

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICA CCNP

JOSE MAXIMILIANO BERNAL PEINADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE INGENIERIA BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA TELECOMUNICACIONES
BARRANQUILLA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JOSE MAXIMILIANO BERNAL PEINADO

Diplomado de opción de grado presentado para optar el
título de INGENIERO EN TELECOMUNICACIONES

DIRECTOR

MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE INGENIERIA BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA TELECOMUNICACIONES
BARRANQUILLA

2022

NOTA DE ACEPTACION

Firma presidente del jurado

Firma del jurado

Firma del jurado

BARRANQUILLA 26 DE JUNIO DE 2022

AGRADECIMIENTOS

Primero, agradezco a Dios por la vida y la salud que me permitieron culminar esta carrera que es un gran paso en mi vida. A mi familia por su apoyo incondicional en el transcurso de mi carrera.

A la Universidad Nacional abierta y a distancia (UNAD) por permitirme ser parte de ella por brindarme buen aprendizaje.

A mi carrera por enseñarme por permitirme ser exigente como persona y como futuro profesional en lo que he obtenido los mejores aprendizajes para mi vida.

A la plataforma Cisco networkng academic por enseñarnos como estudiantes las habilidades técnicas en las redes de datos

INDICE GENERAL

	pág.
AGRADECIMIENTOS.....	4
LISTA DE TABLAS	7
LISTA DE FIGURAS.....	8
GLOSARIO.....	10
RESUMEN.....	11
INTRODUCCION.....	12
PLANTEAMIENTO DEL PROBLEMA.....	13
OBJETIVOS	15
SOLUCION DEL PROBLEMA	16
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz	16
Paso 1: Conectar la red como se muestra en la topología.	16
Paso 2. Configure los ajustes básicos para cada dispositivo.	17
Parte 2: Configurar VRF y enrutamiento estático	22
2.1. En R1, R2 y R3, configuramos VRF-Lite VRF como se muestra en el diagrama de topología.....	22
2.2. En R1, R2 y R3, configuramos las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior	24
2.3. En R1 y R3, configuramos las rutas estáticas predeterminadas que están en dirección a R2.....	29
2.4. En este paso verificamos la conectividad en cada VRF	35
Parte 3: configurar capa 2.....	37
3.1. En D1, D2 y A1 deshabilitamos todas las interfaces.	37

3.2 En D1 y D2, configuramos los enlaces troncales a R1 y R3.	38
3.3 En D1 y A1, configuramos el EtherChannel.	39
3.4 En D1, D2 y A1, configuramos los puertos de acceso para PC1, PC2, PC3 y PC4.	40
3.5 Verificar conectividad de PC a PC.	41
Parte 4: Configure Seguridad	43
4.1. En todos los dispositivos, modo EXE privilegiado.	43
4.2. En todos los dispositivos, creamos una cuenta de usuario local.	44
4.3. En todos los dispositivos, habilitamos AAA.	44
CONCLUSIONES	48
BIBLIOGRAFIA.....	49

LISTA DE TABLAS

	Pág.
Tabla 1: Direccionamiento.	14

LISTA DE FIGURAS

	Pág.
Figura 1: Escenario propuesto bajo uso tecnologia cisco	13
Figura 2: Simulación Escenario	16
Figura 3: Estado e información de interfaces en R1.....	25
Figura 4: Estado e información de interfaces en R2.....	27
Figura 5: Estado e información de interfaces en R3.....	28
Figura 6: Tabla de ruta en IPv4 para VRF GENERAL-USER en R1	29
Figura 7: Tabla de ruta en IPv4 para VRF SPECIAL-USER en R1	30
Figura 8: Tabla de ruta en IPv6 para VRF GENERAL-USER en R1	31
Figura 9: Tabla de ruta en IPv6 para VRF SPECIAL-USER en R1.	31
Figura 10: Tabla de rupa en IPv4 VRF SPECIAL-USER en R3	33
Figura 11: Tabla de ruta en IPv4 para VRF GENERAL-USER en R3	33
Figura 12: Tabla de ruta en IPv6 para VRF GENERAL-USER en R3	34
Figura 13: Tabla de ruta en IPv6 para VRF SPECIAL-USER en R3	35
Figura 14: Ping vrf GENERAL-USER 10.0.208.1	35
Figura 15: Ping vrf GENERAL-USER 2001:db8:acad:208::1	36
Figura 16: ping vrf SPECIAL-USER 10.0.213.1	36
Figura 17: Ping vrf SPECIAL-USER 2001:db8:acad:213::1	36
Figura 18: Detalles del port channel entre A1 y D1	39
Figura 19: Ping de PC1 a PC2 en IPv4.....	41
Figura 20: Ping de PC1 a PC2 en IPv6.....	41

Figura 21: Ping de PC3 a PC4 en IPv4.....42

Figura 22: Ping de PC3 a PC4 en IPv6.....42

GLOSARIO

HOST: Es cualquier dispositivo (computador, Tablet, impresora, switch...) conectada a una red mediante una dirección IP definida.

INTERFAZ DE RED: Es el software específico de red que se comunica con el controlador de dispositivos determinado de red.

PING: Herramienta de diagnóstico que permite realizar un chequeo del estado de conexión de un host local con al menos un dispositivo contemplado en una red de tipo TCP/IP.

PROTOCOLO: Es un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red.

ROUTER: Es un dispositivo que permite interconectar diferentes redes, su funcionamiento consiste en establecer la mejor ruta de destino a cada paquete de datos para llegar a la red y al dispositivo final.

SCRYPT: Es un algoritmo de seguridad de alto nivel que está diseñado para que el programador pueda aumentar o disminuir diferentes variables que impacten en la seguridad.

SWITCH: Es un dispositivo que permite conectar varios elementos dentro de una misma red.

VRF: Es una tecnología que permite que un enrutador ejecute más de una tabla de enrutamiento simultáneamente

RESUMEN

En el presente trabajo se muestra el desarrollo de las habilidades prácticas CCNP del diplomado de profundización si se muestra el estudio de la implementación de red donde se coloca a prueba lo aprendido durante las fases anteriores inicialmente se desarrolla la topología con la configuración de cada uno de los dispositivos que hacen parte de estas redes. A parte enfocado en estudiantes de electrónica y de telecomunicaciones donde se tuvo la oportunidad de poner a prueba lo realizado en la asignación IP a los equipos hosts y routers, se configura los protocolos de enrutamiento y la redundancia de primer salto.

Su principal objetivo, es medir los conocimientos y la capacidad de aplicación de los conceptos demostrando su funcionamiento y conexión, como protocolos de enrutamiento, redistribución de rutas, redes de conmutación y también del módulo CCNP SWITCH y configuración de usuarios.

ABSTRACT

In the present work, the development of the CCNP practical skills of the in-depth diploma course is presented, if the study of the network implementation is shown, where what is learned during the previous phases is put to the test, initially the topology is developed with the configuration of each of the the devices that are part of these networks. A part focused on electronics and telecommunications students where they had the opportunity to test what was done in the IP assignment to hosts and routers, routing protocols and first-hop redundancy were configured.

Its main objective is to measure the knowledge and ability to apply the concepts, demonstrating their operation and connection, such as routing protocols, route redistribution, switching networks and also the CCNP SWITCH module and user configuration.

