DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESUS ALBERTO ROMERO YEPES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
CARTAGENA
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESUS ALBERTO ROMERO YEPES

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

DIRECTOR:
Msc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
CARTAGENA
2023

Nota de Aceptación

_____

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Cartagena, 4 de Mayo de 2023

AGRADECIMIENTOS

Expreso mi gratitud a Dios por ser mi guía; agradezco a mi madre que con su esfuerzo, consejos y dedicación me ha ayuda a alcanzar esta meta.

A mis hermanos por su apoyo incondicional.

A los docentes de la Universidad Nacional Abierta y a Distancia, por haberme formado a los largo de la carrera profesional.

Y por último, a todas y cada una de las personas que han sido un apoyo al confiar en este sueño.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

DIRECCION IP: Es una representación numérica del punto de Internet donde está conectado un dispositivo. Una dirección IP tiene dos partes: el ID de red, compuesto por los tres primeros números de la dirección, y un ID de host, el cuarto número del grupo.

GNS3: Es un simulador gráfico de red, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

INTERFAZ: La conexión física y funcional que se establece entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro.

IPV4: Protocolo de Internet versión 4 (IPv4) es la forma de direccionamiento IP utilizada habitualmente para identificar hosts en una red y utiliza un formato de 32 bits.

IPV6: Protocolo de Internet versión 6 (IPv6) es el estándar de dirección IP de última generación diseñado para sustituir el formato IPv4. IPv6 resuelve el problema de escasez de direcciones mediante el uso de direcciones de 128 bits en lugar de direcciones de 32 bits que se utilizaban en IPv4.

PROTOCOLO AAA: (Authentication, Authorization, Accounting), permite el acceso de los usuarios legítimos a los activos conectados a la red e impide el acceso no autorizado.

RUTAS ESTÁTICAS: Se conocen como rutas explicitas entre dos dispositivos de una red, al ser estáticas estas no se actualizan automáticamente si no que deben ser configuradas manualmente cada que la red o topología sufra algún cambio.

VRF: Permite crear varias instancias de una tabla de enrutamiento en un Router permitiendo así subdividirlo internamente en enrutadores lógicos para que puedan ser implementados en distintitos clientes que se encuentren en la misma red física.

RESUMEN

Los retos que presentan las redes en cuanto a garantizar la estabilidad y la seguridad van en incremento. Por ello en el presente se lleva a cabo la construcción de una red, las configuraciones básicas de los dispositivos que la conforman, el direccionamiento de las interfaces Ethernet que los conectan, la configuración vrf y se asignan rutas estáticas con el fin de establecer comunicación independiente del grupo de los special users y general users que conforman la red, la configuración de la capa 2 y por último se configura la seguridad de la red. De esta manera, se fortalecen las habilidades asegurando buenos profesionales que resuelvan los retos que se van presentando.

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

ABSTRACT

The challenges presented by networks in terms of ensuring stability and security are increasing. For this reason, at present the construction of a network is carried out, the basic configurations of the devices that make it up, the addressing of the Ethernet interfaces that connect them, the vrf configuration and static routes are assigned in order to establish independent communication. from the group of special users and general users that make up the network, the configuration of layer 2 and finally the security of the network is configured. In this way, skills are strengthened, ensuring good professionals who solve the challenges that arise.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Los retos que se presentan en las redes en cuanto a garantizar la estabilidad y la seguridad va en incremento. Debido a que las sucesivas demandas en mantener las comunicaciones las 24 horas del día tanto en un hogar, como en una empresa y asimismo a nivel mundial exige mayores esfuerzos en búsqueda de la eficacia y eficiencia de las redes.

El presente trabajo busca estructurar, diseñar, planificar e implementar una red para fortalecer las habilidades que como profesionales debemos adquirir para enfrentar los retos que se van a ir presentando en el camino; por lo tanto la red propuesta está compuesta por dos grupos los special users y general users que serán independientes a pesar de estar en la misma red , se realizan las respectivas configuraciones que garantizan la independencia de estos grupos por medio de protocolos y asimismo se realizan configuraciones que le permiten a la red un acceso y gestión segura; donde todo esto se realiza por medio del simulador GNS3.

DESARROLLO

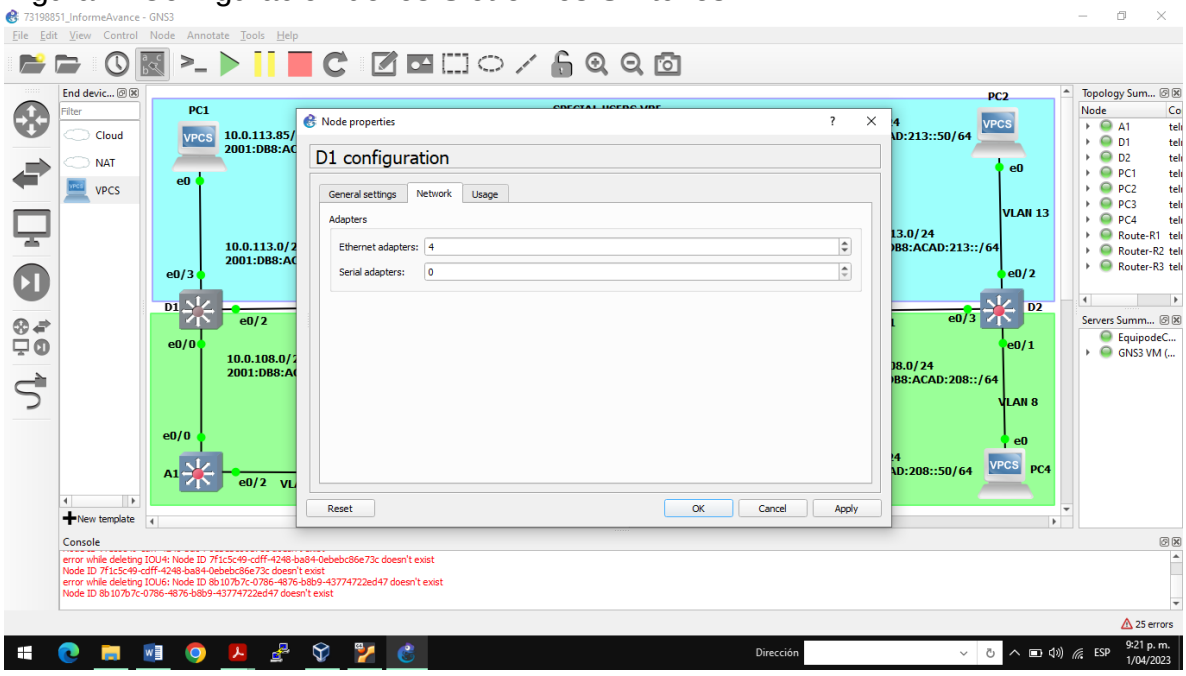
1. ESCENARIO

En este escenario se configurara la técnica multi-VRF en la red para que admita "Usuarios generales" y "Usuarios especiales" motivo por el cual los dos grupos no deberán poder comunicarse entre sí. Se debe configurar los router, los switch y PCs para que acepten tanto la conectividad IPv4 como IPv6, deberá haber accesibilidad completa de un extremo a otro.

