DIPLOMADO DE PROFUNDIZACION CISCO PRUEBAS DE HABILIDADES PRACTICAS CCNP

STHEFANIA HENAO SANTA

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

STHEFANIA HENAO SANTA

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
MANIZALES-CALDAS
2022

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Manizales, 26 de junio del 2022

Agradecimiento

En primer lugar quiero agradecer a Dios por permitirme llegar hasta este nivel formativo y por darme la paciencia, los recursos y la sabiduría para nunca desfallecer, ya que muchas veces tuve ganas de rendirme y gracias a su fuerza no lo hice, también quiero agradecer a todos los tutores que me acompañaron en cada una de las áreas específicas de la carrera de ingeniería electrónica, quienes con sus conocimientos y apoyo me guiaron a través de cada una de las etapas; alcanzando los resultados que buscaba. A la UNAD por brindarme todos los recursos y herramientas que fueron necesarias para llevar a cabo el proceso educativo, los cuales no hubiese podido llegar a estos resultados de no haber sido por su incondicional ayuda.

Por último, quiero agradecer a todos mis compañeros que estuvieron a mi lado en este proceso, compartiendo sus conocimientos en los momentos que más lo necesite. A mi familia, sobre todo a mis padres, mi hermana y sobrino, gracias por el apoyo incondicional que me han dado siempre, fueron ustedes mi motor en este proceso, el cual fue una etapa dura e impórtate en mi vida.

Muchas gracias a todos

Tabla de contenido

Lista de tablas

Lista de figuras

Glosario

EL ENRUTAMIENTO VIRTUAL Y REENVÍO (VRF): Es una tecnología incluida en routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente.

IPV6: Es un nuevo protocolo con el que se generan nuevos tipos de direcciones IP más largos y complejos. Estas direcciones son las matrículas que utilizan los dispositivos a la hora de conectarse a Internet.

IPV4: Es el nombre del protocolo de Internet utilizado actualmente para las direcciones IP de los dominios. Estas direcciones IP se asignan automáticamente cuando se registra un dominio. IPv4 utiliza direcciones de 32 bits con hasta 12 caracteres en cuatro bloques de tres caracteres cada uno, como 212.227.142.131.

LAN: (Red de área local) Es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.

PROTOCOLO BGP (Protocolo de puerta de enlace de frontera): Es un protocolo escalable de dynamic routing usado en la Internet por grupos de enrutadores para compartir información de enrutamiento. BGP usa parámetros de ruta o atributos para definir políticas de enrutamiento y crear un entorno de enrutamiento estable.

PROTOCOLO DE ENRUTAMIENTO: Los protocolos de enrutamiento administran la actividad de enrutamiento en un sistema. Los enrutadores intercambiar información de enrutamiento con otros hosts para mantener las rutas conocidas a las redes remotas.

PROTOCOLO OSPF: Es considerado como un protocolo de estado de enlace que es capaz de detectar cambios en la topología dentro de un Sistema autónomo permitiendo una red de rutas sin bucles, OSPF también se ocupa de problemas de escalabilidad que se produce cuando un numero de router se congestionan y producen inestabilidad en el sistema autónomo

RUTAS ESTATICAS: Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Resumen

Por medio de la topología planteada para el Diplomado de profundización CCNP CISCO, se logra desarrollar las destrezas necesarias para la resolución de problemas relacionados con el diseño e implementación de redes locales, comerciales y empresariales, basándonos en topologías reales que son incorporadas en diferentes escenarios. Con esta topología presentada en la actividad, se construyó una red con sus ajustes básicos para cada uno de sus routers, Pcs y switches, ingresando a sus terminales dando un direccionamiento de las interfaces y subinterfaces en los puertos determinados para cada uno de componentes de enrutamiento, donde se dieron características particulares para cada uno de ellos tales como, los protocolos Ipv4, ipv6, e implementación de VRF para usuarios generales y especiales, consiguiendo una conexión exitosa entre los dispositivos presentes en esta actividad.

Además, se realiza la configuración de troncales y redes de tipo OSPF donde se genera el envió de datos a dispositivos seleccionados por el usuario, como también la configuración de los dispositivos en capa 2. Esta topología fue desarrollada en el software GNS3 el cual es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre él; permitiendo simular las configuraciones en los routers, switches y pcs haciendo enrutamientos adecuados para que la red tenga accesibilidad de extremo a extremo como lo requiere el escenario planteado para esta actividad

Palabras Clave: CISCO, CCNP, OSPF, Router, Switch, Redes Topología, Gsn3, Dispositivos, VRF

Abstract

Through the topology proposed for the CCNP CISCO Deepening Diploma, it is possible to develop the necessary skills to solve problems related to the design and implementation of local, commercial and business networks, based on real topologies that are incorporated in different scenarios. With this topology presented in the activity, a network was built with its basic settings for each of its routers, PCs and switches, entering its terminals giving an address of the interfaces and sub interfaces in the ports determined for each of its routing components. , where particular characteristics were given for each of them, stories such as IPv4, IPv6 protocols, and implementation of VRF for general and special users, achieving a successful connection between the devices present in this activity.

