DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ALBERTO MUÑOZ JOAQUI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – CBTI
INGENIERÍA ELECTRÓNICA
POPAYÁN
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ALBERTO MUÑOZ JOAQUI

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – CBTI
INGENIERÍA ELECTRÓNICA
POPAYÁN
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Popayán, 28 de noviembre 2021

AGRADECIMIENTOS

Antes que nada, debo agradecer a Dios que me permite culminar esta etapa de mi vida por la que he luchado desde hace mucho tiempo, a pesar de las dificultades que se presentaron en este recorrido he podido seguir adelante trabajando por mis sueños y metas. También quiero darle mis más infinitos agradecimientos a mi esposa quien fue la que me impulso, me dio su apoyo para comenzar este nuevo proyecto, me brindo su mano de manera incondicional, su amor y su paciencia fueron esenciales para soportar las horas y días de mi ausencia dedicadas a esta carrera. Es ella el impulso y constancia que me llevo a culminar la profesionalización, a terminar esta etapa de mi vida, con la premisa de iniciar otra llena de bendiciones a su lado.

A mis hijos también quiero mencionarlos aquí, me han brindado su compañía y su apoyo, es en ellos en quienes pienso cada que me siento superado por algo, y deseo dejarles un ejemplo de vida, enseñarles que las metas que nos proponemos se hacen realidad, sin importar la edad y las dificultades, cuando trabajamos en ellas. Quiero también recordarles que con el acompañamiento de la familia todo caminar es más bello y se hace más fácil.

Por último y no menos importante agradecerle a mis familiares, amigos y docentes de la UNAD que estuvieron presentes en esta etapa de mi vida.

CONTENIDO

LISTA DE TABLAS.

LISTA DE FIGURAS

GLOSARIO

BGP (Border Gateway Protocol)**:** Es un protocolo escalable de dymanic routing que utiliza una puerta de enlace (EGP) exterior, usado en internet por grupos de enrutadores para compartir información de enrutamiento, este protocolo usa rutas y atributos para definir políticas de enrutamiento y crear un entorno estable.

GNS3 (Simulación Grafica de Redes): Es un software utilizado para simular grafico de red que permite diseñar, configurar, probar y solucionar problemas de redes virtuales y reales, permite la creación de topologías de red complejas y sencillas y es compatible con cisco.

Interfaz: Se utiliza para la interconexión entre dos sistemas, programas, dispositivos o componentes de cualquier índole, o bien, entre un sistema informático y su usuario humano, proporciona una comunicación de distintos niveles permitiendo el intercambio de información.

Loopback: Es una interfaz lógica interna del router y esta no se puede asignar a un puerto físico, por lo tanto, no se puede conectar a otro dispositivo, es considerada una interfaz de software.

OSPFv2(Open Shortest Path Firts)**:** Es un protocolo de routing de estado de enlace que se implementa con frecuencias, es ajustable de muchas maneras, los métodos de ajuste más comunes incluyen la manipulación del proceso de elección del router designado / router designado de respaldo, la propagación de rutas de predeterminadas, el ajuste de las interfaces OSPFv2 y OSPFv3 y la habilitación de la autenticación.

SCRYPT: Es un algoritmo con alto nivel de seguridad, el nivel de seguridad es ajustable, el administrador puede aumentar o disminuir diversas variables, trabaja dentro de mecanismo de consenso PoW, este algoritmo necesita de bastante memoria porque genera números grandes rápidamente y estos números son almacenados en la RAM del procesador el cual debe acceder de forma continua antes de enviar un resultado.

Switch: Es un dispositivo de interconexión utilizado para conectar varios equipos como computadores, impresoras, dentro de una misma red lo que permite que a los equipos que están conectados compartir información y comunicarse entre sí.

Trama: Es la responsable de la correcta configuración de las reglas y del éxito de la transmisión de los paquetes de datos, los datos de Ethernet son transportados a través de la trama, las tramas de Ethernet tienen un tamaño entre 64 y 1518 byte.

VLAN: Son un mecanismo para que los programadores de la red creen dominios de broadcast lógicos que pueden abarcar un solo Switch o varios Switch múltiples sin importar la proximidad física, es muy útil para reducir el tamaño de dominios de broadcast y permiten que los grupos o los usuarios se agrupen lógicamente sin necesidad de estar físicamente en el mismo lugar.

RESUMEN

El siguiente trabajo del curso diplomado de profundización Cisco Certified Network Practitioner (CCNP) de la Universidad Nacional Abierta y a Distancia (UNAD) tiene como objetivo principal poder demostrar las habilidades de configuración en distintos dispositivos del escenario propuesto, con la solución de seis pasos donde se realizaran las configuraciones de los equipos de la red en diferentes prácticas, estas serán desarrolladas en el software GNS3 que estará conectado a una máquina virtual, en este caso se usara la maquina VMware Workstation Pro.

Se demostrara las configuraciones básicas de los equipos creados en la red, como los protocolos de enrutamiento, Conmutación y STP, el cual nos permite utilizar comandos de configuración en Router y switches para que tengan una comunicación efectiva, ya que en la topología creada existen unas redes de la compañía donde maneja distintos protocolos de enrutamiento, se crearan grupos de HSRPv2 para poder enrutar el tráfico, asegurando la estabilidad de los grupos y proporcionando una mejor resolución de problemas, además se habilita el algoritmo de encripción SCRYPT para mejorar la seguridad de la red ya que en un entorno real y virtual donde la tecnología electrónica de los Switches, Routers y PCs está expuesta a sabotaje y deterioro por diferentes factores, será solo el programador o administrador quien pueda ingresar a la red, hacer cabios y ver los mensajes en el servidor Syslog para prevenir daños futuros analizando el rendimiento de los equipos y la estabilidad de la red.

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

ABSTRACT

The following work of the Cisco Certified Network Practitioner (CCNP) in-depth diploma course of the National Open and Distance University (UNAD) has as its main objective to be able to demonstrate the configuration skills in different devices of the proposed scenario with the six-step solution where they will be carried out the configurations of the network equipment in different practices, these will be developed in the GNS3 software that will be connected to a virtual machine, in this case the VMware Workstation machine will be used.

The basic configurations of the equipment created in the network will be demonstrated, such as routing protocols, Switching and STP, which allows us to use configuration commands in Router and switches so that they have effective communication, since in the created topology there are some Company networks where it handles different routing protocols, HSRPv2 groups are created to be able to route the traffic, ensuring the stability of the groups and better problem solving, in addition, the SCRYPT encryption algorithm is enabled to improve network security since in a real and virtual environment where the electronic technology of the Switches, Routers and PCs is exposed to sabotage and deterioration by different factors, it will be only the programmer or administrator who can enter the network, make changes and see the messages in the Syslog server to prevent future damage by analyzing equipment performance and network stability.

INTRODUCCIÓN

El presente trabajo muestra el desarrollo de un escenario propuesto por el diplomando de profundización Cisco Certified Network Practitioner (CCNP) donde se demostraran las pruebas de habilidades en la configuración de dispositivos como Switches, Routers y PCs que se encontrara en descripción de este curso, el objetivo principal es demostrar la conectividad y accesibilidad de toda la red planteada, ya que en este escenario existen redes de una compañía, por lo que se aplicara y habilitara la correcta configuración de diferentes protocolos como OSPF, BGP, HSRPv2, la creación de VLAN y seguridad de la red, así como también demostrar la configuración administrativa de la red.

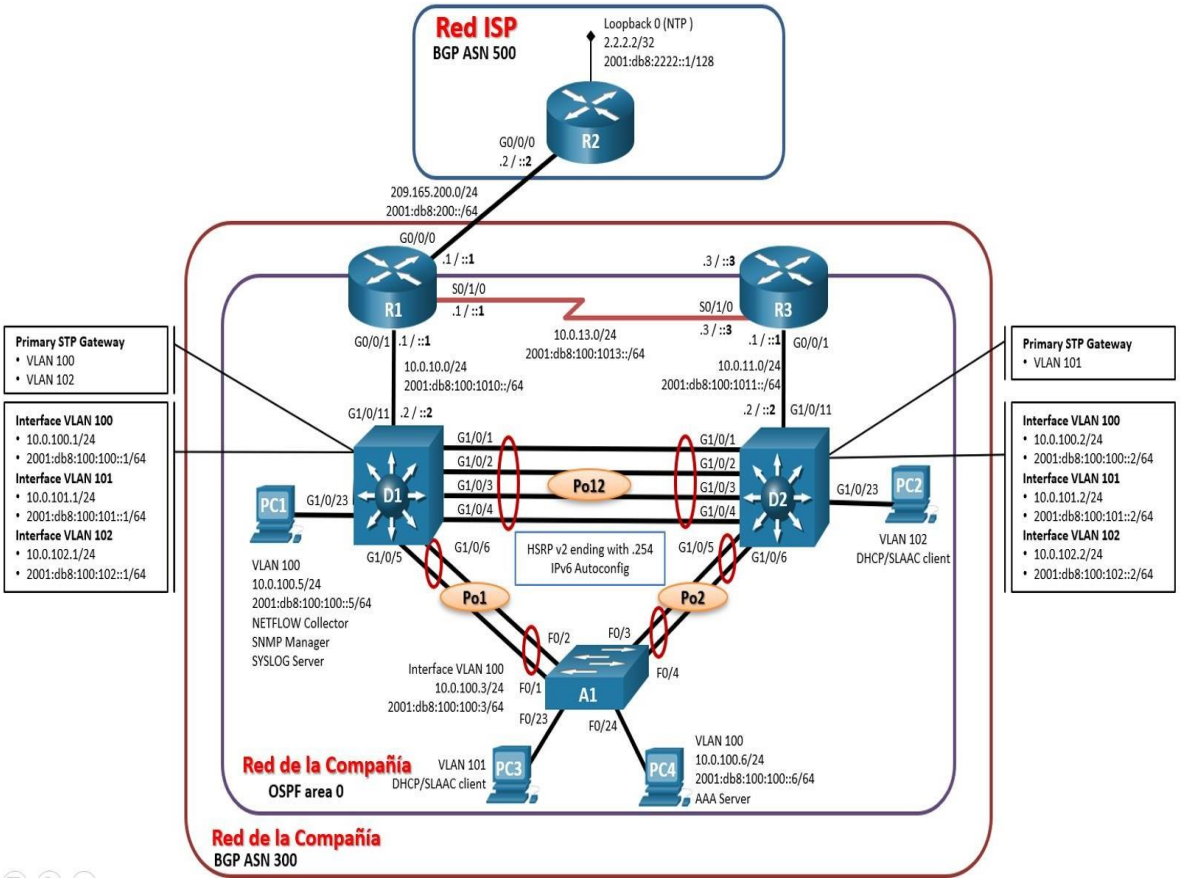
Se encontrará la construcción de la red en el software GNS3, la configuración básica de los dispositivos como nombres de cada equipo, la creación de IPs, el direccionamiento de cada interfaz, la configuración de capa de vinculo de datos para el diseño de protocolos de red y la transferencia de datos, se habilitan los protocolos de enrutamiento OSPF, BGP para que los enrutadores intercambien información de enrutamiento con los demás host.

Se evidenciara la configuración del monitoreo activo de tráfico de la red con la creación de la ip SLA, se configura Hot Standby Routing Protocol (HSRPv2) con la creación de grupos y para poder enrutar el tráfico, asegurando la estabilidad de los grupos y proporcionando una mejor resolución de problemas, también se encontrara la configuración del algoritmo SCRYPT para seguridad en los dispositivos de la red, por último, se mostrarán varias funciones de administración de la red como la configuración de hora y fecha actual en los equipos de la red, la configuración de Syslog para compilar información de registros de control y la resolución de problemas.

DESARROLLO

ESCENARIO 1

Figura 1. Escenario propuesto.



En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Figura 2. Construcción de la red del escenario propuesto en software GNS3.

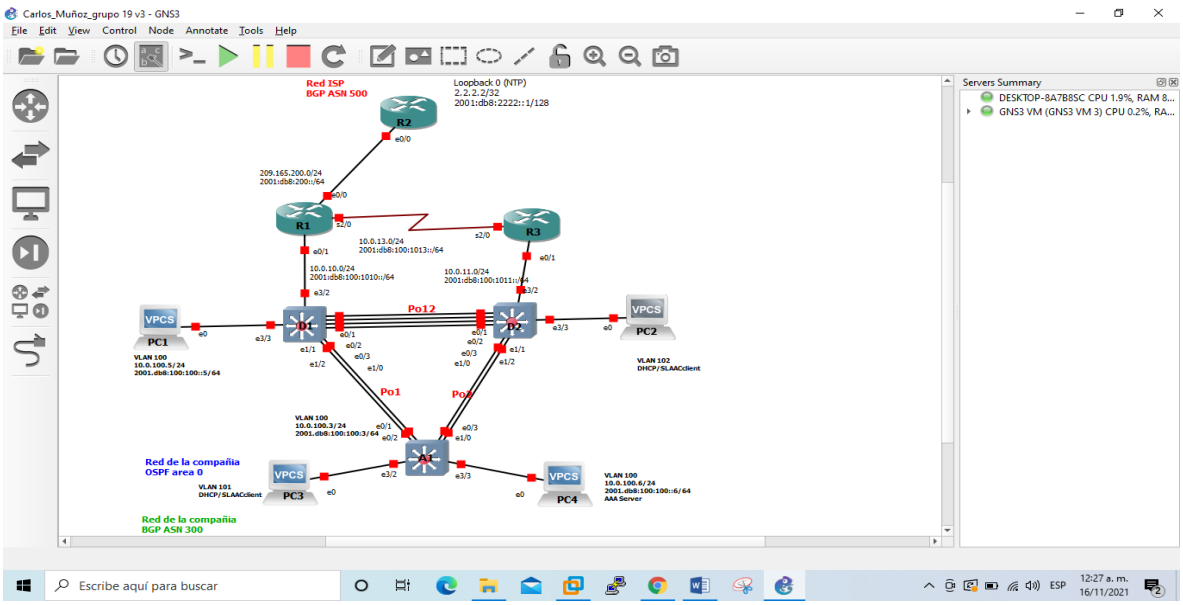


Tabla 1. Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E3/2	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	E3/2	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

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

1.1. 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, en este punto se conectarán los dispositivos según la tabla de direccionamiento usando las interfaces de Ethernet y Serial según sea necesario.

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

Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos, aquí se asignará los nombres a cada dispositivo de la red mediante el comando **hostname**, sus direcciones IP, con el comando **ip address,** se configurarán las direcciones ipv6 de enlace troncal utilizando el comando **ipv6 address fe80::1 link-local** y se levantara la interface con el comando **no shutdow,** luego de tener configurado cada dispositivo se debe colocar el comando **copy running-config startup-confi**g para guardar el archivo de ejecución en la memoria flash, la configuración de cada dispositivo se mostrara a continuación:

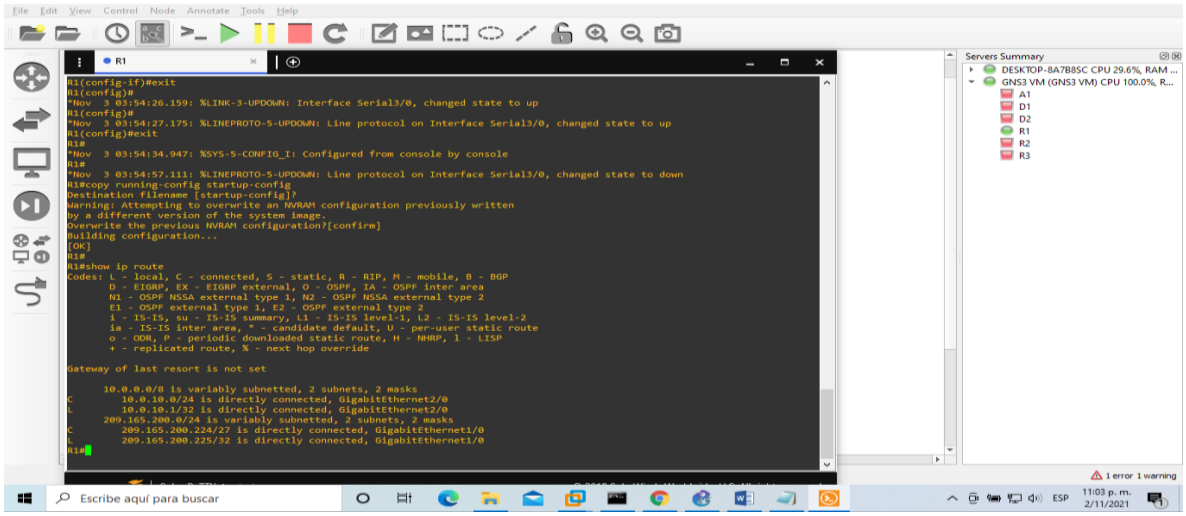
Configuración Router R1

```
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 e0/0
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
interface e0/1
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s2/0
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
```

no shutdown
exit
copy running-config startup-config

Utilizando el comando **show ip route** se mostrará la tabla de enrutamiento de cada dispositivo como se muestra en la figura número 3.

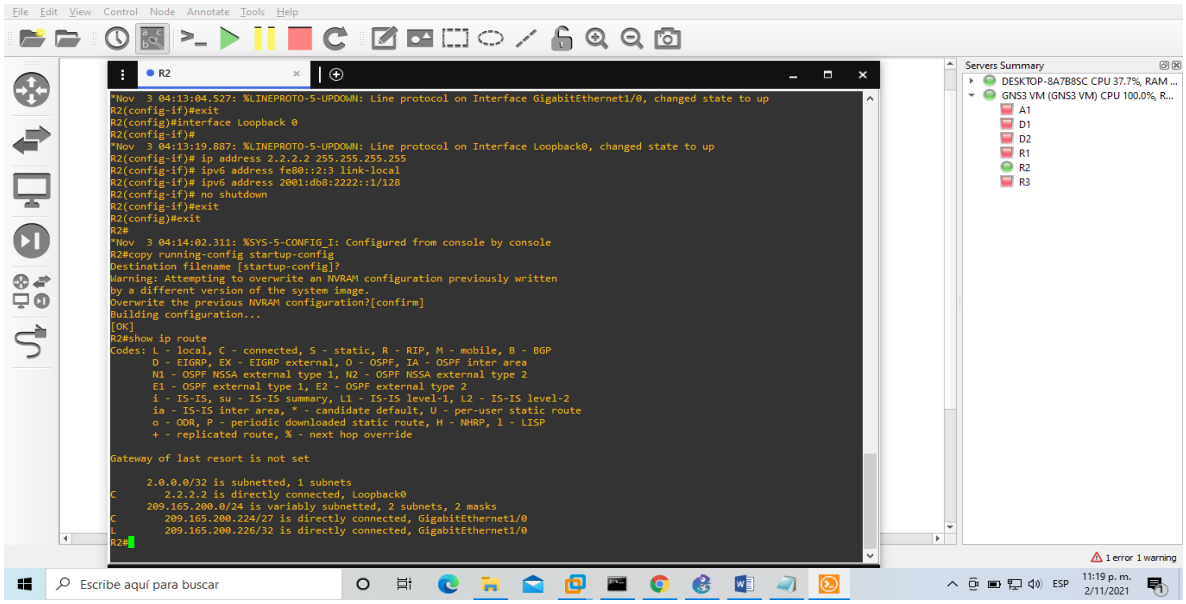
Figura 3. Comando show IP Route en R1.



