DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NESTOR ARCANGEL ESPINEL SALAMANCA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
SOGAMOSO – BOYACA
2021

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NESTOR ARCANGEL ESPINELSALAMANCA

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

DIRECTOR:
MSc. GERARDO GRANADOS
ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
SOGAMOSO – BOYACA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

SOGAMOSO – BOYACA, 29 de noviembre de 2021

AGRADECIMIENTOS

Después de lo que aparentemente ha sido un largo camino desde que inicie el tecnólogo y con la meta de terminar la profesión en un doctorado estamos en un camino en el cual nos está llevando un poco más cerca de la meta planteada. Hay mucho que agradecer y a muchas personas que han contribuid a la formación constante y los cuales siempre han estado motivándome en los momentos de más incertidumbre, esto no sería posible primero sin la ayuda de Dios y segundo por la perseverancia de mi madre que siempre me ha impulsado a ser mejor, con el ardu-esfuerzo de ser constante y diciplinado en todos los entornos de mi vida o cual me ha dado muchos frutos, también tengo que dar un agradecimiento especial a mis hermanos que siempre me han dado ese apoyo motivacional para sobresalir con excelencia durante toda mi formación como ingeniero , hay muchos más los cuales les debo las gracias por estar en momentos cruciales en los cuales dieron un aporte significativo para mi formación gracias a todos.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Protocolo OSPF: Conocido como protocolo de direccionamiento de estado-enlace, está basado en algoritmo de vía corta como “SPF”, permite mantener una base de datos enlace-estado similar a la topología que estámanejando en el área, mediante anuncios que son recibidos y transmitidos por otros dispositivos del área.

Protocolo OSPFv2, OSPFv3: el protocolo OSPFv3 permite que las direcciones ipv6 sean distribuidas con el prefijo de estas, una de sus desventajas es que no cuenta con un soporte para direcciones ipv4, es por ello que si se desea incluir direcciones ipv4 se debe aplicar OSPFv2, esto no implica que sean diferentes ya que los dos cuentan con el mismo algoritmo, presentando el mismo número de paquetes, y los mismos mecanismos para encontrar dispositivos cercanos o vecinos para generar adyacencias entre ellos.

Protocolo BGP: considerado como un protocolo escalable de ruta dinámica, permitiendo la comunicación y compartir información de enrutamiento con el fin de la creación de rutas estables con la ventaja de generar múltiples posibilidades para la divulgación de su red a internet aumentando de manera significativa su tiempo de actividad

Protocolo spanning tree: es un protocolo de expansión de árbol el cual cumple con la función de un controlpermanente de los bucles que son producidos en una red de capa 2, gracias a que controla los excesos de enlaces que usualmente afectan el rendimiento de las redes.

Arquitectura empresarial de redes: es un modelo aplicado ala solución de la jerarquía en una red o infraestructura, permitiendo una mejora en el desarrollo de diseños de redes más densas y escalables, mediante una segmentación de áreas, los cuales se les denomina módulos, permitiendo de esta manera una mejor flexibilidad a la hora de manejo e implementación de redes facilitando de manera considerable la solución de problemas.

RESUMEN

En el presente trabajo se trabajará una topología de CISCO CCNP aplicando el uso de software de GNS3 y las distintas tecnologías Switching para lo cual se desarrollarán las diversas actividades planteadas, desde a configuración inicial de las interfaces y abordando la aplicación el Routing o enrutamiento troncal IEEE 802.1Q, en la utilización de configure single-área OSPFv2, usando el OSPF para a asignación de las ID de losdispositivos que estarán en las “Networking” a trabajar, también se realizarán la configuración de una red ISP, configurando las relaciones de vecino, configurando MP- BGP. También se relacionan las configuraciones IP SLAs, para probar la accesibilidad con más dispositivos, con HSRPv2 configuramos los routers primarios y le damos la prioridad y a cada uno de los dispositivos son anexados a grupos específicos, sin menos preciar los diferentes mecanismos de seguridad, buscando como finalidad garantizar la seguridad de incursiones no deseadas. En cada una de las configuraciones realizadas se realizan pruebas de comprobación para evidenciar la correcta configuración de los dispositivos según lo planteado por la guía y la cual se evidenciará el desarrollo por parte del aprendiz en el diseño de redes y programación las cuales serán de mucha utilidad en entornos y aplicación ya sea en el entorno de las redes de comunicaciones, enfoque de la electrónica o en programación de dispositivos electrónicos que tengan relación con este tipo de topologías.

ABSTRACT

In this work, a CISCO CCNP topology will be worked on applying the use of GNS3 software and the different Switching technologies, for which the various activities proposed will be developed, from the initial configuration of the interfaces and addressing the application of IEEE Routing or trunk routing. 802.1Q, in the use of configure single-area OSPFv2, using OSPF to assign the IDs of the devices that will be in the “Networking” to work, the configuration of an ISP network will also be carried out, configuring the neighbor relationships, configuring MP-BGP. The IP SLAs configurations are also related, to test accessibility with more devices, with HSRPv2 we configure the primary routers and give priority and each of the devices are attached to specific groups, without least appreciating the different security

mechanisms, looking for how purpose to ensure safety from unwanted incursions. In each of the configurations carried out, verification tests are carried out to demonstrate the correct configuration of the devices as proposed by the guide and which will show the development by the learner in the design of networks and programming, which will be very useful in environments and application either in the environment of communications networks, focus on electronics or programming of electronic devices that are related to this type of topologies

INTRODUCCIÓN

El propósito de este diplomado está enfocado en presentar un escenario el cual le representará un reto al estudiante y el cual le permitirá tener un acercamiento a una problemática real, la cual presenta varios entornos de diferentes métodos de programación en lo que respecta a protocolos de enrutamiento, los distintos tipos de seguridad para garantizar que no haya ingresos no deseados.

Uno de los propósitos más significativos de este diplomado es poder desarrollar una topología la cual realice envíos de mensajes y comunicación sin saturación de mensajes y de envió innecesarios que permita garantizar el correcto funcionamiento de la red reduciendo al máximo el reenvió de mensajes innecesarios y haciendo seguimiento de alertas en los mensajes ya sea por perdida de comunicación o por eventos relacionados con la configuración, en busca de una organización del sistema permitiendo tener la jerarquía necesaria para lograr un funcionamiento sostenible gracias a la aplicación de los diferentes protocolos.

Cabe destacar que uno de los muchos propósitos de este diplomado es la realización de la configuración de distintas redes las cuales permitan realizar distintas funciones y que de las mismas no representen un conflicto para interactuar con otras esto buscando características muy específicas almomento de realizar tareas precisas, tales como HSRPv2 el cual nos permitirá tener e cierta manera una segmentación entre los routers determinar cuál de estos es primario y darle estados de prioridad, a su Vez segmentarlos en grupos según sea las interfaces Vlans configuradas.

Para dar una introducción más afondo a lo ya mencionado en el abstracto donde mencionamos la configuración de las interfaces en cada uno de los dispositivos y las cuales cada uno maneja ciertos atributos los cuales se descaran a medida que se vaya desarrollando la actividad como por ejemplo, la aplicación el enrutamiento

troncal IEEE 802.1Q, el cual permite una segmentación de la red para la comunicación permitiendo el tráfico según se haya configurado los enlaces para la comunicación entre VLAN, permitiendo un enlace entre diferentes troncales, adicional a estos en la utilización de configuración de single-área OSPFv2, usando el OSPF, un protocolo aplicado para monitorear el estado de enlaces y de esta forma tener un mejor conocimiento respecto a fallos de enlace como de igual manera ver cambios en la topología, garantizando de manera rápida y precisa las rutas de algoritmo Dijkstra, y verificando la información suministrada por el routing OSPF. para a asignación de las ID de los dispositivos, también se realizarán la configuración de una red ISP, configurando las relaciones de vecino, configurando MP- BGP. también se relacionan las configuraciones IP SLAs, las cuales permiten el acceso a niveles para el seguimiento de servicios IP, garantizando el análisis de los niveles de servicios de aplicaciones, diciéndolo en otras palabras permitirel monitoreo de la red de una manera más confiable y rápida, también se trabajará con varios mecanismos de seguridad esto para evitar intrusiones no deseadas y de esta manera garantizar la protección de los datos que transitan en la red, probando los distintos niveles de seguridad y de privilegio para dar mejor seguridad a la hora de realizar envíos de mensajes.

TOPOLOGIA DE LA RED

Figura 1. Escenario 1

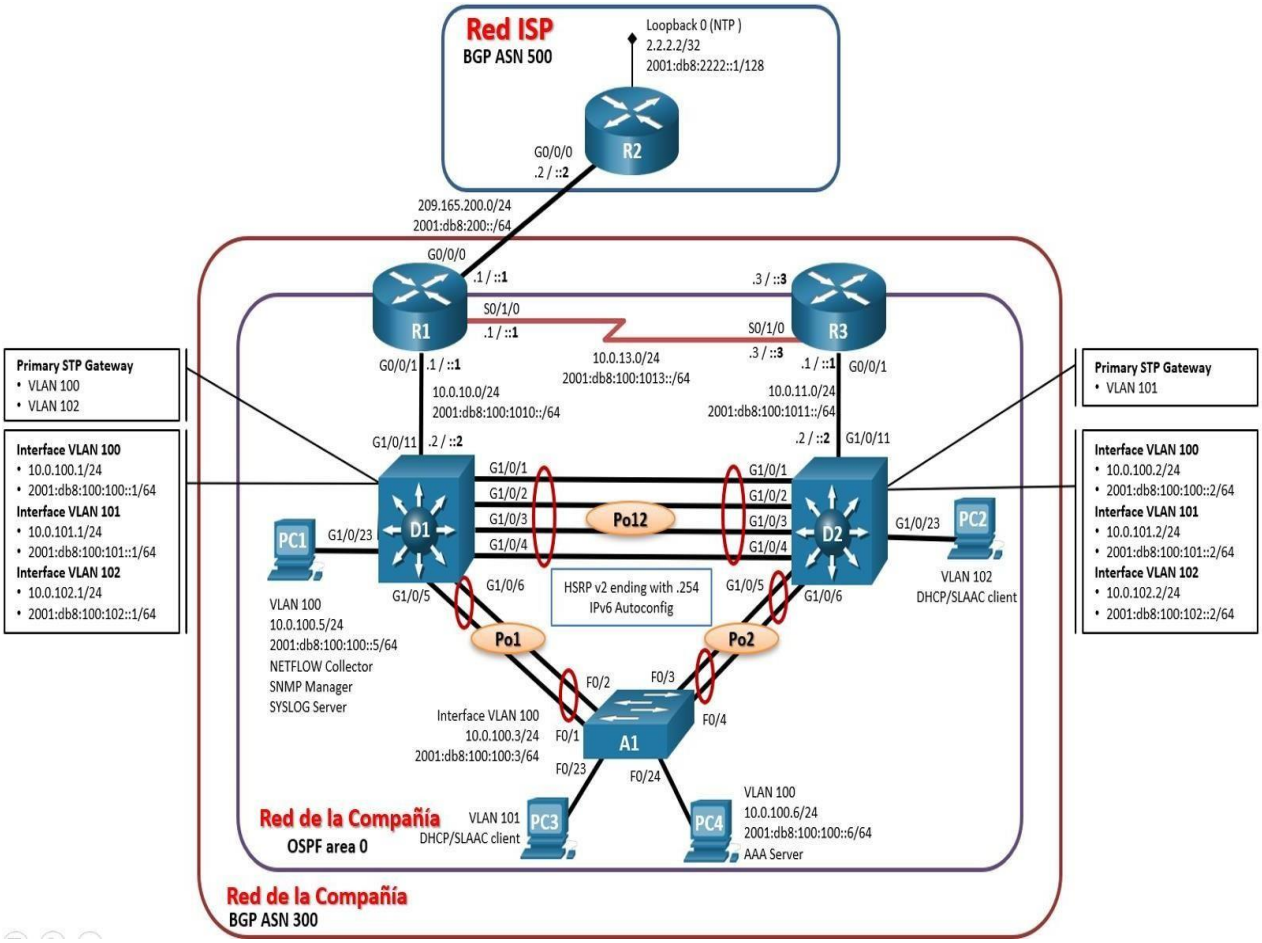


Tabla 1. ***Direccionamiento***

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

Escenario

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 Compañia**" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.
Nota: Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE versión 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS versión 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.
Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.
Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global **sdm prefer dual-ipv4-and-ipv6 default**. Cambiar la plantilla requerirá el reinicio del switch.

8.1. Recursos necesarios

3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

2 switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

1 switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)

4 PCs (utilice el programa de emulación de terminal)

Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola

Los cables Ethernet y seriales van como se muestra en la topología

8.2. 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.

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

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

Router R1

```
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 g0/0/0
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 g0/0/1
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 s0/1/0
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 // para guardar la configuración hecha

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 g0/0/0
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 // para guardar la configuración hecha

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 g0/0/1
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 s0/1/0
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 // para guardar la configuración hecha

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 g1/0/11 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 g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit

Switch D2

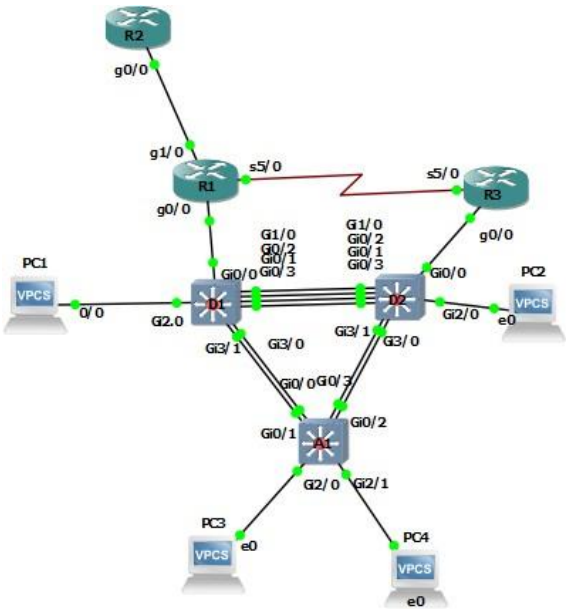
hostname D2 ip routing
ipv6 unicast-routing no ip domain lookup

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 g1/0/11 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 g1/0/1-10, g1/0/12-24, g1/1/1-4 shutdown
exit

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 f0/5-22
shutdown
exit
```

