SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ANDRES FELIPE SILVA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *ELECTRONICA*
PITALITO - HUILA
2022

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ANDRES FELIPE SILVA TORRES

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

DIRECTOR:
HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA ELECTRONICA
PITALITO - HUILA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Pitalito - Huila, 15 de mayo de 2022

Agradecimientos

Quiero agradecer a Dios, a mi familia y a mis amigos por haberme guiado a lo largo de este camino de formación como persona y como ingeniero, brindándome un apoyo incondicional a la hora de tomar decisiones que fueron clave al momento de superar cada uno de los obstáculos que se me presentaron a lo largo de mi proceso formativo y contagiándome siempre de la actitud positiva y el ejemplo que me impulsó a cumplir mis objetivos.

De igual manera, quiero agradecer de manera sincera a cada uno de los docentes de la UNAD que estuvieron siempre prestos a brindarme apoyo en las dificultades académicas mostrando una actitud muy paciente y comprensiva que sacaba a la luz su amor por el campo de la enseñanza y su interés por el aprendizaje de cada uno de sus estudiantes.

Tabla de contenido

Lista de tablas

Lista de figuras

Glosario

PROTOCOLOS DE ENRUTAMIENTO: Hacen referencia a un conjunto de reglas que permiten administrar la actividad de enrutamiento en un Router de manera segura y eficaz, con el fin de compartir algún tipo de información en una red. Algunos de estos protocolos son: RIP, OSPF, BGP, EIGRP.

ROUTER: es un dispositivo que permite realizar la interconexión entre los ordenadores de la red con el fin de compartir una conexión a internet y de esta manera enviar u obtener información.

SWITCH: Es un dispositivo lógico que permite la interconexión de equipos que se encuentran conectados a una red.

VRF (Virtual Routing and Forwarding): Es un tipo de tecnología que permite a múltiples tablas de rutas separadas coexistir en el mismo router y al mismo tiempo; de esta manera, al ser todas las tablas de rutas completamente independientes, las mismas direcciones IP que pueden solapar con otras existentes, evitan conflictos y pueden convivir sin problemas.

STP (Spanning Tree Protocol): Es un protocolo de red de capa 2 que permite habilitar el algoritmo que se encarga de gestionar la presencia de bucles en una topología de enlaces redundantes; evitando de esta manera que se sature y garantizando el funcionamiento de la misma.

SUB-INTERFACE: Se definen como interfaces lógicas que nacen de la segmentación de una interfaz física; las cuales admiten una VLAN y su respectivo direccionamiento IP.

LAN: Son redes constituidas por dispositivos como Routers, Switch, Host o servidores; que se encargan de intercambiar datos y compartir recursos entre los usuarios de la red. Estas redes pueden ser de carácter empresarial o doméstico.

VLAN: Son conocidas como redes de área local virtuales; es una tecnología de red que permite crear redes lógicas dentro de una misma red física, garantizando de esta manera que el tráfico de información sea seguro entre cada subred creada.

Resumen

En el presente documento se muestra el desarrollo del escenario práctico correspondiente al diplomado de profundización CISCO – CCNP; el cual, se encuentra conformado por una topología de red configurada en el software GNS3 que admite dos tipos de usuario (Usuario general y Usuario especial); permitiendo de esta manera generar habilidades para la configuración y el manejo de redes de área local de tipo doméstico o empresarial.

No obstante, se evidencia el manejo de comandos IOS para la configuración de dispositivos como Routers y Switches dentro de la red, con el fin de garantizar la conectividad entre cada una de las interfaces que la conforman; de igual manera, se muestra el proceso para llevar a cabo el direccionamiento IPv4 e IPv6 y la creación de las VRF incluyendo VLAN, rutas estáticas y encapsulamiento de datos para cada uno de los tipos de usuario. Además, se implementará la configuración de capa 2 para puntos de acceso y configuración de seguridad para restringir el acceso de cada tipo de usuario.

Durante el proceso de construcción y configuración de la red se mostrarán elementos como tablas, códigos digitados y capturas de pantalla que evidencien el proceso realizado para llegar al producto final.

Palabras clave: Electrónica, CCNP, CISCO, Topología, Red, Enrutamiento, VRF, Seguridad, Interfaces.

Abstract

This document shows the development of the practical scenario corresponding to the deepening diploma course CISCO - CCNP; which is made up of a network topology configured in the GNS3 software that supports two types of user (General User and Special User); allowing in this way to generate skills for the configuration and management of local area networks of a domestic or business type.

However, the management of IOS commands for the configuration of devices such as Routers and Switches within the network is evident, in order to guarantee connectivity between each of the interfaces that make it up; Likewise, the process to carry out IPv4 and IPv6 addressing and the creation of VRFs including VLANs, static routes and data encapsulation for each of the user types is shown. In addition, layer 2 settings for access points and security settings will be implemented to restrict access for each type of user.

During the process of building and configuring the network, elements such as tables, typed codes and screenshots will be shown that show the process carried out to reach the final product.

Keywords: CCNP, CISCO, Topology, Network, Routing, VRF, Security, Interfaces.

Introducción

Actualmente la transmisión de información a partir de redes de área local ha permitido facilitar el rendimiento de muchas áreas productivas y empresariales; permitiendo de esta manera generar nuevas formas para compartir, almacenar y proteger datos de carácter importante. El presente documento muestra el desarrollo del escenario práctico propuesto como trabajo final para la aprobación del Diplomado de Profundización CISCO CCNP; en el cual se evidencia la construcción de la topología de red que maneja dos tipos de usuario: usuario general y usuario especial; así como la configuración básica de cada uno de sus dispositivos, la configuración de las respectivas VRF, la configuración de capa 2 y la seguridad para la restricción según el tipo de usuario.

Cada una de las 6 etapas desarrolladas durante el escenario práctico han permitido desarrollar distintos tipos de habilidades relacionadas con el manejo de redes LAN de tipo doméstico y empresarial. La configuración básica de cada uno de los dispositivos administrables se realizó a partir de comandos IOS avanzados que permitieron crear redes virtuales locales para transmitir la información entre los usuarios; de igual manera, la configuración VRF permitió garantizar la conectividad entre los router para dar paso a la configuración de capa 2 y el establecimiento del protocolo de seguridad para restringir el acceso a cada una de las interfaces de usuario.

El escenario se desarrolló en el software GNS3 haciendo uso de imágenes de Router y Switch que permitieron la configuración y correcta ejecución de la simulación de la red.

Desarrollo

Topología de la red a implementar:

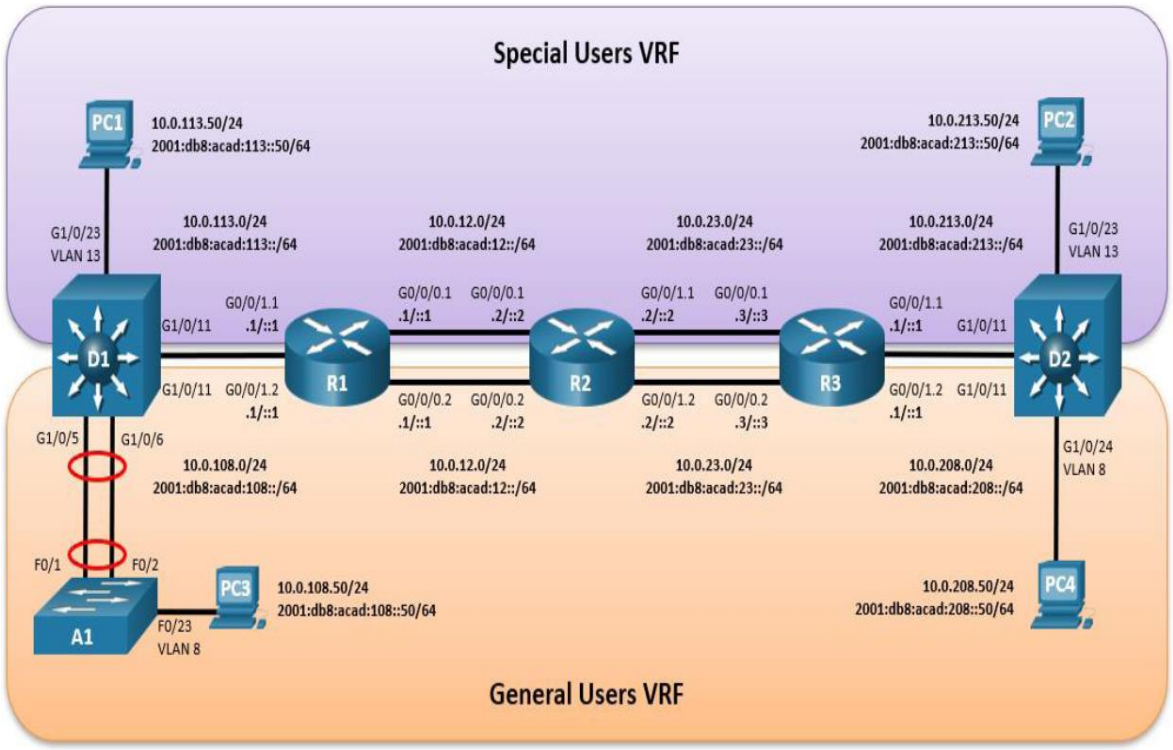


Ilustración 1, Topología a implementar de la red.

Fuente: Guía prueba de habilidades CCNP

Tabla de direccionamiento:

Tabla 1. Tabla de direccionamiento de dispositivos.
Fuente: Guía prueba de habilidades CCNP

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1 *R1 R1 R1*	G0/0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G0/0/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G0/0/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2 *R2 R2 R2*	G0/0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G0/0/1.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G0/0/1.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
R3	G0/0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
R3	G0/0/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
R3	G0/0/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

Objetivos

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.

Parte 2: Configurar VRF y rutas estáticas.

Parte 3: Configurar Capa 2(se entrega finalizado el paso 6).

Parte 4: Configurar seguridad (se entrega finalizado el paso 6).

Escenario

En esta evaluación de habilidades, usted es responsable de completar la configuración multi-VRF de la red que admite "Usuarios generales" y "Usuarios especiales". Una vez finalizado, debería haber accesibilidad completa de un extremo a otro y los dos grupos no deberían poder comunicarse entre sí. Asegúrese de verificar que sus configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

Nota: Se sugiere realizar la topología en el software GNS3, teniendo en cuenta las siguientes imágenes ISO que se encuentran en el siguiente link:

Instrucciones

Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz
En la Parte 1, configurará la topología de la red y configurará los ajustes básicos.

