$9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

Figura 51. show run | include secret D1

D1# show run | include secret
enable secret 9
$9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

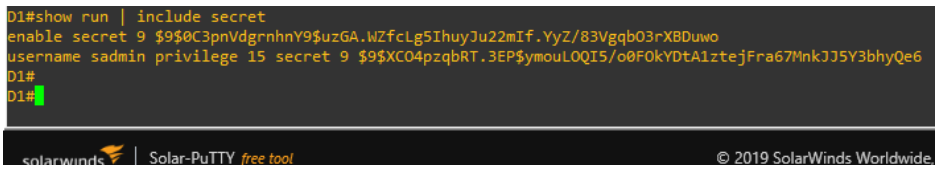

Figura 52. show run | include secret D1

D2# show run | include secret
enable secret 9
$9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

Figura 53. show run | include secret D2

A1# show run | include secret
enable secret 9
$9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

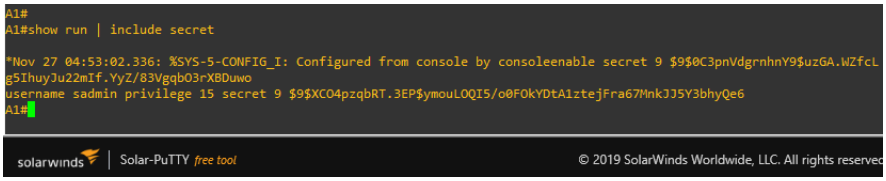

Figura 54. show run | include secret A1

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

Usuario: sadmin
Contraseña: cisco12345cisco

R2# username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco

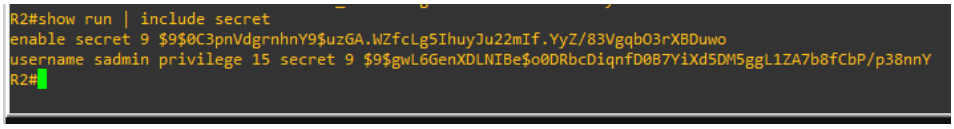

Figura 55. show run | include secret

R3# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

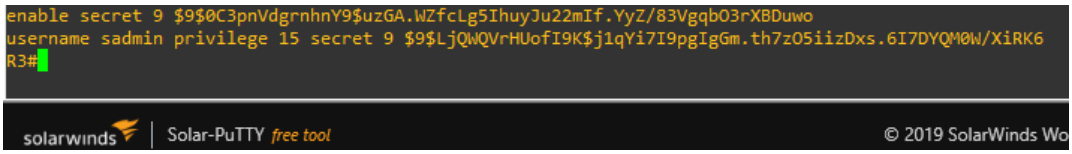

Figura 56. show run | include secret

A1# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Figura 57. show run | include secret