Figura 2. Topología escenario 1 gns3



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

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

Figura 3. Configuración inicial switch D1

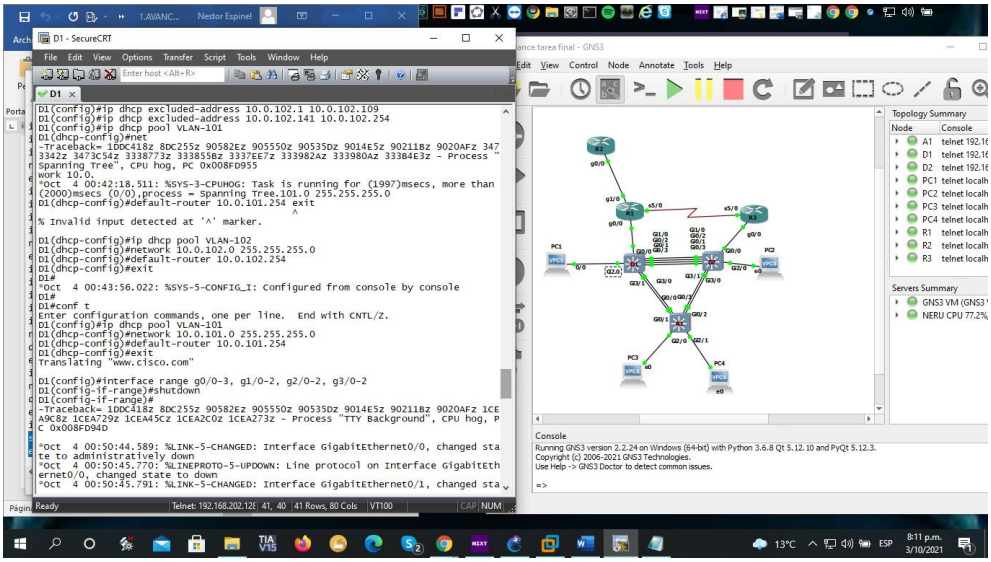


Figura 4. Configuración inicial switch D2

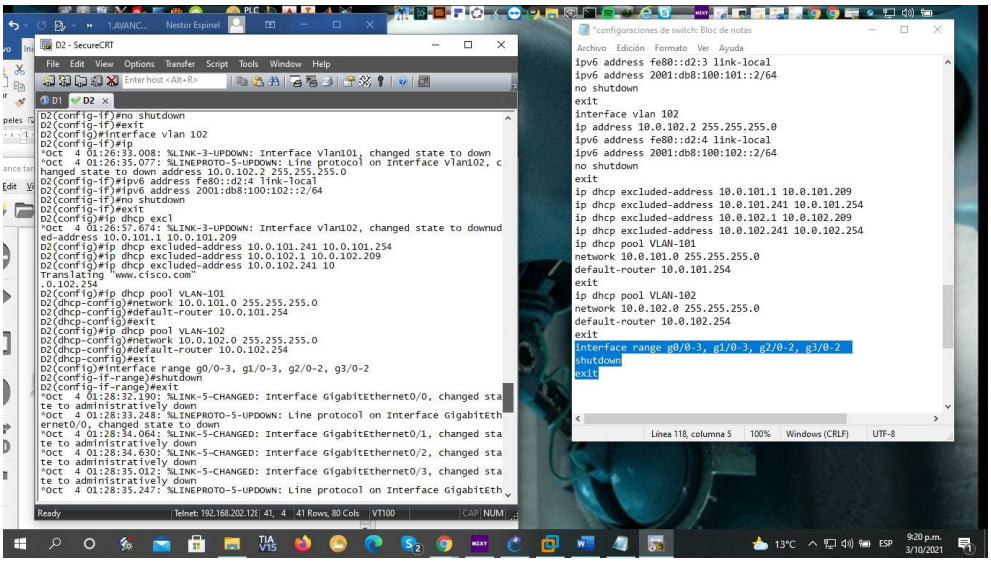


Figura 5. Configuración inicial switch A1

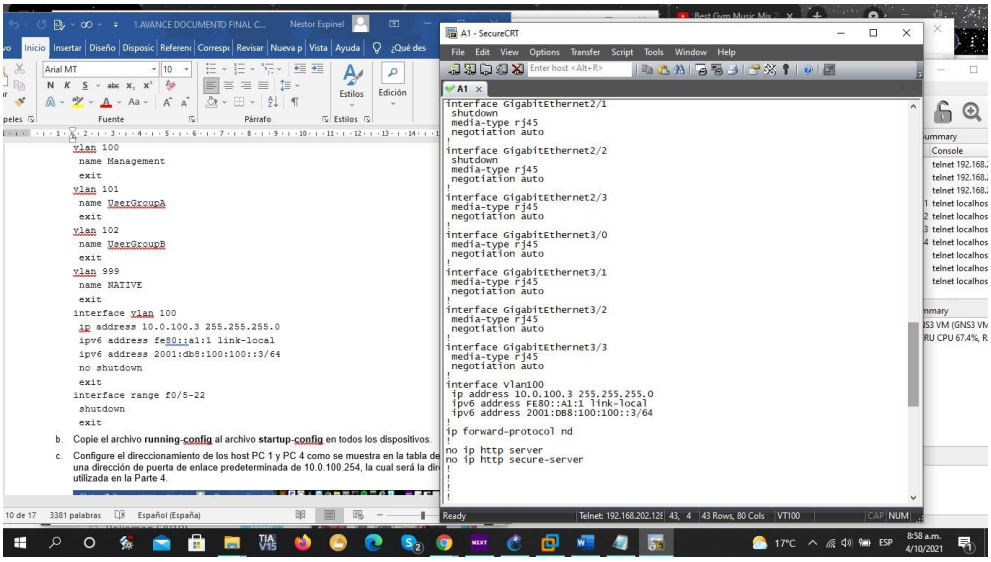


Figura 6. Comprobación dirección PC1

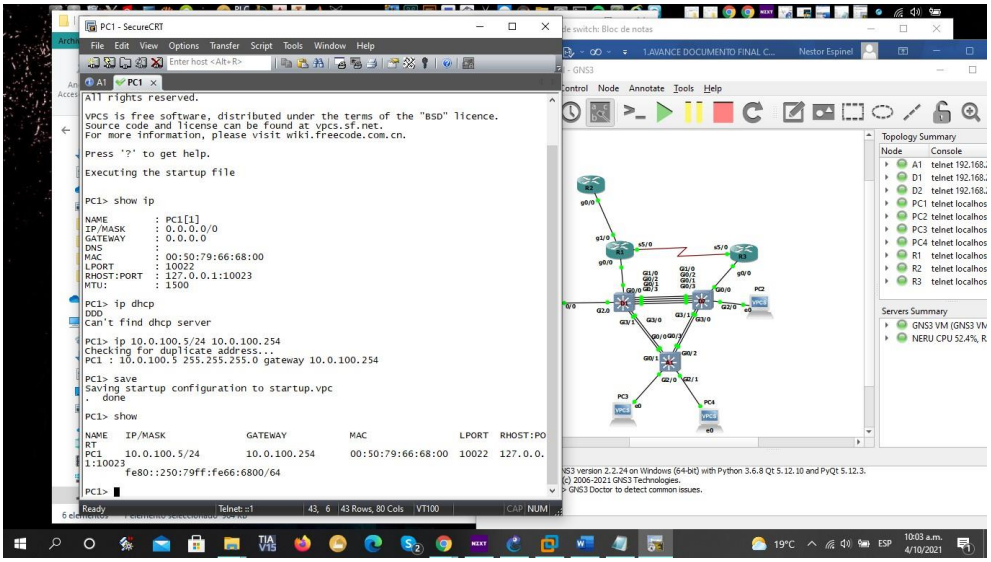
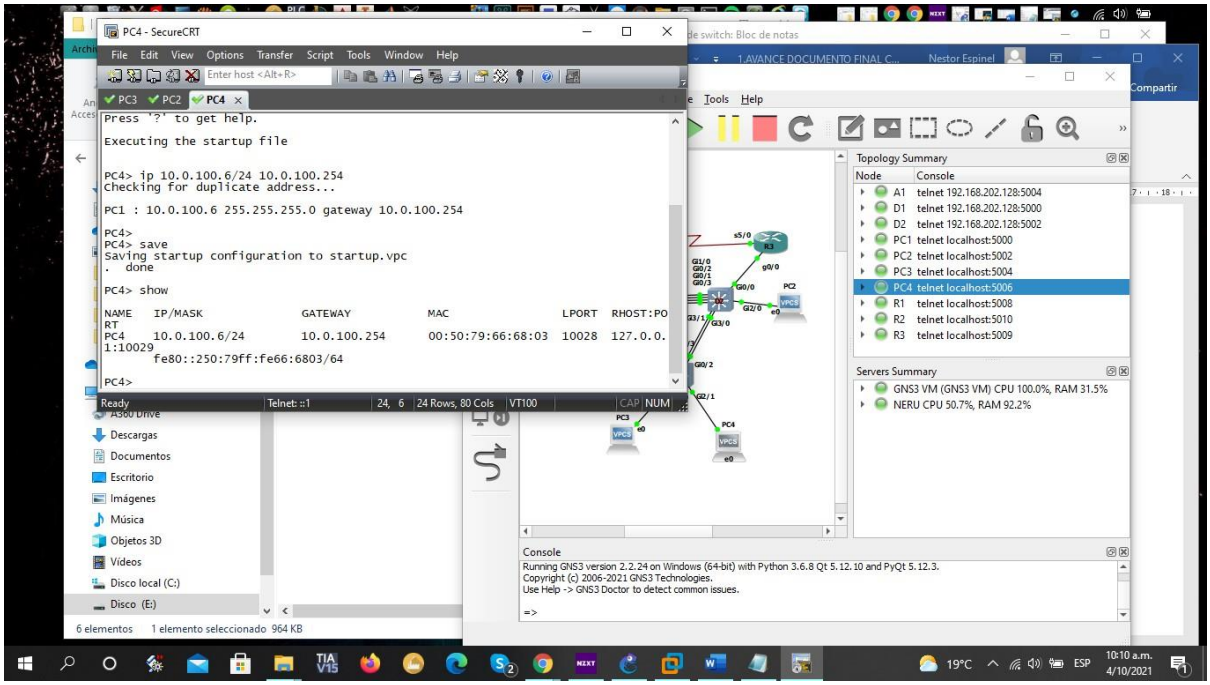


Figura 7. Comprobación dirección PC4



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

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

Tabla 2. Configuración interfaces troncales IEEE

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. Switchport trunk native vlan 999 End
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT). Revisar referencia

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

D1 (config)# Interface g0/1-6
Switchport trunk encaptulation dot1q
Switchport mode trunk
Lo anterior se repite para cada uno de los Switch dependiendo la interface

D1(config)#interface range g0/1-3, g1/0, g3/0-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#no shutdown

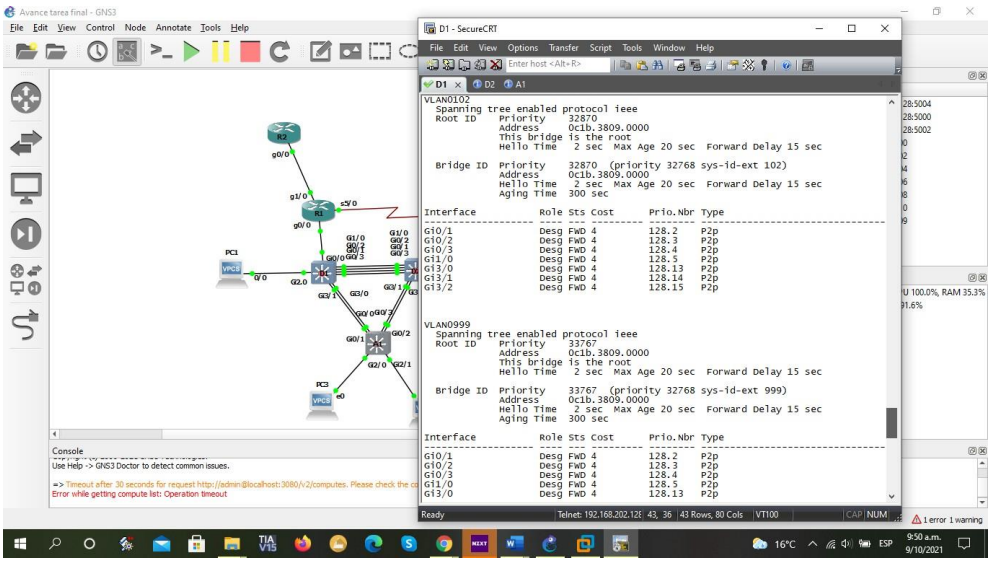
A1(config)#interface range g0/0-3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#no shutdown

D1 (config)# Interface range g0/1-3, g1/0, g3/0-2
D1 (config)# Switchport mode trunk
D1 (config)# Switchport trunk native vlan 999
End

D2 (config)# Interface range g0/1-3, g1/0, g3/0-2
D2 (config)# Switchport mode trunk
D2 (config)# Switchport trunk native vlan 999
D2 (config)#end

A1(config)#interface range g0/0-3
A1(config)#Switchport mode trunk
A1(config)#Switchport trunk native vlan 999
A1(config)#End

Figura 8. Comprobación del protocolo spannig tree y de troncales D1



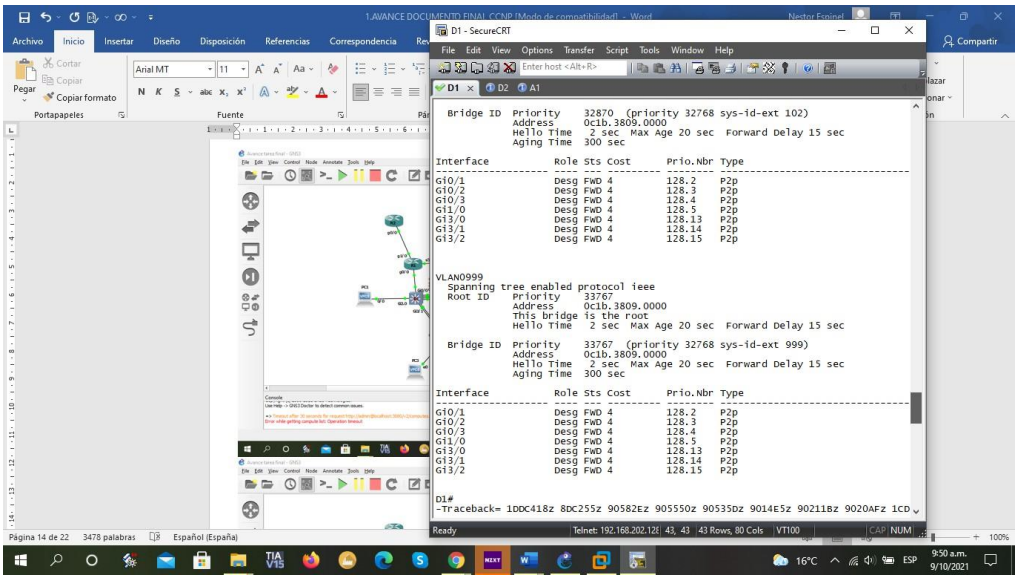


Figura 9. Comprobación del protocolo spannig tree y de troncales D2

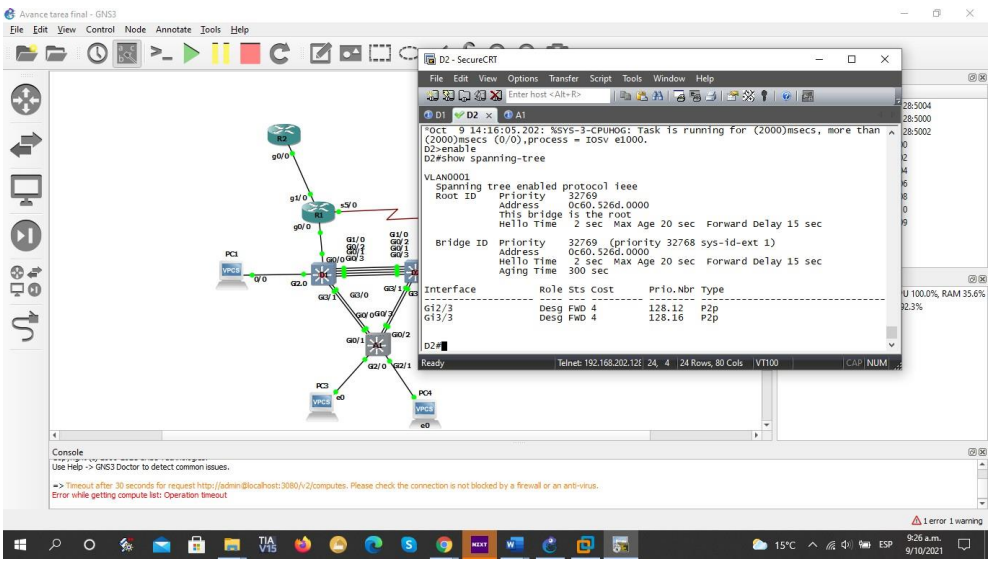


Figura 10. Comprobación del protocolo spannig tree y de troncales A1

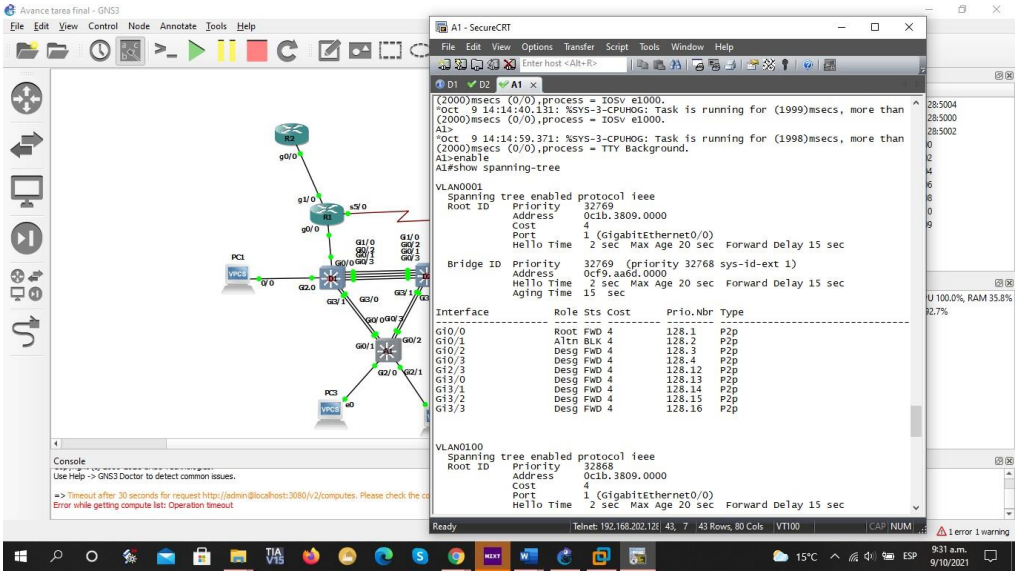


Figura 11. Comprobación del protocolo spannig tree y de troncales A1

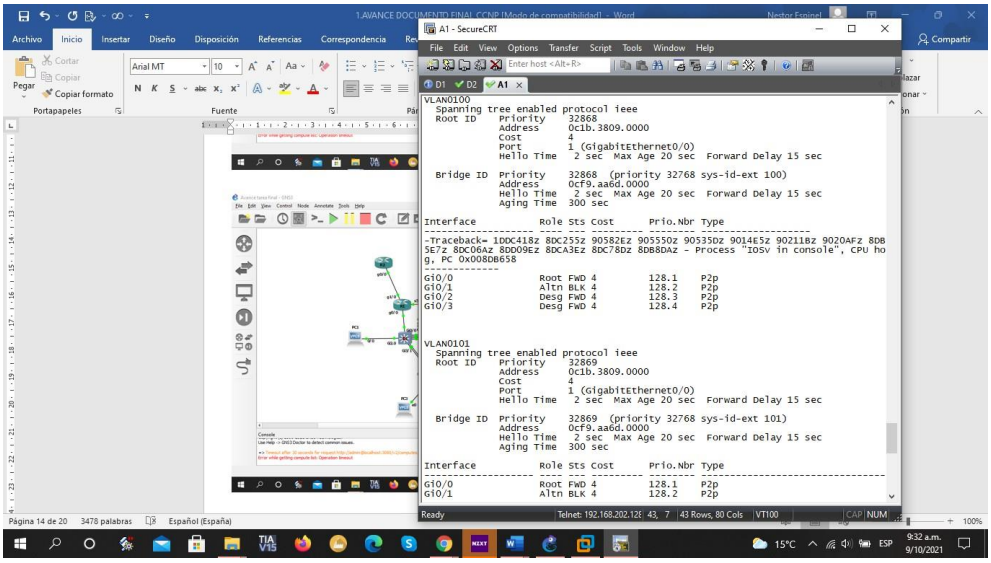


Figura 12. Comprobación del protocolo spannig tree y de troncales A1

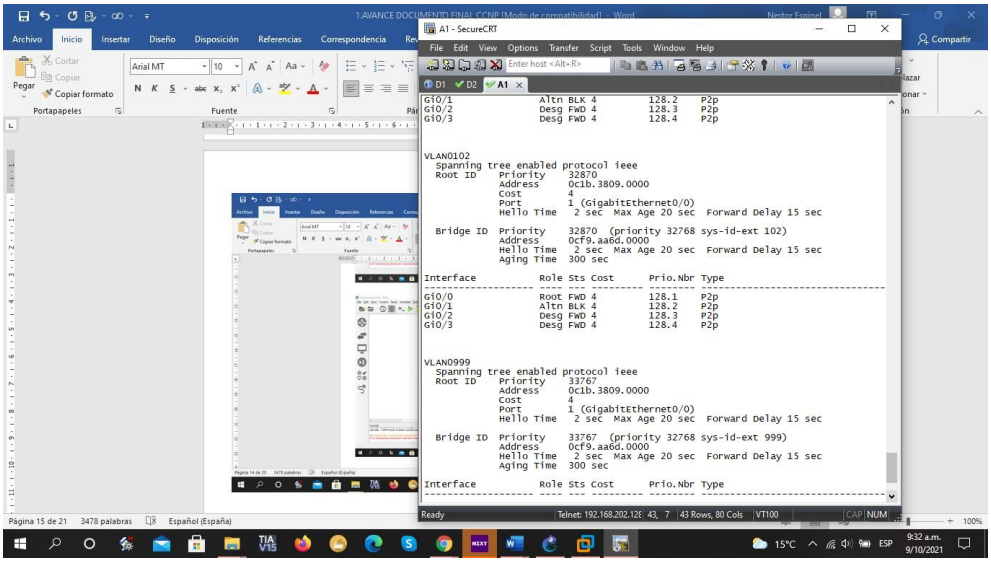


Figura 13. Comprobación del protocolo spannig tree y de troncales A1

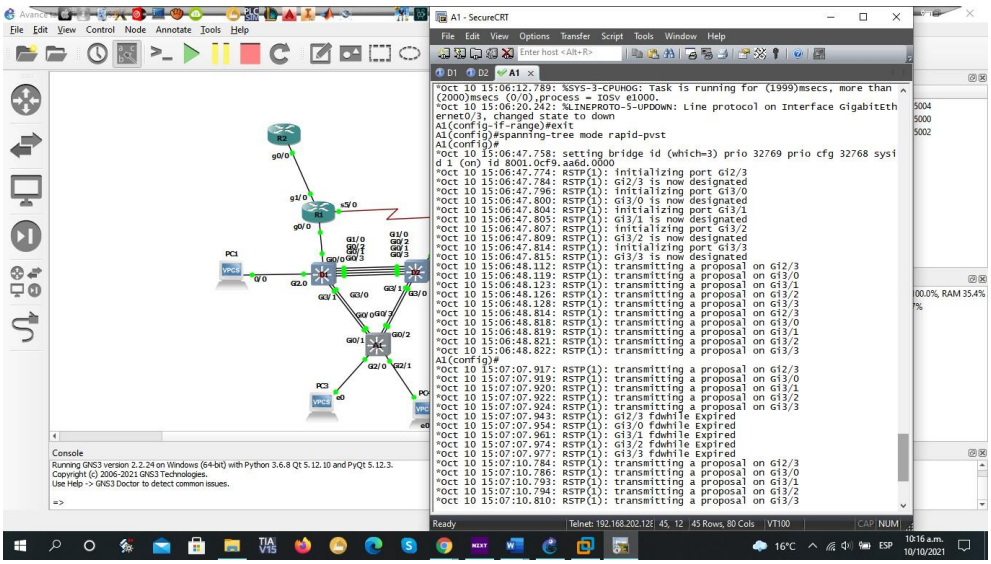


Figura 14. Comprobación del protocolo spannig tree y de troncales A1

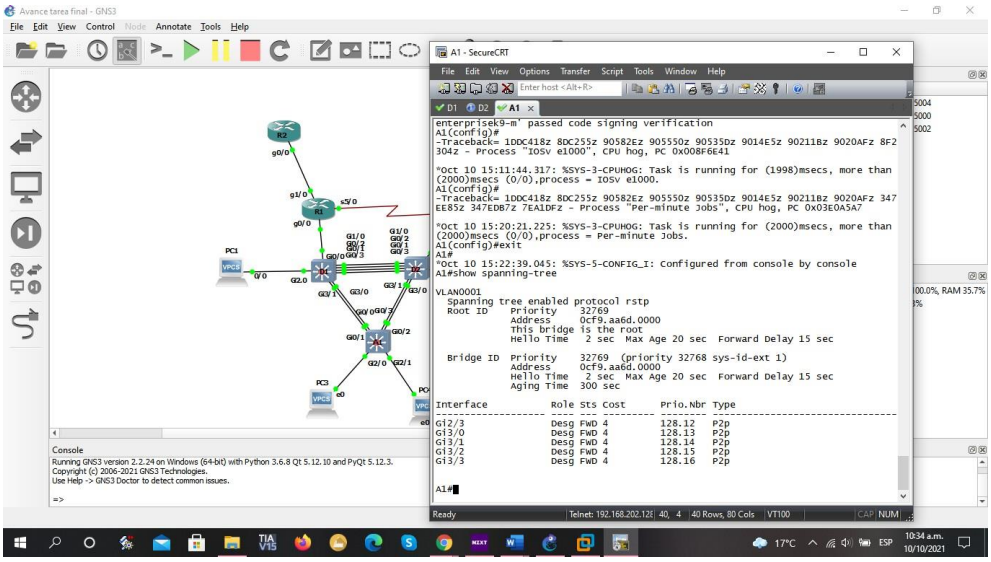


Tabla 3. Configuración RSTP, EtherChannels LACP, puertos de acceso del host

Tarea#	Tarea	Especificación
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