Configuración en 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 e0/0
 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
copy running-config startup-config
show ip route

Figura 4. Comando show IP Route en R2.



Configuración 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 e0/1
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 s2/0
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
copy running-config startup-config

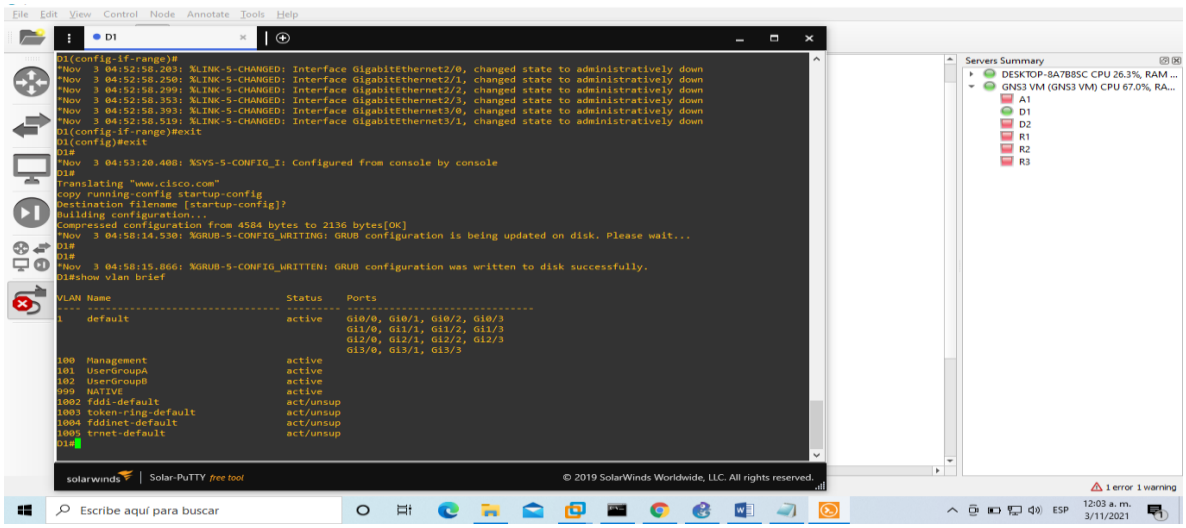
Ahora se configurarán los Switch de la topología donde se asignarán direcciones ip y nombres a VLAN, se ingresa al modo privilegiado y se coloca el comando **vlan(numero)**, luego **name(nombre)**, también se configura la exclusión de direcciones mediante el comando **ip dhcp excluded-address.**

Configuración 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
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e3/2
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
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
interface range e0/0, e1/3, e2/0-3, e3/0-1
shutdown
exit
copy running-config startup-config
show vlan brief

Figura 5. Comando show VLAN brief en Router D1.



Configuración 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
interface e3/2
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
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 range e0/0, e1/3, e2/0-3, e3/0-1
shutdown
exit
copy running-config startup-config
show vlan brief
```

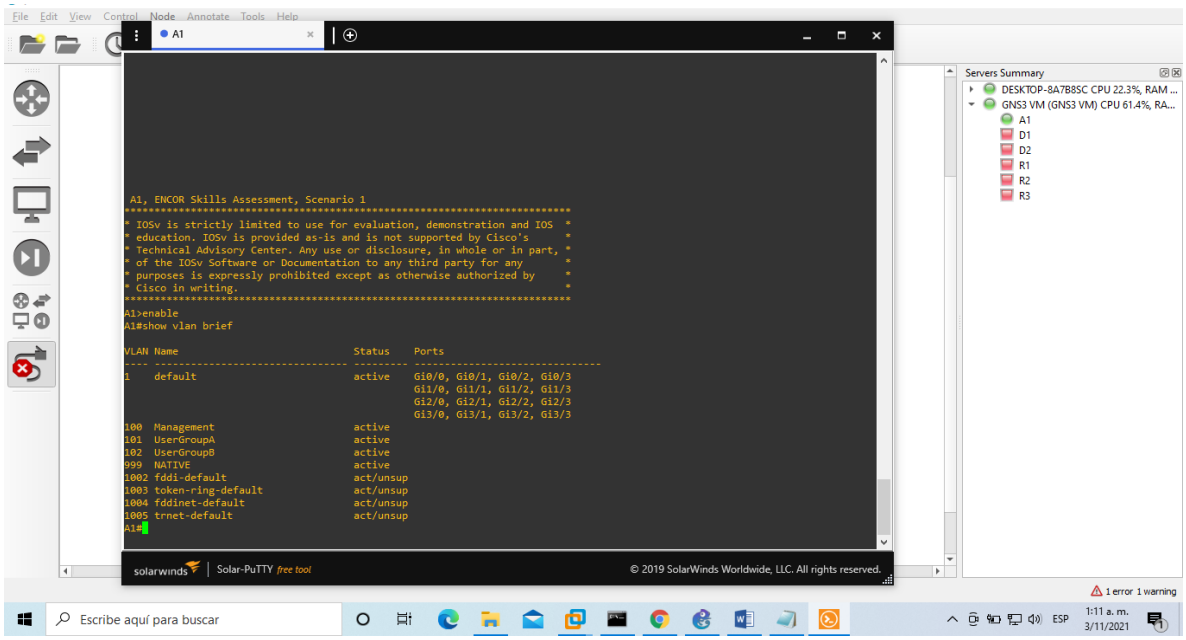
Configuration Switch A1

```
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 range e0/0, e1/1-3, e2/0-3, e3/0-1
shutdown
exit
copy running-config startup-config
show vlan brief
```

Usando el comando show vlan brief se verifican las VLAN, como se muestra en la siguiente figura:

Figura 6. Comando show VLAN brief en Switch A1.



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.

Tabla 2. Tareas de configuración parte 2

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

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

2.1. Configuración de enlaces troncales IEEE 802.1Q.

Los enlaces troncales son enlaces punto a punto entre dispositivos de una red, en este caso se utilizará el protocolo IEEE 802.1Q o Dot1q para etiquetar las tramas y saber a cuál VLAN pertenecen, en esta configuración se utilizará el comando **switchport mode trunk** para cambiar la interfaz a modo troncal permanente.

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

Configuración Switch D1

```
interface range e0/1-3, e1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface range e1/1-2
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
```

Configuración Switch D2

```
interface range e0/1-3, e1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
```

Configuración Switch A1

interface range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown

interface range e0/3, e1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown

Usando el comando **show interfaces trunk** en los switches se puede verificar si la VLAN nativas y de pares coinciden, también sirve para verificar si se ha establecido una troncal entre los switches como se muestra en las siguientes figuras:

Figura 7. Verificando habilitación de enlaces troncales en D1.

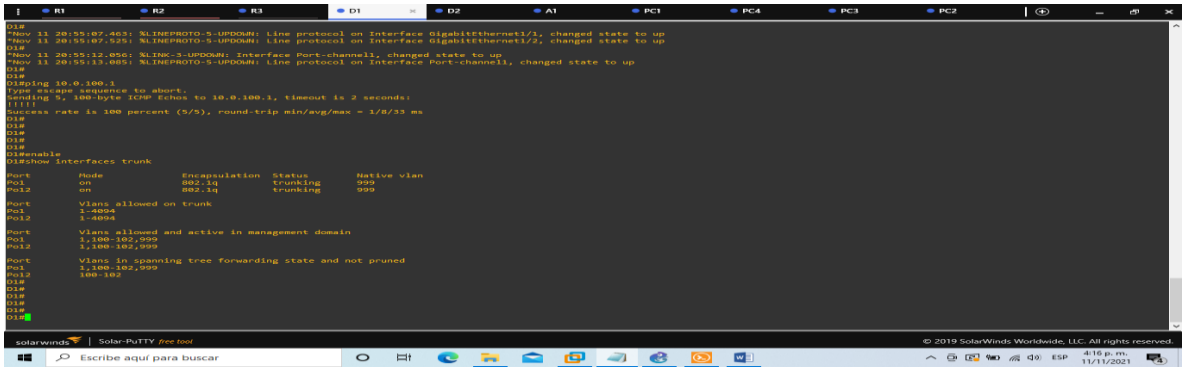


Figura 8. Verificando habilitación de enlaces troncales en A1.

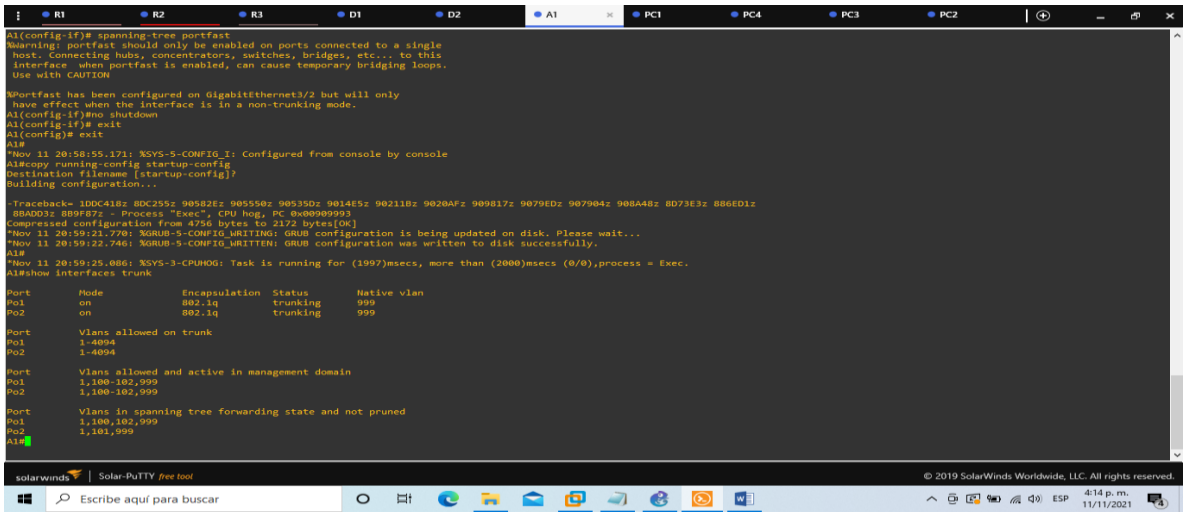


Figura 9. Verificando habilitación de enlaces troncales con el comando show interfaces trunk en D2.

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

Es un protocolo proporciona una convergencia de árbol de extensión más rápida y es utilizado para evitar bucles en las topologías, este protocolo se habilitará en los switches D1, D2 y A1 con el comando **Spanning-Tree mode rapid-pvst.**

2.4. En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología, Configure D1 y D2 como raíz (root) para las VLAN apropiadas.

En este punto se habilita las VLAN 100 y 102 en D1 como puente de raíz primario con el comando **root primary** y la VLAN 101 en D1 como raíz secundaria con el comando **root secondary,** como se muestra en la siguiente configuración:

Configuración Switch D1

```
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

Configuración Switch D2

```
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
```

Configuración Switch A1

```
spanning-tree mode rapid-pvst
```

Para verificar a detalle el puente y los puertos activos en los dispositivos se utiliza el comando **show Spanning-tree** y se mostrará la información detallada como en las siguientes figuras.

Figura 10. Verificación de modo Spanning Tree en D2.

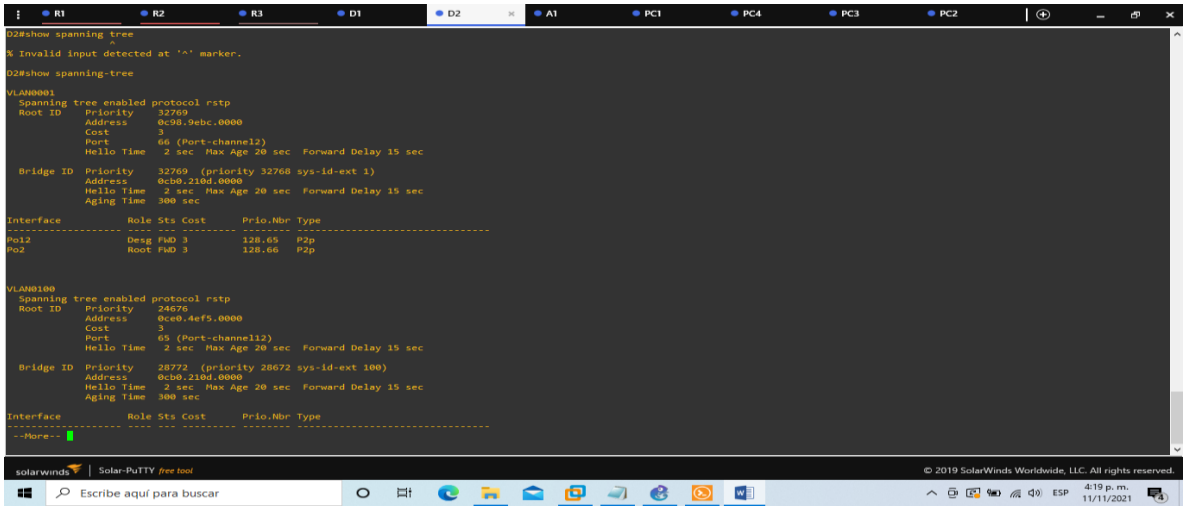
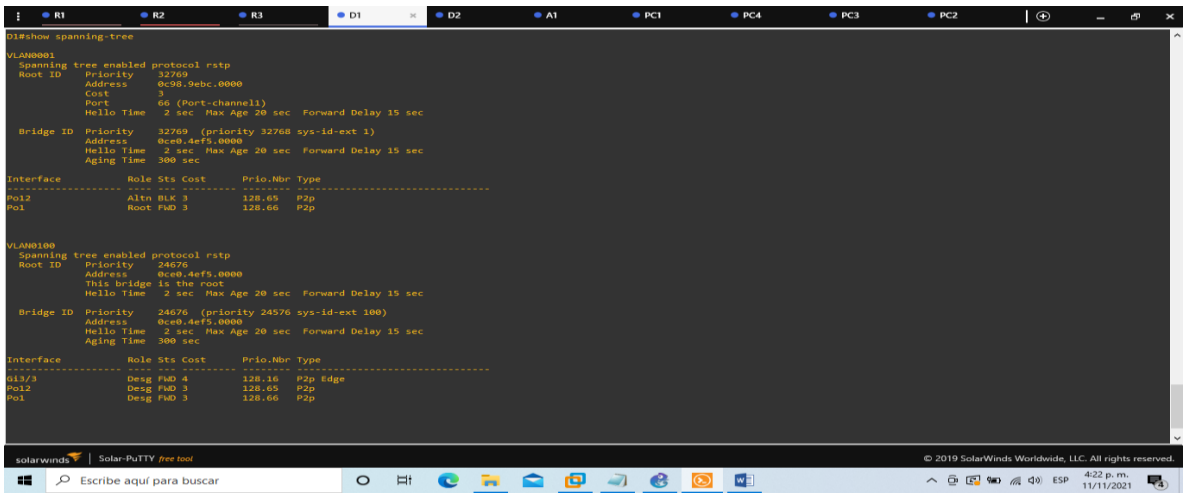


Figura 11. Verificación puente de raíz en D1 Spanning Tree.



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

Los EtherChannels agruparan varios enlaces Ethernet en un único enlace lógico, el cual se utilizará para proporcionar tolerancia a fallos, el comando usado para este fin en los switches es **channel-group mode active,** a continuación, se mostrará la configuración para cada Switch y la interfaz que se configura para este paso.

Use los siguientes números de canales:
D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2

Configuración Switch D1

```
interface range e0/1-3, e1/0
channel-group 12 mode active
no shutdown
interface range e1/1-2
channel-group 1 mode active
no shutdown
exit
```

Configuración Switch D2

```
interface range e0/1-3, e1/0
channel-group 12 mode active
 no shutdown
interface range e1/1-2
channel-group 2 mode active
no shutdown
exit
```

Configuración Switch A1

```
interface range e0/1-2
channel-group 1 mode active
no shutdown
interface range e0/3, e1/0
channel-group 2 mode active
no shutdown
exit
```

Figura 12. Revisando la creación de canales en todos los switches, con el comando show etherchannel summary en D1.

