DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAVIER ANDRES TAMARA HADECHINE

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAVIER ANDRES TAMARA HADECHINE

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

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

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Corozal, 26 de junio de 2022

AGRADECIMIENTOS

Principalmente agradecerle a Dios por darme la vida y regalarme la oportunidad de poder estudiar y cumplir una meta como es terminar mi carrera profesional. A mis padres, Francisco Tamara Novoa y Ana Hadechine Assia por apoyarme a sacar esta profesión adelante, darme ese apoyo que solo los padres saben brindar y ayudarme a levantar en los momentos difíciles, siempre escuche sus consejos, sus palabras de aliento y sus oraciones, sé que este triunfo los llena de mucho orgullo y satisfacción. A mi pareja por estar conmigo alentándome y apoyándome a salir adelante. Por último, a la universidad nacional abierta y a distancia, a los tutores que me apoyaron en todos estos semestres con sus conocimientos y paciencia, y a mis compañeros que siempre estuvieron para darme la mano.

CONTENDIO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DIRECCIÓN IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (Internet Protocol) o que corresponde al nivel de red del modelo TCP/IP.

ENLACES TRONCALES: Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

SWITCH: Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet o técnicamente IEEE 802.3.

TOPOLOGIA DE RED: se define como un mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

VLANs: Nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soporten VLANs para segmentar adecuadamente la red.

VRF: es una tecnología que permite que un enrutador ejecute más de una tabla de enrutamiento simultáneamente**.** Además, dichas tablas son completamente independientes. De esta manera, es posible, por ejemplo, utilizar la misma dirección IP asignada a dos interfaces diferentes en un enrutador al mismo tiempo**.**

RESUMEN

En el presente informe se aborda la prueba de habilidades del diplomado de profundización CISCO CCNP, el cual se debe realizar la configuración electrónica en la topología que se nos da a realizar, con esto se busca de completar la conmutación en todos los dispositivos para que los protocolos operen correctamente en todo el sistema de redes.

Esta prueba consta de 4 puntos básicos, donde se configura cada dispositivo ajustes básicos y se va creando la red dándole forma a la topología que se requiere. Luego se configuran las VRF para crear dos redes una de usuario especial y otra de usuario general y los enrutamientos estáticos dándole protocolos a las capas de redes tanto IPv4 como IPv6, pasando este punto se da configuración de capa dos a los switches para tener comunicación entre los dispositivos. Por último, se aplica la seguridad de los dispositivos para poder administrar la red de manera correcta.

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

ABSTRACT

This report deals with the skills test of the CISCO CCNP deepening diploma course, which must carry out the electronic configuration in the topology that we are given to carry out, with this it is sought to complete the switching in all the devices so that the protocols operate correctly throughout the network system.

This test consists of 4 basic points, where each device is configured with basic settings and the network is created, shaping the topology that is required. Then the VRFs are configured to create two networks, one for a special user and the other for a general user, and the static routings, giving protocols to the network layers, both IPv4 and IPv6, passing this point, layer two configuration is given to the switches to have communication between them. the devices. Finally, device security is applied in order to manage the network correctly.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCION

CCNP son las siglas de Cisco Certified Networking Professional. Es decir, un certificado de networking y telecomunicaciones. Este sirve como requisito para la opción de grado en el diplomado de profundización para obtener el titulo de ingeniero. Este diplomado Cisco CCNP aporta y garantiza conocimiento, implementación, habilidades para resolver problemas en redes de empresas, áreas locales y amplias, garantizando que éstas puedan perdurar en el tiempo y ser de gran utilidad a empresas y proyectos, también permitiendo dar soluciones en seguridad de redes inalámbricas.

Este trabajo conlleva la creación y el diseño de un escenario propuesto por el diplomado de profundización en donde se realiza una topología de la red planteada, se configura cada dispositivo en ella, se crean dos VRFs para diferenciar los usuarios que están en la red. Se realiza la configuración de capa 2 y los protocolos de enrutamiento para que se pueda tener comunicación entre los dispositivos y finalmente se configura la parte de seguridad, para darle la confianza a los usuarios de que sus datos están a salvo.

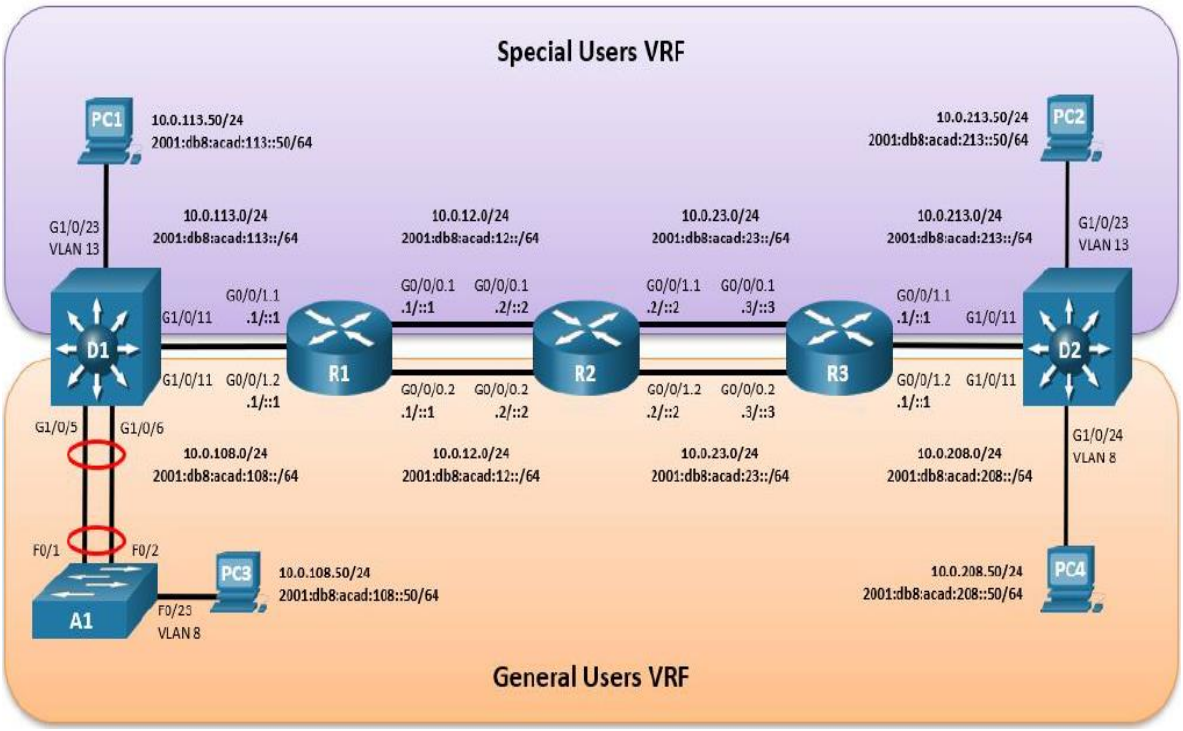
Para realizar la prueba de habilidades de Cisco CCNP se utiliza el software GNS3 con su respectiva maquina virtual, en este caso VMware Workstation, creando la topología dada en la guía desde cero, esta topología de manera física es una, pero de manera virtual esta distribuida entre usuario especial y usuario general, donde los diferentes usuarios solo se pueden comunicar con los que tengan las mismas vlan.

DESARROLLO

ESCENARIO PROPUESTO

A continuación, se muestra en la figura 1, la topología de la red que se estará trabajando como requisitos del diplomado, para su estudio, configuración e implementación.

Figura 1. Topología de la red propuesta.



