DIPLOMADO DE PROFUNDIZACION CISCO PRUEBAS DE HABILIDADES PRACTICAS CCNP

JOHN EDINSON SOLORZANO LUGO

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOHN EDINSON SOLORZANO LUGO

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
INGENIERÍA ELECTRONICA
NEIVA-HUILA
2022

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Nieva, 26 de junio del 2022

Agradecimiento

Quisiera agradecer a mi madre Sonia Lugo Sáenz, a mi colega María Geraldine Tovar por todo su apoyo económico, emocional y motivacional, a todos los que me apoyaron a lo largo de la carrera como ingeniero en formación, Gracias a mis compañeros del grupo de redes sociales, porque sin su apoyo este hubiera sido un camino muy difícil hacia la victoria, ya que influyeron y permitieron superar diferentes dificultades a lo largo de la universidad para concretar la elaboración de este documento.

Doy gracias a Dios por nunca dejarme solo en una dura batalla para lograr mis metas como ingeniero electrónico, agradecerle por los días brillantes que me dio y la esperanza de vida que me dio cada mañana cuando salía el sol, tomó mucho tiempo, pero al final hemos llegado al camino que se esperaba obtener y darme la fuerza para salir a comer por todo el mundo.

También quiero agradecer al grupo de docentes de la Universidad Nacional Abierta y a Distancia (UNAD). quienes, a lo largo de los años estudiantiles con sus conocimientos, habilidades y apoyo me permitieron superar las diferentes etapas y alcanzar los resultados esperados.

Tabla de contenido

Lista de tablas

Lista de figuras

Glosario

ELECTRÓNICA: Es una rama de la física la cual se centra en la especialización de ingeniería, dedicada al estudio y creación de nuevas tecnologías y solución de problemas en relación con el flujo de cargas eléctricas en función a una acción.

ENRUTAMIENTO ESTATICO: El enrutamiento estático proporciona un método que otorga a los ingenieros de redes control absoluto sobre las rutas por las que se transmiten los datos en una internetwork. Para adquirir este control, en lugar de configurar protocolos de enrutamiento dinámico para que creen las tablas de enrutamiento, se crean manualmente.

IPV4: Es un protocolo de internet de cuarta generación, el cual permite la conexión en red con un direccionamiento de 32 bits en 4 bloques de 3 caracteres cada uno.

IPV6: Es el protocolo actualizado del IPv4, el cual resuelve los inconvenientes de agotamiento de direcciones, teniendo como principio el internet sin límites.

PING: es una medida que sirve para medir latencia, la cual es el tiempo que tarda transmitir un paquete de datos dentro de la red.

PROTOCOLO DE ENRUTAMIENTO: Es el protocolo secuencial el cual especifica la forma en la que los routers, se comunican permitiendo crear rutas dando dirección de tráfico para él envió de paquetes de información.

PROTOCOLO EIGRP: Es un protocolo el cual está basado en CISCO, tipo vector distancia dual con un desarrollo algorítmico de actualizaciones difusas enviando información a los dispositivos routers de la misma área.

PROTOCOLO OSPF: Es un protocolo enlace-estado el cual fue creado para implementarlo en las redes con IP, basado en algoritmo con el camino más corto. Es decir que, por medio del algoritmo, se busca la ruta más corta en la comunicación.

TOPOLOGÍA DE RED: Es la forma en la que se realiza la organización de una red, teniendo en cuenta la forma en la que se diseña en plano físico.

VRF: es el enrutamiento virtual y reenvío (VRF) es una tecnología incluida en routers de red IP, que permite a varias instancias de una tabla de enrutamiento existir en un Router y trabajar simultáneamente.

Resumen

Por medio del desarrollo del escenario practico relacionado al diplomado de profundización CCNP CISCO, generando las habilidades necesarias para resolver situaciones relacionadas a la ingeniería electrónica para el manejo de redes locales y empresariales. Creando una topología de red, configurando ajustes básicos de los dispositivos presentes dando un direccionamiento de las interfaces, teniendo en cuenta que la red permita la accesibilidad completa entre los dispositivos y que el host tenga soporte en la puerta de enlace, validando las conexiones necesarias para dar solución a lo propuesto y obtener un correcto enrutamiento.

Se configuran los dispositivos en capa 2, configurando las interfaces como troncales y puentes raíz para que se pueda verificar la conmutación, se configuran parámetros de tipo OSPF y redundancia de primer salto para los hosts, al igual se configuran mecanismos de seguridad y funciones administrativas. se desarrolla la actividad en la herramienta GNS3 la cual tiene una interfaz que permite la emulación y configuración de dispositivos de redes virtuales y reales, utilizando 3 Routers, 3 switches y 4 PCs según la imagen dada de la topología de red del escenario, donde se configura cada dispositivo con el fin de que tenga estos los protocolos de enrutamientos adecuados para que la red tenga accesibilidad de extremo a otro, conmutando la configuración de los hosts y las puertas de enlace default Gateway, teniendo los protocolos configurados según la tabla de direccionamiento, teniendo así un correcto enrutamiento.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica, Gsn3, interfaces virtuales, router, Switch.

Abstract

Through the development of the practical scenario related to the CCNP CISCO deepening diploma, generating the necessary skills to solve situations related to electronic engineering for the management of local and business networks. Creating a network topology, configuring basic settings of the devices present giving an addressing of the interfaces, taking into account that the network allows complete accessibility between the devices and that the host has support in the gateway, validating the necessary connections to give a solution to the proposal and obtain acorrect routing.

Layer 2 devices are configured, configuring the interfaces as trunks and root bridges so that switching can be verified, OSPF type parameters and first-hop redundancy are configured for the hosts, as well as security mechanisms and administrative functions. The activity is carried out in the GNS3 tool, which has an interface that allows the emulation and configuration of virtual and real network devices, using 3 Routers, 3 switches and 4 PCs according to the given image of the network topology of the scenario, where configures each device so that it has the appropriate routing protocols so that the network has end-to-end accessibility, switching the configuration of the hosts and the default gateway, having the protocols configured according to the addressing table, thus having a correct routing.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics, Gsn3, interface virtual, router, Switch.

Introducción

En el presente documento se presenta el trabajo de Diplomado de profundización CISCO prueba de habilidades practicas CCNP. El cual permite fortalecer las habilidades y capacidades dando solución a diferentes situaciones presentes en las redes empresariales tipo LAN y WAN. El correcto desarrollo permite obtener el título de ingeniero, por medio del diplomado de profundización teniendo en cuenta los diferentes requisitos que se deben cumplir para ello. Dado que al terminar el diplomado se tendrán múltiples habilidades sobre el manejo de comandos IOS, dando así soluciones como profesional en redes escalables.

El documento presenta el desarrollo de 6 etapas practicas las cuales ponen a prueba las habilidades adquiridas de comprensión y desarrollo de situaciones relacionadas con el Networking. Se realiza la interacción virtual con los diferentes e-learning y software, desarrollando las temáticas relacionadas a las redes LAN y WAN como los protocolos de enrutamiento avanzados de Routing, en los protocolos soluciones en el ámbito de enrutamiento avanzado tenido en cuenta las configuraciones al igual que mecanismos de seguridad a losdispositivos con el fin de que permita la autenticación de identidad a los usuarios, al igual que la implementación de funciones administrativas de red básicas.

Se desarrolla el laboratorio en la herramienta GNS3 de acuerdo con un escenario propuesto, utilizando 3 Routers, 3 switches y 4 PCs, contrayendo la topología de red, de acuerdo a una serie de pasos, configurando cronológicamente parámetros básicos de direccionamiento, con el fin de que se pueda tener una accesibilidad completa entre los hosts.