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

Habilitación del comando spaning-tree se puede realizar siguiendo los siguientes pasos

D1(config)#spanning-tree mode rapid-pvst
D1#show spanning-tree

D2(config)#spanning-tree mode rapid-pvst
D2#show spanning-tree

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

```
D1(config)#in range g1/0, g0/1-3
  D1(config-if-range)#Switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D1(config-if-range)#no shutdown

D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#in range g1/0, g0/1-3
D2(config-if-range)#Switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

D2(config-if-range)#no shutdown
D2(config-if-range)#end



D1#enable
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#in range g3/0-1
D1(config-if-range)#Switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

D1(config-if-range)#no shutdown
D1#end

A1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#in range g0/0-1
A1(config-if-range)#Switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

A1(config-if-range)#no shutdown
```

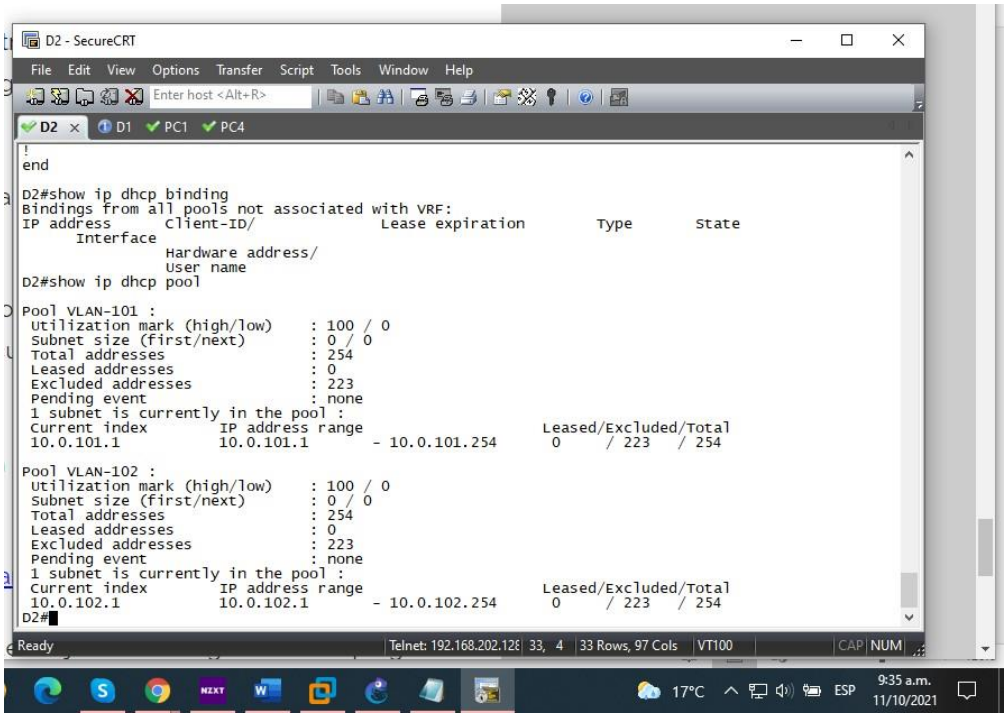
```
A1(config-if-range)#end


D2#enab
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#int range g3/0-1
D2(config-if-range)#Switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#no shutdown
D2#end

A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#int range g0/2-3
A1(config-if-range)#Switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
A1(config-if-range)#no shutdown
A1#end
```

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

```
D1(config)#int g2/0
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#no shutdown

D2(config)#int g2/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#no shutdown

A1(config)#int g2/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#end
```

A1(config)#int g2/1
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#end
Verifique los servicios DHCP IPv4.

Figura 15. Comprobación del DHCP en las interfaces de D2.



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 4. Configuración de protocolos de enrutamiento

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañia” (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 Área 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 Área 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

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

```
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#end
```

Se crea la ruta por defecto

```
R1(config)#interface s5/0
R1(config-if)#ip route 0.0.0.0 0.0.0.0 s5/0
```

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#exit
D1(config)#end
D1(config)#router ospf 4
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface e1/0
D1(config-router)#passive-interface e0/2
```

```
D1(config-router)#passive-interface e0/1
D1(config-router)#passive-interface e0/3
D1(config-router)#passive-interface e2/0
D1(config-router)#passive-interface e3/1
D1(config-router)#passive-interface e3/0

D1(config)#router ospf 4
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface e1/0
D1(config-router)#passive-interface e1/1
D1(config-router)#passive-interface e1/2
D1(config-router)#passive-interface e1/
*Oct 27 01:49:16.018: %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on Ethernet0/0 (not full duplex), with R1 GigabitEthernet0/0 (full
duplex).
D1(config-router)#passive-interface e1/3
D1(config-router)#passive-interface e2/1
D1(config-router)#passive-interface e3/0
D1(config-router)#passive-interface e3/1
D1(config-router)#
```

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config)#end
D2(config)#router ospf 4
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#passive-interface e1/0
D2(config-router)#passive-interface e0/2
D2(config-router)#passive-interface e0/1
D2(config-router)#passive-interface e0/3
D2(config-router)#passive-interface e2/0
D2(config-router)#passive-interface e3/1
D2(config-router)#passive-interface e3/0

D2(config-router)#passive-interface e1/0
D2(config-router)#passive-interface e1/1
```

```
D2(config-router)#passive-interface e1/2
D2(config-router)#passive-interface e1/
D2(config-router)#passive-interface e1/3
D2(config-router)#passive-interface e2/1
D2(config-router)#passive-interface e3/0
D2(config-router)#passive-interface e3/1

R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
```

Figura 16. Comprobación de la configuración de ospf D1

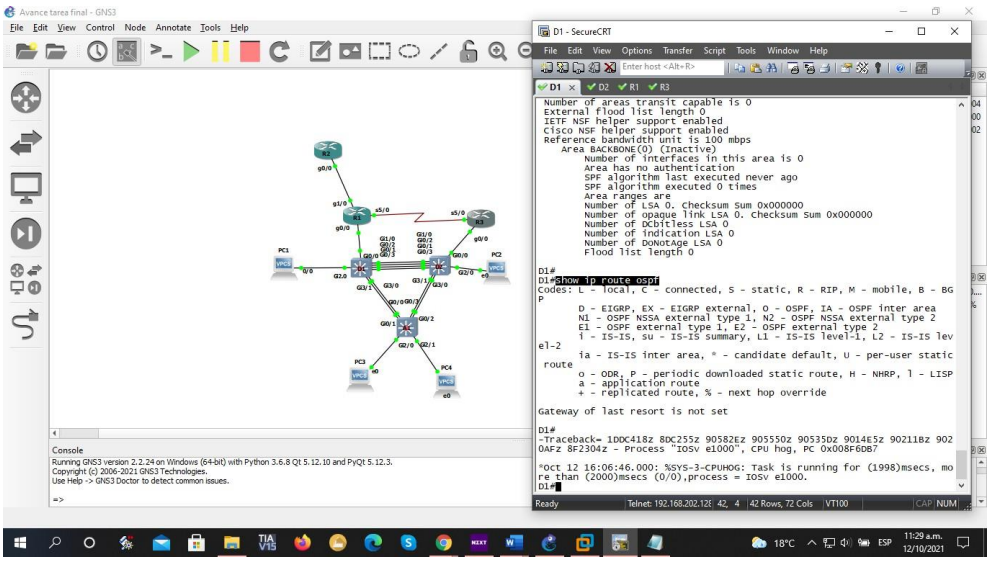


Figura 17. Comprobación de la configuración de ospf R1 comprobación protocolo ospf

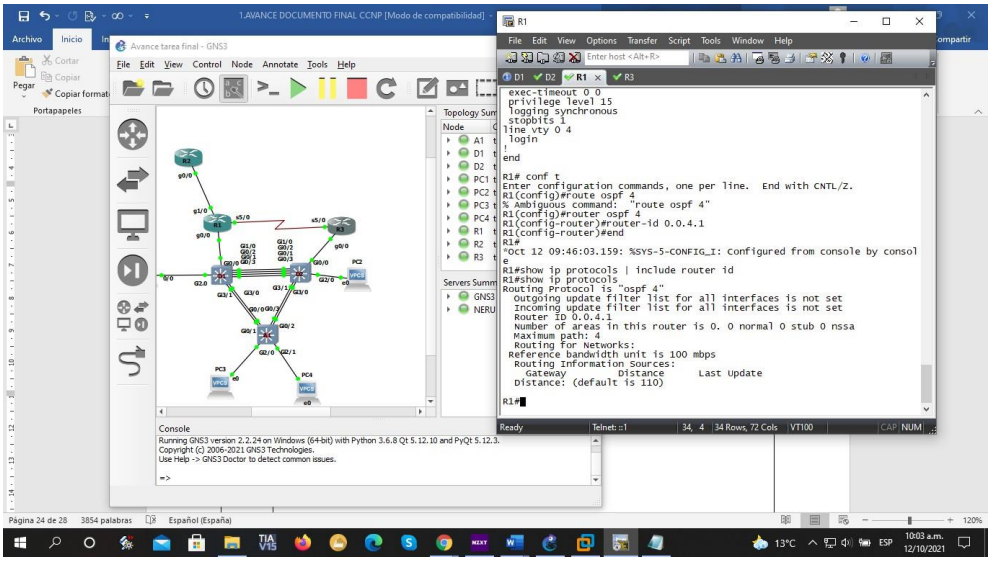


Figura 18. Comprobación de la configuración de ospf R3 comprobación protocolo ospf

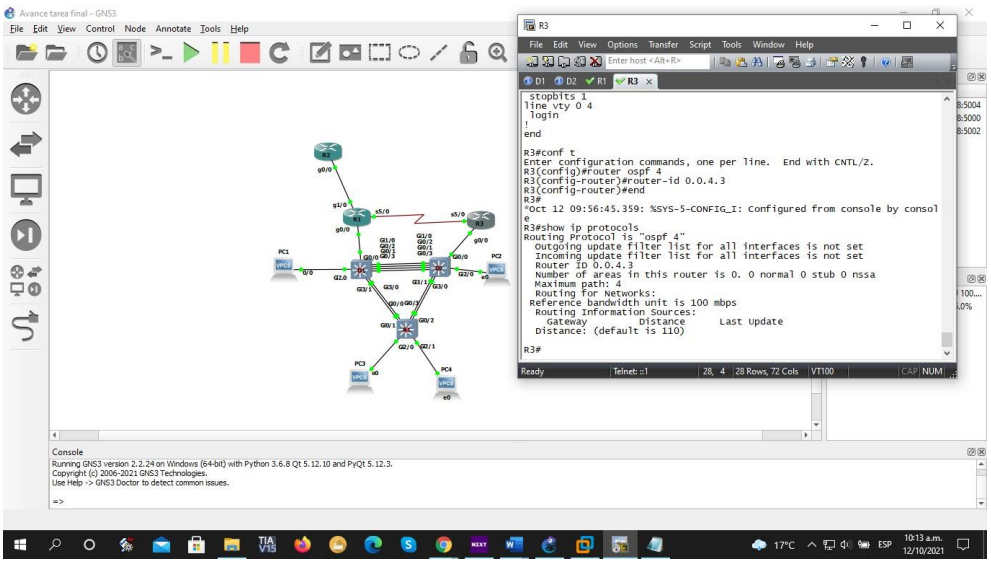


Figura 19. Comprobación de la configuración de ospf D1 comprobación protocolo ospf 4

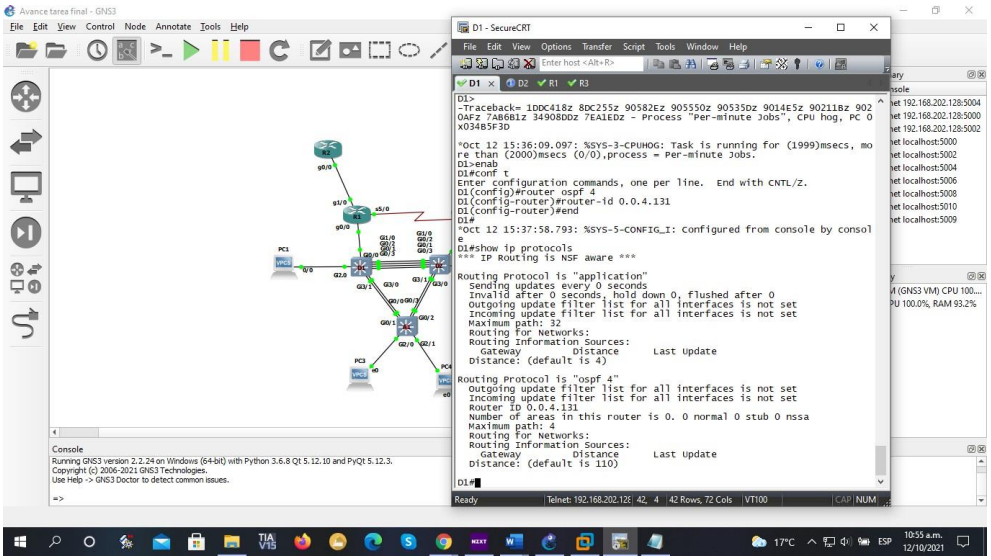


Figura 20. Comprobación de la configuración de ospf D2 comprobación protocolo ospf 4

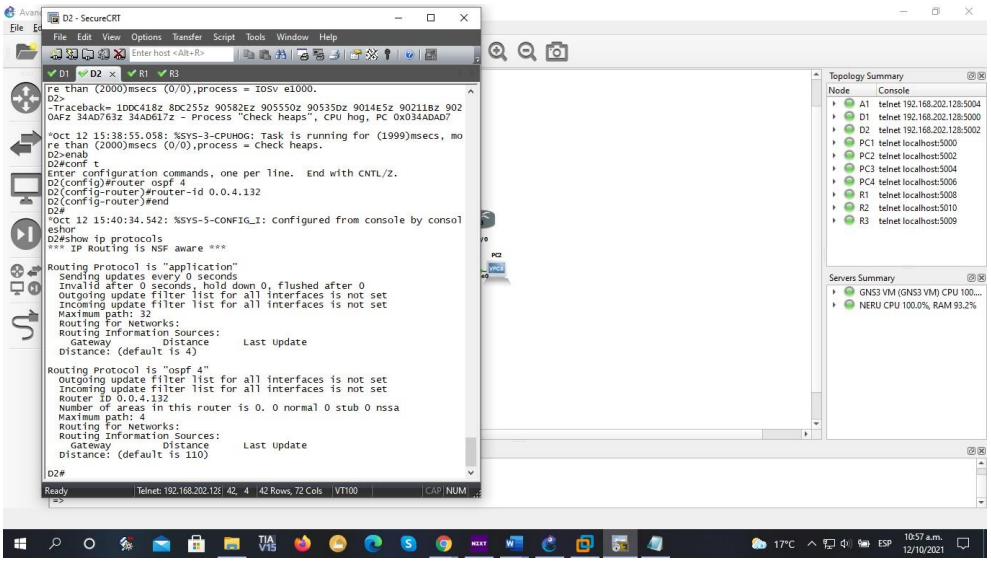
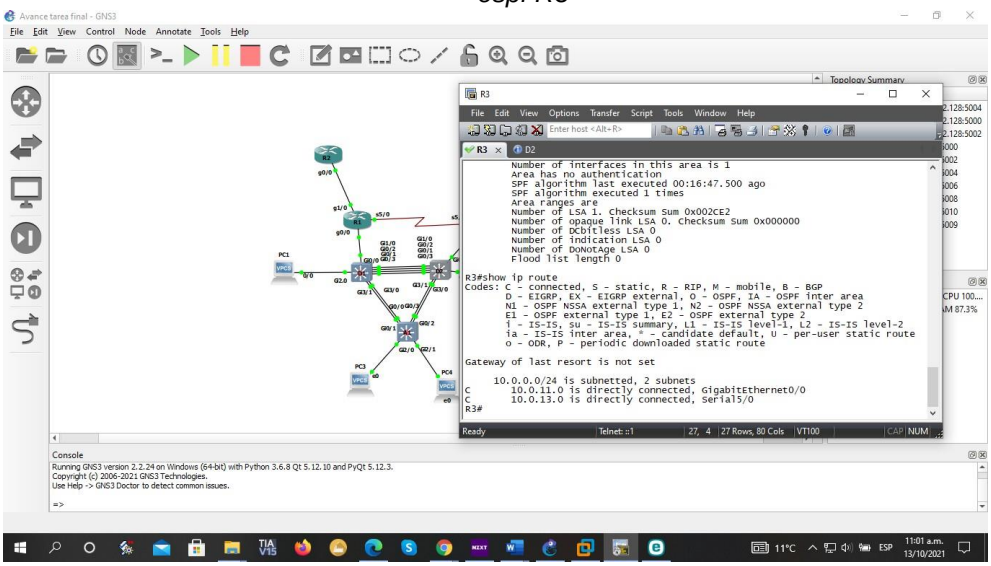


Figura 21. Comprobación de la configuración de ospf R3



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

R3#conf t
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3

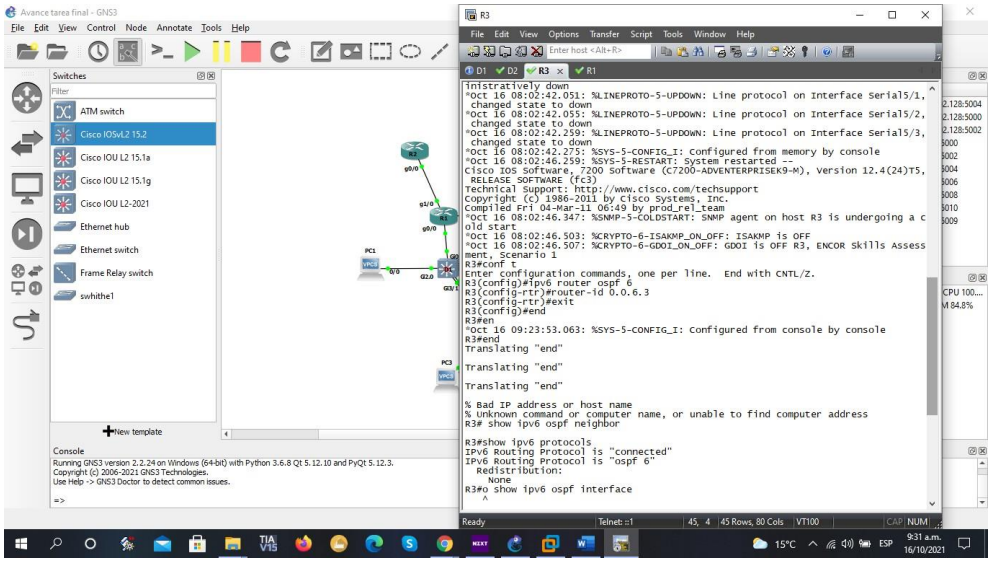
R1#conf t
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config)# ipv6 router ospf 6
R1(config-rtr)# passive-interface default

D2#conf t
D2(config)#*ipv6 unicast-routing*
D2(config)# ipv6 cef
D2(config)#ipv6 router ospf 6
D2 (config-rtr)#router-id 0.0.6.132
D2 (config)#int e0/0
D2(config-if)# ipv6 ospf 1 area 0
D2(config-if)# interface e0/0
D2 (config-if)#ipv6 add 2001:db8:100:100::1/64 area 0
D2 (config-if)#ipv6 add 2001:db8:100:101::1/64 area 0
D2 (config-if)#ipv6 add 2001:db8:100:102::1/64 area 0

D2(config)#ipv6 router ospf 6
D2(config-router)#passive-interface e1/0
D2(config-router)#passive-interface e1/1

D2(config-router)#passive-interface e1/2
D2(config-router)#passive-interface e1/3
D2(config-router)#passive-interface e3/0
D2(config-router)#passive-interface e3/1

Figura 22. Configuración de ospf 6 R3



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.