1.1 PARTE 1: CONSTRUCCIÓN DE LA RED Y DEL DIRECCIONAMIENTO DE LA RED

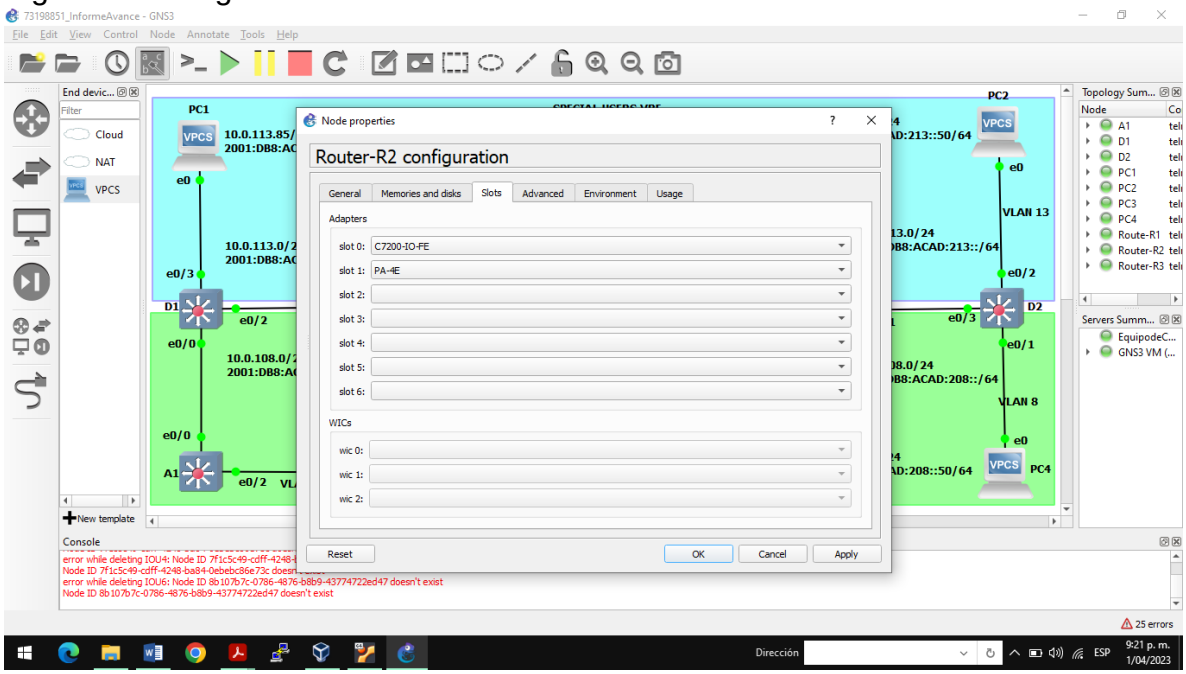
Se ingresa al ambiente de trabajo de la herramienta GNS3 y se agregan los dispositivos: router Cisco (03), switch Cisco (03) y Equipo de cómputo de escritorio (04). Por otra parte, al agregar los dispositivos, primeramente se requiere configurar los slots de cada SW según corresponde en los Switches y Routers.

Figura 1 Configuración de los Slot en los Switches



Fuente: Propia

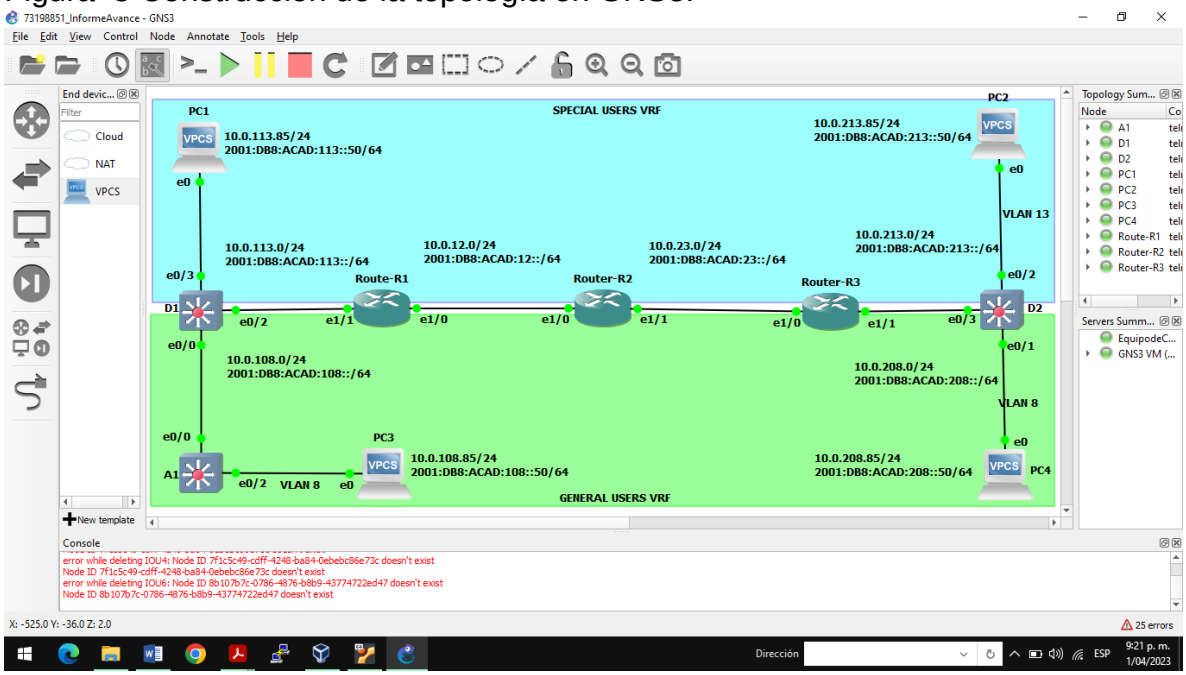
Figura 2 Configuración de los Slot en los Routers



Fuente: Propia

Se construye la red, conectando cada uno de sus dispositivos mediante cables Ethernet como se muestra en la topología.

Figura 3 Construcción de la topología en GNS3.



Fuente: Propia

Tabla 1 Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E1/0.1	10.0.12.8/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.8/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.8/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.8/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.5/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.5/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.1/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.85/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.85/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0 108.85/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.85/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Guía documento final CCNP

1.2 PARTE 2: CONFIGURACION DE LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS Y ASIGNACION DE DIRECCIONES IP A LOS PCS

Se ingresa a cada uno de los dispositivos y se realiza la configuración básica. La cual está compuesta por los siguientes comandos:

Router R1

#configure terminal
#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

Router R2

#configure terminal
#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

Router R3
#configure terminal
#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

Switch D1
#configure terminal
#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

Switch D2
#configure terminal
#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

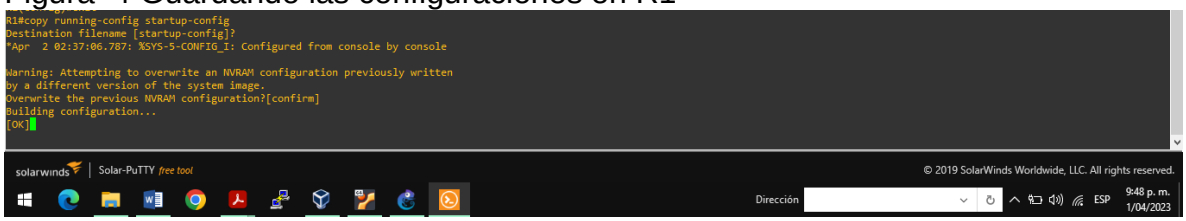
#logging synchronous
#exit
#vlan 8
#name general-users
#exit
#vlan 13
#name special-users
#exit

Switch A1
#configure terminal
#hostname A1
#ip routing
#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
#vlan 13
#name special-users
#exit

Después de colocar los comandos anteriores o realizar cualquier configuración hay que almacenar las configuraciones en cada dispositivo mediante el siguiente comando.

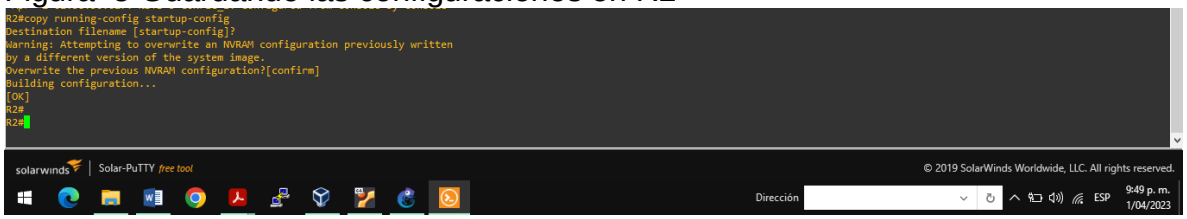
#copy running-config startup-config

Figura 4 Guardando las configuraciones en R1



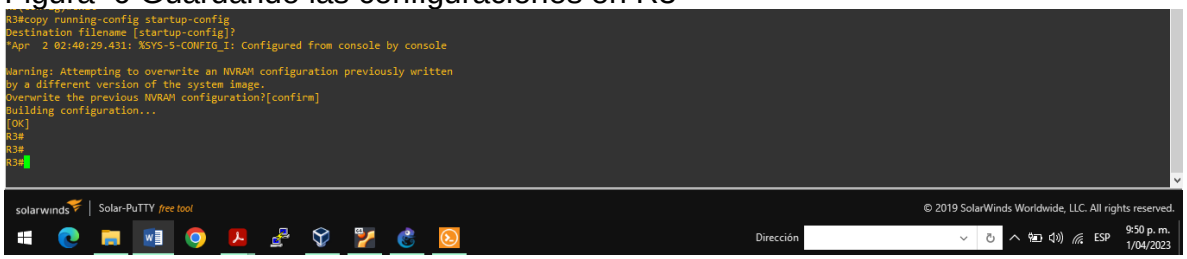
Fuente: Propia

Figura 5 Guardando las configuraciones en R2



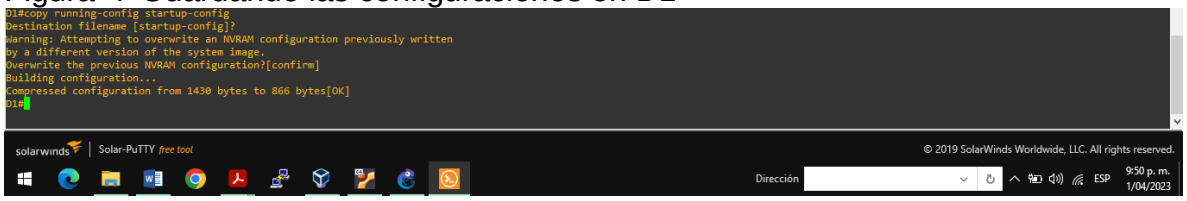
Fuente: Propia

Figura 6 Guardando las configuraciones en R3



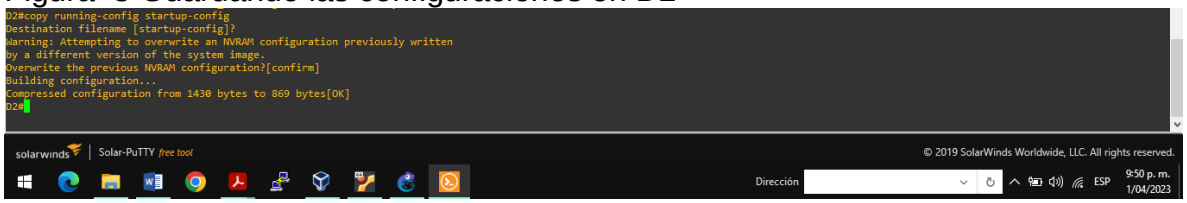
Fuente: Propia

Figura 7 Guardando las configuraciones en D1



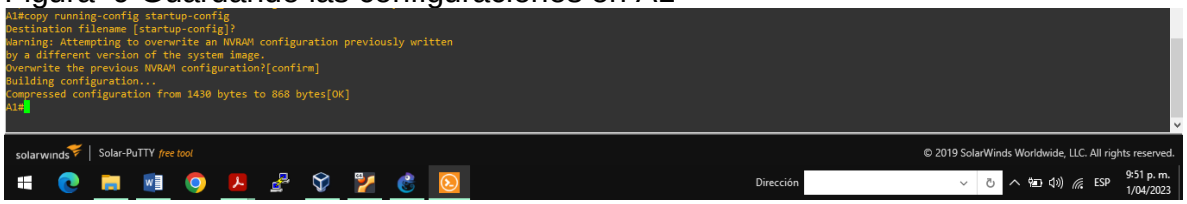
Fuente: Propia

Figura 8 Guardando las configuraciones en D2



Fuente: Propia

Figura 9 Guardando las configuraciones en A1

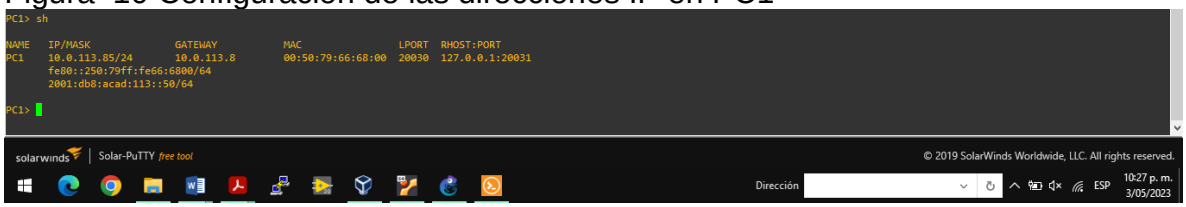


Fuente: Propia

Se asignan las direcciones IPv4 e IPv6 en los PCs, que se encuentran en la tabla 1 según corresponde, por consiguiente a través de las siguientes figuras al emitir el comando sh se observa la dirección IP previamente configurada.

PC1
#ip 10.0.113.85 mascara: 255.255.255.0 gateway: 10.0.113.8
#ip 2001:DB8:ACAD:113::50/64
#save

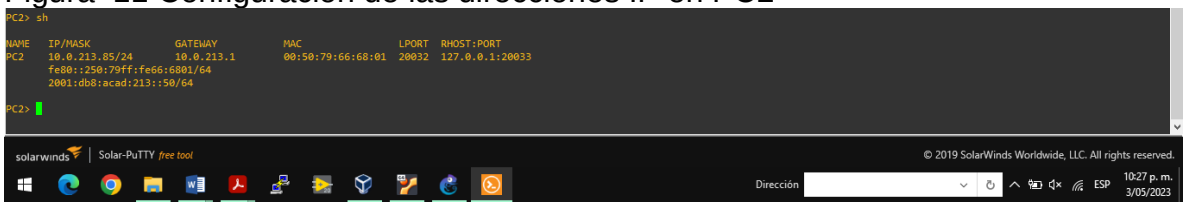
Figura 10 Configuración de las direcciones IP en PC1



Fuente: Propia

PC2
#ip 10.0.213.85 máscara: 255.255.255.0 gateway: 10.0.213.1
#ip 2001:DB8:ACAD:213::50/64
#save

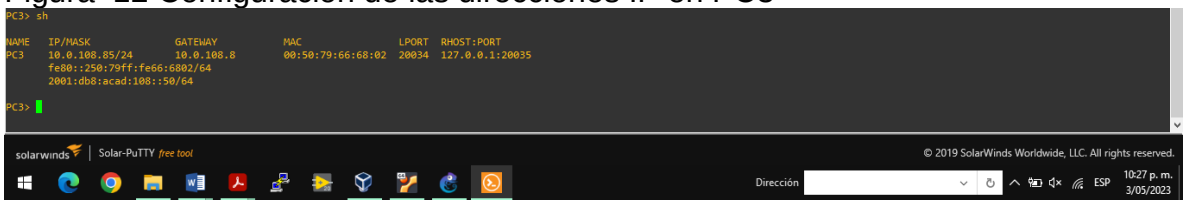
Figura 11 Configuración de las direcciones IP en PC2



Fuente: Propia

PC3
#ip 10.0.108.85/24 máscara: 255.255.255.0 gateway: 10.0.108.8
#ip 2001:DB8:ACAD:108::50/64
#save

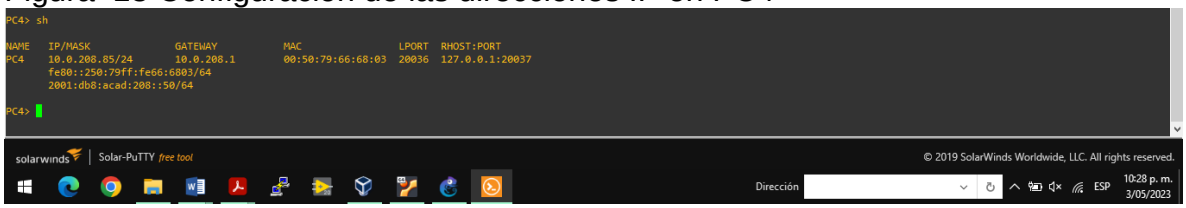
Figura 12 Configuración de las direcciones IP en PC3



Fuente: Propia

PC4
#ip 10.0.208.85 máscara: 25.255.255.0 Gateway: 10.0.208.1
#ip 2001:DB8:ACAD:208::50/64
#save

Figura 13 Configuración de las direcciones IP en PC4



Fuente: Propia

1.3 PARTE 3: CONFIGURACIÓN VRF Y LAS RUTAS ESTÁTICAS

En la configuración recomendada, es necesario indicar en que versión de IP se trabajará, por medio del comando address-family, para así luego de tener creadas las VRFs, asociarlas a las interfaces que trabajarán en cada una de estas. Por lo anterior, es necesario tener en cuenta, que una interfaz física o virtual solo puede pertenecer a una única VRF. Para estas configuraciones se emplean los comandos que se aprecian en las siguientes tablas para cada dispositivo.

Se configura VRF-Lite en los tres enrutadores y las rutas estáticas adecuadas para admitir la accesibilidad de un extremo a otro. Al final de esta parte, R1 debería poder hacer ping a R3 en cada VRF.

Por lo tanto, se inicia en R1, R2 y R3, se configura VRF-Lite VRF como se muestra en la topología. Se configuran dos VRF:

- Usuarios generales (general-users)
- Usuarios especiales (special-users)

Los VRF deben admitir IPv4 e IPv6 mediante los siguientes comandos.

Router R1
#configure terminal
#vrf definition special-users
#description special-users
#address-family ipv4
#exit
#description special-users

#address-family ipv6
#exit
#vrf definition general-users
#description general-users
#address-family ipv4
#exit
#description general-users
#address-family ipv6
#exit

Router R2
#configure terminal
#vrf definition special-users
#description special-users
#address-family ipv4
#exit
#description special-users
#address-family ipv6
#exit
#vrf definition general-users
#description general-users
#address-family ipv4
#exit
#description general-users
#address-family ipv6
#exit

Router R3
#configure terminal
#vrf definition special-users
#description special-users
#address-family ipv4
#exit
#description special-users
#address-family ipv6
#exit
#vrf definition general-users
#description general-users
#address-family ipv4
#exit
#description general-users
#address-family ipv6
#exit

En R1, R2 y R3, se configuran las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento. Todos los enrutadores utilizarán Router-On-A-Stick en sus interfaces para admitir la separación de los VRF. Se crean dos Sub-interfaces:

Sub-interfaz 1:

- En el VRF de Usuarios Especiales (special-users)
- Usa encapsulación dot1q 13
- IPv4 e IPv6 GUA y direcciones locales de enlace
- Habilita las interfaces

Sub-interfaz 2:

- En el VRF de Usuarios Generales (general-users)
- Usa encapsulación dot1q 8
- IPv4 e IPv6 GUA y direcciones locales de enlace
- Habilita las interfaces

Router R1

#configure terminal
#interface e1/0.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.12.8 255.255.255.0
#ipv6 address fe80::1:1 link-local
#ipv6 address 2001:db8:acad:12::1/64
#no shutdown
#exit
#interface e1/0.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.12.8 255.255.255.0
#ipv6 address fe80::1:2 link-local
#ipv6 address 2001:db8:acad:12::1/64
#no shutdown
#exit
#interface e1/0
#no ip address
#no shutdown
#exit
#interface e1/1.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.113.8 255.255.255.0

#ipv6 address fe80::1:3 link-local
#ipv6 address 2001:db8:acad:113::1/64
#no shutdown
#exit
#interface e1/1.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.108.8 255.255.255.0
#ipv6 address fe80::1:4 link-local
#ipv6 address 2001:db8:acad:108::1/64
#no shutdown
#exit
#interface e1/1
#no ip address
#no shutdown
#exit

Router R2
#configure terminal
#interface e1/0.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.12.5 255.255.255.0
#ipv6 address fe80::2:1 link-local
#ipv6 address 2001:db8:acad:12::2/64
#no shutdown
#exit
#interface e1/0.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.12.5 255.255.255.0
#ipv6 address fe80::2:2 link-local
#ipv6 address 2001:db8:acad:12::2/64
#no shutdown
#exit
#interface e1/0
#no ip address
#no shutdown
#exit
#interface e1/1.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.23.5 255.255.255.0
#ipv6 address fe80::2:3 link-local
#ipv6 address 2001:db8:acad:23::2/64

#no shutdown
#exit
#interface e1/1.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.23.5 255.255.255.0
#ipv6 address fe80::2:4 link-local
#ipv6 address 2001:db8:acad:23::2/64
#no shutdown
#exit
#interface e1/1
#no ip address
#no shutdown
#exit

Router R3
#configure terminal
#interface e1/0.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.23.1 255.255.255.0
#ipv6 address fe80::3:1 link-local
#ipv6 address 2001:db8:acad:23::3/64
#no shutdown
#exit
#interface e1/0.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.23.1 255.255.255.0
#ipv6 address fe80::3:2 link-local
#ipv6 address 2001:db8:acad:23::3/64
#no shutdown
#exit
#interface e1/0
#no ip address
#no shutdown
#exit
#interface e1/1.1
#encapsulation dot1q 13
#vrf forward special-users
#ip address 10.0.213.1 255.255.255.0
#ipv6 address fe80::3:3 link-local
#ipv6 address 2001:db8:acad:213::1/64
#no shutdown
#exit

#interface e1/1.2
#encapsulation dot1q 8
#vrf forward general-users
#ip address 10.0.208.1 255.255.255.0
#ipv6 address fe80::3:4 link-local
#ipv6 address 2001:db8:acad:208::1/64
#no shutdown
#exit
#interface e1/1
#no ip address
#no shutdown
#exit

La configuración de rutas estáticas VRF para IPv4 e IPv6 en ambos VRF, por medio de los siguientes comandos:

Router R1
#configure terminal
#ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.5
#ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.5
#ipv6 route vrf special-users ::/0 2001:db8:acad:12::2
#ipv6 route vrf general-users ::/0 2001:db8:acad:12::2

Router R2
#configure terminal
#ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.8
#ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.1
#ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.8
#ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.23.1
#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
#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

Router R3
#configure terminal
#ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.5
#ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.5
#ipv6 route vrf special-users ::/0 2001:db8:acad:23::2
#ipv6 route vrf general-users ::/0 2001:db8:acad:23::2

Ahora bien, por medio del comando ping podemos probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red, en esta parte de la configuración primero verificamos la conexión desde el Router R1 al R3, como se evalúa a continuación:

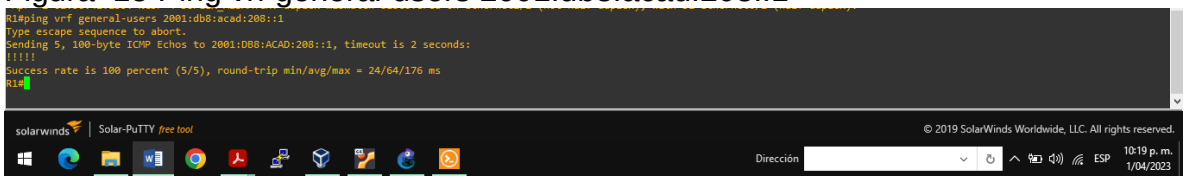
#ping vrf general-users 10.0.208.1

Figura 14 Ping vrf general-users 10.0.208.1

Fuente: Propia

#ping vrf general-users 2001:db8:acad:208::1

Figura 15 Ping vrf general-users 2001:db8:acad:208::1



Fuente: Propia

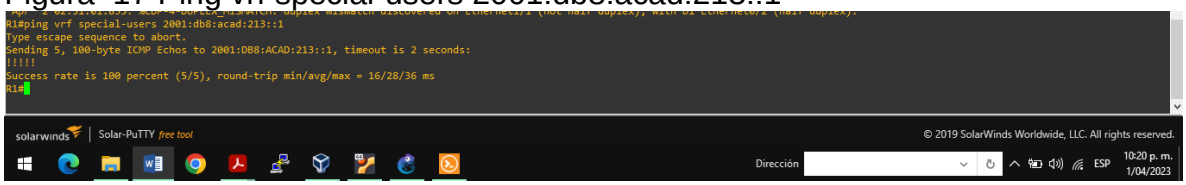
#ping vrf special-users 10.0.213.1

Figura 16 Ping vrf special-users 10.0.213.1

Fuente: Propia

#ping vrf special-users 2001:db8:acad:213::1

Figura 17 Ping vrf special-users 2001:db8:acad:213::1



Fuente: Propia

1.4 PARTE 4: CONFIGURACIÓN DE LA CAPA 2

En esta parte se configuran los switches para soportar conectividad con los dispositivos que conforman la red. Por lo tanto, para iniciar con esta parte de la configuración de la red, primero se deshabilitan los puertos de los switches D1, D2 y A1.

Switch D1
#interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
#shutdown
#exit

Switch D2
#interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
#shutdown
#exit

Switch A1
#interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 2/0-3, ethernet 3/0-3
#shutdown
#exit

Seguidamente en D1 y D2, se configuran los enlaces troncales a R1 y R3. Teniendo en cuenta que los enlaces troncales es un enlace de capa 2 del modelo OSI entre dos switches que transportan el tráfico para todas las VLAN. Asimismo en esta parte se configura y habilita el enlace e0/3 como enlace troncal.

Switch D1 hacia R1
#interface e0/2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#no shutdown
#exit

Switch D2 hacia R3
#interface e0/3
#switchport trunk encapsulation dot1q
#switchport mode trunk
#no shutdown
#exit

En D1 y A1, se configura el EtherChannel, por consiguiente se tiene en cuenta para cada switch que:

En D1, se configura y se habilita:

- Interfaz e0/0 y e0/1
- Canal de puerto 1 usando PAgP

En A1, se configura y se habilita:

- Interfaz e0/0 y e0/1
- Canal de puerto 1 usando PAgP

Switch D1

#interface e0/0
#switchport trunk encapsulation dot1q
#switchport mode trunk
#channel-group 1 mode desirable
#no shutdown
#exit
#interface e0/1
#switchport trunk encapsulation dot1q
#switchport mode trunk
#channel-group 1 mode desirable
#no shutdown
#exit

Switch A1

#interface e0/0
#switchport trunk encapsulation dot1q
#switchport mode trunk
#channel-group 1 mode desirable
#no shutdown
#exit
#interface e0/1
#switchport trunk encapsulation dot1q
#switchport mode trunk
#channel-group 1 mode desirable
#no shutdown
#exit

En D1, D2 y A1, se configuran los puertos de acceso para PC1, PC2, PC3 y PC4. Teniendo en cuenta que para llevar esto a cabo, se configura y habilitan los puertos de acceso de la siguiente forma:

- En D1, configure la interfaz E0/3 como un puerto de acceso en la VLAN 13 y habilite Portfast.
- En D2, configure la interfaz E0/2 como un puerto de acceso en la VLAN 13 y habilite Portfast.

- En D2, configure la interfaz E0/1 como un puerto de acceso en VLAN 8 y habilite Portfast.
- En A1, configure la interfaz E0/2 como un puerto de acceso en la VLAN 8 y habilite Portfast.

Switch D1
#interface e0/3
#switchport mode access
#switchport access vlan 13
#spanning-tree portfast
#no shutdown
#exit

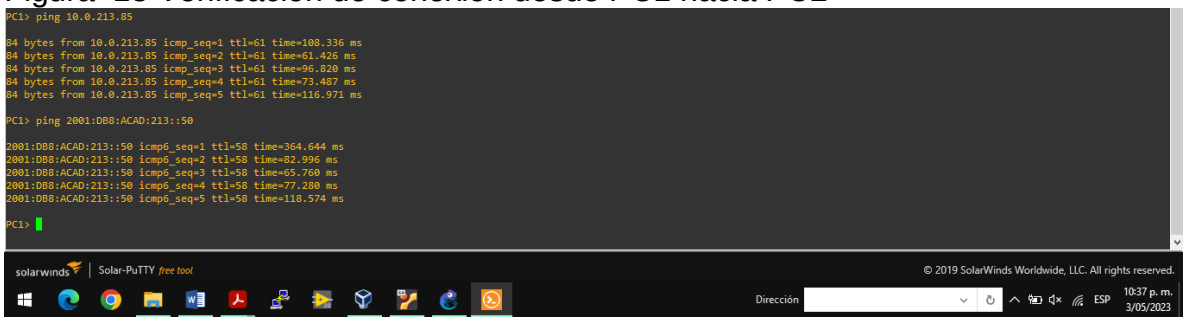
Switch D2
#interface e0/2
#switchport mode access
#switchport access vlan 13
#spanning-tree portfast
#no shutdown
#exit
#interface e0/1
#switchport mode access
#switchport access vlan 8
#spanning-tree portfast
#no shutdown
#exit

Switch A1
#interface e0/2
#switchport mode access
#switchport access vlan 8
#spanning-tree portfast
#no shutdown
#exit

En esta parte, por último se verifica la conectividad de PC a PC, por medio de colocar el comando ping desde la PC1 a la PC2 y desde la PC3 a la PC4.

PC1 hacia la PC2
#ping 10.0.213.85
#ping 2001:DB8:ACAD:213::50

Figura 18 Verificación de conexión desde PC1 hacia PC2



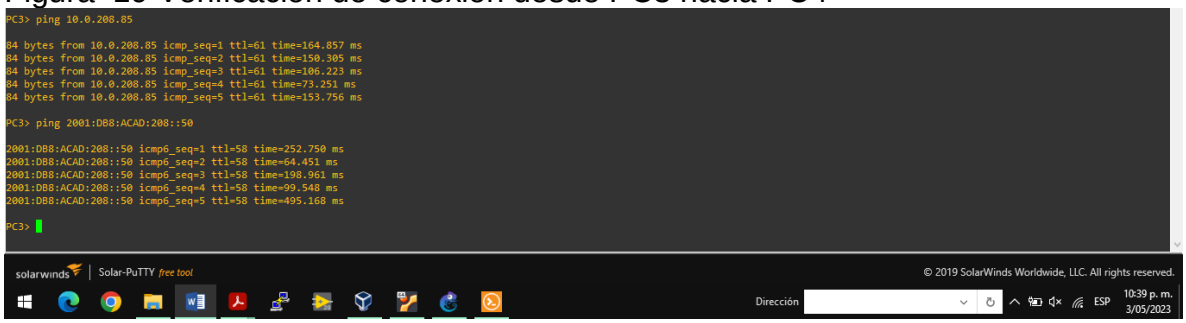
Fuente: Propia

PC3 hacia la PC4

#ping 10.0.208.85

#ping 2001:DB8:ACAD:208::50

Figura 19 Verificación de conexión desde PC3 hacia PC4



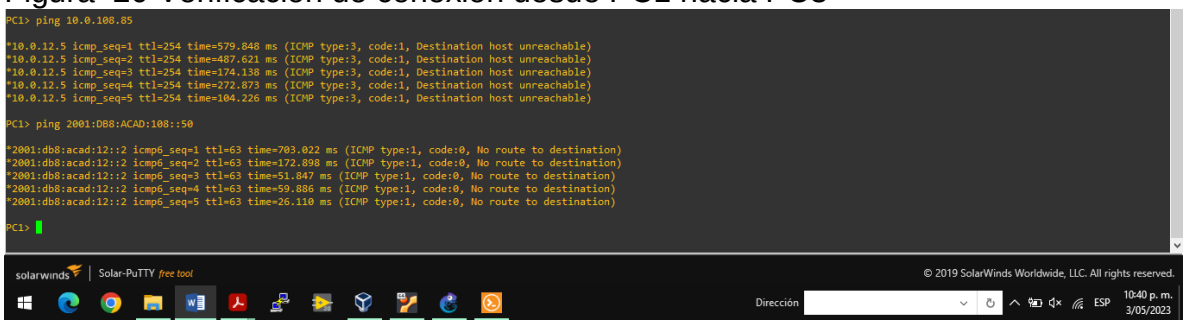
Fuente: Propia

PC1 hacia la PC3

#ping 10.0.108.85

#ping 2001:DB8:ACAD:108::50

Figura 20 Verificación de conexión desde PC1 hacia PC3



Fuente: Propia

1.5 PARTE 5: CONFIGURACIÓN DE LA SEGURIDAD

Esta parte, está compuesta de distintos mecanismos que garantizan la seguridad de los dispositivos. Para lo cual, en todos los dispositivos en el modo EXE privilegiado seguro. Se configura un secreto de habilitación de la siguiente manera:

- Tipo de algoritmo: scrypt
- Contraseña: Jesus851

Router R1
#enable algorithm-type scrypt secret Jesus851

Router R2
#enable algorithm-type scrypt secret Jesus851

Router R3
#enable algorithm-type scrypt secret Jesus851

Switch D1
#enable algorithm-type scrypt secret Jesus851

Switch D2
#enable algorithm-type scrypt secret Jesus851

Switch A1
#enable algorithm-type scrypt secret Jesus851

En todos los dispositivos, se crea una cuenta de usuario local. Teniendo en cuenta los siguientes ítems:

- Nombre: admin
- Nivel de privilegio: 15
- Tipo de algoritmo: scrypt
- Contraseña: Jesus851

Router R1
#username admin privilege 15 algorithm-type scrypt secret Jesus851

Router R2
#username admin privilege 15 algorithm-type scrypt secret Jesus851

Router R3
#username admin privilege 15 algorithm-type scrypt secret Jesus851

Switch D1
#username admin privilege 15 algorithm-type scrypt secret Jesus851

Switch D2
#username admin privilege 15 algorithm-type scrypt secret Jesus851

Switch A1
#username admin privilege 15 algorithm-type scrypt secret Jesus851

En fin en todos los dispositivos, se habilita AAA y se habilita la autenticación AAA.

Router R1
#aaa new-model
#aaa authentication login default local

Router R2
#aaa new-model
#aaa authentication login default local

Router R3
#aaa new-model
#aaa authentication login default local

Switch D1
#aaa new-model
#aaa authentication login default local

Switch D2
#aaa new-model
#aaa authentication login default local

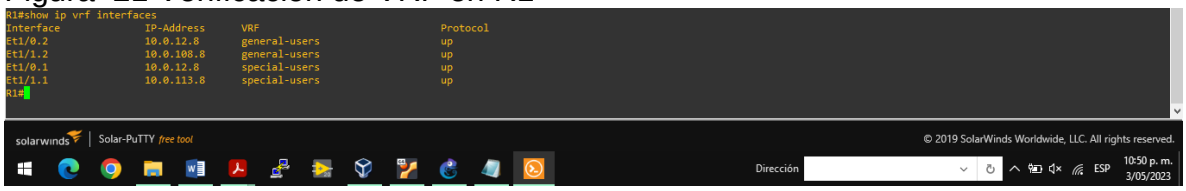
Switch A1
#aaa new-model
#aaa authentication login default local

1.6 PARTE 6: VERIFICACIÓN DE LAS CONFIGURACIONES DE LA RED

Después de colocar los comandos anteriores en el puerto de consola de cada dispositivo según corresponda, se realizan validaciones de que estén bien realizadas las configuraciones. Por lo tanto, se colocan los siguientes comandos:

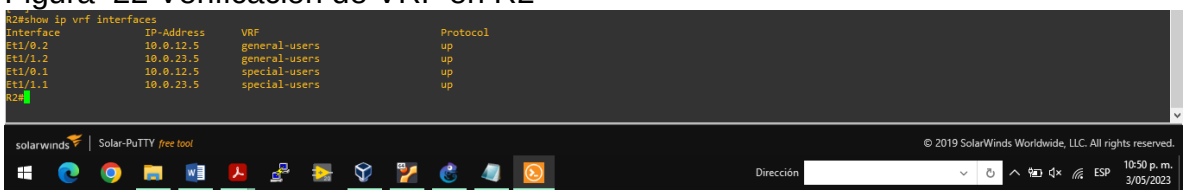
Comando de verificación de VRF
#show ip vrf interfaces

Figura 21 Verificación de VRF en R1



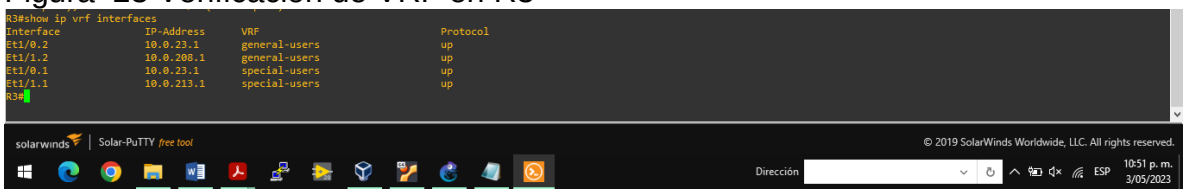
Fuente: Propia

Figura 22 Verificación de VRF en R2



Fuente: Propia

Figura 23 Verificación de VRF en R3

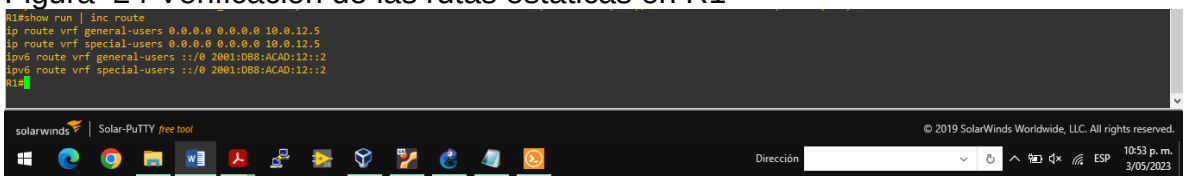


Fuente: Propia

Comandos de verificación de rutas estáticas

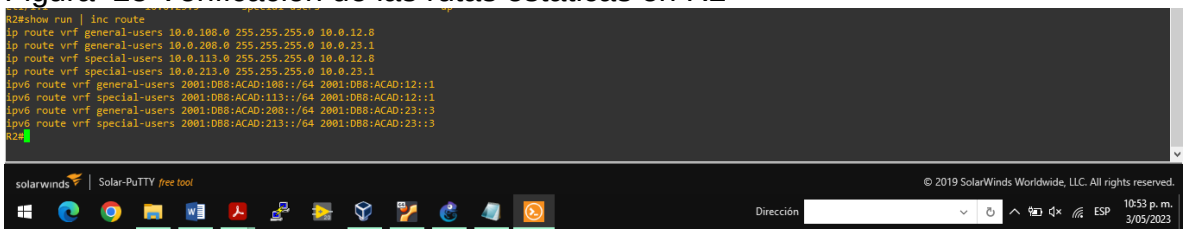
#show run | inc route

Figura 24 Verificación de las rutas estáticas en R1



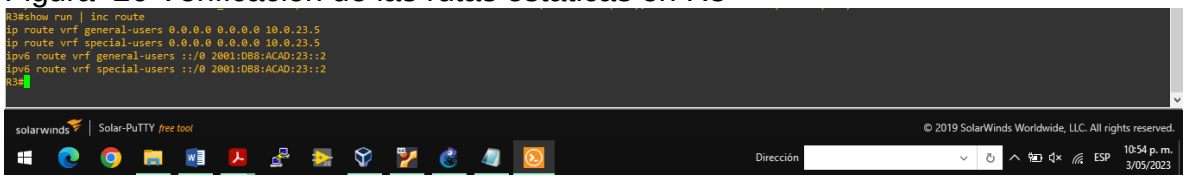
Fuente: Propia

Figura 25 Verificación de las rutas estáticas en R2



Fuente: Propia

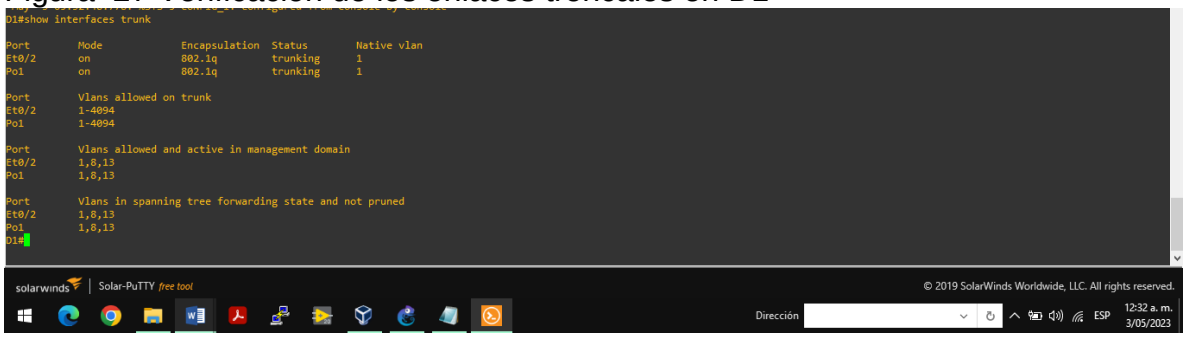
Figura 26 Verificación de las rutas estáticas en R3



Fuente: Propia

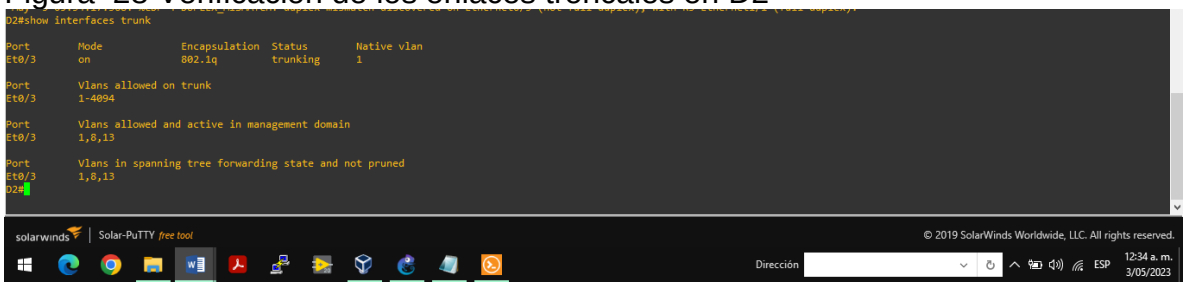
Comando de verificación de la capa 2
#show interfaces trunk

Figura 27 Verificación de los enlaces troncales en D1



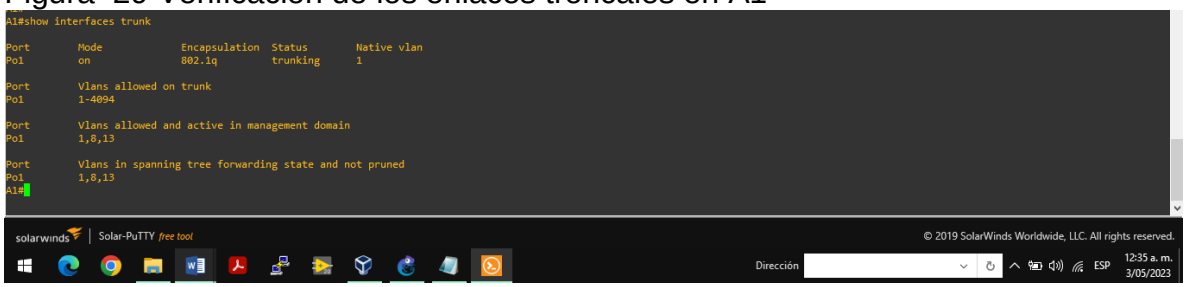
Fuente: Propia

Figura 28 Verificación de los enlaces troncales en D2



Fuente: Propia

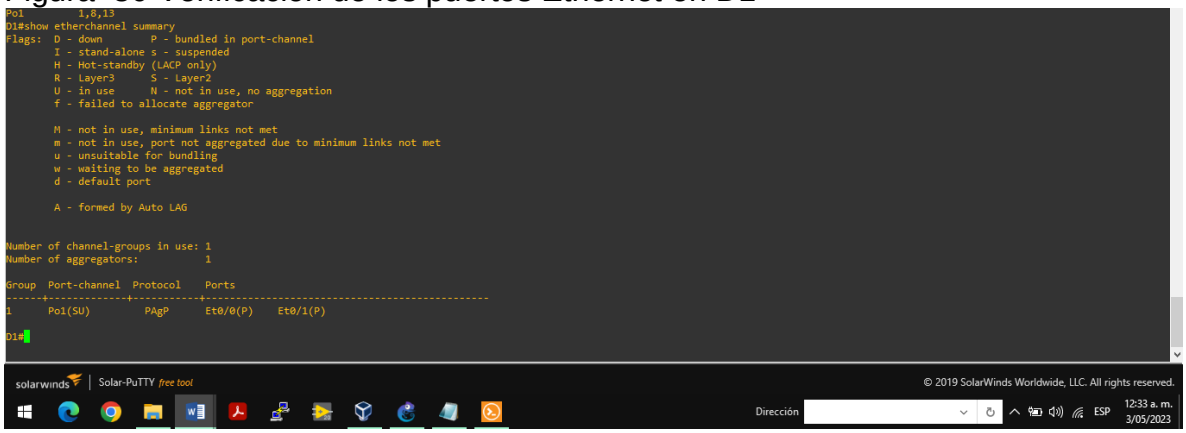
Figura 29 Verificación de los enlaces troncales en A1



Fuente: Propia

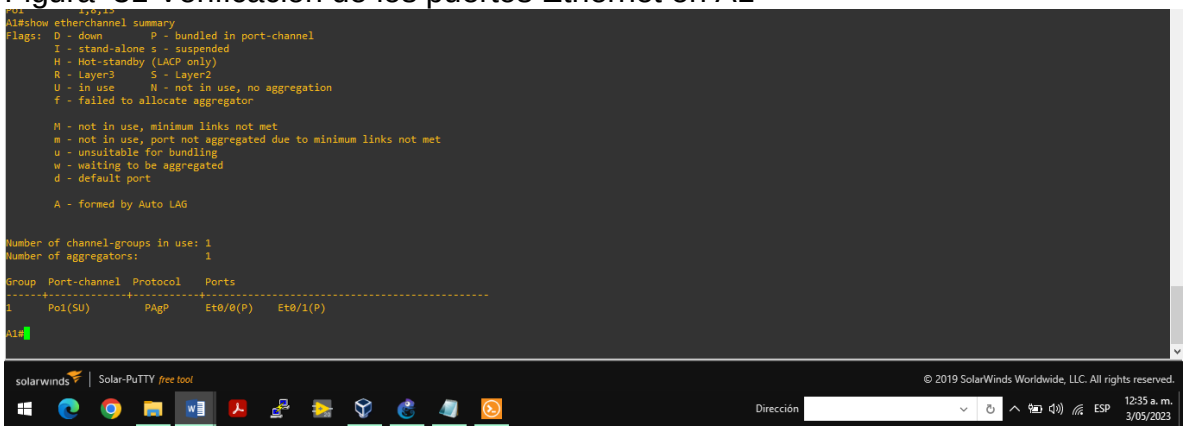
#show etherchannel summary

Figura 30 Verificación de los puertos Ethernet en D1



Fuente: Propia

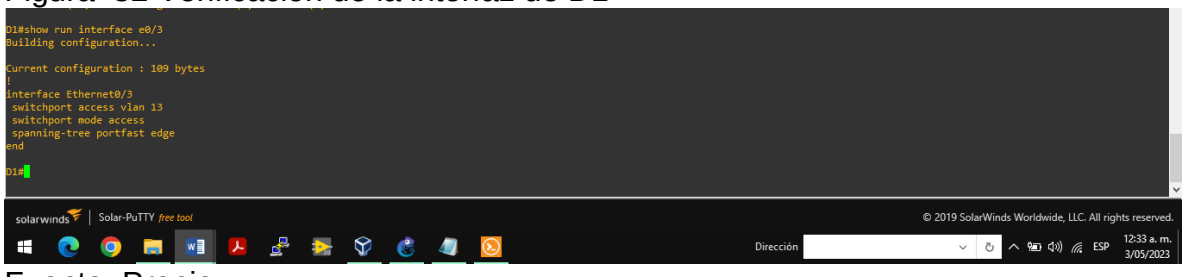
Figura 31 Verificación de los puertos Ethernet en A1



Fuente: Propia

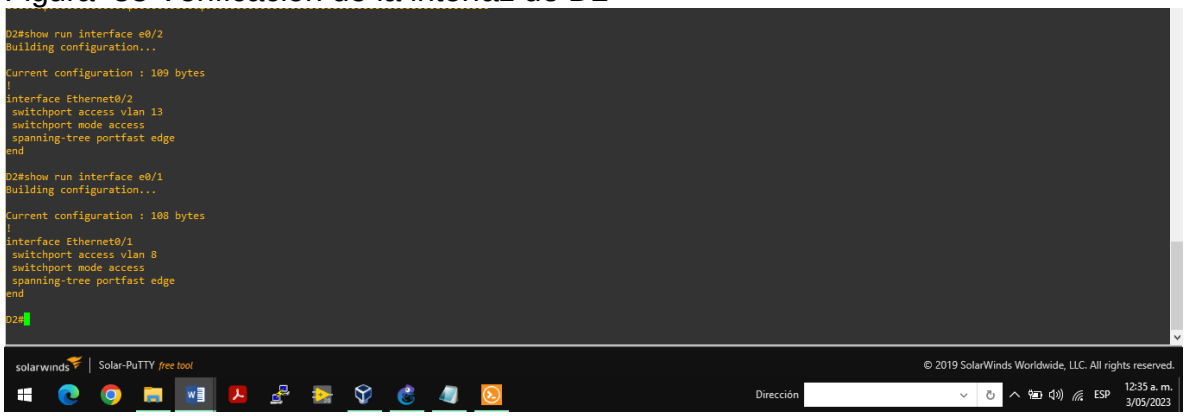
Comando de verificación exacta de la configuración de una interfaz
#show run interface

Figura 32 Verificación de la interfaz de D1



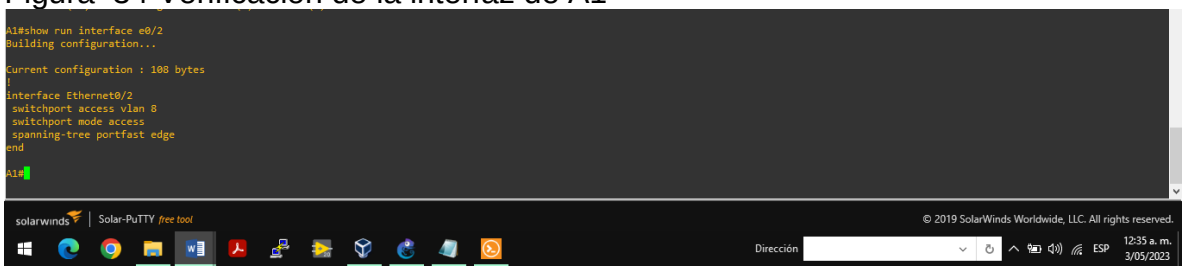
Fuente: Propia

Figura 33 Verificación de la interfaz de D2



Fuente: Propia

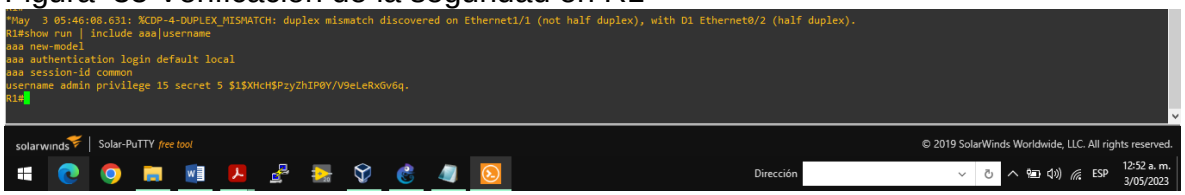
Figura 34 Verificación de la interfaz de A1



Fuente: Propia

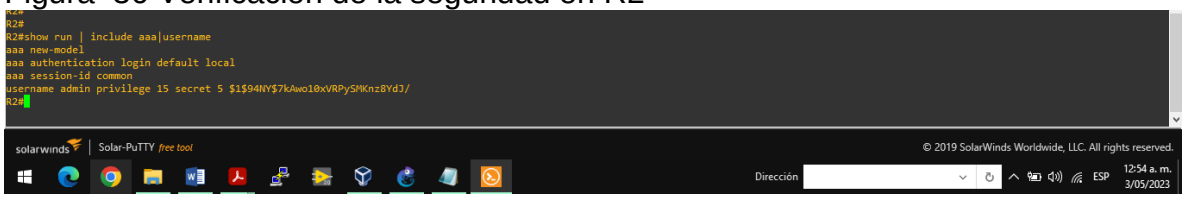
Comando de verificación de las configuraciones de seguridad.
#show run | include aaa|username

Figura 35 Verificación de la seguridad en R1



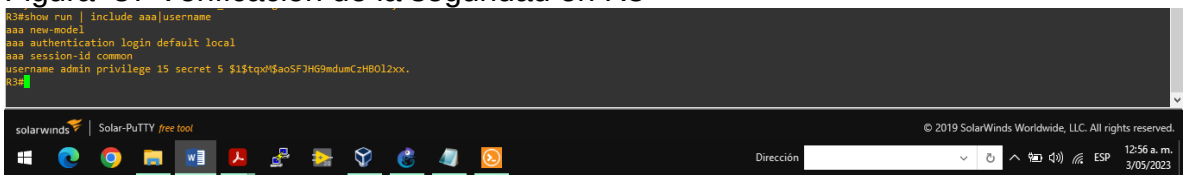
Fuente: Propia

Figura 36 Verificación de la seguridad en R2



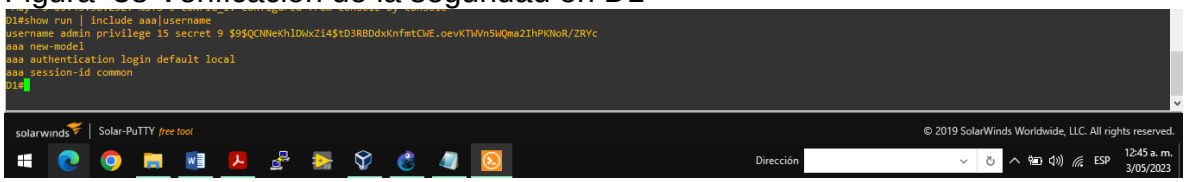
Fuente: Propia

Figura 37 Verificación de la seguridad en R3



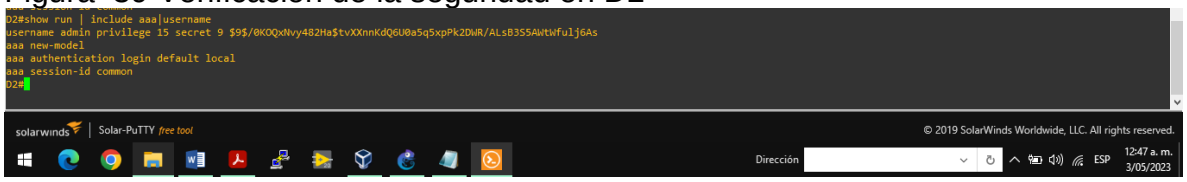
Fuente: Propia

Figura 38 Verificación de la seguridad en D1



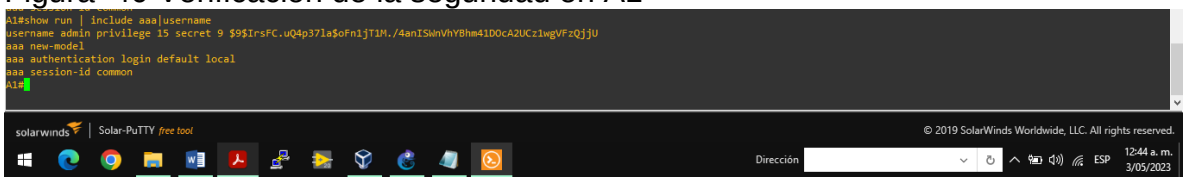
Fuente: Propia

Figura 39 Verificación de la seguridad en D2



Fuente: Propia

Figura 40 Verificación de la seguridad en A1



Fuente: Propia

CONCLUSIONES

Luego de analizar la red e integrar todas las configuraciones, se pudo evidenciar la importancia de los comandos show; razón por la cual, antes de configurar una red se deben tener las bases para alcanzar los requerimientos que está necesite como fue el caso; obteniendo una satisfactoria conectividad tanto para los usuarios generales como especiales.

De esta manera, con la implementación de la configuración VRF se obtiene una mayor facilidad para garantizar la autonomía en una red, logrando mayores beneficios como son la seguridad, privacidad y el desempeño de la red.

Por otra parte, la configuración de los enlaces troncales de VLAN 13 y 8 en las interfaces, faculta a los dispositivos para que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a diferentes switches se puedan comunicar sin la mediación necesaria de un router. Observado que efectivamente se logró la conexión desde PC1 hacia PC2 que estaban separados por tres routers y entre PC3 y PC4 sin necesidad de más configuraciones.

Asimismo, se comprobó que la configuración de los puertos Etherchannels en D1 y A1; crea una negociación con uno de dos protocolos: PAgP o LACP. Y estos protocolos permiten que los puertos con características similares formen un canal mediante una negociación dinámica en este caso entre D1 y A1.

Después de realizar la configuración de seguridad por medio del protocolo AAA; fue conveniente salir y volver a ingresar a los dispositivos, notando que para poder establecer comunicación entre los dispositivos se tuvo que ingresar con el usuario y contraseña establecido a cada uno de los dispositivos y luego si hacer ping desde los PCs dependiendo de los grupos. Por lo tanto se verifico que efectivamente este protocolo si proporciona un acceso totalmente seguro.

REFERENCIAS

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

UNAD (2020). Configuración de Switches y Routers [OVA]. https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8