Desarrollo

Topología de la Red para trabajar según documento

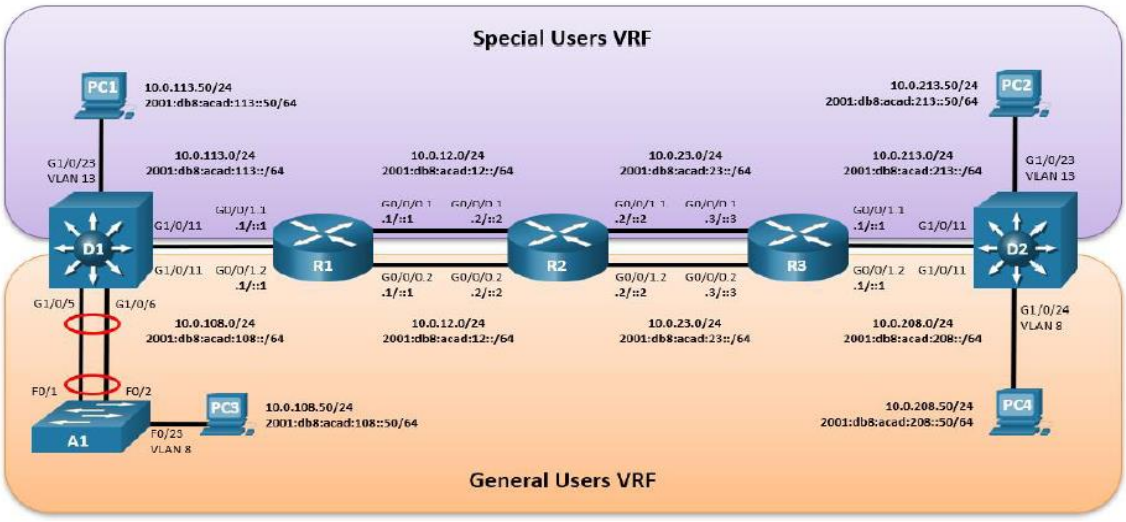

Figura 1 Topología escenario propuesto

Fuente: Pruebas habilidades CCNP

Tabla 1: Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G1/0.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G1/0.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G1/0.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3

	G1/0.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G1/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G1/0.2	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

Tabla 1 Tabla de direccionamiento

Fuente: Pruebas y habilidades CCNP

Objetivos

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

https://www.mediafire.com/file/o3sddfnyk7huef2/Componentes_Cisco.zip/file

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

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

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

Rta: Se realiza el cableado de los equipos según la topología requerida y con los cables necesarios.

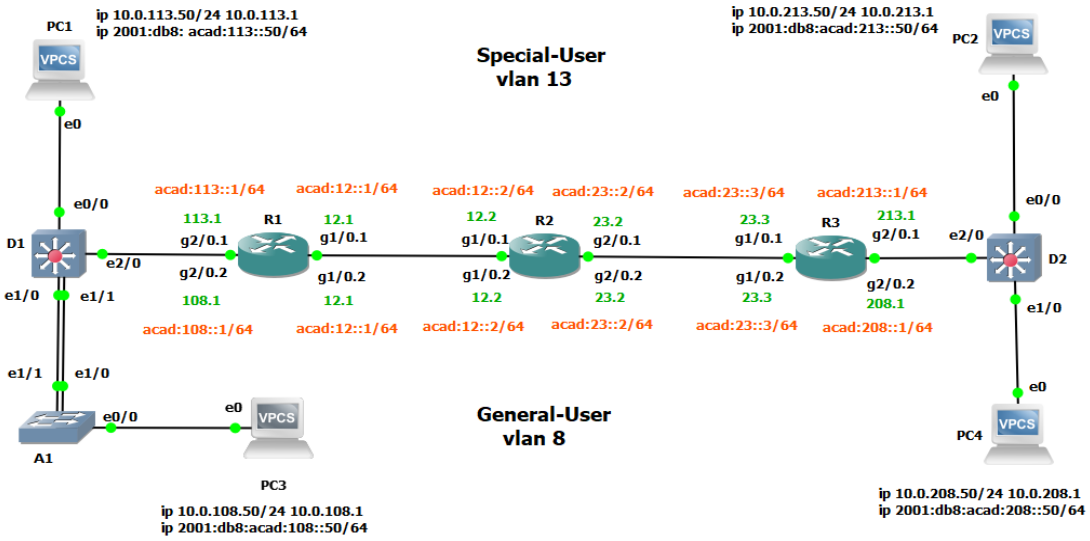

Figura 2 Topología realizada en Gsn3

Fuente: Prueba de habilidades CCNP

1.2: 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.

Router R1

hostname R1

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

Router R2

hostname R2

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

Router R3

hostname R2

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

Switch D1

hostname D1

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

vlan 8

name General-Users

exit

vlan 13

name Special-Users

exit

Switch D2

hostname D2

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

vlan 8

name General-Users

exit

vlan 13

name Special-Users

exit

Switch A1

hostname A1

ipv6 unicast-routing

no ip domain lookup

banner motd #R1, ENCOR Skills Assessment Scenario 2 # line console 0

excec-timeout 0 0

logging synchronous

exit

vlan 8

name General-Users

exit

1.3Guarde las configuraciones en cada uno de los dispositivos.