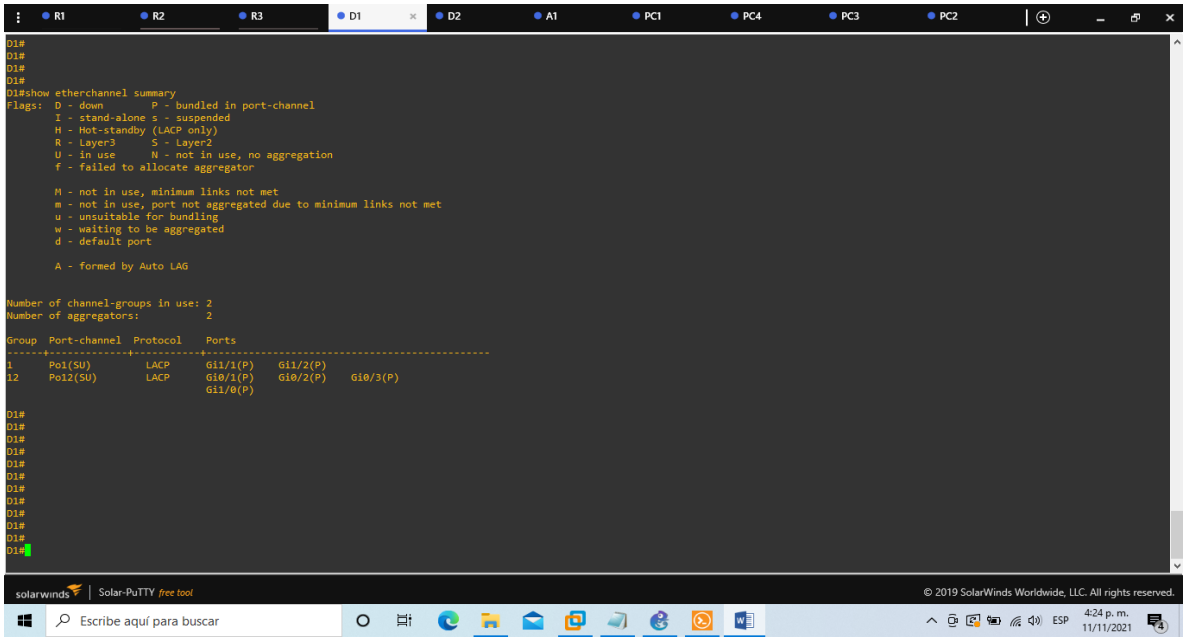
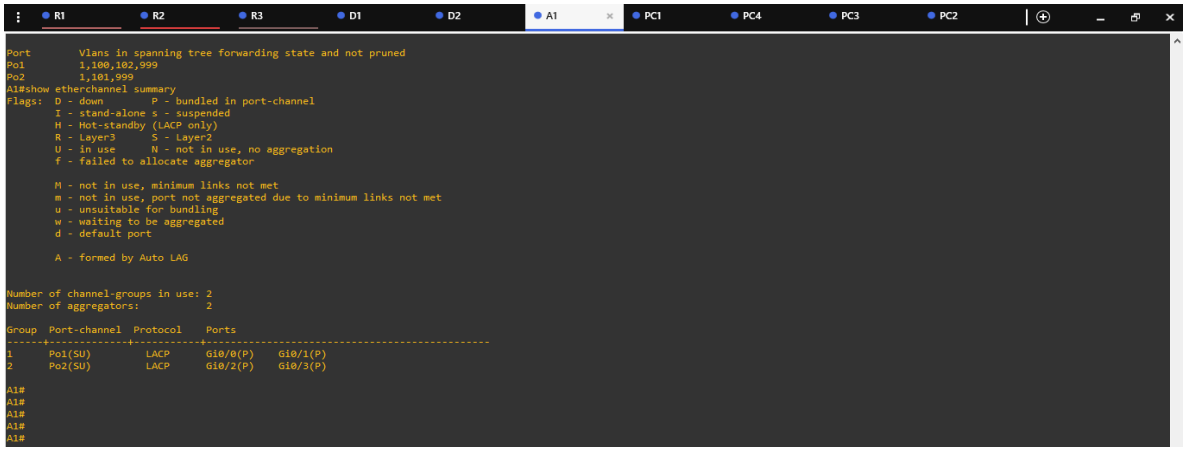


Figura 13. Creación de canales en todos los switches, verificando con el comando show etherchannel summary en D1.

Figura 14. Creación de canales en el Switch A1, verificando con el comando show etherchannel summary.



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.

PortFast es una función que permite a los usuarios obtener un acceso inmediato a la red de capa 2, aquí se utiliza el comando **spanning-tree portfast,** el comando **switchport mode access** configura el puerto como un puerto de acceso lo que hace que este puerto solo podrá comunicarse con otros dispositivos que estén en la misma VLAN.

Configuración Switch D1

interface e3/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit

Configuración Switch D2

```
interface e3/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end
copy running-config startup-config
```

Configuración Switch A1

```
interface e3/2
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface e3/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end
copy running-config startup-config
```

Para verificar que los puertos fueron creados correctamente se usa el comando **show run interface,** seguido del nombre de la interface que se va consultar, en las siguientes figuras se mostrará un ejemplo:

Figura 15. Verificando creación de puertos de acceso interface e3/3 en D2.

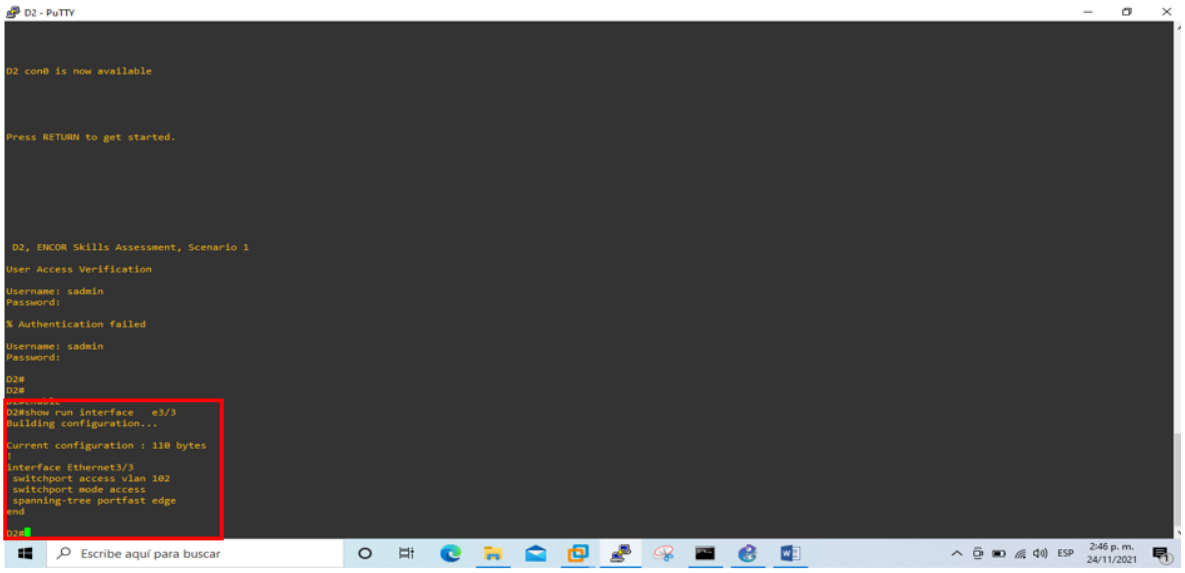
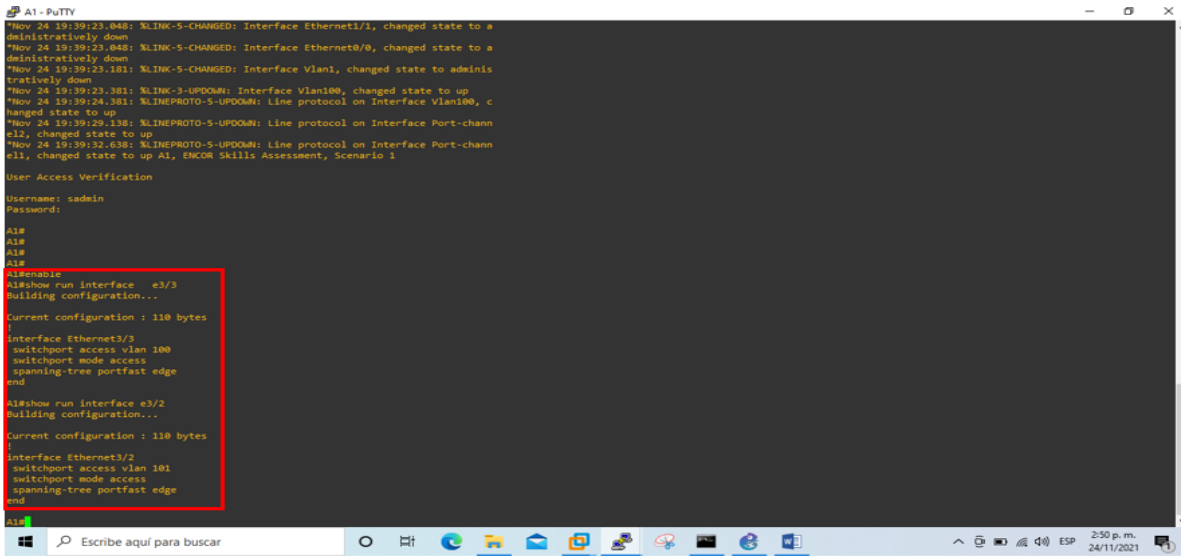


Figura 16. Verificando creación de puertos de acceso en A1 interface e3/3 y e3/2.



2.7. Configuración ip de PCs.

Para la configuración de las IP en los PCs 1 y 4 se utiliza el comando **ip** seguido de la dirección correspondiente, en los PCs 2 y 3 se utiliza el comando **ip dhcp**, automáticamente se asignará la dirección, luego de ingresar estos datos es muy importante ingresar el comando **save,** para que queden guardadas las configuraciones.

Configuración PC1

ip 10.0.100.5/24
ip 2001:db8:100:100::5/64
save

Configuración PC2

ip dhcp
save

Configuración PC3

ip dhcp
save

Configuración PC4

ip 10.0.100.6/24
ip 2001:db8:100:100::6/64
save

Para verificar la configuración en los PCs 2 y 3 los cuales reciben dirección DHCP se utiliza el comando **show.**

Figura 17. Verificando que PC2 recibe IPv4 validas con el comando show.

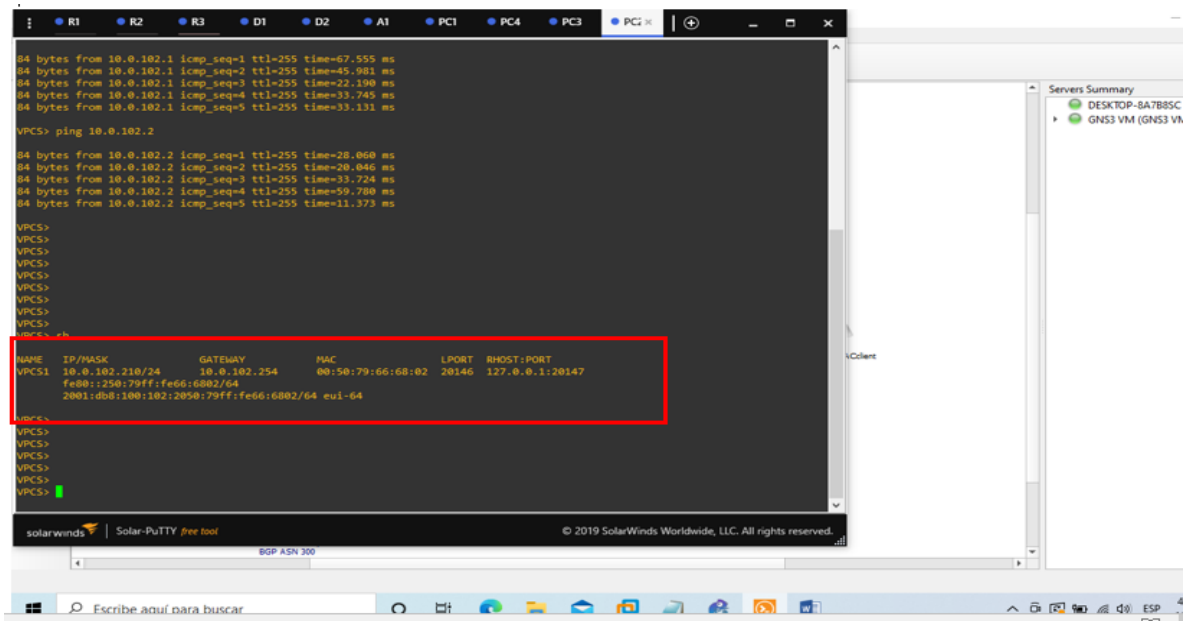
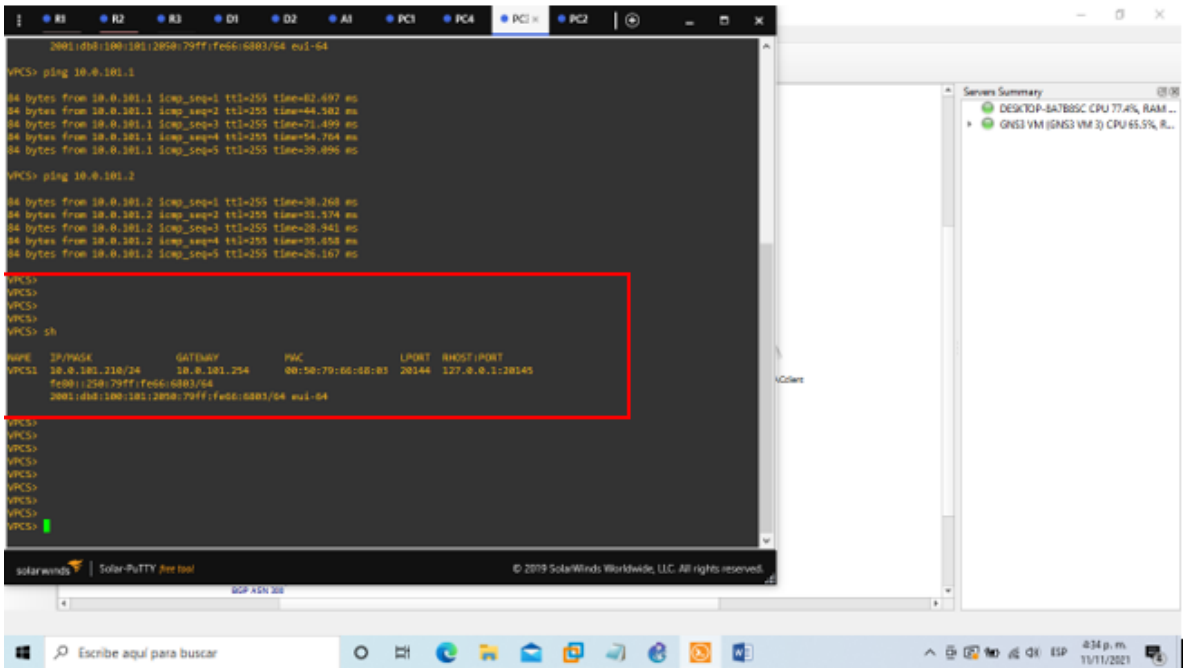


Figura 18. Verificando que PC3 recibe IPv4 validas con el comando show.



2.8 Verifique la conectividad de la LAN local, en este punto se realiza ping desde la Pc1 a los otros dispositivos de la red y deben ser satisfactorios.

Figura 19. Ping de PC-1 a D1-D2-PC4.

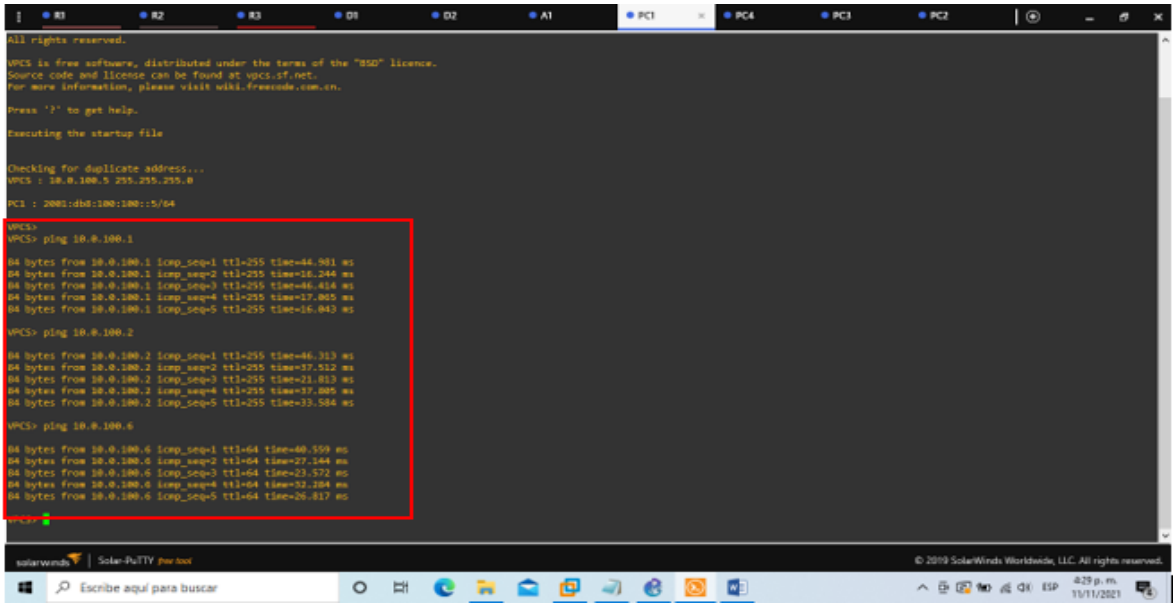


Figura 20. Ping de PC-2 a D1 y D2.

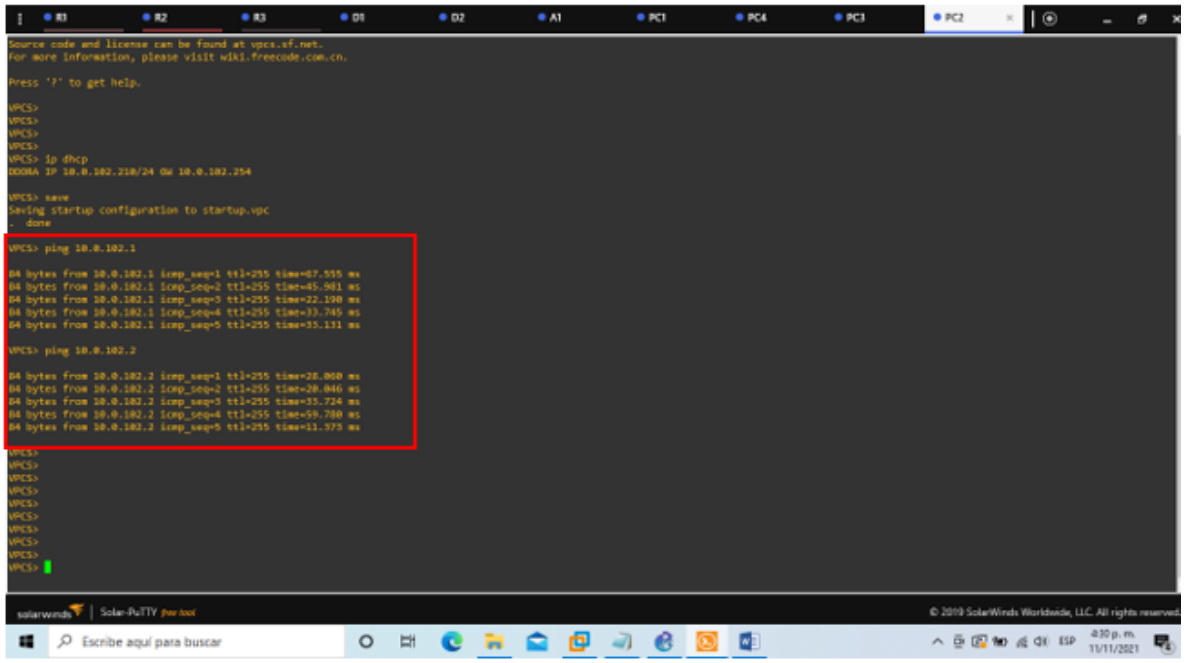


Figura 21. Ping de PC-3 a D1 y D2.