INTRODUCCION

En el presente trabajo daremos solución al escenario propuesto como trabajo final, en Diplomado de profundización CCNP, se busca mediante las tecnologías conocidas como VRF, que permite a un router ejecute más de una tabla de enrutamiento simultáneamente, aplicarla en esta práctica.

Aplicamos configuración port channel entre los Switches de capa 2 y capa 3, también trabajamos con VLANs, rutas estáticas, puertos de acceso para los PC, accesos troncales entre los routers y switches, se configuraron autenticaciones antes de permitir el acceso al modo Exec privilegiado, cuentas de usuarios local y en todos los dispositivos habilitamos el protocolo AAA.

Realizamos las tareas asignadas, acompañado de los respectivos procesos documentados de la solución, el montaje del escenario se trabajó en el programa GNS3 y la máquina virtual VMware que nos ofrece un ambiente muy semejante a la realidad.

PLANTEAMIENTO DEL PROBLEMA

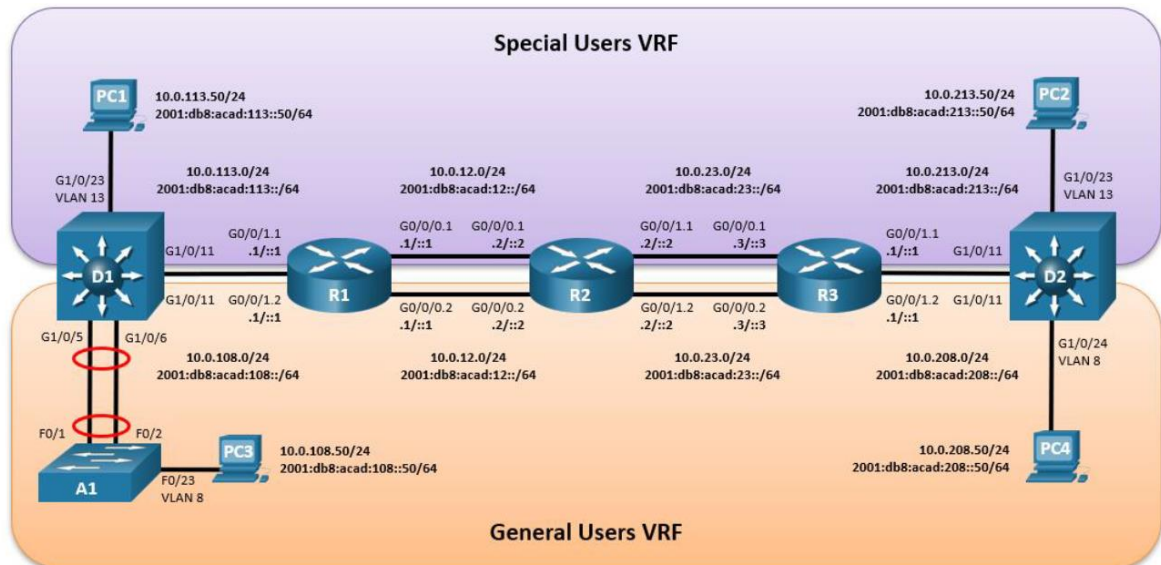
En este escenario nos presentan una red conformada por 3 routers, 2 switch capa 3, 1 switch capa 2 y 4 PC, podemos observar la configuración de multi-VRF que admite Usuarios Generales y Usuarios Especiales, podemos apreciar un port channel entre el switch D1 y A1.

En este tipo de escenarios que presentan dos redes diferentes, aunque compartan la misma estructura física, no se puede comunicar entre sí.

La interconexión entre Switch – Router y Router -Router se realiza mediante un solo cable ya sea fibra óptica o cobre entre las interfaces que intervienen excepto en el port channel que utilizamos 2 cables o conductores para cada interface.

Al terminar todas las configuraciones pudimos constatar que estas cumplan según lo requerido, realizamos pruebas de comunicación con el comando ping entre los PC de la misma VRF tanto en IPv4 como en IPv6, que resulto exitoso y entre los PC de los dos grupos de VRF no se pueden comunicar.

Figura 1: Escenario propuesto bajo uso tecnología cisco



Direccionamiento de las direcciones IP de los dispositivos de red

Tabla 1: Direccionamiento.

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G2/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G2/0.2	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	G2/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G2/0.2	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	G1/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G1/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G2/0.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G2/0.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC 1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC 2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC 3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC 4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

OBJETIVOS

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

Parte 2: Configurar VRF y rutas estáticas.

Parte 3: Configurar Capa 2.

Parte 4: Configurar seguridad.

SOLUCION DEL PROBLEMA

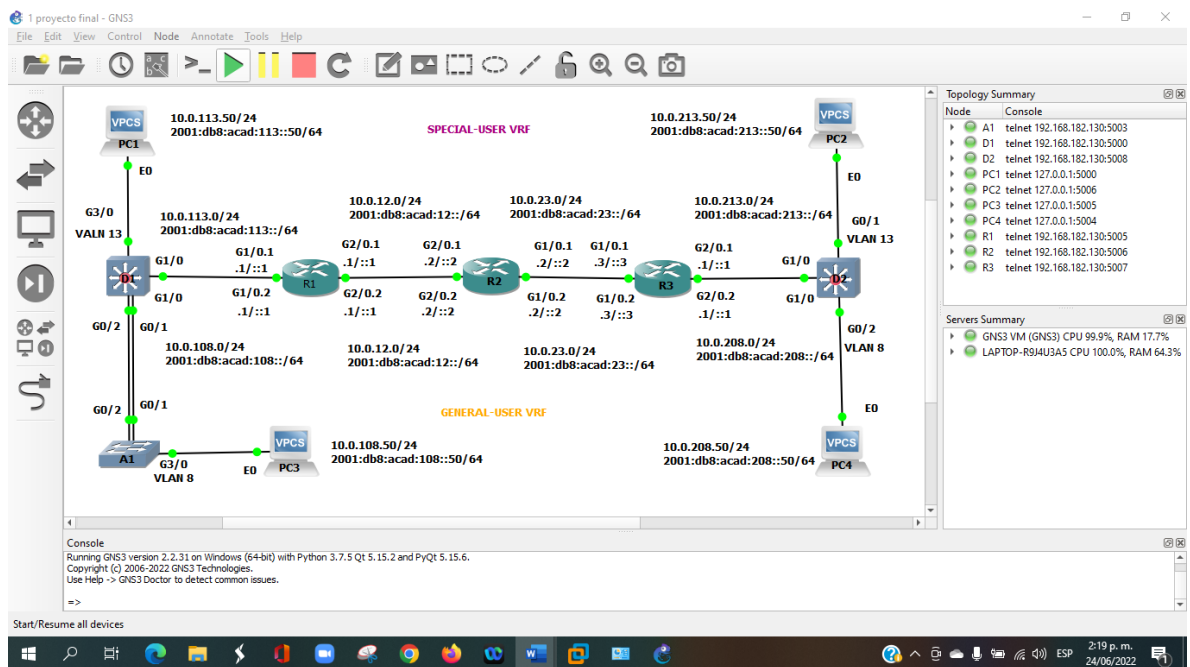
Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

En el desarrollo de esta actividad utilizamos el software GNS3 y la máquina virtual VMware, que nos permite configurar los diferentes tipos de dispositivos de una manera más real.