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

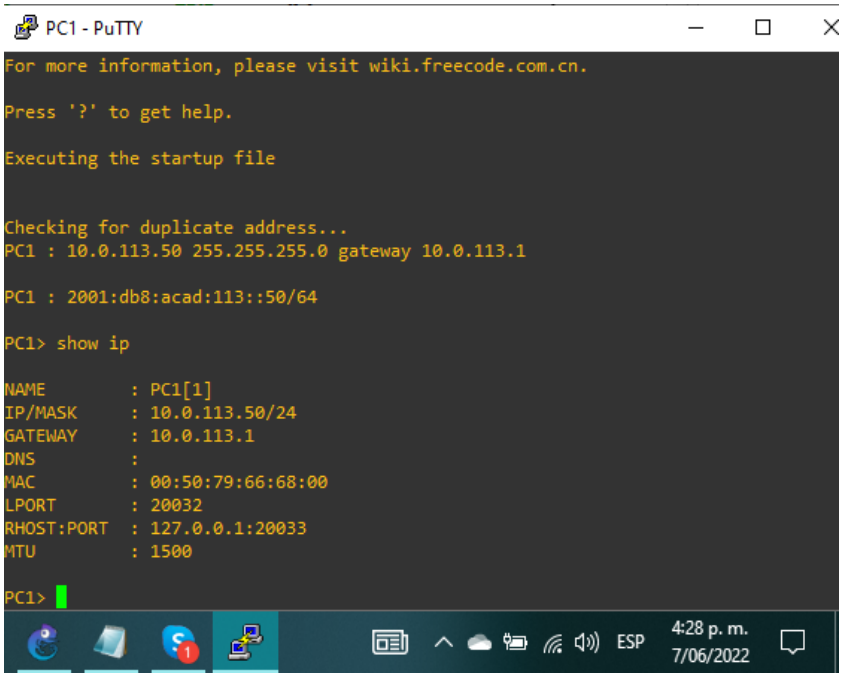

Figura 3 configuración PC1 en GNS3

Fuente: Propia

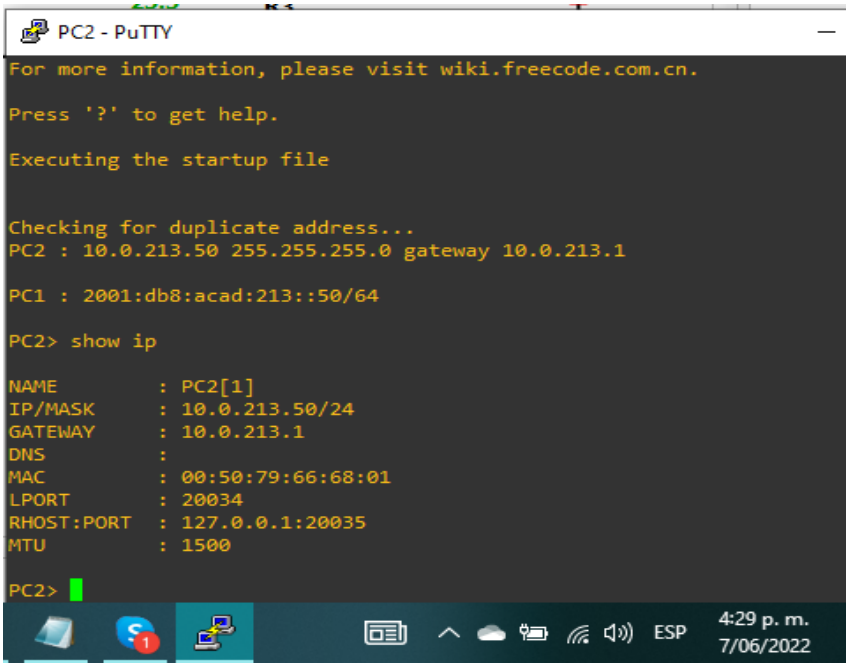

Figura 4 configuración PC2 en GNS3

Fuente: Propia

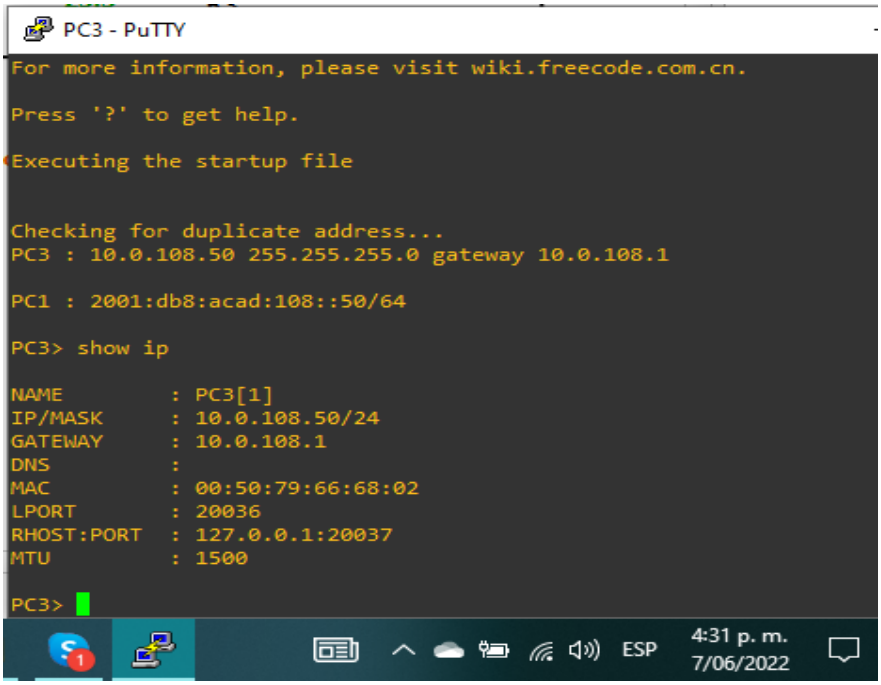

Figura 5 configuración PC3 en GNS3

Fuente: Propia

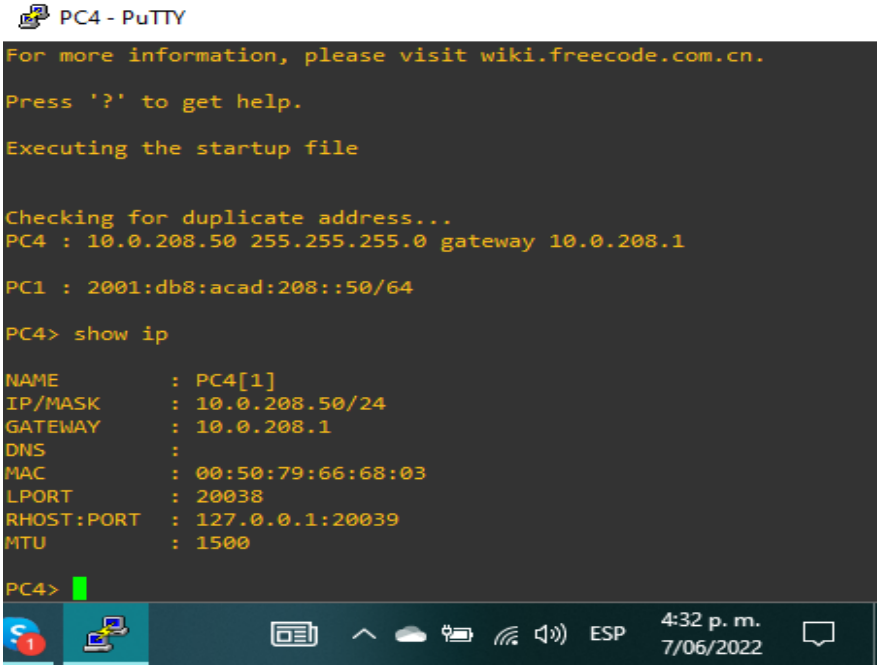

Figura 6 configuración PC4 en GNS3

Fuente: Propia

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 pinga R3 en cada VRF.Sus tareas de configuración son las siguientes:

Task#	Task	Specific ation
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.
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 theVRFs. 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
2.3	On R1 and R3, configure default static routes pointing to R2.	Configure VRF static routes for both IPv4 andIPv6 in both VRFs.
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

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

Configuración de las subinterfaces VRF	
R1	**configuración VRF-Router 1** config term // entramos a la configuración global vrf definition Special-User // definimos nombre del VRF virtual vlan 13 address-family ipv4 // agregamos la familia del protocolo ipv4 address-family ipv6 // agregamos la familia del protocolo ipv6 exit //salida de la configuración vrf definition General-User // definimos nombre del VRF virtual vlan 8 address-family ipv4 // agregamos la familia del protocolo ipv4 address-family ipv6 // agregamos la familia del protocolo ipv6 exit // salida del modo interface

Configuración de las subinterfaces VRF	
R2	**configuración VRF-Router 2** config term // entramos a la configuración global vrf definition Special-User // definimos nombre del VRF virtual vlan 13 address-family ipv4 // agregamos la familia del protocolo ipv4 address-family ipv6 // agregamos la familia del protocolo ipv6 exit // salida de configuración vrf definition General-User // definimos nombre VRF virtual vlan 8 address-family ipv4 // agregamos familia del protocolo ipv4 address-family ipv6 // agregamos familia del protocolo ipv6 exit // salida del modo interface

Configuración VRF para General - Special	
R3	**configuración VRF-Router 1** config term // ingresamos a la configuración global vrf definition Special-User // definimos nombre del VRF virtual address-family ipv4 // agregamos la familia del protocolo ipv4 address-family ipv6 // agregamos la familia del protocolo ipv6 exit // salida de la configuración vrf definition General-User // definimos nombre del VRF virtual address-family ipv4 // agregamos la familia del protocolo ipv4 address-family ipv6 // agregamos la familia del protocolo ipv6 exit // salida de la configuración