Fuente: Guía avances documento final CCNP

Tabla 1. Direccionamiento de la topología propuesta

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
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	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
	G0/0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	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

Fuente: Guía avance documento final CCNP

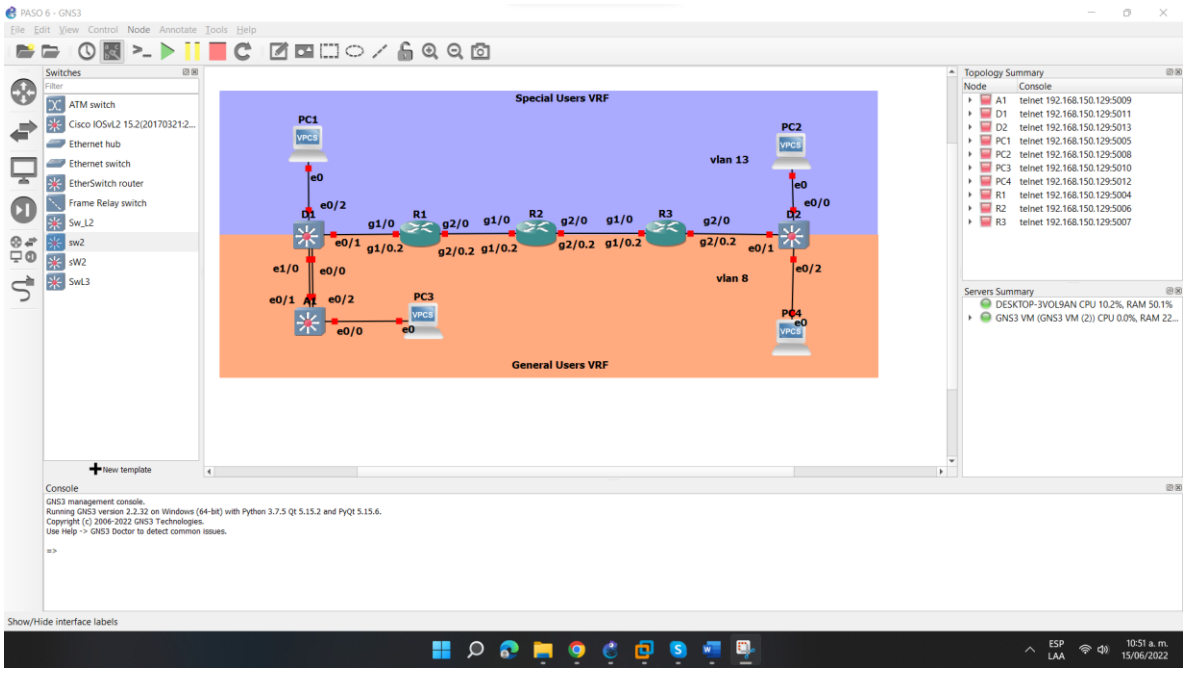
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

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.

Figura 2. Topología de la red propuesta en GNS3



Fuente: Autoría propia

Paso 2: Configure los ajustes básicos para cada dispositivo.

Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2 y R3, según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red y se guarda la configuración.

Se procede a configurar cada uno de los enrutadores. 1, 2, 3.
Se asignan nombre y protocolos de comunicación mediante EIGRP que fueron asignados.
Se adjunta tabla del código.

Tabla 2. Código de configuración básica en Router R1

Route#enable	Ingreso a modo privilegiado
Route#configure terminal	Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z	
Route(config)#hostname R1	Asigno nombre al router
R1(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
R1(config)#no ip domain lookup	habilita la traducción de nombre a direcciones
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	Mensaje R1
R1(config)#line con 0	Se accede al modo de configuración de línea
R1(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
R1(config-line)#logging synchronous	Sincronización de mensajes de actualización
R1(config-line)#exit	

Fuente: Autoría propia

Tabla 3. Código de configuración básica en Router R2

Route#enable	Ingreso a modo privilegiado
Route#configure terminal	Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z	
Route(config)#hostname R2	Asigno nombre al router
R2(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
R2(config)#no ip domain lookup	habilita la traducción de nombre a direcciones
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 2 #	Mensaje R2
R2(config)#line con 0	Se accede al modo de configuración de línea
R2(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
R2(config-line)#logging synchronous	Sincronización de mensajes de actualización
R2(config-line)#exit	

Fuente: Autoría propia

Tabla 4. Código de configuración básica en Router R3

Route#enable	Ingreso a modo privilegiado
Route#configure terminal	Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z	
Route(config)#hostname R3	Asigno nombre al router
R3(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
R3(config)#no ip domain lookup	Habilita la traducción de nombre a direcciones
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	Mensaje R3
R3(config)#line con 0	Se accede al modo de configuración de línea
R3(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
R3(config-line)#logging synchronous	Sincronización de mensajes de actualización
R3(config-line)#exit	

Fuente: Autoría propia

Tabla 5. Código de configuración básica en Switch D1

Switch#enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname D1	Asigno nombre al switch
D1(config)#ip routing	
D1(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
D1(config)#no ip domain lookup	Habilita la traducción de nombre a direcciones
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	Mensaje D1
D1(config)#line con 0	Se accede al modo de configuración de línea
D1(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
D1(config-line)#logging synchronous	Sincronización de mensajes de actualización
D1(config-line)#exit	
D1(config)#vlan 8	Crea la vlan 8
D1(config-vlan)#name General-Users	Se le asigna un nombre a la vlan
D1(config-vlan)#exit	
D1(config)#vlan 13	Crea la vlan 13
D1(config-vlan)#name Special-Users	Se le asigna un nombre a la vlan
D1(config-vlan)#exit	

Fuente: Autoría propia

Tabla 6. Código de configuración básica en Switch D2

Switch#enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname D2	Asigno nombre al switch
D2(config)#ip routing	
D2(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
D2(config)#no ip domain lookup	Habilita la traducción de nombre a direcciones
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	Mensaje D2
D2(config)#line con 0	Se accede al modo de configuración de línea
D2(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
D2(config-line)#logging synchronous	Sincronización de mensajes de actualización
D2(config-line)#exit	
D2(config)#vlan 8	Crea la vlan 8
D2(config-vlan)#name General-Users	Se le asigna un nombre a la vlan

D2(config-vlan)#exit	
D2(config)#vlan 13	Crea la vlan 13
D2(config-vlan)#name Special-Users	Se le asigna un nombre a la vlan
D2(config-vlan)#exit	

Fuente: Autoría propia

Tabla 7. Código de configuración básica en Switch A1

Switch#enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname A1	Asigno nombre al switch
A1(config)#ip routing	
A1(config)#ipv6 unicast-routing	Habilita el direccionamiento ipv6
A1(config)#no ip domain lookup	Habilita la traducción de nombre a direcciones
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	Mensaje D2
A1(config)#line con 0	Se accede al modo de configuración de línea
A1(config-line)#exec-timeout 0 0	Tiempo fuera de sincronización
A1(config-line)#logging synchronous	Sincronización de mensajes de actualización
A1(config-line)#exit	
A1(config)#vlan 8	Crea la vlan 8
A1(config-vlan)#name General-Users	Se le asigna un nombre a la vlan
A1(config-vlan)#exit	

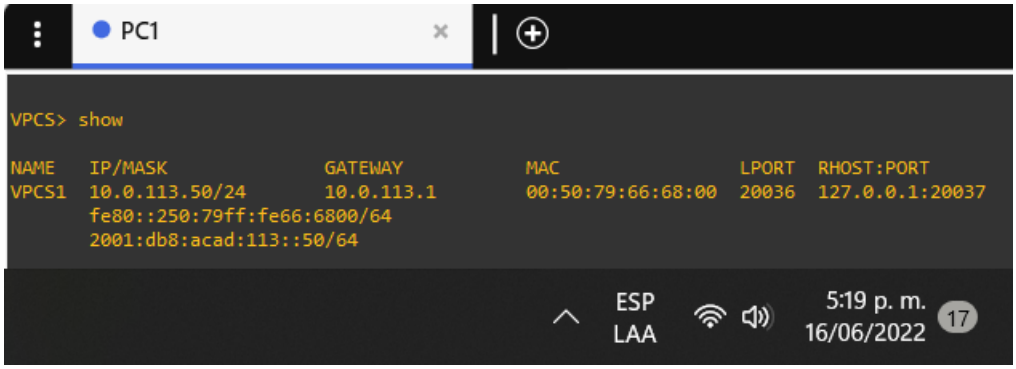
Fuente: Autoría propia

Paso 2.1. Configurar el direccionamiento host en PC1, PC2, PC3 Y PC4

Configure el direccionamiento de host PC1, PC2, PC3 y PC4 como se muestra en la tabla de direccionamiento, se observa la ip con el comando show ip.