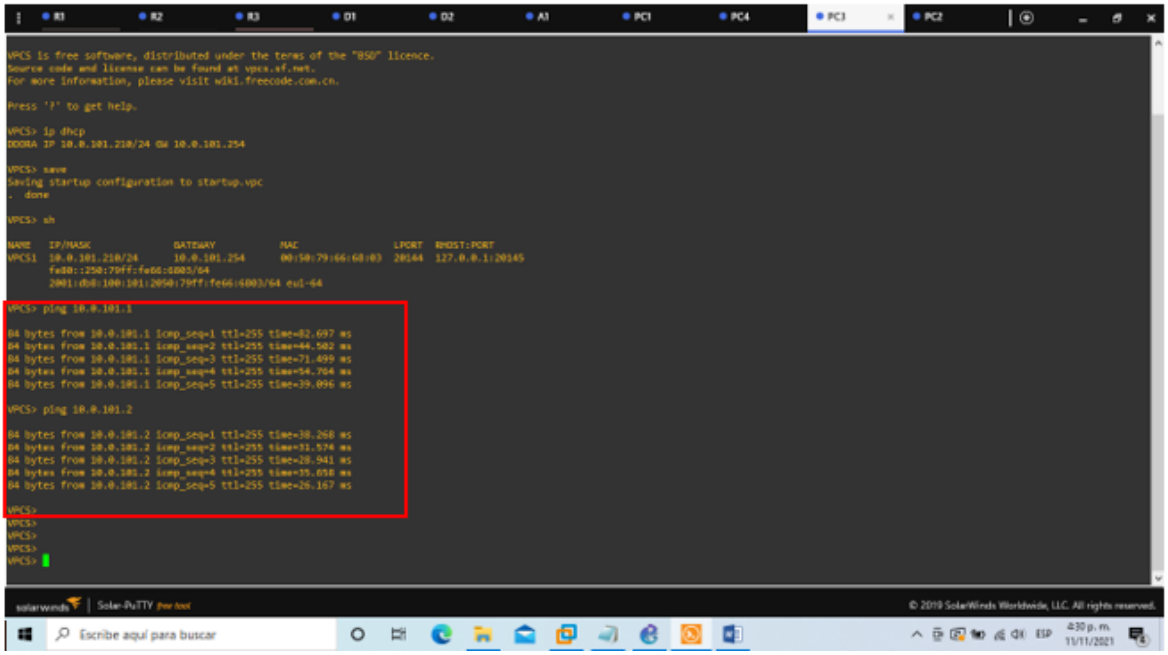
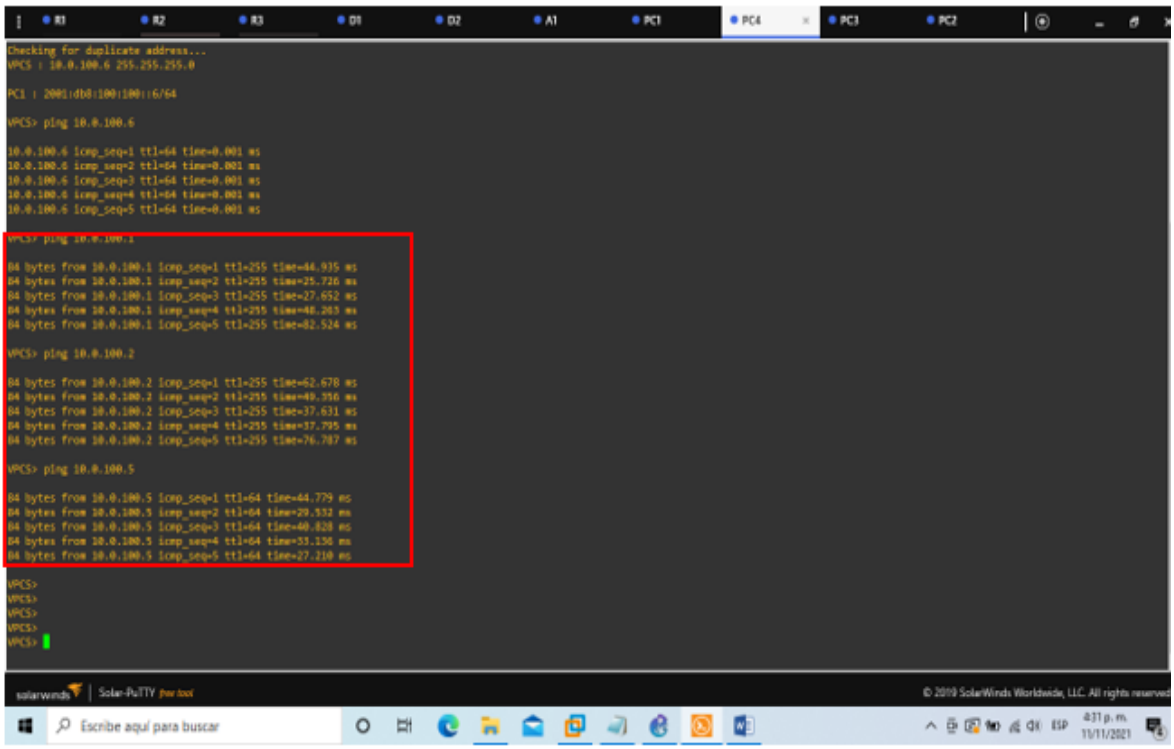


Figura 22. Ping de PC-4 a D1 - D2 y PC-1.



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.

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

Las tareas de configuración son las siguientes:

Tabla 3. Tareas de configuración parte 3

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

Tarea#	Tarea	Especificación
3.3	En R2 en la “Red ISP”, configure MP-BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MP-BGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

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

3.1.1 Use OSPF Process ID 4 y asigne los siguientes router- IDs:

- R1: 0.0.4.1
- R3: 0.0.4.3
- D1: 0.0.4.131
- D2: 0.0.4.132

Para poder configurar OSPFv2 se necesita que OSPF este activo en el router con las direcciones de red y el área especificada, el comando para habilitar OSPF es **router ospf (id_proceso),** id_proceso va hacer el número de enrutamiento que se utilizara para la identificación de OSPF, luego de este paso se debe especificar las redes por donde se enviaran los mensajes de actualización de rutas, cada red se debe identificar con el área a la que pertenece, para esto se usa el comando **network (dirección_red).**

A continuación, se muestra la configuración en los dispositivos requeridos.

Configuración en Router R1

```
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
exit
```

Configuración en Router R3

```
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
exit
```

Configuración Switch D1

```
router ospf 4
router-id 0.0.4.131
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
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e3/2
exit
```

Configuración Switch D2

```
router ospf 4
router-id 0.0.4.132
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
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e3/2
exit
```

Se usa el comando **show run** en los dispositivos donde se habilitó el protocolo OSPF y se busca la sección de OSPF, ahí mostrara los datos configurados anteriormente como id del proceso la direcciones y el área al que pertenece.

Figura 23. Router OSPF Identidad de R1: 0.0.4.1.

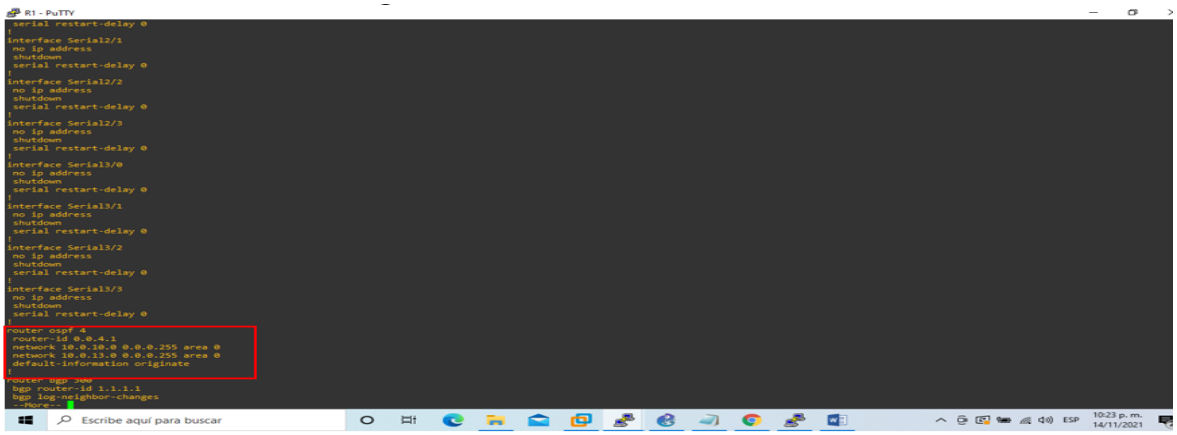


Figura 24. Router OSPF Identidad de R3: 0.0.4.3.

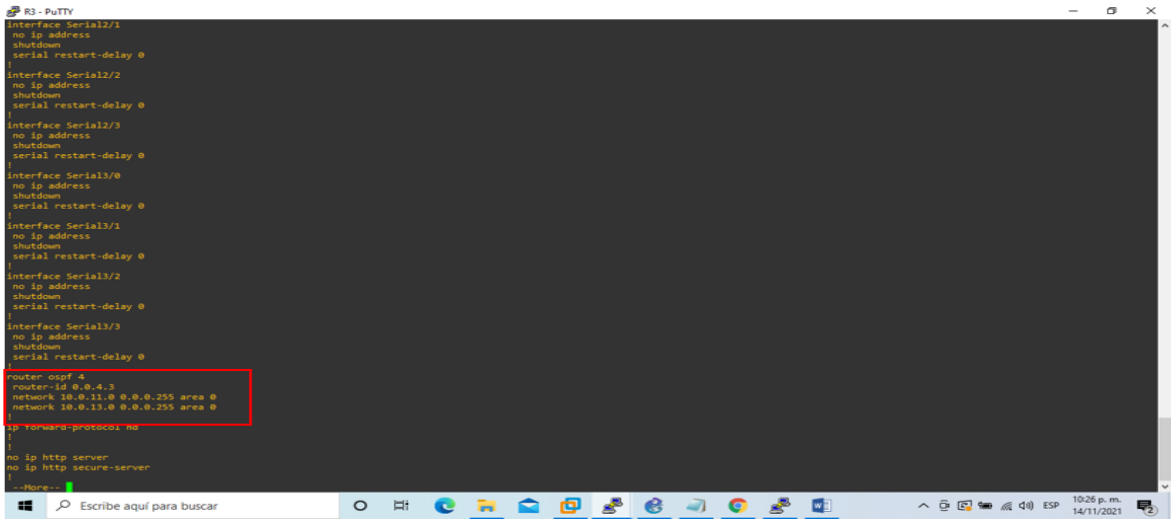
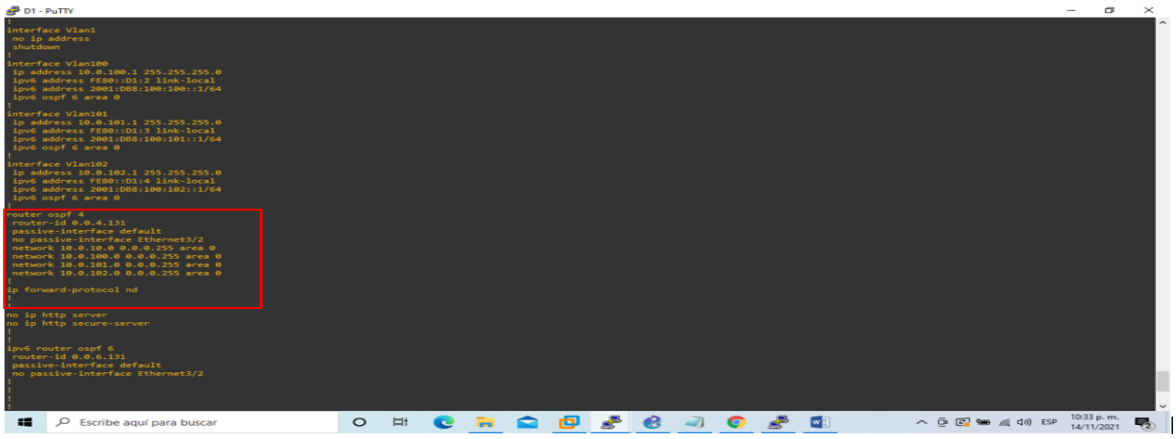


Figura 25. Router OSPF Identidad de D1: 0.0.4.131.



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

Use OSPF Process ID **6** y asigne los siguientes router- IDs:

- R1: 0.0.6.1
- R3: 0.0.6.3
- D1: 0.0.6.131
- D2: 0.0.6.132

En este paso se utiliza el comando **ipv6 router ospf6**, para habilitar el enrutamiento ipv6.

Configuración en Router R1

```
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface e0/1
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```

Configuración en Router R3

```
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e0/1
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```

En los Switches D1 y D2 se utilizará el comando **passive-interface default** para que no reciban actualizaciones de enrutamiento, y se configura una interfaz por la cual se autoriza el enrutamiento con el uso del comando **no passive-interface (nombre_interface).**

Configuración Switch D1

```
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e3/2
exit
interface e3/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
```

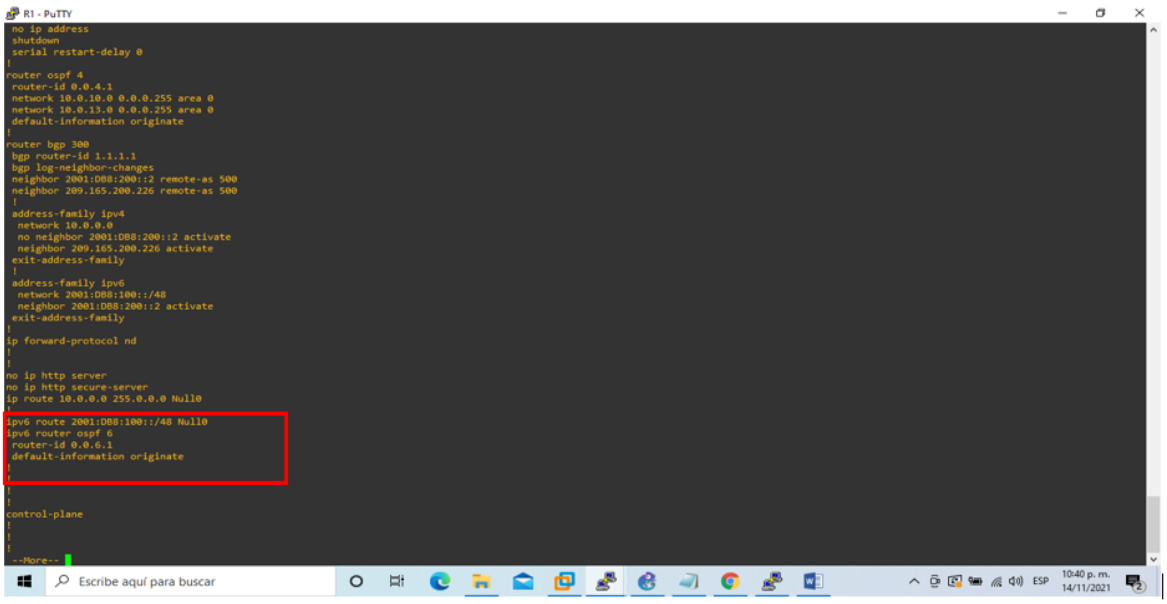
```
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

Configuración Switch D2

```
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface e3/2
exit
interface e3/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

La verificación de la activación de esta configuración se realiza con el comando **show run** y se va hasta la sección de ipv6, donde mostrará la información configurada como se muestra en la figura 26.

Figura 26. Configuración en R1 ipv6 ospf, comando show run.



Utilizando el comando **show ipv6 interface brief** en los dispositivos R1 y R3 de la topología se observarán las interfaces configuradas correctamente, figura 27 y 28.

Figura 27. Configuración interfaces en R1 ipv6 ospf.

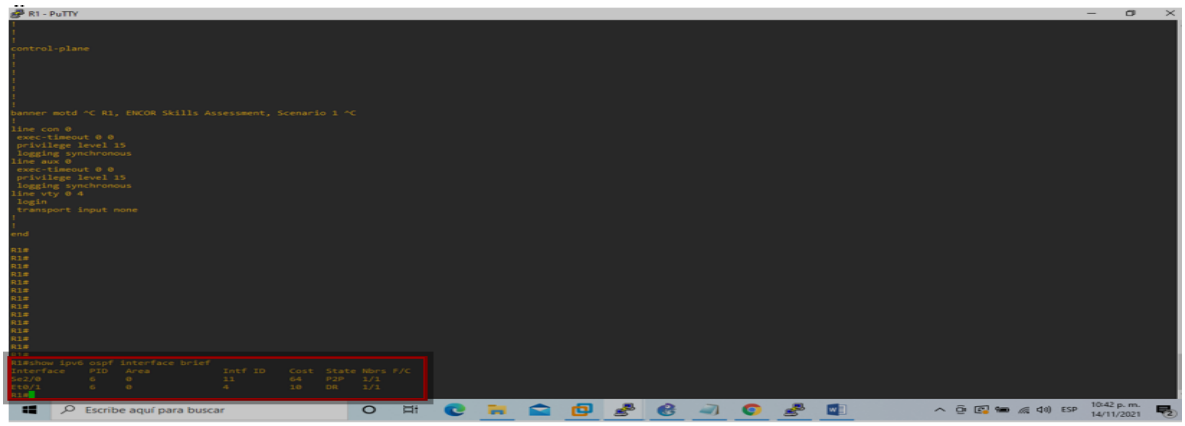
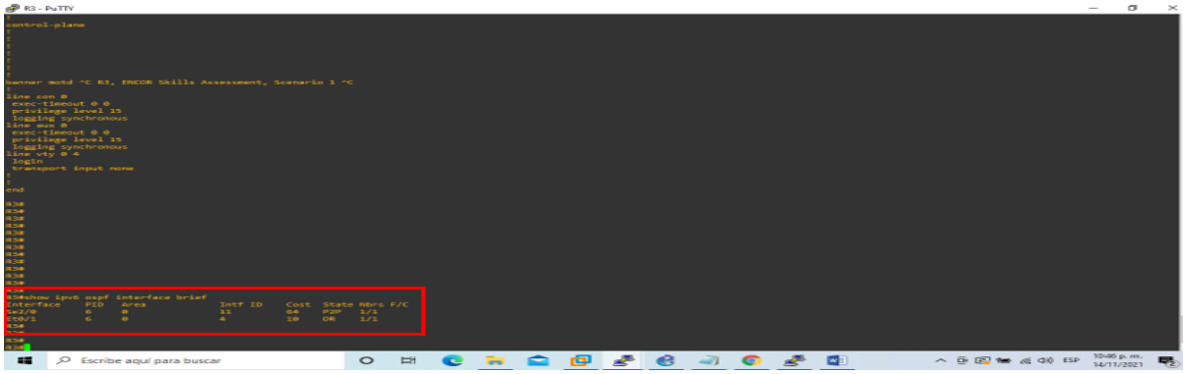
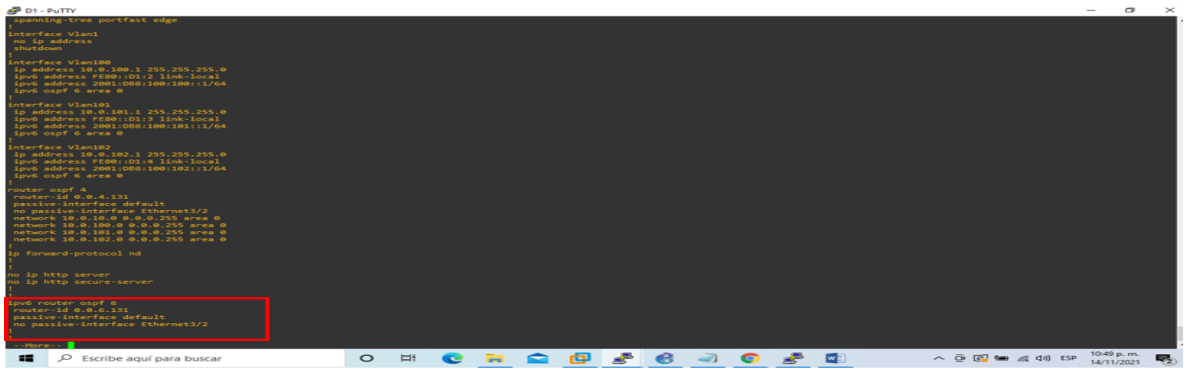


Figura 28. Configuración interfaces en R3 ipv6 ospf.