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

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

A continuación, se estructura la topología sugerida en el software GNS3.

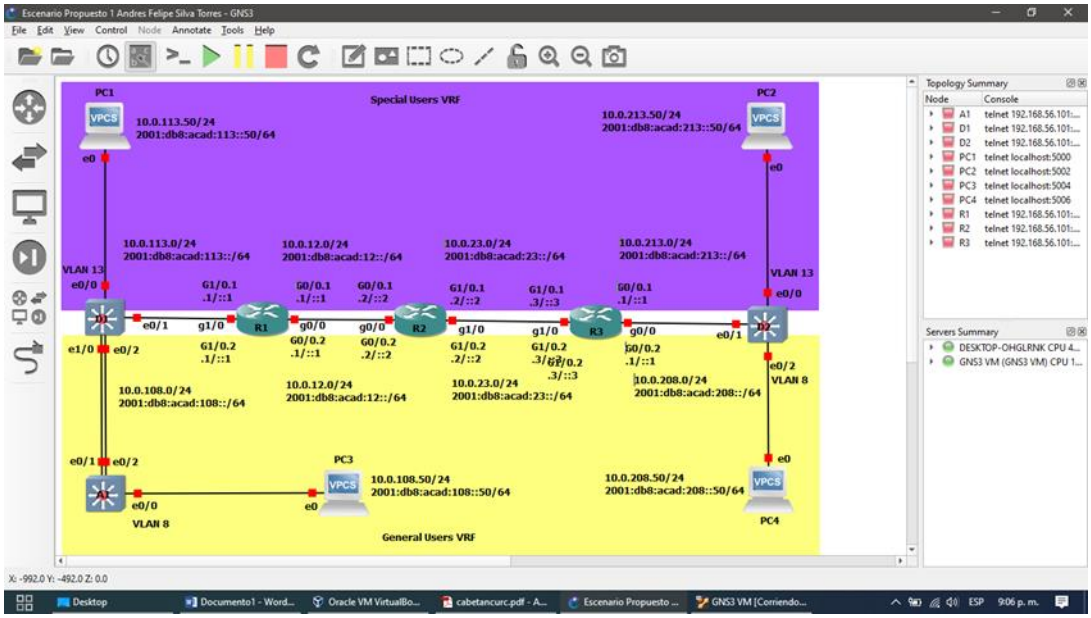


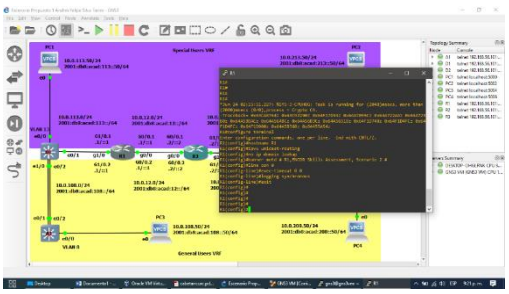
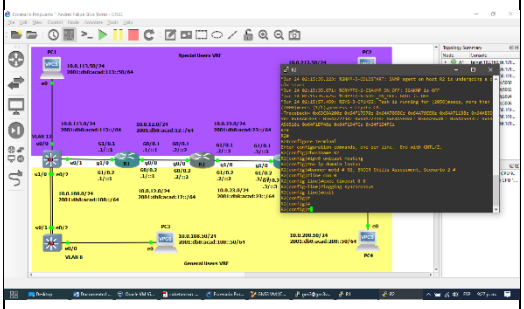
Ilustración 2, Topología de la red en el software GNS3

Fuente: Autor

Paso 2: Configure los ajustes básicos para cada dispositivo.

a. Ingrese al modo de configuración global en cada uno de los dispositivos y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Tabla 2, Configuracion básica Routers.
Fuente: Autor.

Router R1 hostname R1 ipv6 unicast-routing no ip domain lookup banner motd # R1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit	 *Ilustración 3, configuracion básica R1* *Fuente: Autor*
Router R2 hostname R2 ipv6 unicast-routing no ip domain lookup banner motd # R2, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit	 *Ilustración 4, Configuración Básica R2.* *Fuente: Autor.*

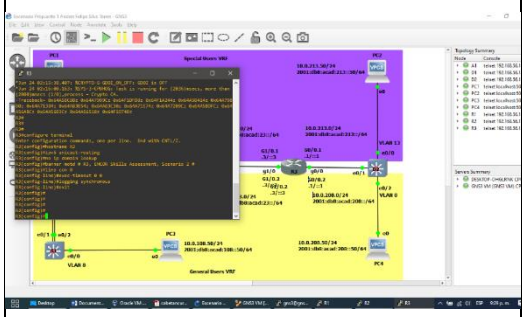
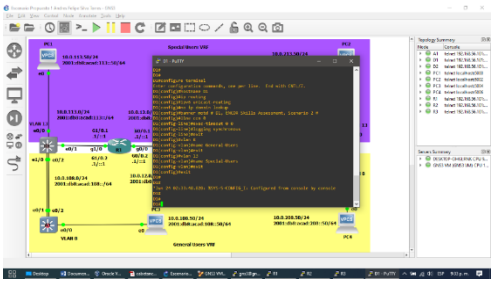
Router R3 hostname R3 ipv6 unicast-routing no ip domain lookup banner motd # R3, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit	 *Ilustración 5, Configuración básica R3. Fuente: Autor*

Tabla 3, Configuración básica Switches. Fuente: Autor.

Switch D1 hostname D1 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit vlan 13 name Special-Users exit	 *Ilustración 6, Configuración básica D1. Fuente: Autor.*

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
 logging synchronous
 exit
vlan 8
 name General-Users
 exit
vlan 13
 name Special-Users
 exit
```

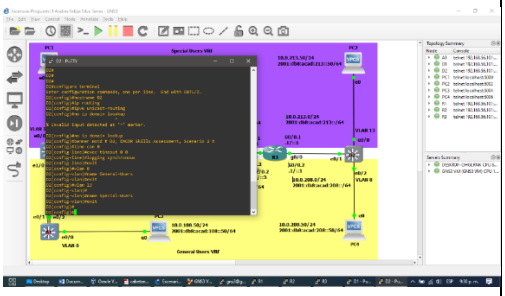


Ilustración 7,Configuración básica D2. Fuente: Autor.

Switch A1