D1# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

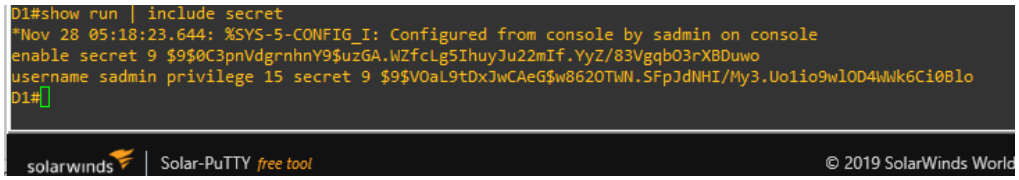

Figura 58. show run | include secret D1

D2# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

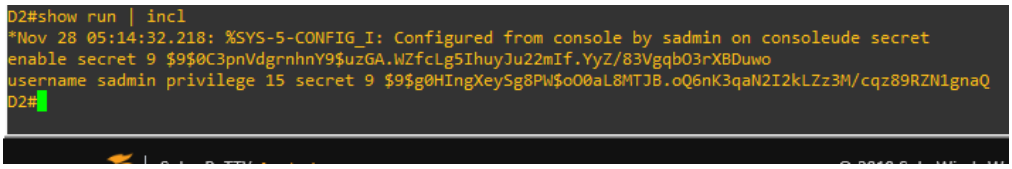

Figura 59. show run | include secret D2

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

A1# aaa new-model

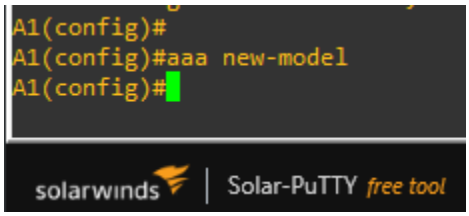

Figura 60. aaa new-model

R2# aaa new-model

Figura 61. aaa new-model

R3# aaa new-model

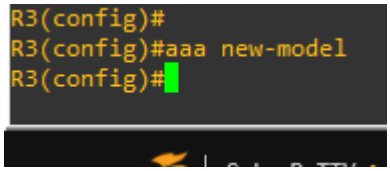

Figura 62. aaa new-model

D1# aaa new-model

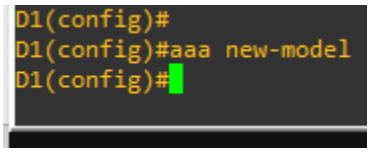

Figura 63. aaa new-model

D1# aaa new-model

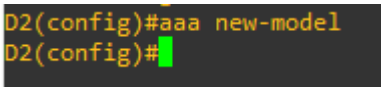

Figura 64. aaa new-model

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

D1#
aaa new-model
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
 exit
aaa authentication login default group radius local

end

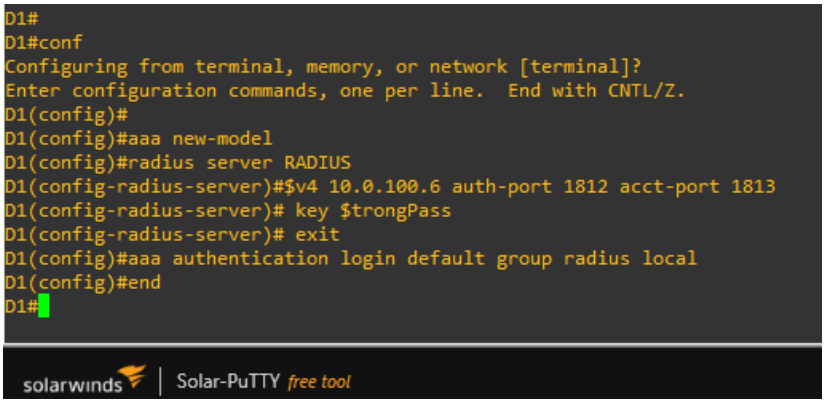

Figura 65. RADIUS D1

D#2
aaa new-model
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
 exit
aaa authentication login default group radius local
end

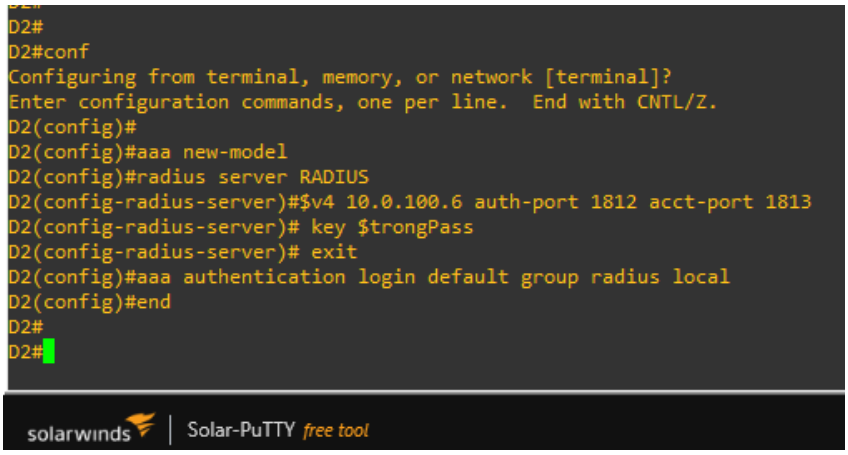

Figura 66. RADIUS D2

A1#
aaa new-model
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
 exit
aaa authentication login default group radius local

end

```
A1#
A1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#end
A1#
A1#
```

Figura 67. RADIUS A1

R3#
aaa new-model
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
 exit
aaa authentication login default group radius local
end

```
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#
R3(config)#aaa new-model
R3(config)#
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#end
R3#
*Nov 28 03:46:13.331: %SYS-5-CONFIG_I: Configured from console by console
R3#
```