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

Conectamos los dispositivos en sus interfaces de acuerdo a la tabla de enrutamiento.

Figura 2: Simulación Escenario



Fuente: Topología realizada en el software GNS3

Paso 2. Configure los ajustes básicos para cada dispositivo.

Ingresando al modo de configuración global en cada uno de los dispositivos, aplicamos las configuraciones básicas.

Configuración para router R1

Enable	//Ingresar en modo administrador
Conf terminal	//Se accede a modo de configuración global.
hostname R1	//Se configura el nombre del router R1.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # R1, ENCOR Skills Assessment, Scenario 2 #	//Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Para salir del modo de configuración global.

Configuración para router R2

R2 se configura igual a R1, la diferencia está en el nombre dado al dispositivo.

Enable	//Ingresar en modo administrador
conf terminal	//Se accede a modo de configuración global.
hostname R2	//Se configura el nombre del router R2.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # R2, ENCOR Skills Assessment, Scenario 2 #	//Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Para salir del modo de configuración global.

Configuración para router R3

R3 se configura igual a R1, la diferencia está en el nombre dado al dispositivo.

Enable	//Ingresar en modo administrador
conf terminal	//Se accede a modo de configuración global.
hostname R3	//Se configura el nombre del router R3.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # R3, ENCOR Skills Assessment, Scenario 2 #	//Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Para salir del modo de configuración global

Configuración para switch D1

Enable	//Ingresar en modo administrador
config terminal	//Se accede a modo de configuración global.
hostname D1	//Se configura el nombre del switch D1.
ip routing	//Se habilita el ruteo en el switch D1.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #	//Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Para salir del modo de configuración global
vlan 8	//Se crea la vlan 8.
name General-User	//Se define el nombre de la vlan 8.
exit	//Salimos del modo de configuración de vlan.
vlan 13	//Se crea la vlan 13.
name Special-User	//Se define el nombre de la vlan 13.
exit	//Salimos del modo de configuración de vlan.

Configuración para switch D-2

A continuación, se realiza la misma configuración que en D1, lo que cambia es el nombre del switch.

Enable	//Ingresar en modo administrador
config terminal	//Se accede a modo de configuración global.
hostname D2	//Se configura el nombre del switch D2.
ip routing	//Se habilita el ruteo en el switch D1.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # D2, ENCOR Skills Assessment, Scenario 2 #	//Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Salir
vlan 8	//Se crea la vlan 8.
name General-User	//Se define el nombre de la vlan 8.
exit	//Salimos del modo de configuración de vlan.
vlan 13	//Se crea la vlan 13.
#name Special-User	//Se define el nombre de la vlan 13.
#exit	//Salimos del modo de configuración de global

Configuración para switch A1

Enable	//Ingresar en modo administrador
config terminal	//Se accede a modo de configuración global.
hostname A1	//Se configura el nombre del switch D2.
ipv6 unicast-routing	//Se habilita el direccionamiento IPv6.
no ip domain lookup	//Se desactiva la búsqueda del DNS.
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #	// Mensaje del día
line con 0	//Se configura el puerto de acceso por consola.
exec-timeout 0 0	//Se configura sin límite de tiempo por inactividad.
logging synchronous	//Para evitar mensajes en pantalla.
exit	//Salir
vlan 8	//Se crea la vlan 8.
name General-User	//Se define el nombre de la vlan 8.
exit	//Salimos del modo de configuración de vlan.

Guardamos las configuraciones en cada uno de los dispositivos, utilizando el comando correspondiente.

Para guardar las configuraciones realizadas en los dispositivos como son los Routers y los switches utilizamos el comando.

R1#copy running-config startup-config.

Para los PC cuando trabajamos en GNS3 utilizamos el comando.

PC1> save

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

En la configuración de los PC es un más directa.

Colocamos IP seguido de la dirección que queremos asignar más la máscara y por último la dirección Gateway o dirección de salida, para IPv6 aplicamos el mismo principio

Configuración PC1

En el PC 1 la dirección Gateway o dirección de salida es **10.0.113.1**

```
PC1> ip 10.0.113.50 255.255.255.0 10.0.113.1
Checking for duplicate address...
PC1 : 10.0.113.50 255.255.255.0 10.0.113.1
```

Configuración para IPv6

```
PC1> ip 2001:db8:acad:113::50/64 2001:db8:acad:113::1
PC1 : 2001:db8:acad:113::50/64
```

Configuración PC2

En el PC 2 la dirección Gateway o dirección de salida es **10.0.231.1**

```
PC2> ip 10.0.213.50 255.255.255.0 10.0.213.1
Checking for duplicate address...
PC2: 10.0.213.50 255.255.255.0 10.0.213.1
```

Configuración para IPv6

```
PC2> ip 2001:db8:acad:213::50/64 2001:db8:acad:213::1
PC2: 2001:db8:acad:213::50/64
```

Configuración PC3

En el PC 3 la dirección Gateway o dirección de salida es 10.0.108.1

```
PC3> ip 10.0.108.50 255.255.255.0 10.0.108.1
Checking for duplicate address...
PC3: 10.0.108.50 255.255.255.0 10.0.108.1
```

Configuración para IPv6

```
PC3> ip 2001:db8:acad:108::50/64 2001:db8:acad:108::1
PC3: 2001:db8:acad:108::50/64
```

Configuración PC4

En el PC 4 la dirección Gateway o dirección de salida es 10.0.208.1

```
PC4> ip 10.0.208.50 255.255.255.0 10.0.208.1
Checking for duplicate address...
PC4: 10.0.208.50 255.255.255.0 10.0.208.1
```

Configuración para IPv6

```
PC4> ip 2001:db8:acad:208::50/64 2001:db8:acad:208::1
PC4: 2001:db8:acad:208::50/64
```

Parte 2: Configurar VRF y enrutamiento estático

Se configuro VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al finalizar las configuraciones se verifico con el comando Ping la conectividad desde R1 a R3 en IPv4 y en IPv6 de las VRF General-user y Special-User.

El resultado es exitoso.

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

El enrutamiento y reenvío virtual (VRF) crea routers virtuales separados en un router físico. A continuación, en los routers R1, R2 y R3 creamos estos routers virtuales tanto para IPv4 como para IPv6.

Ingresamos al modo de configuración global en R1, R2 y R3

R#(Configure terminal)

Configuramos en Router 1

VRFs Sepecial-User

vrf definition SPECIAL-USER	//Se crea la tabla de enrutamiento VRF Special User.
address-family ipv4	//Se inicializa la familia de direcciones IPv4.
exit	//Salir
address-family ipv6	//Se inicializa la familia de direcciones IPv6.
Exit	//Salir

VRFs General-User

R1(config)#vrf definition GENERAL-USER	//Se crea la tabla de enrutamiento VRF Genral User.
R1(config-vrf)#ADDRESS-family IPV4	//Se inicializa la familia de direcciones IPv4.
R1(config-vrf-af)#EXIT	//Salir
R1(config-vrf)#ADDRESS-family IPV6	//Se inicializa la familia de direcciones IPv6.
R1(config-vrf-af)#EXIT	

Configuramos en Router 2

Al igual que en R1 se crean las tablas de enrutamiento VRF “Special y General User” luego se inicializan las familias de direcciones tanto en IPv4 como para IPv6.