Ahora se revisará la configuración ipv6 ospf en los switches D1 y D2 con el comando **show run** en la parte de ipv6 route.

Figura 29. Configuración ipv6 ospf. En Switch D1.



Utilizando el comando **show ipv6 interface brief** en los dispositivos D1 y D2 de la topología se observará las interfaces configuradas correctamente.

Figura 30. Configuración interfaces ipv6 ospf. En Switch D1.

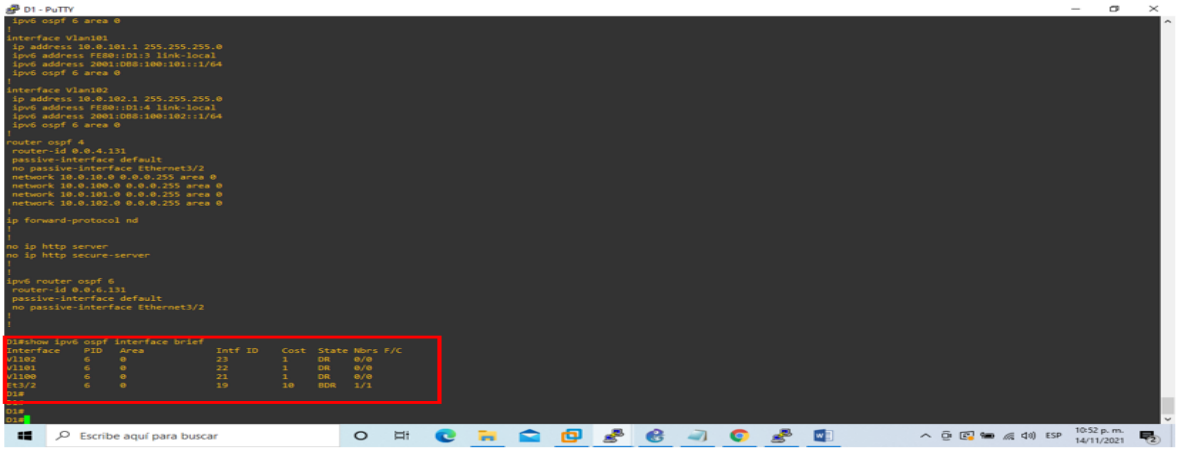


Figura 31. Configuración interfaces ipv6 ospf. En Switch D2.

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

En la configuración del Router R2, se inicia configurando las rutas estáticas con el comando **ip route,** el cual se configura con la interfaz Loopback 0. Para configurar la ruta estática IPv6 se usa el comando **ipv6 route** con la interfaz Loopback.

Configuración en Router R2

Configuración de rutas estáticas IPv4 y IPv6

R2# ip route 0.0.0.0 0.0.0.0 loopback 0
R2# ipv6 route ::/0 loopback 0

Configuración BGP ASN 500 con identidad 2.2.2.2.

El BGP multiprotocolo se habilitará para que permita transporte de información de enrutamiento de varias capas de red y familias de direcciones, en este punto se utilizará el comando **router bgp (ASN),** el cual habilita el dominio de BGP y define el número de sistema autónomo, el ASN es proporcionado por su proveedor de servicios, luego se le asignara una identidad con el comando **bgp router-id (numero_identidad)**, a continuación, se muestra la configuración:

R2# router bgp 500
R2# bgp router-id 2.2.2.2

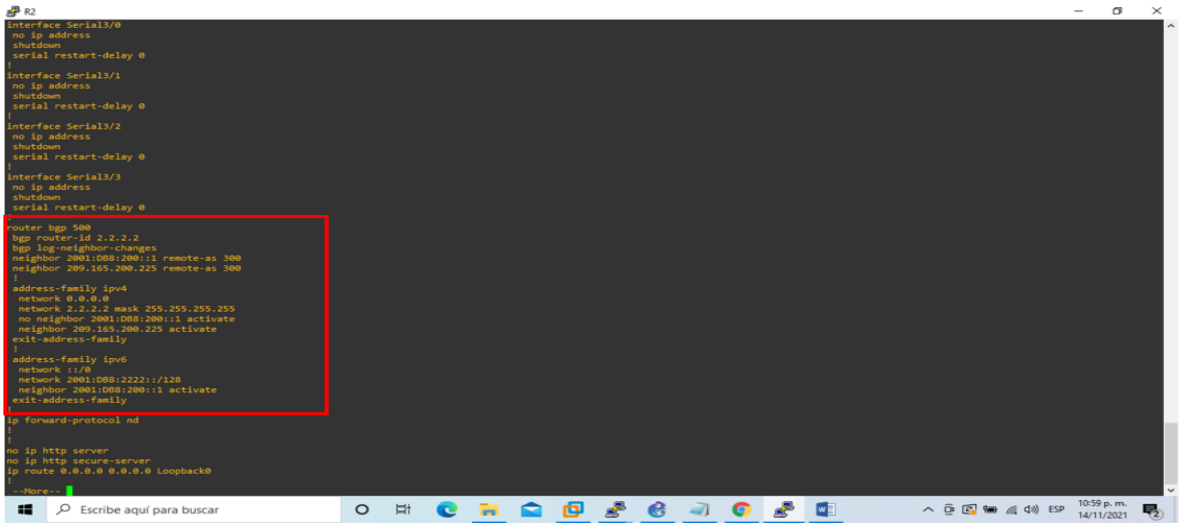
Configuración de IPv4 y IPv6 address family.

La configuración se llevará a cabo con los siguientes comandos **neighbor (dirección) remote-as(numero_ASN),** definirá el vecino como miembro del ASN remoto. El comando **address-family ipv4 y address-family ipv6**, permite ingresar el modo de comando ip de familia.

R2# neighbor 209.165.200.225 remote-as 300
R2# neighbor 2001:db8:200::1 remote-as 300
R2# address-family ipv4
R2# neighbor 209.165.200.225 activate
R2# no neighbor 2001:db8:200::1 activate
R2# network 2.2.2.2 mask 255.255.255.255
R2# network 0.0.0.0
R2# exit-address-family
R2# address-family ipv6
R2# no neighbor 209.165.200.225 activate
R2# neighbor 2001:db8:200::1 activate
R2# network 2001:db8:2222::/128
R2# network ::/0
R2# exit-address-family
exit

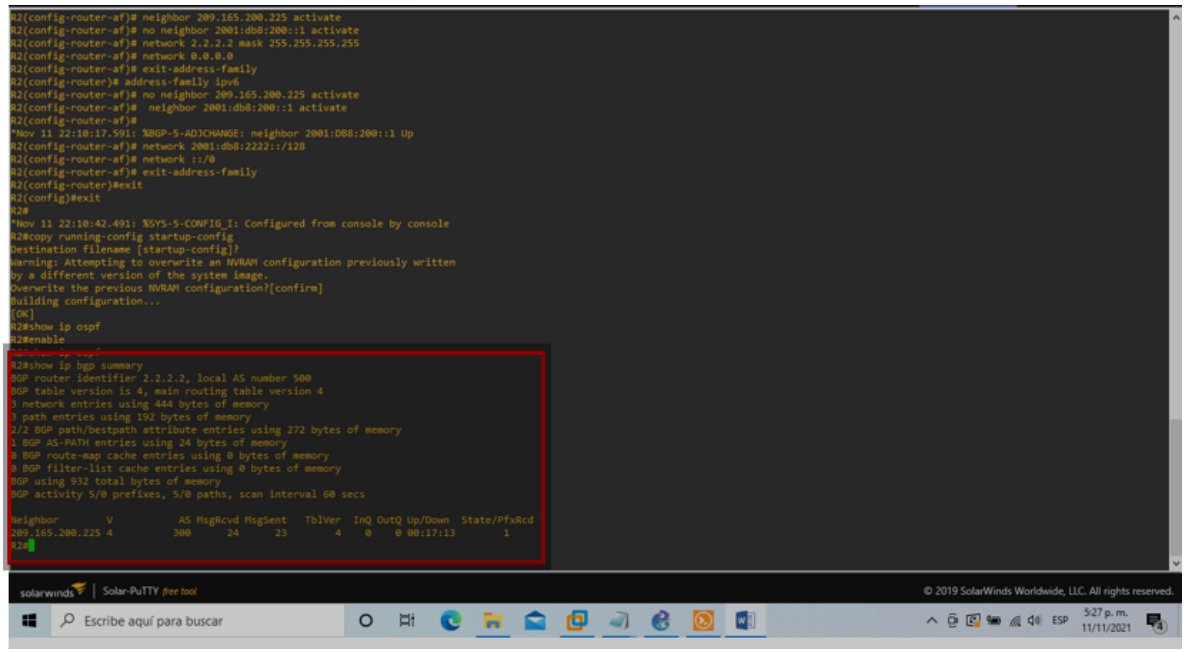
En este paso se utilizará el comando **show run** y se debe ir hasta la sección donde muestre la configuración de BGP y address family como se muestra en la siguiente figura.

Figura 32. Configuración de Router R2 BGP y address family IPv4 y IPv6.



Con el comando **show ip bgp summary** se mostrará un resumen de la configuración del modo BGP, como se muestra en la figura 33.

Figura 33. Configuración de router R2 BGP y address family IPv4 y IPv6.



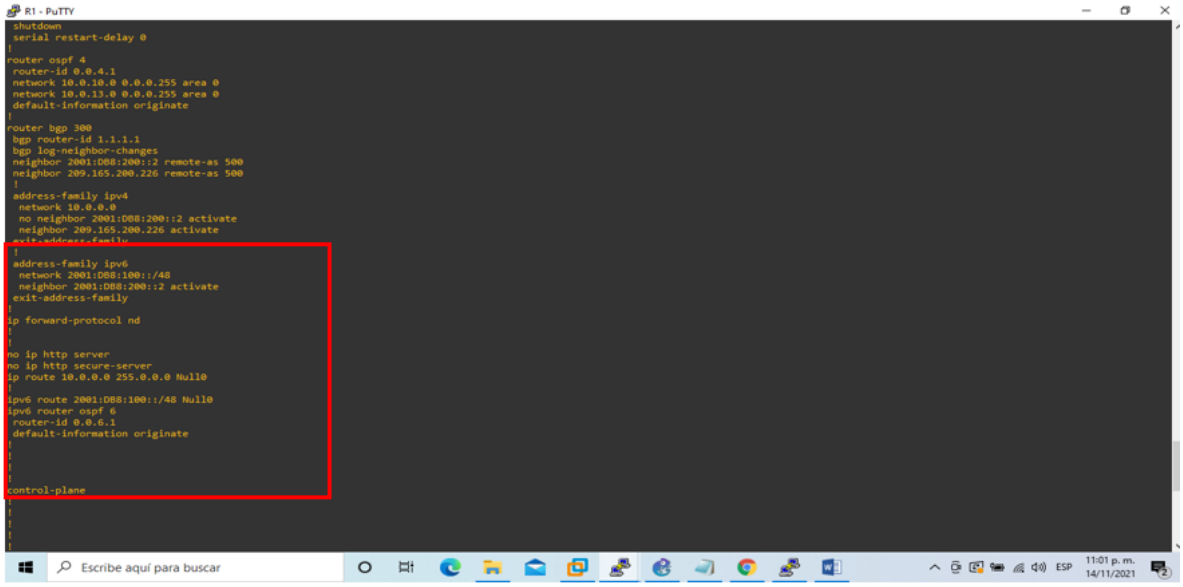
3.4. En R1 en la “Red ISP”, configure MP- BGP.

Configuración en Router R1

R1# router bgp 300
R1# bgp router-id 1.1.1.1
R1# neighbor 209.165.200.226 remote-as 500
R1# neighbor 2001:db8:200::2 remote-as 500
R1# address-family ipv4 unicast
R1# neighbor 209.165.200.226 activate
R1# no neighbor 2001:db8:200::2 activate
R1# network 10.0.0.0 mask 255.0.0.0
R1# exit-address-family
R1# address-family ipv6 unicast
R1# no neighbor 209.165.200.226 activate
R1# neighbor 2001:db8:200::2 activate
R1# network 2001:db8:100::/48
R1# exit-address-family
R1# exit

Se verifica la correcta configuración con el comando **show run** y se revisa la parte de BGP donde se mostrará la id del router bgp, adrress family IPv4 y IPV6, en R1.

Figura 34. Configuración de router R1 BGP y address family IPv4 y IPv6.



Se verifica también OSPF y BGP para IPv4 en el Router R1 con el comando **show ip route** donde mostrará la tabla de direcciones como lo muestran las siguientes figuras.

Figura 35. Configuración en router IPv4 BGP y OSPF de R1.

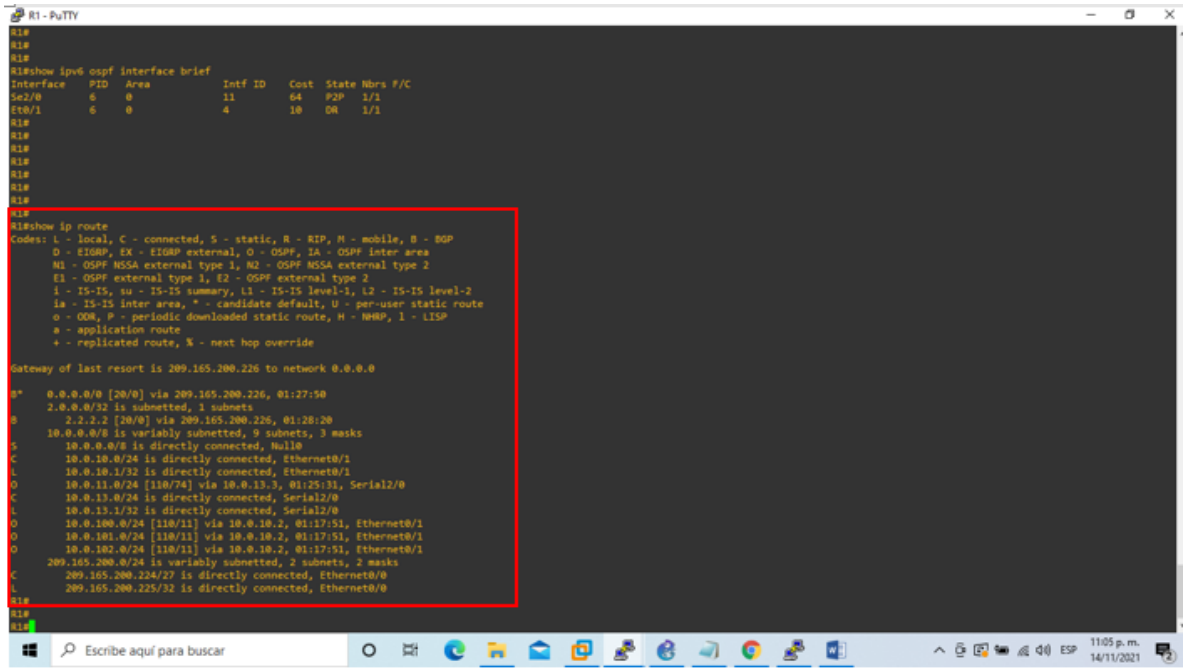
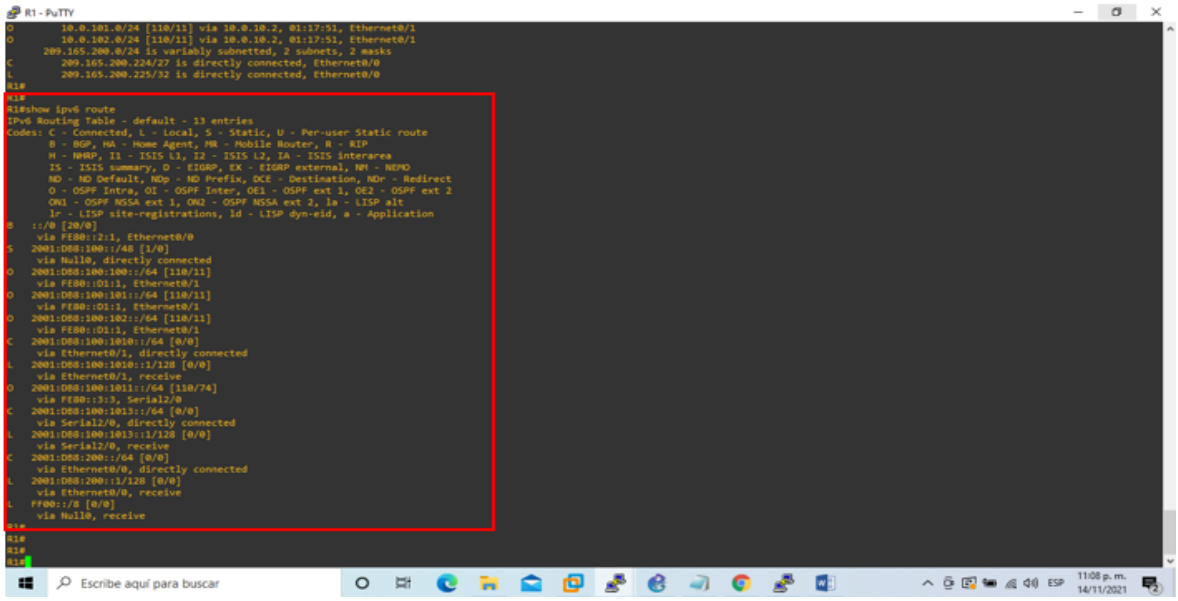


Figura 36. Configuración de router R2 BGP y OSPF IPv6, comando show ipv6 route.