In addition, the configuration of trunks and OSPF-type networks is carried out where the sending of data to devices selected by the user is generated, as well as the configuration of devices in layer 2. This topology was developed in the GNS3 software, which is a graphical network simulator that allows complex network topologies to be designed and simulations to be carried out on it, allowing configurations to be simulated in routers, switches and PCs, acquiring adequate routing so that the network has end-to-end accessibility as required by the scenario proposed for this activity

Keywords: CISCO, CCNP, OSPF, Router, Switch, Networks, Topology, Gsn3, Devices, VRF

Introducción

En el presente trabajo del Diplomado de profundización CISCO se planteó el desarrollo de una topología de red, en la cual se debían realizar unas configuraciones básicas y cableado entre 3 routers, 3 switches y 4 Pcs, ingresando a sus terminales y asignándole configuraciones previas de direccionamiento, para poder realizar una conexión eficaz entre los dispositivos involucrados en el entorno. Haciendo uso de una topología donde se pretende involucrar direccionamientos en entornos IPV4 e IPV6 dando como resultado el uso de redes de área locales virtuales, por las cuales por medio de saltos se hace envío de datos entre dispositivos de tal manera que se usen redes tanto físicas como virtuales.

Este desarrollo se realiza en 6 etapas practicas donde se evidencia el paso a paso de la elaboración de este escenario, haciendo uso del software GNS3, el cual es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre él.

Con esta actividad se ponen a prueba las habilidades adquiridas de comprensión y desarrollo de situaciones relacionadas con protocolos de enrutamiento y diseño e instalación de redes LAN y WAN en escenarios virtuales, dándonos una preparación eficiente a la hora de enfrentarnos a entornos laborales reales, como la implementación de redes locales, comerciales y empresariales.

Desarrollo

Topología de la Red para trabajar según documento

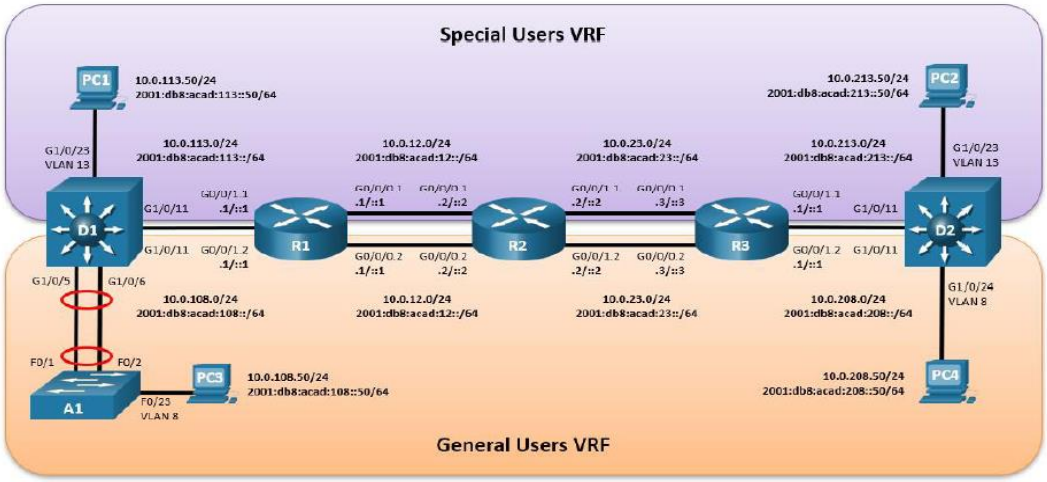

Figura 1 Topología escenario propuesto

Fuente: Pruebas habilidades CCNP

Tabla 1: Tabla de direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0/0.1	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

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.

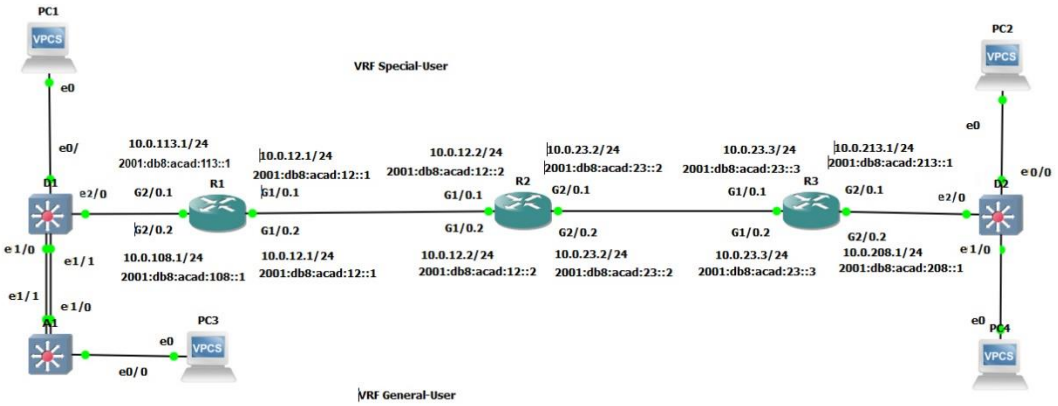

Figura 2I implementación de Topología

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.

Configuración básica para cada uno de los dispositivo	
R1	hostname R1 ipv6 unicast-routing no ip domain lookup banner motd # R1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit

R2	hostname R2 ipv6 unicast-routing no ip domain lookup banner motd # R2, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit
R3	hostname R3 ipv6 unicast-routing no ip domain lookup banner motd # R3, ENCOR Skills Assessment, Scenario 2# line con 0 exec-timeout 0 0 logging synchronous exit
D1	hostname D1 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit vlan 13 name Special-Users exit
D2	hostname D2 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D2, ENCOR Skills Assessment, Scenario 2 #

	line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit vlan 13 name Special-Users exit
A1	hostname A1 ipv6 unicast-routing no ip domain lookup banner motd # A1, ENCOR Skills Assessment, Scenario 2 # line con 0 exec-timeout 0 0 logging synchronous exit vlan 8 name General-Users exit

Tabla 2 configuración Básicas de dispositivos

Fuente: Pruebas y habilidades CCNP

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.