Tabla 5. Configuración de MP-BGP

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

```
R2(config)#ipv6 unicast-routing
R2(config)#Router bgp 500
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#
*Oct 28 20:14:44.635: %BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#neighbor 209.165.200.225 update-source loopback0
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 update-source loopback0
R2(config-router)#exit
```

```
R1(config)#router bgp 300
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#
*Oct 28 20:48:57.315: %BGP-5-ADJCHANGE: neighbor 209.165.200.226 Up
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#exit
R1(config)#end
```

```
R1(config)#router bgp 300
R1(config-router)#address-family IPV4 unicast
R1(config-router-af)#neighbor 209.165.200.226 active ?
% Unrecognized command
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)##network 209.165.200.226 mask  255.255.255.224
R1(config-router-af)#exit-address-family
R1(config-router)#address-family IPV6 unicast
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:200::/0
R1(config-router-af)#exit
```

Figura 23. Configuración de ISP R1

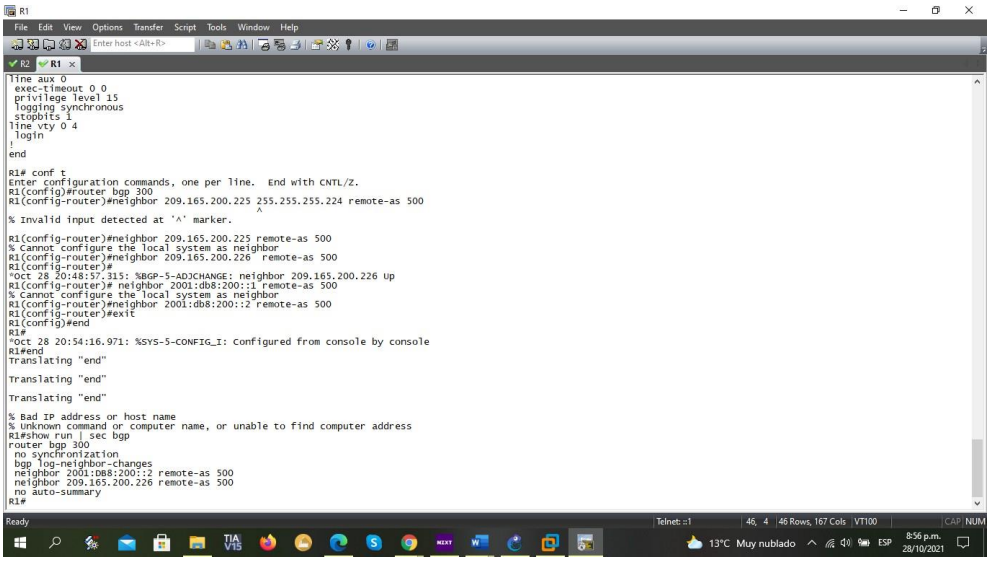


Figura 24. Configuración de ISP R2

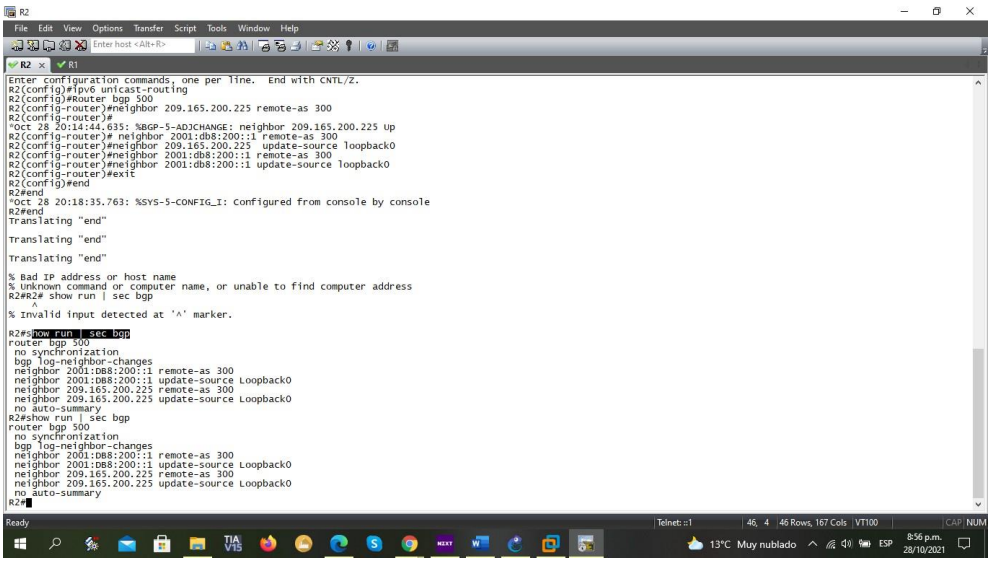
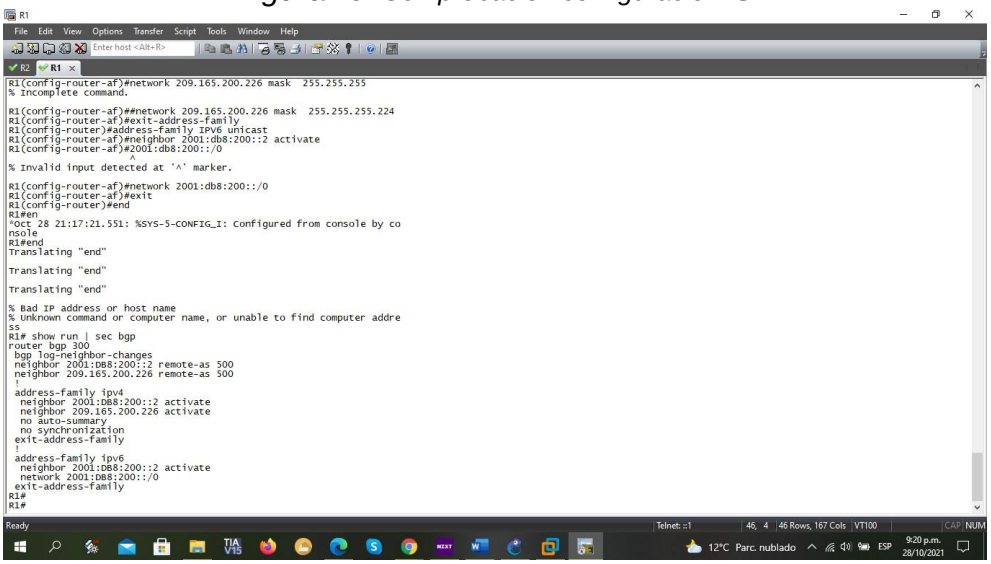


Figura 25. Comprobación configuración ISP R1



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

R1#conf t
R1(config)#Ipv6 unicast-routing
R1(config)# Router bgp 300
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# network 10.0.0.0 mask 255.255.0.0
R1(config-router)# ip route 10.0.0.0 255.255.0.0 null 0
R1(config-router)# network 2001:db8:200::/64
R1(config-router)# ip route 2001:db8:200::0 null 0
R1# show run | sec bgp

R2#conf t
R2(config)#Ipv6 unicast-routing
R2(config)# Router bgp **500**
R2(config-router)# neighbor 209.165.200.225 remote-as 300
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300
R2# show run | sec bgp

R2(config)# Router bgp **500**
R2(config-router)# address-family IPV4 unicast
R2(config-router-af)#neighbor 10.0.0.0 remote-as 300

```
R2(config-router-af)# neighbor 10.0.0.0 activate
R2(config-router-af)# network 10.0.0.0 mask 255.255.0.0
R2(config-router-af)# no neighbor 2001:db8:200::1
R2(config-router-af)#exit-address-family
R2(config-router)# address-family IPV6 unicast
R2(config-router-af)#neighbor 2001:db8:100::0 remote-as 300
R2(config-router-af)# neighbor 2001:db8:100::0 activate
R2(config-router-af)# network  2001:db8:100::/48
R2(config-router-af)# no neighbor 10.0.0.0
```

Figura 26. Comprobación configuración ISP R2

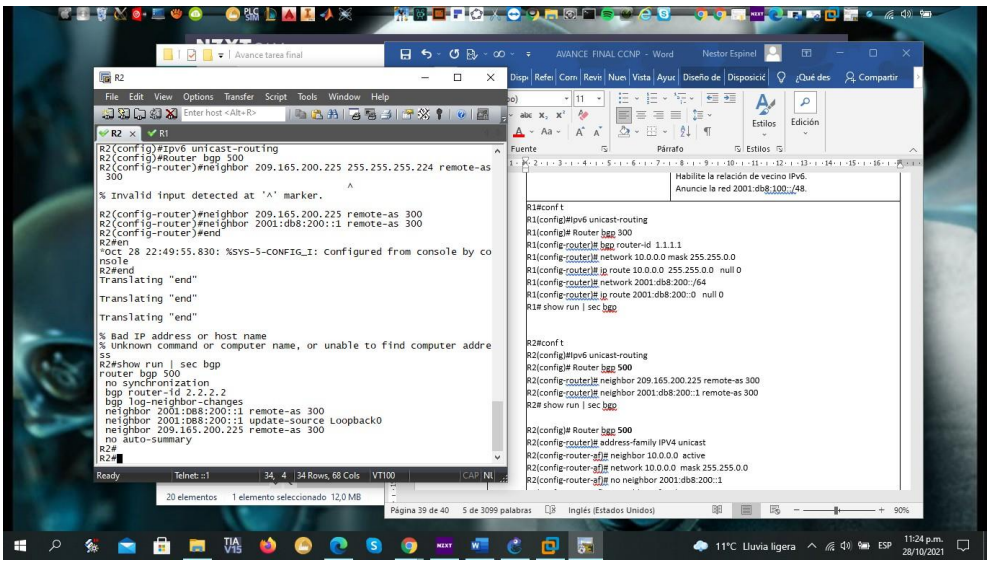
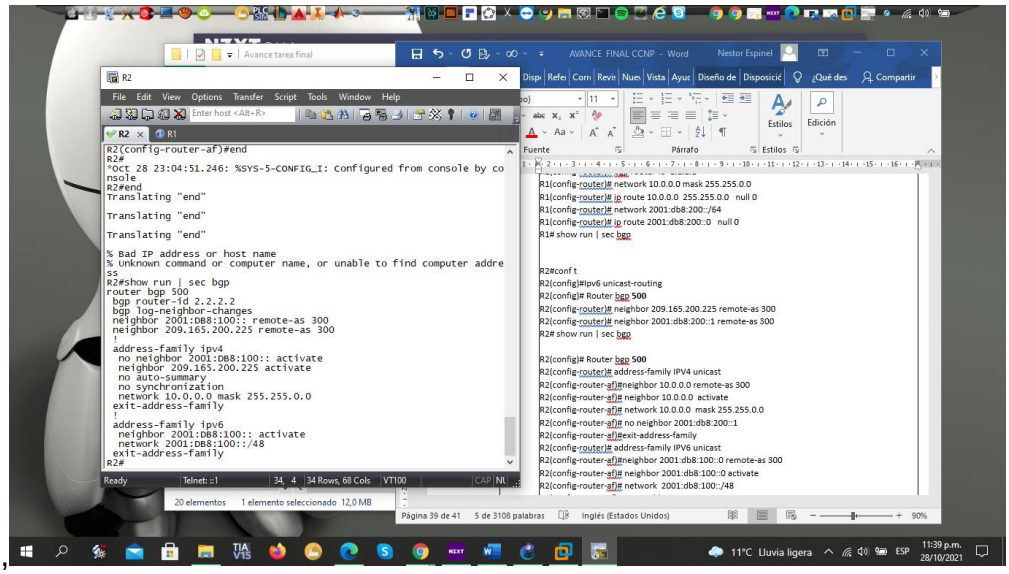


Figura 27. Comprobación configuración ISP R2



,,

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”.
Las tareas de configuración son las siguientes:

Tabla 6. Configuración de IP SLAS

Tarea #	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	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 G0/0/1 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 G0/0/1.	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 G0/0/1 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.

En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

```
R1(config)#ip sla 4
R1(config-ip-sla)# Icmp-echo 10.0.10.2
```

R1(config-ip-sla-echo)#Frequency 5
R1(config-ip-sla-echo)#Ip sla schedule 4 start-time now life forever
R1(config)#end
En R1
Configure terminal
R1(config)#ip sla 6
R1(config-ip-sla)# Icmp-echo 2001:db8:100:1010::2
R1(config-ip-sla-echo)#Frequency 5
R1(config-ip-sla-echo)#Ip sla schedule 6 start-time now life forever
R1(config)#end

Comprobacion
Show ip sla configuration
D1(config)#ip sla 4
D1(config-ip-sla)# Icmp-echo 10.0.10.1
D1(config-ip-sla-echo)#Frequency 5
D1(config-ip-sla-echo)#Ip sla schedule 4 start-time now life forever
D1(config)#end

D1(config)#ip sla 6
D1(config-ip-sla)# Icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)#Frequency 5
D1(config-ip-sla-echo)#Ip sla schedule 6 start-time now life forever
D1(config)#end

D1(config)#track 4 ip sla 4 state
D1(config-track)#delay up 10 down 15
D1(config-track)#end
D1(config)#track 6 ip sla 6 state
D1(config-track)#delay up 10 down 15
D1(config-track)#end