Figura 68. RADIUS R3

R3#
aaa new-model
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
 exit

aaa authentication login default group radius local
end

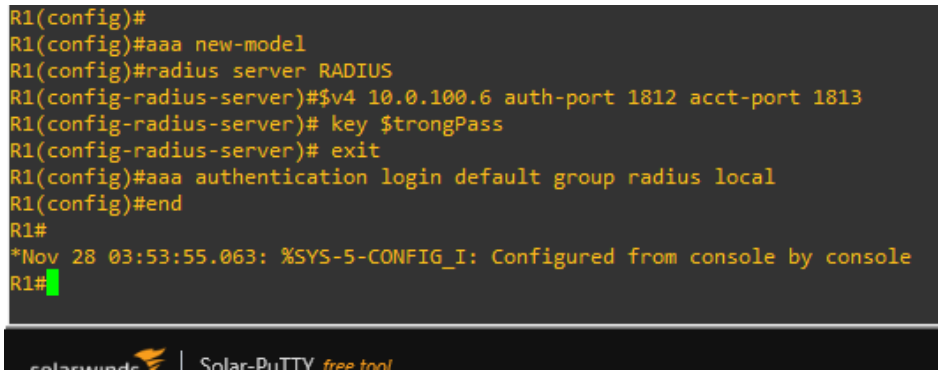

Figura 69. RADIUS R1

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

R1# show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
aaa new-model
aaa session-id common

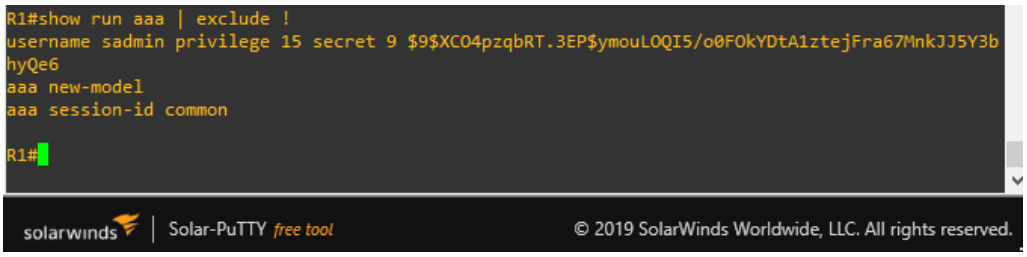

Figura 70. show run aaa | exclude ! R1

R3# show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
aaa new-model
aaa session-id common

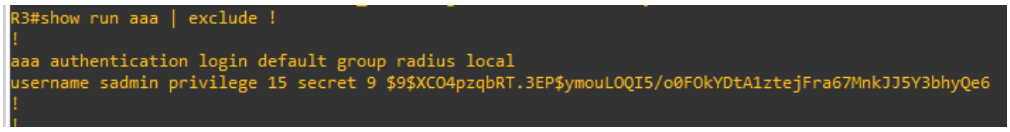

Figura 71. show run aaa | exclude ! R3

D1# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
aaa new-model
aaa session-id common

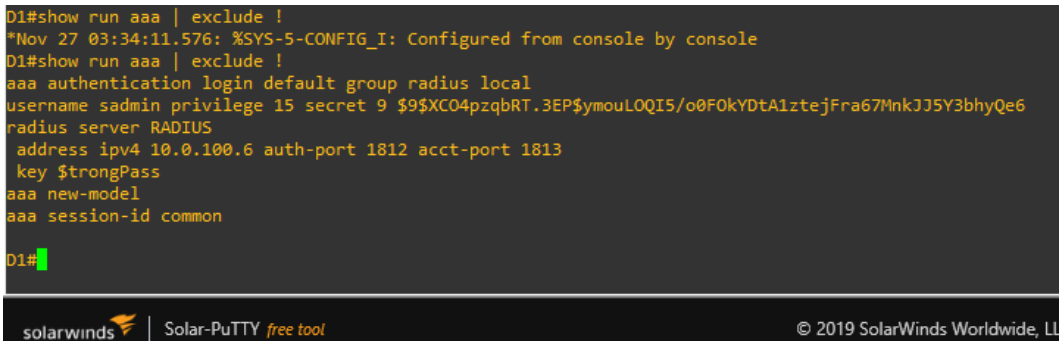

Figura 72. show run aaa | exclude ! D1

D2# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
aaa new-model
aaa session-id common