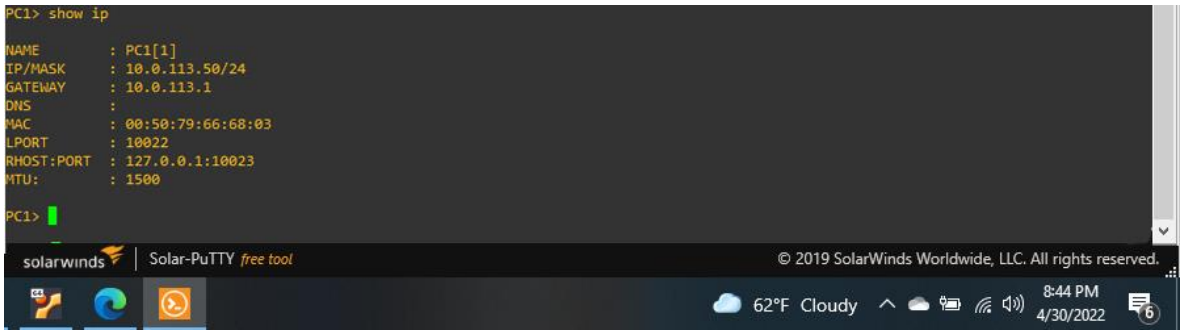

Figura 3 Configuración básica en PC1

Fuente: Propia

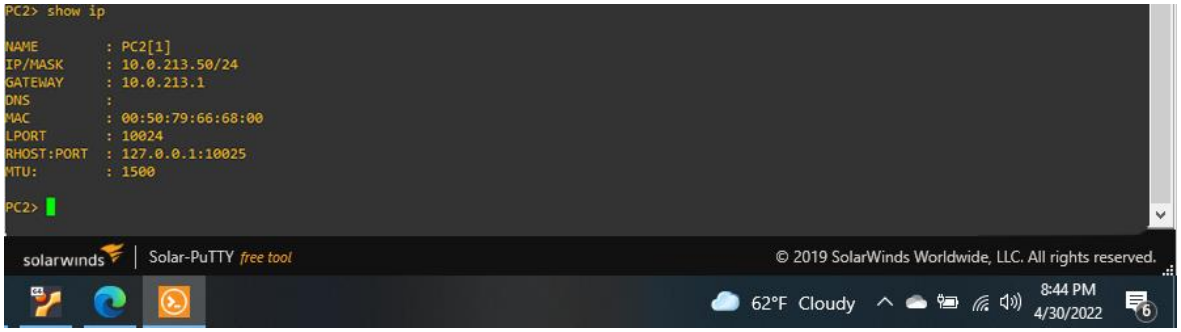

Figura 4 Configuración básica en PC2

Fuente: Propia

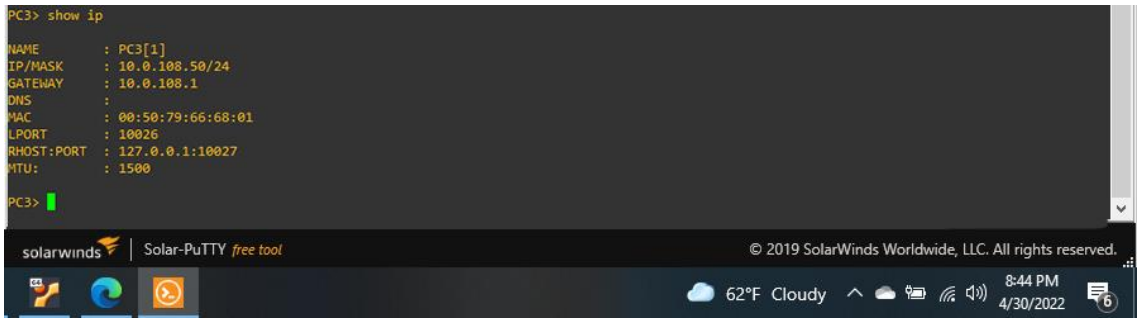

Figura 5 Configuración básica en PC3

Fuente: Propia

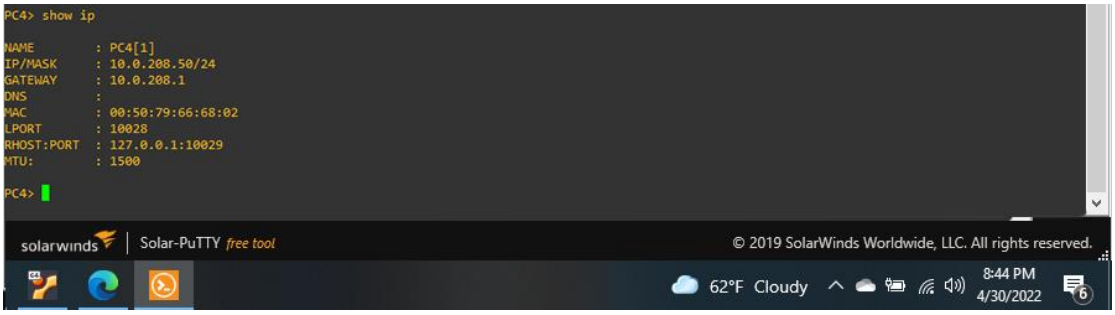

Figura 6 Configuración básica en PC4

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 VRF en R1	
R1	config terminal // entrada a la configuración global vrf definition Special-Users // se define el nombre del VRF virtual vlan 13 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit //salida de la configuración vrf definition General-Users // se define el nombre del VRF virtual vlan 8 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit // salida de la interface