Figura 28. Comprobación configuración IP SLAs R1

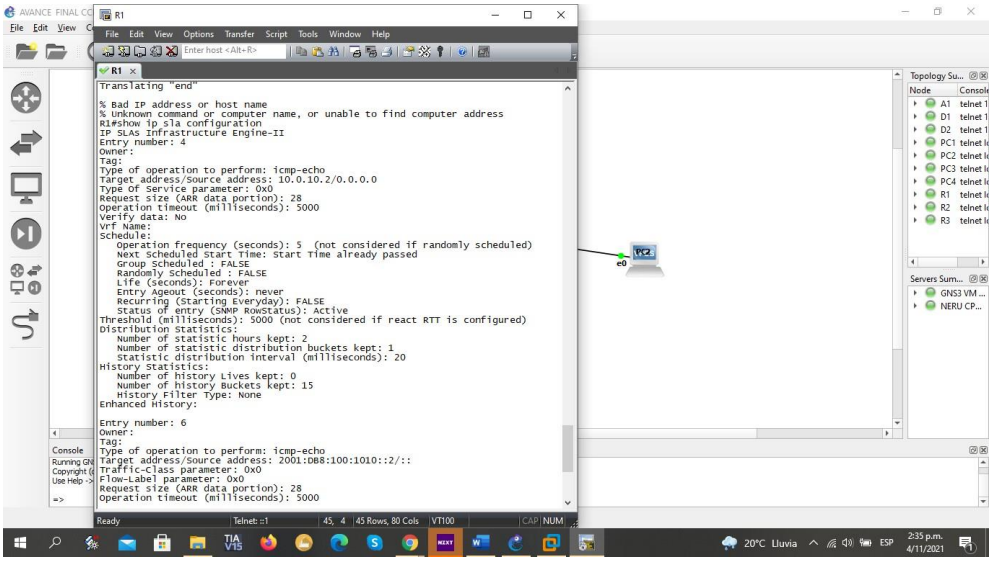


Figura 29. Comprobación configuración IP SLAs R1

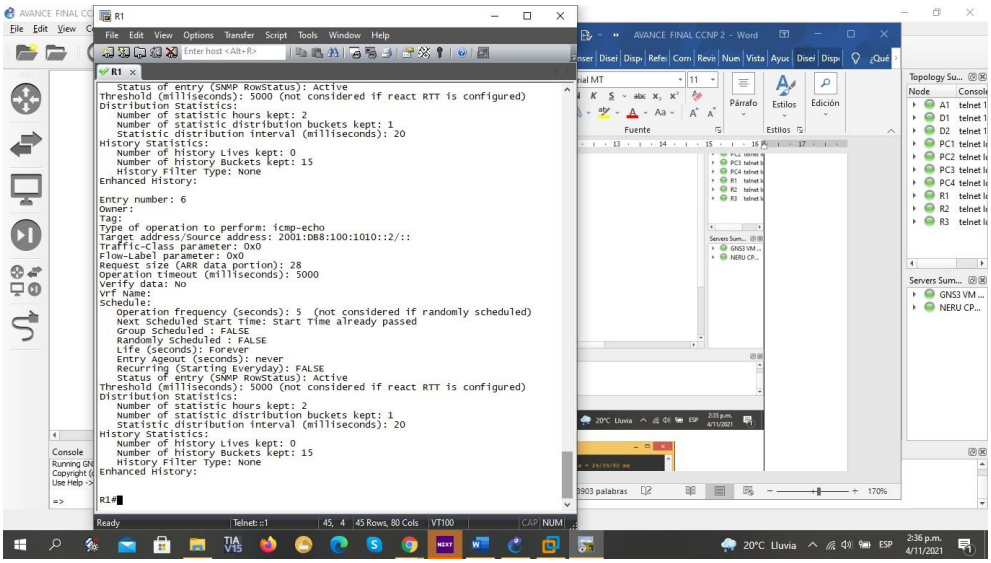


Figura 30. Comprobación configuración IP SLAs D1

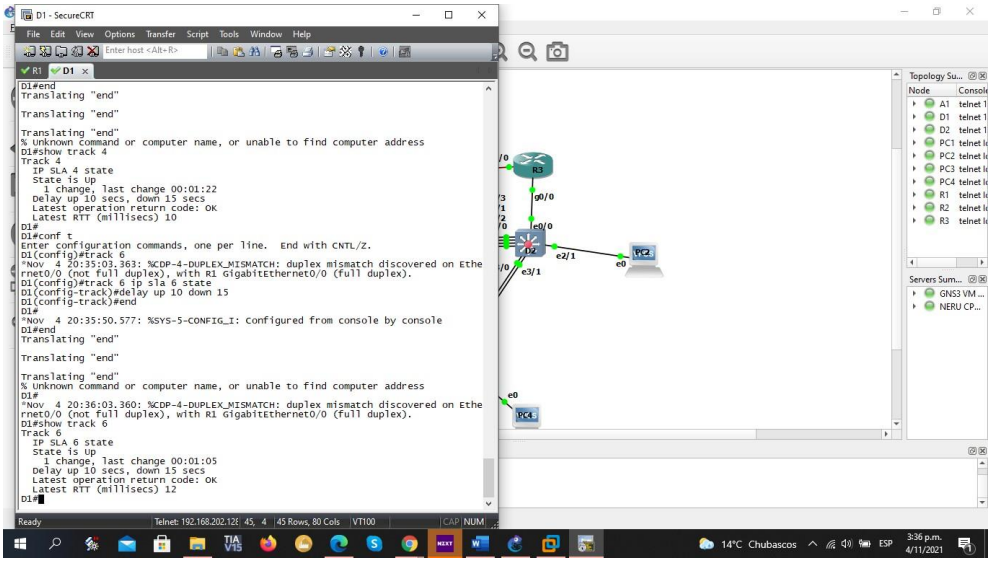
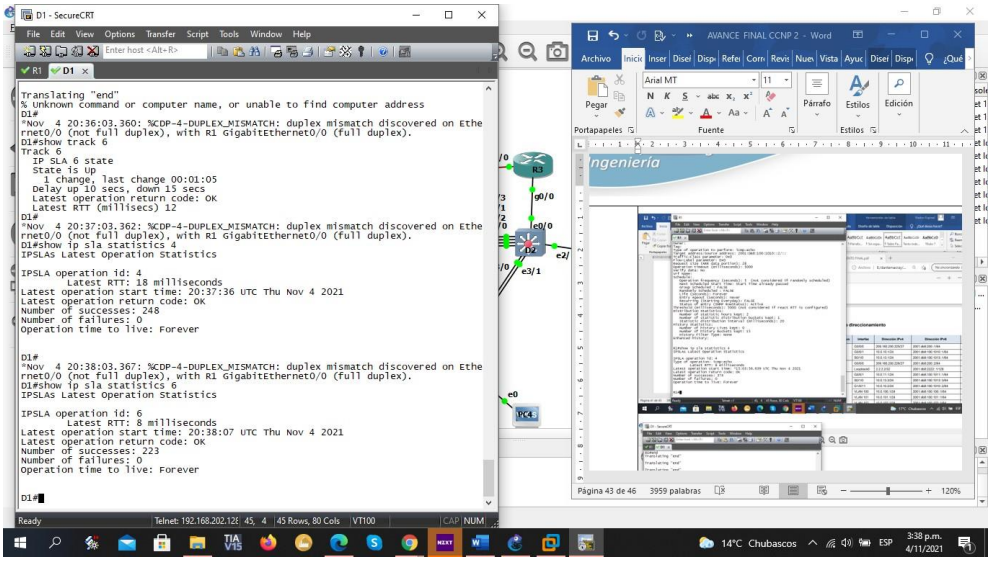


Figura 31. Comprobación configuración IP SLAs D1



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

D2(config)#ip sla 4
D2(config-ip-sla)#Icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5

D2(config-ip-sla-echo)#Ip sla schedule 4 start-time now life forever
D2(config)#end

D2(config)#ip sla 6
D2(config-ip-sla)#Icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#Ip sla schedule 6 start-time now life forever
D2(config)#end
Show ip sla configuration
D1(config)#track 4 ip sla 4 state
D1(config-track)#delay up 10 down 15
D1(config-track)#end
D1(config)#track 6 ip sla 6 state
D1(config-track)#delay up 10 down 15
D1(config-track)#end
D2Show track 6

Figura 32. Comprobación configuración IP SLAs D2

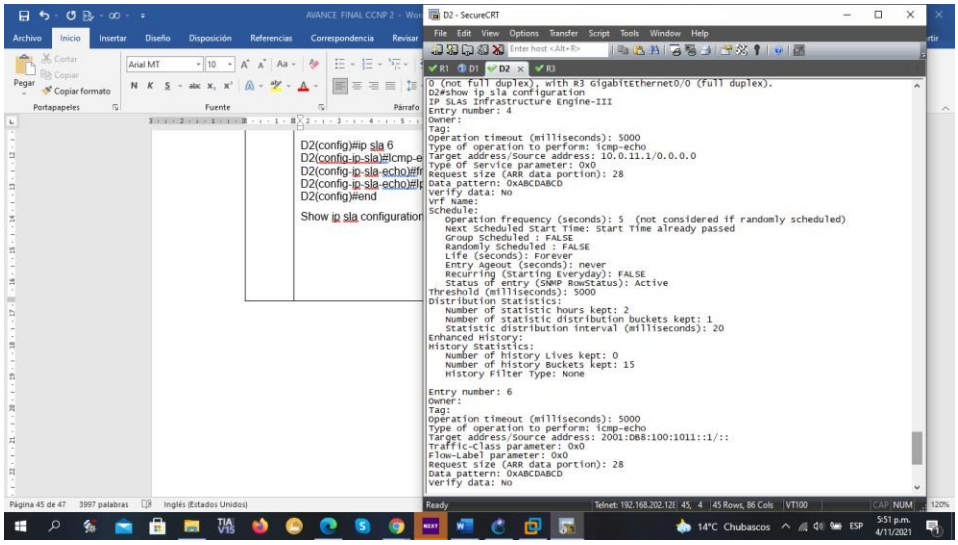


Figura 33. Comprobación configuración IP SLAs D2

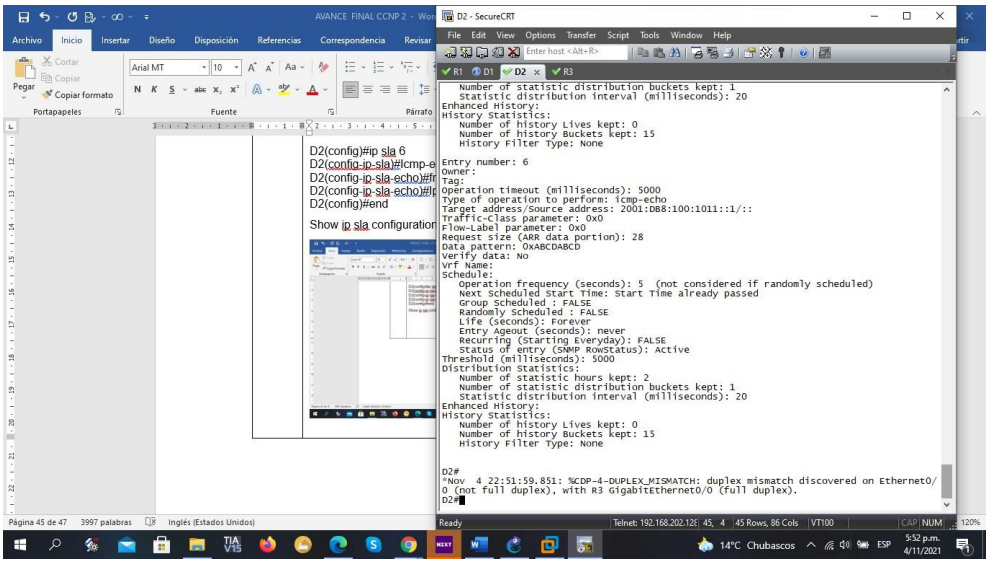


Figura 34. Comprobación configuración IP SLAs D2

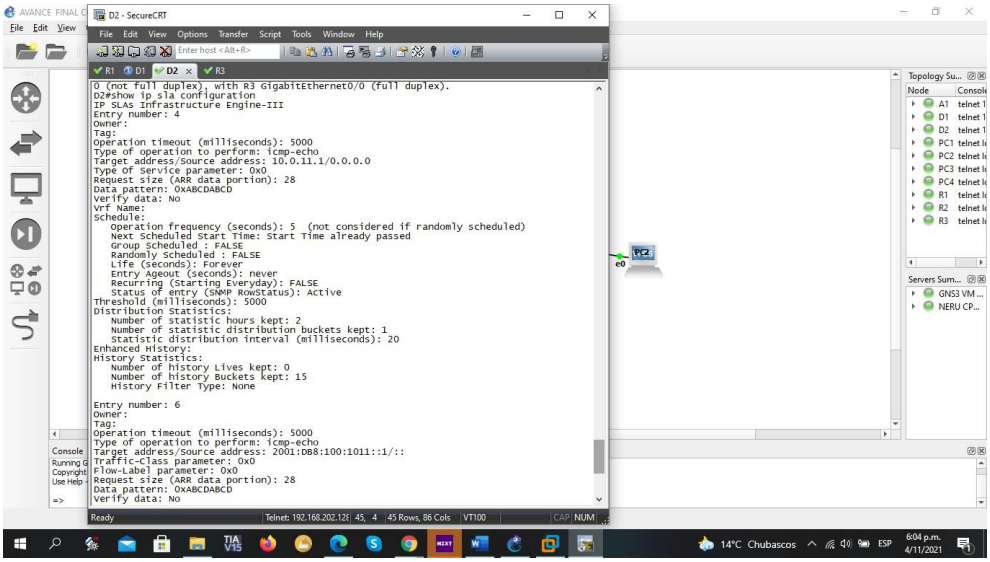


Figura 35. Comprobación de dirección destino IP SLAs D1

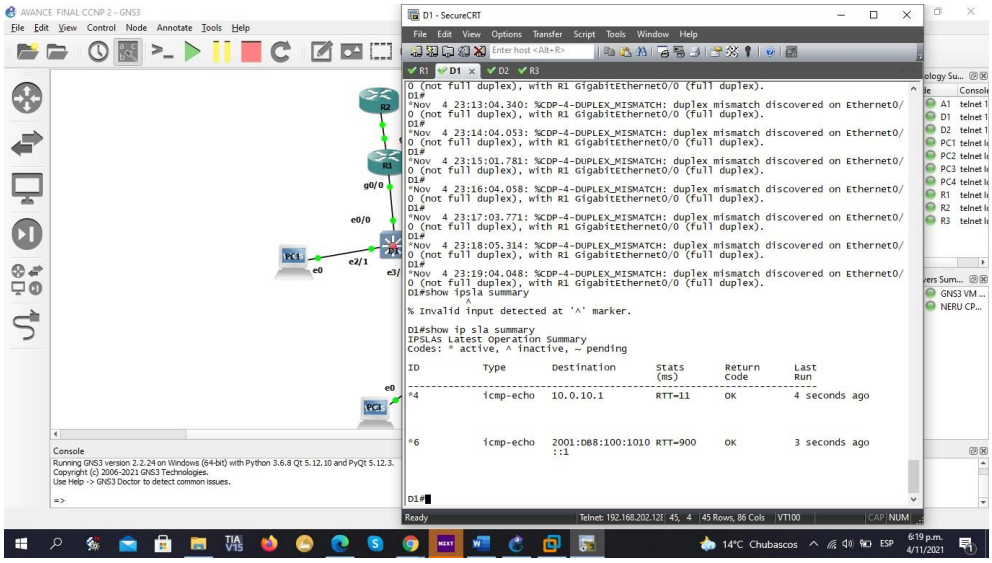
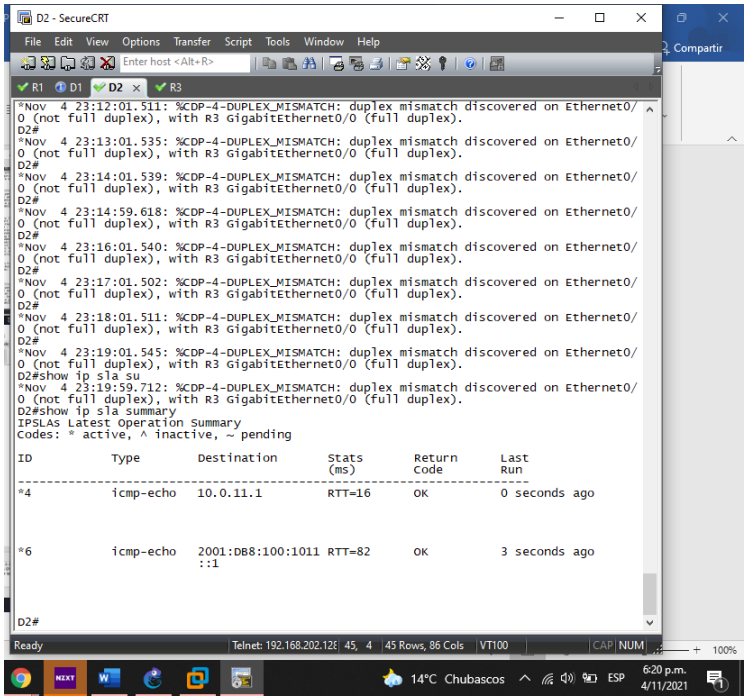


Figura 36. Comprobación de dirección destino IP SLAs D2



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 version 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.

En D2, configure HSRPv2.
D2(config-if)#ip routing
D2(config)#int vlan 100

```
D2(config-if)#ip add 10.0.100.2 255.255.255.0
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104  preempt delay minimum 60
D2(config-if)#standby 104 track 4
D2(config-if)#exit

D2(config)#int vlan 101
D2(config-if)#ip add 10.0.101.2 255.255.255.0
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114  preempt delay minimum 60
D2(config-if)#stanbdy 114 track 4
D2(config-if)#exit


D2(config)#int vlan 102
D2(config-if)#ip add 10.0.102.2 255.255.255.0
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 priority 150
D2(config-if)#standby 124 preempt delay minimum 60
D2(config-if)#standby 124 track 4
D2(config-if)#exit

D2(config)#int vlan 100
D2(config-if)#ip add 10.0.100.2  255.255.255.0
*Nov 9 16:33:16.633: %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet0/0 (full
duplex).
D2(config-if)#ip add 10.0.100.2 255.255.255.0
D2(config-if)#standby version 2
D2(config-if)#standby 106 ipv6  autoconfig
D2(config-if)#
*Nov 9 16:34:16.594: %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet0/0 (full
duplex).
D2(config-if)#
D2(config-if)#standby 106 priority 150
D2(config-if)#standby 106  preempt delay minimum 60
D2(config-if)#standby 106 track 6
D2(config-if)#exit


D2(config)#int vlan 101
```

```
D2(config-if)#ip add 10.0.101.2 255.255.255.0
D2(config-if)#standby version 2
D2(config-if)#
*Nov 9 16:36:16.565: %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet0/0 (full
duplex).
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 preempt delay minimum 60
D2(config-if)#standby 116 track 6
D2(config-if)#exit


D2(config-if)#exit
D2(config)#int vlan 102
D2(config-if)#ip add 10.0.102.2 255.255.255.0
D2(config-if)#
*Nov 9 16:38:16.568: %CDP-4-DUPLEX_MISMATCH: duplex mismatch
discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet0/0 (full
duplex).
D2(config-if)#standby version 2
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126  priority 150
D2(config-if)#standby 126 preempt delay minimum 60
D2(config-if)#standby 126 track 6
D2(config-if)#exit
```

Figura 37. Comprobación de standby D2

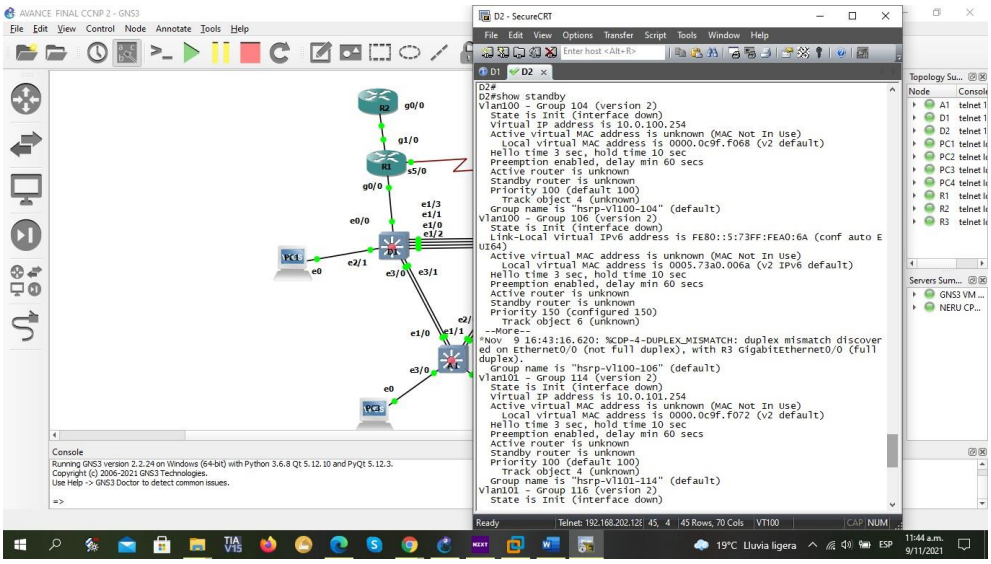


Figura 38. Comprobación de standby D2

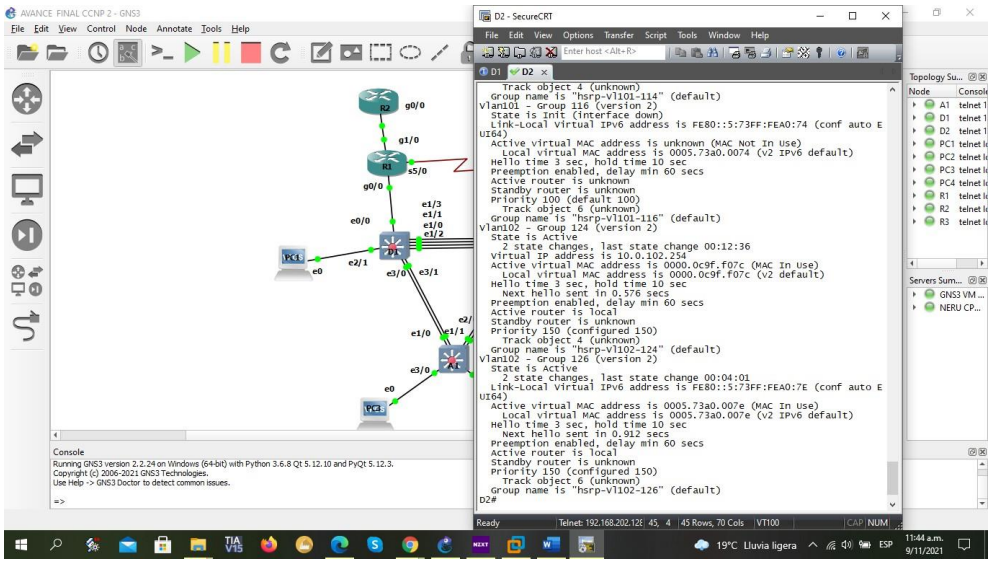
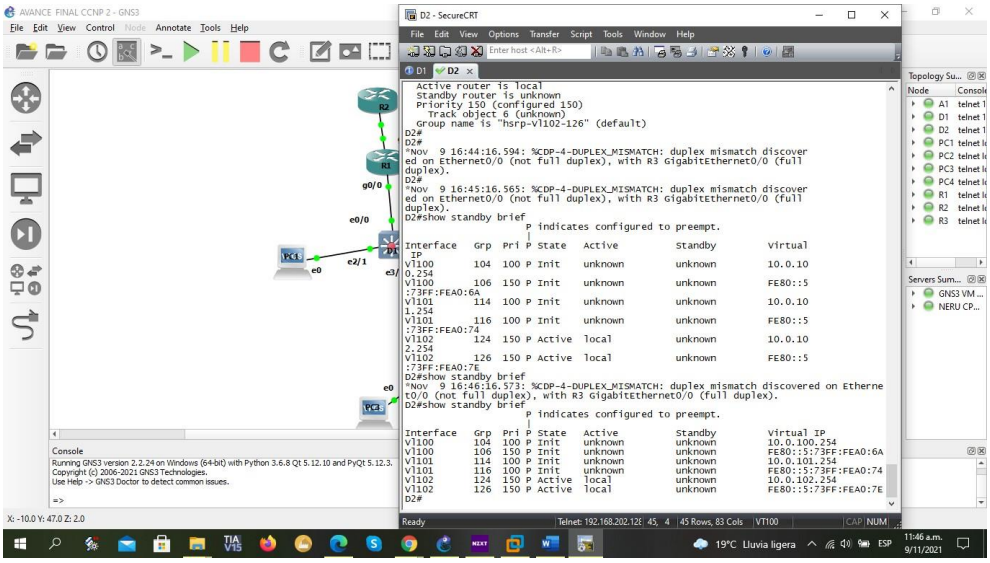


Figura 38. Comprobación de standby D2



Parte 5: Seguridad

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

Tabla 7. Configuración de mecanismos de seguridad

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 o llave : **$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**.