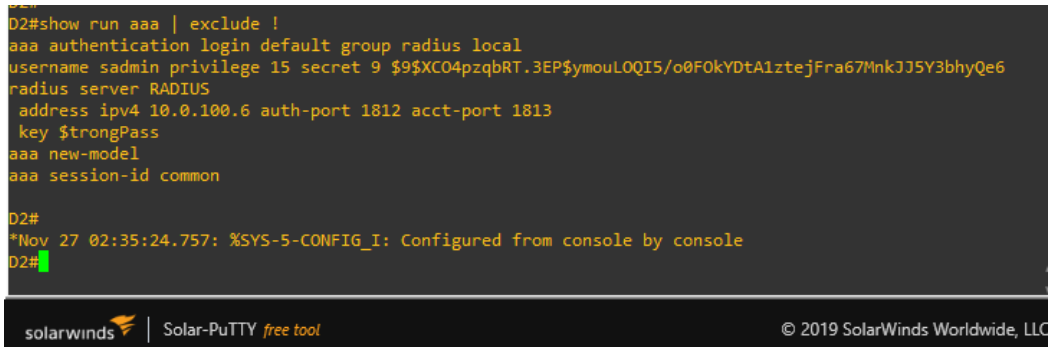

Figura 73. show run aaa | exclude ! D2

A1# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
9XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
aaa new-model
aaa session-id common

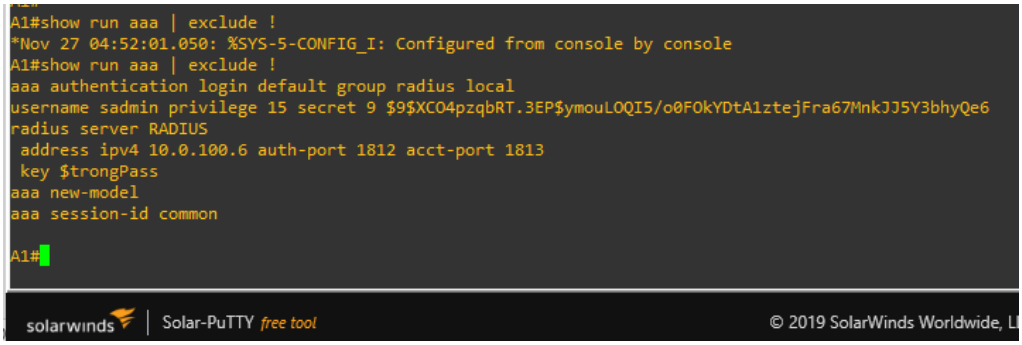

Figura 74. show run aaa | exclude ! A1

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

Figura 75. show run aaa A1

Figura 76. show run aaa D2

Figura 77. show run aaa D1

Figura 78. show run aaa R3

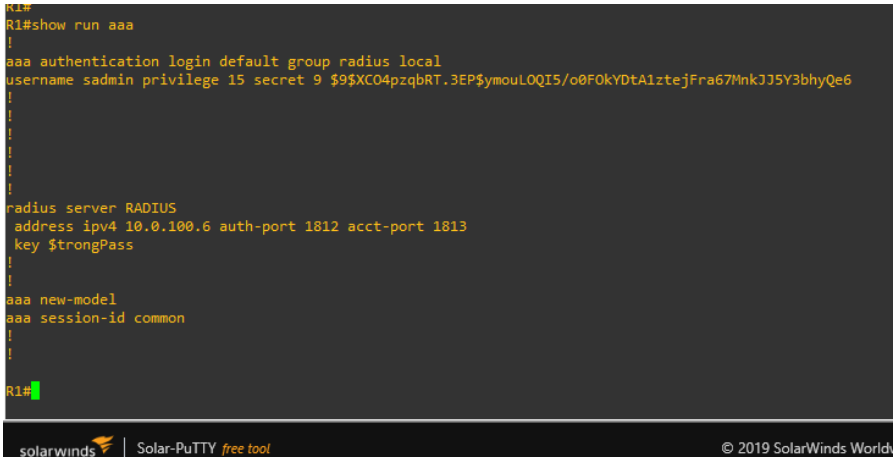

Figura 79. show run aaa R1

Parte 6: Configure las funciones de Administración de Red En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