Configuración VRF en R2	
R2	config terminal // entrada a la configuración global vrf definition Special-Users // se define el nombre del VRF virtual vlan 13 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit //salida de la configuración vrf definition General-Users // se define el nombre del VRF virtual vlan 8 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit // salida de la interface

Configuración VRF en R3	
R3	config terminal // entrada a la configuración global vrf definition Special-Users // se define el nombre del VRF virtual vlan 13 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit //salida de la configuración vrf definition General-Users // se define el nombre del VRF virtual vlan 8 address-family ipv4 // se agrega la familia del protocolo ipv4 address-family ipv6 // se agrega la familia del protocolo ipv6 exit // salida de la interface

Tabla 3 configuración de VRF en R1,R2 y R3

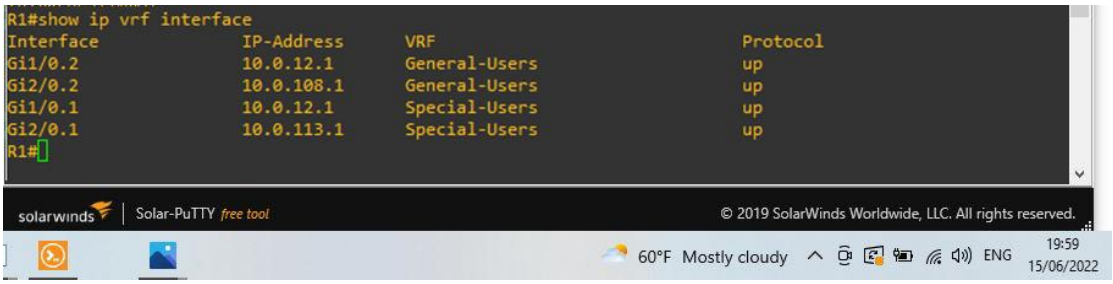

Figura 7 Configuracion de VRF en R1

Fuente: propia

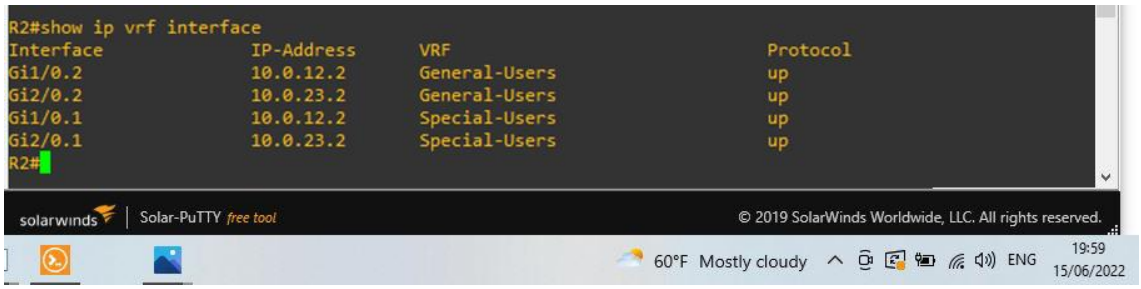

Figura 8 Configuracion de VRF en R2

Fuente: propia

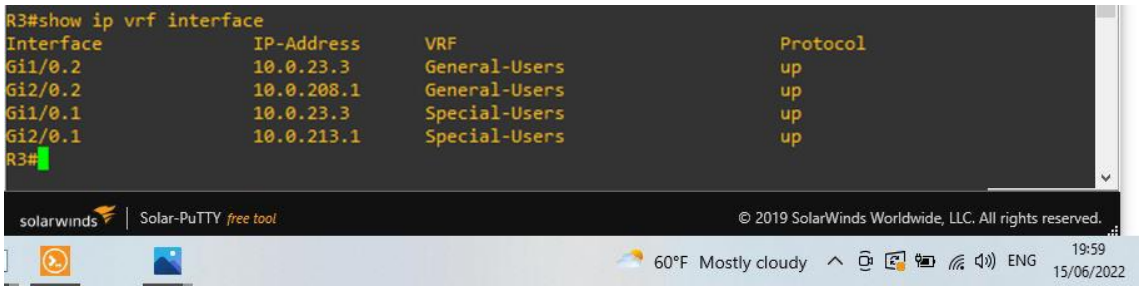

Figura 9 Configuracion de VRF en R3

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 interfaces IPv4 e IPv6 en cada VRF del R1	
R1	Config terminal // se ingresa a la configuración global interface g1/0 // se ingresa a la interface del R1 g1/0 no shutdown // habilita la interface g1/0 interface g1/0.1 // se ingresa a las subinterfaces encapsulation dot1Q 13 // protocolo que permite un enlace troncal Vlan 13 vrf forwarding Special-Users //se agrega el VRF configurado ip address 10.0.12.1 255.255.255.0 // se agrega la ip y mascara ipv4 ipv6 address 2001:db8:acad:12::1/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::1:1 link-local // se agrega su link local no shutdown // habilita la interface exit // salida de la interface interface g1/0.2 // se ingresa a las subinterfaces encapsulation dot1Q 8 // protocolo que permite un enlace troncal Vlan 8 vrf forwarding General-Users // se agrega el VRF configurado ip address 10.0.12.1 255.255.255.0 // se agrega la ip y mascara ipv4 ipv6 address 2001:db8:acad:12::1/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::1:2 link-local // se agrega el link local