Tabla 2 configuración VRF Vlan 13,8

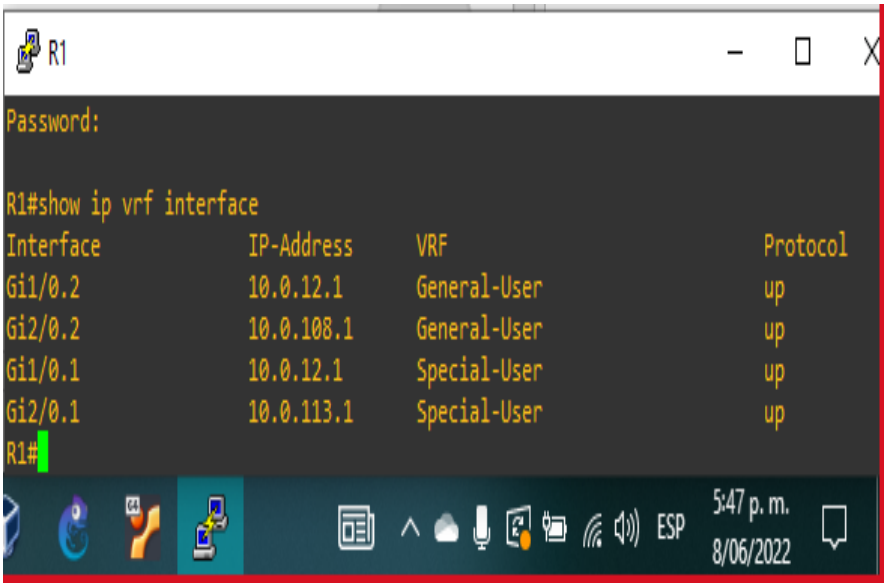

Figura 7 interfaces vrf Router 1

Fuente: propia

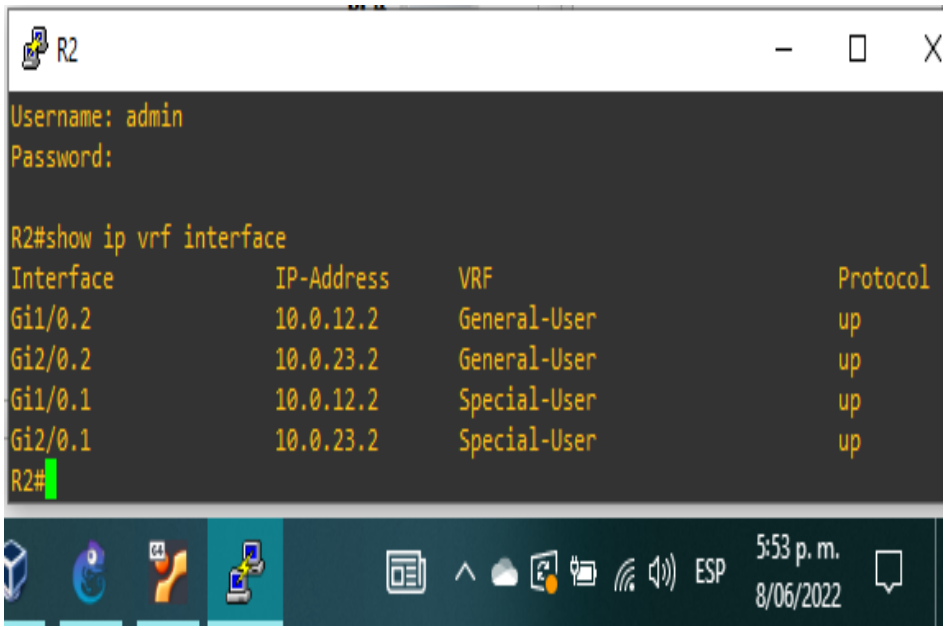

Figura 8 interfaces vrf Router 2

Fuente: propia

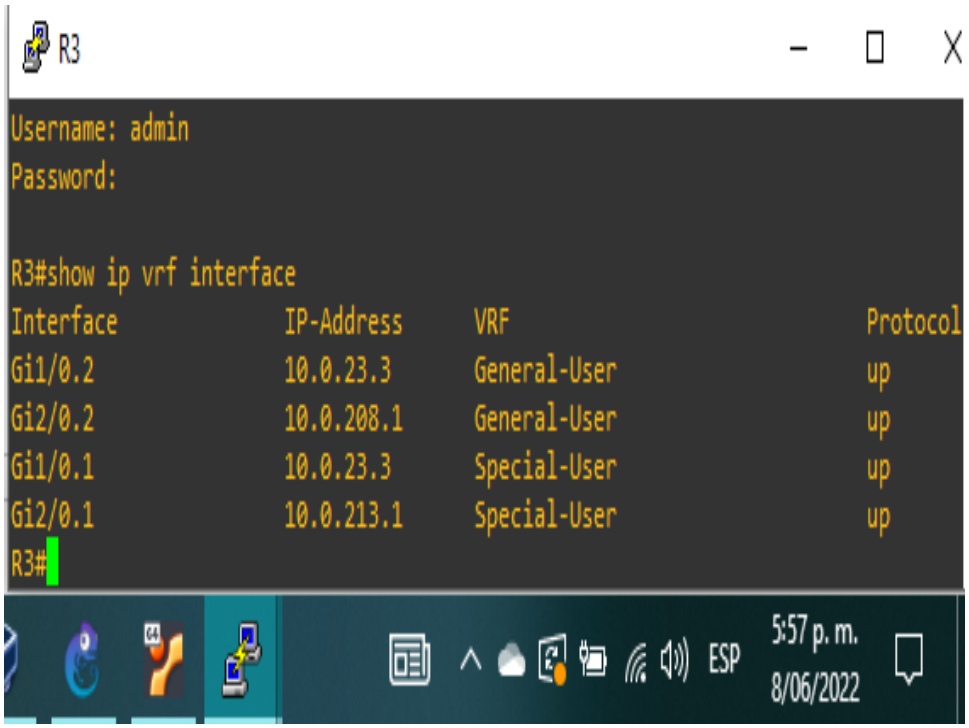

Figura 9 interfaces vrf Router 3

Fuente: propia

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

Configuración de las subinterfaces VRF 2.2	
R1	Config term // ingresamos al modo configuración global interface g1/0 // ingresamos a la interface del Router 1 g1/0 no shutdown // habilitamos la interface g1/0 **interface g1/0.1 // ingresamos a las subinterfaces** encapsulation dot1Q 13 // protocolo permite un enlace troncal Vlan 13 vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.12.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:12::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::1:1 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface **interface g1/0.2 // ingresamos a las subinterfaces** encapsulation dot1Q 8 // protocolo permite un enlace troncal Vlan 8 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.12.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:12::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::1:2 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface

	interface g2/0.1 // ingresamos a las subinterfaces encapsulation dot1Q 13 // protocolo permite un enlace troncal Vlan 13 vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.113.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:108::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::1:3 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida de la configuración **interface g2/0.2 // ingresamos a las subinterfaces** encapsulation dot1Q 8 // protocolo permite un enlace troncal Vlan 8 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.108.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:108::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::1:4 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface wr // guardamos configuración

Configuración de las subinterfaces VRF 2.2	
R2	Config term // ingresamos al modo configuración global interface g1/0 // ingresamos a la interface del Router 2 g1/0 no shutdown // habilitamos la interface g1/0 **interface g1/0.1 // ingresamos a las subinterfaces** encapsulation dot1Q 13 // protocolo permite un enlace troncal Vlan 13

	vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.12.2 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:12::2/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::2:1 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface **interface g1/0.2 // ingresamos a las subinterfaces** encapsulation dot1Q 8 // protocolo permite un enlace troncal Vlan 8 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.12.2 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:12::2/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::2:2 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface **interface g2/0.1 // ingresamos a las subinterfaces** encapsulation dot1Q 13 // protocolo permite un enlace troncal Vlan 13 vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.23.2 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:23::2/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::2:3 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida de la configuración **interface g2/0.2 // ingresamos a las subinterfaces**

	encapsulation dot1Q 8 // protocolo permite un enlace troncal Vlan 8 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.23.2 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:23::2/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::2:4 link-local // agregamos su link local no shutdown // habilitamos la interface exit // salida del modo interface wr // guardamos configuración

