

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JORGE GRACIANO APONTE MENDIVELSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA EN TELECOMUNICACIONES
BOGOTÁ
2022

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JORGE GRACIANO APONTE MENDIVELSO

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
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 26 de junio de 202

AGRADECIMIENTOS

En primer lugar, agradezco a dios por darme la oportunidad de tener una familia tan maravillosa, que me ha apoyado en todo este proceso de estudio y su ayuda fue fundamental para cumplir los objetivos y proyectos propuestos a lo largo de la carrera, siempre estuvieron en los momentos difíciles ayudándome a tomar las mejores decisiones para mi futuro como profesional.

Agradezco a la Universidad Nacional Abierta y a Distancia por abrirme las puertas y darme el chance de llevar a cabo mis estudios en ingeniería en telecomunicaciones, brindándome la oportunidad de formarme tanto personal como profesionalmente.

Finalmente agradezco la ayuda de los tutores por las enseñanzas y conocimientos brindados en cada momento y su disposición para atender las dudas e inquietudes que se presentaron a lo largo de cada asignatura por medio de los foros y la atención vía webconferencia, además agradezco a los compañeros de cada asignatura por su compromiso en cada trabajo colaborativo, aportando ideas y conocimientos indispensables para enriquecer nuestro proceso de enseñanza-aprendizaje y buscar siempre la excelencia en los trabajos a entregar. Muchas gracias a todos

CONTENIDO

AGRADECIMIENTOS.....	4
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN	10
DESARROLLO	11
ESCENARIO.....	11
Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces	12
Paso 1: Cablee la red como se muestra en la topología.....	12
Paso 2: Configure los ajustes básicos para cada dispositivo	13
Parte 2: configurar VRF y enrutamiento estático	17
Tarea 2.1	18
Tarea 2.2.....	19
Tarea 2.3.....	22
Tarea 2.4.....	26
Parte 3. Configurar Capa 2.....	28
Tarea 3.1	29
Tarea 3.2.....	29
Tarea 3.3.....	30
Tarea 3.4.....	31
Tarea 3.5.....	32
Parte 4. Configurar Seguridad	33
Tarea 4.1	34
Tarea 4.2.....	34
Tarea 4.3.....	34
CONCLUSIONES	36
BIBLIOGRAFÍA.....	37

LISTAS DE TABLAS

TABLA 1. DIRECCIONAMIENTO DE TOPOLOGÍA DE RED PROPUESTA.....	11
TABLA 2. TABLA DE DIRECCIONAMIENTO SE CAMBIAN INTERFACES.....	12
TABLA 3. CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO.....	17
TABLA 4. CONFIGURAR CAPA 2.....	28
TABLA 5. CONFIGURAR SEGURIDAD	33

LISTA DE FIGURAS

FIGURA 1. ESCENARIO PROPUESTO	11
FIGURA 2. SIMULACIÓN DE ESCENARIO	12
FIGURA 3. GUARDADO DE LAS CONFIGURACIONES	16
FIGURA 4. CONFIGURACIÓN PC1, PC2, PC3 Y PC4	16
FIGURA 5. CONFIGURACIÓN DE RUTAS (GENERAL-USERS)	23
FIGURA 6. CONFIGURACIÓN DE RUTAS (SPECIAL-USERS)	23
FIGURA 7. CONFIGURACIÓN DE RUTAS (GENERAL-USERS)	24
FIGURA 8. CONFIGURACIÓN DE RUTAS (SPECIAL-USERS)	25
FIGURA 9. CONFIGURACIÓN DE RUTAS (GENERAL-USERS)	26
FIGURA 10. CONFIGURACIÓN DE RUTAS (SPECIAL-USERS)	26
FIGURA 11. PING DE R1 A R3 (SPECIAL-USERS)	26
FIGURA 12. PING DE R1 A R3 (GENERAL-USERS)	27
FIGURA 13. PING DE R3 A R1 (SPECIAL-USERS)	27
FIGURA 14. PING DE R3 A R1 (GENERAL-USERS)	27
FIGURA 15. CONECTIVIDAD PC1 A PC2	32
FIGURA 16. CONECTIVIDAD PC3 A PC4	33
FIGURA 17. AUTENTICACIÓN AAA EN R1	34
FIGURA 18. AUTENTICACIÓN AAA EN R2	34
FIGURA 19. AUTENTICACIÓN AAA EN R3	35
FIGURA 20. AUTENTICACIÓN AAA EN D1	35
FIGURA 21. AUTENTICACIÓN AAA EN D2	35
FIGURA 22. AUTENTICACIÓN AAA EN A1	35

GLOSARIO

Enrutamiento estático: Este enrutamiento se encarga de enviar el tráfico por la red hacia una ruta definida por el administrador, es decir en cada Router de la red se configura manualmente las rutas de sus vecinos y se crea una tabla de enrutamiento específica que contenga todas las rutas existentes de la red, con el fin de enviar el tráfico de manera controlada, hacia una ruta específica.

EtherChannel: Esta tecnología permite agrupar varias interfaces de un Switch, para formar interfaces lógicas, es decir para comunicar 2 Switch por EtherChannel podemos usar el protocolo de Cisco PAgP, Con el fin de dar redundancia al canal y balancear la carga del tráfico.

Protocolo de enrutamiento: son reglas que se encargan de definir el camino más óptimo para que un paquete viaje a través de la red y llegue a su destino de manera exitosa.

Router: Es un dispositivo electrónico que conecta dispositivos a nivel de red, trabaja en la capa 3 del modelo OSI, permitiendo la comunicación con otros routers de diferentes redes por medio de protocolos de enrutamiento como (RIP, OSPF, EIGRP, BGP, entre otros), con el fin de buscar la mejor ruta para enviar los paquetes en la red.

Switch: Es un dispositivo electrónico que conecta dispositivos finales en una red local como (impresoras, AP, teléfonos IP, cámaras, computadoras, datafonos, entre otros), este dispositivo trabaja en la capa 2 del modelo OSI, enviando los paquetes de acuerdo a la dirección física MAC de cada dispositivo.

VFR (Virtual Routing and Forwarding): Es una tecnología que permite particionar el router físico en varios routers virtuales, esto garantiza tablas de enrutamiento totalmente independientes dentro del router físico, además de brindar seguridad para los clientes ya que el tráfico está totalmente aislado para cada VRF. esta tecnología se puede trabajar con IPV4 e IPV6

VLAN (Virtual LAN): es una tecnología que permite agrupar puertos lógicos dentro de un switch, con el fin de crear servicios dentro del mismo como (Datos, voz, Internet, entre otros), además las Vlan ayudan al rendimiento de la red y proporcionan una seguridad adicional para cada servicio.

RESUMEN

La prueba de habilidades prácticas del diplomado de profundización cisco CCNP, adscrito a la ECBTI a través de los programas de Ingeniería en Electrónica, Telecomunicaciones y Sistemas, ofertado por la universidad nacional abierta y a distancia UNAD, tiene el propósito de desarrollar en el estudiante habilidades y conocimientos para la solución de problemas en redes de telecomunicaciones, para ello se plantea un escenario el cual busca medir la capacidad de los estudiantes de implementación y configuración de los dispositivos que se encuentran en la red, mediante la implementación de comandos IOS en los equipos (switches y routers) en el software GNS3.

Paralelamente a la implementación y configuración del escenario propuesto, se realiza la descripción detallada de cada una de las etapas del desarrollo y se verifica el correcto funcionamiento de cada configuración mediante pruebas de conectividad como ping vrf y ping, con el fin de asegurar que haya conectividad en toda la red y los dispositivos estén funcionando correctamente.