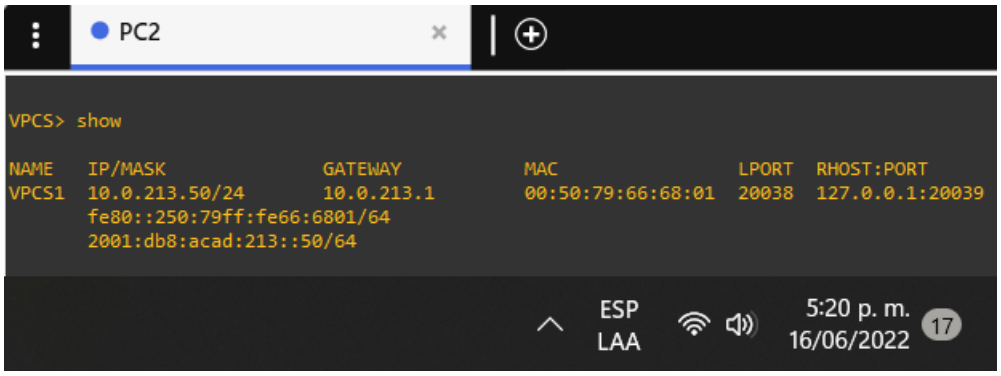
Se adjunta pantallazo de la configuración

Figura 3. Configuración del direccionamiento host de PC1



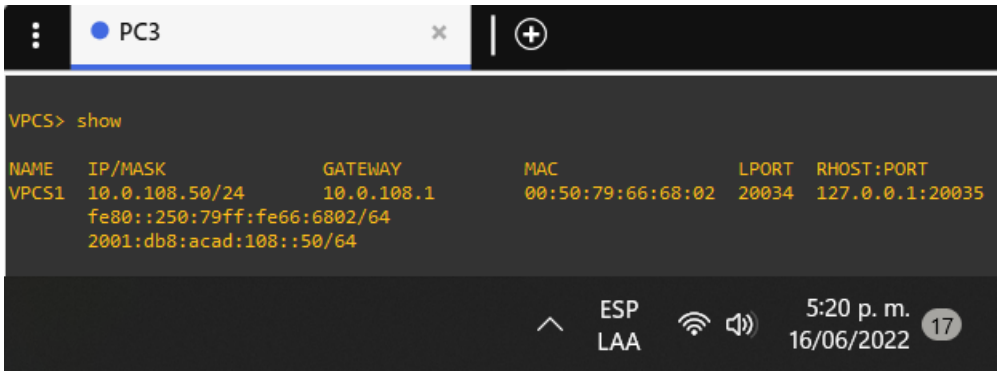
Fuente: Escenario de configuración GNS3

Figura 4. Configuración del direccionamiento host de PC2



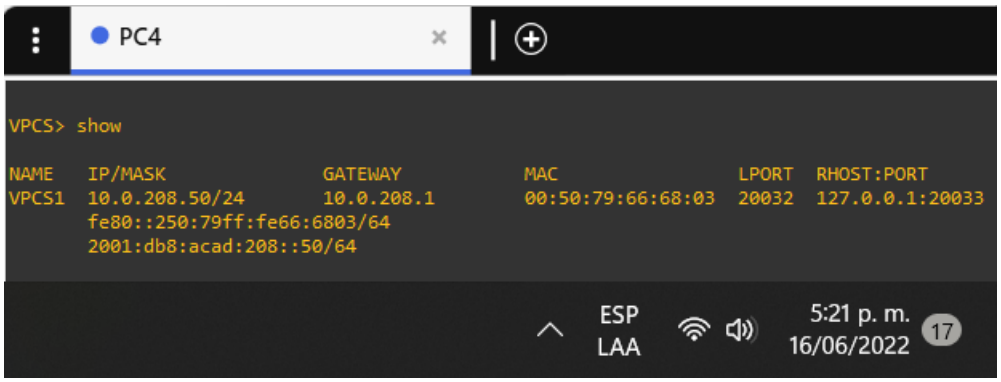
Fuente: Escenario de configuración GNS3

Figura 5. Configuración del direccionamiento host de PC3



Fuente: Escenario de configuración GNS3

Figura 6. Configuración del direccionamiento host de PC4



Fuente: Escenario de configuración GNS3

Parte 2: Configurar VRF y enrutamiento estático

En esta parte de la evaluación de habilidades, configurará VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF. Como se indica en la Figura 7.

Tabla 8. Tareas de configuración

Tarea#	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.	Configure dos VRF: • Usuarios generales • Usuarios especiales Los VRF deben admitir IPv4 e IPv6.
2.2	En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	Todos los enrutadores utilizarán Router-On-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF. Sub-interfaz 1: • En el VRF de Usuarios Especiales • Usar encapsulamiento dot1q 13 • IPv4 e IPv6 GUA y direcciones link-local • Habilitar las interfaces Sub-interfaz 2: • En el VRF de Usuarios Generales • Usar encapsulamiento dot1q 8 • IPv4 e IPv6 GUA y direcciones locales de enlace • • Habilite las interfaces
2.3	En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.

2.4	Verifique la conectividad en cada VRF.	Desde R1, verifique la conectividad con 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

Fuente: Guía avance documento final CCNP

Paso 2.1 En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.

Aplique la configuración a cada uno de los routers para que tengan dos VRF como lo muestra la topología, uno para usuario general y otro para usuario especial y configurando los routers para que admitan ipv4 y ipv6.

Se adjunta tabla del código para cada router

Tabla 9. Código para crear las familias de VRF en el router R1

R1#configure terminal	Ingreso a modo de configuración
R1(config)#vrf definition General-Users	Se le da nombre al VRF
R1(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R1(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R1(config-vrf-af)#exit	
R1(config-vrf)#exit	
R1(config)#vrf definition Special-Users	Se le da el segundo nombre al VRF
R1(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R1(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R1(config-vrf-af)#exit	
R1(config-vrf)#exit	
R1(config)#exit	
R1#wr	Se guarda la configuración

Fuente: Autoría propia

Tabla 10. Código para crear las familias de VRF en el router R2

R2#configure terminal	Ingreso a modo de configuración
R2(config)#vrf definition General-Users	Se le da nombre al VRF
R2(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R2(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R2(config-vrf-af)#exit	
R2(config-vrf)#exit	
R2(config)#vrf definition Special-Users	Se le da el segundo nombre al VRF
R2(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R2(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R2(config-vrf-af)#exit	
R2(config-vrf)#exit	
R2(config)#exit	
R2#wr	Se guarda la configuración

Fuente: Autoría propia

Tabla 11. Código para crear las familias de VRF en el router R3

R3#configure terminal	Ingreso a modo de configuración
R3(config)#vrf definition General-Users	Se le da nombre al VRF
R3(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R3(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R3(config-vrf-af)#exit	
R3(config-vrf)#exit	
R3(config)#vrf definition Special-Users	Se le da el segundo nombre al VRF
R3(config-vrf)#address-family ipv4	Se configura para admitir ipv4
R3(config-vrf-af)#address-family ipv6	Se configura para admitir ipv6
R3(config-vrf-af)#exit	
R3(config-vrf)#exit	
R3(config)#exit	
R3#wr	Se guarda la configuración

Fuente: Autoría propia

Paso 2.2 En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.

Configuro en R1, R2 y R3, las interfaces IPv4 e IPv6 en cada VRF. Se usa Router-On-A-Stick en todas las interfaces para admitir la separación de los VRF, los usuarios especiales usan encapsulamiento dot1q 13, se agregan la IPv4 y la IPv6 y direcciones link-local y se habilita las interfaces y para los usuarios generales se hace el mismo proceso pero cambiando el encapsulamiento a dot1q 8.