VRFs Sepecial-User

vrf definition SPECIAL-USER	//Se crea la tabla de enrutamiento VRF Special User.
ADDRESS-FAMILY IPV4	//Se inicializa la familia de direcciones IPv4.
EXIT	// Salir
ADDRESS-FAMILY IPV6	//Se inicializa la familia de direcciones IPv6.
EXIT	//Salir

VRFs General-User

vrf definition GENERAL-USER	//Se crea la tabla de enrutamiento VRF Special User.
ADDRESS-FAMILY IPV4	//Se inicializa la familia de direcciones IPv4.
EXIT	//Salir
ADDRESS-FAMILY IPV6	//Se inicializa la familia de direcciones IPv6.
EXIT	//Salir

Configuramos en Router 3

Al igual que R1 y R2 se crean las VRF y familias de direcciones IPv4 e IPv6.

VRFs Sepecial-User

vrf definition SPECIAL-USER	//Se crea la tabla de enrutamiento VRF Special User.
address-family ipv4	//Se inicializa la familia de direcciones IPv4.
exit	//Salir
address-family ipv6	//Se inicializa la familia de direcciones IPv6.
exit	//Salir

VRFs General-User

vrf definition GENERAL-USER Special User.	//Se crea la tabla de enrutamiento VRF
address-family ipv4	//Se inicializa la familia de direcciones IPv4.
Exit	//Salir
address-family ipv6	//Se inicializa la familia de direcciones IPv6.
Exit	//Salir

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

Especificamos las interfaces virtuales con las VRF SPECIAL-USER o GENERAL-USER según corresponda

Configuramos en Router 1

int gi 1/0.1 con la VRF "Special".	//Se especifica la interfaz g1/0.1 que asociaremos
vrf forwarding SPECIAL-USER	//Se asocia la instancia VRF con la subinterfaz.
encapsulation dot1Q 13	//Se habilita 802.1Q en la subinterfaz y se asocia a la vlan 13.
ip address 10.0.113.1 255.255.255.0	//Se asocia la IP a la subinterfaz.
ipv6 address 2001:DB8:ACAD:113::1/64	//Se asocia la IPv6 a subinterfaz.

int gi1/0.2 con la VRF "General".	//Se especifica la interfaz que asociaremos
vrf forwarding GENERAL-USER	//Se asocia la VRF con la subinterfaz.
encapsulation dot1Q 8	//802.1Q habilitado y asociado a la vlan 8 en g1/0.2.
ip address 10.0.108.1 255.255.255.0	//Se asocia la IPv4 a subinterfaz.
ipv6 address 2001:DB8:ACAD:108::1/64	//Se asocia la IPv6 a subinterfaz.

int G2/0.1	//Configurar la interfaz G2/0.1
VRF forwarding SPECIAL-USER de Capa 3	//Asocia el VRF con la interfaz
encapsulation dot1q 13	//Habilitamos el trunk standar
ip address 10.0.12.1 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:12::1/64	//Establecer la dirección IPv6

int G2/0.2	//Configurar la interfaz G2/0.2
VRF forwarding GENERAL-USER	//Asocia el VRF con la interfaz de Capa 3
encapsulation dot1q 13	//Habilitamos el trunk standar
ip address 10.0.12.1 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:12::1/64	//Establecer la dirección IPv6
interf gi1/0	//Configuramos interfaz gi1/0
no shutdown	//Se habilita la interfaz física g1/0 en R1.
interf gi2/0	//Configuramos interfaz gi2/0
no shutdown	//Se habilita la interfaz física g1/0 en R1.

Verificamos el estado de las interfaces en R1 utilizando el siguiente comando.

R1#show ip interface brief

Figura 3: Estado e información de interfaces en R1

```

R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    unassigned      YES NVRAM    administratively down down
GigabitEthernet1/0 unassigned      YES NVRAM    up          up
GigabitEthernet1/0.1 10.0.113.1     YES NVRAM    up          up
GigabitEthernet1/0.2 10.0.108.1     YES NVRAM    up          up
GigabitEthernet2/0  unassigned      YES NVRAM    up          up
GigabitEthernet2/0.1 10.0.12.1      YES NVRAM    up          up
GigabitEthernet2/0.2 10.0.12.1      YES NVRAM    up          up
GigabitEthernet3/0  unassigned      YES NVRAM    administratively down down
GigabitEthernet4/0  unassigned      YES NVRAM    administratively down down
R1#

```

Fuente: Resultado de configuración en GNS3

Configuramos en Router 2

int gi 1/0.1	//Se especifica la interfaz g1/0.1 que asociaremos con la VRF "Special".
vrf forwarding SPECIAL-USER	//Se asocia la instancia VRF con la subinterfaz.
R2(config-subif)#encapsulation dot1Q 13	//Se habilita 802.1Q en la subinterfaz y se asocia a la vlan 13.
ip address 10.0.23.2 255.255.255.0	//Se asocia la IP a la subinterfaz.
ipv6 address 2001:DB8:ACAD:23::2/64	//Se asocia la IPv6 a subinterfaz.

int gi1/0.2	//Se especifica la interfaz que asociaremos con la VRF "General".
vrf forwarding GENERAL-USER	//Se asocia la VRF con la subinterfaz.
encapsulation dot1Q 8	//802.1Q habilitado y asociado a la vlan 8 en g1/0.2.
ip address 10.0.23.1 255.255.255.0	//Se asocia la IPv4 a subinterfaz.
ipv6 address 2001:DB8:ACAD:23::2/64	//Se asocia la IPv6 a subinterfaz.

int G2/0.1	//Configurar la interfaz G2/0.1
VRF forwarding SPECIAL-USER	//Asocia el VRF con la interfaz de Capa 3
encapsulation dot1q 13	//Habilitamos el trunk standar
ip address 10.0.12.2 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:12::2/64	//Establecer la dirección IPv6

int G2/0.2	//Configurar la interfaz G2/0.2
VRF forwarding GENERAL-USER	//Asocia el VRF con la interfaz de Capa 3
encapsulation dot1q 8	//Habilitamos el trunk standar
ip address 10.0.12.2 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:12::2/64	//Establecer la dirección IPv6
interf gi1/0	//Configuramos interfaz gi1/0
no shutdown	//Se habilita la interfaz física g1/0 en R2.
interf gi2/0	//Configuramos interfaz gi2/0
no shutdown	//Se habilita la interfaz física g1/0 en R2.

Verificamos el estado de las interfaces en R2 utilizando el siguiente comando.

R2#show ip interface brief

Figura 4: Estado e información de interfaces en R2

```
R2#show ip interface brief
Interface                IP-Address      OK? Method Status              Protocol
FastEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0     unassigned      YES NVRAM  up                  up
GigabitEthernet1/0.1   10.0.23.2       YES NVRAM  up                  up
GigabitEthernet1/0.2   10.0.23.2       YES NVRAM  up                  up
GigabitEthernet2/0     unassigned      YES NVRAM  up                  up
GigabitEthernet2/0.1   10.0.12.2       YES NVRAM  up                  up
GigabitEthernet2/0.2   10.0.12.2       YES NVRAM  up                  up
GigabitEthernet3/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0     unassigned      YES NVRAM  administratively down down
R2#
```

Fuente: Resultado de configuración en GNS3

Configuramos en Router 3

int gi 1/0.1	//Se especifica la interfaz g1/0.1 que asociaremos con la VRF "Special".
vrf forwarding SPECIAL-USER	//Se asocia la instancia VRF con la subinterfaz.
encapsulation dot1Q 13	//Se habilita 802.1Q en la subinterfaz y se asocia a la vlan 13.
ip address 10.0.23.3 255.255.255.0	//Se asocia la IP a la subinterfaz.
ipv6 address 2001:DB8:ACAD:23::3/64	//Se asocia la IPv6 a subinterfaz.

int gi1/0.2	//Se especifica la interfaz que asociaremos con la VRF "General".
vrf forwarding GENERAL-USER	//Se asocia la VRF con la subinterfaz.
encapsulation dot1Q 8	//802.1Q habilitado y asociado a la vlan 8 en g1/0.2.
ip address 10.0.23.3 255.255.255.0	//Se asocia la IPv4 a subinterfaz.
ipv6 address 2001:DB8:ACAD:23::3/64	//Se asocia la IPv6 a subinterfaz.

int G2/0.1	//Configurar la interfaz G2/0.1
VRF forwarding SPECIAL-USER	//Asocia el VRF con la interfaz de Capa 3
encapsulation dot1q 13	//Habilitamos el trunk standar
ip address 10.0.213.1 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:213::1/64	//Establecer la dirección IPv6

int G2/0.2	//Configurar la interfaz G2/0.2
VRF forwarding GENERAL-USER	//Asocia el VRF con la interfaz de Capa 3
encapsulation dot1q 8	//Habilitamos el trunk standar
ip address 10.0.208.1 255.255.255.0	//Establecer la dirección IPv4
ipv6 address 2001:db8:acad:208::1/64	//Establecer la dirección IPv6
interf gi1/0	//Configuramos interfaz gi1/0
no shutdown	//Se habilita la interfaz física g1/0 en R2.
interf gi2/0	//Configuramos interfaz gi2/0
no shutdown	//Se habilita la interfaz física g1/0 en R2.

Verificamos el estado de las interfaces en R3 utilizando el siguiente comando.

R3#show ip interface brief

Figura 5: Estado e información de interfaces en R3

```

R3#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    unassigned      YES NVRAM    administratively down  down
GigabitEthernet1/0 unassigned      YES NVRAM    up              up
GigabitEthernet1/0.1 10.0.23.3      YES NVRAM    up              up
GigabitEthernet1/0.2 10.0.23.3      YES NVRAM    up              up
GigabitEthernet2/0  unassigned      YES NVRAM    up              up
GigabitEthernet2/0.1 10.0.213.1     YES NVRAM    up              up
GigabitEthernet2/0.2 10.0.208.1     YES NVRAM    up              up
GigabitEthernet3/0  unassigned      YES NVRAM    administratively down  down
GigabitEthernet4/0  unassigned      YES NVRAM    administratively down  down
R3#

```

Fuente: Resultado de configuración en GNS3

2.3. En R1 y R3, configuramos las rutas estáticas predeterminadas que están en dirección a R2.

Configuramos en Router 1

En R1 se creamos la ruta IP estática con el siguiente salto (a R2) en el VRF GENERAL-USER.

```
R1(config)#ip route vrf GENERAL-USER 0.0.0.0 0.0.0.0 10.0.12.2
```

Luego verificamos utilizando el siguiente comando.

```
R1#show ip route vrf GENERAL-USER
```

Figura 6: Tabla de ruta en IPv4 para VRF GENERAL-USER en R1

```
R1#show ip route vrf GENERAL-USER
Routing Table: GENERAL-USER
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.12.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.0.12.2
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C     10.0.12.0/24 is directly connected, GigabitEthernet2/0.2
L     10.0.12.1/32 is directly connected, GigabitEthernet2/0.2
C     10.0.108.0/24 is directly connected, GigabitEthernet1/0.2
L     10.0.108.1/32 is directly connected, GigabitEthernet1/0.2
R1#
```

Fuente: Resultado de configuración en GNS3

En R1 se creamos la ruta IP estática con el siguiente salto (a R2) en el VRF SPECIAL-USER.

```
R1(config)#ip route vrf SPECIAL-USER 0.0.0.0 0.0.0.0 10.0.12.2
```

Luego verificamos utilizando el siguiente comando.

R1#show ip route vrf SPECIAL-USER

Figura 7: Tabla de ruta en IPv4 para VRF SPECIAL-USER en R1

```
R1#show ip route vrf SPECIAL-USER

Routing Table: SPECIAL-USER
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.12.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.0.12.2
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C     10.0.12.0/24 is directly connected, GigabitEthernet2/0.1
L     10.0.12.1/32 is directly connected, GigabitEthernet2/0.1
C     10.0.113.0/24 is directly connected, GigabitEthernet1/0.1
L     10.0.113.1/32 is directly connected, GigabitEthernet1/0.1
R1#
```

Fuente: Resultado de configuración en GNS3

Configuramos en Ipv6

R1(config)#ipv6 route vrf GENERAL-USER ::/0 2001:db8:acad:12::2

Luego verificamos utilizando el siguiente comando.

R1#show ipv6 route vrf GENERAL-USER

Figura 8: Tabla de ruta en IPv6 para VRF GENERAL-USER en R1

```
R1#show ipv6 route vrf GENERAL-USER
IPv6 Routing Table - GENERAL-USER - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
S    ::/0 [1/0]
     via 2001:DB8:ACAD:12::2
C    2001:DB8:ACAD:12::/64 [0/0]
     via GigabitEthernet2/0.2, directly connected
L    2001:DB8:ACAD:12::1/128 [0/0]
     via GigabitEthernet2/0.2, receive
C    2001:DB8:ACAD:108::/64 [0/0]
     via GigabitEthernet1/0.2, directly connected
L    2001:DB8:ACAD:108::1/128 [0/0]
     via GigabitEthernet1/0.2, receive
L    FF00::/8 [0/0]
     via Null0, receive
R1#
```

Fuente: Resultado de configuración en GNS3

R1(config)#ipv6 route vrf SPECIAL-USER ::/0 2001:db8:acad:12::2

Luego verificamos utilizando el siguiente comando.

R1#show ipv6 route vrf SPECIAL-USER

Figura 9: Tabla de ruta en IPv6 para VRF SPECIAL-USER en R1.

```
R1#show ipv6 route vrf SPECIAL-USER
IPv6 Routing Table - SPECIAL-USER - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
S    ::/0 [1/0]
     via 2001:DB8:ACAD:12::2
C    2001:DB8:ACAD:12::/64 [0/0]
     via GigabitEthernet2/0.1, directly connected
L    2001:DB8:ACAD:12::1/128 [0/0]
     via GigabitEthernet2/0.1, receive
C    2001:DB8:ACAD:113::/64 [0/0]
     via GigabitEthernet1/0.1, directly connected
L    2001:DB8:ACAD:113::1/128 [0/0]
     via GigabitEthernet1/0.1, receive
L    FF00::/8 [0/0]
     via Null0, receive
R1#
```

Fuente: Resultado de configuración en GNS3

Router 2

A continuación, creamos las rutas estáticas en R2 hacia R1 y R3:

```
R2(config)#ip route vrf GENERAL-USER 10.0.208.0 255.255.255.0 10.0.23.3
R2(config)#ip route vrf SPECIAL-USER 10.0.213.0 255.255.255.0 10.0.23.3
R2(config)#ip route vrf GENERAL-USER 10.0.108.0 255.255.255.0 10.0.12.1
R2(config)#ip route vrf SPECIAL-USER 10.0.113.0 255.255.255.0 10.0.12.1
```

```
R2(config)#ipv6 route vrf GENERAL-USER 2001:DB8:ACAD:208::/64
2001:DB8:ACAD:23::3
R2(config)#ipv6 route vrf SPECIAL-USER 2001:db8:acad:213::/64
2001:db8:acad:23::3
R2(config)#ipv6 route vrf GENERAL-USER 2001:db8:acad:108::/64
2001:db8:acad:12::1
R2(config)#ipv6 route vrf SPECIAL-USER 2001:db8:acad:113::/64
2001:db8:acad:12::1
```

Router 3

A continuación, se crean las rutas estáticas en R3 hacia R2:

```
R3(config)#ip route vrf SPECIAL-USER 0.0.0.0 0.0.0.0 10.0.23.2
```

Luego verificamos utilizando el siguiente comando.

```
R3#show ip route vrf SPECIAL-USER
```

Figura 10: Tabla de rupa en IPv4 VRF SPECIAL-USER en R3

```
R3#show ip route vrf SPECIAL-USER

Routing Table: SPECIAL-USER
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 10.0.23.2 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 10.0.23.2
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C   10.0.23.0/24 is directly connected, GigabitEthernet1/0.1
L   10.0.23.3/32 is directly connected, GigabitEthernet1/0.1
C   10.0.213.0/24 is directly connected, GigabitEthernet2/0.1
L   10.0.213.1/32 is directly connected, GigabitEthernet2/0.1
R3#
```

Fuente: Resultado de configuración en GNS3

R3(config)#ip route vrf GENERAL-USER 0.0.0.0 0.0.0.0 10.0.23.2

Luego verificamos utilizando el siguiente comando.

R3#show ip route vrf GENERAL-USER

Figura 11: Tabla de ruta en IPv4 para VRF GENERAL-USER en R3

```
R3#show ip route vrf GENERAL-USER

Routing Table: GENERAL-USER
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 10.0.23.2 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 10.0.23.2
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C   10.0.23.0/24 is directly connected, GigabitEthernet1/0.2
L   10.0.23.3/32 is directly connected, GigabitEthernet1/0.2
C   10.0.208.0/24 is directly connected, GigabitEthernet2/0.2
L   10.0.208.1/32 is directly connected, GigabitEthernet2/0.2
R3#
```

Fuente: Resultado de configuración en GNS3

Configuramos en IPV6

```
R3(config)#ipv6 route vrf GENERAL-USER ::/0 2001:db8:acad:23::2
```

Luego verificamos utilizando el siguiente comando.

```
R3#show ipv6 route vrf GENERAL-USER
```

Figura 12: Tabla de ruta en IPv6 para VRF GENERAL-USER en R3

```
R3#show ipv6 route vrf GENERAL-USER
IPv6 Routing Table - GENERAL-USER - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
S  ::/0 [1/0]
   via 2001:DB8:ACAD:23::2
C  2001:DB8:ACAD:23::/64 [0/0]
   via GigabitEthernet1/0.2, directly connected
L  2001:DB8:ACAD:23::3/128 [0/0]
   via GigabitEthernet1/0.2, receive
C  2001:DB8:ACAD:208::/64 [0/0]
   via GigabitEthernet2/0.2, directly connected
L  2001:DB8:ACAD:208::1/128 [0/0]
   via GigabitEthernet2/0.2, receive
L  FF00::/8 [0/0]
   via Null0, receive
R3#
```

Fuente: Resultado de configuración en GNS3

```
R3(config)#ipv6 route vrf SPECIAL-USER ::/0 2001:db8:acad:23::2
```

Luego verificamos utilizando el siguiente comando.

```
R3#show ipv6 route vrf SPECIAL-USER
```

Figura 13: Tabla de ruta en IPv6 para VRF SPECIAL-USER en R3

```
R3#show ipv6 route vrf SPECIAL-USER
IPv6 Routing Table - SPECIAL-USER - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S    ::/0 [1/0]
     via 2001:DB8:ACAD:23::2
C    2001:DB8:ACAD:23::/64 [0/0]
     via GigabitEthernet1/0.1, directly connected
L    2001:DB8:ACAD:23::3/128 [0/0]
     via GigabitEthernet1/0.1, receive
C    2001:DB8:ACAD:213::/64 [0/0]
     via GigabitEthernet2/0.1, directly connected
L    2001:DB8:ACAD:213::1/128 [0/0]
     via GigabitEthernet2/0.1, receive
L    FF00::/8 [0/0]
     via Null0, receive
R3#
```

Fuente: Resultado de configuración en GNS3

2.4. En este paso verificamos la conectividad en cada VRF

Se realizó la verificación y se pudo constatar la conectividad desde R1 a R3
En IPv4 y en IPv6

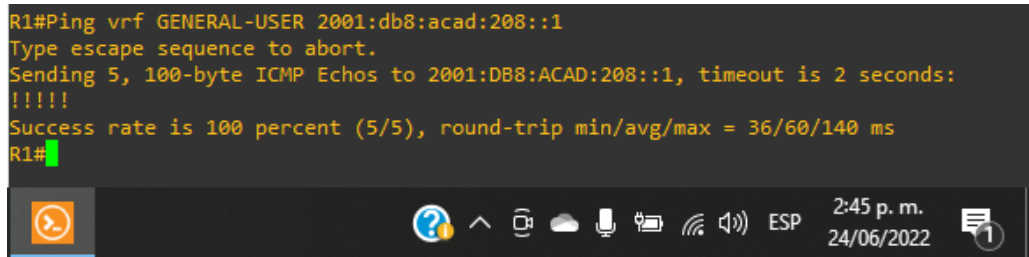
Figura 14: Ping vrf GENERAL-USER 10.0.208.1

```
R1#ping vrf GENERAL-USER 10.0.208.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.208.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/49/68 ms
R1#
```

Fuente: Resultado de configuración en GNS3

Figura 15: Ping vrf GENERAL-USER 2001:db8:acad:208::1

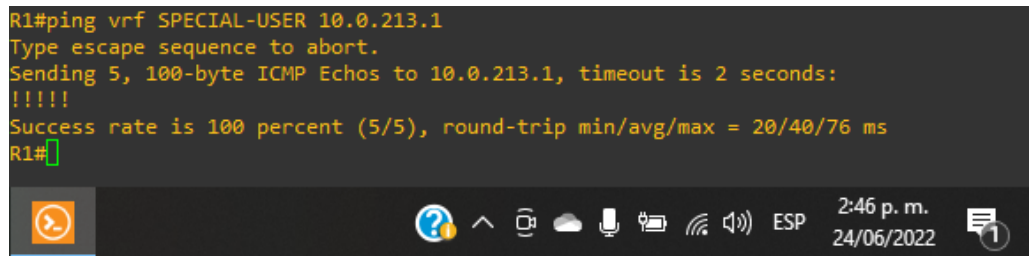
```
R1#ping vrf GENERAL-USER 2001:db8:acad:208::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:208::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/60/140 ms
R1#
```



Fuente: Resultado de configuración en GNS3

Figura 16: ping vrf SPECIAL-USER 10.0.213.1

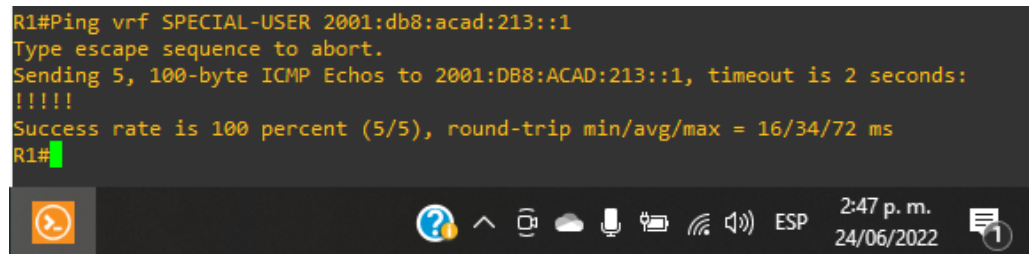
```
R1#ping vrf SPECIAL-USER 10.0.213.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.213.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/40/76 ms
R1#
```



Fuente: Resultado de configuración en GNS3

Figura 17: Ping vrf SPECIAL-USER 2001:db8:acad:213::1

```
R1#ping vrf SPECIAL-USER 2001:db8:acad:213::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:213::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/34/72 ms
R1#
```



Fuente: Resultado de configuración en GNS3

Parte 3: configurar capa 2

En la parte 3 configuramos los switches para soportar la conectividad con los dispositivos de finales.

Las tareas de configuración que realizamos son las siguientes.

3.1. En D1, D2 y A1 deshabilitamos todas las interfaces.

En D1 y D2, deshabilitamos G1/0/1 a G1/0/24. En A1, apagamos F0/1 – F0/24, G0/1 – G0/2.

Este procedimiento lo podemos realizar utilizando el comando Shutdown

Deshabilitamos las interfaces en D1.

interface range gi 0/0-3	//Configuramos interfaz gi0/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi1/0-3	//Configuramos interfaz gi1/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi2/0-3	//Configuramos interfaz gi2/0-3
D1(config-if-range)#shutdown	//Deshabilitamos las interfaces
interface range gi3/0-3	//Configuramos interfaz gi1/0
shutdown	//Deshabilitamos las interfaces

Deshabilitamos las interfaces en D2.

interface range gi0/0-3	//Configuramos interfaz gi0/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi1/0-3	//Configuramos interfaz gi1/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi2/0-3	//Configuramos interfaz gi2/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi3/0-3	//Configuramos interfaz gi3/0-3
shutdown	//Deshabilitamos las interfaces

Deshabilitamos las interfaces en A1.

interface range gi1/0-3	//Configuramos interfaz gi1/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi2/0-3	//Configuramos interfaz gi2/0-3
shutdown	//Deshabilitamos las interfaces
interface range gi3/0-3	//Configuramos interfaz gi3/0-3
shutdown	//Deshabilitamos las interfaces

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

En el switch D1 configuramos el Gi1/0 en modo troncal, que está conectado al Gi1/0 del R1.

interface gi1/0	//Se ingresa a modo de configuración de interfaz para g1/0.
sw trunk en dot1Q	//Se selecciona el protocolo de encapsulación (802.1Q).
sw mode trunk	//Se define la interfaz g1/0 en modo troncal.
no shutdown	//Habilitamos las interfaz

En el switch D2 configuramos el Gi1/0 en modo troncal, que está conectado al Gi2/0 del R3.

interface gi1/0	//Se ingresa a modo de configuración de interfaz para g1/0.
sw trunk en dot1Q	//Se selecciona el protocolo de encapsulación (802.1Q).
sw mode trunk	//Se define la interfaz g1/0 en modo troncal.
no shutdown	//Habilitamos las interfaz

3.3 En D1 y A1, configuramos el EtherChannel.

interf ra gi0/1-2	//Se ingresa a la configuración de las interfaces gi0/1-2
channel-group 1 mode desirable	//Se habilita canalPAgP numero 1
no shutdown	//Habilitamos las interfaz

interf ra gi0/1-2	//Se ingresa a la configuración de las interfaces gi0/1-2
channel-group 1 mode desirable	//Se habilita canalPAgP numero 1
no shutdown	//Habilitamos las interfaces

Luego verificamos utilizando el siguiente comando.

```
A1#show etherchannel summary
```

Figura 18: Detalles del port channel entre A1 y D1

```
A1#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)         PAgP       Gi0/1(P)  Gi0/2(P)
```

Fuente: Resultado de configuración en GNS3

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

Configuramos y habilitamos los puertos de acceso de la siguiente manera

En D1, configuramos la interfaz G3/0 como un puerto de acceso en la VLAN 13 y habilitamos Portfast, para PC1.

inter gi3/0	//Se ingresa a la configuración de la interfaz gi3/0
switchport mode Access	//Se configura la interface como puerto de acceso
switchport acces vlan 13	//Se relaciona el puerto de acceso a la vlan 13
no shutdown	//Habilitamos las interfaces

En D2, configuramos las interfaces G0/1 como un puerto de acceso en la VLAN 13 y habilitamos Portfast, para PC2.

inter gi0/1	//Se ingresa a la configuración de la interfaz gi0/1
switchport mode Access	//Se configura la interface como puerto de acceso
switchport acces vlan 13	//Se relaciona el puerto de acceso a la vlan 13
no shutdown	//Habilitamos las interfaces

En D2, configuramos las interfaces G0/2 como un puerto de acceso en la VLAN 8 y habilitamos Portfast, para PC4.

inter gi0/2	//Se ingresa a la configuración de la interfaz gi0/2
switchport mode Access	//Se configura la interface como puerto de acceso
switchport acces vlan 8	//Se relaciona el puerto de acceso a la vlan 8
no shutdown	//Habilitamos las interfaces

En A1, configuramos las interfaces G3/0 como un puerto de acceso en la VLAN 8 y habilitamos Portfast, para PC3.

inter gi3/0	//Se ingresa a la configuración de la interfaz gi3/0
switchport mode Access	//Se configura la interface como puerto de acceso
switchport acces vlan 8	//Se relaciona el puerto de acceso a la vlan 8
no shutdown	//Se habilita la interfaz

3.5 Verificar conectividad de PC a PC.

Utilizando el comando PING verificamos la conectividad entre PC.

Se realiza ping desde el PC 1 al PC 2 en IPv4, dirección IP 10.0.213.50

Figura 19: Ping de PC1 a PC2 en IPv4

```
PC1> ping 10.0.213.50
84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=83.684 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=75.436 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=176.924 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=88.332 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=73.200 ms
```

Fuente: Resultado de configuración en GNS3

Se realiza ping desde el PC 1 al PC 2 en IPv6, dirección 2001:db8:acad:213::50

Figura 20: Ping de PC1 a PC2 en IPv6

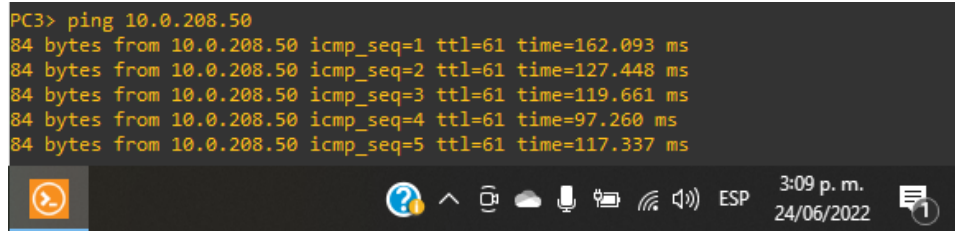
```
PC1> ping 2001:db8:acad:213::50
2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=233.648 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=101.725 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=123.220 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=93.925 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=98.570 ms
```

Fuente: Resultado de configuración en GNS3

Se realiza ping desde el PC 3 al PC 4 en IPv4, dirección IP 10.0.208.50

Figura 21: Ping de PC3 a PC4 en IPv4

```
PC3> ping 10.0.208.50
84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=162.093 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=127.448 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=119.661 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=97.260 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=117.337 ms
```

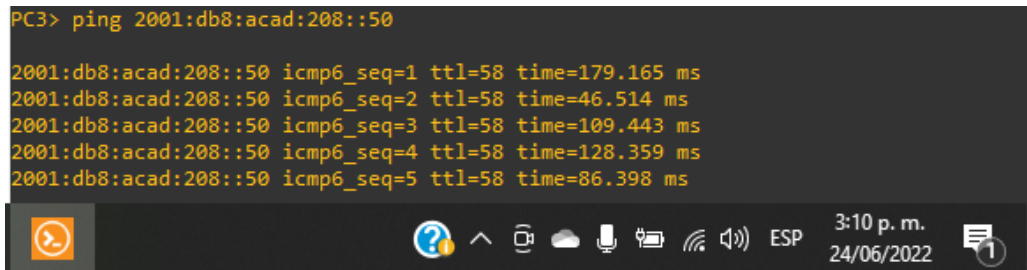


Fuente: Resultado de configuración en GNS3

Se realiza ping desde el PC 3 al PC 4 en IPv6, dirección 2001:db8:acad:208::50

Figura 22: Ping de PC3 a PC4 en IPv6

```
PC3> ping 2001:db8:acad:208::50
2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=179.165 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=46.514 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=109.443 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=128.359 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=86.398 ms
```



Fuente: Resultado de configuración en GNS3

Parte 4: Configure Seguridad

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

Las tareas de configuración son las siguientes:

4.1. En todos los dispositivos, modo EXE privilegiado.

En este paso configuramos en R1, R2, R3, D1, D2 y A1 las autenticaciones antes de permitir el acceso al modo Exec privilegiado.

Configuramos de la siguiente manera.

- Algorithm type: SCRYPT
- Password: cisco12345cisco.

```
R1(config)#enable secret cisco12345cisco
```

```
R2(config)#enable secret cisco12345cisco
```

```
R3(config)#enable secret cisco12345cisco
```

```
D1(config)#enable algorithm-type scrypt secret cisco12345cisco  
! se utiliza contraseña para habilitar
```

```
D2(config)#enable algorithm-type scrypt secret cisco12345cisco  
! se utiliza contraseña para habilitar
```

```
A1(config)#enable algorithm-type scrypt secret cisco12345cisco  
! se utiliza contraseña para habilitar
```

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

Configuramos en R1, R2, R3, D1, D2 y A1 los siguientes parámetros.

- Nombre: administrador
- Nivel de privilegio: 15, incluye todos los comandos de permiso
- Tipo de algoritmo: SCRYPT
- Contraseña: cisco12345cisco.

```
R1(config)#username admin privilege 15 secret cisco12345cisco
```

```
R2(config)#username admin privilege 15 secret cisco12345cisco
```

```
R3(config)#username admin privilege 15 secret cisco12345cisco
```

```
D1(config)#username admin privilege 15 algorithm-type scrypt secret  
cisco12345cisco
```

```
D2(config)#username admin privilege 15 algorithm-type scrypt secret  
cisco12345cisco
```

```
A1(config)#username admin privilege 15 algorithm-type scrypt secret  
cisco12345cisco
```

4.3. En todos los dispositivos, habilitamos AAA.

Configuraremos en R1, R2, R3, D1, D2 y A1 la autenticación AAA usando la base de datos local en todas las líneas.

Aplicando los protocolos AAA que nos permite el acceso a la red a los usuarios legítimos activos e impide el acceso no autorizado.

Ingresamos al modo de configuración global en R1, R2, R3, D1, D2 y A1

```
R#(Configure terminal)
```

Configuramos en Router 1

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local inicio de sesion administrador local.	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	// Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

Configuramos en Router 2

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local para inicio de sesion administrador local.	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	//Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

Configuramos en Router 3

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	//Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

Configuramos en switch D1

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	//Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

Configuramos en switch D2

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	//Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

Configuramos en switch A1

aaa new-model	//Se habilita la autenticación AAA
aaa authentication login Admin local	//Se habilita autenticación AAA para inicio de sesion administrador local.
aaa authorization exec Admin local	//Autorización AAA mode exec para administrador local.
aaa authorization console	//Se habilita autorización AAA para consola.
line vty 0 1500	//Se establecen sesiones Telnet
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.
line console 0	//Ingresamos al modo de configuración de linea
login authentication Admin	//Autenticación de administrador de inicio de sesion.
authorization exec Admin	//Autorización mode exec para administrador.

CONCLUSIONES

Podemos concluir que durante el desarrollo de esta actividad el uso de metodologías y técnicas de investigación permitieron validar los resultados obtenidos, así como el marco conceptual referente a las preguntas de investigación alusivas a los escenarios de los pollitos dando así el cumplimiento a cada uno de los lineamientos establecidos En la guía.

Al desarrollar esta actividad de prueba de habilidades de diplomados CCNP se ejecutó la configuración y diseño de un escenario propuesto, se realizó la configuración desde la etapa 1 se construyó la una red también se construyó la configuración básica de cada dispositivo se realizó configuración de reglas y protocolos de enrutamiento.

Esta actividad consistía, en el proceso de conceptualización de conocimientos que a su vez realizando las aplicaciones prácticas en programas de simulación lógica diseñando Cómo lo es GNS3 y VMawre como máquina virtual en lo que su principal objetivo, es medir los conocimientos y las capacidades de aplicación de conceptos durante el curso de Cisco CCNP.

Para tener en cuenta, en las configuraciones realizadas en GNS3, es muy importante salvar la información en los router, switch y PC en cada momento del proceso, ya que estas se borran si no las guardan, elegir dispositivos correctos para realizar el montaje, el GNS3 sin la máquina virtual no funciona.

Hemos visto a lo largo de todo el diplomado la importancia de comprender todos los escenarios de red, su funcionamiento, para que se requiere y así poder dar una solución eficaz y eficiente, en base a las necesidades de los usuarios.

BIBLIOGRAFIA

Castaño Rosero, J. A., & Rojas Muñoz, J. E. (2008). Estudio de Viabilidad para la Optimización de Enrutamiento IP con el Protocolo BGP. Disponible en: <http://repositorio.unicauca.edu.co:8080/xmlui/handle/123456789/2022> Cuesta

Martín, C. A. (2015). Análisis de desempeño con respecto al Jitter y Delay, en redes soportadas en MPLS, BGP y OSPF transmitiendo video sobre IP. <https://repository.usta.edu.co/handle/11634/309>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>