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

ABSTRACT

The test of practical skills of the cisco CCNP deepening diploma, attached to the ECBTI through the programs of Engineering in Electronics, Telecommunications and Systems, offered by the national open and distance university UNAD, has the purpose of developing in the student skills and knowledge for the solution of problems in telecommunications networks, For this, a scenario is proposed which seeks to measure the capacity of the students to implement and configure the devices that are in the network, through the implementation of IOS commands in the equipment (switches and routers) in the GNS3 software.

Parallel to the implementation and configuration of the proposed scenario, the detailed description of each of the stages of development is made and the correct functioning of each configuration is verified through connectivity tests such as ping vrf and ping, in order to ensure that there is connectivity throughout the network and the devices are working correctly.

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

INTRODUCCIÓN

En el presente trabajo se presenta el desarrollo de la prueba de habilidades prácticas del diplomado de profundización cisco CCNP, la cual busca fortalecer en los estudiantes la comprensión, administración y configuración de dispositivos cisco en la industria, por medio de escenarios simulados en el software GNS3, implementando comandos IOS en los equipos (switches y routers), con ello se busca que los estudiantes diseñen e implementen soluciones a problemáticas reales en redes de telecomunicaciones, aparte de ello practicar y estudiar para posteriormente presentar el examen de certificación Cisco CCNA o CCNP y con ello mejorar su curriculum e ingresos, esto se traduciría en tener una mejor calidad de vida.

En la parte 1 y 2 del escenario propuesto, se construyó la red y se configuraron los ajustes básicos según la topología propuesta, también se configuro las rutas estáticas de manera manual en cada Router teniendo en cuenta la información de los Routers vecinos, además se implementó y configuro la tecnología VRF en los routers cisco, con el propósito de tener 2 tablas de enrutamiento exclusivas con el mismo segmento de red, para los clientes Special-Users y General-Users.

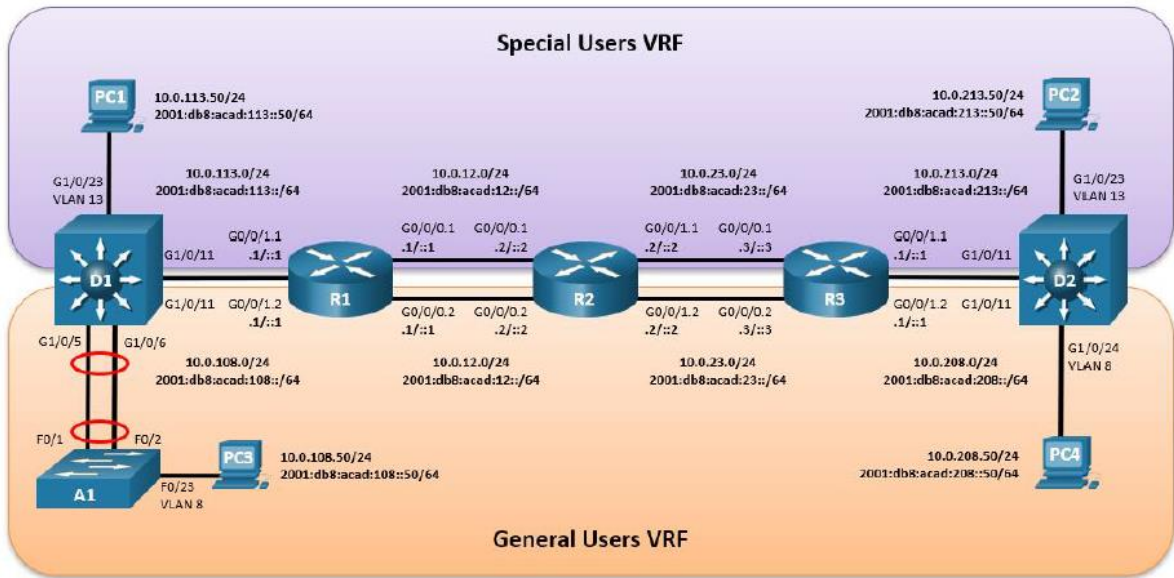
En la parte 3 y 4 del escenario propuesto, se configuro la capa 2 en los Switches, primeramente, se configuro los puertos troncales para el transporte del trafico hacia los routers vecinos, luego se implementó el protocolo PAgP en los Switch D1 y A1, para agrupar lógicamente varias interfaces físicas, esto con el fin de obtener redundancia y equilibrar el tráfico entre los puertos, por último se configuro los puertos de acceso para conectar los PCs y terminar con la conectividad total de la red.

Para finalizar se implementa seguridad en los equipos (R1, R2, R3, D1, D2 y A1), para ello se habilita la autenticación AAA de manera local y se restringe el acceso EXEC privilegiado por medio de la creación de un usuario y contraseña, con el fin de proteger los equipos ante piratas informáticos.

DESARROLLO

ESCENARIO

Figura 1. Escenario propuesto



Fuente: Guías UNAD CCNP

Tabla 1. Direccionamiento de topología de red propuesta

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0/0.1	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0/0.2	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G0/0/1.1	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G0/0/1.2	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0/0.1	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0/0.2	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G0/0/1.1	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G0/0/1.2	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0/0.1	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G0/0/0.2	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0/1.1	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0/1.2	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4

PC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Guías UNAD CCNP

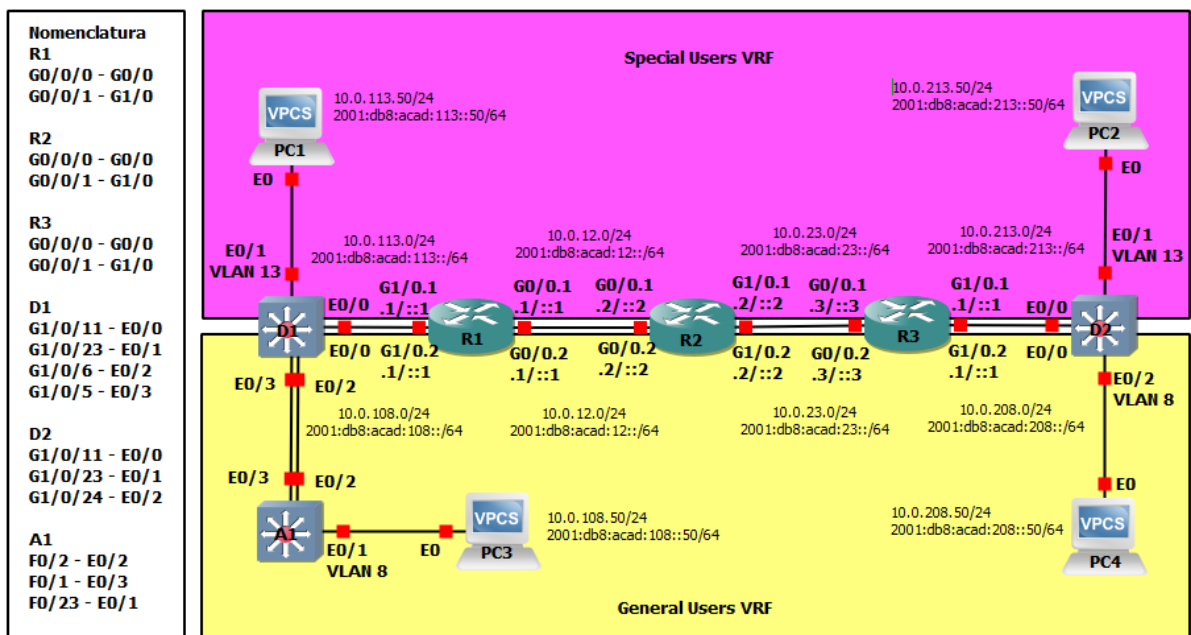
Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

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

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

Realizar la implementación de la red en el software GNS3, para ello se utilizó las siguientes referencias de equipos (Router Cisco C7200 y Swich i86bi-linux-l2-adventerprisek9-15.2d). además, se cableo la red y se cambio la nomenclatura de las interfaces de los equipos como se muestra en la figura 2.

Figura 2. Simulación de escenario



Fuente: Software GNS3 (Autoría propia)

Tabla 2. Tabla de direccionamiento se cambian interfaces

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	G0/0/0.1 - G0/0	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0/0.2 - G0/0	10.0.12.1/24	2001:db8:acad:12::1/64	fe80::1:2
	G0/0/1.1 - G1/0	10.0.113.1/24	2001:db8:acad:113::1/64	fe80::1:3
	G0/0/1.2 - G1/0	10.0.108.1/24	2001:db8:acad:108::1/64	fe80::1:4
R2	G0/0/0.1 - G0/0	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0/0.2 - G0/0	10.0.12.2/24	2001:db8:acad:12::2/64	fe80::2:2
	G0/0/1.1 - G1/0	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:3
	G0/0/1.2 - G1/0	10.0.23.2/24	2001:db8:acad:23::2/64	fe80::2:4
R3	G0/0/0.1 - G0/0	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:1
	G0/0/0.2 - G0/0	10.0.23.3/24	2001:db8:acad:23::3/64	fe80::3:2
	G0/0/1.1 - G1/0	10.0.213.1/24	2001:db8:acad:213::1/64	fe80::3:3
	G0/0/1.2 - G1/0	10.0.208.1/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	NIC	10.0.113.50/24	2001:db8:acad:113::50/64	EUI-64
PC2	NIC	10.0.213.50/24	2001:db8:acad:213::50/64	EUI-64
PC3	NIC	10.0.108.50/24	2001:db8:acad:108::50/64	EUI-64
PC4	NIC	10.0.208.50/24	2001:db8:acad:208::50/64	EUI-64

Fuente: Guías UNAD CCNP

Paso 2: Configure los ajustes básicos para cada dispositivo

a. Ingrese al modo de configuración global en cada uno de los dispositivos y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Realizar la configuración básica de cada dispositivo según indicaciones y documentar la función de cada comando aplicado a la configuración

Router R1

```
enable                ! cambia a modo privilegiado
configure terminal    ! ingreso a modo configuración
hostname R1          ! le asigno el nombre al router
ipv6 unicast-routing ! habilita el enrutamiento IPv6
no ip domain lookup  ! desactiva la búsqueda de DNS
banner motd # R1, ENCOR Skills Assessment, Scenario 2 # ! mensaje cuando
alguien accede por consola al router
line con 0           ! configuración de la línea de la consola y el cero es la
```

```
primera interfaz de consola
exec-timeout 0 0      ! no hay límite de tiempo para las sesiones
logging synchronous  ! evita los mensajes inesperados en la consola cuando
estamos escribiendo código
exit                  ! salida del modo de configuración
```

```
Router R2
enable
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
enable
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
enable                ! cambia a modo privilegiado
configure terminal    ! ingreso a modo configuración
hostname D1          ! le asigno el nombre al Switch
ip routing            ! utilizado para para habilitar IPV6
ipv6 unicast-routing  ! habilita el enrutamiento IPv6
no ip domain lookup   ! desactiva la búsqueda de DNS
banner motd # D1, ENCOR Skills Assessment, Scenario 2 # ! mensaje cuando
alguien accede por consola al router
line con 0            ! configuración de la línea de la consola y el cero es la
primera interfaz de consola
exec-timeout 0 0      ! no hay límite de tiempo para las sesiones
```

```
logging synchronous      ! evita los mensajes inesperados en la consola cuando
estamos escribiendo código
exit                    ! salida del modo de configuración
vlan 8                  ! crea una red virtual
name General-Users      ! entra a la configuración de la vlan y crea un nuevo
grupo llamado General-Users
exit                    ! salida del modo de configuración
vlan 13                 ! crea una red virtual
name Special-Users      ! entra a la configuración de la vlan y crea un nuevo
grupo llamado Special-Users
exit                    ! salida del modo de configuración
```

```
Switch D2
enable
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
```

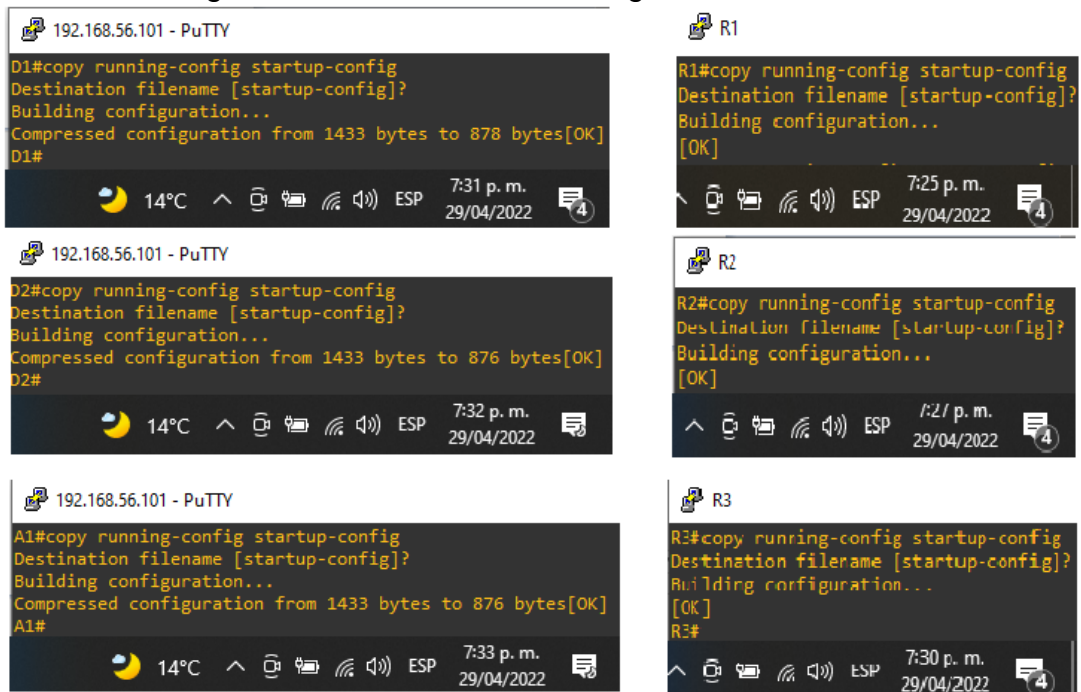
```
Switch A1
enable
configure terminal
hostname A1
ipv6 unicast-routing
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 2 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 8
name General-Users
```

exit

b. Guarde las configuraciones en cada uno de los dispositivos.

Aplicar el comando `copy running-config startup-config`, para copiar el archivo `running-configuration` de RAM en NVRAM y guardar como archivo `startup-configuration`, con el fin de que los dispositivos no pierdan las configuraciones cuando de reinician

Figura 3. Guardado de las configuraciones



Fuente: Software GNS3 (Autoría propia)

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

Realizar la configuración IPV4 e IPV6 en los PC de la red, según las indicaciones de la tabla de direccionamiento y guardar su configuración con el comando `save`

Figura 4. Configuración PC1, PC2, PC3 y PC4

The image displays four terminal windows from the GNS3 software, arranged in a 2x2 grid. Each window shows the configuration for a different PC (PC1, PC2, PC3, and PC4). The top-left window shows PC1's configuration, including IP address 10.0.113.1 and IPv6 address fe80::250:79ff:fe66:6801/64. The top-right window shows PC2's configuration, including IP address 10.0.213.1 and IPv6 address fe80::250:79ff:fe66:6803/64. The bottom-left window shows PC3's configuration, including IP address 10.0.108.1 and IPv6 address fe80::250:79ff:fe66:6800/64. The bottom-right window shows PC4's configuration, including IP address 10.0.208.1 and IPv6 address fe80::250:79ff:fe66:6802/64. Each window also displays the MAC address, LPORT, RHOST:PORT, and MTU for both IPv4 and IPv6.

Fuente: Software GNS3 (Autoría propia)

Parte 2: configurar VRF y enrutamiento estático

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

Sus tareas de configuración son las siguientes:

Tabla 3. configurar VRF y enrutamiento estático

Tarea#	Tarea	Especificación
2.1	En R1, R2 y R3, configure VRF-Lite VRF como se muestra en el diagrama de topología.	Configure dos VRF: <ul style="list-style-type: none"> • Usuarios generales • Usuarios especiales Los VRF deben admitir IPv4 e IPv6.
2.2	En R1, R2 y R3, configure las interfaces IPv4 e IPv6 en cada VRF como se detalla en la tabla de direccionamiento anterior.	Todos los enrutadores utilizarán Router-On-A-Stick en sus interfaces G0/0/1.x para admitir la separación de los VRF. Sub-interfaz 1: <ul style="list-style-type: none"> • En el VRF de Usuarios Especiales • Usar encapsulación dot1q 13 • IPv4 e IPv6 GUA y direcciones locales de enlace • Habilitar las interfaces Subinterfaz 2: <ul style="list-style-type: none"> • En el VRF de Usuarios Generales • Usar encapsulación dot1q 8 • IPv4 e IPv6 GUA y direcciones locales de enlace • Habilitar las interfaces
2.3	En R1 y R3, configure las rutas estáticas predeterminadas que apuntan a R2.	Configure rutas estáticas VRF para IPv4 e IPv6 en ambos VRF.
2.4	Verifique la conectividad en cada VRF.	Desde R1, verifique la conectividad a R3: <ul style="list-style-type: none"> • ping vrf Usuarios generales 10.0.208.1 • ping vrf Usuarios generales 2001:db8:acad:208::1 • ping vrf usuarios especiales 10.0.213.1 • ping vrf Usuarios especiales 2001:db8:acad:213::1

Fuente: Guías UNAD CCNP

Tarea 2.1

Realizar la configuración de las dos VRFs General-Users y Special-Users en los Routers R1,R2 y R3, además habilitar la familia IPV4 e IPV6

Para R1

configure terminal	! ingreso a modo configuración
ipv6 unicast-routing	! habilita el enrutamiento IPv6
vrf definition General-Users	! se crea la vrf y se asigna el nombre General-Users
address-family ipv4 este caso IPV4	! se le informa con que familia de IP trabajara en este caso IPV4
address-family ipv6 este caso IPV6	! se le informa con que familia de IP trabajara en este caso IPV6
exit	! salida del modo de configuración vrf

exit	! salida del modo de configuración vrf
vrf definition Special-Users	! se crea la vrf y se asigna el nombre Special-Users
address-family ipv4	! se le informa con que familia de IP trabajara en
este caso IPV4	
address-family ipv6	! se le informa con que familia de IP trabajara en
este caso IPV6	
exit	! salida del modo de configuración vrf
exit	! salida del modo de configuración vrf

Para R2

```

configure terminal
ipv6 unicast-routing
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
exit
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
exit

```

Para R3

```

configure terminal
ipv6 unicast-routing
vrf definition General-Users
address-family ipv4
address-family ipv6
exit
exit
vrf definition Special-Users
address-family ipv4
address-family ipv6
exit
exit

```

Tarea 2.2

Asignar las direcciones IPV4 e IPV6 según la tabla de direccionamiento a cada interfaz virtual en los tres Routers, además asignar las VRFs correspondientes y se encapsulan en su correspondiente ID, por último, habilitar los puertos de las subinterfaces.

Para R1

```
configure terminal          ! ingreso a modo configuración
interface GigabitEthernet0/0.1 ! selecciono la interfaz virtual
encapsulation dot1Q 13      ! se le aplica el ID 13 de Vlan a la sub interfaz
vrf forwarding Special-Users ! se le asigna la vrf Special-Users a la subinterfaz
para la tabla de enrutamiento
ip address 10.0.12.1 255.255.255.0 ! se le asigna la dirección IPV4 a la
subinterfaz
ipv6 address fe80::1:1 link-local ! se le asigna la dirección local IPV6 a la
subinterfaz y se utiliza para la comunicación con los vecinos
ipv6 address 2001:db8:acad:12::1/64 ! se le asigna la dirección IPV6 a la
subinterfaz
no shutdown                ! se habilita el puerto de la subinterfaz
exit                       ! salida del modo de configuración
interface GigabitEthernet0/0.2 ! selecciono la interfaz virtual
encapsulation dot1Q 8       ! se le aplica el ID 8 de Vlan a la sub interfaz
vrf forwarding General-Users ! se le asigna la vrf General-Users a la subinterfaz
para la tabla de enrutamiento
ip address 10.0.12.1 255.255.255.0 !se le asigna la dirección IPV4 a la subinterfaz
ipv6 address fe80::1:2 link-local ! se le asigna la dirección local IPV6 a la
subinterfaz y se utiliza para la comunicación con los vecinos
ipv6 address 2001:db8:acad:12::1/64 ! se le asigna la dirección IPV6 a la
subinterfaz
no shutdown                ! se habilita el puerto de la subinterfaz
interface GigabitEthernet1/0.1 ! selecciono la interfaz virtual
encapsulation dot1Q 13      ! se le aplica el ID 13 de Vlan a la sub interfaz
vrf forwarding Special-Users ! se le asigna la vrf Special-Users a la subinterfaz
para la tabla de enrutamiento
ip address 10.0.113.1 255.255.255.0 ! se le asigna la dirección IPV4 a la
subinterfaz
ipv6 address fe80::1:3 link-local ! se le asigna la dirección local IPV6 a la
subinterfaz y se utiliza para la comunicación con los vecinos
ipv6 address 2001:db8:acad:113::1/64 ! se le asigna la dirección IPV6 a la
subinterfaz
no shutdown                ! se habilita el puerto de la subinterfaz
exit                       ! salida del modo de configuración
interface GigabitEthernet1/0.2 ! selecciono la interfaz virtual
encapsulation dot1Q 8       ! se le aplica el ID 8 de Vlan a la sub interfaz
vrf forwarding General-Users ! se le asigna la vrf General-Users a la subinterfaz
para la tabla de enrutamiento
ip address 10.0.108.1 255.255.255.0 ! se le asigna la dirección IPV4 a la
subinterfaz
```

ipv6 address fe80::1:4 link-local ! se le asigna la dirección local IPV6 a la subinterfaz y se utiliza para la comunicación con los vecinos
ipv6 address 2001:db8:acad:108::1/64 ! se le asigna la dirección IPV6 a la subinterfaz
no shutdown ! se habilita el puerto de la subinterfaz

Para R2

```
interface GigabitEthernet0/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:acad:12::2/64
no shutdown
exit
interface GigabitEthernet0/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.12.2 255.255.255.0
ipv6 address fe80::2:2 link-local
ipv6 address 2001:db8:acad:12::2/64
no shutdown
exit
interface GigabitEthernet1/0.1
encapsulation dot1Q 13
vrf forwarding Special-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:acad:23::2/64
no shutdown
exit
interface GigabitEthernet1/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.2 255.255.255.0
ipv6 address fe80::2:4 link-local
ipv6 address 2001:db8:acad:23::2/64
no shutdown
exit
```

Para R3

```
interface GigabitEthernet0/0.1
encapsulation dot1Q 13
```

```

vrf forwarding Special-Users
ip address 10.0.23.3 255.255.255.0
ipv6 address fe80::3:1 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit
interface GigabitEthernet0/0.2
encapsulation dot1Q 8
vrf forwarding General-Users
ip address 10.0.23.3 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:acad:23::3/64
no shutdown
exit
interface GigabitEthernet1/0.1
encapsulation dot1Q 13
vrf forwarding 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
exit
interface GigabitEthernet1/0.2
encapsulation dot1Q 8
vrf forwarding 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

```

Tarea 2.3

Realizar la configuración de las rutas estáticas IPV4 e IPV6 en los Routers R1, R2 y R3 con base en la tabla de direccionamiento y según su topología, además verificar las tablas de enrutamiento para cada VRF en todos los routers

Para R1

Ruta de R1 a R2

```

configure terminal    ! ingreso a modo configuración
ip route vrf Special-Users 10.0.23.0 255.255.255.0 10.0.12.2    ! se configura la ruta
estática IPV4 desconocida para el envío de paquetes

```

```

ipv6 route vrf Special-Users 2001:db8:acad:23::/64 2001:db8:acad:12::2 ! se
configura la ruta estática IPV6 desconocida para el envío de paquetes
configure terminal ! ingreso a modo configuración
ip route vrf General-Users 10.0.23.0 255.255.255.0 10.0.12.2 ! se configura la ruta
estática IPV4 desconocida para el envío de paquetes
ipv6 route vrf General-Users 2001:db8:acad:23::/64 2001:db8:acad:12::2 ! se
configura la ruta estática IPV6 desconocida para el envío de paquetes

```

Ruta de R1 a R3

configure terminal

```
ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.12.2
```

```
ipv6 route vrf Special-Users 2001:db8:acad:213::0/64 2001:db8:acad:12::2
```

```
ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.12.2
```

```
ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:12::2
```

Figura 5. Configuración de rutas (General-Users)

```

R1#sho ip route vrf General-Users
Routing Table: General-Users
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 not set

 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, GigabitEthernet0/0.2
L    10.0.12.1/32 is directly connected, GigabitEthernet0/0.2
S    10.0.23.0/24 [1/0] via 10.0.12.2
C    10.0.108.0/24 is directly connected, GigabitEthernet1/0.2
L    10.0.108.1/32 is directly connected, GigabitEthernet1/0.2
S    10.0.208.0/24 [1/0] via 10.0.12.2
----

```

Fuente: Software GNS3 (Autoría propia)

Figura 6. Configuración de rutas (Special-Users)

```

R1#sho ip route vrf Special-Users
Routing Table: Special-Users
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 not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, GigabitEthernet0/0.1
L    10.0.12.1/32 is directly connected, GigabitEthernet0/0.1
S    10.0.23.0/24 [1/0] via 10.0.12.2
C    10.0.113.0/24 is directly connected, GigabitEthernet1/0.1
L    10.0.113.1/32 is directly connected, GigabitEthernet1/0.1
S    10.0.213.0/24 [1/0] via 10.0.12.2

```

Fuente: Software GNS3 (Autoría propia)

Para R2

Ruta de R2 a R1

configure terminal

ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.12.1

ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:12::1

ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.12.1

ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:12::1

Ruta de R2 a R3

configure terminal

ip route vrf Special-Users 10.0.213.0 255.255.255.0 10.0.23.3

ipv6 route vrf Special-Users 2001:db8:acad:213::/64 2001:db8:acad:23::3

ip route vrf General-Users 10.0.208.0 255.255.255.0 10.0.23.3

ipv6 route vrf General-Users 2001:db8:acad:208::/64 2001:db8:acad:23::3

Figura 7. Configuración de rutas (General-Users)

```

R2#sho ip route vrf General-Users

Routing Table: General-Users
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 not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, GigabitEthernet0/0.2
L    10.0.12.2/32 is directly connected, GigabitEthernet0/0.2
C    10.0.23.0/24 is directly connected, GigabitEthernet1/0.2
L    10.0.23.2/32 is directly connected, GigabitEthernet1/0.2
S    10.0.108.0/24 [1/0] via 10.0.12.1
S    10.0.208.0/24 [1/0] via 10.0.23.3

```

Fuente: Software GNS3 (Autoría propia)

Figura 8. Configuración de rutas (Special-Users)

```

R2#sho ip route vrf Special-Users

Routing Table: Special-Users
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 not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.0.12.0/24 is directly connected, GigabitEthernet0/0.1
L    10.0.12.2/32 is directly connected, GigabitEthernet0/0.1
C    10.0.23.0/24 is directly connected, GigabitEthernet1/0.1
L    10.0.23.2/32 is directly connected, GigabitEthernet1/0.1
S    10.0.113.0/24 [1/0] via 10.0.12.1
S    10.0.213.0/24 [1/0] via 10.0.23.3

```

Fuente: Software GNS3 (Autoría propia)

Para R3

Ruta de R3 a R2

configure terminal

ip route vrf Special-Users 10.0.12.0 255.255.255.0 10.0.23.2

ipv6 route vrf Special-Users 2001:db8:acad:12::/64 2001:db8:acad:23::2

configure terminal

ip route vrf General-Users 10.0.12.0 255.255.255.0 10.0.23.2

ipv6 route vrf General-Users 2001:db8:acad:12::/64 2001:db8:acad:23::2

Ruta de R3 a R1

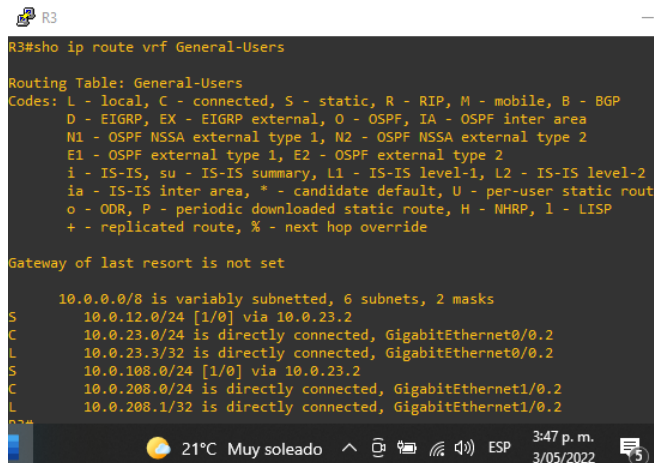
configure terminal

ip route vrf Special-Users 10.0.113.0 255.255.255.0 10.0.23.2

ipv6 route vrf Special-Users 2001:db8:acad:113::/64 2001:db8:acad:23::2

```
ip route vrf General-Users 10.0.108.0 255.255.255.0 10.0.23.2
ipv6 route vrf General-Users 2001:db8:acad:108::/64 2001:db8:acad:23::2
```

Figura 9. Configuración de rutas (General-Users)



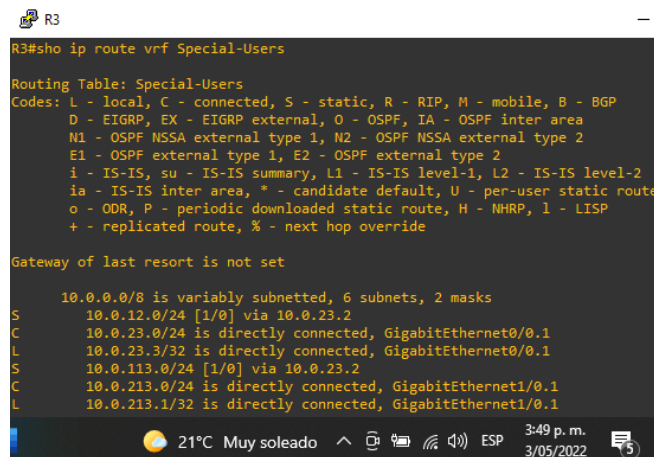
```
R3#sho ip route vrf General-Users
Routing Table: General-Users
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF 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 not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S       10.0.12.0/24 [1/0] via 10.0.23.2
C       10.0.23.0/24 is directly connected, GigabitEthernet0/0.2
L       10.0.23.3/32 is directly connected, GigabitEthernet0/0.2
S       10.0.108.0/24 [1/0] via 10.0.23.2
C       10.0.208.0/24 is directly connected, GigabitEthernet1/0.2
L       10.0.208.1/32 is directly connected, GigabitEthernet1/0.2
```

Fuente: Software GNS3 (Autoría propia)

Figura 10. Configuración de rutas (Special-Users)



```
R3#sho ip route vrf Special-Users
Routing Table: Special-Users
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 not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S       10.0.12.0/24 [1/0] via 10.0.23.2
C       10.0.23.0/24 is directly connected, GigabitEthernet0/0.1
L       10.0.23.3/32 is directly connected, GigabitEthernet0/0.1
S       10.0.113.0/24 [1/0] via 10.0.23.2
C       10.0.213.0/24 is directly connected, GigabitEthernet1/0.1
L       10.0.213.1/32 is directly connected, GigabitEthernet1/0.1
```

Fuente: Software GNS3 (Autoría propia)

Tarea 2.4

Realizar la verificación de conectividad IPV4 e IPV6 para los Routers R1, R2 y R3

Figura 11. PING DE R1 A R3 (Special-Users)

```
R1#
R1#ping vrf Special-Users 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 = 40/76/196 ms
R1#ping vrf Special-Users 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 = 36/46/56 ms
---
```

Fuente: Software GNS3 (Autoría propia)

Figura 12. PING DE R1 A R3 (General-Users)

```
R1#
R1#ping vrf General-Users 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 = 36/46/68 ms
R1#ping vrf General-Users 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 = 32/36/44 ms
---
```

Fuente: Software GNS3 (Autoría propia)

Figura 13. PING DE R3 A R1 (Special-Users)

```
R3#
R3#ping vrf Special-Users 10.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.113.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/91/200 ms
R3#ping vrf Special-Users 2001:db8:acad:113::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:113::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/47/64 ms
---
```

Fuente: Software GNS3 (Autoría propia)

Figura 14. PING DE R3 A R1 (General-Users)

```

R3#ping vrf General-Users 10.0.108.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.108.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/50/76 ms
R3#ping vrf General-Users 2001:db8:acad:108::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:108::1, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/40 ms
R3#

```

Fuente: Software GNS3 (Autoría propia)

Parte 3. Configurar Capa 2

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

Las tareas de configuración, son las siguientes:

Tabla 4. Configurar capa 2

Tarea#	Tarea	Especificación
3.1	En D1, D2 y A1, deshabilite todas las interfaces.	En D1 y D2, apague G1/0/1 a G1/0/24. En A1, apague F0/1 – F0/24, G0/1 – G0/2.
3.2	En D1 y D2, configure los enlaces troncales a R1 y R3.	Configure y habilite el enlace G1/0/11 como enlace troncal.
3.3	En D1 y A1, configure el EtherChannel.	En D1, configure y habilite: <ul style="list-style-type: none"> • Interfaz G1/0/5 y G1/0/6 • Port Channel 1 using PAgP En A1, configure habilitar: <ul style="list-style-type: none"> • Interfaz F0/1 y F0/2 • Port Channel 1 using PAgP

Tarea#	Tarea	Especificación
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	Configure y habilite los puertos de acceso de la siguiente manera: <ul style="list-style-type: none"> • En D1, configure la interfaz G1/0/23 como un puerto de acceso en la VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/23 como puerto de acceso en la VLAN 13 y habilite Portfast. • En D2, configure la interfaz G1/0/24 como un puerto de acceso en VLAN 8 y habilite Portfast. • En A1, configure la interfaz F0/23 como un puerto de acceso en la VLAN 8 y habilite Portfast.
3.5	Verifique la conectividad de PC a PC.	Desde la PC1, verifique la conectividad IPv4 e IPv6 a la PC2. Desde la PC3, verifique la conectividad IPv4 e IPv6 a la PC4.

Fuente: Guías UNAD CCNP

Tarea 3.1

Deshabilitar de todas las interfaces del Switch D1
configure terminal ! ingreso a modo configuración
interface range Et0/0-3, Et1/0-3, Et2/0-3, Et3/0-3 ! se seleccionan todas la interfaces del Switch
shutdown ! se realiza el apagado de todas las interfaces

Deshabilitar de todas las interfaces del Switch D2
configure terminal
interface range Et0/0-3, Et1/0-3, Et2/0-3, Et3/0-3
shutdown

Deshabilitar de todas las interfaces del Switch A1
configure terminal
interface range Et0/0-3, Et1/0-3, Et2/0-3, Et3/0-3
shutdown

Tarea 3.2

Para el Switch D1 configurar el enlace ethernet 0/0 como enlace troncal a R1
configure terminal ! ingreso a modo configuración
interface Et0/0 ! selecciona la interfaz
no shutdown ! habilito la interfaz

```
switchport trunk encapsulation dot1q ! se establece en la interfaz el modo de
encapsulación 802.1Q
switchport mode trunk ! pone a la interfaz en modo troncalizado,
para permitir el trafico de las Vlan de la red
switchport trunk allowed vlan 8,13 ! añade la Vlan 8 (General-Users) y la
Vlan 13 (Special-Users) al enlace troncal
```

```
Para el Switch D2 configurar el enlace ethernet 0/0 como enlace troncal a R3
configure terminal
interface Et0/0
no shutdown
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 8,13
```

Tarea 3.3

Para el switch D1 configurar el EtherChannel en la interfaz ethernet 0/2 y la interfaz ethernet 0/3

```
configure terminal ! ingreso a modo configuración
interface port-channel 1 ! configura un canal de puerto ethernet, para agrupar
lógicamente varias interfaces físicas
switchport ! configura el puerto a capa 2 (enlaces de datos)
switchport mode Access ! cambia el puerto a puerto de acceso, para que solo
permita el tráfico de la Vlan 8 (General-Users)
switchport access vlan 8 ! agrega la Vlan 8 (General-Users) al puerto de acceso
```

```
interface ethernet 0/2 ! selecciona la interfaz
switchport ! configura el puerto a capa 2 (enlaces de datos)
channel-group 1 mode desirable ! cambia el puerto a negociación automática que
usa PAgP
switchport mode Access ! cambia el puerto a puerto de acceso, para que solo
permita el tráfico de la Vlan 8 (General-Users)
switchport access vlan 8 ! agrega la Vlan 8 (General-Users) al puerto de acceso
no shutdown ! se habilita el puerto
```

```
interface ethernet 0/3
switchport
channel-group 1 mode desirable
switchport mode Access
switchport access vlan 8
no shutdown
```

Para el switch A1 configurar el EtherChannel en la interfaz ethernet 0/2 y la interfaz ethernet 0/3

```
configure terminal
interface port-channel 1
switchport
switchport mode Access
switchport access vlan 8

interface ethernet 0/2
switchport
channel-group 1 mode desirable
switchport mode Access
switchport access vlan 8
no shutdown

interface ethernet 0/3
switchport
channel-group 1 mode desirable
switchport mode Access
switchport access vlan 8
no shutdown
```

Tarea 3.4

Para el switch A1, configurar la interfaz ethernet 0/1 como un puerto de acceso en la VLAN 8

```
configure terminal      ! ingreso a modo configuración
interface ethernet 0/1  ! selecciona la interfaz
switchport mode Access ! cambia el puerto a puerto de acceso, para que solo
                        ! permita el tráfico de la Vlan 8 (General-Users)
switchport access vlan 8 ! agrega la Vlan 8 (General-Users) al puerto de acceso
no shutdown             ! se habilita el puerto
```

Para el switch D1, configurar la interfaz ethernet 0/1 como un puerto de acceso en la VLAN 13

```
configure terminal
interface ethernet 0/1
switchport mode access
switchport access vlan 13
no shutdown
```

Para el switch D2, configurar la interfaz ethernet 0/1 como un puerto de acceso en la VLAN 13

```
configure terminal
interface ethernet 0/1
switchport mode access
switchport access vlan 13
no shutdown
```

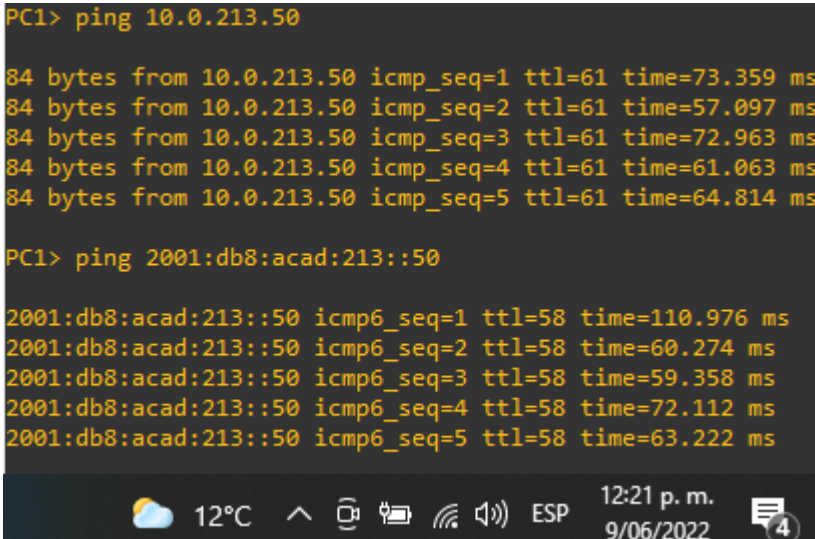
Para el switch D2, configurar la interfaz ethernet 0/2 como un puerto de acceso en la VLAN 8

```
configure terminal
interface ethernet 0/2
switchport mode access
switchport access vlan 8
no shutdown
```

Tarea 3.5

Desde la PC1, se verifica la conectividad IPv4 e IPv6 a la PC2

Figura 15. Conectividad PC1 a PC2



```
PC1> ping 10.0.213.50

84 bytes from 10.0.213.50 icmp_seq=1 ttl=61 time=73.359 ms
84 bytes from 10.0.213.50 icmp_seq=2 ttl=61 time=57.097 ms
84 bytes from 10.0.213.50 icmp_seq=3 ttl=61 time=72.963 ms
84 bytes from 10.0.213.50 icmp_seq=4 ttl=61 time=61.063 ms
84 bytes from 10.0.213.50 icmp_seq=5 ttl=61 time=64.814 ms

PC1> ping 2001:db8:acad:213::50

2001:db8:acad:213::50 icmp6_seq=1 ttl=58 time=110.976 ms
2001:db8:acad:213::50 icmp6_seq=2 ttl=58 time=60.274 ms
2001:db8:acad:213::50 icmp6_seq=3 ttl=58 time=59.358 ms
2001:db8:acad:213::50 icmp6_seq=4 ttl=58 time=72.112 ms
2001:db8:acad:213::50 icmp6_seq=5 ttl=58 time=63.222 ms
```

Fuente: Software GNS3 (Autoría propia)

Desde la PC3, se verifica la conectividad IPv4 e IPv6 a la PC4

Figura 16. Conectividad PC3 a PC4

```

PC3> ping 10.0.208.50

84 bytes from 10.0.208.50 icmp_seq=1 ttl=61 time=75.856 ms
84 bytes from 10.0.208.50 icmp_seq=2 ttl=61 time=64.115 ms
84 bytes from 10.0.208.50 icmp_seq=3 ttl=61 time=64.535 ms
84 bytes from 10.0.208.50 icmp_seq=4 ttl=61 time=73.896 ms
84 bytes from 10.0.208.50 icmp_seq=5 ttl=61 time=64.986 ms

PC3> ping 2001:db8:acad:208::50

2001:db8:acad:208::50 icmp6_seq=1 ttl=58 time=204.752 ms
2001:db8:acad:208::50 icmp6_seq=2 ttl=58 time=63.273 ms
2001:db8:acad:208::50 icmp6_seq=3 ttl=58 time=62.768 ms
2001:db8:acad:208::50 icmp6_seq=4 ttl=58 time=59.240 ms
2001:db8:acad:208::50 icmp6_seq=5 ttl=58 time=57.297 ms
    
```

Fuente: Software GNS3 (Autoría propia)

Parte 4. Configurar Seguridad

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

Las tareas de configuración son las siguientes:

Tabla 5. Configurar Seguridad

Tarea#	Tarea	Especificación
4.1	En todos los dispositivos, modo EXE privilegiado seguro.	Configure un secreto de habilitación de la siguiente manera: <ul style="list-style-type: none"> • Tipo de algoritmo: SCRYPT • Contraseña: cisco12345cisco.
4.2	En todos los dispositivos, cree una cuenta de usuario local.	Configurar un usuario local: <ul style="list-style-type: none"> • Nombre: admin • Nivel de privilegio: 15 • Tipo de algoritmo: SCRYPT • Contraseña: cisco12345cisco.
4.3	En todos los dispositivos, habilite AAA y habilite la autenticación AAA.	Habilite la autenticación AAA utilizando la base de datos local en todas las líneas.

Tarea 4.1

Aplicar cifrado a todas las contraseñas, para restringir el acceso al modo EXEC privilegiado en todos los equipos (R1, R2, R3, D1, D2 y A1)

```
configure terminal          ! ingreso a modo configuración
service password-encryption ! Aplica cifrado débil a las contraseñas
enable secret cisco12345cisco ! Restringe el acceso al modo EXEC privilegiado
```

Tarea 4.2

En todos los equipos (R1, R2, R3, D1, D2 y A1), crear una cuenta de usuario local

```
username admin secret 0 cisco12345cisco ! se crea el nombre de
usuario y la contraseña para la autenticación del usuario de forma local
username admin privilege 15 secret cisco12345cisco ! encripta la contraseña en
la configuración del equipo
```

Tarea 4.3

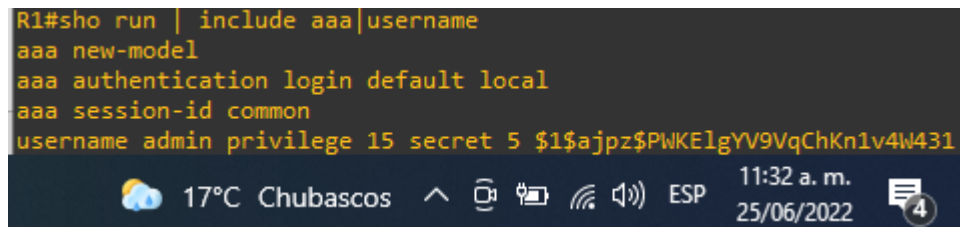
En todos los equipos (R1, R2, R3, D1, D2 y A1), habilitar la autenticación AAA de manera local

```
aaa new-model          ! habilitación de autenticación AAA
aaa authentication login default local ! autentica el login desde la base de datos
local del equipo
```

Verificar la seguridad en cada dispositivo

Figura 17. Autenticación AAA en R1

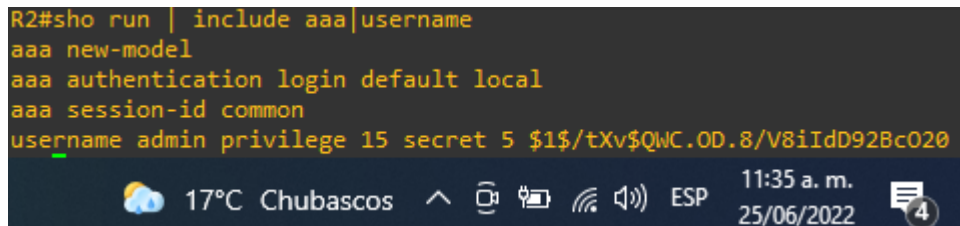
```
R1#sho run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$a!pz$PwKElgYV9VqChKn1v4W431
```



Fuente: Software GNS3 (Autoría propia)

Figura 18. Autenticación AAA en R2

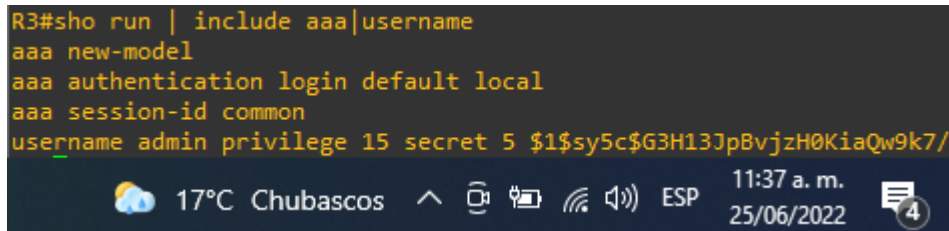
```
R2#sho run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$/tXv$QwC.Od.8/V8iIdD92Bc020
```



Fuente: Software GNS3 (Autoría propia)

Figura 19. Autenticación AAA en R3

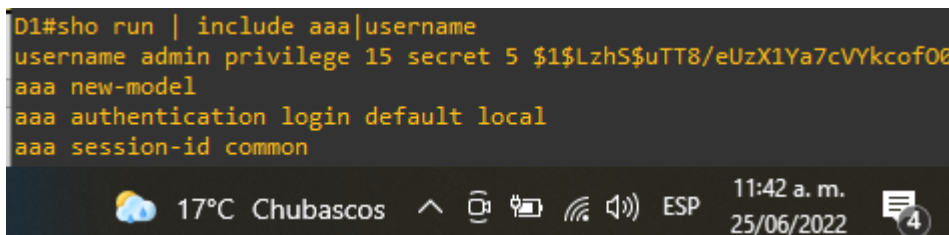
```
R3#sho run | include aaa|username
aaa new-model
aaa authentication login default local
aaa session-id common
username admin privilege 15 secret 5 $1$sy5c$G3H13JpBvjzH0KiaQw9k7/
```



Fuente: Software GNS3 (Autoría propia)

Figura 20. Autenticación AAA en D1

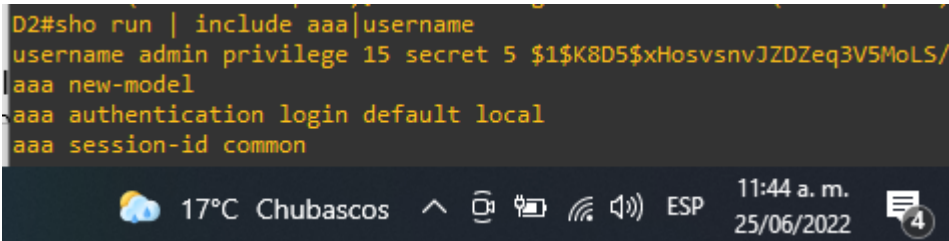
```
D1#sho run | include aaa|username
username admin privilege 15 secret 5 $1$LzhS$uTT8/eUzX1Ya7cVYkcof00
aaa new-model
aaa authentication login default local
aaa session-id common
```



Fuente: Software GNS3 (Autoría propia)

Figura 21. Autenticación AAA en D2

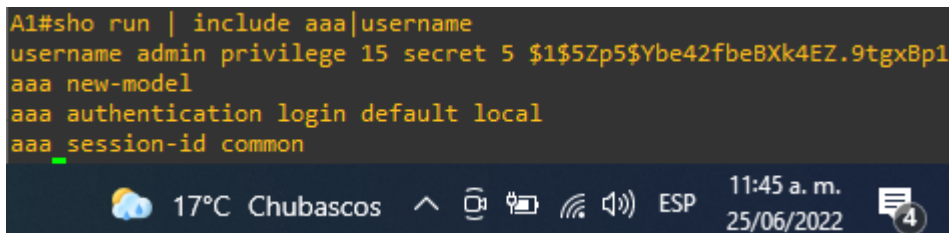
```
D2#sho run | include aaa|username
username admin privilege 15 secret 5 $1$K8D5$xHosvsnvJZDZeq3V5MoLS/
aaa new-model
aaa authentication login default local
aaa session-id common
```



Fuente: Software GNS3 (Autoría propia)

Figura 22. Autenticación AAA en A1

```
A1#sho run | include aaa|username
username admin privilege 15 secret 5 $1$5Zp5$Ybe42fbeBXk4EZ.9tgxBp1
aaa new-model
aaa authentication login default local
aaa session-id common
```



Fuente: Software GNS3 (Autoría propia)

CONCLUSIONES

El protocolo de enrutamiento estático ayuda a tener más control y seguridad en la red, ya que el administrador de la red puede decirle al router que rutas debe conocer y por donde enviar los paquetes, básicamente las rutas se configuran de manera manual en cada Router con la información de la red de los routers vecinos, cabe resaltar que este protocolo está diseñado para redes pequeñas que no sean escalables, ya que cualquier cambio que se realice en la topología se debe actualizar manualmente cada Router otra vez y esto lo que produce una carga administrativa mayor. Para redes grandes se recomienda utilizar el enrutamiento dinámico como (OSPF, RIP, EIGRP, entre otros).

Al implementar vrf podemos tener enrutadores virtuales dentro de un mismo router físico, es decir podemos aislar el tráfico para los clientes Special-Users y General-Users en dos tablas de enrutamiento exclusivas con el mismo segmento de red, pero aisladas una de la otra, cada vrf es independiente y toma sus propias decisiones dentro del Router sin afectar a las demás.

Es importante realizar pruebas de conectividad como (ping, ping vrf, entre otros), durante el desarrollo del escenario propuesto, esto con el fin de verificar que los dispositivos estén funcionando correctamente y allí comunicación entre ellos, además podemos observar dentro de cada dispositivo las configuraciones realizadas, esto ayuda a que el administrador de la red, pueda solucionar inconvenientes en caso de fallos o problemas de la red de manera inmediata.

Se adquirió habilidades para la configuración de dispositivos Cisco, enfocadas a solucionar problemas y optimizar el rendimiento de las redes WAN, con el uso de la tecnología vrf incluida en los routers Cisco.

BIBLIOGRAFÍA

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). 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>

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