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

Configuración de las interfaces IPv4 e IPv6 en cada VRF del R2	
R2	Config terminal // se ingresa al modo configuración global interface g1/0 // ingresamos a la interface del R2 g1/0 no shutdown // habilita la interface g1/0 interface g1/0.1 // ingresamos a las subinterfaces encapsulation dot1Q 13 // protocolo que permite un enlace troncal Vlan 13 vrf forwarding Special-Users // se ingresa el VRF configurado ip address 10.0.12.2 255.255.255.0 // se ingresa la ip y la mascara ipv4 ipv6 address 2001:db8:acad:12::2/64 // se ingresa la ip y la mascara ipv6 ipv6 address fe80::2:1 link-local // se ingresa el link local no shutdown // habilita la interface exit // salida del modo interface interface g1/0.2 // se ingresa a las subinterfaces encapsulation dot1Q 8 // protocolo que permite un enlace troncal Vlan 8 vrf forwarding General-Users // se agrega el VRF configurado ip address 10.0.12.2 255.255.255.0 // se agrega la ip y la mascara ipv4 ipv6 address 2001:db8:acad:12::2/64 // se agrega la ip y la mascara ipv6 ipv6 address fe80::2:2 link-local // se agrega el link local no shutdown // habilita la interface

	exit // salida de la interface interface g2/0.1 // se ingresa a las subinterfaces encapsulation dot1Q 13 // protocolo que permite un enlace troncal Vlan 13 vrf forwarding Special-Users // se agrega el VRF configurado ip address 10.0.23.2 255.255.255.0 // se agrega sla ip y la mascara ipv4 ipv6 address 2001:db8:acad:23::2/64 // se agrega la ip y la mascara ipv6 address fe80::2:3 link-local // se agrega el link local no shutdown // se habilita la interfaz exit // salida de la configuración interface g2/0.2 // se ingresa a las subinterfaces encapsulation dot1Q 8 // protocolo que permite enlace troncal Vlan 8 vrf forwarding General-Users // el VRF configurado ip address 10.0.23.2 255.255.255.0 // se agrega ip y mascara ipv4 ipv6 address 2001:db8:acad:23::2/64 // se agrega ip y mascara ipv6 ipv6 address fe80::2:4 link-local // se agrega el link local no shutdown // habilita la interface exit // salida de la interface

Configuración de las interfaces IPv4 e IPv6 en cada VRF del R3	
R3	Config terminal // se ingresa al modo configuración global interface g1/0 // se ingresa a la interface física del R3 g1/0 no shutdown // habilitamos la interface interface g1/0.1 // se ingresa a las subinterfaces encapsulation dot1Q 13 // protocoloque permite un enlace troncal Vlan 13 vrf forwarding Special-Users // VRF configurado ip address 10.0.23.3 255.255.255.0 // se agrega la ip y mascara ipv4 ipv6 address 2001:db8:acad:23::3/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::3:1 link-local // se agrega el link local no shutdown // habilita la subinterfaz exit // salida de la interface interface g1/0.2 // se ingresa a las subinterfaces encapsulation dot1Q 8 // protocolo que permite un enlace troncal vlan8 vrf forwarding General-Users // VRF configurado ip address 10.0.23.3 255.255.255.0 // se agrega la ip y mascara ipv4 ipv6 address 2001:db8:acad:23::3/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::3:2 link-local // se ingresa el link local no shutdown // habilita la subinterfaz exit // salida de la interface interface g2/0 //se ingresa a la interface física del R3 g2/0 no shutdown // habilita la interface

	interface g2/0.1 // se ingresa a la subinterfaces encapsulation dot1Q 13 // protocolo que permite un enlace troncal vlan 13 vrf forwarding Special-Users // se agrega el VRF configurado ip address 10.0.213.1 255.255.255.0 // se agrega su ip y mascara ipv4 ipv6 address 2001:db8:acad:208::1/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::3:3 link-local // se agrega el link local no shutdown //se habilita la subinterfaz exit // salida de la interface interface g2/0.2 // se ingresa a las subinterfaces v encapsulation dot1Q 8//protocolo que permite un enlace troncal vlan13 vrf forwarding General-Users // agregamos el VRF configurado ip address 10.0.208.1 255.255.255.0 // se agrega la ip y mascara ipv4 ipv6 address 2001:db8:acad:208::1/64 // se agrega la ip y mascara ipv6 ipv6 address fe80::3:4 link-local // se agrega el link local no shutdown // habilita la interfaz exit // salida de la interface

Tabla 4 Configuración de las interfaces IPv4 e IPv6 en cada VRF de los dispositivos