En las siguientes imágenes se mostrarán las configuraciones del router R3 con respecto a las tablas de direcciones figura número 37 IPV4., usando el comando **show ip route ospf** y figura número 38 IPv6, usando el comando **show ipv6 route ospf**.

Figura 37. Configuración de direcciones IPv4 en router R3.

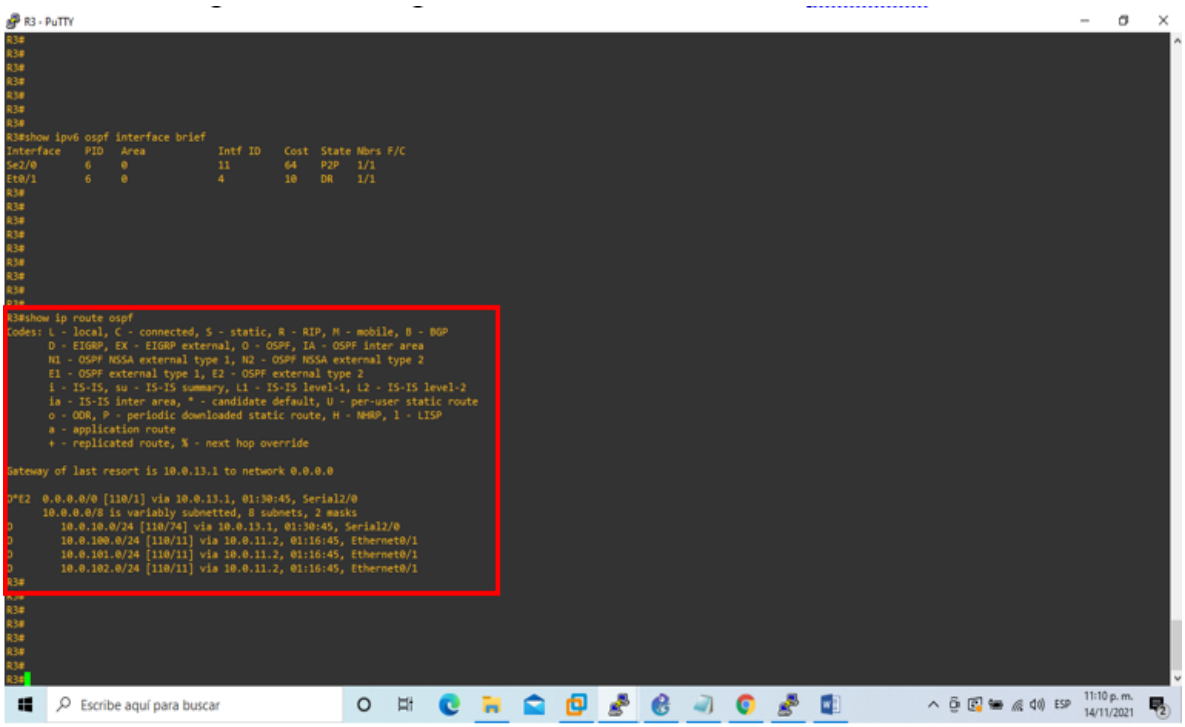
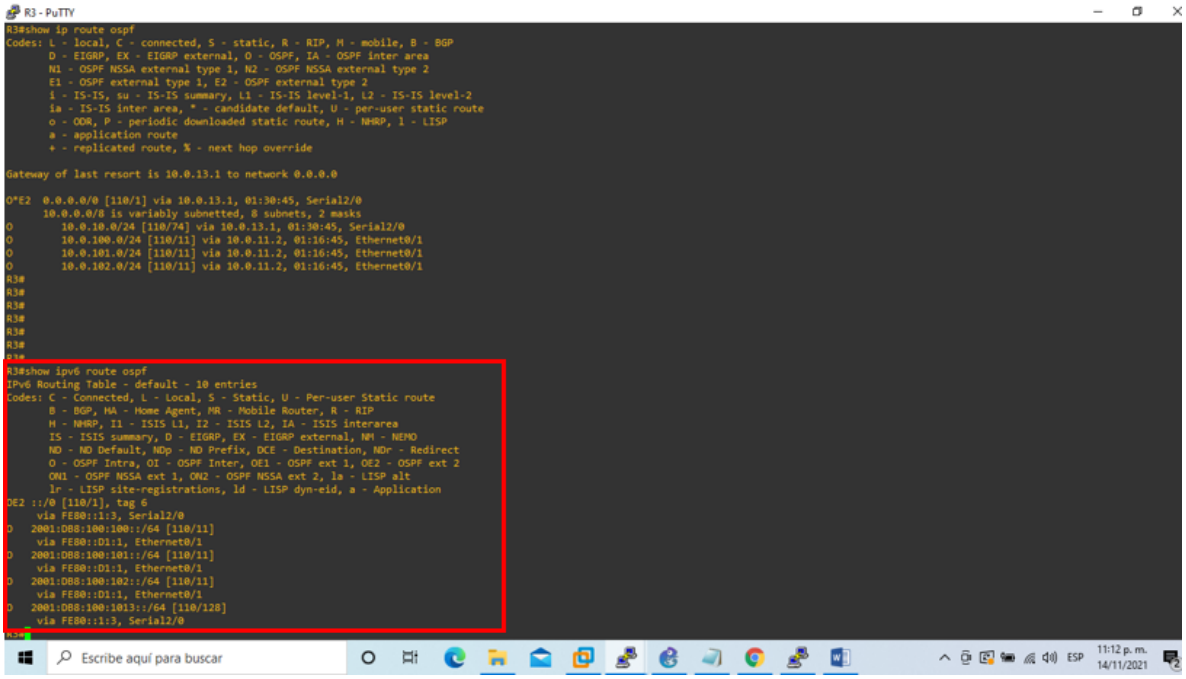


Figura 38. Configuración de direcciones IPv6 en Router R3.



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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Tabla 4. Tareas de configuración parte 4

Tarea #	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 E0/1	Cree dos IP SLAs. Use la SLA número 4 para IPv4. Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 E0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. Use el número de rastreo 4 para la IP SLA 4. Use el número de rastreo 6 para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 E0/1	Cree IP SLAs. Use la SLA número 4 para IPv4. Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R3 E0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. Use el número de rastreo 4 para la IP SLA 4. Use el número de rastreo 6 para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos
4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: Asigne la dirección IP virtual 10.0.100.254. Establezca la prioridad del grupo en 150. Habilite la preferencia (preemption). Rastree el objeto 4 y decremente en 60.

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

		Configure IPv6 HSRP grupo 106 para la VLAN 100: Asigne la dirección IP virtual usando ipv6 autoconfig. Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: Asigne la dirección IP virtual usando ipv6 autoconfig. Establezca la prioridad del grupo en 150. Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: Asigne la dirección IP virtual usando ipv6 autoconfig. Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60.

4.1. En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 E0/1.

Las IP SLAs analizan los niveles de servicio de aplicaciones y servicios de IP, se usará el comando **ip sla (numero_identidad),** para iniciar la configuración, el número de identidad se utiliza para identificar la operación, para configurar la operación de la ip sla se usa el siguiente comando **icmp-echo (dirección_ip),** luego se establece la velocidad a la que se quiere que se repita la operación con el comando **frequency(segundos),** los segundos pueden ir de 10 a 500 segundos.

Para la configuración de los parámetros de programación de una única operación se usa el comando **ip sla schedule (numero_identidad) life forever start-time now,** la operación queda configurada para ejecutarse indefinidamente y para comenzar inmediatamente.

En la configuración de SLA Tracking o rastreo de una operación IP SLA se ingresa con el comando **track (numero_rastreo) ip sla (numero_identidad)**, se configura el periodo de tiempo en segundos el cual rastreara los cambios de estado de un número de rastreo ejecutando el comando **delay down (segundos) up (segundos),** donde down y up indica el periodo de tiempo para retrasar los cambios de estado.

Configuración en D1

```
D1# ip sla 4
D1# icmp-echo 10.0.10.1
D1# frequency 5
D1# exit
D1#ip sla 6
D1# icmp-echo 2001:db8:100:1010::1
D1# frequency 5_
D1# exit
D1#ip sla schedule 4 life forever start-time now
D1#ip sla schedule 6 life forever start-time now
D1#track 4 ip sla 4
D1# delay down 10 up 15
D1# exit
```

D1#track 6 ip sla 6
D1# delay down 10 up 15
D1# exit
D1#copy running-config startup-config

4.2. En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R1 E0/1

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

Para revisar la configuración de IP SLAs usamos el comando **show run** y buscamos la sección donde se encuentre las IP SLA, como se muestra en la figura número 39 con el Switch D1 y figura 40 en el Switch D2.

Figura 39. Verificando configuración IP SLAs en D1con el comando **show run**.

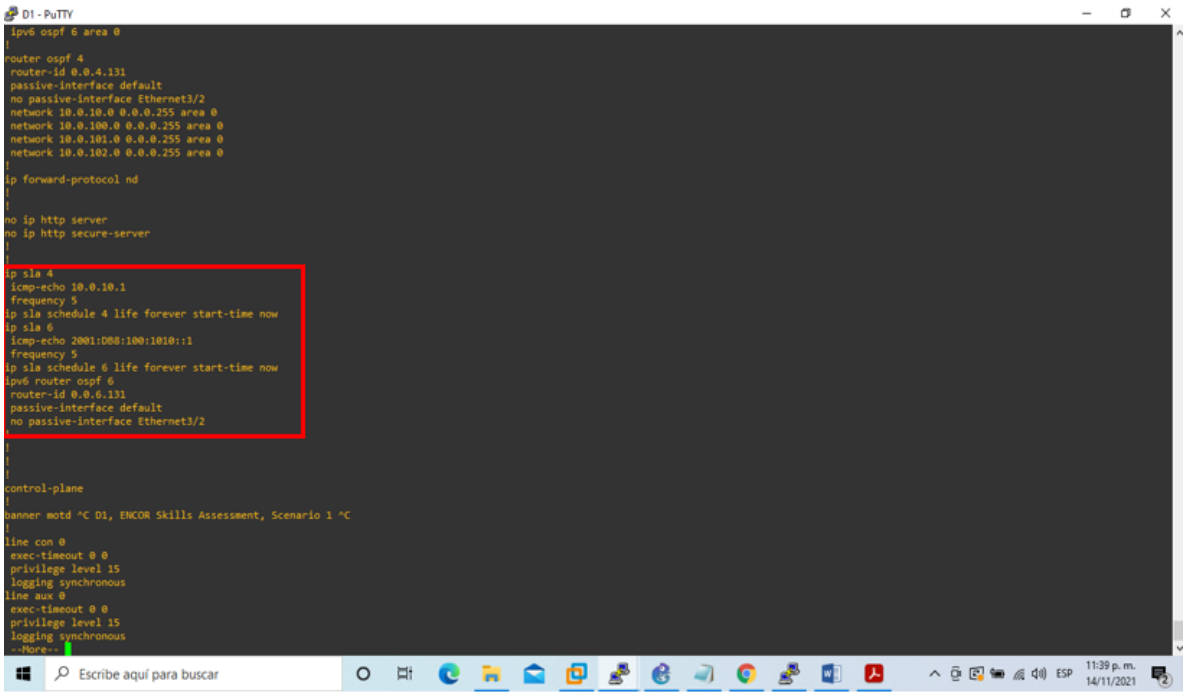
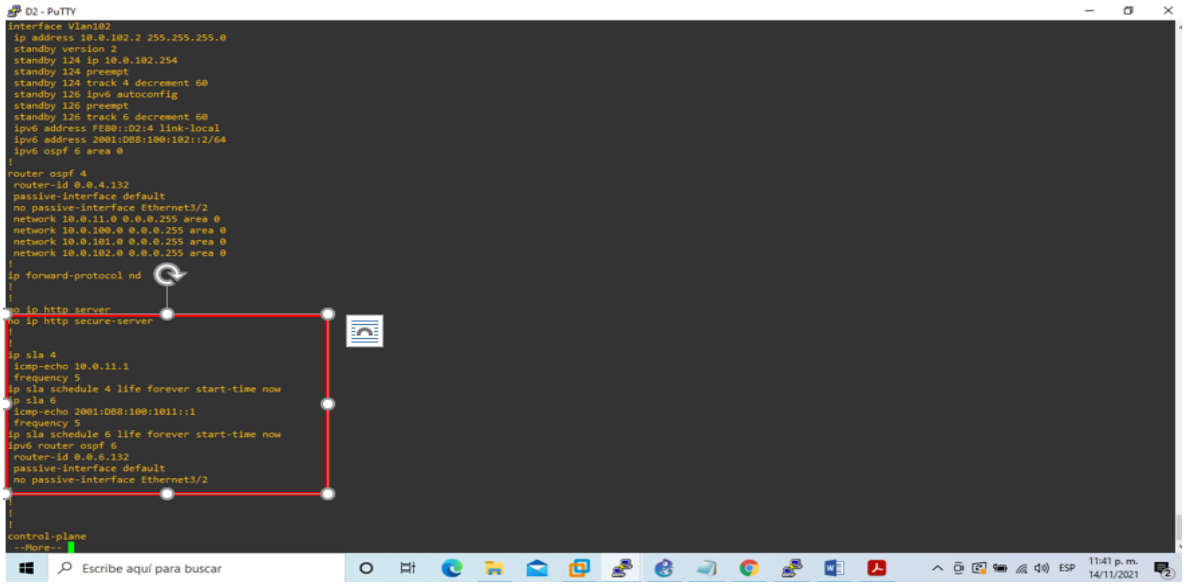


Figura 40. Verificando configuración IP SLAs en D2 con el comando show run.



4.3. En D1 configure HSRPv2, D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

La HSRPv2 es la encargada de anunciar y aprender valores del temporizador en milisegundos, asegurando la estabilidad de los grupos HSRP y proporciona una mejor resolución de problemas, Para configurar HSRPv2 en D1 se deben tener en cuenta los siguientes comandos, **interface (nombre_vlan),** este comando se utiliza para configurar una interface e ingresar al modo de configuración, luego el comando **standby version 2,** para cargar la version de HSRP, el siguiente comando es **standby (numero_grupo) ip (dirección_ip),** el cual asigna un grupo en espera y una dirección ip en espera, usando el comando **standby (numero_grupo)preempt,** permite que el dispositivo se convierta en un dispositivo activo cuando tiene la prioridad más alta, el comando **standby(numero_grupo) track(numero_rastreo) decrement 60,** configura HSRP para rastrear un objeto y cambiar el host a standby.

Configuración en D1

D1#interface vlan 100
D1#standby version 2
D1# standby 104 ip 10.0.100.254
D1#standby 104 priority 150
D1# standby 104 preempt
D1# standby 104 track 4 decrement 60
D1#standby 106 ipv6 autoconfig
D1#standby 106 priority 150
D1# standby 106 preempt
D1#standby 106 track 6 decrement 60
D1#exit
D1#interface vlan 101
D1# standby version 2
D1# standby 114 ip 10.0.101.254
D1# standby 114 preempt
D1# standby 114 track 4 decrement 60

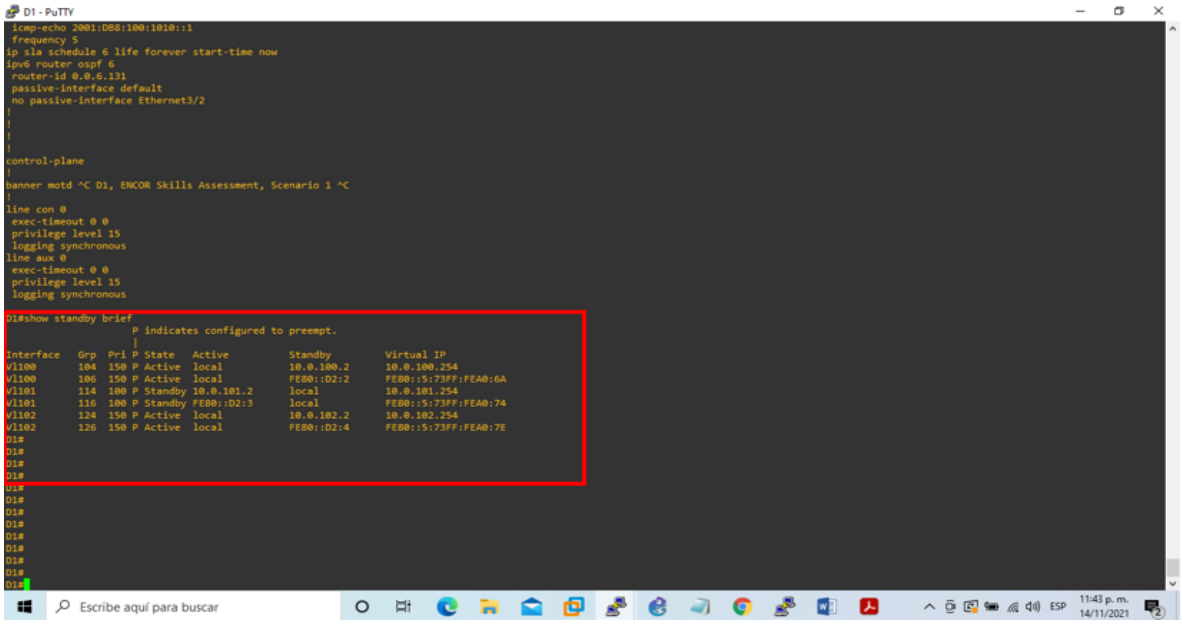
```
D1# standby 116 ipv6 autoconfig
D1# standby 116 preempt
D1# standby 116 track 6 decrement 60
D1# exit
D1#interface vlan 102
D1# standby version 2
D1# standby 124 ip 10.0.102.254
D1# standby 124 priority 150
D1# standby 124 preempt
D1# standby 124 track 4 decrement 60
D1# standby 126 ipv6 autoconfig
D1#standby 126 priority 150
D1# standby 126 preempt
D1# standby 126 track 6 decrement 60
D1# exit
D1# end
copy running-config startup-config
```