Se adjunta código

Tabla 12. Código de configuración en R1 para agregar los encapsulados de las vlans, a que vrf van asignadas y las interfaces IPv4 e IPv6

R1#configure terminal	
R1(config)#interface g0/0	se entra a la interfaz
R1(config-if)# no shutdown	se habilita la interfaz
R1(config-if)#exit	
R1(config)#interface g0/0.1	se entra a la sub-interfaz
R1(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R1(config-subif)#vrf forwarding Special-Users	se agrega el nombre de la VRF
R1(config-subif)#ip address 10.0.12.1 255.255.255.0	se agrega la dirección ipv4

R1(config-subif)#ipv6 address fe80::1:1 link-local	se agrega la dirección ipv6 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:12::1/64	se agrega dirección ipv6
R1(config-subif)#exit	
R1(config)#exit	
R1#wr	
R1#configure terminal	
R1(config)#interface g0/0.2	se entra a la sub-interfaz
R1(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R1(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R1(config-subif)#ip address 10.0.12.1 255.255.255.0	se agrega la dirección ipv4
R1(config-subif)#ipv6 address fe80::1:2 link-local	se agrega la dirección ipv6 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:112::1/64	se agrega dirección ipv6
R1(config-subif)#no shutdown	se habilita la interfaz
R1(config-subif)#exit	
R1(config)#exit	
R1#wr	
R1#configure terminal	
R1(config)#interface e2/0	se entra a la interfaz
R1(config-if)# no shutdown	se habilita la interfaz
R1(config-if)#exit	
R1(config)#interface e2/0.1	se entra a la sub-interfaz
R1(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R1(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R1(config-subif)#ip address 10.0.113.1 255.255.255.0	se agrega la dirección ipv4
R1(config-subif)#ipv6 address fe80::1:3 link-local	se agrega la dirección ipv6 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:113::1/64	se agrega dirección ipv6
R1(config-subif)#no shutdown	se habilita la interfaz
R1(config-subif)#exit	
R1(config)#exit	
R1#wr	

R1#configure terminal	
R1(config)#interface e2/0.2	se entra a la sub-interfaz
R1(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R1(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R1(config-subif)#ip address 10.0.108.1 255.255.255.0	se agrega la dirección ipv4
R1(config-subif)#ipv6 address fe80::1:4 link-local	se agrega la dirección ipv6 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:108::1/64	se agrega dirección ipv6
R1(config-subif)#exit	
R1(config)#exit	
R1#wr	

Fuente: Autoría propia

Tabla 13. Código de configuración en R2 para agregar los encapsulados de las vlans, a que vrf van asignadas y las interfaces IPv4 e IPv6

R2#configure terminal	
Enter configuration commands, one per line. End with CNTL/Z.	
R2(config)# interface g2/0	se entra a la interfaz
R2(config-if)#no shutdown	se habilita la interfaz
R2(config-if)#exit	
R2(config)#interface g1/0.1	se entra a la sub-interfaz
R2(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R2(config-subif)#vrf forwarding Special-Users	se agrega el nombre de la VRF
R2(config-subif)#ip address 10.0.12.2 255.255.255.0	se agrega la dirección ipv4
R2(config-subif)#ipv6 address fe80::2:1 link-local	se agrega la dirección ipv6 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64	se agrega dirección ipv6
R2(config-subif)#exit	
R2(config)#interface g1/0.2	se entra a la sub-interfaz
R2(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R2(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R2(config-subif)#ip address 10.0.12.2 255.255.255.0	se agrega la dirección ipv4

R2(config-subif)#ipv6 address fe80::2:2 link-local	se agrega la dirección ipv6 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:12::2/64	se agrega dirección ipv6
R2(config-subif)#no shutdown	
R2(config-subif)#exit	
R2(config)#interface g1/0	se entra a la interfaz
R2(config-if)#no shutdown	se habilita la interfaz
R2(config-if)#exit	
R2(config)#interface g2/0.1	se entra a la sub-interfaz
R2(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R2(config-subif)#vrf forwarding Special-Users	se agrega el nombre de la VRF
R2(config-subif)#ip address 10.0.23.2 255.255.255.0	se agrega la dirección ipv4
R2(config-subif)#ipv6 address fe80::2:3 link-local	se agrega la dirección ipv6 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64	se agrega dirección ipv6
R2(config-subif)#no shutdown	
R2(config-subif)#exit	
R2(config)#interface g2/0.2	se entra a la sub-interfaz
R2(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R2(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R2(config-subif)#ip address 10.0.23.2 255.255.255.0	se agrega la dirección ipv4
R2(config-subif)#ipv6 address fe80::2:4 link-local	se agrega la dirección ipv6 link-local
R2(config-subif)#ipv6 address 2001:db8:acad:23::2/64	se agrega dirección ipv6
R2(config-subif)#exit	
R2(config)#exit	
R2#wr	Se guardan los datos

Fuente: Autoría propia

Tabla 14. Código de configuración en R3 para agregar los encapsulados de las vlans, a que vrf van asignadas y las interfaces IPv4 e IPv6

R3#configure terminal	
Enter configuration commands, one per line. End with CNTL/Z.	
R3(config)#interface g1/0	se entra a la interfaz
R3(config-if)#no shutdown	se habilita la interfaz
R3(config-if)#exit	
R3(config)#interface g1/0.1	se entra a la sub-interfaz
R3(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R3(config-subif)#vrf forwarding Special-Users	se agrega el nombre de la VRF
R3(config-subif)#ip address 10.0.23.3 255.255.255.0	se agrega la dirección ipv4
R3(config-subif)#ipv6 address fe80::3:1 link-local	se agrega la dirección ipv6 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64	se agrega dirección ipv6
R3(config-subif)#exit	
R3(config)#interface g1/0.2	se entra a la sub-interfaz
R3(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R3(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R3(config-subif)#ip address 10.0.23.3 255.255.255.0	se agrega la dirección ipv4
R3(config-subif)#ipv6 address fe80::3:2 link-local	se agrega la dirección ipv6 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:23::3/64	se agrega dirección ipv6
R3(config-subif)#no shutdown	
R3(config-subif)#exit	
R3(config)#interface g2/0	se entra a la interfaz
R3(config-if)#no shutdown	se habilita la interfaz
R3(config-if)#exit	
R3(config)#interface g2/0.1	se entra a la sub-interfaz
R3(config-subif)#encapsulation dot1q 13	se agrega el encapsulado para la vlan 13
R3(config-subif)#vrf forwarding Special-Users	se agrega el nombre de la VRF
R3(config-subif)#ip address 10.0.213.1 255.255.255.0	se agrega la dirección ipv4

R3(config-subif)#ipv6 address fe80::3:3 link-local	se agrega la dirección ipv6 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:213::1/64	se agrega dirección ipv6
R3(config-subif)#no shutdown	
R3(config-subif)#exit	
R3(config)#interface g2/0.2	se entra a la sub-interfaz
R3(config-subif)#encapsulation dot1q 8	se agrega el encapsulado para la vlan 8
R3(config-subif)#vrf forwarding General-Users	se agrega el nombre de la VRF
R3(config-subif)#ip address 10.0.208.1 255.255.255.0	se agrega la dirección ipv4
R3(config-subif)#ipv6 address fe80::3:4 link-local	se agrega la dirección ipv6 link-local
R3(config-subif)#ipv6 address 2001:db8:acad:208::1/64	se agrega dirección ipv6
R3(config-subif)#exit	
R3(config)#exit	
R3#wr	Se guardan los datos

Fuente: Autoría propia

Paso 2.3 En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.

Configuro en R1 y R3, las rutas estáticas predeterminadas que apuntan a R2. Configurando las rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.

Se adjunta el código

Tabla 15. Código de configuración para las rutas estáticas en R1

R1#configure terminal	ingresa al modo de configuración
R1(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2	Se agrega la ruta ip a el vrf Special-Users
R1(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2	Se agrega la ruta ip a el vrf General-Users
R1(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:12::2	Se agrega la ruta ipv6 a el vrf Special-Users
R1(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:12::2	Se agrega la ruta ipv6 a el vrf General-Users
R1(config)#exit	

Fuente: Autoría propia

Tabla 16. Código de configuración para las rutas estáticas en R2

R2#configure terminal	
R2(config)#ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1	Se agrega la ruta ip a el vrf General-Users
R2(config)#ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3	Se agrega la ruta ip a el vrf General-Users
R2(config)#ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1	Se agrega la ruta ip a el vrf Special-Users
R2(config)#ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3	Se agrega la ruta ip a el vrf Special-Users
R2(config)#ipv6 route vrf General-Users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1	Se agrega la ruta ipv6 a el vrf General-Users
R2(config)#ipv6 route vrf Special-Users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1	Se agrega la ruta ipv6 a el vrf Special-Users
R2(config)#R2(config)#ipv6 route vrf General-Users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3	Se agrega la ruta ipv6 a el vrf General-Users
R2(config)#ipv6 route vrf Special-Users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3	Se agrega la ruta ipv6 a el vrf Special-Users
R2(config)#exit	

Fuente: Autoría propia

Tabla 17. Código de configuración para las rutas estáticas en R3

R3#configure terminal	ingresa al modo de configuración
R3(config)#ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2	Se agrega la ruta ip a el vrf Special-Users
R3(config)#ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2	Se agrega la ruta ip a el vrf General-Users
R3(config)#ipv6 route vrf Special-Users ::/0 2001:db8:acad:23::2	Se agrega la ruta ipv6 a el vrf Special-Users
R3(config)#ipv6 route vrf General-Users ::/0 2001:db8:acad:23::2	Se agrega la ruta ipv6 a el vrf General-Users
R3(config)#exit	

Paso 2.4. Verifique la conectividad en cada VRF.