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

Configuración rutas estáticas para R1	
R1	ip route 0.0.0.0 0.0.0.0 10.0.12.2 // rutas estáticas para llegar a R3 ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.12.2 // ruta ipv4 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.12.2 // ruta ipv4 ipv6 route vrf General-Users::/0 2001:DB8:ACAD:12::2 // rutas ipv6 ipv6 route vrf Special-Users::/0 2001:DB8:ACAD:12::2 // rutas ipv6
Configuración rutas estáticas R1 y R3	
R2	ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1 ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3 ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1 ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3 ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1 ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3 ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1 ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3
R3	ip route vrf General-Users 0.0.0.0 0.0.0.0 10.0.23.2 // ruta ipv4 ip route vrf Special-Users 0.0.0.0 0.0.0.0 10.0.23.2 ruta ipv4 ipv6 route vrf General-Users ::/0 2001:DB8:ACAD:23::2 ruta ipv6 ipv6 route vrf Special-Users ::/0 2001:DB8:ACAD:23::2 ruta ipv6

Tabla 5 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-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

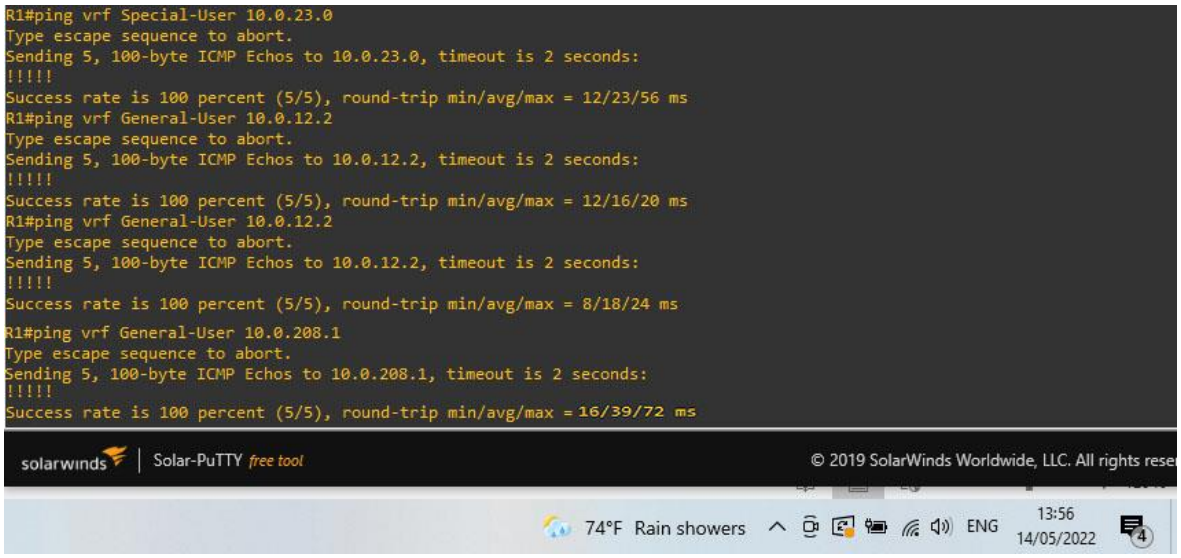

Figura 10 Ping en interfaces vrf General Users y Special-Users

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,D2 y A1 Deshabilitar interfaces	
D1	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// apagado de las interfaces seleccionadas
D2	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// apagado de las interfaces seleccionadas
A1	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// apagado de las interfaces seleccionadas

Tabla 6 configuración de apagado de las interfaces en D1, D2 Y A1

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	Config term // ingresar a la configuración global inter ether 2/0 // interfaceenlace troncal del R1 switchport trunk encapsulation dot1Q // define el tipo encapsulación switchport mode trunk // habilita el enlace troncal switchport trunk allowed Vlan 13,8 // se asigna a vlan 13,8 no shutdown // habilita la interface
D2	Config term // ingresar al modo configuración global inter ether 2/0 // interface del enlace troncal del Router 3 switchport trunk encapsulation dot1Q // define el tipo encapsulación switchport mode trunk // habilitael enlace troncal switchport trunk allowed Vlan 13,8 // se asocia a vlan 13,8 no shutdown // habilita la interface

Tabla 7 configuración enlace troncales en D1 y 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 EtherChannel D1 y A1	
D1	Config terminal // se ingresa al modo configuración global inter range e1/0-1 // se ingresa las interfaces del EtherChannel switchport trunk encapsulation dot1Q // se especifica el tipo encapsulación switchport mode trunk // habilita modo enlace troncal channel-group 1 mode desirable // la interface será administrada grupo 1 no shutdown // habilita la interface
A1	Config term // se ingresa al modo configuración global inter range e1/0-1 // se ingresa a las interfaces del EtherChannel switchport trunk encapsulation dot1Q // se especifica el tipo encapsulación switchport mode trunk // se habilita modo enlace troncal channel-group 1 mode desirable // la interface será administrada grupo 1 no shutdown // habilita la interface

Tabla 8 configuración del etherchannel en D1 y A1

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 de puertas de acceso en D1, D2 y A1	
D1	inter e0/0 // interface donde se conecta la pc1 switchport mode Access // se activa en puerto en modo acceso switchport access vlan 13 // se agrega en vlan 13 modo acceso spanning-tree portfast // establece automáticamente el valor de prioridad no shutdown // habilita la interface exit // salida del modo interface
D2	inter e0/0 // interface donde se conecta la pc2 switchport mode Access // se activa en puerto en modo acceso switchport access vlan 13 //se agréga en vlan 13 modo acceso spanning-tree portfast // establece automáticamente el valor de prioridad no shutdown // habilita la interface exit // salida de la interface inter e1/0 // interface donde está conectada la pc4 switchport mode Access // se activa en puerto en modo acceso switchport access vlan 8 // se agréga 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
A1	inter e0/0 // interface donde está conectada la pc3 switchport mode Access // se activa en puerto en modo acceso switchport access vlan 8 // se agrega en vlan 8 modo acceso spanning-tree portfast // establecer automáticamente el valor de prioridad no shutdown // habilitar la interface exit // salida de la interface