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

R1# ntp server 2.2.2.2
R2# ntp server 10.0.10.1
R3# ntp server 10.0.10.1
A1# ntp server 10.0.10.1
D1# ntp server 10.0.10.1
D2# ntp server 10.0.10.1

6.2 Configure R2 como un NTP maestro.

R2# show run | include ntp
ntp master 3

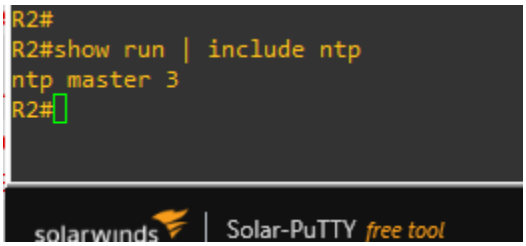

Figura 80. show run | include ntp R2

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

R1# ntp server 2.2.2.2

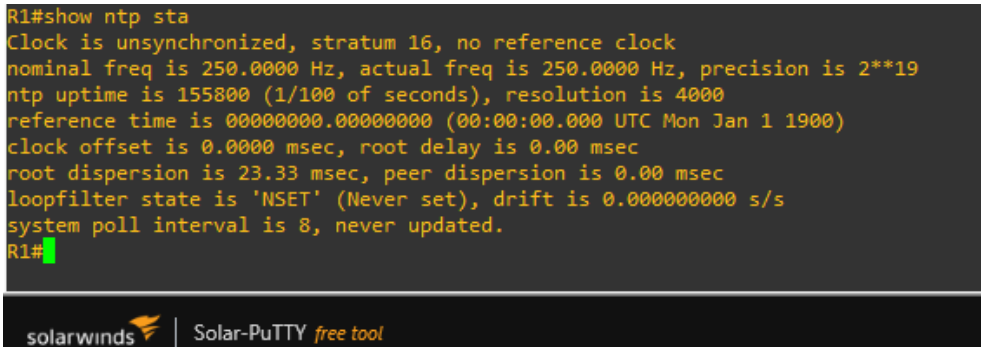

Figura 81. NTP R1

D1# ntp server 10.0.10.1

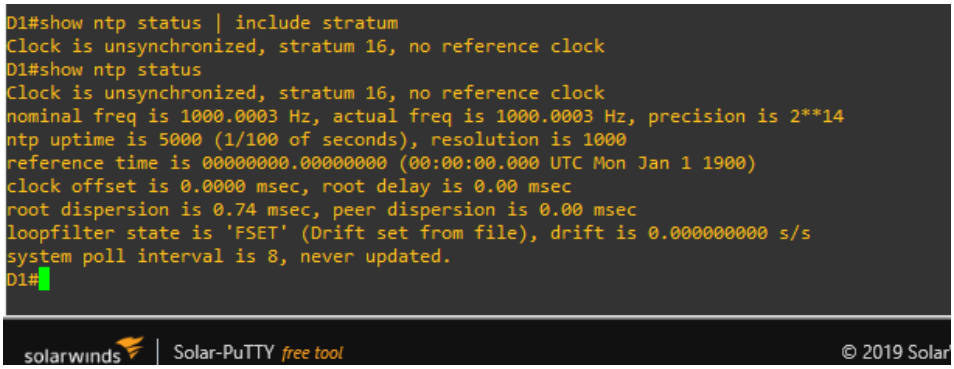

Figura 82. NTP D1

D2# ntp server 10.0.10.1

```
D2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#ntp server 10.0.10.1
D2(config)#exit
D2#show ntp status
*Nov 27 02:10:00.008: %SYS-5-CONFIG_I: Configured from console by console
D2#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 1000.0003 Hz, actual freq is 1000.0003 Hz, precision is 2**14
ntp uptime is 400 (1/100 of seconds), resolution is 1000
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.05 msec, peer dispersion is 0.00 msec
loopfilter state is 'FSET' (Drift set from file), drift is 0.000000000 s/s
system poll interval is 8, never updated.
D2#
```

Figura 83. NTP D2

A1# ntp server 10.0.10.1

```
A1#sh
*Nov 27 04:49:40.878: %SYS-5-CONFIG_I: Configured from console by console
A1#sh ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 1000.0003 Hz, actual freq is 1000.0003 Hz, precision is 2**14
ntp uptime is 1800 (1/100 of seconds), resolution is 1000
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.25 msec, peer dispersion is 0.00 msec
loopfilter state is 'FSET' (Drift set from file), drift is 0.000000000 s/s
system poll interval is 8, never updated.
A1#
solarwinds | Solar-PuTTY free tool © 20
```