Se verifica la conectividad de cada VRF desde R1 hasta R3:
ping vrf General-Users 10.0.208.1

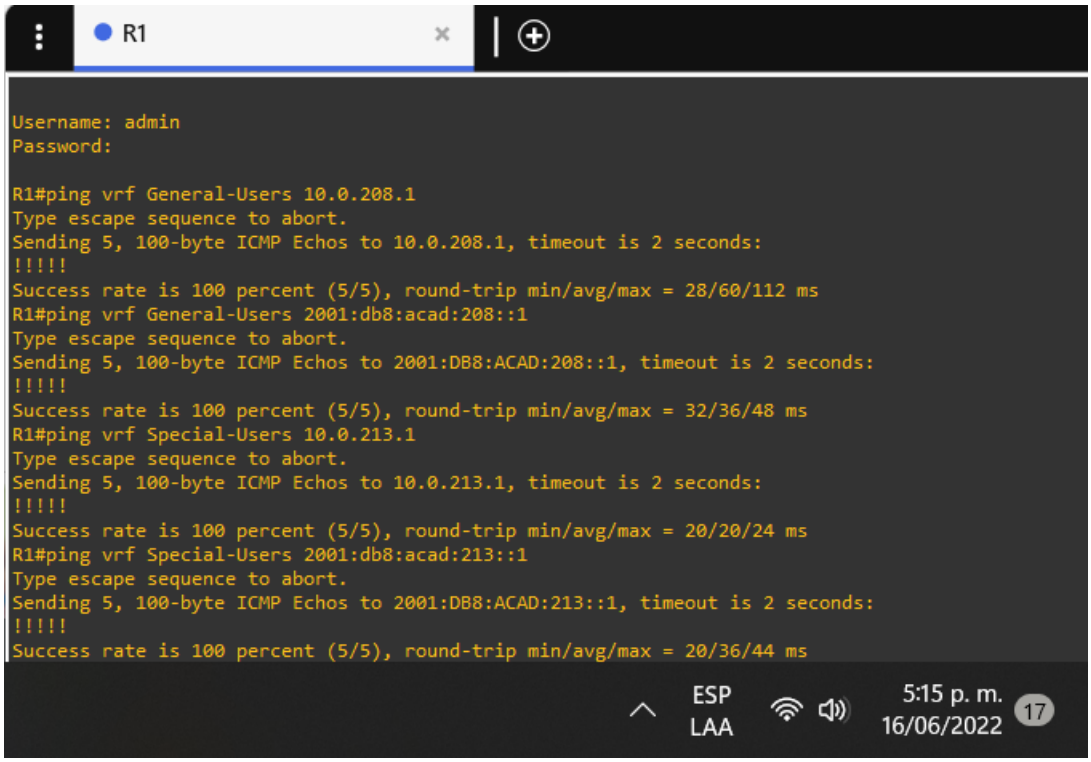
ping vrf General-Users 2001:db8:acad:208::1

ping vrf Special-Users 10.0.213.1

ping vrf Special-Users 2001:db8:acad:213::1

Se adjunta pantallazo de veracidad de los ping

Figura 7. Se comprueba la conectividad entre R1 y R3



Fuente: Escenario de configuración GNS3

Parte 3. Configurar Capa 2

En esta parte, tendrá que configurar los Switches para soportar la conectividad con los dispositivos finales.

Las tareas de configuración, son las siguientes:

Tabla 18. Tareas de configuración

Task#	Task	Specification
3.1	En D1, D2 y A1, deshabilite todas las interfaces.	En D1 y D2, apague G1/0/1 a G1/0/24. En A1, apague F0/1 – F0/24, G0/1 – G0/2.
3.2	En D1 y D2, configure los enlaces troncales a R1 y R3.	Configure y habilite el enlace G1/0/11 como enlace troncal.
3.3	En D1 y A1, configure el EtherChannel.	• En D1, configure y habilite: • Interfaz G1/0/5 y G1/0/6 • Canal de puerto 1 usando PAgP En A1, configure y habilite: • Interfaz F0/1 y F0/2 • Canal de puerto 1 usando PAgP
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	• Configure y habilite los puertos de acceso de la siguiente manera: • En D1, configure la interfaz G1/0/23 como un puerto de acceso en la VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/23 como puerto de acceso en la VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/24 como un puerto de acceso en VLAN 8 y habilite Portfast. • En A1, configure la interfaz F0/23 como un puerto de acceso en la VLAN 8 y habilite Portfast.
3.5	Verifique la conectividad de PC a PC.	Desde la PC1, verifique la conectividad IPv4 e IPv6 a la PC2. Desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4.

Fuente: Guía documento final

Paso 3.1. En D1, D2 y A1, deshabilite todas las interfaces.

Se deshabilitan todas las interfaces en D1, D2 y A1. En mi caso van desde la interfaz Ethernet 0/0-3 hasta la interfaz Ethernet 3/0-3 en todos los switches

Tabla 19. Código de configuración para deshabilitar las interfaces en D1

D1# configure terminal	Ingresa al modo de configuración
D1(config)# interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Se ingresa a las interfaces del switch
D1(config-if-range)# shutdown	Se deshabilitan las interfaces
D1(config-if-range)# exit	

Fuente: Autoría propia

Tabla 20. Código de configuración para deshabilitar las interfaces en D2

D2# configure terminal	Ingresa al modo de configuración
D2(config)# interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Se ingresa a las interfaces del switch
D2(config-if-range)# shutdown	Se deshabilitan las interfaces
D2(config-if-range)# exit	

Fuente: Autoría propia

Tabla 21. Código de configuración para deshabilitar las interfaces en A1

A1# configure terminal	Ingresa al modo de configuración
A1(config)# interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3	Se ingresa a las interfaces del switch
A1(config-if-range)# shutdown	Se deshabilitan las interfaces
A1(config-if-range)# exit	

Fuente: Autoría propia

Paso 3.2. En D1 y D2, configure los enlaces troncales a R1 y R3

Se configura y se habilita el enlace troncal en e0/1 en el switch D1 y e0/1 en el switch D2

Tabla 22. Código de configuración para habilitar enlaces troncales en D1

D1#configure terminal	Ingresa al modo de configuración
D1(config)# interface e0/1	Se ingresa a la interfaz
D1(config-if)#switchport trunk encapsulation dot1q	Se habilita el enlace para permitir enlaces troncales
D1(config-if)#switchport mode trunk	Se hace que el enlace sea un enlace troncal
D1(config-if)#no shutdown	Se habilita la interfaz
D1(config-if)#exit	

Fuente: Autoría propia

Tabla 23. Código de configuración para habilitar enlaces troncales en D2

D2#configure terminal	Ingresa al modo de configuración
D2(config)# interface e0/1	Se ingresa a la interfaz
D2(config-if)#switchport trunk encapsulation dot1q	Se habilita el enlace para permitir enlaces troncales
D2(config-if)#switchport mode trunk	Se hace que el enlace sea un enlace troncal
D2(config-if)#no shutdown	Se habilita la interfaz
D2(config-if)#exit	

Fuente: Autoría propia

Paso 3.3 En D1 y A1, configure el EtherChannel.

En D1, se configura y se habilita la interfaz e0/0 y e1/0 en el canal de puerto 1 usando PAgP y en A1, se configura y habilita la Interfaz e0/1 y e0/2 en el canal de puerto 1 usando PAgP

Tabla 24. Código de configuración para habilitar las interfaces EtherChannel en D1

D1#Configure terminal	Ingresa al modo de configuración
D1(config)# interface range e0/0, e1/0	Se entra a las interfaces
D1(config-if-range)# switchport trunk encapsulation dot1q	Se permite que el switch tenga enlace troncal
D1(config-if-range)# switchport mode trunk	Se cambia la interfaz al modo troncal permanente
D1(config-if-range)# channel-group 1 mode desirable	Se le asigna un canal para estar en un mismo grupo
D1(config-if-range)# no shutdown	Se habilitan las interfaces
D1(config-if-range)# exit	

Fuente: Autoría propia

Tabla 25. Código de configuración para habilitar las interfacez EtherChannel en A1

A1#Configure terminal	Ingresa al modo de configuración
A1(config)# interface range e0/1-2	Se entra a las interfaces
A1(config-if-range)# switchport trunk encapsulation dot1q	Se permite que el switch tenga enlace troncal
A1(config-if-range)# switchport mode trunk	Se cambia la interfaz al modo troncal permanente
A1(config-if-range)# channel-group 1 mode desirable	Se le asigna un canal para estar en un mismo grupo
A1(config-if-range)# no shutdown	Se habilitan las interfaces
A1(config-if-range)# exit	

Fuente: Autoría propia

Paso 3.4 En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.

Se configuran y habilitan los puertos de acceso en D1, configurando la interfaz e0/2 como un puerto de acceso en la VLAN 13 y habilitando Portfast.

En D2, se configura la interfaz e0/0 como puerto de acceso en la VLAN 13 y habilitando Portfast y se configura la interfaz e0/2 como un puerto de acceso en VLAN 8 y habilitando Portfast.

En A1, se configura la interfaz e0/0 como un puerto de acceso en la VLAN 8 y habilitando Portfast.

Tabla 26. Código para configurar los puertos de acceso de D1 a PC1

D1#Configure terminal	Ingresa al modo de configuración
D1(config)#interface e0/2	Se entra a las interfaces
D1(config-if)#switchport mode access	Se permite que el switch entre al modo de acceso permanente
D1(config-if)#switchport access vlan 13	Se da acceso a la vlan13
D1(config-if)#spanning-tree portfast	Se
D1(config-if)#no shutdown	Se habilitan las interfaces
D1(config-if)#exit	

Fuente: Autoría propia

Tabla 27. Código para configurar los puertos de acceso de D2 a PC2

D2#Configure terminal	Ingresa al modo de configuración
D2(config)#interface e0/0	Se entra a las interfaces
D2(config-if)#switchport mode access	Se permite que el switch entre al modo de acceso permanente
D2(config-if)#switchport access vlan 13	Se da acceso a la vlan13
D2(config-if)#spanning-tree portfast	Se
D2(config-if)#no shutdown	Se habilitan las interfaces
D2(config-if)#exit	

Fuente: Autoría propia

Tabla 28. Código para configurar los puertos de acceso de D2 a PC4

D2#Configure terminal	Ingresa al modo de configuración
D2(config)#interface e0/2	Se entra a las interfaces
D2(config-if)#switchport mode access	Se permite que el switch entre al modo de acceso permanente
D2(config-if)#switchport access vlan 8	Se da acceso a la vlan8
D2(config-if)#spanning-tree portfast	Se
D2(config-if)#no shutdown	Se habilitan las interfaces

D2(config-if)#exit	

Fuente: Autoría propia

Tabla 29. Código para configurar los puertos de acceso de A1 a PC3

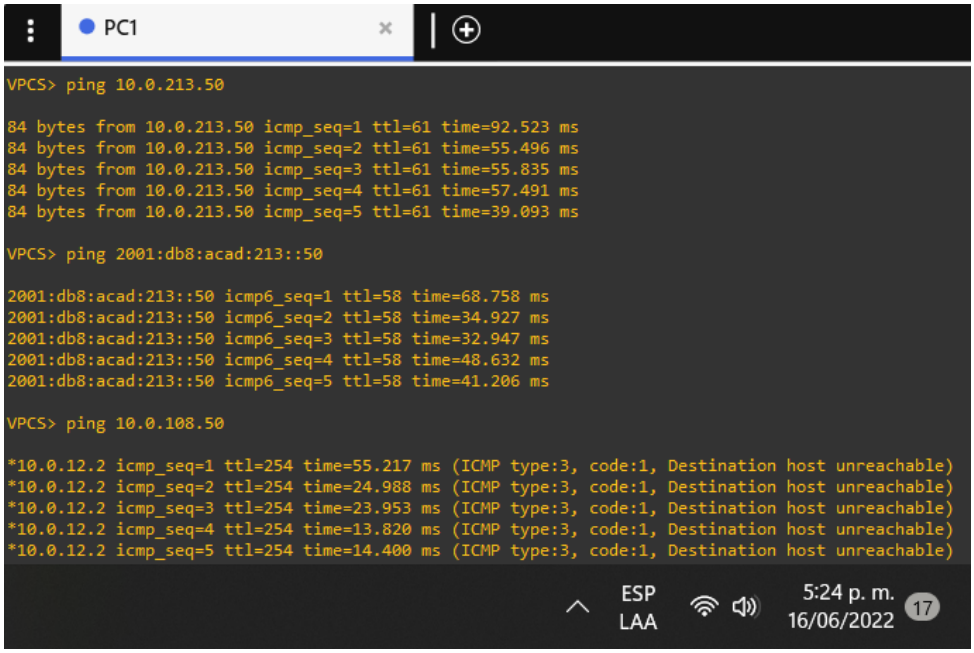
A1#Configure terminal	Ingresa al modo de configuración
A1(config)#interface e0/0	Se entra a las interfaces
A1(config-if)#switchport mode access	Se permite que el switch entre al modo de acceso permanente
A1(config-if)#switchport access vlan 8	Se da acceso a la vlan8
A1(config-if)#spanning-tree portfast	Se
A1(config-if)#no shutdown	Se habilitan las interfaces
A1(config-if)#exit	

Fuente: Autoría propia

Paso 3.5 Verifique la conectividad de PC a PC.

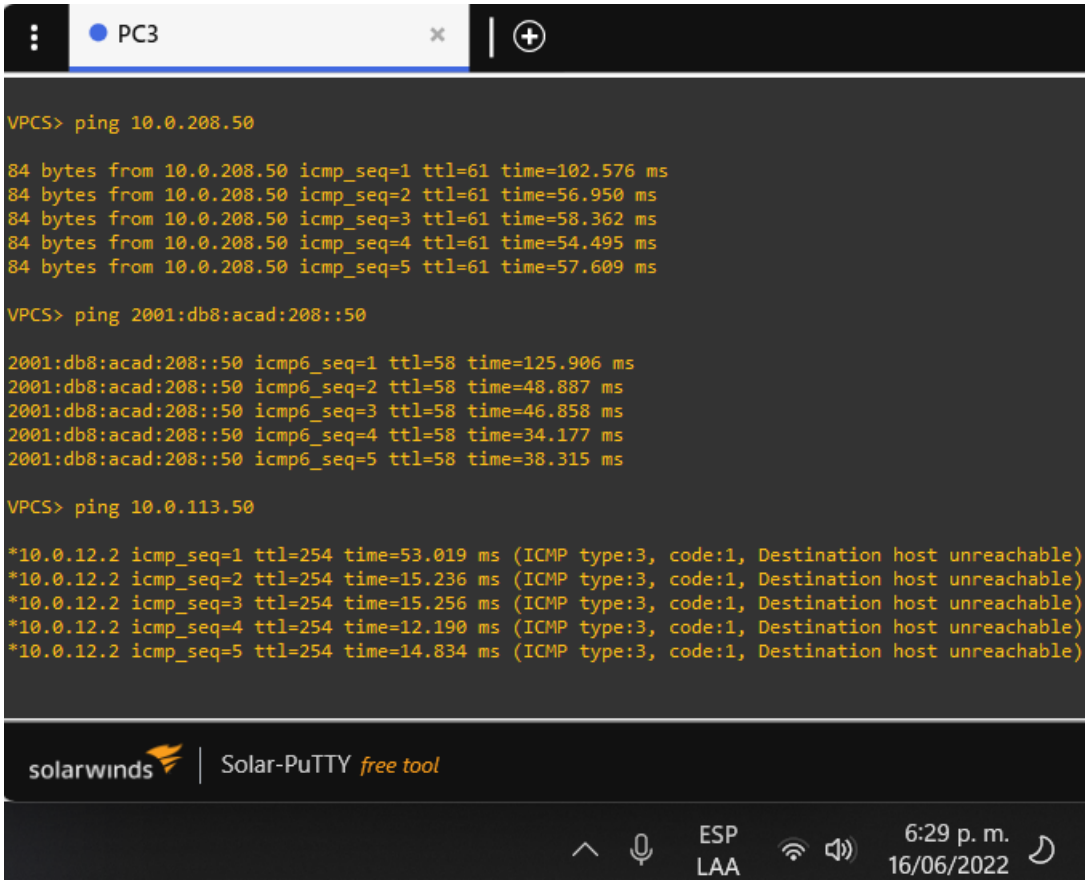
Desde la PC1, se verifica la conectividad IPv4 e IPv6 a la PC2 y que no haga conectividad con otro pc y desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4 y que no haga conectividad con otro pc.

Figura 8. Se verifica la conectividad de PC1 a PC2 y que no haga conectividad con PC3



Fuente: Escenario de configuración GNS3

Figura 9. Se verifica la conectividad de PC3 a PC4 y que no haga conectividad con PC1



Fuente: Escenario de configuración GNS3

Parte 4. Configurar la seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 30. Tareas de configuración

Task#	Task	Specification
4.1	En todos los dispositivos, modo EXE privilegiado seguro.	• Configure un secreto de habilitación de la siguiente manera: • Tipo de algoritmo: **SCRYPT** • Contraseña: **cisco12345cisco**
4.2	En todos los dispositivos, cree una cuenta de usuario local.	• Configure un usuario local: • Nombre: **admin** • Nivel de privilegio: **15** • Tipo de algoritmo: **SCRYPT** • Contraseña: **cisco12345cisco** .
4.3	En todos los dispositivos, habilite AAA y habilite la autenticación AAA.	Habilite la autenticación AAA usando la base de datos local en todas las líneas.

Fuente: Guía documento final

Paso 4.1 En todos los dispositivos, modo EXE privilegiado seguro.

Se agrega el modo EXE privilegiado seguro para poder tener el tipo de algoritmo SCRYPT como lo solicita la guía.

Tabla 31. Código de configuración para el modo EXE privilegiado seguro en R1

R1# configure terminal	Ingresa al modo de configuración
R1(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
R1(config)# exit	

Fuente: Autoría propia

Tabla 32. Código de configuración para el modo EXE privilegiado seguro en R2

R2# configure terminal	Ingresa al modo de configuración
R2(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
R2(config)# exit	

Fuente: Autoría propia

Tabla 33. Código de configuración para el modo EXE privilegiado seguro en R3

R3# configure terminal	Ingresa al modo de configuración
R3(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
R3(config)# exit	

Fuente: Autoría propia

Tabla 34. Código de configuración para el modo EXE privilegiado seguro en D1

D1# configure terminal	Ingresa al modo de configuración
D1(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
D1(config)# exit	

Fuente: Autoría propia

Tabla 35. Código de configuración para el modo EXE privilegiado seguro en D2

D2# configure terminal	Ingresa al modo de configuración
D2(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
D2(config)# exit	

Fuente: Autoría propia

Tabla 36. Código de configuración para el modo EXE privilegiado seguro en A1

A1# configure terminal	Ingresa al modo de configuración
A1(config)# enable algorithm-type SCRYPT secret cisco12345cisco	Se agrega el modo EXE privilegiado seguro
A1(config)# exit	

Fuente: Autoría propia

Paso 4.2 En todos los dispositivos, cree una cuenta de usuario local.

Se crea una cuenta de usuario local con sus respectivos caracteres en cada uno de los dispositivos y habilitando el modelo AAA y habilitando la autenticación AAA.

Tabla 37. Código de configuración para crear una cuenta de usuario local con todos los protocolos en R1

R1# configure terminal	Ingresa al modo de configuración
R1(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
R1(config)# aaa new-model	Se habilita el modelo AAA

R1(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
R1(config)# exit	

Fuente: Autoría propia

Tabla 38. Código de configuración para crear una cuenta de usuario local con todos los protocolos en R2

R2# configure terminal	Ingresa al modo de configuración
R2(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
R2(config)# aaa new-model	Se habilita el modelo AAA
R2(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
R2(config)# exit	

Fuente: Autoría propia

Tabla 39. Código de configuración para crear una cuenta de usuario local con todos los protocolos en R3

R3# configure terminal	Ingresa al modo de configuración
R3(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
R3(config)# aaa new-model	Se habilita el modelo AAA
R3(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
R3(config)# exit	

Fuente: Autoría propia

Tabla 40. Código de configuración para crear una cuenta de usuario local con todos los protocolos en D1

D1# configure terminal	Ingresa al modo de configuración
D1(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
D1(config)# aaa new-model	Se habilita el modelo AAA
D1(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
D1(config)# exit	

Fuente: Autoría propia

Tabla 41. Código de configuración para crear una cuenta de usuario local con todos los protocolos en D2

D2# configure terminal	Ingresa al modo de configuración
D2(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
D2(config)# aaa new-model	Se habilita el modelo AAA
D2(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
D2(config)# exit	

Fuente: Autoría propia

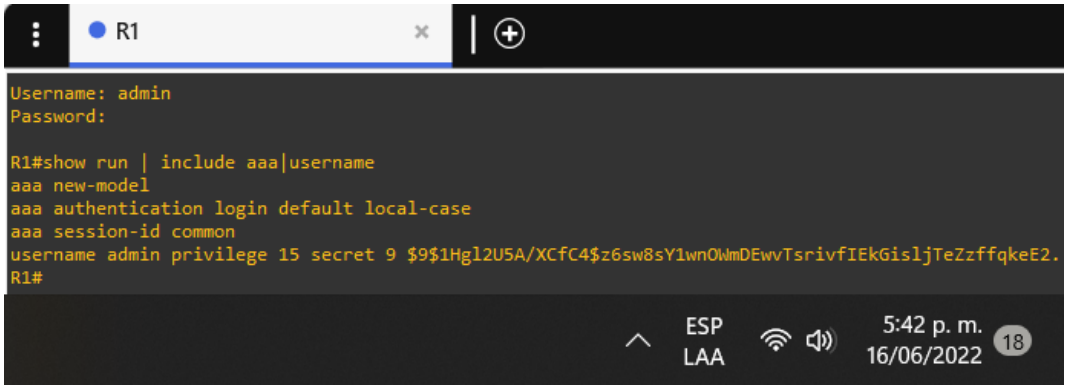
Tabla 42. Código de configuración para crear una cuenta de usuario local con todos los protocolos en A1

A1# configure terminal	Ingresa al modo de configuración
A1(config)# username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Se le agrega un usuario, en privilegio nivel 15 y con un algoritmo tipo SCRYPT
A1(config)# aaa new-model	Se habilita el modelo AAA
A1(config)# aaa authentication login default local-case	Se habilita la autenticación del modelo AAA con datos locales en todas las líneas
A1(config)# exit	

Fuente: Autoría propia

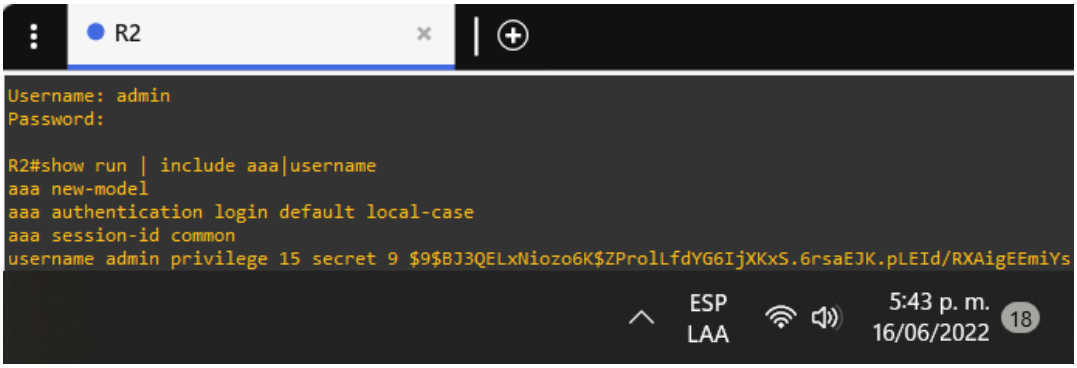
Paso 4.3 En todos los dispositivos, habilite AAA y habilite la autenticación AAA.