Tabla 9 configuración de puertos de acceso en D1, D2 y A1

3.5 verificar la conectividad de pc1 a pc2

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

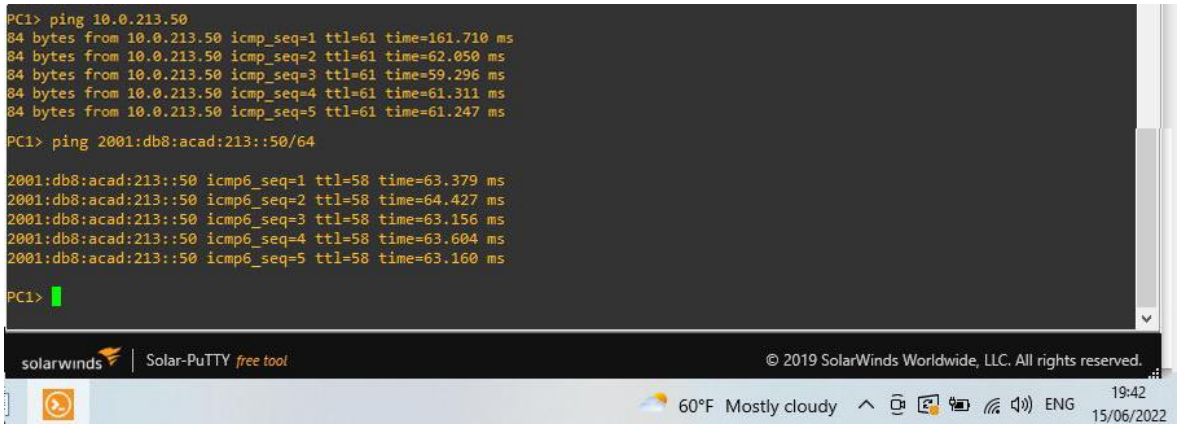

Figura 11 Ping de pc1 a pc2 por medio de ipv4 y ipv6

Fuente: propia

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

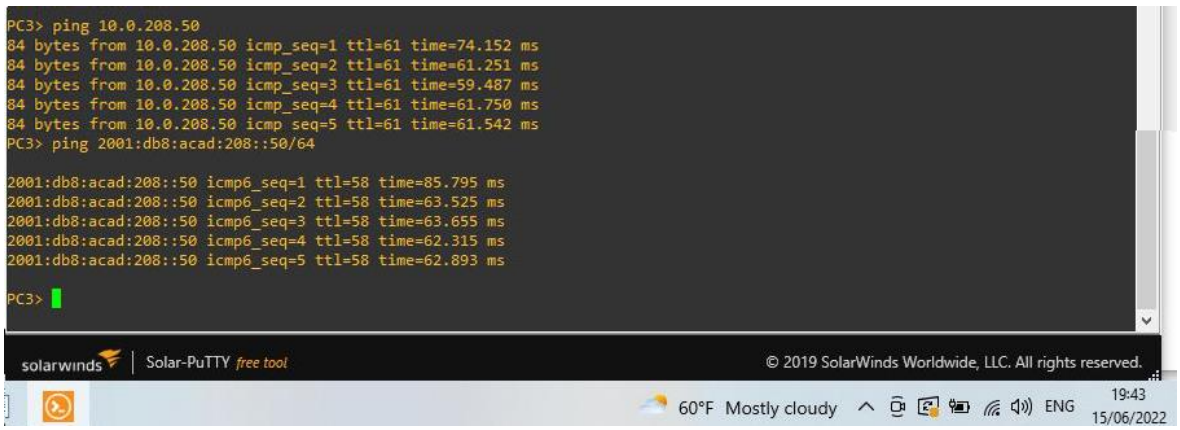

Figura 12 Ping de pc3 a pc4 por medio ipv4 y ipv6

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 enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña
R2	R2 config ter // ingresamos al modo configuración global enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña
R3	R3 config ter // ingresamos al modo configuración global enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña
D1	D1 config ter // ingresamos al modo configuración global enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña

D2	D2 config terminal // ingresamos al modo configuración global enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña
A1	A1 config terminal// ingresamos al modo configuración global enable algorithm-type SCRYPT secret cisco12345cisco // proporciona mayor seguridad encriptando la contraseña

Tabla 10 configuración EXEC privilegiado en todos los dipositivos

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

R1	R1 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado
R2	R2 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado
R3	R3 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado
D1	D1 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado
D2	D2 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado
A1	A1 config ter // ingresamos al modo configuración global username admin privilege 15 algorithm-type SCRYPT secret cisco12345cisco// indica el nombre del usuario y le da un nivel privilegiado

Tabla 11 configuración de la cuenta de 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 12 configuración AAA y su autenticación