Configuración en D2

```
D2# interface vlan 100
D2# standby version 2
D2# standby 104 ip 10.0.100.254
D2#standby 104 priority 150
D2# standby 104 preempt
D2# standby 104 track 4 decrement 60
D2# standby 106 ipv6 autoconfig
D2#standby 106 priority 150
D2#standby 106 preempt
D2#standby 106 track 6 decrement 60
D2# exit
D2#interface vlan 101
D2#standby version 2
D2#standby 114 ip 10.0.101.254
D2#standby 114 preempt
D2#standby 114 track 4 decrement 60
D2# standby 116 ipv6 autoconfig
D2#standby 116 preempt
D2#standby 116 track 6 decrement 60
D2#exit
D2#interface vlan 102
D2#standby version 2
D2#standby 124 ip 10.0.102.254
D2#standby 124 priority 150
D2#standby 124 preempt
D2#standby 124 track 4 decrement 60
D2#standby 126 ipv6 autoconfig
D2# standby 126 priority 150
D2#standby 126 preempt
D2#standby 126 track 6 decrement 60
D2#exit
D2#end
D2#copy running-config startup-config
```

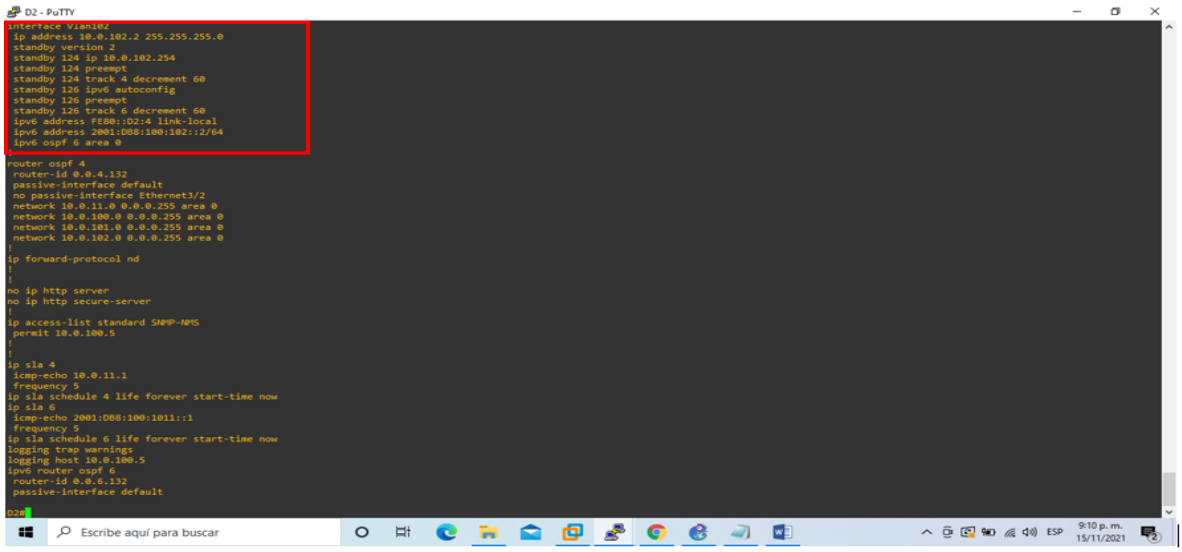
Para la verificación de la correcta configuración se utilizará el comando **show standby brief** en los Switches D1 y D2 como se muestra a continuación.

Figura 41. Verificando configuración en D1.



En la figura número 42 se verifica la configuración de HSRPv2 en el Switch D2 utilizando el comando **show run** y se va hasta la sección de interface VLAN102 donde muestra la dirección virtual de la interface con su decremento de 60.

Figura 42. Verificando configuración D2.



5. Parte 5: Seguridad

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

Tabla 5. Tareas de configuración parte 5

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

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT, Contraseña: cisco12345cisco, en R2 no se configura la protección.

El algoritmo Scrypt es de alto nivel de seguridad y su nivel de seguridad es ajustable y esta creado para que el programador pueda aumentar o disminuir diferentes variables y se usa el siguiente comando **algorithm-type SCRYPT secret (contraseña)**

Configuración R1

R1# enable algorithm-type SCRYPT secret cisco12345cisco

Configuración R3

R3# enable algorithm-type SCRYPT secret cisco12345cisco

Configuración D1

D1# enable algorithm-type SCRYPT secret cisco12345cisco

Configuración D2

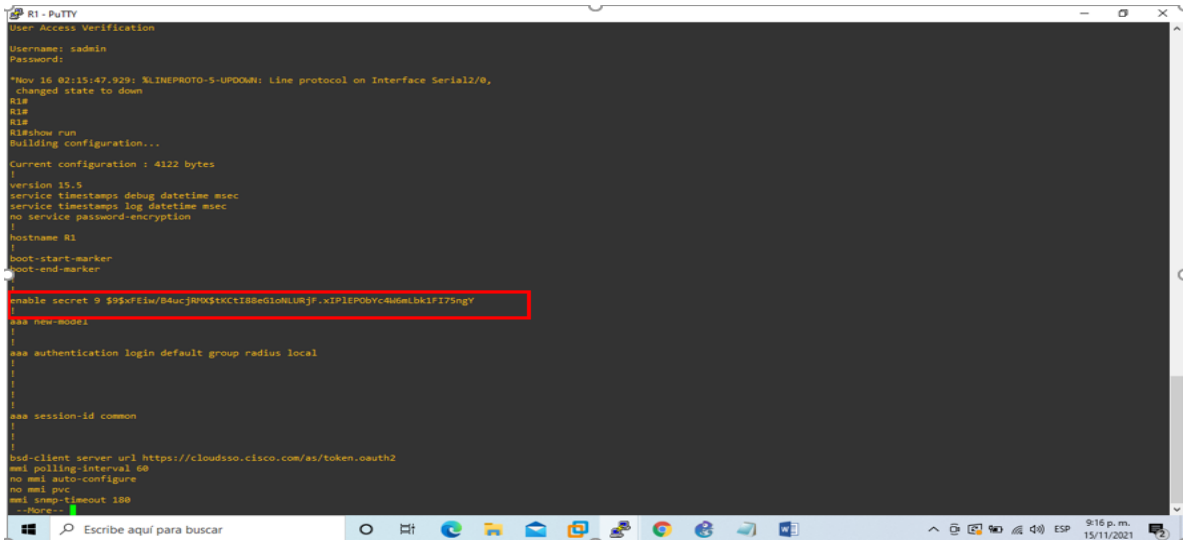
D2# enable algorithm-type SCRYPT secret cisco12345cisco

Configuración A1

A1# enable algorithm-type SCRYPT secret cisco12345cisco

Para verificar la configuración en los dispositivos se utiliza el comando show run y se dirige hasta la sección de secret como se indica en la figura 43.

Figura 43. Verificando configuración de seguridad en R1.



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

Detalles de la cuenta encriptada SCRYPT:
Nombre de usuario Local: **sadmin**
Nivel de privilegio **15**
Contraseña: **cisco12345cisco**

Para realizar esta configuración es necesario crear un nombre, el nivel de privilegio y una contraseña y habilitarlo con el siguiente comando, **username (nombre) privilege (nivel_ privilegio) algorithm-type SCRYPT secret (contraseña).**

Configuración R1

R1# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Configuración R3

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

Configuración D1

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

Configuración D2

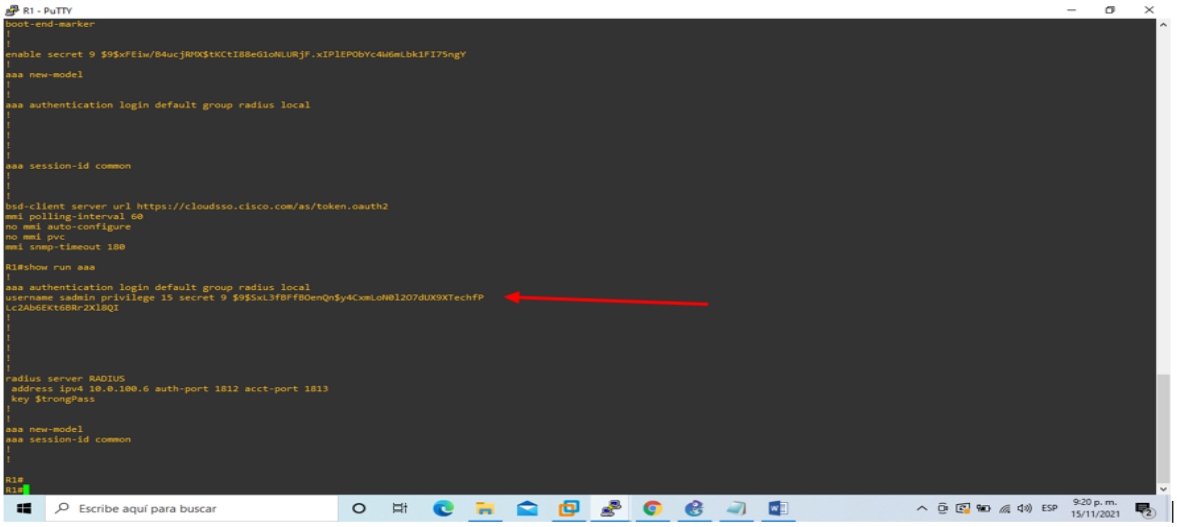
D2# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Configuración A1

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

Para verificar la configuración en los dispositivos se utiliza el comando **show run aaa**, en este caso se demostrará en el router R1 figura 44

Figura 44. Verificando configuración de seguridad en R1.



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

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

Para poder habilitar AAA primero de usa el comando **aaa new-model** en la configuración global, este comando habilita instantáneamente la autenticación local en todas las líneas e interfaces, luego se

debe configurar el nombre del servidor con el comando **radius server RADIUS,** hecho este paso de sede registrar la dirección ip que utiliza el servidor de acceso para comunicarse con el servidor AAA usando el comando **addressipv4(dirección_ip)auth-port(numero_puerto)acct-port (numero_puerto),** se agrega la contraseña con **key (contraseña),** por último se solicita la autenticación para verificar a los usuarios antes de permitirles acceso a la red, esto se habilita con el comando **aaa authentication login default group radius local.**

Configuración R1

```
R1# aaa new-model
R1# radius server RADIUS
R1# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1#  key $trongPass
R1# exit
R1# aaa authentication login default group radius local
R1# end
R1# copy running-config startup-config
```

Configuración R3

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

Configuración D1

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

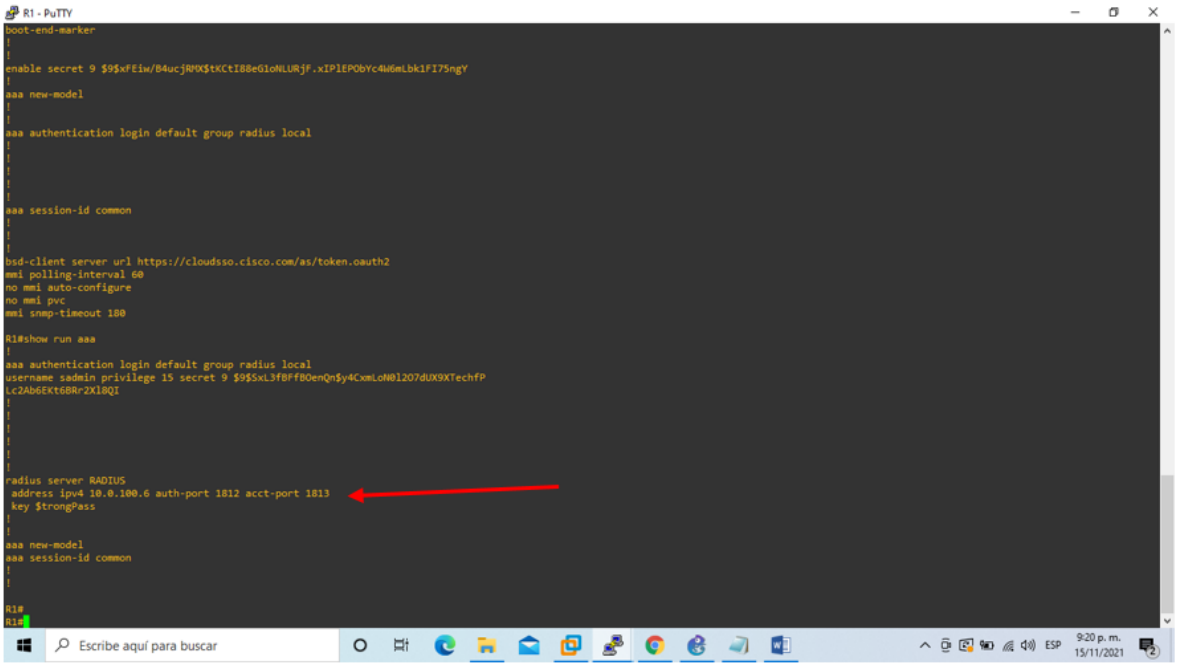
Configuración D2

```
D2# aaa new-model
D2# radius server RADIUS
D2# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2#  key $trongPass
D2# exit
D2# aaa authentication login default group radius local
D2# end
D2# copy running-config startup-config
```

Configuración A1

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

Figura 45. Verificación de servidor RADIUS en R1.



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

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

Tabla 6. Tareas de configuración parte 6

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Únicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

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

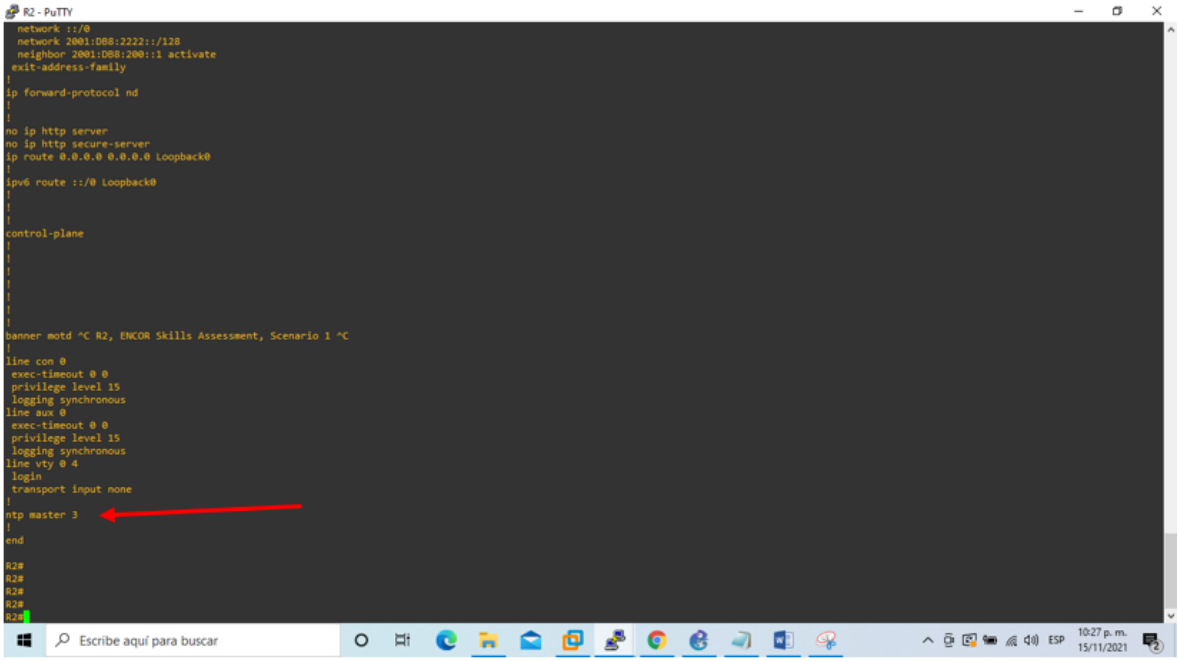
6.2. Configure R2 como un NTP maestro, Configurar R2 como NTP maestro en el nivel de estrato 3.

En este paso para ingresar al modo EXEC privilegiado los dispositivos van a solicitar nombre y contraseña, para la configuración del Router R2 como un NTP maestro se utiliza el comando **ntp master 3.**

Configuración R2

R2# enable and enter password
R2# ntp master 3
R2# end
R2# copy running-config startup-config

Figura 46. Verificando NTP maestro en R2.



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

Para configura NTP (Red Time Protocol) en estos dispositivos se usa el comando **ntp server (dirección_ip).**

6.4 Configure Syslog en todos los dispositivos excepto R2.

Syslog es un protocolo de registro que compila información de registros para control y resolución de problemas, tiene la capacidad de especificar los destinos de los mensajes Syslog capturados, los mensajes de Syslog tienen un nivel de gravedad en este punto se configuraran para que lleguen al PC1 mensajes con advertencias de gravedad error, crítico y emergencia para ello se utiliza el siguiente comando **logging trap warning,** luego el comando **logging host(ip_destino)**

Configuración de R1

R1# enable name and enter password
R1#ntp server 2.2.2.2
R1# logging trap warning
R1# logging host 10.0.100.5
R1# logging on

Configuración de R3

R3# enable name and enter password
R3#ntp server 10.0.10.1
R3# logging trap warning
R3# logging host 10.0.100.5
R3# logging on

Configuración de D1

D1# enable name and enter password
D1# ntp server 10.0.10.1
D1# logging trap warning
D1# logging host 10.0.100.5
D1# logging on

Configuración de D2

D2# enable name and enter password
D2# ntp server 10.0.11.1
D2# logging trap warning
D2#logging host 10.0.100.5
D2# logging on

Configuración de A1

A1# enable name and enter password
A1# ntp server 10.0.10.1
A1# logging trap warning
A1# logging host 10.0.100.5
A1# logging on

Se verifica configuración de hora en los dispositivos con el comando **show clock** como se muestra en la siguiente figura

Figura 47. Verificando configuración de hora en dispositivos.

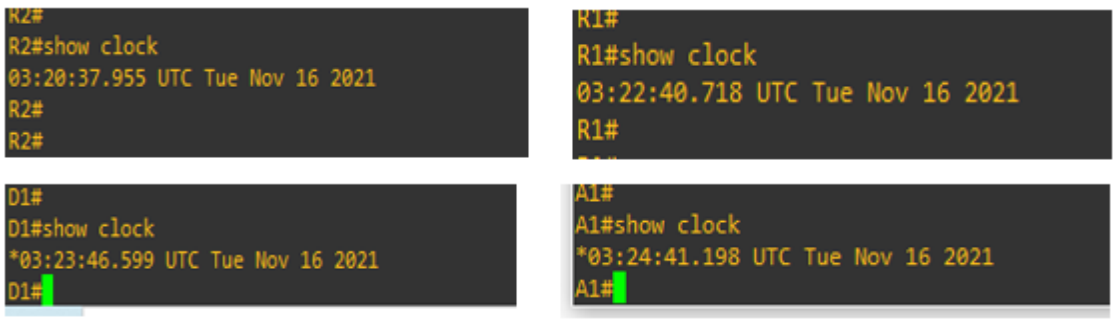


Figura 48. Verificando configuración de NTP status en R1.