Configuración de las subinterfaces VRF 2.2	
R3	Router 3 Config term // ingresamos al modo configuración global interface g1/0 // ingresamos a la interface física del Router 3 g1/0 no shutdown // habilitamos la interface **interface g1/0.1 // ingresamos a las subinterfaces virtual** encapsulation dot1Q 13 // protocolo permite un enlace troncal Vlan 13 vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.23.3 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:23::3/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::3:1 link-local // agregamos su link local no shutdown // habilitamos la subinterfaz virtual exit // salida del modo interface **interface g1/0.2 // ingresamos a las subinterfaces virtual** encapsulation dot1Q 8 // protocolo que permite un enlace troncal vlan8 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.23.3 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:23::3/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::3:2 link-local // agregamos su link local

	no shutdown // habilitamos la subinterfaz virtual exit // salida del modo interface interface g2/0 // ingresamos a la interface física del Router 3 g2/0 no shutdown // habilitamos la interface **interface g2/0.1 // ingresamos a las subinterfaces virtual** encapsulation dot1Q 13 // protocolo que permite un enlace troncal vlan 13 vrf forwarding Special-User // agregamos el VRF configurado ip address 10.0.213.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:208::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::3:3 link-local // agregamos su link local no shutdown // habilitamos la subinterfaz virtual exit // salida del modo interface **interface g2/0.2 // ingresamos a las subinterfaces virtual** encapsulation dot1Q 8//protocolo que permite un enlace troncal vlan13 vrf forwarding General-User // agregamos el VRF configurado ip address 10.0.208.1 255.255.255.0 // agregamos su ip y mascara ipv4 ipv6 address 2001:db8:acad:208::1/64 // agregamos su ip y mascara ipv6 ipv6 address fe80::3:4 link-local // agregamos su link local no shutdown // habilitamos la interface virtual exit // salida del modo interface

Tabla 3 configuración interfaces ipv4 y ipv6 en las VRF

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

Configuración rutas estáticas para Router 1 protocolo ipv4 y ipv6	
R1	Protocolo ipv4 ip route 0.0.0.0 0.0.0.0 10.0.12.2 // rutas estáticas para llegar a R3 ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.12.2 // ruta ipv4

	ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.12.2 // ruta ipv4 protocolos ipv6 ipv6 route vrf General-User::/0 2001:DB8:ACAD:12::2 // rutas ipv6 ipv6 route vrf Special-User::/0 2001:DB8:ACAD:12::2 // rutas
Configuración rutas estáticas Router 2 protocolo ipv4 y ipv6	
R2	 protocolos ipv4 ip route vrf General-User 10.0.108.0 255.255.255.0 10.0.12.1 ip route vrf General-User 10.0.208.0 255.255.255.0 10.0.23.3 ip route vrf Special-User 10.0.113.0 255.255.255.0 10.0.12.1 ip route vrf Special-User 10.0.213.0 255.255.255.0 10.0.23.3 protocolos ipv6 ipv6 route vrf General-User 2001:db8:acad:108::/64 2001:db8:acad:12::1 ipv6 route vrf General-User 2001:db8:acad:208::/64 2001:db8:acad:23::3 ipv6 route vrf Special-User 2001:db8:acad:113::/64 2001:db8:acad:12::1 ipv6 route vrf Special-User 2001:db8:acad:213::/64 2001:db8:acad:23::3
R3	Configuración rutas estáticas Router 3 protocolo ipv4 y ipv6 Protocolo ipv4 ip route vrf General-User 0.0.0.0 0.0.0.0 10.0.23.2 // ruta ipv4 ip route vrf Special-User 0.0.0.0 0.0.0.0 10.0.23.2 ruta ipv4 protocolo ipv6 ipv6 route vrf General-User ::/0 2001:DB8:ACAD:23::2 ruta ipv6 ipv6 route vrf Special-User ::/0 2001:DB8:ACAD:23::2 ruta ipv6

Tabla 4 configuración de las rutas estáticas R1 R2 R3

2.4 Verifique la conectividad en cada VRF

Desde R1, verifique la conectividad a R3:

Ping vrf General-User 10.0.208.1
Ping vrf General-User 2001:db8:acad:208::1

Ping vrf Special-User 10.0.213.1
Ping vrf Special-User 2001:db8:acad:213::1

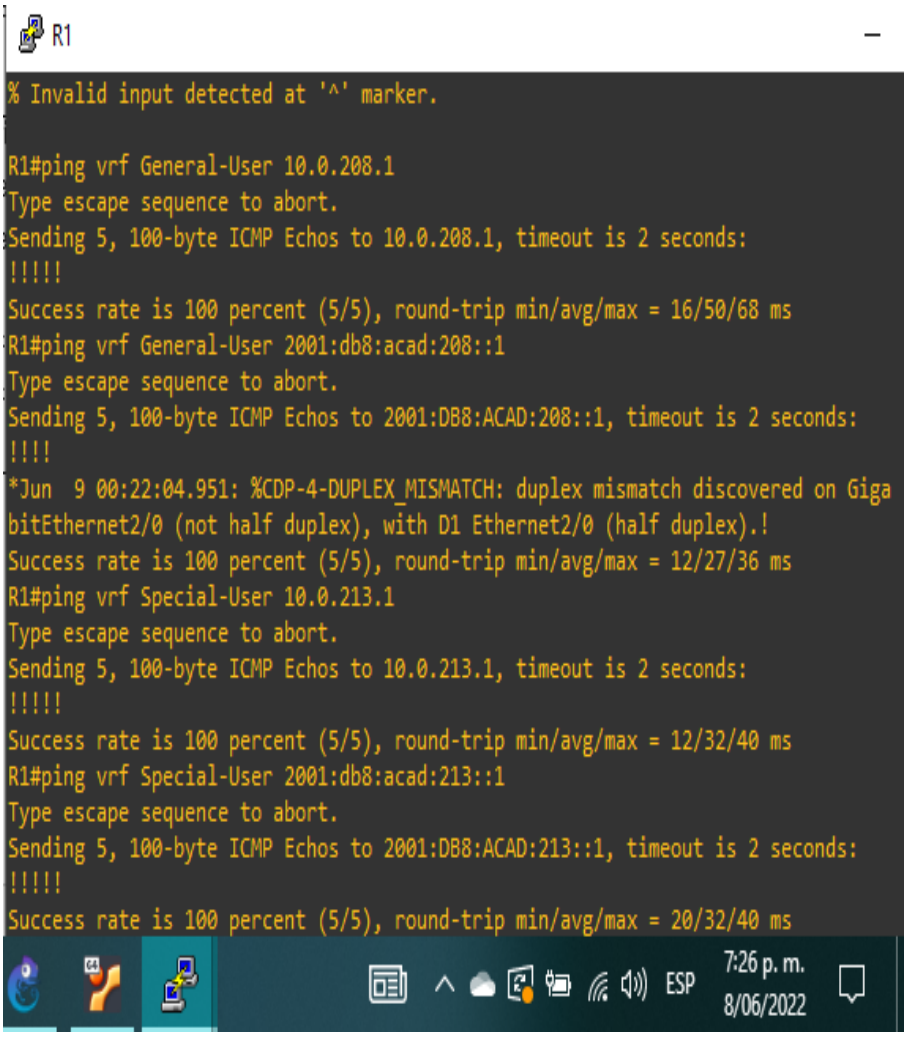

Figura 10 ping interfaces vrf Genera-Special – IPV6-IPV4

Fuente: Propia

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:

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.
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.
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
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.
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.

3.1 en D1, D2 y A1 deshabilitar todas las interfaces, en D1 y D2 apague e0/0, e1/0, e2/0, e3/0.

Configuración del Switch D1	
D1	**3.1 apagar las interfaces** Config term // ingresar al modo configuración global interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 // rango de interface de 1 a 3 shutdown// comando para apagar las interfaces seleccionadas

Configuración del Switch D2	
D2	**3.1 apagar las interfaces** Config term // ingresar al modo configuración global interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 // rango de interface de 1 a 3 shutdown// comando para apagar las interfaces seleccionadas

Configuración del Switch A1	
A1	**3.1 apagar las interfaces** Config term // ingresar al modo configuración global interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 // rango de interface de 1 a 3 shutdown// comando para apagar las interfaces seleccionadas

Tabla 5 configuración de apagar las interfaces de los Switch

3.2 en los Switch D1 Y D2 configurar los enlaces troncales de R1 Y R3

Configure y habilite el enlace e1/0-1 como enlace troncal.