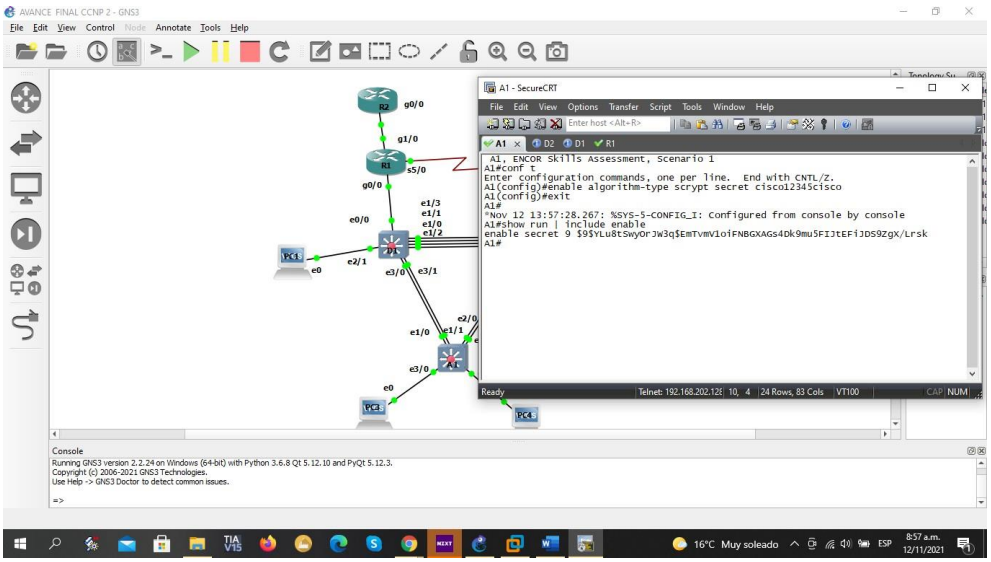
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D1#show run | include enable

D2(config)#enable algorithm-type scrypt secret cisco12345cisco
D2#show run | include enable

A1(config)#enable algorithm-type scrypt secret cisco12345cisco
A1#show run | include enable

R1(config)#line console 0
R1(config-line)#password cisco12345cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret cisco12345cisco
R1(config)#service password-encryption
R1(config)#exit
show run | include enable
R2(config)#line console 0
R2(config-line)#password cisco12345cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#enable secret cisco12345cisco
R2(config)#service password-encryption
R2(config)#exit
show run | include enable
R3(config)#line console 0
R3(config-line)#password cisco12345cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#enable secret cisco12345cisco
R3(config)#service password-encryption
R3(config)#exit
R3#show run | include enable

Figura 39. Encriptación de contraseña



A1(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
A1#show run | include username

D1(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
D1#show run | include username

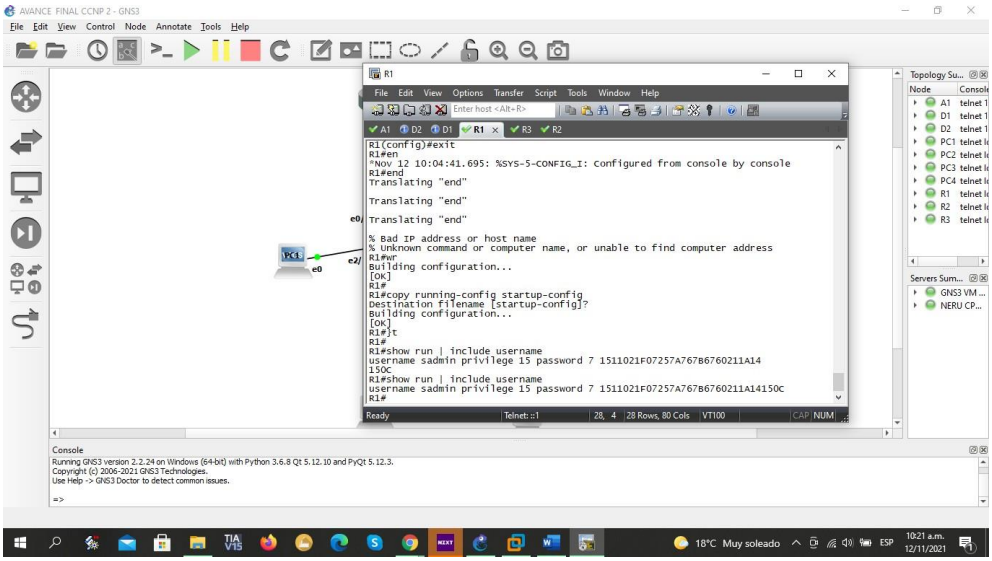
D2(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
D2#show run | include username

R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#username sadmin privilege 15 password cisco12345cisco
R1(config)#enable secret password cisco12345cisco
R1(config)#enable secret username sadmin
R1(config)#service password-encryption

R2(config)#line console 0
R2(config-line)#login local
R2(config-line)#username sadmin privilege 15 password cisco12345cisco
R2(config)#enable secret password cisco12345cisco
R2(config)#enable secret username sadmin
R2(config)#service password-encryption

R3(config)#line console 0
R3(config-line)#login local
R3(config-line)#username sadmin privilege 15 password cisco12345cisco
R3(config)#enable secret password cisco12345cisco
R3(config)#enable secret username sadmin
R3(config)#service password-encryption

Figura 40. Comprobación de usuario en nivel de privilegio



En todos los dispositivos (excepto R2), habilite AAA.
En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.
En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.

Username: sadmin
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port 1813
R1(config)#radius-server key $trongPass
R1(config)#aaa authentication login default group radius local
R1(config)# username raduser password upass123

```
Username: sadmin
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#aaa new-model
R3(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port 1813
R3(config)#radius-server key $trongPass
R3(config)#aaa authentication login default group radius local
R3(config)#username raduser password upass123
R3(config)#exit


D1(config)#aaa new-model
D1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port 1813
Warning: The CLI will be deprecated soon 'radius-server host 10.0.100.6 auth-
port 1812 acct-port 1813'
 Please move to 'radius server <name>' CLI.
D1(config)#radius-server key $trongPass
D1(config)#aaa authentication login default group radius local
D1(config)#username raduser password upass123
D1(config)#exit


D2(config)#aaa new-model
D2(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port 1813
Warning: The CLI will be deprecated soon 'radius-server host 10.0.100.6 auth-
port 1812 acct-port 1813' Please move to 'radius server <name>' CLI.
D2(config)#radius-server key $trongPass
D2(config)#aaa authentication login default group radius local
D2(config)#username raduser password upass123
D2(config)#exit

Username: sadmin
Password:
A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#aaa new-model
A1(config)#radius-server host 10.0.100.6 auth-port 1812 acct-port 1813
Warning: The CLI will be deprecated soon 'radius-server host 10.0.100.6 auth-
port 1812 acct-port 1813' Please move to 'radius server <name>' CLI.
A1(config)#radius-server key $trongPass
A1(config)#aaa authentication login default group radius local
A1(config)#username raduser password upass123
A1(config)#exit
```