Figura 10. Se habilita AAA y habilita la autenticación AAA en R1



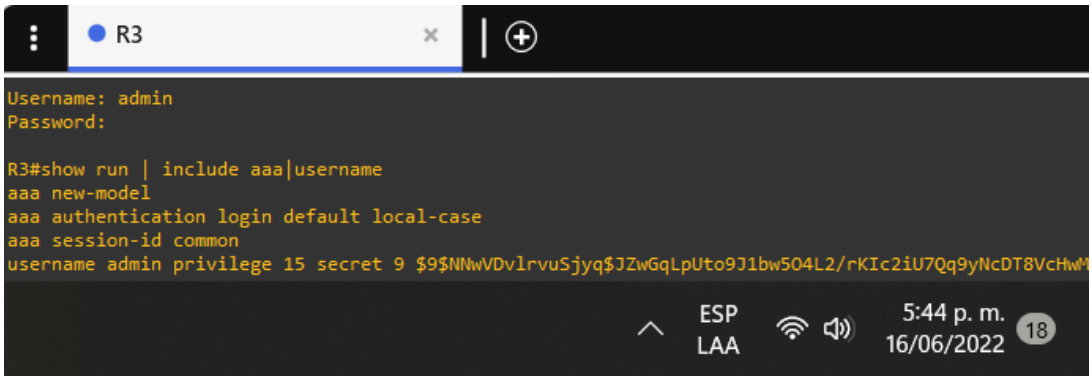
Fuente: Escenario de configuración GNS3

Figura 11. Se habilita AAA y habilita la autenticación AAA en R2



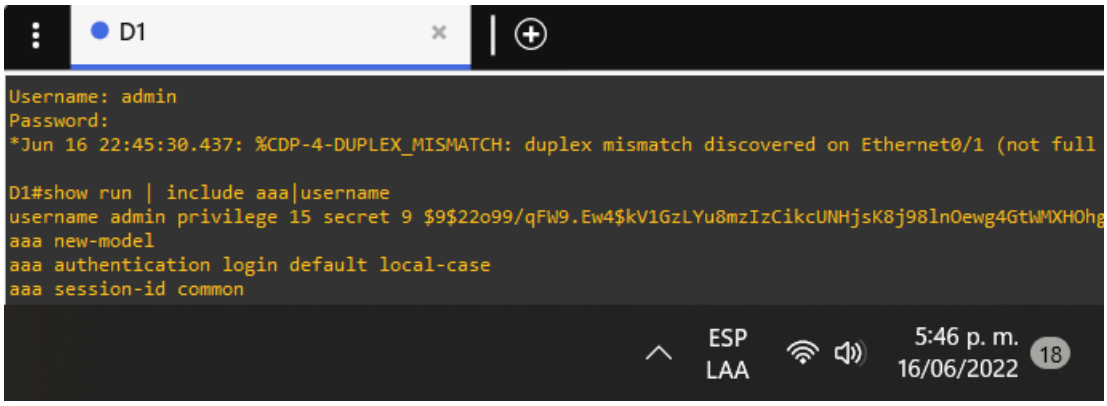
Fuente: Escenario de configuración GNS3

Figura 12. Se habilita AAA y habilita la autenticación AAA en R3



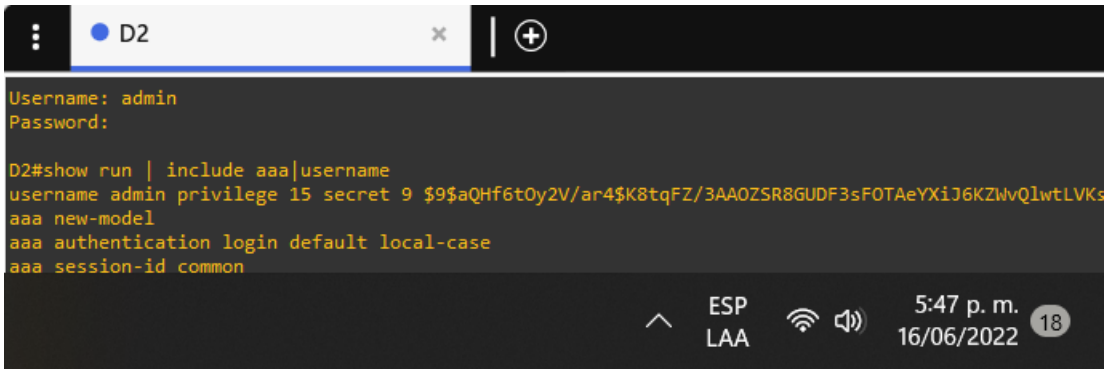
Fuente: Escenario de configuración GNS3

Figura 13. Se habilita AAA y habilita la autenticación AAA en D1



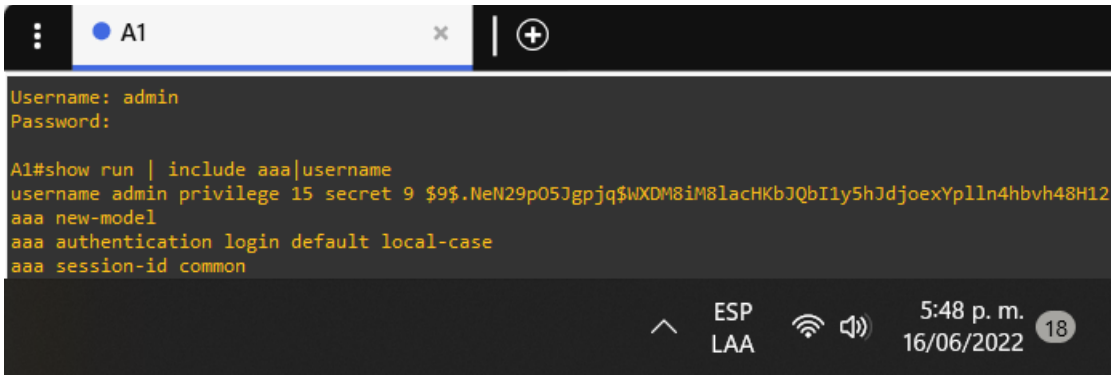
Fuente: Escenario de configuración GNS3

Figura 14. Se habilita AAA y habilita la autenticación AAA en D2



Fuente: Escenario de configuración GNS3

Figura 15. Se habilita AAA y habilita la autenticación AAA en A1



Fuente: Escenario de configuración GNS3

CONCLUSIONES

Con el desarrollo de esta prueba de habilidades del diplomado CCNP se logra realizar el diseño del escenario propuesto de manera satisfactoria, luego se realiza la configuración paso a paso de las configuraciones básicas en cada dispositivo. También se hace la configuración de capa dos, dando comunicación a los switches para que se comuniquen entre sí, por ende, las PC han podido dar ping.

Se estudian las configuraciones para crear VRFs en los routers, con el fin de crear una red que tenga dos VRFs una llamada Special-Users y otra llamada General-Users con sus respectivos encapsulados para poder diferenciarlas. En otro sentido se implementó los protocolos de enrutamiento de la red, para la configuración de las rutas estáticas, con el fin de comunicar el sistema creado, estableciendo la comunicación de la red y subredes del escenario.

Con este trabajo se pudo concluir que un conocimiento profundo de cómo configurar la seguridad de la red IP de Cisco es una necesidad para cualquier rama de la ingeniería que trabaje en el mundo interconectado de hoy en día. No hay duda de que los ataques a las redes empresariales están aumentando en frecuencia y sofisticación, por eso el adquirir conocimiento, habilidades, capacidades y destrezas para realizar diagnósticos rápidos y configuraciones eficientes evitaran que personas ajenas extraigan información que circulan en la red.

Para el desarrollo de este diplomado se utiliza el simulador GNS3 ya que Packet Tracer no soporta ciertos comandos que eran necesarios para poder realizar el escenario propuesto, dificultando o haciendo nulo que se pueda realizar y ejecutar de manera correcta todos los puntos dados en la guía.

BIBLIOGRAFIA

EDGEWORTH, Bradley, et al. IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, et al. Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, et al. Spanning Tree Protocol**.** CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, et al. Advanced Spanning Tree**.** CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, et al. Multiple Spanning Tree Protocol**.** CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, et al. VLAN Trunks and EtherChannel Bundles**.** CCNP and CCIE Enterprise Core ENCOR 350-401. ciscopress. [en línea], 2020. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8