Configuración del Switch D1	
D1	**3.2 Configuración enlace troncal D1**

	Config term // ingresar al modo configuración global inter ether 2/0 // enlace troncal del Router 1 switchport trunk encapsulation dot1Q // especifica el tipo encapsulación switchport mode trunk // habilita modo enlace troncal switchport trunk allowed Vlan 13,8 // se asocia a vlan 13,8 no shutdown // habilitamos la interface

Configuración del Switch D2	
D2	**3.2 configuración enlace troncal D2** Config term // ingresar al modo configuración global inter ether 2/0 // interface del enlace troncal del Router 3 switchport trunk encapsulation dot1Q // especifica el tipo encapsulación switchport mode trunk // habilita modo enlace troncal switchport trunk allowed Vlan 13,8 // se asocia a vlan 13,8 no shutdown // habilitamos la interface

Tabla 6 configuración enlace troncal de los switch D1 D2

3.3 en D1 Y A1 configuramos el EtherChannel

En D1 configure y habilite interface e1/0 e1/1
Canal de puerto 1 usando PAgP

En A1 configure y habilite interface e1/0 e1/1
Canal de puerto 1 usando PAgP

Configuración del Switch D1	
D1	**configuración del EtherChannel D1 interface e1/0-1** Config term // ingresar al modo configuración global inter range e1/0-1 // ingresamos las interfaces del EtherChannel switchport trunk encapsulation dot1Q // especifica el tipo encapsulación

	switchport mode trunk // habilita modo enlace troncal channel-group 1 mode desirable // la interface será administrada grupo 1 no shutdown // habilitar la interface

Configuración de los Switch A1	
A1	**3.3 configuración del EtherChannel D1** Config term // ingresar al modo configuración global inter range e1/0-1 // ingresamos las interfaces del EtherChannel switchport trunk encapsulation dot1Q // especifica el tipo encapsulación switchport mode trunk // habilita modo enlace troncal channel-group 1 mode desirable // la interface será administrada grupo 1 no shutdown // habilitamos la interface

Tabla 7 configuración del ethernet channel interface e1/0-1

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 interface e0/0 como un puerto de acceso de vlan 13 y habilite el portfast.

En D2 configure la interface e0/0 como un puerto de acceso de vlan 13 y habilite el portfast.

En D2 configure la interface e1/0 como un puerto de acceso de vlan 8 y habilite el portfast.

En A1 configure la interface e0/0 como un puerto de acceso de vlan 8 y habilite el portfast.

Configuración del Switch D1	
D1	**configuración de puertos de acceso SW D1** inter e0/0 // interface donde está conectada la pc1 switchport mode Access // colocar en puerto en modo acceso

	switchport access vlan 13 // agréguese en vlan 13 modo acceso spanning-tree portfast // establecer automáticamente el valor de prioridad no shutdown // habilitar la interface exit // salida del modo interface

Configuración de los Switch D2	
D2	**3.4 configuración de puertos de acceso SW D2** inter e0/0 // interface donde está conectada la pc2 switchport mode Access // colocar en puerto en modo acceso switchport access vlan 13 // agréguese en vlan 13 modo acceso spanning-tree portfast // establecer automáticamente el valor de prioridad no shutdown // habilitar la interface exit // salida del modo interface inter e1/0 // interface donde está conectada la pc4 switchport mode Access // colocar en puerto en modo acceso switchport access vlan 8 // agréguese en vlan 8 modo acceso spanning-tree portfast // establecer automáticamente el valor de prioridad no shutdown // habilitamos la interface exit // salida del modo interface wr // guardamos la configuración del Switch

Configuración de los Switch A1	
A1	**configuración de puertos de acceso SW A1** inter e0/0 // interface donde está conectada la pc3 switchport mode Access // colocar en puerto en modo acceso switchport access vlan 8 // agréguese en vlan 8 modo acceso spanning-tree portfast // establecer automáticamente el valor de prioridad no shutdown // habilitar la interface exit // salida del modo interface wr // guardamos la configuración

Tabla 8 configuración de puertos de acceso de los switch D1 D2 A1

3.5 verificar la conectividad de pc1 a pc2

Desde la PC1, verifique la conectividad IPv4 e IPv6 a la PC2.

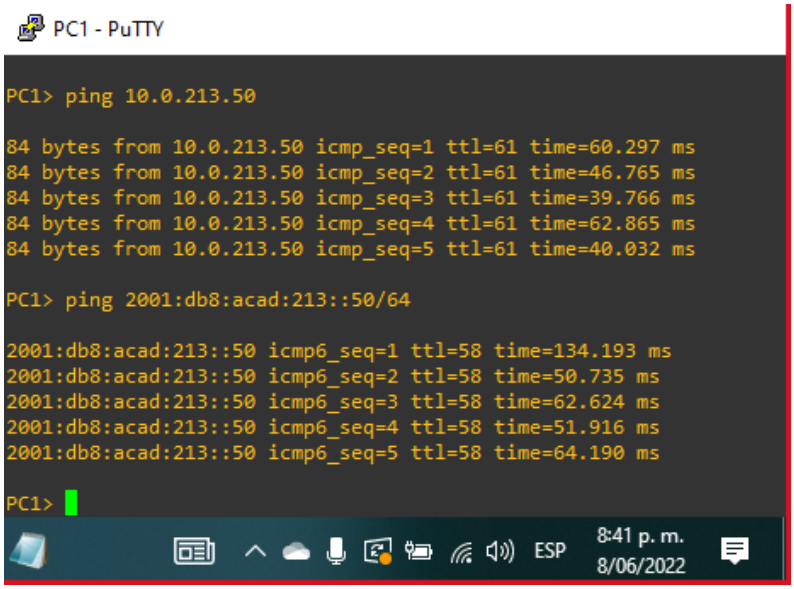

Figura 11 Ping de pc1 hasta pc2 ipv4 y ipv6

Fuente: propia

Desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4

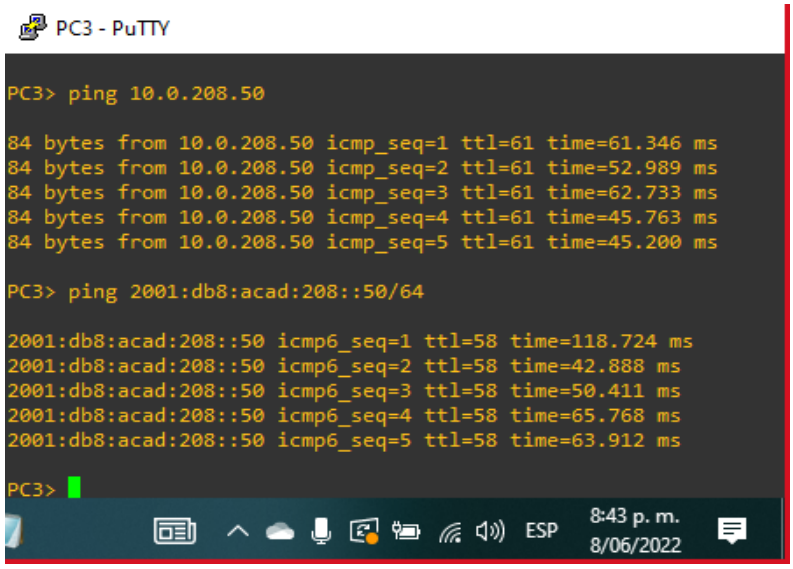

Figura 12 Ping de pc3 hasta pc4

Fuente: propia

Parte 4. Configure Security

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

Las tareas de configuración son las siguientes:

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	On all devices, create a local user account.	Configure a local user: • Name: **admin** • Privilege level: **15** • Algorithm type: **SCRYPT** • Password: **cisco12345cisco**.
4.3	On all devices, enable AAA and enable AAA authentication.	Enable AAA authentication using the local database on all lines.

4.1 En todos los dispositivos, modo EXE privilegiado seguro

R1	R1 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad
R2	R2 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad
R3	R3 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad
D1	D1 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad

D2	D2 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad
A1	A1 config ter // ingresamos al modo configuración global Service password-encryption // comando para cifrar contraseñas Enable secret cisco12345cisco // proporciona mayor seguridad

Tabla 9 configuración EXEC privilegiado usando el algoritmo SCRYPT

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

R1	R1 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig
R2	R2 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig
R3	R3 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig
D1	D1 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig
D2	D2 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig
A1	A1 config ter // ingresamos al modo configuración global Username admin secret 0 cisco12345cisco // indica nombre de usuario Username admin privilege 15 secret cisco12345cisco // usuario nivel privilig

Tabla 10 configuración de la cuenta encriptada SCRYPT con usuario local

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

R1	R1(config)#aaa new-model // aplica la autenticación local a la interface R1(config)# aaa authentication login default local // autenticación de dispositivos R1(config)# username admin password cisco12345cisco // uso usuario y contraseñas

R2	R2(config)#aaa new-model // aplica la autenticación local a la interface R2(config)# aaa authentication login default local // autenticación de dispositivos R2(config)# username admin password cisco12345cisco // uso de usuario y contraseñas
R3	R3(config)#aaa new-model // aplica la autenticación local a la interface R3(config)# aaa authentication login default local // autenticación de dispositivos R3(config)# username admin password cisco12345cisco // uso de usuario y contraseñas
D1	D1(config)#aaa new-model // aplica la autenticación local a la interface D1(config)# aaa authentication login default local // autenticación de dispositivos D1(config)# username admin password cisco12345cisco // uso de usuario y contraseñas
D2	D2(config)#aaa new-model // aplica la autenticación local a la interface D2(config)# aaa authentication login default local // autenticación de dispositivos D2(config)# username admin password cisco12345cisco // uso de usuario y contraseñas
A1	A1(config)#aaa new-model // aplica la autenticación local a la interface A1(config)# aaa authentication login default local // autenticación de dispositivos A1(config)# username admin password cisco12345cisco // uso de usuario y contraseñas