Figura 84. NTP A1

R3# ntp server 10.0.10.1

```
R3#show ntp st
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
ntp uptime is 53400 (1/100 of seconds), resolution is 4000
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 8.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'NSET' (Never set), drift is 0.000000000 s/s
system poll interval is 8, never updated.
R3#
```

Figura 85. NTP A1

R2# ntp server 10.0.10.1

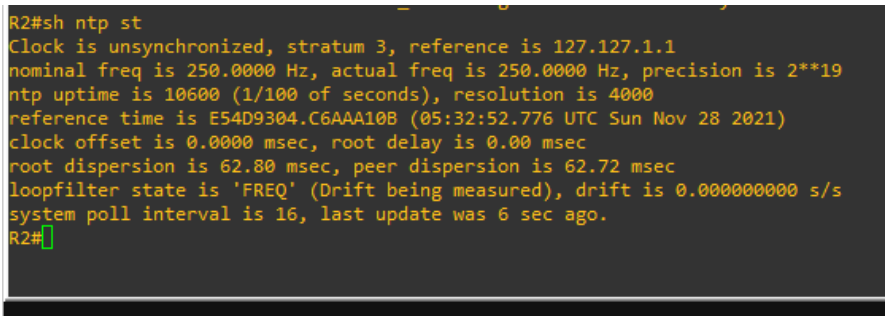

Figura 86. NTP A1

6.4 Configure Syslog en todos los dispositivos excepto R2

R1#
logging host 10.0.100.5
logging trap warning
logging on

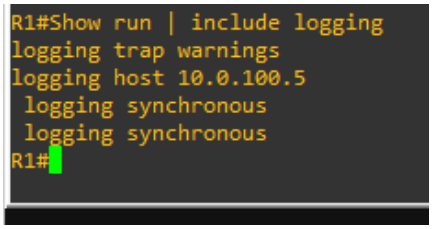

Figura 87. Show run | include logging R1

R3#
logging host 10.0.100.5
logging trap warning
logging on

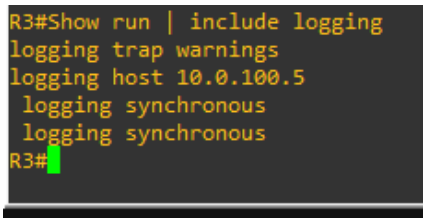

Figura 88. Show run | include logging R3

A1#
logging host 10.0.100.5
logging trap warning
logging on

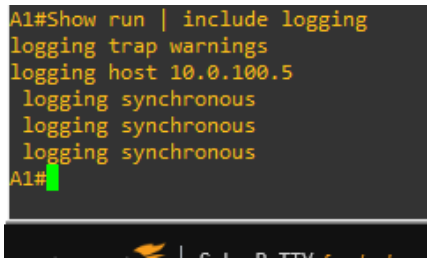

Figura 89. Show run | include logging A1

D1#
logging host 10.0.100.5
logging trap warning
logging on

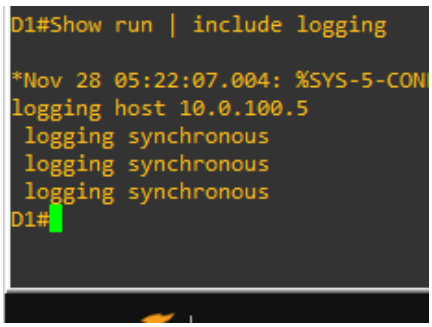

Figura 90. Show run | include logging D1

D2#
logging host 10.0.100.5
logging trap warning
logging on

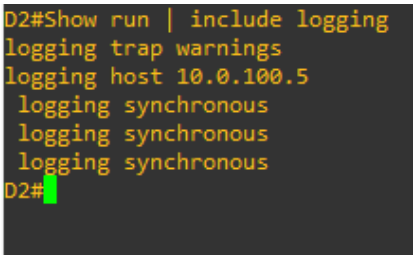

Figura 91. Show run | include logging D2

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

R1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors

snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server host 10.0.100.5 version 2c ENCORSA