Figura 41. Comprobación protocolo AAA en A1

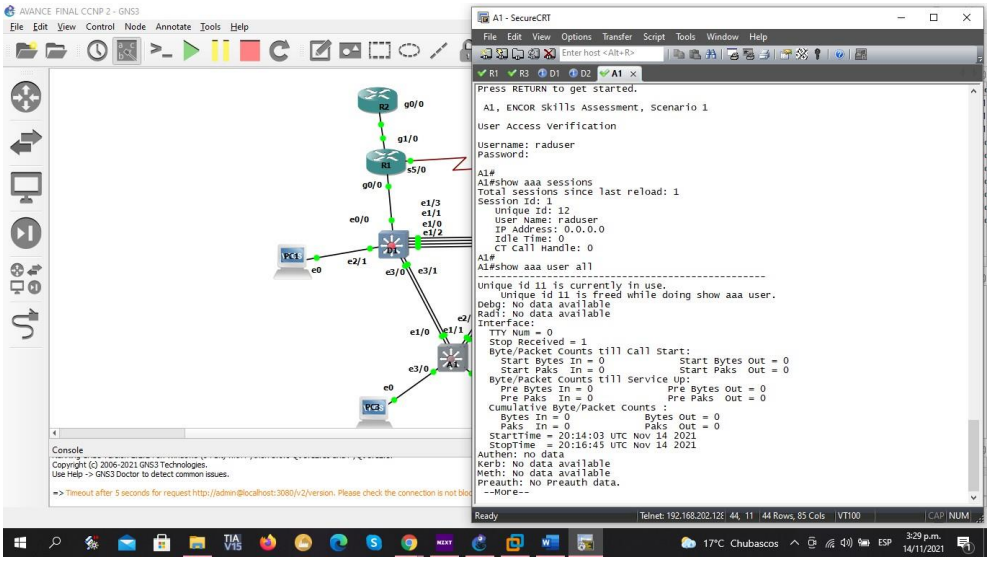


Figura 42. Verificación de sesión AAA en A1

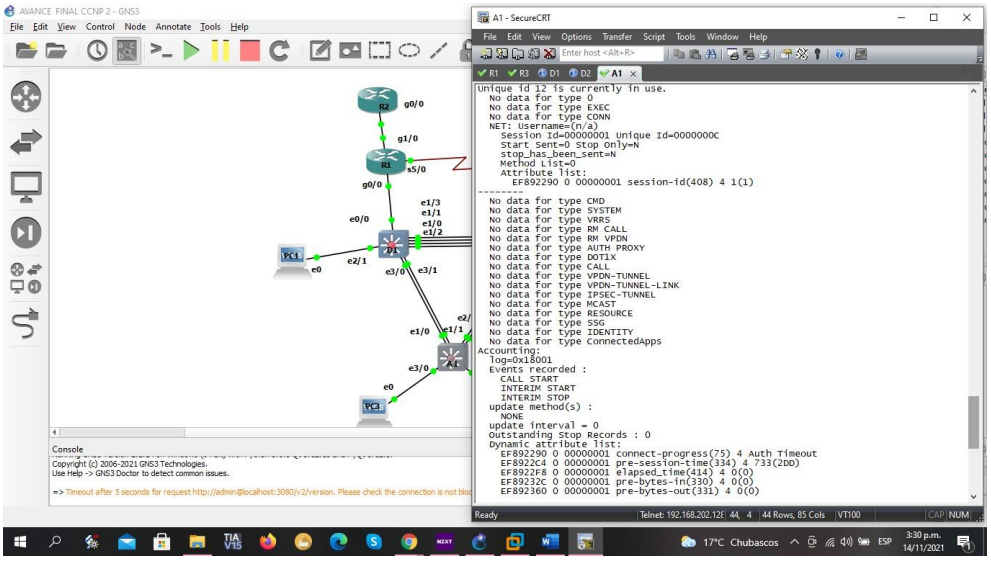


Figura 43. Verificación de conexión-procesos AAA en A1

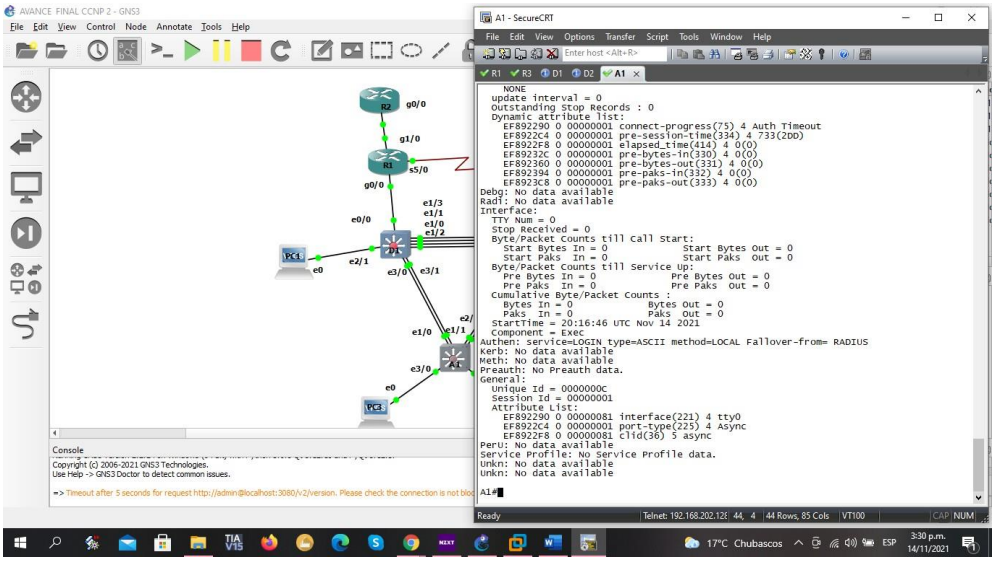


Figura 44. Verificación de sesión AAA en D2

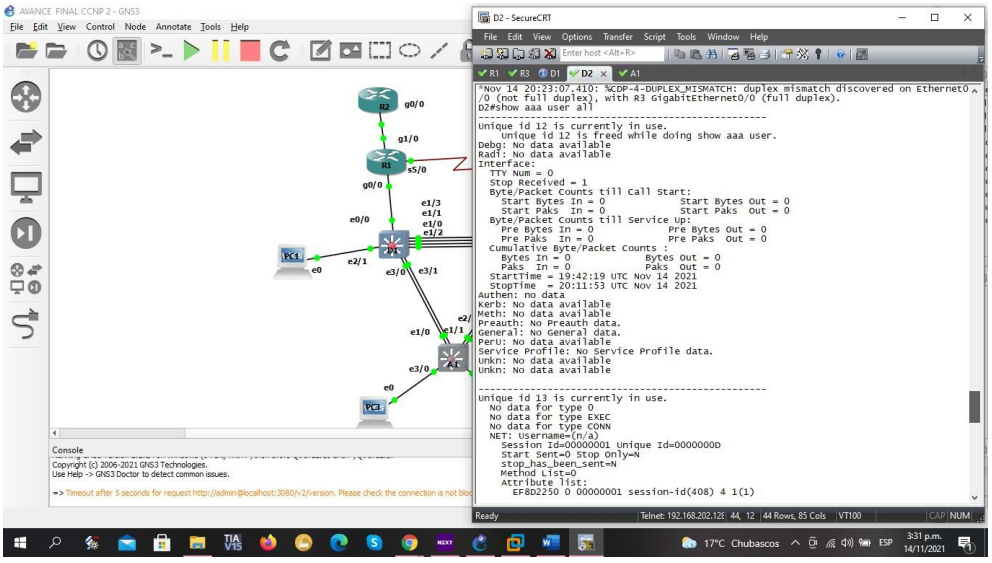


Figura 45. Verificación de sesión AAA en D1

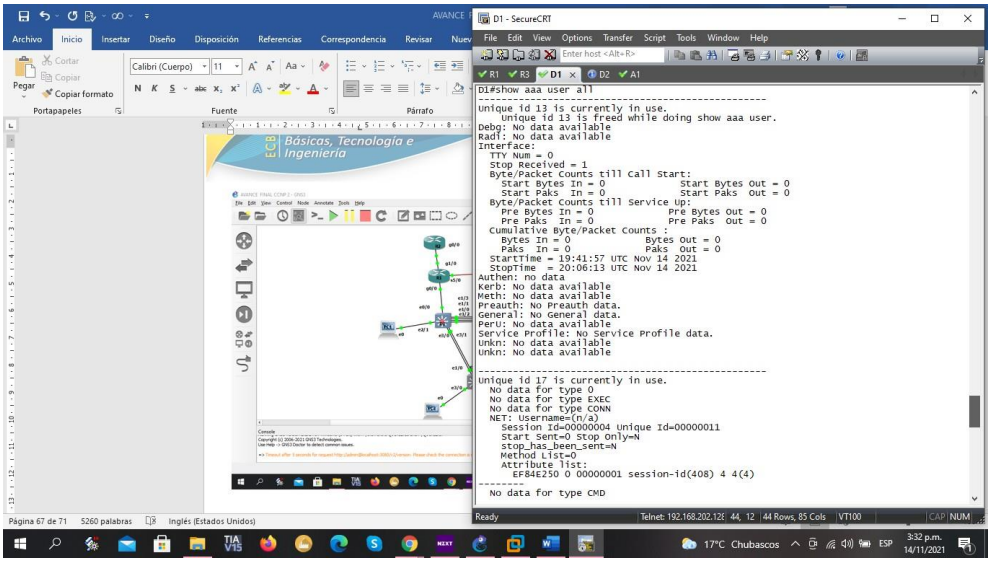


Figura 46. Verificación de sesión AAA en R3

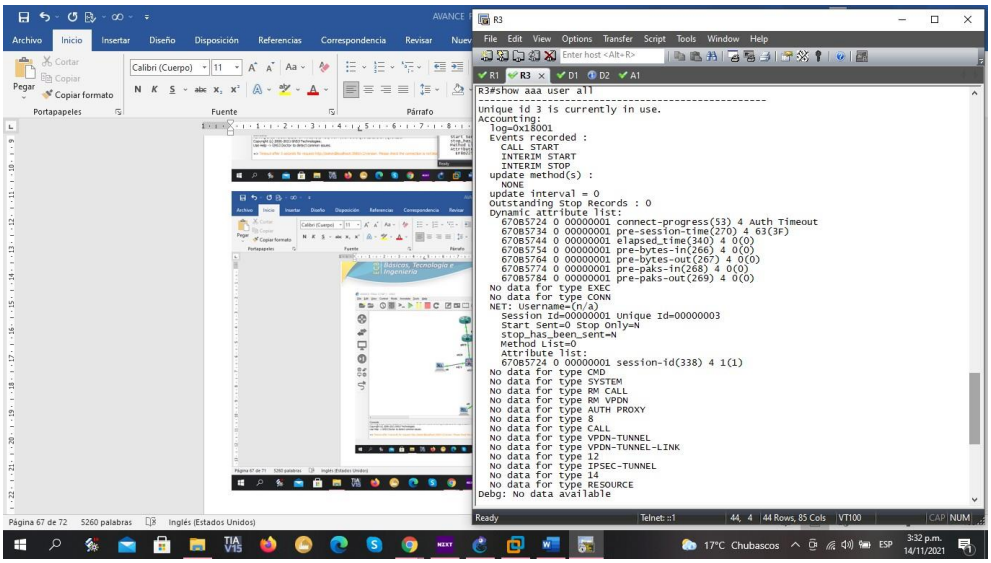
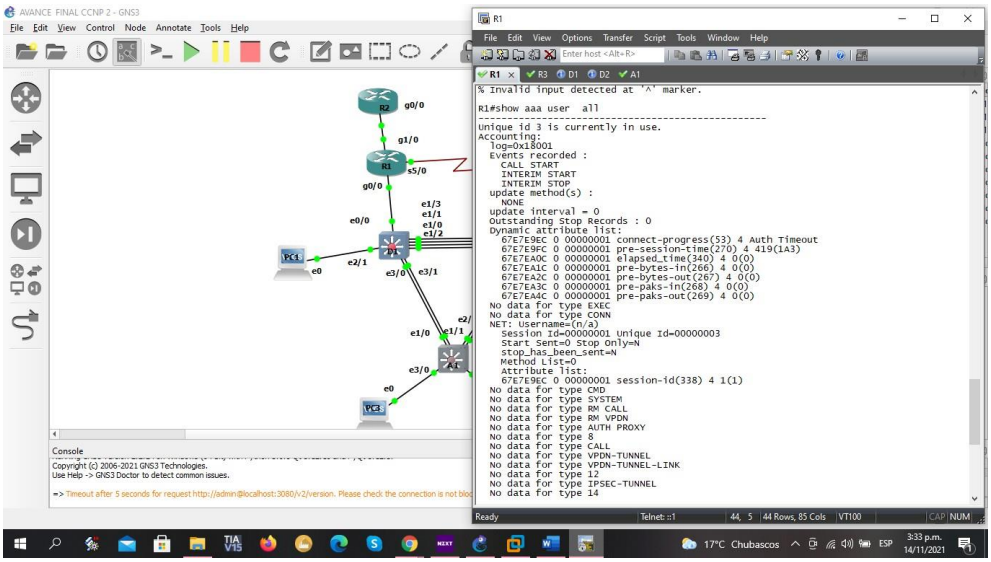


Figura 47. Verificación de sesión AAA en R1



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:

Tabla 8. Configuración de funciones de administración de red

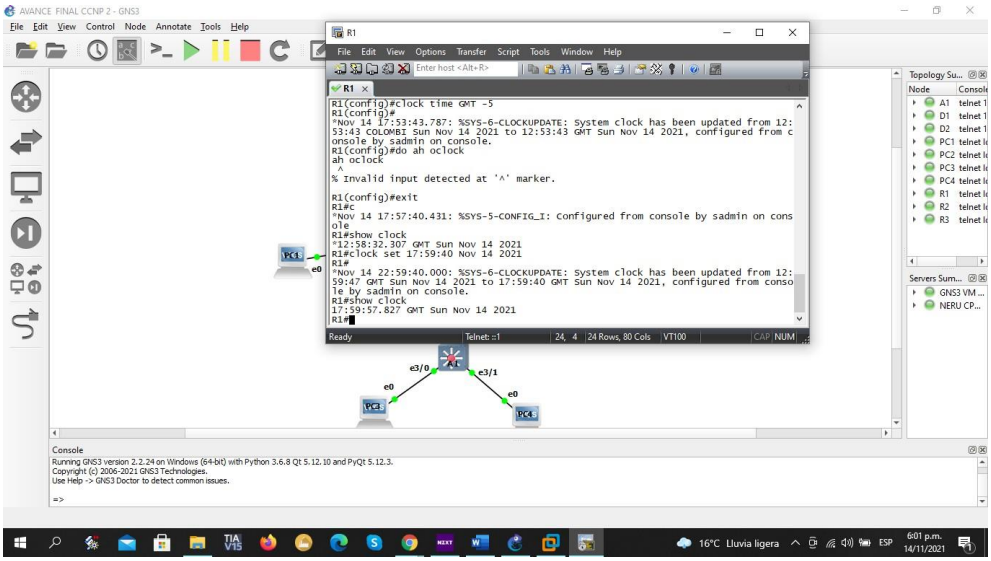
Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.

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

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

```
R1(config)#clock time UTC -5
R1#clock set 17:59:40 Nov 14 2021
R1#show clock

R2(config)#clock time UTC -5
R2#clock set 18:06:40 Nov 14 2021
R1#show clock

R3(config)#clock time UTC -5
R3#clock set 18:06:50 Nov 14 2021
R3#show clock

D1(config)#clock time UTC -5
D1#clock set 18:08:40 Nov 14 2021
D1(config)#exit

D2(config)#clock time UTC -5
D2#clock set 18:10:00 Nov 14 2021
D2(config)#exit

A1(config)#clock time UTC -5
A1#clock set 18:12:12 Nov 14 2021
A1(config)#exit
```

Figura 48. Comprobación de UTC R1



Configure R2 como un NTP maestro.

Username: sadmin
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3
R2(config)#end

Tabla 9. Configuración de funciones de administración de red

Tarea#	Tarea	Especificación
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: • Unicamente 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*.

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

Username: sadmin
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 209.165.200.226
R1(config)#ntp update-calendar
R1(config)#exit
R1#show ntp associations

R3(config)#ntp server 10.0.13.1
R3(config)#ntp update-calendar
R3(config)#exit

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp peer 10.0.13.2
R1(config)#ntp peer 10.0.10.2
*Nov 15 20:36:33.155: %BGP-5-ADJCHANGE: neighbor 209.165.200.226 Down BGP Notification sent
R1(config)#ntp peer 10.0.10.2

*Nov 15 20:36:33.155: %BGP-3-NOTIFICATION: sent to neighbor 209.165.200.226 4/0 (hold time expired) 0 bytes
R1(config)#ntp peer 10.0.10.2
R1(config)#ntp peer 10.0.100.3
R1(config)#end

D1(config)#ntp peer 10.0.10.1
D1(config)#exit

A1(config)#ntp peer 10.0.10.1
A1(config)#end

Figura 49. Configuración NTP y Comprobación de UTC R1

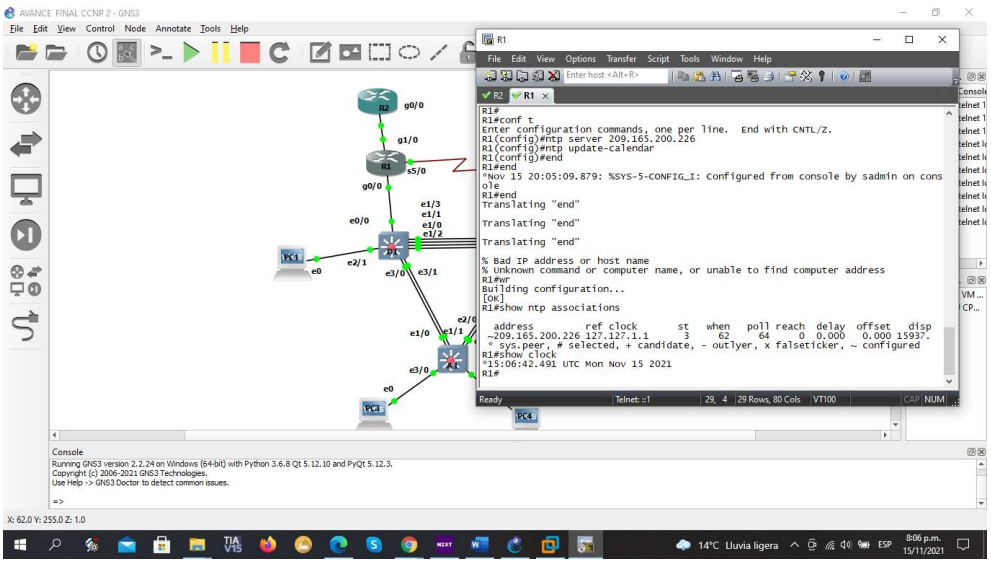


Figura 50. Comprobación NTP R3

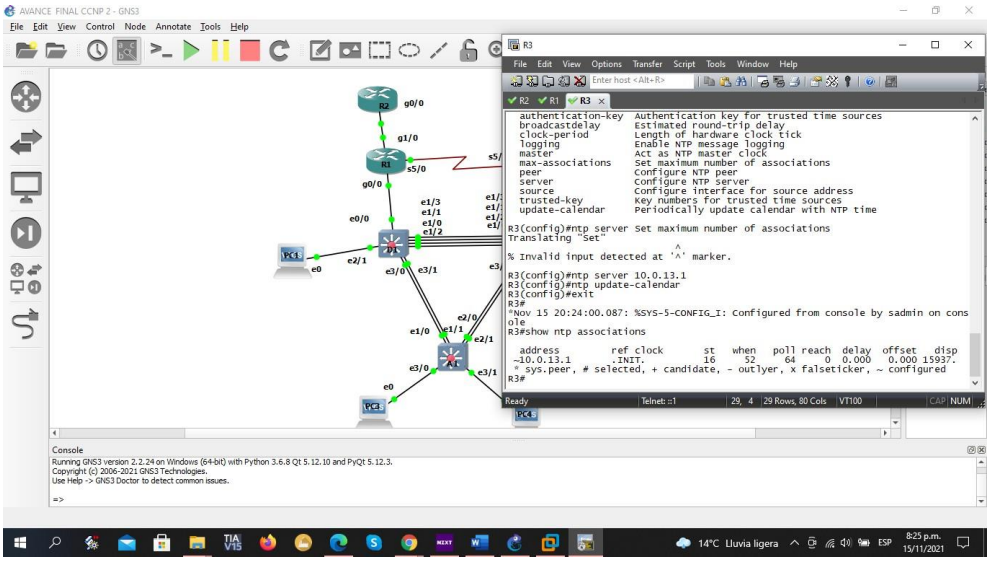


Figura 51. Comprobación NTP asociación R1

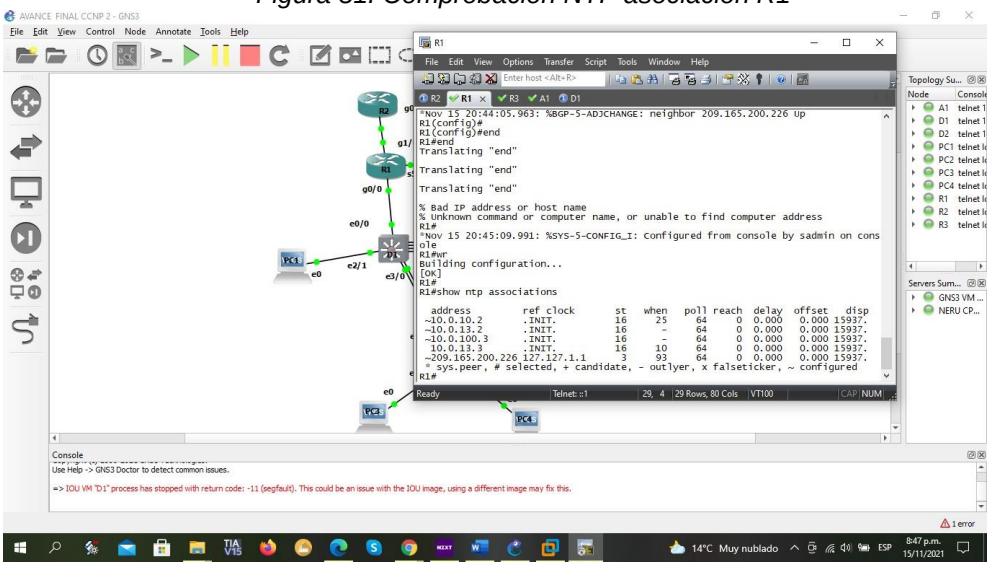


Figura 52. Comprobación NTP asociación R3

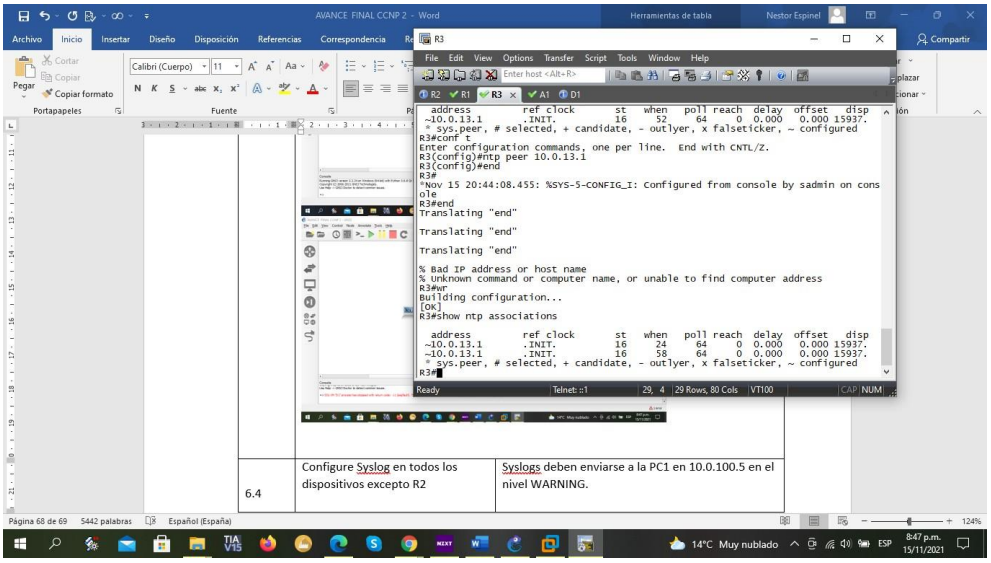


Figura 53. Comprobación NTP asociación A1

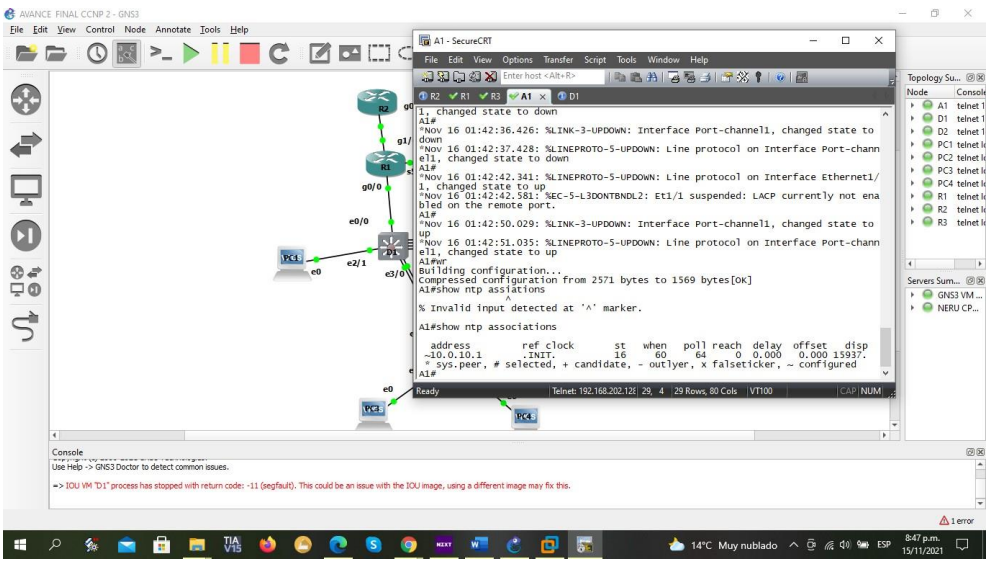
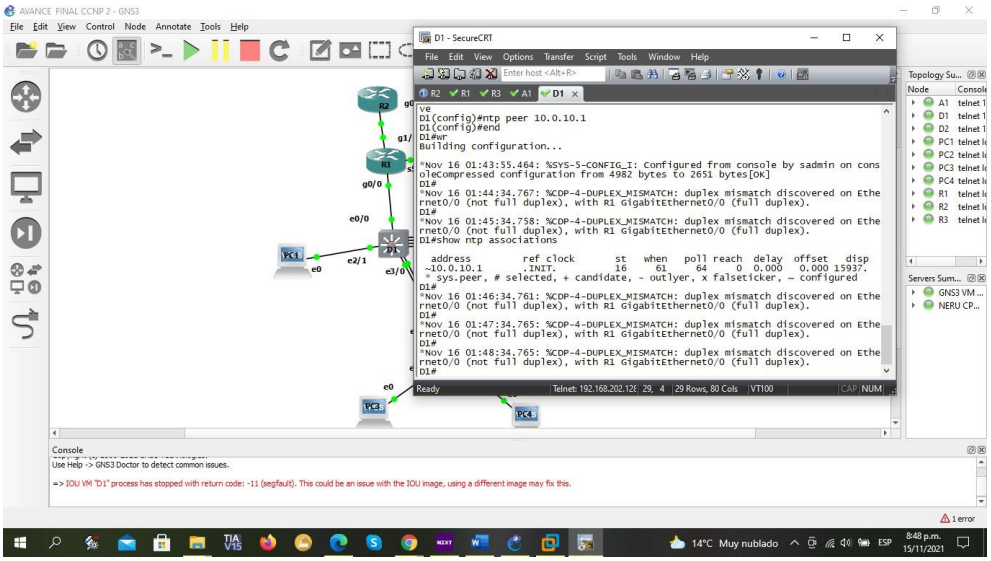


Figura 54. Comprobación NTP asociación D1



Configure Syslog en todos los dispositivos excepto R2

R3(config)#logging 10.0.100.5
R3(config)#logging trap warnings
R3(config)#logging trap 4

R1(config)#logging 10.0.100.5
R1(config)#logging trap warnings
R1(config)#logging trap 4
R1(config)# end

D1(config)#logging host 10.0.100.5
D1(config)#logging trap warnings
D1(config)#logging trap 4
D1(config)#end

D2(config)#logging host 10.0.100.5
D2(config)#logging trap warnings
D2(config)#logging trap 4
D2(config)#end

A1(config)#logging host 10.0.100.5
A1(config)#logging trap warnings
A1(config)#logging trap 4