```
hostname A1
ipv6 unicast-routing
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
vlan 8
 name General-Users
 exit
```

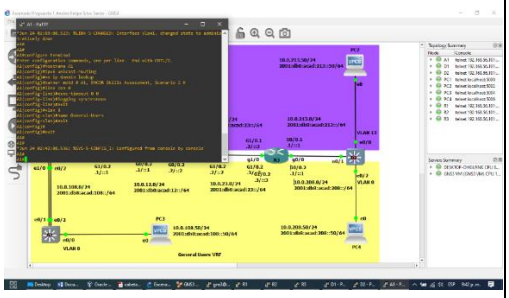
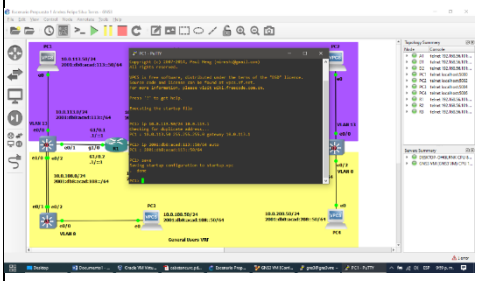
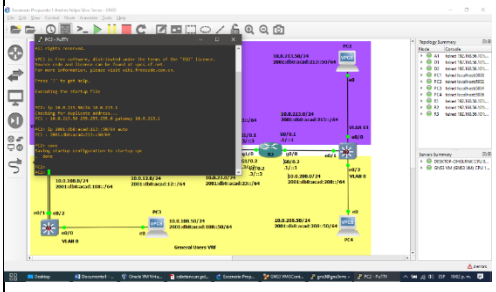
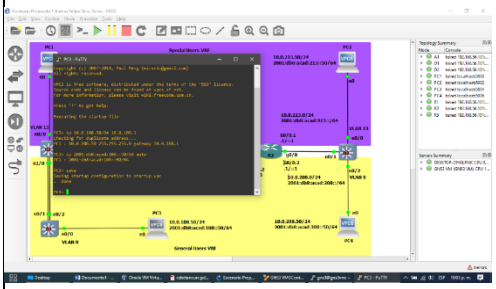


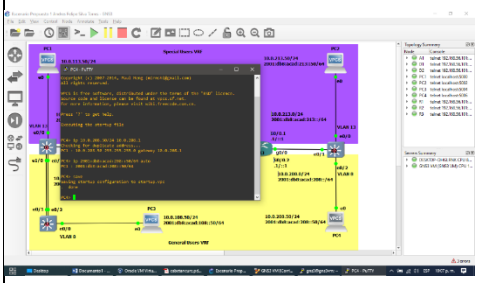
Ilustración 8, Configuración básica A1. Fuente: Autor.

b. Guarde las configuraciones en cada uno de los dispositivos.

c. c. Configure los PC1, PC2, PC3 y PC4 de acuerdo con la tabla de direccionamiento.

Tabla 4, Configuración básica PCs.
Fuente: Autor.

PC1 ip 10.0.113.50/24 10.0.113.1 ip 2001:db8:acad:113::50/64 auto save	 *Ilustración 9, Configuración PC1. Fuente:Autor*
PC2 ip 10.0.213.50/24 10.0.213.1 ip 2001:db8:acad:213::50/64 auto save	 *Ilustración 10, Configuración PC2. Fuente:Autor.*
PC3 ip 10.0.108.50/24 10.0.108.1 ip 2001:db8:acad:108::50/64 auto save	 *Ilustración 11, Configuracion PC3. Fuente: Autor.*

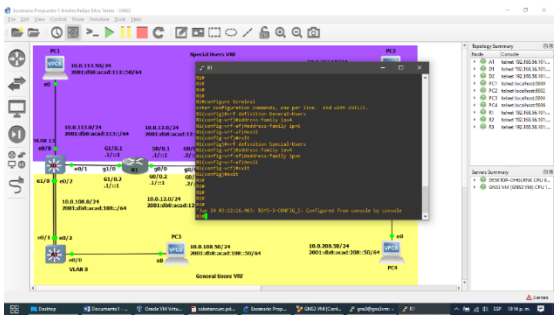
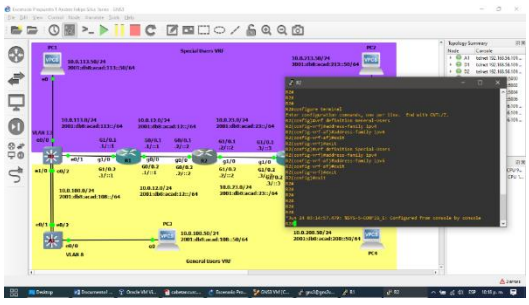
PC4 ip 10.0.208.50/24 10.0.208.1 ip 2001:db8:acad:208::50/64 auto save	 *Ilustración 12, Configuración PC4. Fuente: Autor.*

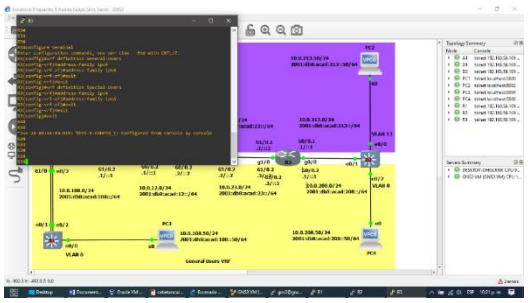
Parte 2: configurar VRF y enrutamiento estático

2.1. Configuración VRF-Lite y VRFs en los Routers.

Task#	Task	Specification
2.1	On R1, R2, and R3, configure VRF-Lite VRFs as shown in the topology diagram.	Configure two VRFs: General-Users Special-Users The VRFs must support IPv4 and IPv6.

Tabla 5, Configuración VRF routers.
Fuente: Autor.

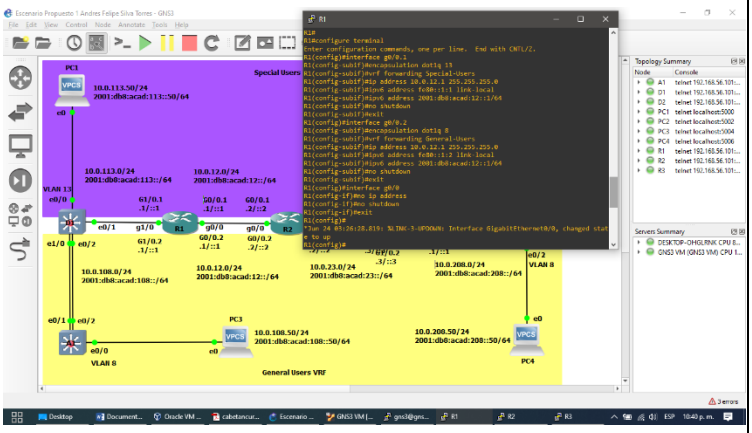
R1 vrf definition General-Users address-family ipv4 address-family ipv6 exit vrf definition Special-Users address-family ipv4 address-family ipv6 exit	 *Ilustración 13, Configuración VRF R1.* *Fuente: Autor.*
R2 vrf definition General-Users address-family ipv4 address-family ipv6 exit vrf definition Special-Users address-family ipv4 address-family ipv6 exit	 *Ilustración 14, Configuración VRF R2.* *Fuente:Autor.*

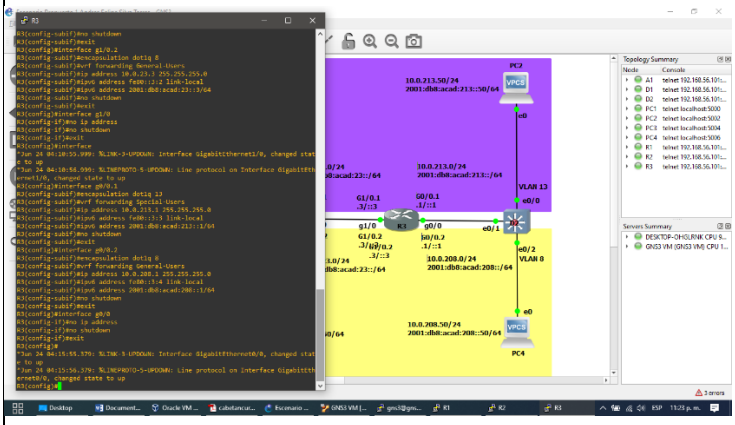
R3 vrf definition General-Users address-family ipv4 address-family ipv6 exit vrf definition Special-Users address-family ipv4 address-family ipv6 exit	 *Ilustración 15, Configuración VRF R3. Fuente:Autor.*

2.2. Configuración de las interfaces IPv4 y IPv6 en los Routers.

Task#	Task	Specification
2.2	On R1, R2, and R3, configure IPv4 and IPv6 interfaces on each VRF as detailed in the addressing table above.	All routers will use Router-On-A-Stick on their G0/0/1.x interfaces to support separation of the VRFs. Sub-interface 1: In the Special Users VRF Use dot1q encapsulation 13 IPv4 and IPv6 GUA and link-local addresses Enable the interfaces Sub-interface 2: In the General Users VRF Use dot1q encapsulation 8 IPv4 and IPv6 GUA and link-local addresses Enable the interfaces

Tabla 6, Configuración IPv6 e IPv4 Routers.
Fuente: Autor.

R1 interface g0/0.1 encapsulation dot1q 13 vrf forwarding Special-Users ip address 10.0.12.1 255.255.255.0 ipv6 address fe80::1:1 link-local ipv6 address 2001:db8:acad:12::1/64 no shutdown exit interface g0/0 no ip address no shutdown exit interface g1/0.1 encapsulation dot1q 13 vrf forwarding Special-Users ip address 10.0.113.1 255.255.255.0 ipv6 address fe80::1:3 link-local ipv6 address 2001:db8:acad:113::1/64 no shutdown exit interface g1/0.2 encapsulation dot1q 8 vrf forward General-Users ip address 10.0.108.1 255.255.255.0 ipv6 address fe80::1:4 link-local	 *Ilustración 16, Configuración IPv4 e IPv6 R1.* *Fuente: Autor.*

ipv6 address 2001:db8:acad:108::1/64 no shutdown exit interface g1/0 no ip address no shutdown exit	
R2 interface g0/0.1 encapsulation dot1q 13 vrf forwarding Special-Users ip address 10.0.12.2 255.255.255.0 ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:acad:12::2/64 no shutdown exit interface g0/0.2 encapsulation dot1q 8 vrf forwarding General-Users ip address 10.0.12.2 255.255.255.0 ipv6 address fe80::2:2 link-local ipv6 address 2001:db8:acad:12::2/64 no shutdown exit interface g0/0 no ip address no shutdown exit	 *Ilustración 17, Configuración IPv4 e IPv6 R2.* *Fuente: Autor.*

interface g1/0.1
  encapsulation dot1q 13
  vrf forwarding Special-Users
  ip address 10.0.23.2 255.255.255.0
  ipv6 address fe80::2:3 link-local
  ipv6 address 2001:db8:acad:23::2/64
  no shutdown
  exit
interface g1/0.2
  encapsulation dot1q 8
  vrf forwarding General-Users
  ip address 10.0.23.2 255.255.255.0
  ipv6 address fe80::2:4 link-local
  ipv6 address 2001:db8:acad:23::2/64
  no shutdown
  exit
interface g1/0
  no ip address
  no shutdown
exit	

interface g1/0.1
  encapsulation dot1q 13
  vrf forwarding Special-Users
  ip address 10.0.23.3 255.255.255.0
  ipv6 address fe80::3:1 link-local
  ipv6 address 2001:db8:acad:23::3/64	

no shutdown exit interface g1/0.2 encapsulation dot1q 8 vrf forwarding General-Users ip address 10.0.23.3 255.255.255.0 ipv6 address fe80::3:2 link-local ipv6 address 2001:db8:acad:23::3/64 no shutdown exit interface g1/0 no ip address no shutdown exit interface g0/0.1 encapsulation dot1q 13 vrf forwarding Special-Users ip address 10.0.213.1 255.255.255.0 ipv6 address fe80::3:3 link-local ipv6 address 2001:db8:acad:213::1/64 no shutdown exit interface g0/0.2 encapsulation dot1q 8 vrf forward General-Users ip address 10.0.208.1 255.255.255.0 ipv6 address fe80::3:4 link-local	

ipv6 address 2001:db8:acad:208::1/64 no shutdown exit interface g0/0 no ip address no shutdown exit	

2.3. Configuración rutas estáticas predeterminadas que dirigen a los Routers.

Task#	Task	Specification
2.3	On R1 and R3, configure default static routes pointing to R2.	Configure VRF static routes for both IPv4 and IPv6 in both VRFs.

Tabla 7, Configuracion rutas estáticas routers.

Fuente: Autor.

```
R1
  ip route vrf Special-
  Users 0.0.0.0
  0.0.0.0 10.0.12.2
   ip route vrf General-
  Users 0.0.0.0
  0.0.0.0 10.0.12.2
   ipv6 route vrf Special-
  Users ::/0
  2001:db8:acad:12::2
   ipv6 route vrf General-
  Users ::/0
  2001:db8:acad:12::2
   end
```

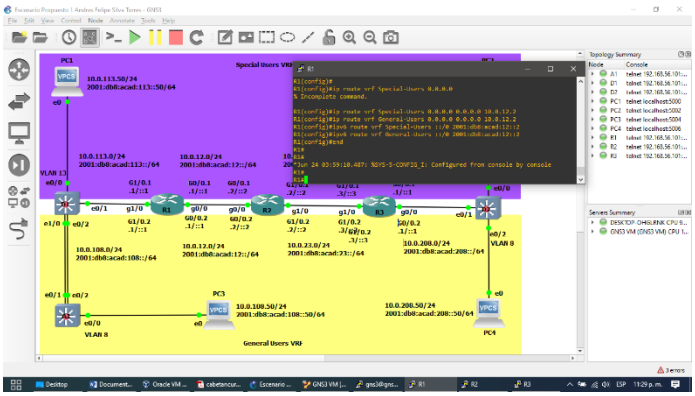


Ilustración 18, Rutas estáticas R1.

Fuente: Autor.

```
R2
 ip route vrf Special-
Users 10.0.113.0
255.255.255.0
10.0.12.1
 ip route vrf Special-
Users 10.0.213.0
255.255.255.0
10.0.23.3
 ipv6 route vrf Special-
Users
2001:db8:acad:113::/64
2001:db8:acad:12::1
 ipv6 route vrf Special-
Users
2001:db8:acad:213::/64
2001:db8:acad:23::3
 ip route vrf General-
Users 10.0.108.0
255.255.255.0
10.0.12.1
 ip route vrf General-
Users 10.0.208.0
255.255.255.0
10.0.23.3
 ipv6 route vrf General-
Users
2001:db8:acad:108::/64
2001:db8:acad:12::1
 ipv6 route vrf General-
Users
2001:db8:acad:208::/64
2001:db8:acad:23::3
 end
```

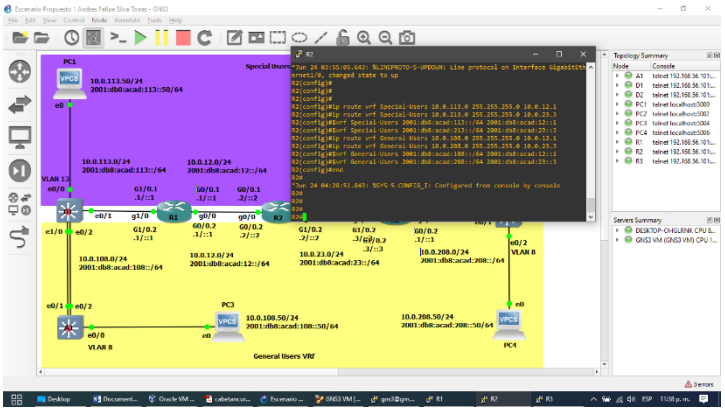
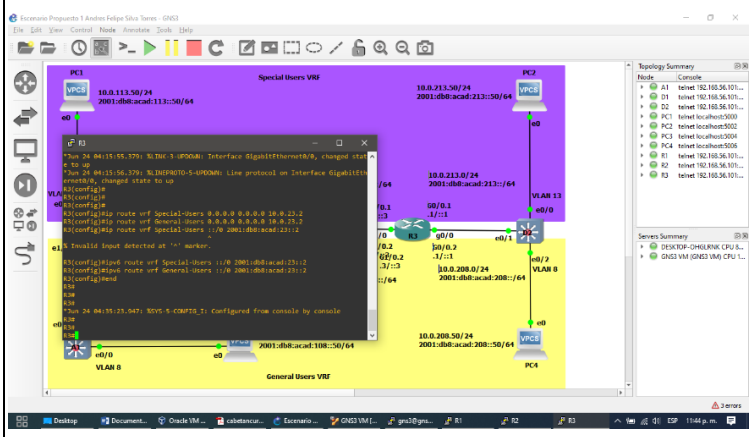


Ilustración 19, Rutas estáticas R2.

Fuente: Autor.

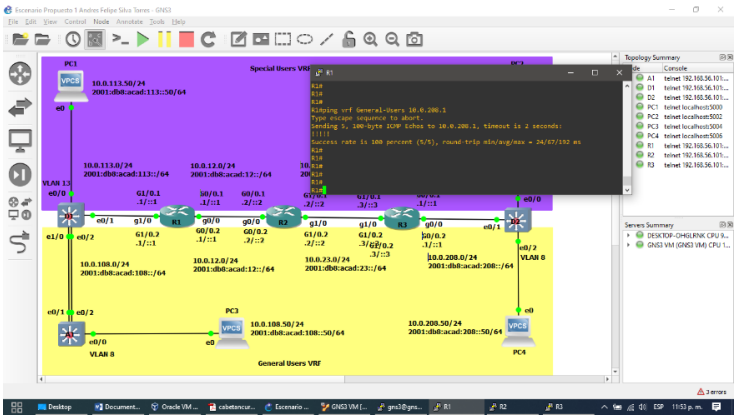
R3 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2 ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2 ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2 ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2 end	 *Ilustración 20, Rutas estáticas R3.* *Fuente: Autor.*

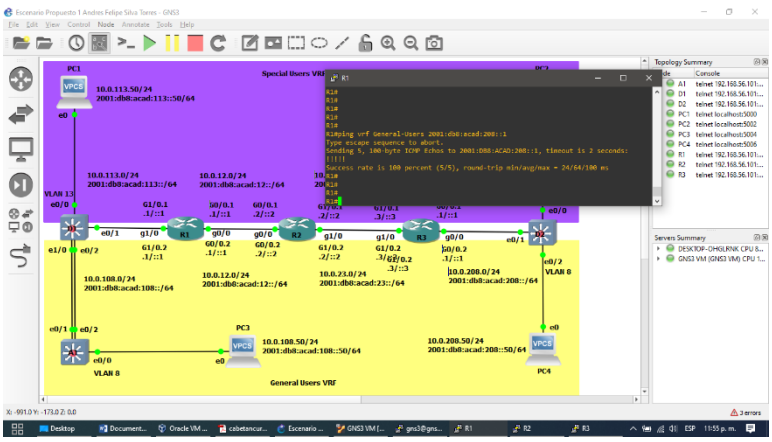
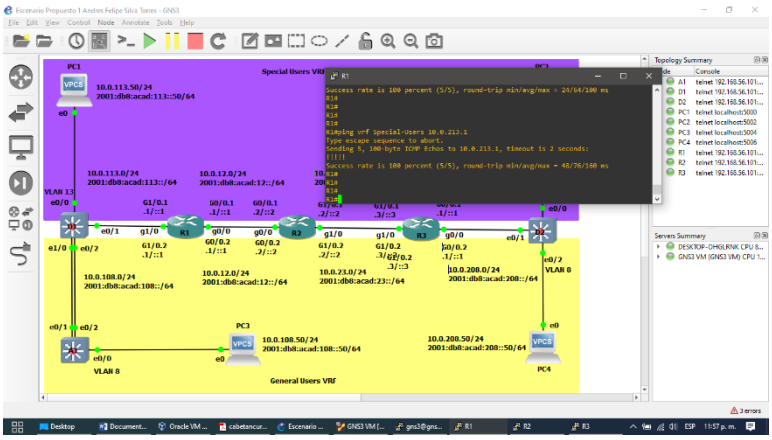
2.4. Verificar conectividad en cada VRF.

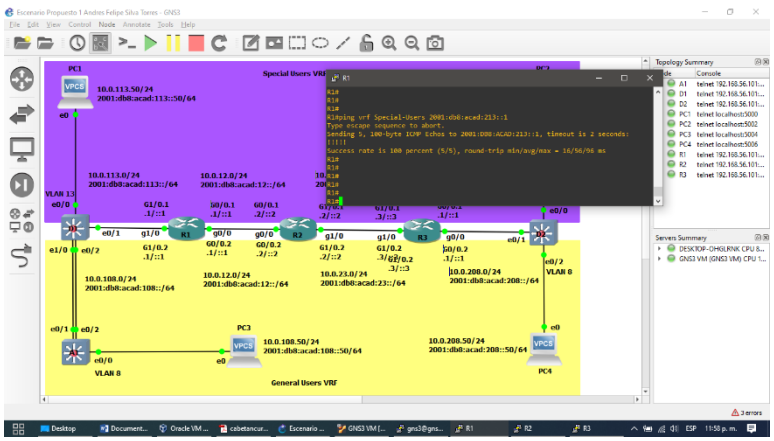
Task#	Task	Specification
2.4	Verify connectivity in each VRF.	From R1, verify connectivity to R3: ping vrf General-Users 10.0.208.1 ping vrf General-Users 2001:db8:acad:208::1 ping vrf Special-Users 10.0.213.1 ping vrf Special-Users 2001:db8:acad:213::1

Tabla 8, Verificación de conectividad VRF.

Fuente: Autor.

R1 Ping vrf General-Users 10.0.208.1	 *Ilustración 21, Verificación VRF R1 - General Users.* *Fuente: Autor*

R1 Ping vrf General-Users 2001:db8:acad:208::1	 *Ilustración 22, Verificación VRF IPv6 R1 - General Users.* *Fuente: Autor.*
R1 Ping vrf Special-Users 10.0.213.1	 *Ilustración 23, Verificación VRF R1 - Special users.* *Fuente: Autor.*

R1 Ping vrf Special-Users 2001:db8:acad:213::1	 *Ilustración 24, Verificación VRF R1 - Special Users IPv6.* *Fuente: Autor.*

Parte 3. Configurar Capa 2

3.1. Deshabilitar las interfaces en los Switch.

Task#	Task	Specification
3.1	On D1, D2, and A1, disable all interfaces.	On D1 and D2, shutdown G1/0/1 to G1/0/24. On A1, shutdown F0/1 – F0/24, G0/1 – G0/2.

Tabla 9, Deshabilitación de las interfaces de los switch.

Fuente: Autor.

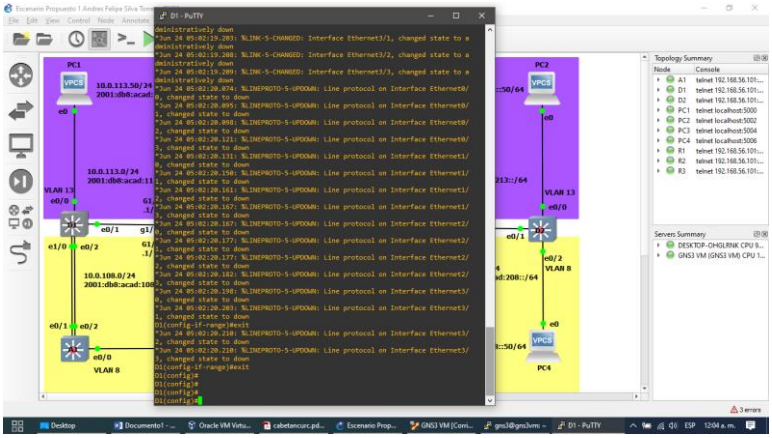
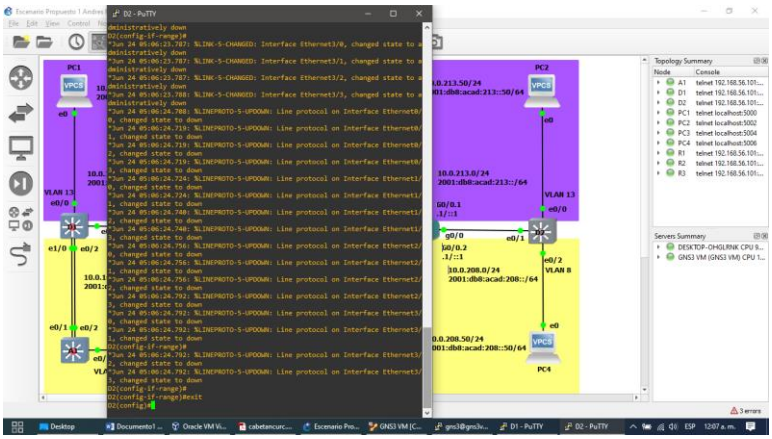
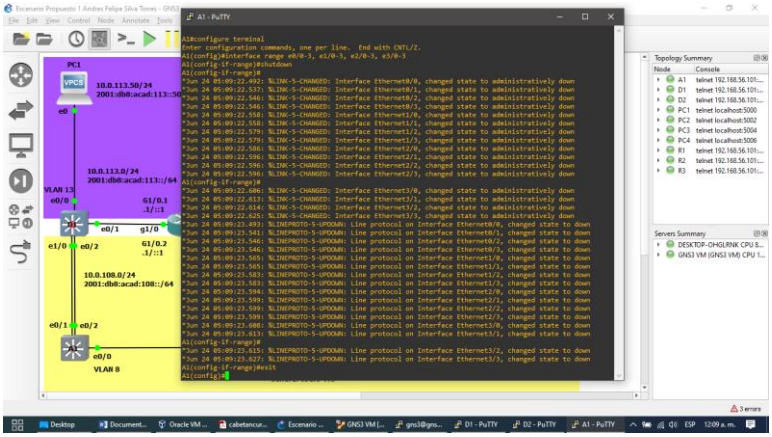
D1 interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	

Ilustración 25, Deshabilitación interfaces D1.

Fuente: Autor.

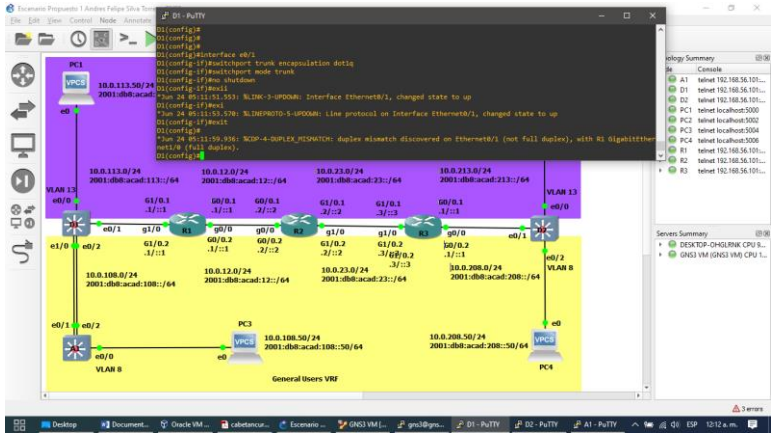
D2 interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	 *Ilustración 26, Deshabilitación interfaces D2.* *Fuente: Autor.*
A1 interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 shutdown exit	 *Ilustración 27, Deshabilitación interfaces D3.* *Fuente: Autor.*

3.2. Configuración de los enlaces troncales a los Routers 1 y 3 en los Switch 1 y 2.

Task#	Task	Specification
3.2	On D1 and D2, configure the trunk links to R1 and R3.	Configure and enable the G1/0/11 link as a trunk link.

Tabla 10, Configuración enlaces troncales.

Fuente: Autor.

D1 interface e0/1 switchport trunk encapsulation dot1q switchport mode trunk no shutdown exit	 *Ilustración 28, Enlaces troncales D1.* *Fuente: Autor.*

D2

interface e0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

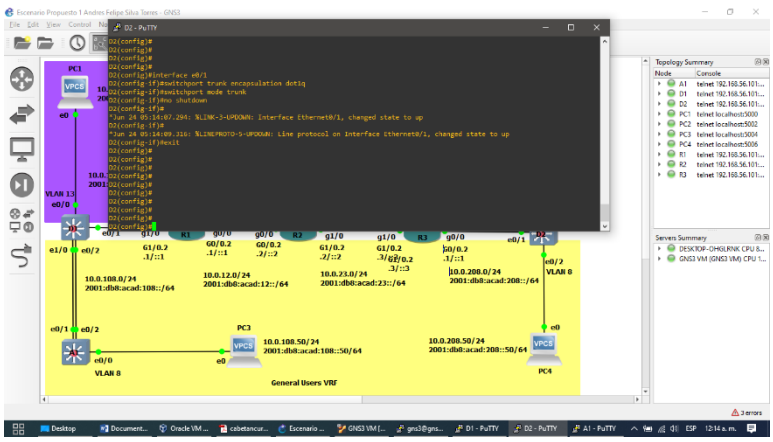


Ilustración 29, Configuración enlaces troncales D2.

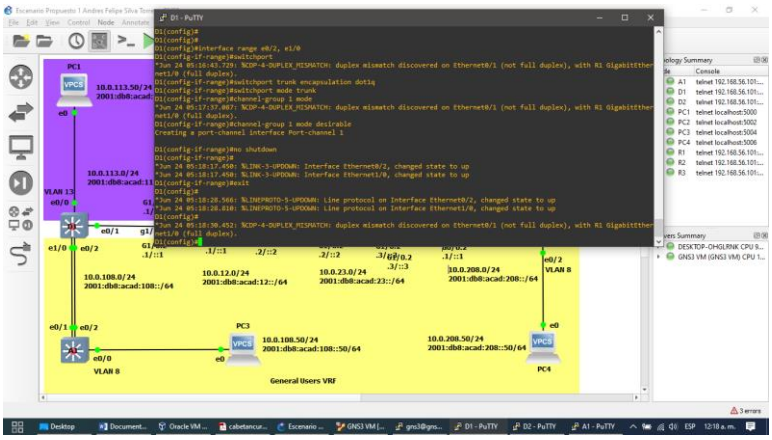
Fuente: Autor.

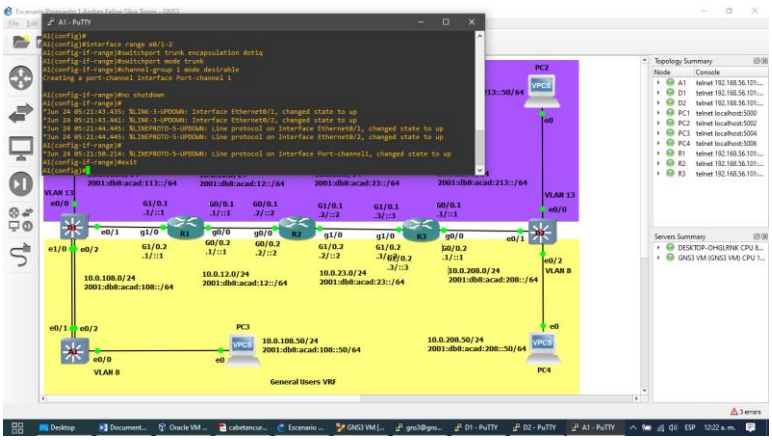
3.3. Configuración del EtherChannel en los Switch.

Task#	Task	Specification
3.3	On D1 and A1, configure the EtherChannel.	On D1, configure and enable: Interface G1/0/5 and G1/0/6 Port Channel 1 using PAgP On A1, configure enable: Interface F0/1 and F0/2 Port Channel 1 using PAgP

Tabla 11, Configuración EtherChannel switch.

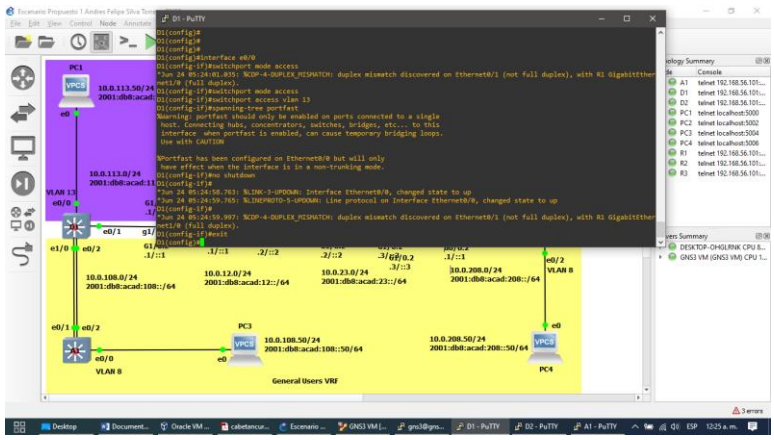
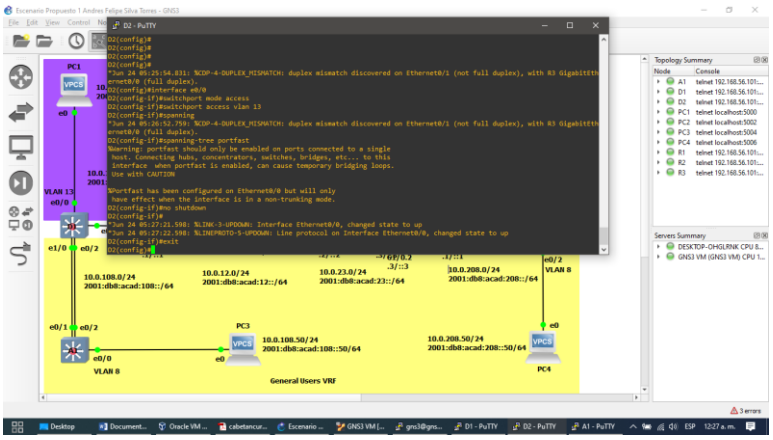
Fuente: Autor.

D1 interface range e0/2, e1/0 switchport trunk encapsulation dot1q switchport mode trunk channel-group 1 mode desirable no shutdown exit	 *Ilustración 30, EtherChannel D1.* *Fuente: Autor.*

A1 interface range e0/1-2 switchport trunk encapsulation dot1q switchport mode trunk channel-group 1 mode desirable no shutdown exit	 *Ilustración 31, EtherChannel A1.* *Fuente: Autor.*

3.4. Configuración puertos de acceso de los PCs en los Switch.

Task#	Task	Specification