Figura 13 Configuración de seguridad en R1

Fuente: propia

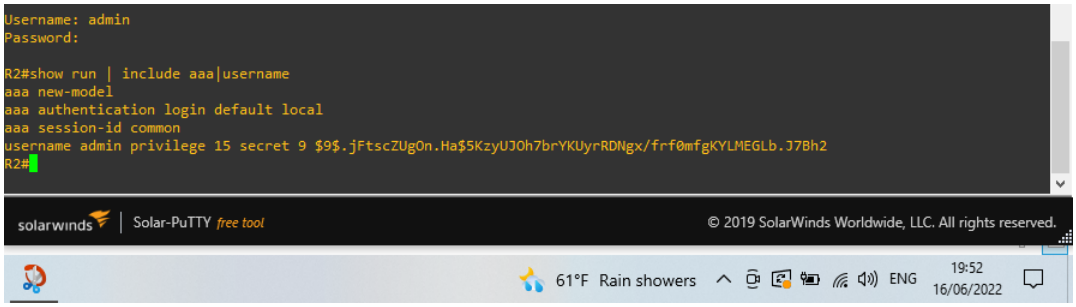

Figura 14 Configuración de seguridad en R2

Fuente: propia

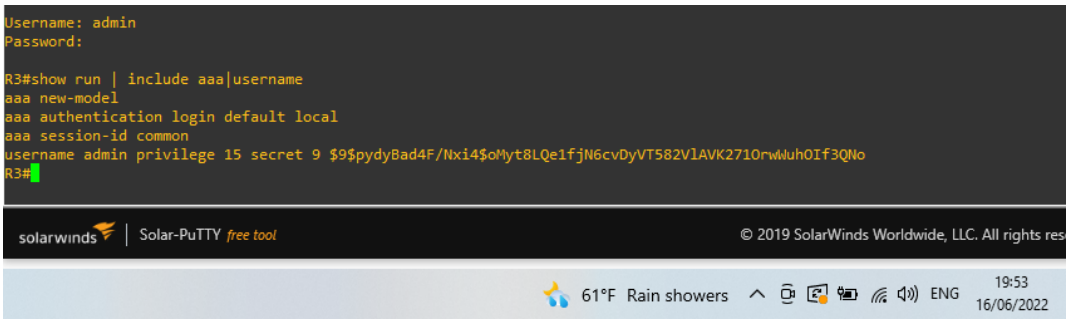

Figura 15 Configuración de seguridad en R3

Fuente: propia

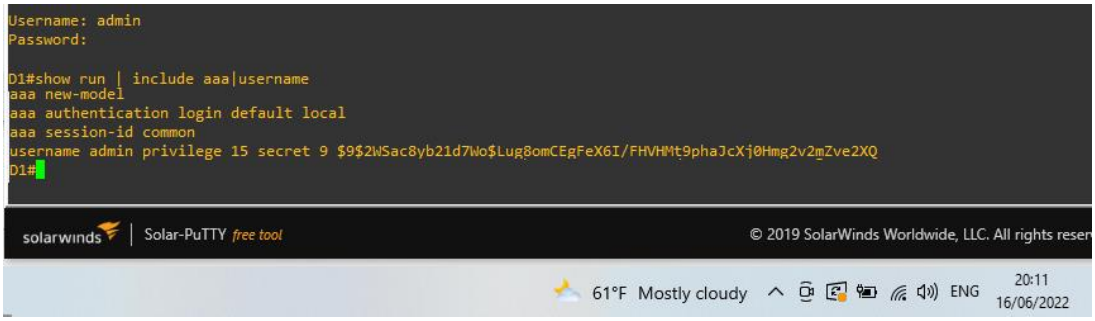

Figura 16 Configuración de seguridad en D1

Fuente: propia

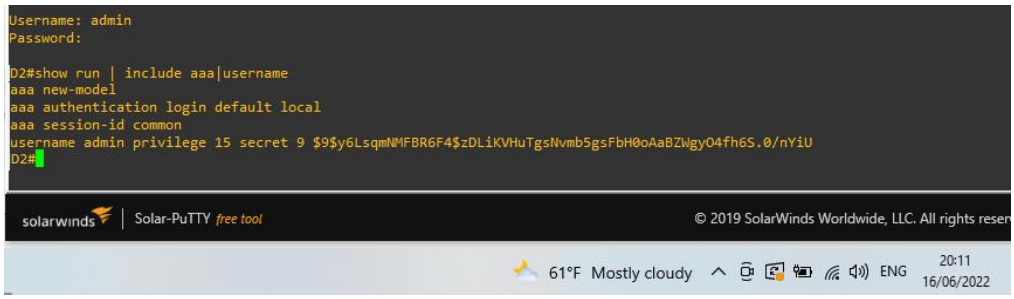

Figura 17 Configuración de seguridad en D2

Fuente: propia

Figura 18 Configuración de seguridad en A1

Fuente: propia

CONCLUSIONES

Se desarrollo la actividad propuesta para este Diplomado de profundización CISCO donde se planteó la realización de una topología de red en el software GNS3, en la cual se debió ejecutar las configuraciones básicas y cableado entre routers, switches y pcs, ingresando a sus terminales y asignándole las configuraciones debidas, las cuales fueron mencionadas en el documento.

Se afianzaron los conocimientos sobre cómo funcionaba una VRF y como se pueden trabajar con ipv4 y ipv6, haciendo conexiones puntuales entre dispositivos como routers, switches y pcs; logrando el envío de datos sin ningún inconveniente, haciendo ping entre ellos, como muestran las capturas de pantalla encontradas en el documento

Se implemento la configuración final sobre seguridad y autenticación de usuario, permitiendo la validación del password y el usuario local a través del comando show run | include aaa|username, donde se repitió este mismo procedimiento en cada uno de los routers y switches involucrados en esta topología

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/