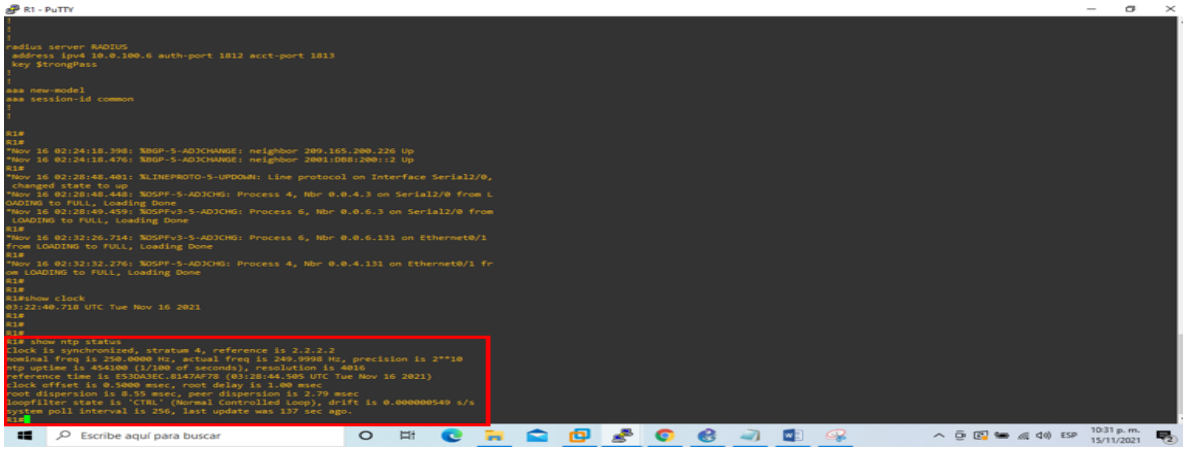
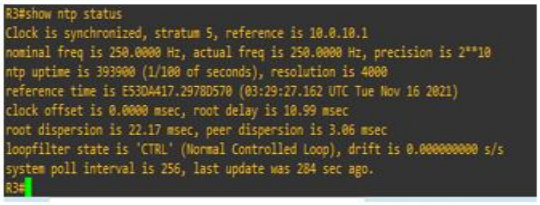
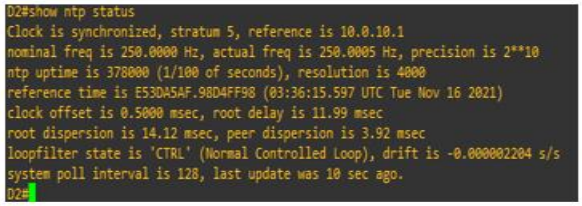
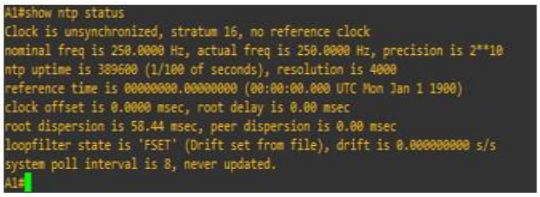
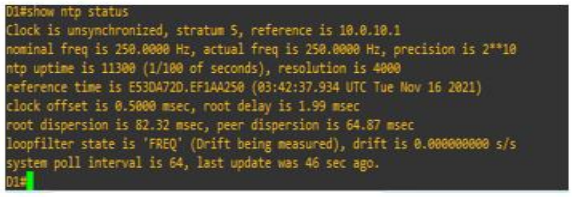


Figura 49. Verificando configuración de NTP status en R3, D2, A1, D1.









Ahora se verificara la configuracion de Syslog del paso 6.3 en todos los dispossitivos excluyendo a R2, con el comando **show run** y revisando hasta la parte donde este logging.

Figura 50. Verificando configuración de logging en R3 y R1.

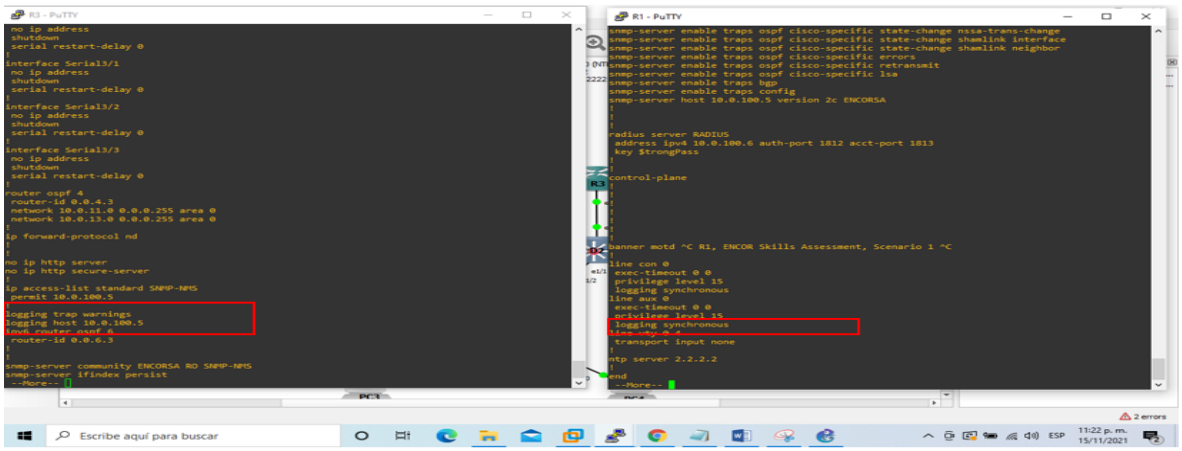
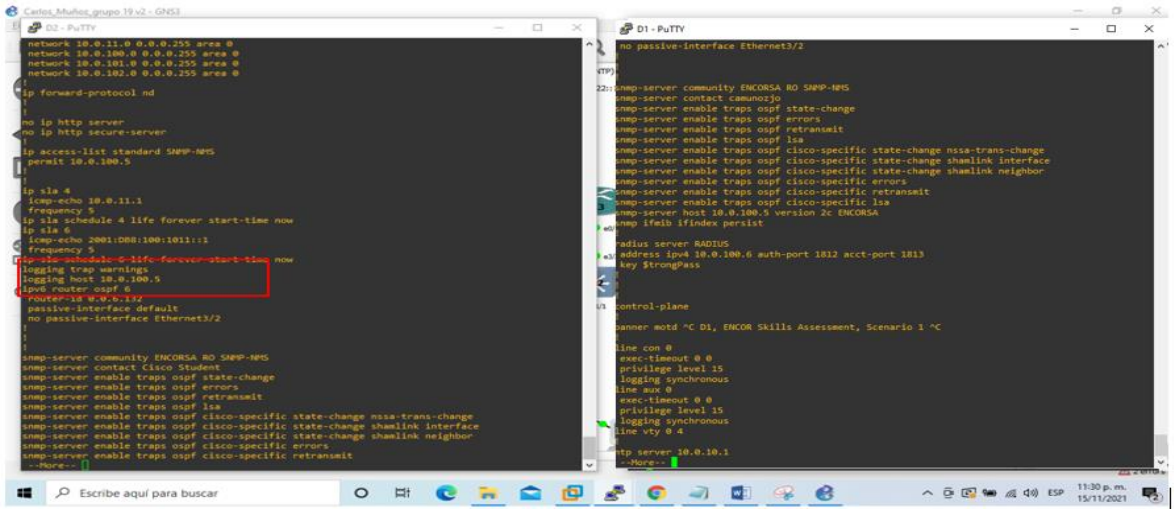


Figura 51. Verificando configuración de logging en D1 y D2.



6.5 Configure SNMPv2c en todos los dispositivos excepto R2.

El protocolo Simple de administración de red de la capa de aplicación facilita el intercambio de información de administración entre dispositivos de la red, y utiliza UDP como protocolo de capa de transporte a continuación se muestra códigos de configuración en los dispositivos de la red.

Configuración de R1

R1# enable name and enter password
R1#ip access-list standard SNMP-NMS
R1# permit host 10.0.100.5
R1# exit
R1# snmp-server contact camunozjo
R1# snmp-server community ENCORSA ro SNMP-NMS
R1# snmp-server host 10.0.100.5 version 2c ENCORSA
R1# snmp-server ifindex persist
R1# snmp-server enable traps bgp
R1# snmp-server enable traps config
R1# snmp-server enable traps ospf
R1# end
R1#copy running-config startup-config

Configuración de R3

R3# enable name and enter password
R3#ip access-list standard SNMP-NMS
R3# permit host 10.0.100.5
R3# exit
R3# snmp-server contact camunozjo
R3# snmp-server community ENCORSA ro SNMP-NMS

R3# snmp-server host 10.0.100.5 version 2c ENCORSA
R3# snmp-server ifindex persist
R3# snmp-server enable traps config
R3# snmp-server enable traps ospf

R3# end
R3# copy running-config startup-config

Configuración de D1

D1# enable name and enter password
D1# ip access-list standard SNMP-NMS
D1# permit host 10.0.100.5
D1# exit
D1# snmp-server contact camunozjo
D1# snmp-server community ENCORSA ro SNMP-NMS
D1# snmp-server host 10.0.100.5 version 2c ENCORSA
D1# snmp-server ifindex persist
D1# snmp-server enable traps config
D1# snmp-server enable traps ospf
D1# end
D1# copy running-config startup-config

Configuración de D2

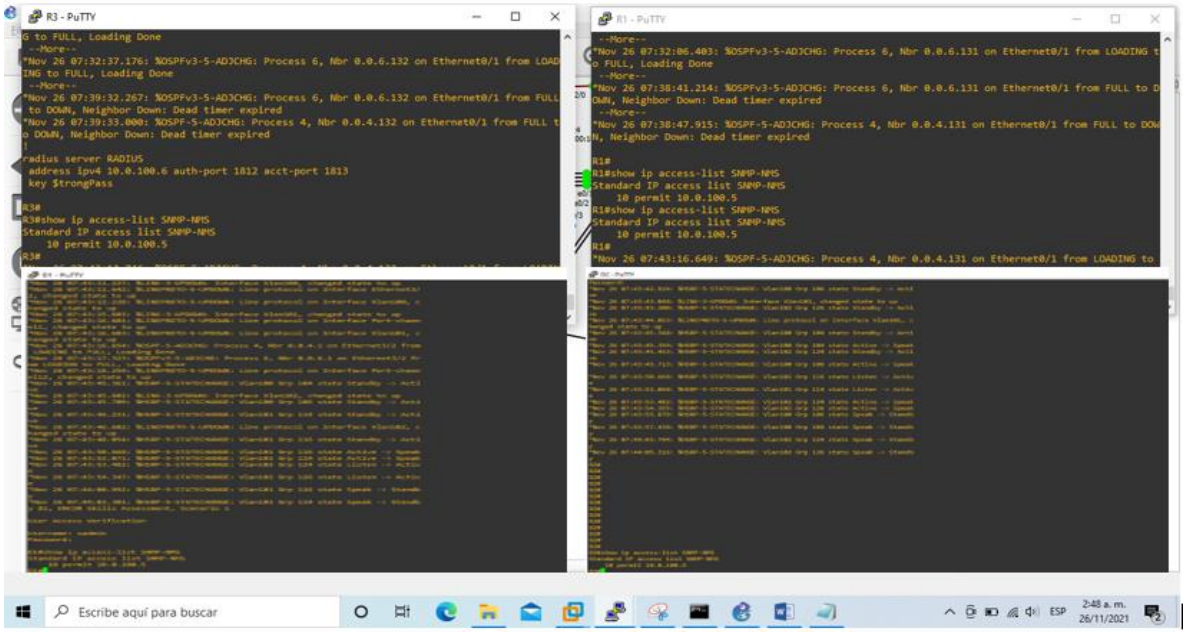
D2# enable name and enter password
D2#ip access-list standard SNMP-NMS
D2# permit host 10.0.100.5
D2# exit
D2# snmp-server contact camunozjo
D2# snmp-server community ENCORSA ro SNMP-NMS
D2# snmp-server host 10.0.100.5 version 2c ENCORSA
D2# snmp-server ifindex persist
D2# snmp-server enable traps config
D2# snmp-server enable traps ospf
D2#end
D2#copy running-config startup-config

Configuración de A1

A1# enable name and enter password
A1# ip access-list standard SNMP-NMS
A1# permit host 10.0.100.5
A1# exit
A1# snmp-server contact camunozjo
A1# snmp-server community ENCORSA ro SNMP-NMS
A1# snmp-server host 10.0.100.5 version 2c ENCORSA
A1# snmp-server ifindex persist
A1# snmp-server enable traps config
A1# snmp-server enable traps ospf
A1#end
A1#copy running-config startup-config

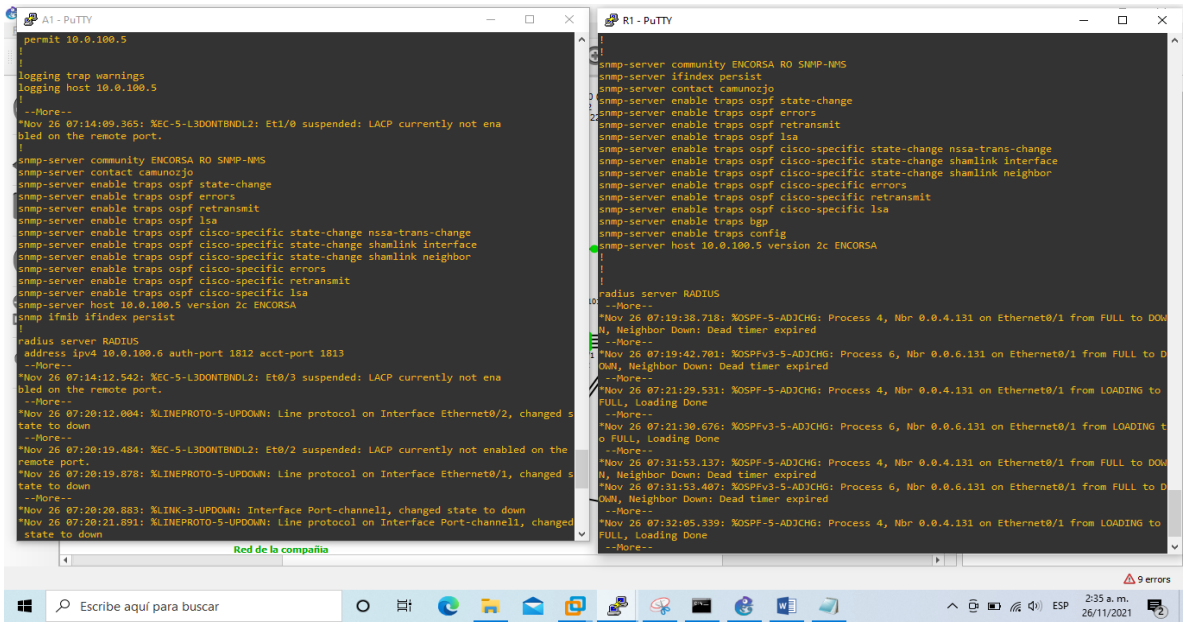
Se verifica configuración de dispositivos con el comando **show ip access-list SNMP-NMS** como se muestra en la siguiente imagen.

Figura 52. Verificando configuración D1, D2, R3 y R1.



Utilizando el comando show run hasta encontrar la configuración de las configuraciones de SNMPv2 en los dispositivos configurados encontramos lo siguiente:

Figura 53. Verificando configuración A1 y R1.



CONCLUSIONES

En el desarrollo de este escenario se construyó una topología en la aplicación de GNS3 y la máquina virtual VMware Workstation pro, que cuenta con tres redes las cuales deben conectarse satisfactoriamente, para poder recibir y enviar mensajes de un extremo a otro, para ello fue necesario la configuración de los Routers, la aplicación de Switch, PCs que se pudieran programar según los requerimientos solicitados, en la primera parte se configurara la capa 2 la cual se encarga del direccionamiento físico de los datos y detección de errores en la transmisión.

Se pudo conocer y configurar enlaces troncales con el estándar IEEE 802.1Q, este estándar es el que permite que las tramas viajen por la red con una etiqueta, ya que estos son de gran importancia para poder tener un buen desempeño en la red puesto que su principal función es facilitar la comunicación entre las distintas VLAN, y como en este escenario hay varias se hace importante su aplicación, además se observó que es muy útil cuando hay switches instalados en la red.

En una red como la que se planteo es muy importante el protocolo de comunicación, en este escenario se utilizó y conoció el protocolo OSPF (Open Shortest parth Firts), este es un protocolo que va a mantener un mapa de la topología de la red lo cual va a hacer que seleccione caminos más cortos, también está diseñado para aceptar crecimientos de la red, cambios en la red de la topología y encaminamiento según el tipo de servicio, además también acepta protocolos TCP/IP, como este escenario es de una red de una compañía es ideal para su uso y aplicación.

GRE puede encapsular gran variedad de paquetes de protocolos de túneles IP, esto crea un enlace punto apunto virtual a los Router, también administra el transporte de trafico multiprotocolo y de multidifusión IP entre distintos sitios lo que quiere decir que permite transportar paquetes de una red a través de otra red diferente.

Aunque la configuración de la hora y la fecha no son realmente necesarios en los dispositivos de la red para que realicen sus funciones correctamente, esta se debe configurar para poder tener información real en los archivos log y los mensajes debug, ya que ahí aparecerá la hora y la fecha correcta ayudando al programador a tener registros del tiempo real y de las fallas presentadas, también se puede observar la fecha y hora real cuando ingresan a cualquier dispositivo de la red.

La ciberseguridad en una red es un factor importante por ello la configuración del algoritmo Syslog en este escenario es fundamental, ya que activa un esquema de monitorización de infraestructura de la red, el cual nos va permitir conocer eventos internos que se presenten en los dispositivos y/o servicios, para así poder garantizar la calidad y continuidad de un buen nivel de servicio.

BIBLIOGRAFÍA

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

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!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. 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). IP Services. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Understanding Wireless Roaming and Location Services. CCNP and CCIE Enterprise Core ENCOR 350-401.https://1drv.ms/b/s!AAIGg5JUgUBthk8

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