3.4	On D1, D2, and A1, configure access ports for PC1, PC2, PC3, and PC4.	Configure and enable the access ports as follows: On D1, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast. On D2, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast. On D2, configure interface G1/0/24 as an access port in VLAN 8 and enable Portfast. On A1, configure interface F0/23 as an access port in VLAN 8 and enable Portfast.

D1 interface e0/0 switchport mode access switchport access vlan 13 spanning-tree portfast no shutdown exit	 *Ilustración 32, Puertos de acceso PCs D1.* *Fuente: Autor.*
D2 interface e0/0 switchport mode access switchport access vlan 13 spanning-tree portfast no shutdown exit interface e0/2 switchport mode access switchport access vlan 8 spanning-tree portfast no shutdown exit	 *Ilustración 33, Puertos de acceso PCs D2.* *Fuente: Autor.*

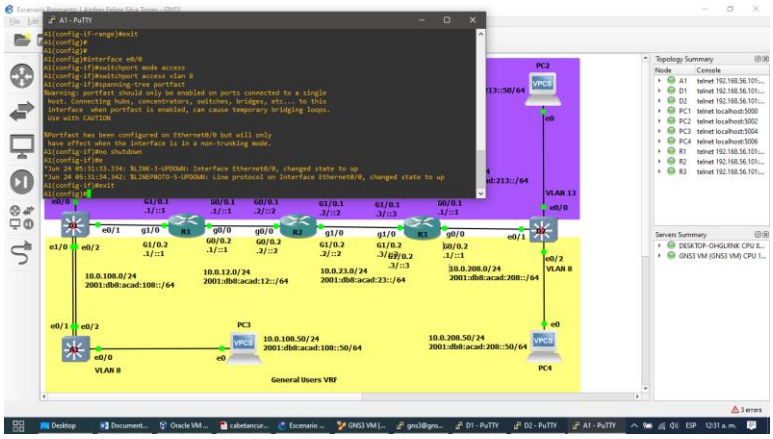
A1 interface e0/0 switchport mode access switchport access vlan 8 spanning-tree portfast no shutdown exit	 *Ilustración 34, Puertos de acceso PCs A1.* *Fuente: Autor.*

Ilustración 35, Configuración puertos de acceso de los PCs en los Switch.

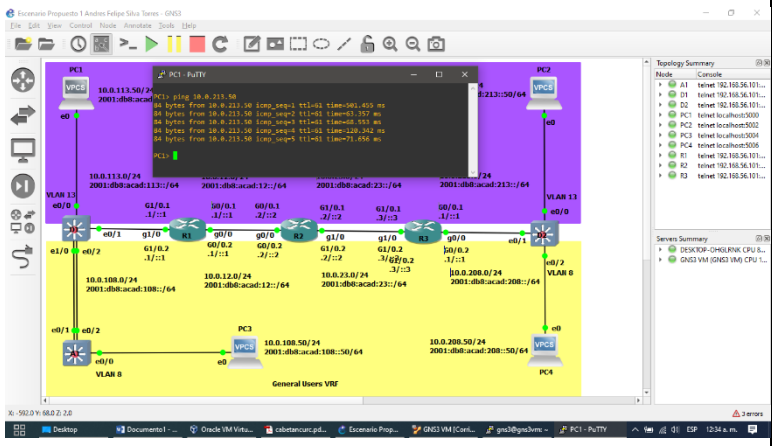
Fuente: Autor.

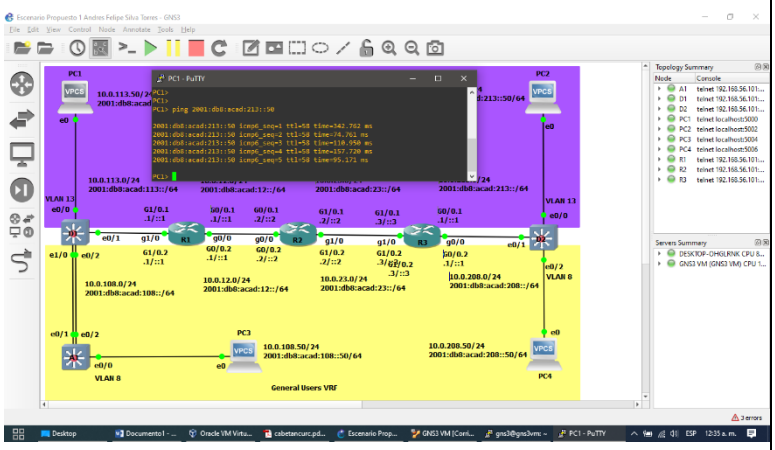
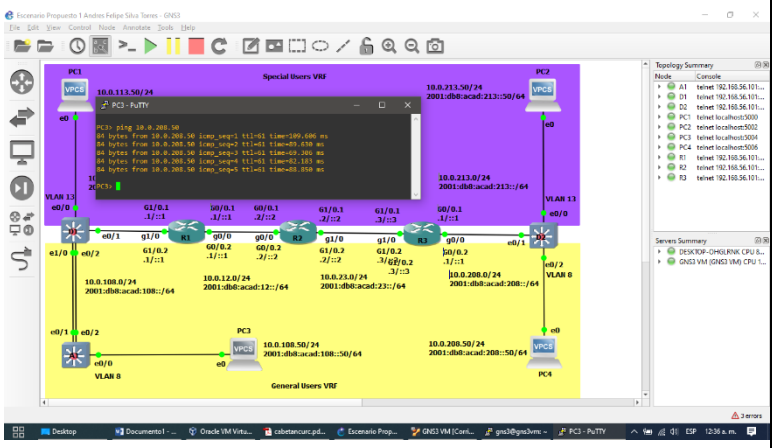
3.5. Verificación de la conectividad IPv4 a IPv6 de PC a PC del VRF Special Users.

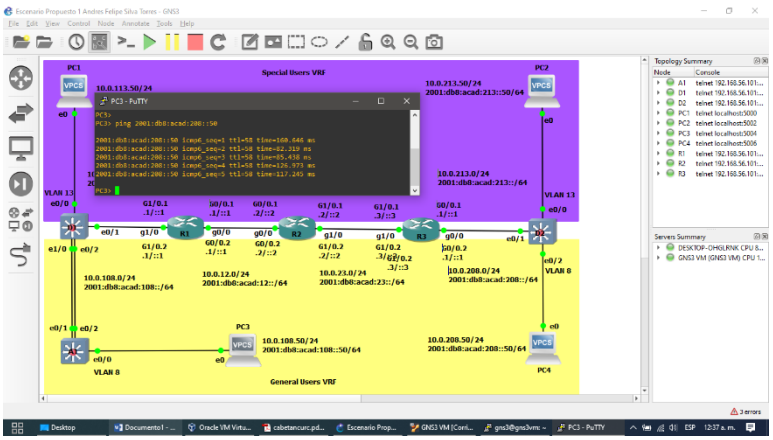
Task#	Task	Specification
3.5	Verify PC to PC connectivity.	From PC1, verify IPv4 and IPv6 connectivity to PC2. From PC3, verify IPv4 and IPv6 connectivity to PC4.

Tabla 12,Verificación de conectividad PC - PC.

Fuente: Autor.

PC1 a PC2 Ping 10.0.213.50	 *Ilustración 36, Ping PC1 - PC2.* *Fuente: Autor.*

PC1 a PC2 Ping 2001:db8:acad:213::50	 *Ilustración 37, Ping PC1 -- PC2 IPv6.* *Fuente: Autor.*
PC3 a PC4 Ping 10.0.208.50	 *Ilustración 38, Ping PC3 - PC4.* *Fuente: Autor.*

PC3 a PC4 Ping 2001:db8:acad:208::50	 *Ilustración 39, Ping PC3 - PC4 IPv6.* *Fuente: Autor.*

Parte 4. Configure Security

4.1. Configuración de seguridad privilegiada en modo EXE en los dispositivos.

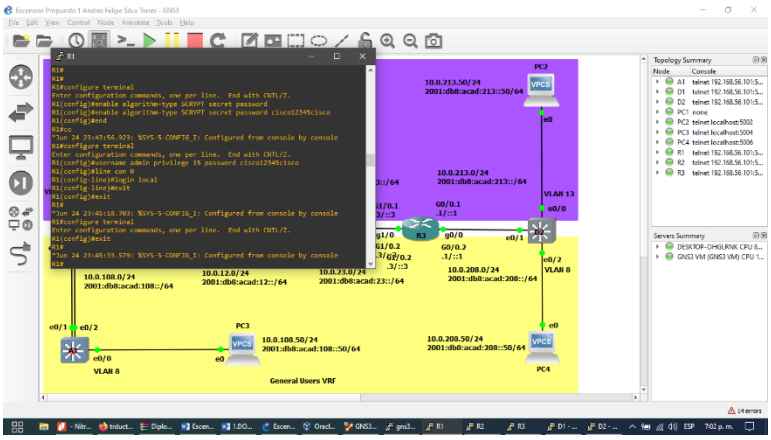
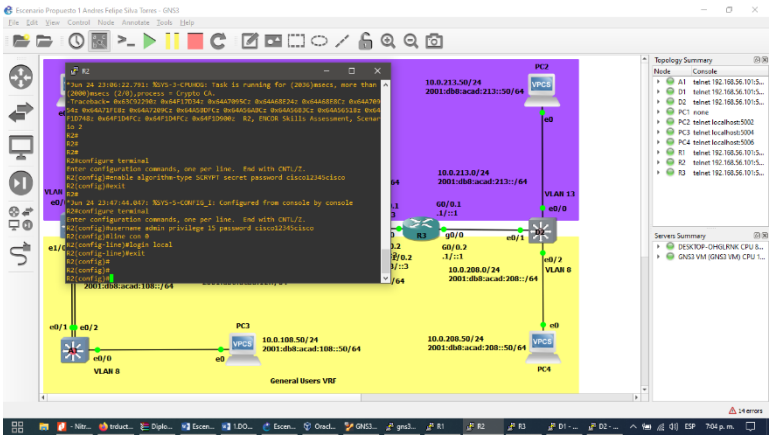
Task#	Task	Specification
4.1	On all devices, secure privileged EXE mode.	Configure an enable secret as follows: Algorithm type: **SCRYPT** Password: **cisco12345cisco**.

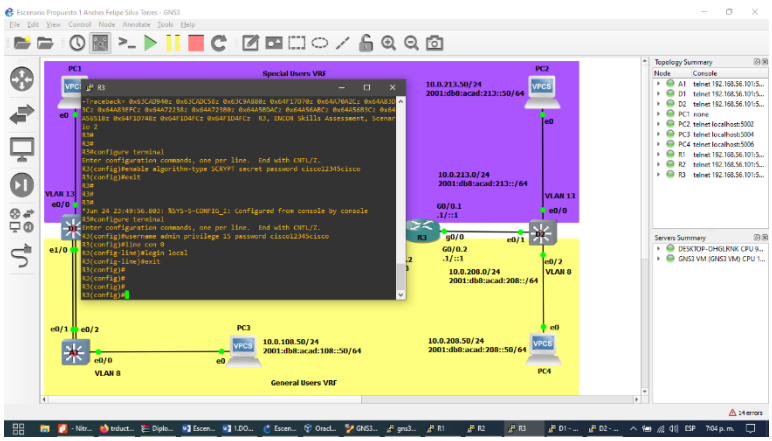
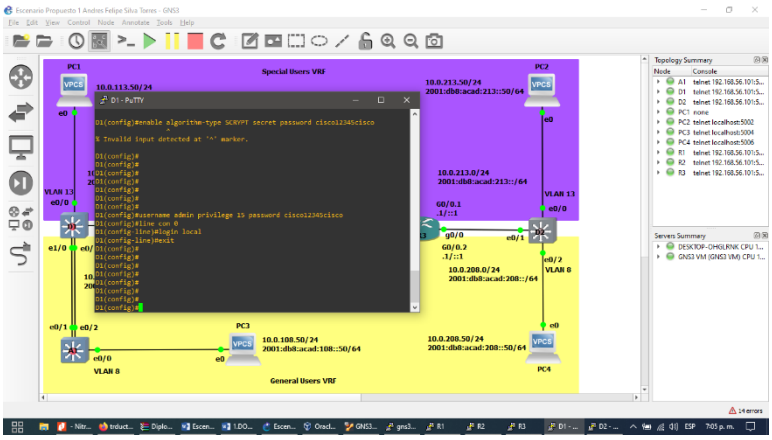
4.2. Crear una cuenta de usuario local en los dispositivos

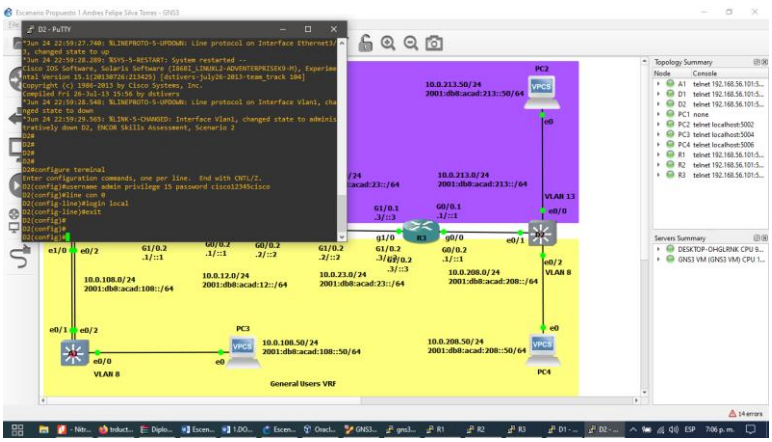
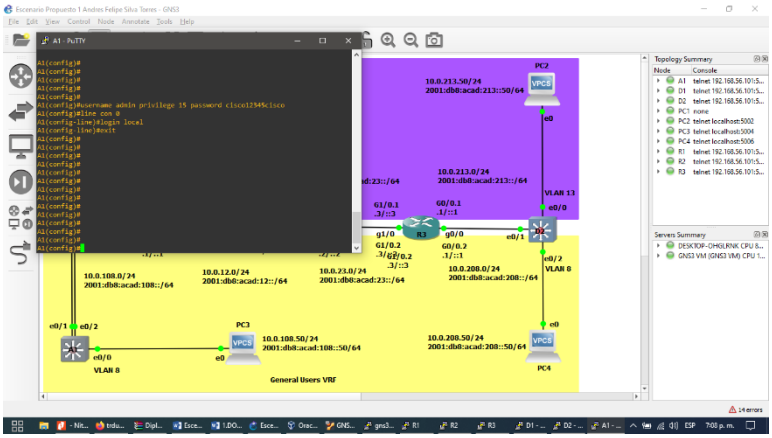
Task#	Task	Specification
4.2	On all devices, create a local user account.	Configure a local user: Name: **admin** Privilege level: **15** Algorithm type: **SCRYPT** Password: **cisco12345cisco**.

Tabla 13, Cuenta usuario dispositivos.

Fuente: Autor.

R1 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 40, Cuenta usuario R1.* *Fuente: Autor.*
R2 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 41, Cuenta usuario R2.* *Fuente: Autor.*

R3 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 42, Cuenta usuario R3.* *Fuente: Autor.*
D1 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 43, Cuenta usuario D1.* *Fuente: Autor.*

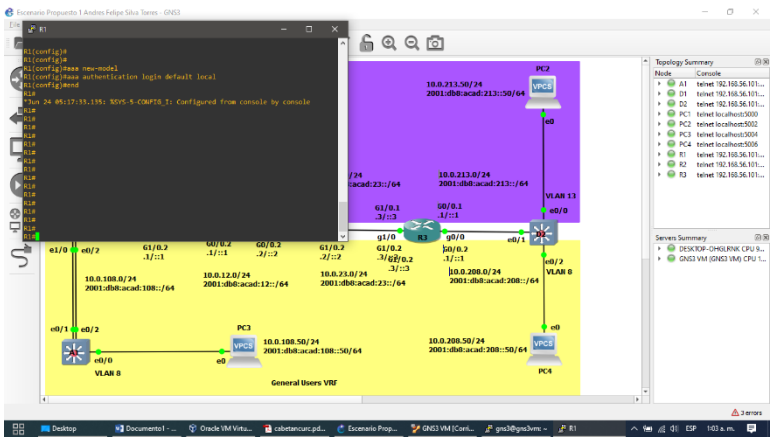
D2 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 44, Cuenta usuario D2.* *Fuente: Autor.*
A1 enable algorithm-type SCRYPT secret password cisco12345cisco exit Username admin privilege 15 password cisco12345cisco Line con 0 Login local exit	 *Ilustración 45, Cuenta usuario A1.* *Fuente: Autor.*

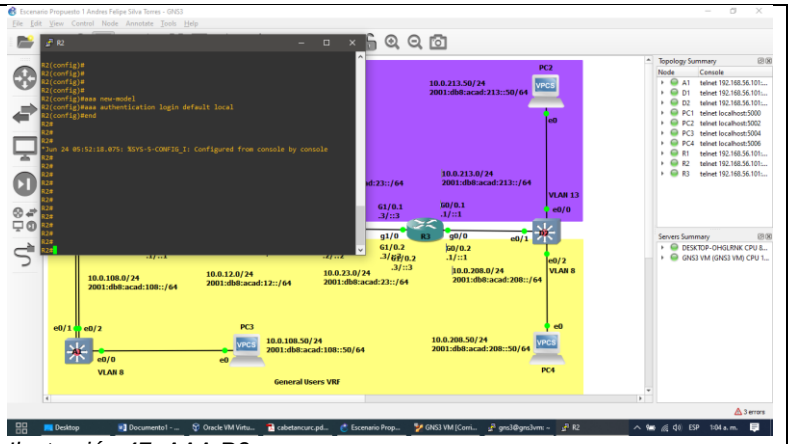
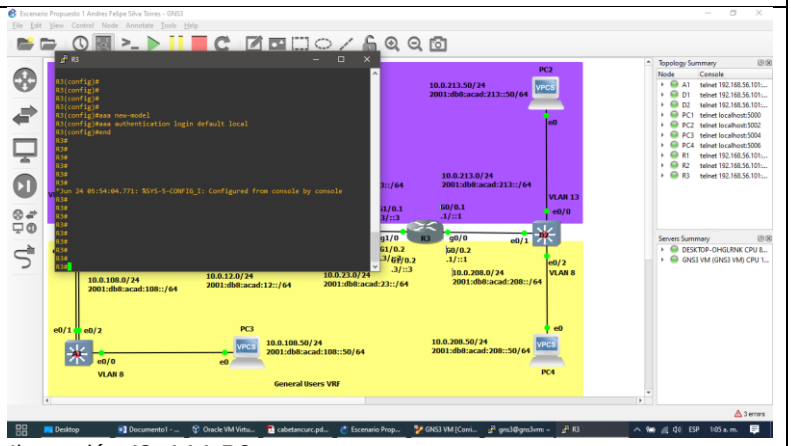
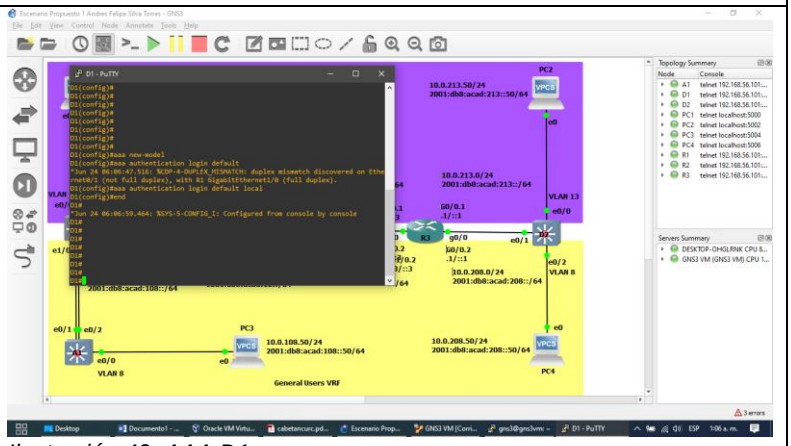
4.3. Habilitar la autenticación aaa en los dispositivos.

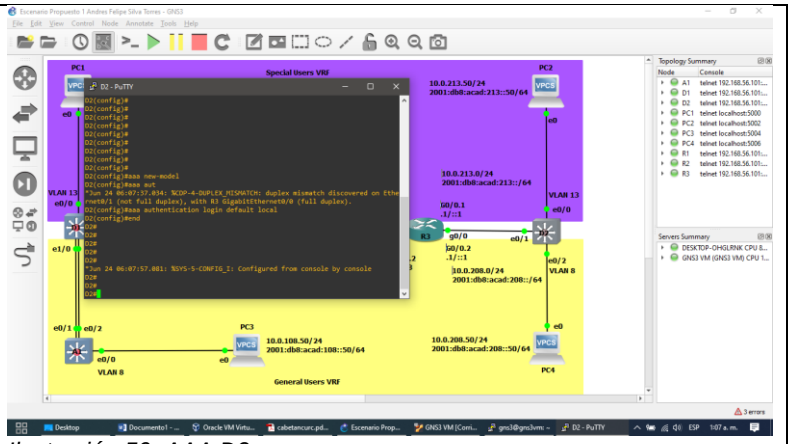
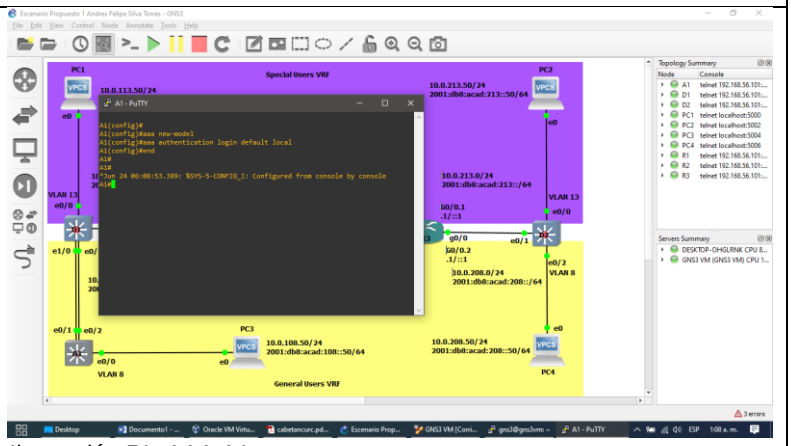
Task#	Task	Specification
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

Tabla 14, Habilitación AAA dispositivos.

Fuente: Autor.

R1 aaa new-model aaa authentication login default local end	 *Ilustración 46, AAA R1.* *Fuente: Autor.*

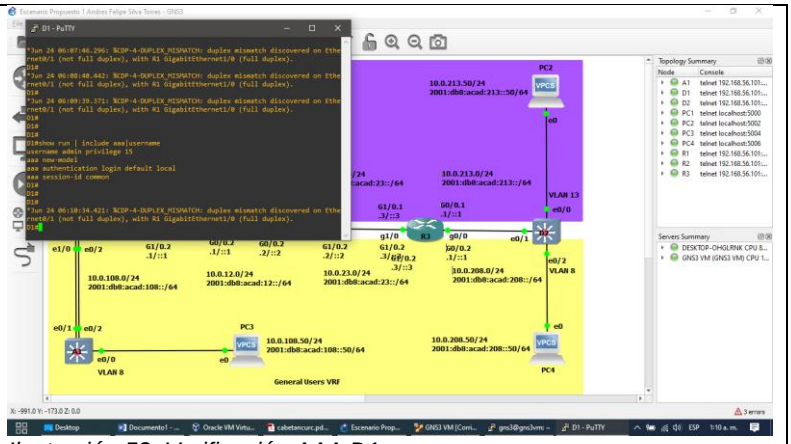
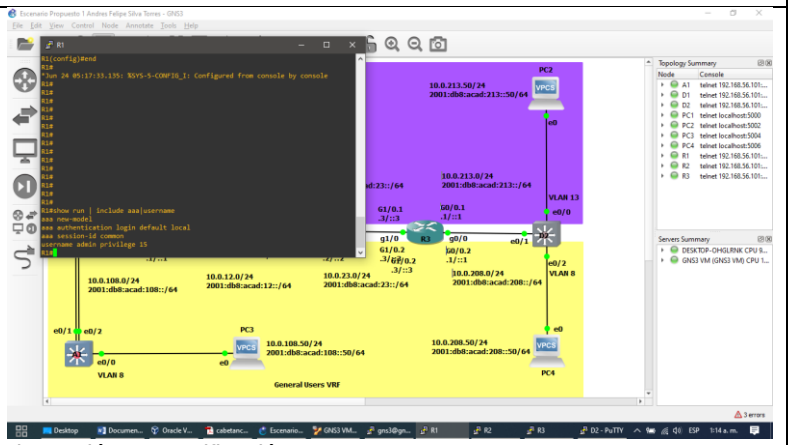
R2 aaa new-model aaa authentication login default local end	 *Ilustración 47, AAA R2.* *Fuente: Autor.*
R3 aaa new-model aaa authentication login default local end	 *Ilustración 48, AAA R3.* *Fuente: Autor.*
D1 aaa new-model aaa authentication login default local end	 *Ilustración 49, AAA D1.* *Fuente: Autor.*

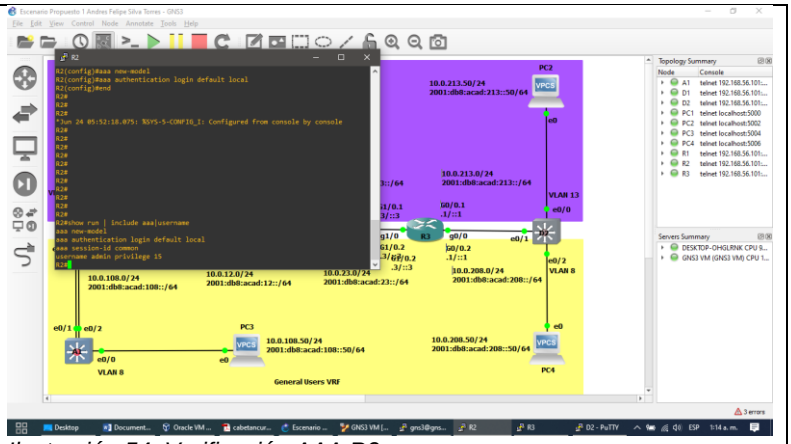
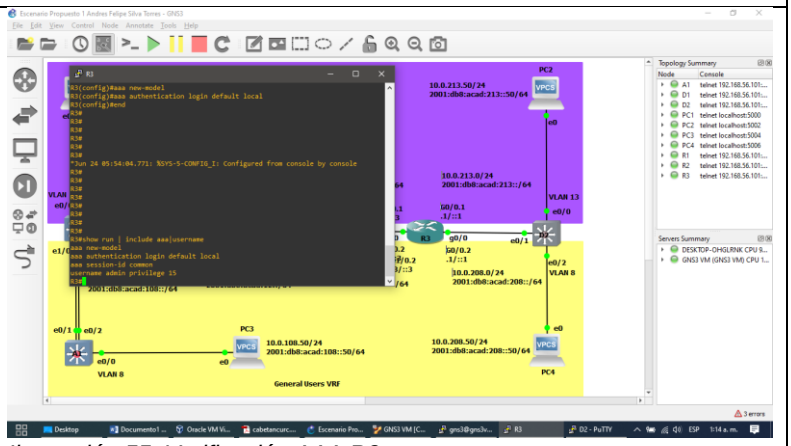
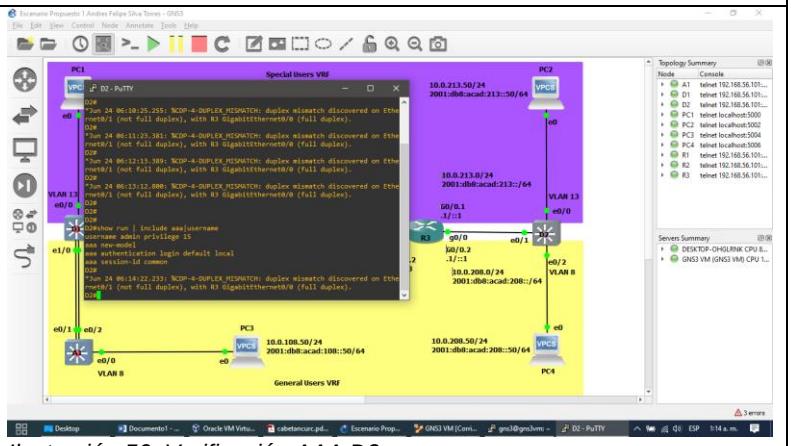
D2 aaa new-model aaa authentication login default local end	 *Ilustración 50, AAA D2.* *Fuente: Autor.*
A1 aaa new-model aaa authentication login default local end	 *Ilustración 51, AAA A1.* *Fuente: Autor.*

4.3. Verificación nombre de usuario y la autenticación aaa.

Tabla 15, Verificación AAA.

Fuente: Autor.

D1 Show run | include aaa|username	 *Ilustración 52, Verificación AAA D1.* *Fuente: Autor.*
R1 Show run | include aaa|username	 *Ilustración 53, Verificación AAA R1.* *Fuente: Autor.*

R2 Show run | include aaa|username	 *Ilustración 54, Verificación AAA R2.* *Fuente: Autor.*
R3 Show run | include aaa|username	 *Ilustración 55, Verificación AAA R3.* *Fuente: Autor*
D2 Show run | include aaa|username	 *Ilustración 56, Verificación AAA D2.* *Fuente: Autor.*

Conclusiones

La red trabajada en el escenario práctico se configuró a partir de VLANs, las cuales permitieron crear redes lógicas en una misma red física que se configuran en los Switches para realizar la conexión con los PCs, con el fin de garantizar la transmisión de la información de una forma segura entre los usuarios que pertenecen a cada VLAN.

El protocolo de autenticación AAA permite crear niveles privilegiados con el fin de restringir el acceso a una red teniendo en cuenta si el ingreso se realiza por medio del rol de usuario o administrador; con el fin de proteger la información que se transmite de accesos no autorizados.

El software GNS3 posee grandes ventajas respecto al software de simulación CISCO Packet Tracer; ya que, además de poseer más variedad de imágenes de modelos de Switches y Routers, también posee una mayor compatibilidad o aceptación de comandos.

Referencias bibliográficas

Enlace del 802.1Q entre los switches de catalyst que funcionan con CatOS y el software del sistema del cisco IOS. (2018, 2 febrero). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/8021q/8760-67.html

Creación de VLAN de ethernet en switches catalyst. (2021, 14 julio). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vlan/10023-3.html

Juniper Networks. (s. f.). 404. (29 de noviembre de 2021), de https://www.juniper.net/documentation/en_US/junose15.1/topics/example/simple/+mbgp-disable-default-address-family.html

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. (En linea). (2020) (21 de Junio de 2022) Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8