Tabla 11 configuración AAA y su autenticación

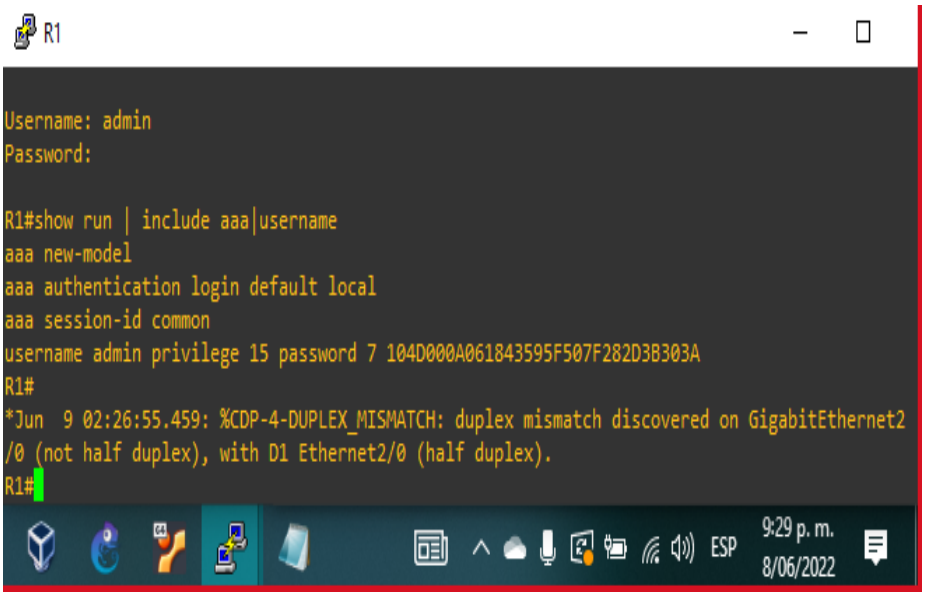

Figura 13 configuración de password – encryption de router R1

Fuente: propia

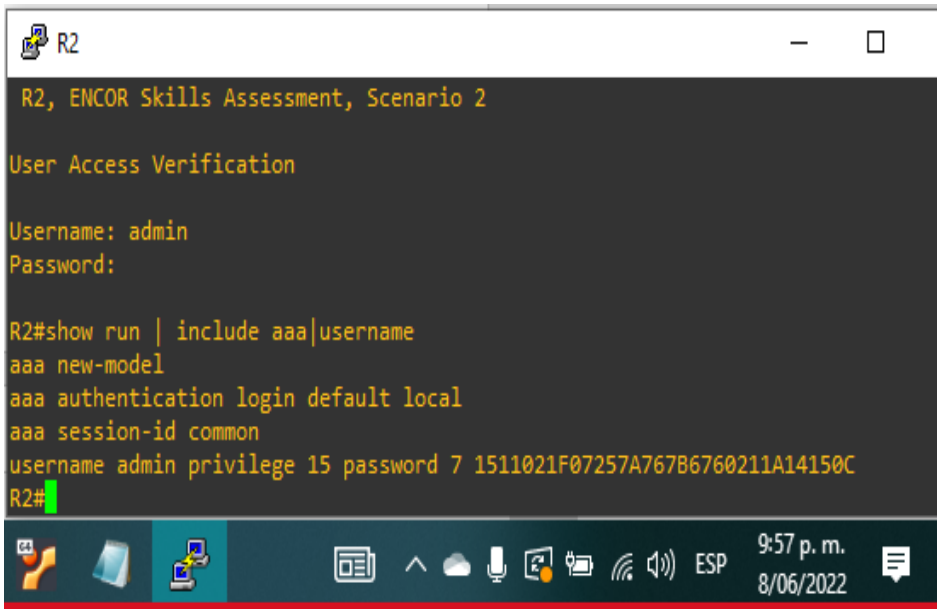

Figura 14 configuración de password – encryption de router R2

Fuente: propia

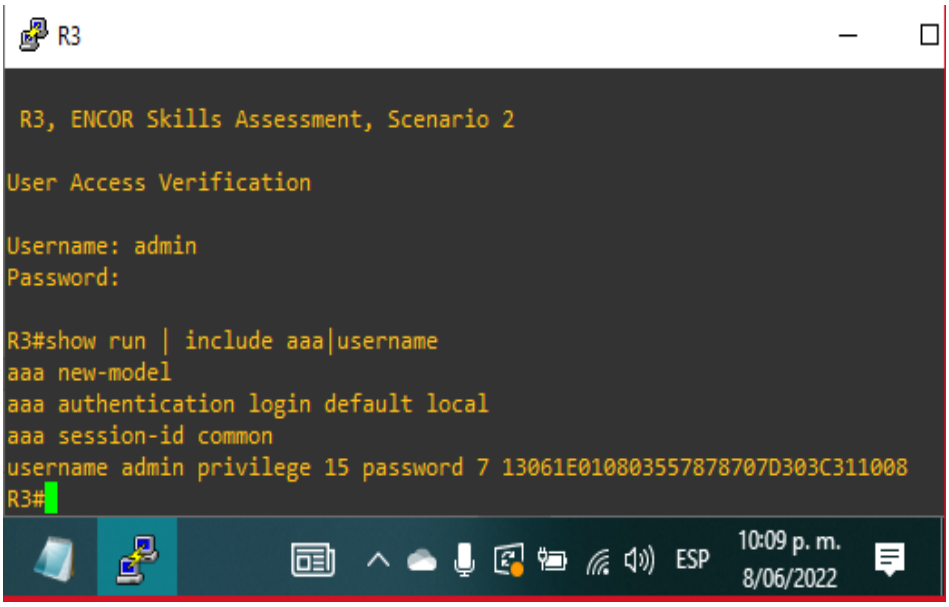

Figura 15 configuración de password – encryption de router R3

Fuente: propia

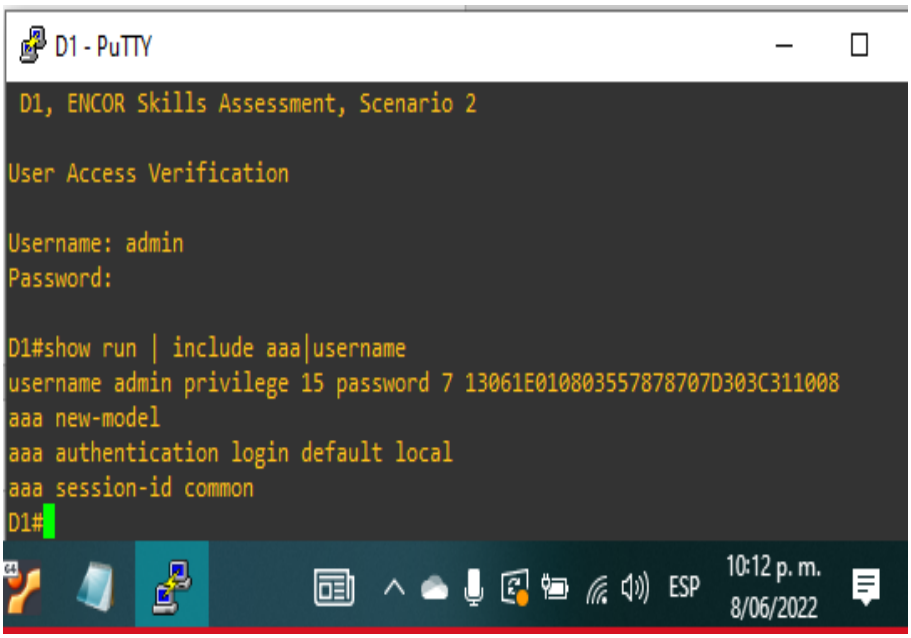

Figura 16 configuración de password – encryption de Switch D1

Fuente: propia

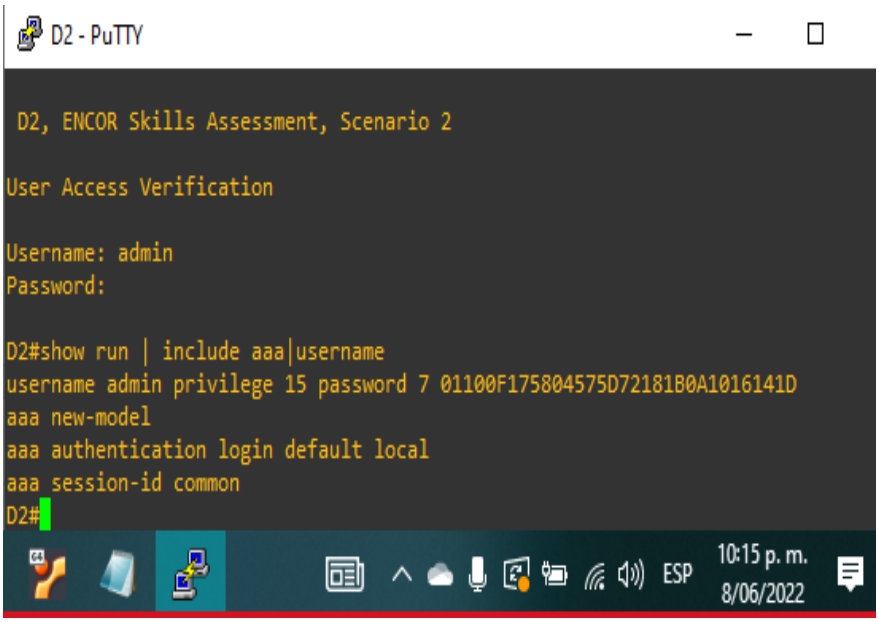

Figura 17 configuración de password – encryption de Switch D2

Fuente: propia

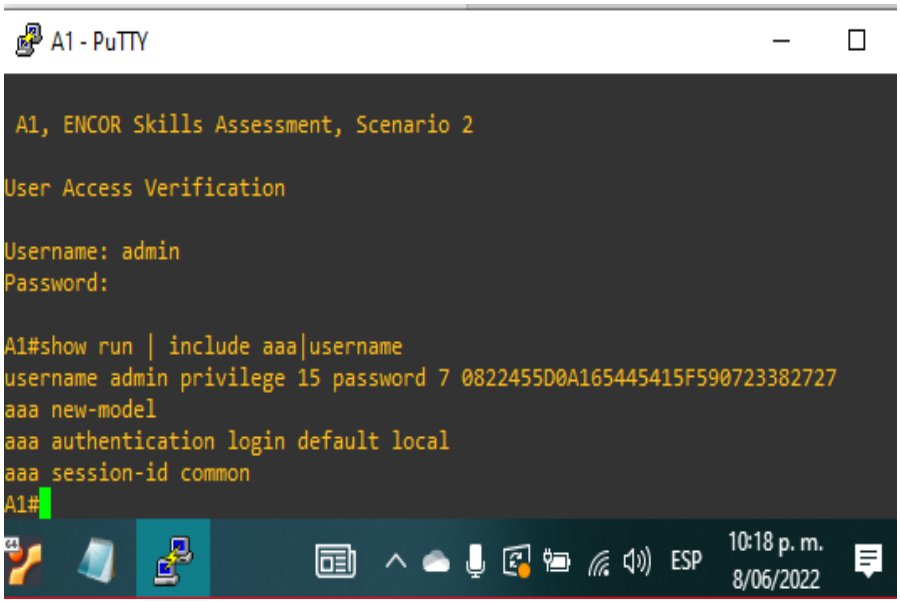

Figura 18 configuración de password – encryption de Switch A1

Fuente: propia

CONCLUSIONES

Es de mencionar que, para los laboratorios de CISCO, donde se requiera la utilización de varios dispositivos para simular topologías extensas o configurar en varis capas es más eficiente el simulador GNS3 respecto al Packet Tracer, dadala interfaz de usuario, variedad de imágenes de dispositivos y la aceptación de diferentes comandos.

Es de resaltar que para las configuraciones cuando se requiera utilizar una interfaz como puerto troncal en un switch se debe enviar el comando para encapsular en Dot1Q, dado que si se activa el modo troncal antes de encapsular el sistema arroja un error y no nos permite realizar bien la configuración.

Al configurar los dispositivos en capa 3 se tiene una mayor política de seguridad en la red dado que se configuran usuarios y mecanismo de autenticación permitiendo así tener un control de los dispositivos que quieran acceder a la red, con esto se mitigan las amenazas de seguridad y daños.

REFERENCIAS BIBLIOGRAFICAS

CCNA3 - etherchannel - PAgP y LACP. (2016, 10 diciembre). [Vídeo]. YouTube.https://www.youtube.com/watch?v=7YTL9fH_BH4

Comparación del funcionamiento de la capa 2 en CatOs y cisco IOS systemsoftware en catalyst 6500/6000. (2021, 14 julio). Cisco.29 denoviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6000-series-switches/12155-101.html

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. 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/8021q/8760-67.html

NAT-PT estático por el ejemplo de la configuración del IPv6. (2020, 24 febrero).Cisco. 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/113275-nat-ptv6.html

Sepúlveda, M. (2020, 13 diciembre). Configuración de VLANs y protocolo ruteo OSPF para el CCNA 200–301. eClassVirtual - Cursos Cisco en línea.29 de noviembre de 2021, de https://eclassvirtual.com/configuracion-de-vlans-y-protocolo-ruteo-ospf-para-el-ccna-200-301/