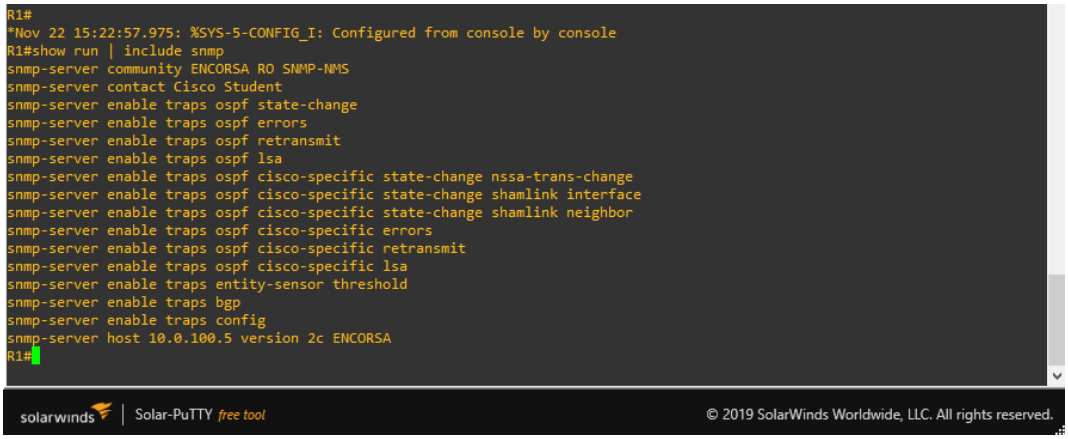

Figura 92. show run | include snmp R1

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

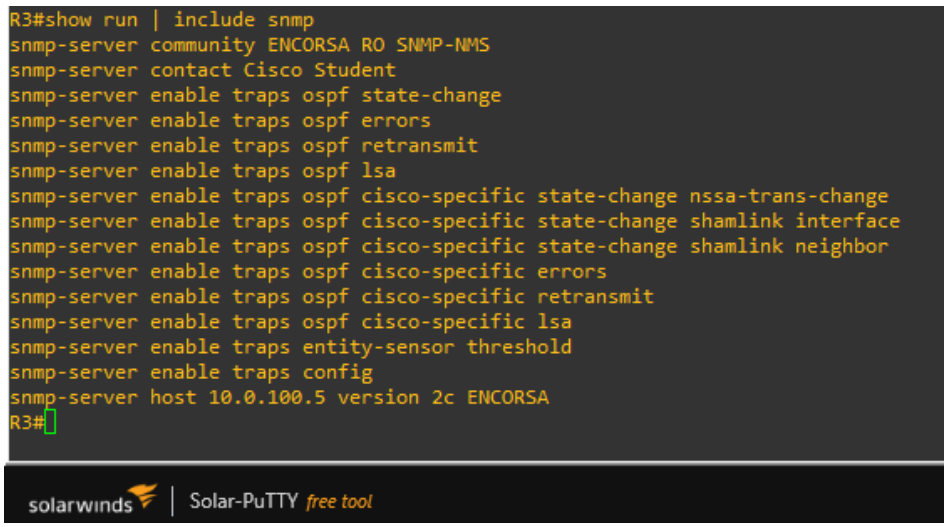

Figura 93. show run | include snmp R3

D1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

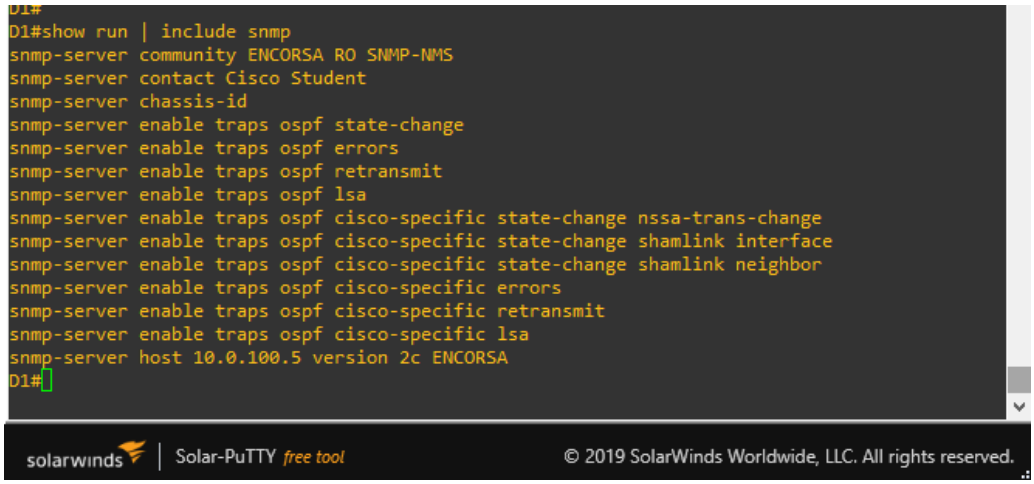

Figura 94. show run | include snmp

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

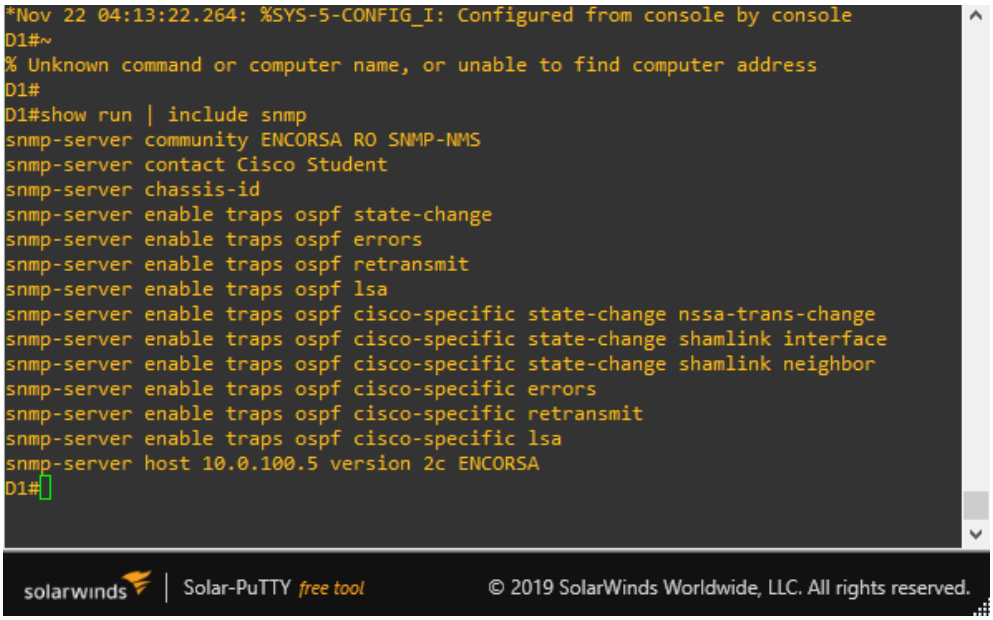

Figura 95. show run | include snmp

A1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server chassis-id
snmp-server host 10.0.100.5 version 2c ENCORSA

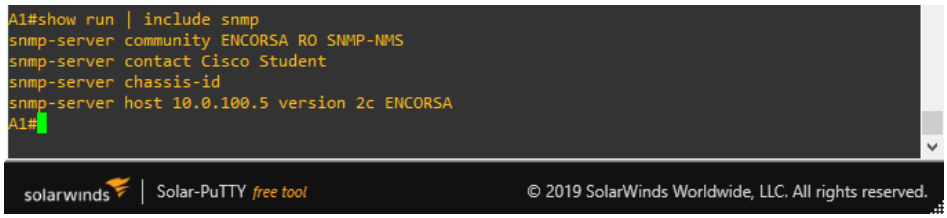

Figura 96. show run | include snmp A1

7. CONCLUSIONES

Utilicé el simulador Packet Tracer y permitió realizar diferentes análisis y pruebas, observando el comportamiento de cada dispositivo, con los diversos protocolos y comandos para el desarrollo de la actividad.

Se configuraron los Router y switches dados en la guía, donde se mostró en al final del escenario una red convergente.

Adquirí habilidades en la parte de gestion de redes, profundizando más mis conocimientos, implementado e interpretando la problemática.

Es importante diseñar e implementar administraciones con este tipo de topologías que comparten datos, ya que a menudo nos encontramos con empresas que buscan fortalecer y dar soluciones de seguridad y redes.

8. BIBLIOGRAFIAS

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

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

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

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