A1(config)#exit

Figura 55. Comprobación de Syslog R3

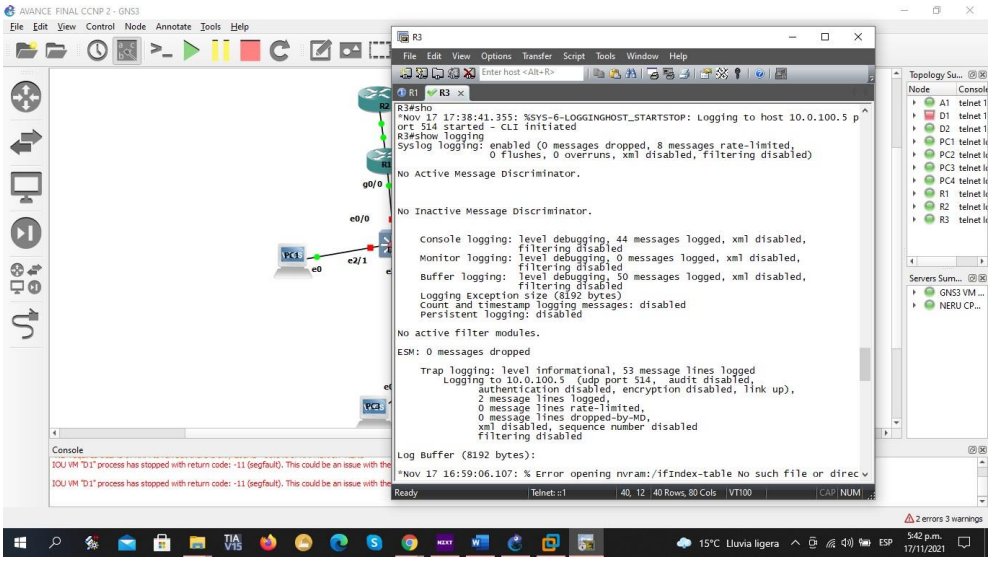


Figura 56. Comprobación de Syslog R1

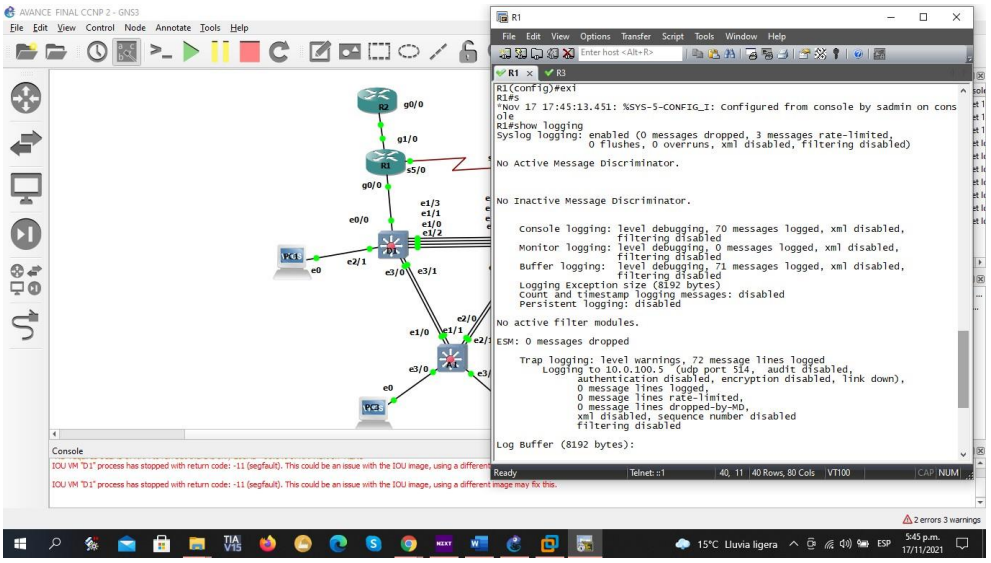
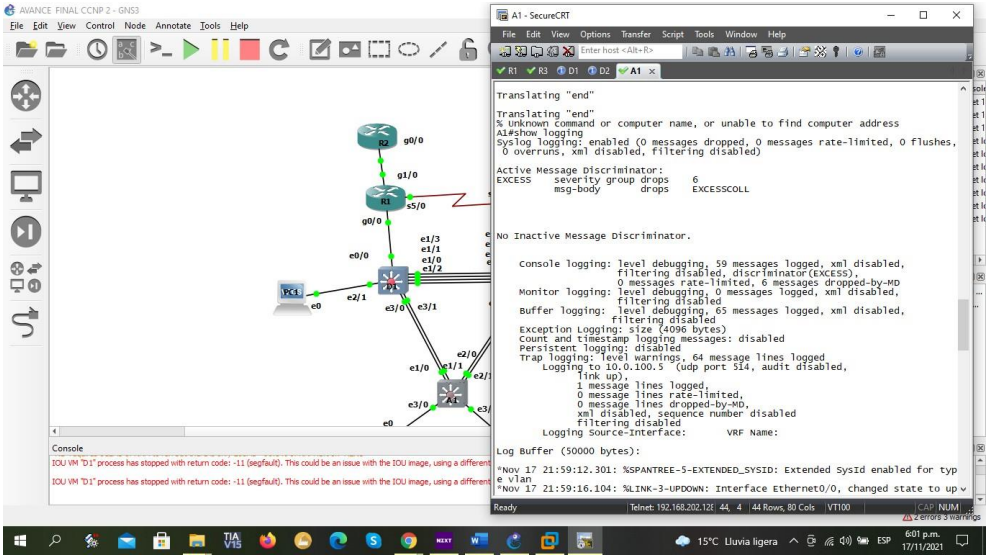


Figura 57. Comprobación de Syslog A1



Configure SNMPv2c en todos los dispositivos excepto R2

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#snmp-server community string ENCORSA
R3(config)#snmp-server location ?
  LINE The physical location of this node
R3(config)#snmp-server location Espinel
R3(config)#snmp-server contact Nestor_Arcangel
R3(config)#snmp-server host 10.0.100.5 version 2c string
R3(config)#ip access-list standard ENCORSA
R3(config)#snmp-server enable traps
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config-std-nacl)#permit 10.0.100.5
R3(config-std-nacl)#

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp-server community string ENCORSA
R1(config)#snmp-server location Espinel
R1(config)#snmp-server contact Nestor Arcangel
R1(config)#snmp-server host 10.0.100.5 version 2c string

```
R1(config)#ip access-list standard ENCORSA
D1(config)#snmp-server enable traps
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps bgp
D1(config)#snmp-server enable traps ospf
R1(config-std-nacl)#permit 10.0.100.5
R1(config-std-nacl)#exit

D1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#
D1(config)#snmp-server community string ENCORSA
D1(config)#snmp-server location Espinel
D1(config)#snmp-server contact Nestor Arcangel
D1(config)#snmp-server host 10.0.100.5 version 2c string
D1(config)#ip access-list standard ENCORSA
D1(config)#snmp-server enable traps
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config-std-nacl)#permit 10.0.100.5
D1(config-std-nacl)#exit

D2#
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#snmp-server community string ENCORSA
D2(config)#snmp-server location Espinel
D2(config)#snmp-server contact Nestor Arcangel
D2(config)#snmp-server host 10.0.100.5 version 2c string
D2(config)#ip access-list standard ENCORSA
D2(config)#snmp-server enable traps
D2(config)#snmp-server enable traps config
D2(config)#snmp-server enable traps ospf
D2(config-std-nacl)#permit 10.0.100.5
D2(config-std-nacl)#exit

Username: sadmin
Password:
A1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#snmp-server community string ENCORSA
A1(config)#snmp-server location Espinel
A1(config)#snmp-server contact Nestor Arcangel
A1(config)#snmp-server host 10.0.100.5 version 2c string
A1(config)#ip access-list standard ENCORSA
```

```
A1(config)#snmp-server enable traps
A1(config)#snmp-server enable traps config
A1(config-std-nacl)#permit 10.0.100.5
A1(config-std-nacl)#exit
```

Figura 59. Comprobación de SNMP R1

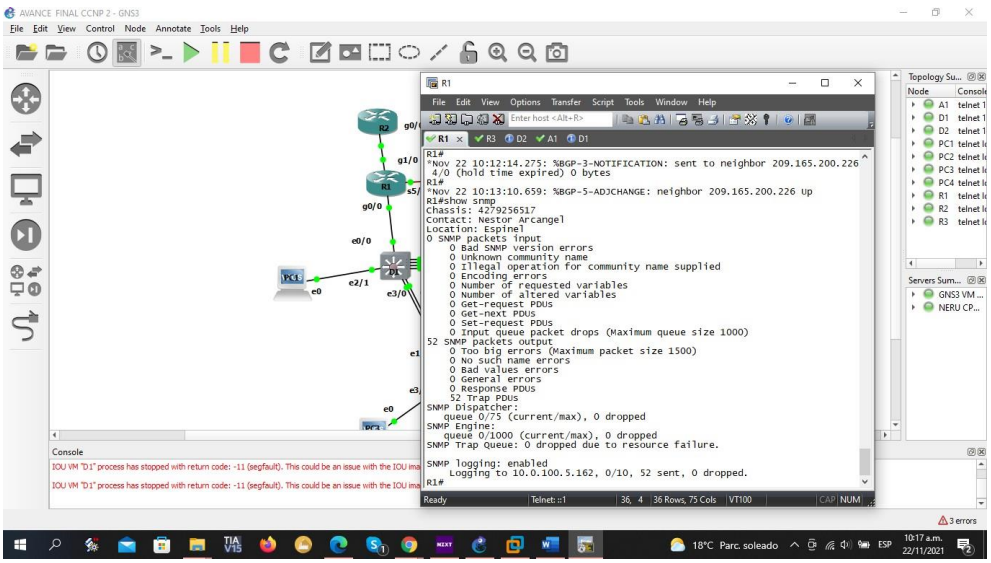


Figura 60. Comprobación de SNMP R3

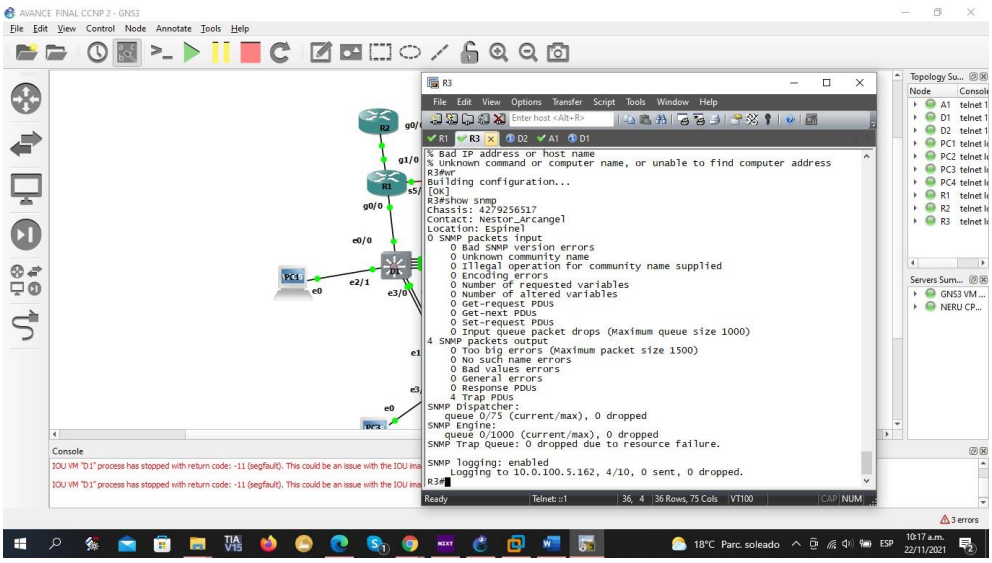


Figura 61. Comprobación de SNMP D2

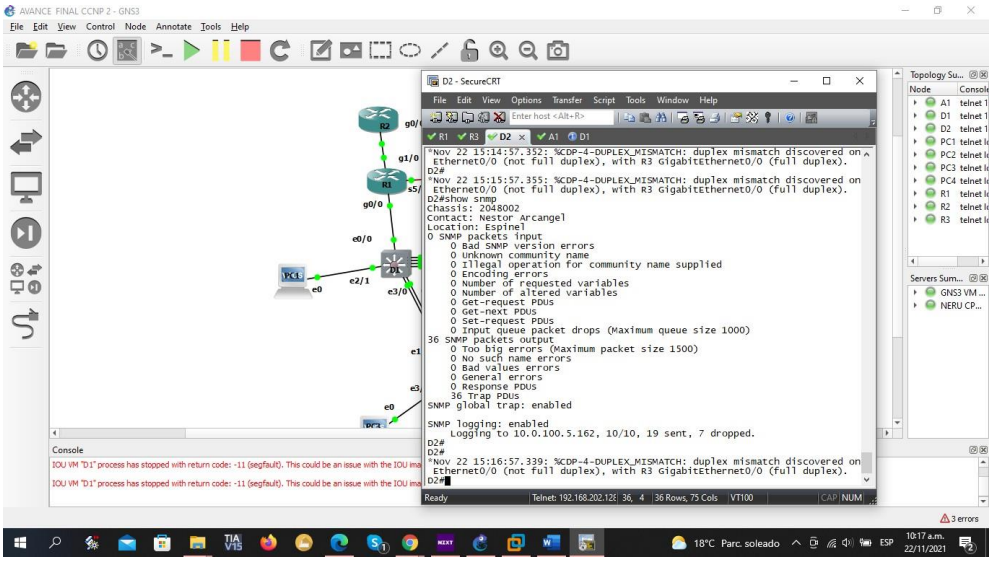


Figura 62. Comprobación de SNMP A1

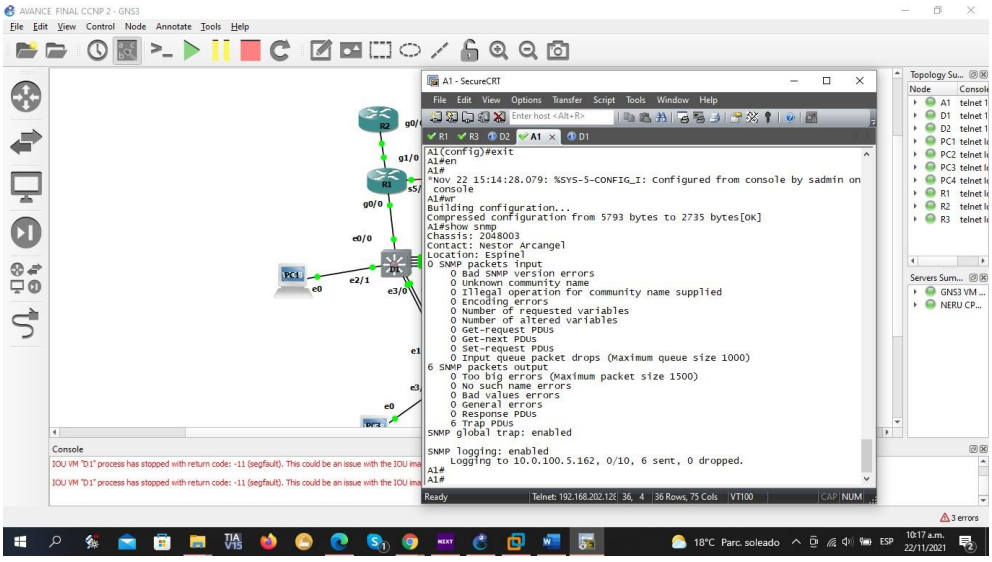
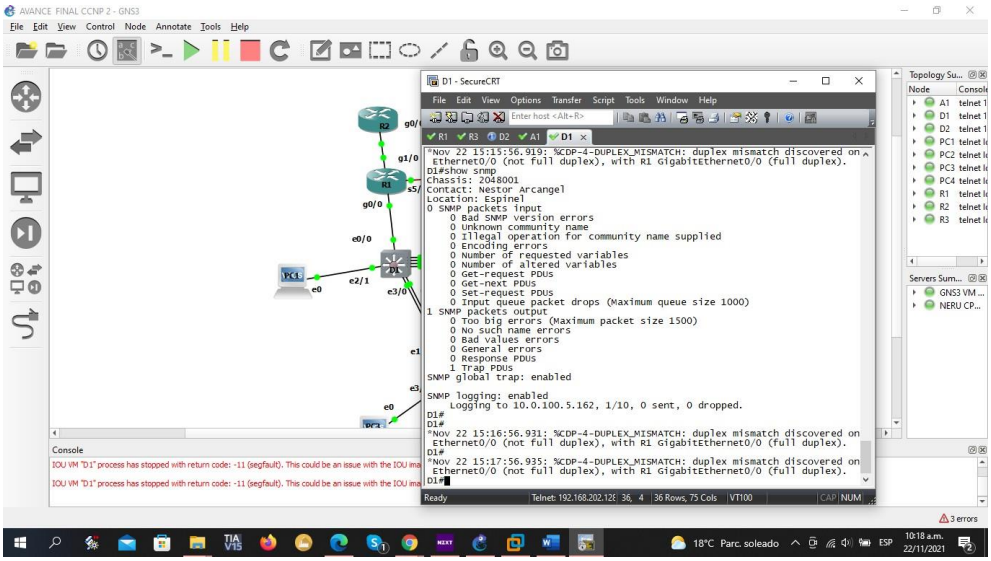


Figura 63. Comprobación de SNMP D1



CONCLUSIONES

Podemos concluir que en la realización de la actividad se presentaron algunas problemáticas respecto a la realización de la actividad ya que en el entorno donde se desarrolló “GNS3” represento todo un reto ya que este programa tiene muchas dificultades tanto al momento de realizar las configuraciones como al momento de validarlas y al momento de ser guardadas a que hay que realizar tanto la importación como la exportación de las imágenes utilizadas, lo cual en ocasiones ocasionaba fallos en el guardado.

El desarrollo de este diplomado permitió tener una mejor perspectiva frente a problemas que pueden pasar en la practica y los cuales no siempre son sencillos de solucionar gracias a lo aprendido se logro realizar múltiples configuraciones y de iguálenmela muchas formas de poder comprobar las distintas configuraciones realizadas, permitiendo de esta manera identificar de manera más precisa los posibles fallos encontrados, ser corregidos de manera satisfactoria.

Se evidencia que este tipo de programe “GNS3” permite realizar ciertas configuración que otros programas como packet tracer no perite realizarlas y de esta manera tener un mejor conocimiento del seguimiento a problemas de la red, como de igual manera se detecta ciertas desventajas el programa ya que se requiere cierto nivel de preparación del mismo para desarrollar de manera satisfactoria ciertos laboratorios que requieren de imágenes especificas debido al nivel de aceptación de ciertos comandos.

Como ultimo desde el punto de vista personal considero que por falta de mejor manejo del entorno en el cual se trabajó considero que los resultados pueden haber sido mejor en otro entorno o por el contrario con

más tiempo de preparación esto debido a que se realizó múltiples simulaciones y pruebas para encontrar los dispositivos que realmente tenían las aplicaciones necesarias para realizar las configuraciones solicitadas, teniendo encuentra la cantidad de elementos y aplicaciones que abarca este entorno de trabajo, me quedo con una satisfacción un sobresaliente ya que se logra presentar un trabajo parcial demostrando las capacidades del estudiante para enfrentarse a entornos prácticos.

BIBLIOGRÁFIA

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

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

UNAD (2017). **Configuración de Switches y Routers [OVA]**. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC