DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOJAN DANIEL PRADO FULA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE TELECOMUNICACIONES*
BOGOTÁ
2023

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOJAN DANIEL PRADO FULA

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

DIRECTOR:

JOHN HAROLD PÉREZ CALDERÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE TELECOMUNICACIONES*
BOGOTÁ
2023

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del jurado

Firma del jurado

Bogotá,10 de mayo de 2023

AGRADECIMIENTOS

Expreso el más sincero y profundo agradecimiento a Dios que me condescendió llegar hasta esta etapa de la vida otorgándome la sabiduría en esta trayectoria como ingeniero.

A mis padres por brindarme apoyo emocional e incondicional para llegar a superar los retos de mi vida cotidiana, profesional y educativa.

A la Universidad Nacional Abierta y a Distancia que me permitió ser parte de la comunidad Unadista para formarme como ingeniero y realizar diplomado de profundización cisco.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLA

Pág.

GLOSARIO

CCNP: Cisco Certified Network Professional.

HOST: dispositivo electrónico que permite la conexión a una red.

IPV4: protocolo de internet versión 4, que es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema.

IPV6: protocolo de internet que es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones, tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits.

LAN: grupo de dispositivos o equipos en un mismo espacio geográfico que permiten el intercambio de información entre ellos de forma local.

OSPF: Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado.

PING: emplea él envió de paquetes ICMP de solicitud y respuesta para la validación de comunicación entre equipos.

WAN: es una topología de red que grupa e interconecta diferentes redes en un área geográfico no tan extensa.

RESUMEN

El diplomado en Cisco CCNP (Cisco Certified Network Professional) es un programa de formación avanzada en redes de computadoras y tecnologías de la información. Este diplomado está dirigido a profesionales de TI que deseen mejorar sus habilidades en la configuración, implementación y mantenimiento de redes empresariales.

El diplomado CCNP se divide en tres cursos principales: Implementing Cisco IP Routing (ROUTE), Implementing Cisco IP Switched Networks (SWITCH) y Troubleshooting and Maintaining Cisco IP Networks (TSHOOT). Se enfoca en áreas específicas de la red, como la configuración de enrutadores, switches y protocolos de enrutamiento avanzados, la implementación de tecnologías de switching de capa 2 y 3, y la solución de problemas en redes complejas.

El diplomado CCNP también incluye temas avanzados como la seguridad de la red, la virtualización, la automatización de la red y la gestión de la red.

Palabras Clave: Cisco, Ccnp, Conmutación, Enrutamiento, Redes, Telecomunicaciones

ABSTRACT

The Cisco CCNP (Cisco Certified Network Professional) Diploma is an advanced training program in computer networks and information technology. This diploma is for IT professionals who want to improve their skills in configuring, deploying, and maintaining enterprise networks.

The CCNP diploma is divided into three main courses: Implementing Cisco IP Routing (ROUTE), Implementing Cisco IP Switched Networks (SWITCH), and Troubleshooting and Maintaining Cisco IP Networks (TSHOOT). It focuses on specific areas of the network, such as configuring routers, switches, and advanced routing protocols, implementing Layer 2 and 3 switching technologies, and troubleshooting complex networks.

The CCNP diploma also includes advanced topics such as network security, virtualization, network automation, and network management.

Keywords: Cisco, Ccnp, Switching, Routing, Networks, Telecommunications

INTRODUCCIÓN

El trabajo en un diplomado en Cisco CCNP es un campo emocionante y en constante evolución en el mundo de las redes y tecnologías de la información. El objetivo principal de este programa de formación avanzada es capacitar a los estudiantes para que adquieran conocimientos y habilidades especializados en la configuración, implementación y mantenimiento de redes empresariales.

Hay que realizar diferentes configuraciones en dispositivos de red y aplicar protocolos avanzados de enrutamiento, hasta proporcionar soporte técnico a los usuarios de la red. Los trabajos en este campo requieren una sólida comprensión de los conceptos y principios fundamentales de las redes de computadoras y la capacidad de aplicarlos en situaciones reales.

Es necesario estar actualizado con las últimas tecnologías y tendencias del mercado para poder brindar una educación de calidad a los estudiantes y ayudarles a desarrollar habilidades técnicas y conocimientos avanzados en el campo de las redes. Además, se requiere una actitud colaborativa y un enfoque de aprendizaje continuo para asegurar el éxito en este campo en constante evolución.

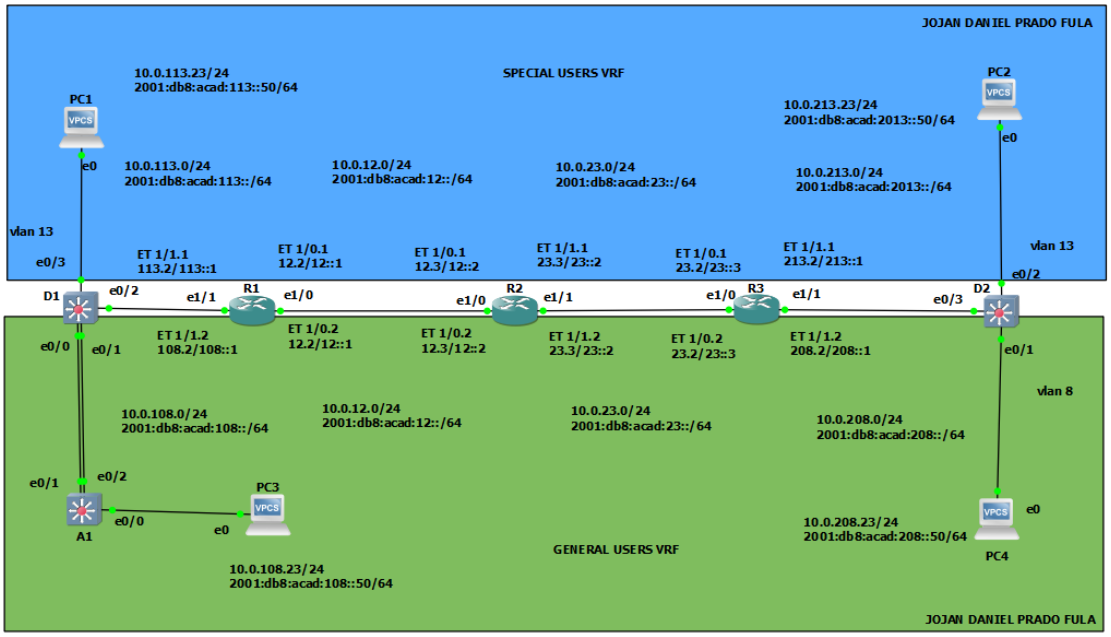
ESCENARIO 1

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ

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.

Figura 1. Topología de Red



Fuente: propia

Tabla 1. Direccionamiento IP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	E1/0.1	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:1
	E1/0.2	10.0.12.2/24	2001:db8:acad:12::1/64	fe80::1:2
	E1/1.1	10.0.113.2/24	2001:db8:acad:113::1/64	fe80::1:3
	E1/1.2	10.0.108.2/24	2001:db8:acad:108::1/64	fe80::1:4
R2	E1/0.1	10.0.12.3/24	2001:db8:acad:12::2/64	fe80::2:1
	E1/0.2	10.0.12.3/24	2001:db8:acad:12::2/64	fe80::2:2
	E1/1.1	10.0.23.3/24	2001:db8:acad:23::2/64	fe80::2:3
	E1/1.2	10.0.23.3/24	2001:db8:acad:23::2/64	fe80::2:4
R3	E1/0.1	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:1
	E1/0.2	10.0.23.2/24	2001:db8:acad:23::3/64	fe80::3:2
	E1/1.1	10.0.213.2/24	2001:db8:acad:213::1/64	fe80::3:3
	E1/1.2	10.0.208.2/24	2001:db8:acad:208::1/64	fe80::3:4
PC1	Nada	10.0.113.23/24	2001:db8:acad:113::50/64	EUI-64
PC2	Nada	10.0.213.23/24	2001:db8:acad:213::50/64	EUI-64
PC3	Nada	10.0.108.23/24	2001:db8:acad:108::50/64	EUI-64
PC4	Nada	10.0.208.23/24	2001:db8:acad:208::50/64	EUI-64

Fuente: propia

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.

ROUTER R1

```
Enable                                  // modo privilegiado
configure terminal                      // modo de configuración
hostname R1                             // nombre del equipo
ipv6 unicast-routing                    // habilita el routing IPv6.
no ip domain lookup                     // Habilita la traducción de nombre a dirección basado en DNS del host
banner motd # R1, ENCOR SKills Assessment, Scenario 2 #     // mensaje emergente
line console 0                          // configuración de la consola.
exec-time 0 0                           // establece el tiempo de espera inactivo de la sesión remota
logging synchronous.                    // Sincroniza los mensajes no solicitados
Exit                                    // cierra la sesión del usuario actual
```

ROUTER R2

```
Enable                                  // modo privilegiado
configure terminal                      // modo de configuración
hostname R2                             // nombre del equipo
ipv6 unicast-routing                    // habilita el routing IPv6 en el router.
no ip domain lookup                     // Habilita la traducción de nombre a dirección basado en DNS del host
banner motd # R2, ENCOR SKills Assessment, Scenario 2 #     //mensaje emergente hay iniciar el dispositivo
line console 0                          // configuración de la consola.
exec-time 0 0                           // establece el tiempo de espera inactivo de la sesión remota
logging synchronous.                    // Sincroniza los mensajes no solicitados
Exit                                    // cierra la sesión del usuario actual
```

ROUTER R3

```
Enable                                  // modo privilegiado
configure terminal                      // modo de configuración
hostname R3                             // nombre del equipo
ipv6 unicast-routing                    // habilita el routing IPv6 en el router.
no ip domain lookup                     // Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # R3, ENCOR SKills Assessment, Scenario 2 #     //mensaje emergente
hay iniciar el dispositivo
line console 0                          // Entra en la configuración de la consola.
exec-time 0 0                           // establece el tiempo de espera inactivo
de la sesión remota
logging synchronous.                    // Sincroniza los mensajes no solicitados
Exit                                    // cierra la sesión del usuario actual
```

SWITCH D1

```
Enable                                  // modo privilegiado
configure terminal                      // modo de configuración
hostname D1                             // nombre del equipo
ip routing                              // gestiona rutas estáticas
ipv6 unicast-routing                    // habilita el routing IPv6 en el router
no ip domain lookup                     //Habilita la traducción de nombre a dirección
basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 #     //mensaje emergente
hay iniciar el dispositivo
line con 0                              // configuración de la consola.
exec-timeout 0 0                        // establece el tiempo de espera inactivo
logging synchronous                     // Sincroniza los mensajes no solicitados
exit                                    // cierra la sesión del usuario actual
vlan 8                                  //se nombre y crea una vlan
name general-users                      // se asigna nombre a la vlan
exit                                    // cierra la sesión del usuario actual
vlan 13                                 //se nombre y crea una vlan
name special-users                      // se asigna nombre a la vlan
exit                                    // cierra la sesión del usuario actual
```

SWITCH D2

Enable // modo privilegiado
configure terminal // modo de configuración
hostname D2 // nombre del equipo
ip routing // gestiona rutas estáticas en la tabla de direccionamiento
ipv6 unicast-routing // habilita el routing IPv6 en el router
no ip domain lookup //Habilita la traducción de nombre a dirección basado en DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 2# //mensaje emergente hay iniciar el dispositivo
line con 0 // configuración de la consola.
exec-timeout 0 0 // establece el tiempo de espera inactivo
logging synchronous // Sincroniza los mensajes no solicitados y el resultado de la depuración
exit // cierra la sesión del usuario actual
vlan 8 //se nombre y crea una vlan
name general-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
vlan 13 //se nombre y crea una vlan
name special-users // se asigna nombre a la vlan

SWITCH A1

Enable // modo privilegiado
configure terminal // modo de configuración
hostname D1 // nombre del equipo
ip routing // gestiona rutas estáticas en la tabla de direccionamiento
ipv6 unicast-routing // habilita el routing IPv6 en el router
no ip domain lookup //Habilita la traducción de nombre a dirección basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 2 # //mensaje emergente hay iniciar el dispositivo
line con 0 // configuración de la consola.
exec-timeout 0 0 // establece el tiempo de espera inactivo
logging synchronous // Sincroniza los mensajes no solicitados
exit // cierra la sesión del usuario actual
vlan 8 //se nombre y crea una vlan
name general-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual
vlan 13 //se nombre y crea una vlan
name special-users // se asigna nombre a la vlan
exit // cierra la sesión del usuario actual

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

ROUTER R1
Copy running-config startup-config // Guarda la configuración

ROUTER R2
Copy running-config startup-config // Guarda la configuración

ROUTER R3
Copy running-config startup-config // Guarda la configuración

SWITCH D1
Copy running-config startup-config // Guarda la configuración

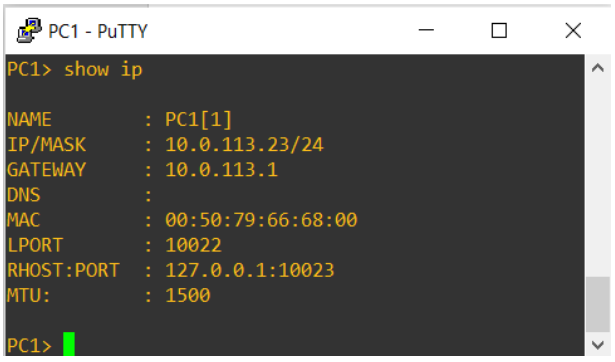
SWITCH D2
Copy running-config startup-config // Guarda la configuración

SWITCH A1
Copy running-config startup-config // Guarda la configuración

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

COMPUTADOR PC1
Ip 10.0.113.23/24 10.0.113.1 // dirección IPV4
Ip 2001:db8:acad:113::50/64 // dirección IPV6
save

Figura 2. Establecimiento de la dirección IP en PC1

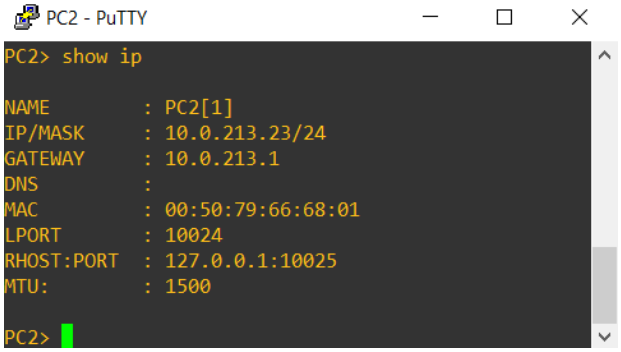


Fuente: propia

COMPUTADOR PC2

Ip 10.0.213.23/24 10.0.213.1 // dirección IPV4
Ip 2001:db8:acad:213::50/64 // dirección IPV6
save

Figura 3. Establecimiento de la dirección IP en PC2

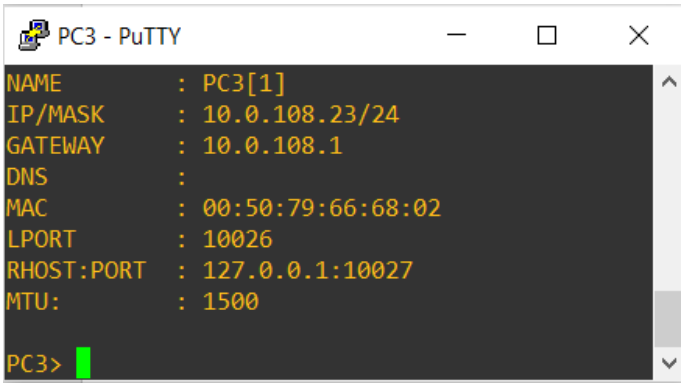


Fuente: propia

COMPUTADOR PC3

IP 10.0.108.23/24 10.0.108.1 // dirección IPV4
IP 2001:db8:acad:108::50/64 // dirección IPV6
Sabe

Figura 4. Establecimiento de la dirección IP en PC3

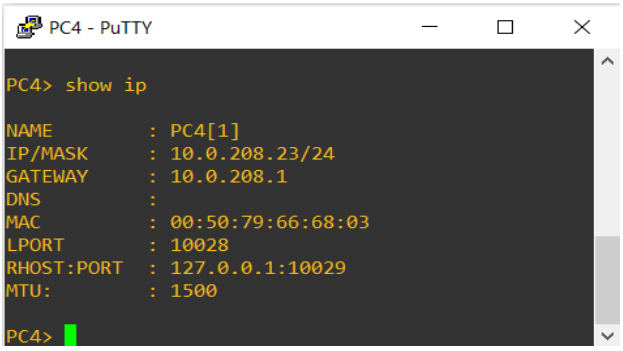


Fuente: propia

COMPUTADOR PC4

IP 10.0.208.23/24 10.0.208.1 // dirección IPV4
IP 2001:db8:acad:208::50/64 // dirección IPV6
save

Figura 5. Establecimiento de la dirección IP en PC4



Fuente: propia

PARTE 2: CONFIGURAR VRF Y ENRUTAMIENTO ESTÁTICO

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

Sus tareas de configuración son las siguientes:

Tabla 2. Configuracion 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: • Usuarios generales • Usuarios especiales Los VRF deben soportar 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 e1/1.x para admitir la separación de los VRF. Sub-interfaz 1: • En el VRF de Usuarios Especiales • Encapsulación Use dot1q • IPv4 e IPv6 GUA y direcciones locales de enlace • Habilitar las interfaces Subinterfaz 2: • En el VRF de Usuarios Generales • Encapsulación Usedot1q

Tarea	Tarea	Especificación
		• 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: • ping vrf Usuarios generales 10.0.208.Z • ping vrf Usuarios generales 2001:db8:acad:208::1 • ping vrf Usuarios especiales 10.0.213.Z • ping vrf Usuarios especiales 2001:db8:acad:213::1

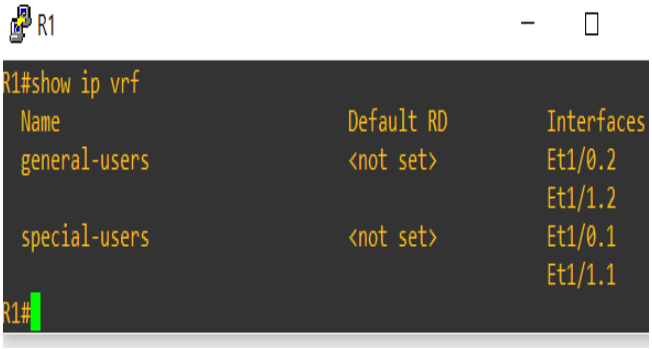
Fuente: propia

2.1 EN R1, R2 Y R3, CONFIGURE VRF-LITE VRF COMO SE MUESTRA EN EL DIAGRAMA DE TOPOLOGÍA.

ROUTER R1

```
vrf definition general-users                 // crea una vrf
description general-users                    // describe la vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión
vrf definition special-users                 // crea una vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión
do show vrf                                  // muestra las vrf creadas
```

Figura 6. Comprobación VRF en Router R1

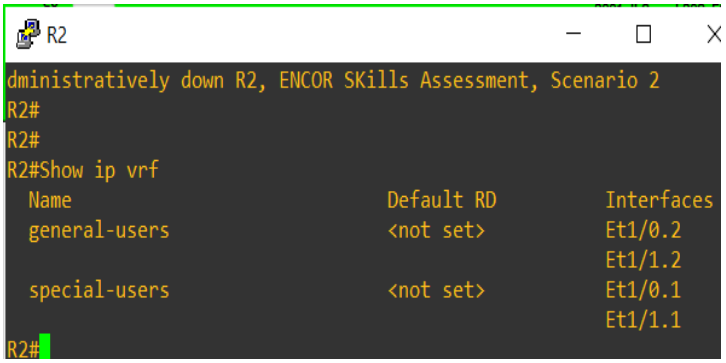


Fuente: propia

ROUTER R2

```
vrf definition general-users                 // crea una vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión del usuario
vrf definition special-users                 // crea una vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión
do show vrf                                  // muestra las vrf creadas
```

Figura 7. Comprobación VRF en Router R2



Fuente: propia

ROUTER R3

```
vrf definition general-users                 // crea una vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión
vrf definition special-users                 // crea una vrf
address-family ipv4                          // habilitar vrf con ipv4
address-family ipv6                          // habilitar vrf con ipv6
exit                                         // cierra la sesión
do show vrf                                  // muestra las vrf creadas
```

Figura 8. Comprobación VRF en Router R3

Fuente: propia

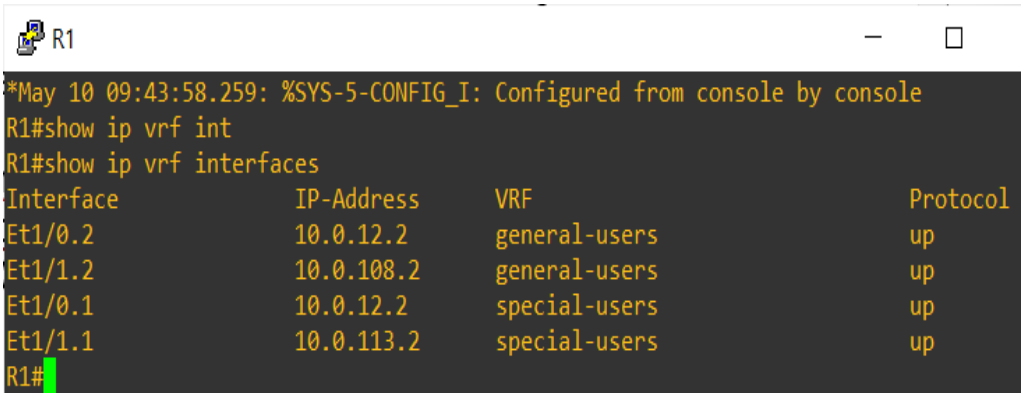
2.2 EN R1, R2 Y R3, CONFIGURE LAS INTERFACES IPV4 E IPV6 EN CADA VRF COMO SE DETALLA EN LA TABLA DE DIRECCIONAMIENTO ANTERIOR.

ROUTER R1

```
interface ethernet 1/0                    // ingresa a la interfaz
no shutdown                               // enciende la interfaz
interface ethernet 1/0.1                  // ingresa a la subinterfaz
no shutdown                               // enciende la interfaz
encapsulation dot1Q 13                    // encapsula los mensajes
vrf forwarding special-users              // reenvía a la VRF special-users
ip address 10.0.12.2 255.255.255.0        // asigna dirección IPV4
ipv6 address 2001:db8:acad:12::1/64       // asigna dirección IPV6
ipv6 address fe80::1:1 link-local         // asigna dirección IPV6
exit                                      // cierra la sesión
interface Ethernet 1/0.2                  // ingresa a la interfaz
no shutdown                               // enciende la interfaz
encapsulation dot1Q 8                     // encapsula los mensajes
vrf forwarding general-users              // reenvía a la VRF general-users
Ip address 10.0.12.2 255.255.255.0        // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::1/64       // asigna dirección IPV6
Ipv6 address fe80::1:2 link-local         // asigna dirección IPV6
Exit                                      // cierra la sesión
interface Ethernet 1/1                    // ingresa a la interfaz
no shutdown                               // enciende la interfaz
interface Ethernet 1/1.1                  // ingresa a la subinterfaz
no shutdown                               // enciende la interfaz
encapsulation dot1Q 13                    //  encapsula los mensajes
vrf forwarding special-users              // reenvía a la VRF general-users
Ip address 10.0.113.2 255.255.255.0       // asigna dirección IPV4
Ipv6 address 2001:db8:acad:113::1/64      // asigna dirección IPV6
```

```
Ipv6 address fe80::1:3 link-local          // asigna dirección IPV6
Exit                                       // cierra la sesión
interface Ethernet 1/1.2                   // ingresa a la interfaz
no shutdown                                // enciende la interfaz
Encapsulation dot1q 8                      //  encapsula los mensajes
Vrf forwarding general-users               // reenvía a la VRF general-users
Ip address 10.0.108.2 255.255.255.0        // asigna dirección IPV4
Ipv6 address 2001:db8:acad:108::1/64       // asigna dirección IPV6
Ipv6 address fe80::1:4 link-local          // asigna dirección IPV6
Exit                                       // cierra la sesión
show ip vrf int                            //muestra las vrf activas
```

Figura 9. Comprobación ip en interfaces en Router R1



Fuente: propia

ROUTER R2

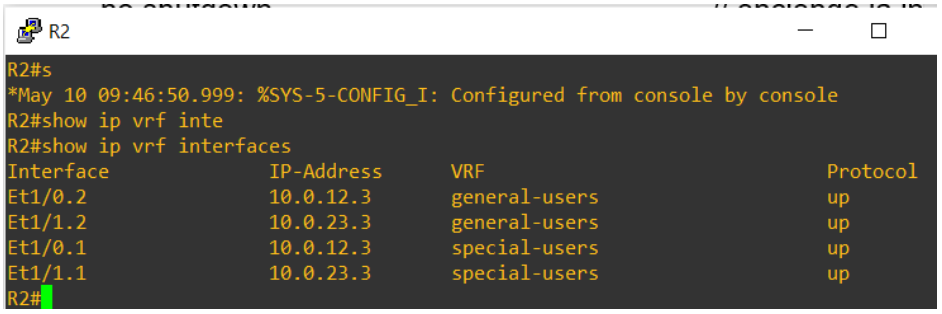
```
interface ethernet 1/0                     // ingresa a la interfaz
no shutdown                                // enciende la interfaz
interface ethernet 1/0.1                   // ingresa a la subinterfaz
no shutdown                                // enciende la interfaz
encapsulation dot1Q 13                     // encapsula los mensajes
vrf forwarding special-users               // reenvía a la VRF general-users
Ip address 10.0.12.3 255.255.255.0         // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::2/64        // asigna dirección IPV6
Ipv6 address fe80::2:1 link-local          // asigna dirección IPV6
Exit                                       // cierra la sesión

interface Ethernet1/0.2                    // ingresa a la interfaz
no shutdown                                // enciende la interfaz
encapsulation dot1Q 8                      // encapsula los mensajes
vrf forwarding general-users               // reenvía a la VRF general-users
Ip address 10.0.12.3 255.255.255.0         // asigna dirección IPV4
Ipv6 address 2001:db8:acad:12::2/64        // asigna dirección IPV6
```

```
Ipv6 address fe80::2:2 link-local                // asigna dirección IPV6
Exit

interface ethernet 1/1                           // ingresa a la interfaz
no shutdown                                      // enciende la interfaz
interface Ethernet1/1.1                          // ingresa a la subinterfaz
no shutdown                                      // enciende la interfaz
encapsulation dot1Q 13                           // encapsula los mensajes
vrf forwarding special-users                     // reenvía a la VRF general-users
Ip address 10.0.23.3 255.255.255.0               // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::2/64              // asigna dirección IPV6
Ipv6 address fe80::2:3 link-local                // asigna dirección IPV6
Exit                                             // cierra la sesión
interface Ethernet1/1.2                          // ingresa a la interfaz
no shutdown                                      // enciende la interfaz
encapsulation dot1Q 8                            //  encapsula los mensajes
vrf forwarding general-users                     // reenvía a la VRF general-users
Ip address 10.0.23.3 255.255.255.0               // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::2/64              // asigna dirección IPV6
Ipv6 address fe80::2:4 link-local                // asigna dirección IPV6
Exit                                             // cierra la sesión
show ip vrf int                                  // muestra las vrf activas
```

Figura 10. Comprobación ip en interfaces en Router R2



Fuente: propia

ROUTER R3

```
interface ethernet 1/0                           // ingresa a la interfaz
no shutdown                                      // enciende la interfaz
interface ethernet 1/0.1                         // ingresa a la subinterfaz
no shutdown                                      // enciende la interfaz
encapsulation dot1Q 13                           // encapsula los mensajes
vrf forwarding special-users                     // reenvía a la VRF general-users
Ip address 10.0.23.2 255.255.255.0               // asigna dirección IPV4
```

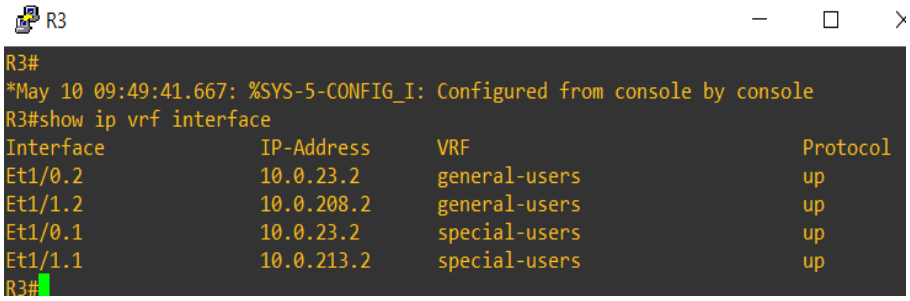
```
Ipv6 address 2001:db8:acad:23::3/64          // asigna dirección IPV6
Ipv6 address fe80::3:1 link-local            // asigna dirección IPV6
Exit                                         // cierra la sesión

interface Ethernet1/0.2                      // ingresa a la subinterfaz
no shutdown                                  // enciende la interfaz
encapsulation dot1Q 8                        // encapsula los mensajes
vrf forwarding general-users                 // reenvía a la VRF general-users
Ip address 10.0.23.2 255.255.255.0           // asigna dirección IPV4
Ipv6 address 2001:db8:acad:23::3/64          // asigna dirección IPV6
Ipv6 address fe80::3:2 link-local            // asigna dirección IPV6
Exit                                         // cierra la sesión

interface Ethernet1/1                        // ingresa a la interfaz
no shutdown                                  // enciende la interfaz
interface Ethernet1/1.1                      // ingresa a la subinterfaz
no shutdown                                  // enciende la interfaz
encapsulation dot1Q 13                       // encapsula los mensajes
vrf forwarding special-users                 // reenvía a la VRF general-users
Ip address 10.0.213.2 255.255.255.0          // asigna dirección IPV4
Ipv6 address 2001:db8:acad:213::1/64         // asigna dirección IPV6
Ipv6 address fe80::3:3 link-local            // asigna dirección IPV6
Exit                                         // cierra la sesión

interface Ethernet1/1.2                      // ingresa a la subinterfaz
no shutdown                                  // enciende la interfaz
encapsulation dot1Q 8                        // encapsula los mensajes
vrf forwarding general-users                 // reenvía a la VRF general
Ip address 10.0.208.2 255.255.255.0          // asigna dirección IPV4
Ipv6 address 2001:db8:acad:208::1/64         // asigna dirección IPV6
Ipv6 address fe80::3:4 link-local            // asigna dirección IPV6
End                                          // cierra la sesión
show ip vrf int                              // muestra las vrf activas
```

Figura 11. Verificación ip en interfaces en Router R3



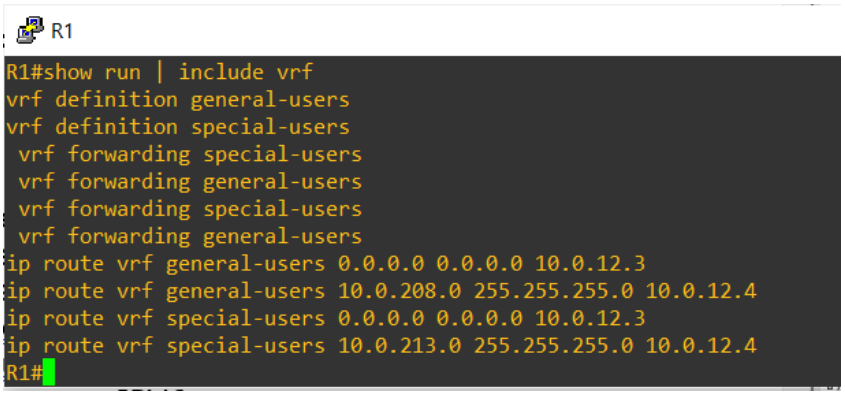
Fuente: propia

2.3 EN R1 Y R3, CONFIGURE LAS RUTAS ESTÁTICAS PREDETERMINADAS QUE APUNTAN A R2.

ROUTER R1

ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.12.3 // ruta estatica es special-users en IPV4
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.12.3 // ruta estatica es general-users en IPV4
ipv6 route vrf special-users ::/0 2001:db8:acad:12::2 // ruta estatica es general-users en IPV6
ipv6 route vrf general-users ::/0 2001:db8:acad:12::2 // ruta estatica es general-users en IPV6

Figura 12. Comprobación ip en interface R1

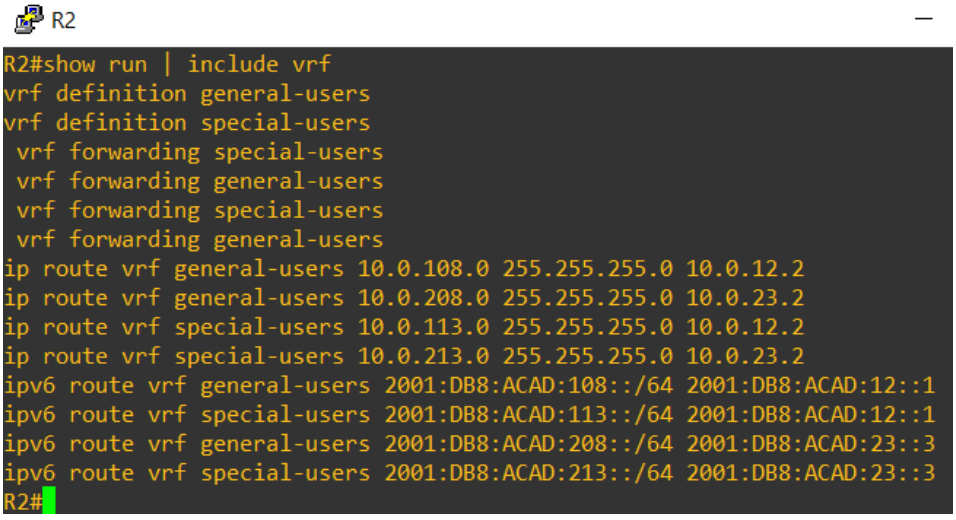


Fuente: propia

ROUTER R2

ip route vrf special-users 10.0.113.0 255.255.255.0 10.0.12.2 // ruta estatica es special-users en IPV4
ip route vrf special-users 10.0.213.0 255.255.255.0 10.0.23.2 // ruta estatica es special-users en IPV4
ip route vrf general-users 10.0.108.0 255.255.255.0 10.0.12.2 // ruta estatica es general-users en IPV4
ip route vrf general-users 10.0.208.0 255.255.255.0 10.0.23.2 // ruta estatica es general-users en IPV4
ipv6 route vrf special-users 2001:DB8:ACAD:113::/64 2001:DB8:ACAD:12::1 // ruta estatica es special-users en IPV6
ipv6 route vrf special-users 2001:DB8:ACAD:213::/64 2001:DB8:ACAD:23::3 // ruta estatica es special-users en IPV6
ipv6 route vrf general-users 2001:DB8:ACAD:108::/64 2001:DB8:ACAD:12::1 // ruta estatica es general-users en IPV6
ipv6 route vrf general-users 2001:DB8:ACAD:208::/64 2001:DB8:ACAD:23::3 // ruta estatica es general-users en IPV6

Figura 13. Comprobación ip en interface R2

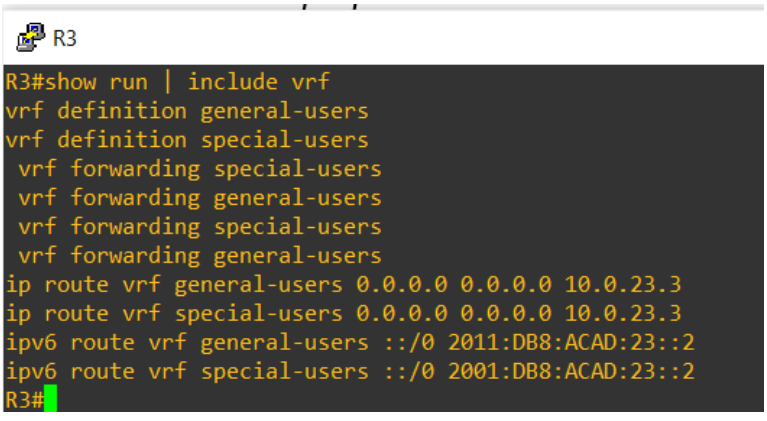


Fuente: propia

ROUTER R3

ip route vrf special-users 0.0.0.0 0.0.0.0 10.0.23.4 // ruta estatica es special-users en IPV4
ip route vrf general-users 0.0.0.0 0.0.0.0 10.0.23.4 // ruta estatica es general-users en IPV4
ipv6 route vrf special-users ::/0 2001:DB8:ACAD:23::2 // ruta estatica es special-users en IPV6
ipv6 route vrf general-users ::/0 2011:DB8:ACAD:23::2 // ruta estatica es general-users en IPV6

Figura 14. Comprobación ip en interface R3



Fuente: propia

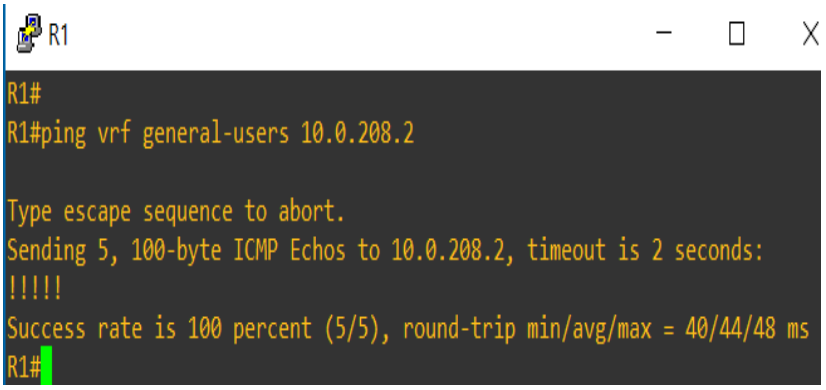
2.4 VERIFIQUE LA CONECTIVIDAD EN CADA VRF.

Desde R1, verifique la conectividad a R3:

• **ping vrf Usuarios generales 10.0.208.Z**

ping vrf general-users 10.0.208.2 // ping en IPV4

Figura 15. Comprobación conectividad en la IP 10.0208.1

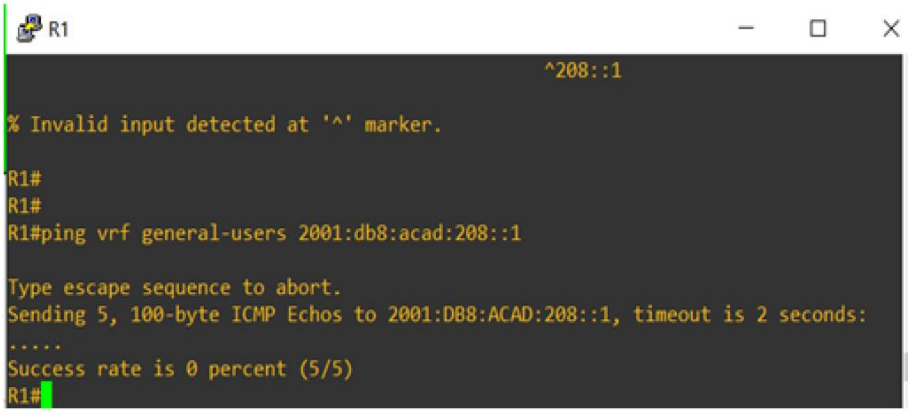


Fuente: propia

• **ping vrf Usuarios generales 2001:db8:acad:208::1**

ping vrf general-users 2001:db8:acad:208::1 // ping en IPV6

Figura 16. Comprobación conectividad en la IP 2001:db8:acad:208::1

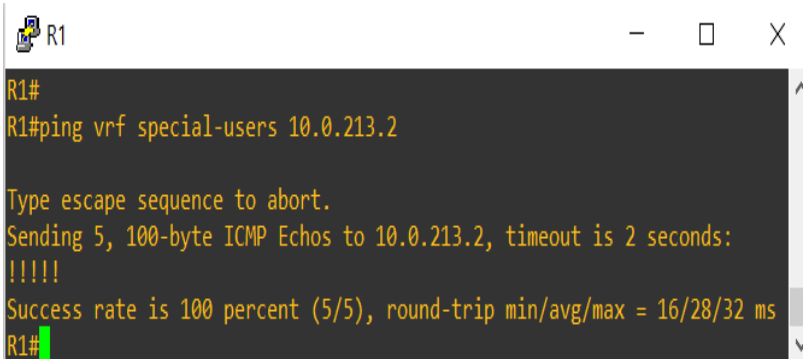


Fuente: propia

• **ping vrf Usuarios especiales 10.0.213.Z**

ping vrf special-users 10.0.213.2 // ping en IPV4

Figura 17. Comprobación conectividad en la IP 10.0.213.1

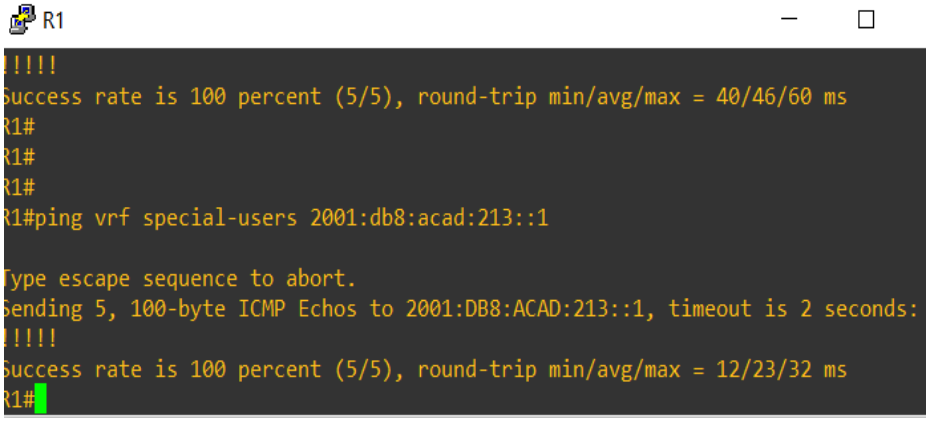


Fuente: propia

• **ping vrf Usuarios especiales 2001:db8:acad:213::1**

ping vrf special-users 2001:db8:acad:213::1 // ping en IPV6

Figura 18. Comprobación conectividad en la IP 2001:db8:acad:2013::1



Fuente: propia

ESCENARIO 2

PARTE 3. CONFIGURAR CAPA 2

Tabla 3. Configuración 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: • Interfaz G1/0/5 y G1/0/6 • Canal de puerto 1 usando PAgP En A1, configure habilitar: • Interfaz F0/1 y F0/2 • Canal de puerto 1 usando PAgP
3.4	En D1, D2 y A1, configure los puertos de acceso para PC1, PC2, PC3 y PC4.	Configure and enable the access ports as follows: • On D1, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface G1/0/23 as an access port in VLAN 13 and enable Portfast. • On D2, configure interface G1/0/24 as an access port in VLAN 8 and enable Portfast. • On A1, configure interface F0/23 as an access port in VLAN 8 and enable Portfast.
3.5	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: propia

3.1 EN D1, D2 Y A1, DESHABILITE TODAS LAS INTERFACES.

SWITCH D1

```
Configure terminal                  // modo de configuración
interface range e1/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e2/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e3/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
```

SWITCH D2

```
Configure terminal                  // modo de configuración
Interface e0/0                      // ingresa a la interfaz
Shutdown                            // apaga la intefaz
Exit                                // cierra la sesión
interface range e1/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e2/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e3/0-3              // rango de interfaces
shutdown                            // apaga la interfaz
exit                                // cierra la sesión
```

SWITCH A1

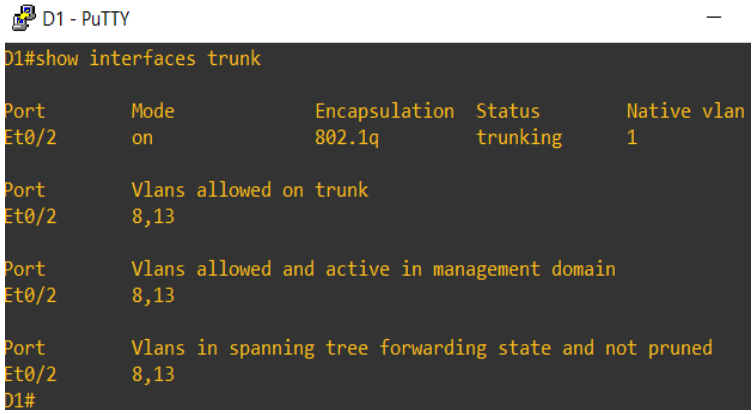
```
Configure terminal                  // modo de configuración
interface e0/3                      // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e1/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e2/0-3              // rango de interfaces
shutdown                            // apaga la intefaz
exit                                // cierra la sesión
interface range e3/0-3              // rango de interfaces
```

shutdown // apaga la intefaz
exit // cierra la sesión

3.2 EN D1 Y D2, CONFIGURE LOS ENLACES TRONCALES A R1 Y R3. SWITCH D1

Configure terminal // modo de configuración
Vlan 13 // crea la VLAN 13
Name Special-Users // nombre de la VLAN creada
Exit // cierra la sesión
Vlan 8 // crea la VLAN 8
name General-Users // nombre de la VLAN creada
exit // cierra la sesión
interface ethernet 0/2 // ingresa a la intefaz
switchport trunk encapsulation dot1q // encapsula los mensajes
switchport mode trunk // modo troncal
switchport trunk allowed vlan 13 // activa el modo para el paso de la VLAN 13
switchport trunk allowed vlan add 8 // activa el modo para el paso de la VLAN 8

Figura 19. Comprobación modo troncal Switch D1

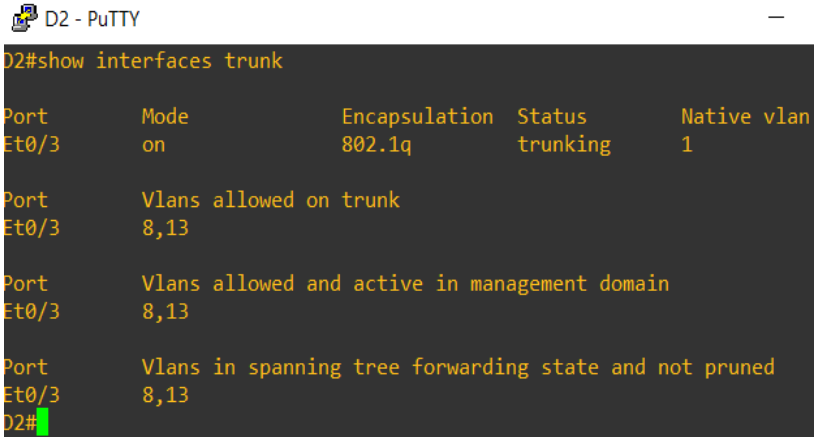


Fuente: propia

SWITCH D2

```
Configure terminal                          // modo de configuración
Vlan 13                                     // crea la VLAN 13
Name Special-Users                          // nombre de la VLAN creada
Exit                                        // cierra la sesión
Vlan 8                                      // crea la VLAN 8
name General-Users                          // nombre de la VLAN creada
exit                                        // cierra la sesión
interface ethernet 0/3                      // ingresa a la interfaz
switchport trunk encapsulation dot1q        // encapsula los mensajes
switchport  mode trunk                      // se activa el modo troncal
switchport trunk allowed vlan 13            // activa el modo para el paso de la
VLAN 13
switchport trunk allowed vlan add 8         // activa el modo para el paso de la VLAN
8
```

Figura 20. Comprobación modo troncal Switch D2



Fuente: propia

3.3 EN D1 Y A1, CONFIGURE EL ETHERCHANNEL.

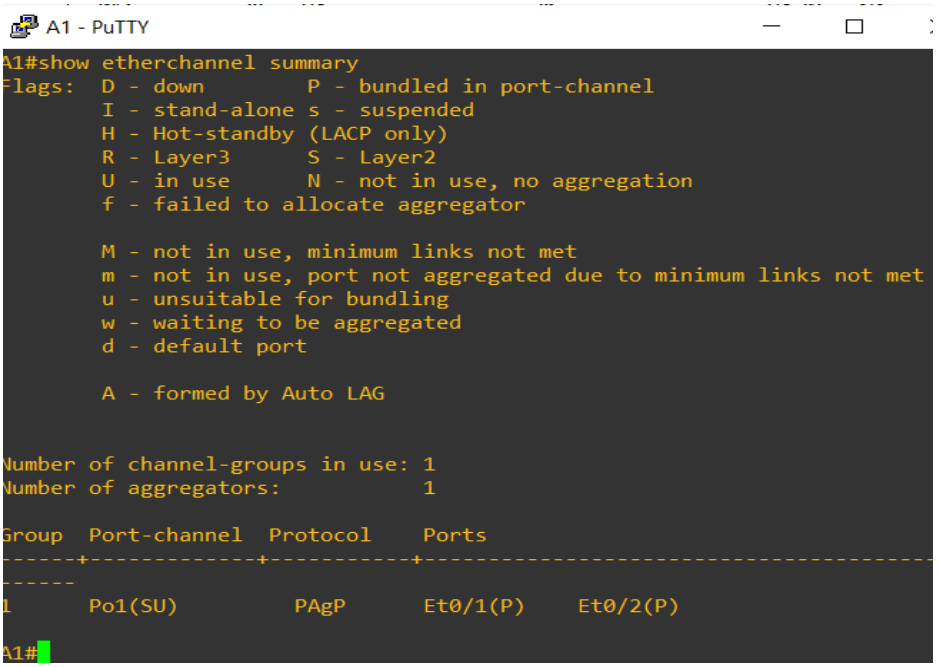
SWITCH D1

SWITCH D1

```
Configure terminal                          // modo de configuración
Interface port-channel 1                    // ingresa al port-channel 1
Switchport mode Access                      // establezca el puerto en modo de
acceso.
Switchport Access vlan 8                    // establezca el puerto en modo de
acceso a la VLAN 8
Exit                                        // cierra la sesión
```

Interface e0/0 // ingrese a la interfaz
Channel-group 1 mode desirable // crea canal en modo grupo 1
Switchport mode Access // establece el modo acceso
Switchport Access vlan 8 // establezca el puerto en modo de acceso vlan 8
No shutdown // enciende la interfaz
Exit // cierra la sesión del usuario
Interface e0/1 // ingresa a la interfaz
Channel-group 1 mode desirable // crea canal en modo grupo 1
Switchport mode Access // establezca el puerto en modo de acceso.
Switchport Access vlan 8 // establezca el puerto en modo de acceso a la VLAN 8

Figura 21. Comprobación modo troncal Switch A1

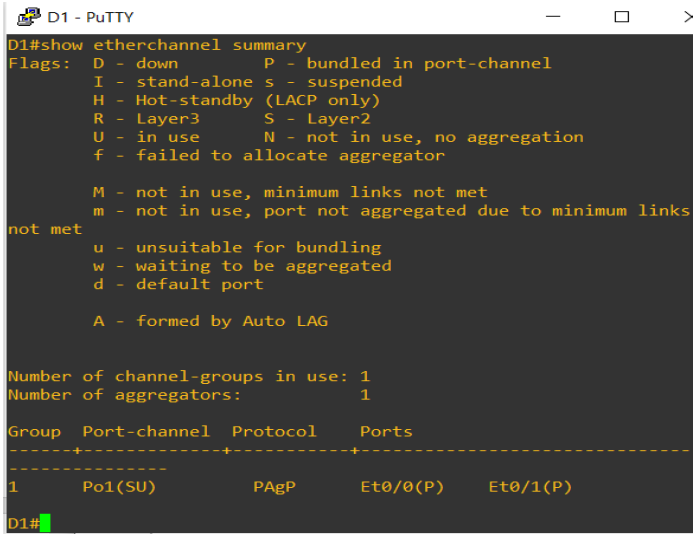


Fuente: propia

SWITCH A1

Configure terminal	// modo de configuración
Interface port-channel 1	// ingresa al port-channel 1
Switchport mode Access	// establezca el puerto en modo de acceso.
Switchport Access vlan 8	// establezca el puerto en modo de acceso vlan 8
Exit	// cierra la sesión del usuario
Interface e0/1	// ingresa a la interfaz
Channel-group 1 mode desirable	// crea canal en modo grupo 1
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 8	// establezca el puerto en modo de acceso vlan 8
No shutdown	// enciende la interfaz
Exit	// cierra la sesión del usuario
Interface e0/2	// ingresa a la interfaz
Channel-group 1 mode desirable	// crea canal en modo grupo 1
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 8	// establezca el puerto en modo de acceso vlan 8
No shutdown	// enciende la interfaz

Figura 22. Comprobación modo troncal Switch D1



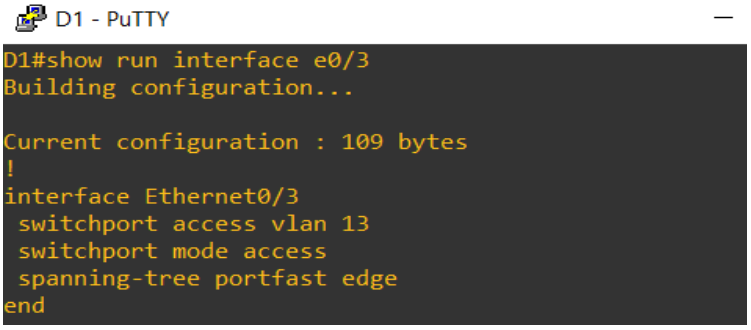
Fuente: propia

3.4 EN D1, D2 Y A1, CONFIGURE LOS PUERTOS DE ACCESO PARA PC1, PC2, PC3 Y PC4.

Configuración puertos de acceso para PC1 en SWITCH D1

Configure terminal	// modo de configuración
Interface e0/3	// ingresa a la interfaz
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 13	// establezca el puerto en modo de acceso vlan 13
Spaning-tree portfast	// habilita la protección BPDU en todos los puertos
No shutdown	// enciende la interfaz

Figura 23. Comprobación modo de acceso Switch D1

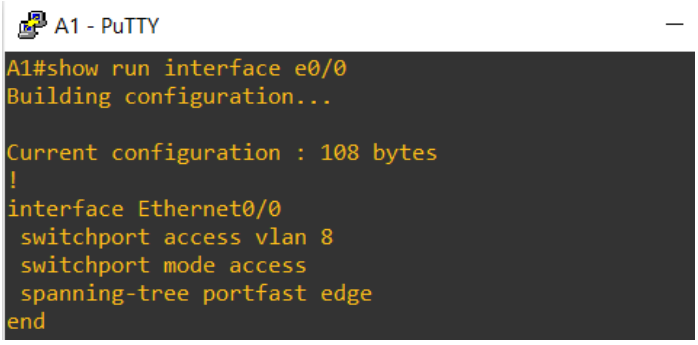


Fuente: propia

Configuración puertos de acceso para PC3 en SWITCH A1

Configure terminal	// modo de configuración
Interface e0/0	// ingresa a la interfaz
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 8	// establezca el puerto en modo de acceso vlan 8
Spaning-tree portfast	// habilita la protección BPDU en todos los puertos
No shutdown	// enciende la interfaz

Figura 24. Comprobación modo de acceso Switch A1

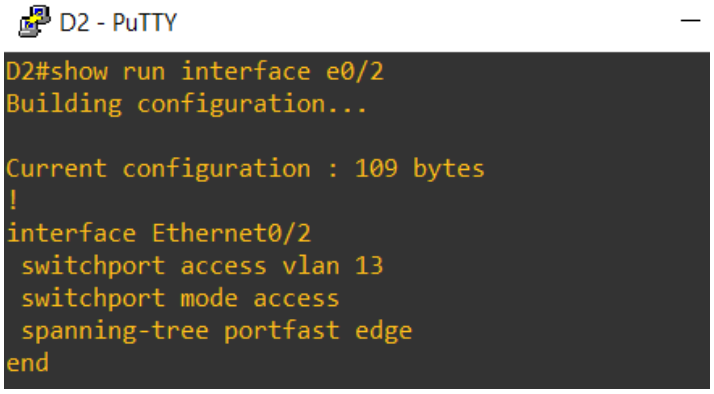


Fuente: propia

Configuración puertos de acceso para PC2 en SWITCH D2

Configure terminal	// modo de configuración
Interface e0/2	// ingresa a la interfaz
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 13	// establezca el puerto en modo de acceso vlan 13
Spaning-tree portfast	// habilita la protección BPDU en todos los puertos
No shutdown	// enciende la interfaz

Figura 25. Comprobación modo de acceso Switch D2

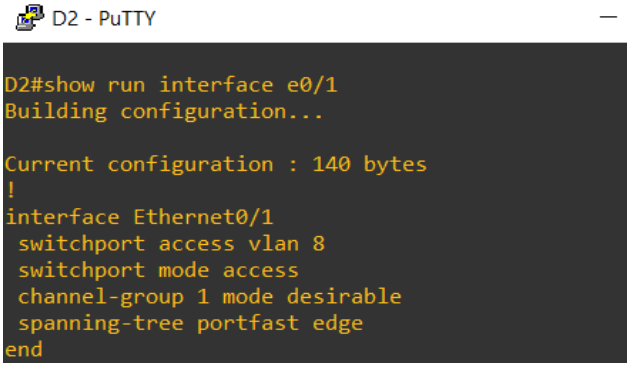


Fuente: propia

Configuración puertos de acceso para PC4 en SWITCH D2

Configure terminal	// modo de configuración
Interface e0/1	// ingresa a la interfaz
Switchport mode Access	// establece el modo acceso
Switchport Access vlan 8	// establezca el puerto en modo de acceso vlan 8
Spaning-tree portfast	// habilita la protección BPDU en todos los puertos
No shutdown	// enciende la interfaz

Figura 26. Comprobación modo de acceso Switch D2

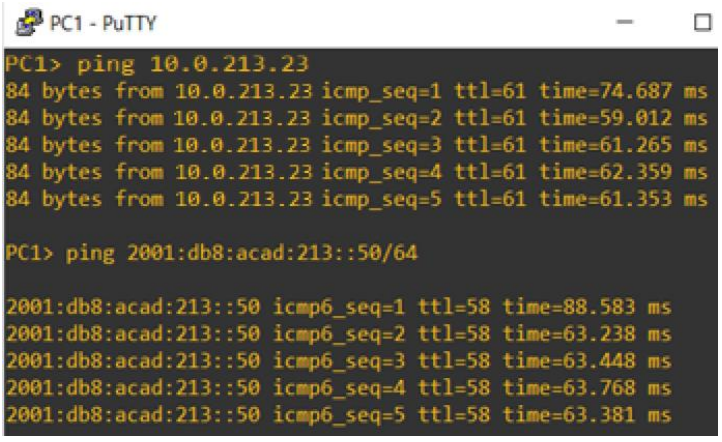


Fuente: propia

3.5 VERIFIQUE LA CONECTIVIDAD DE PC A PC.

Desde la pc1, verifique la conectividad ipv4 e ipv6 a la pc2.

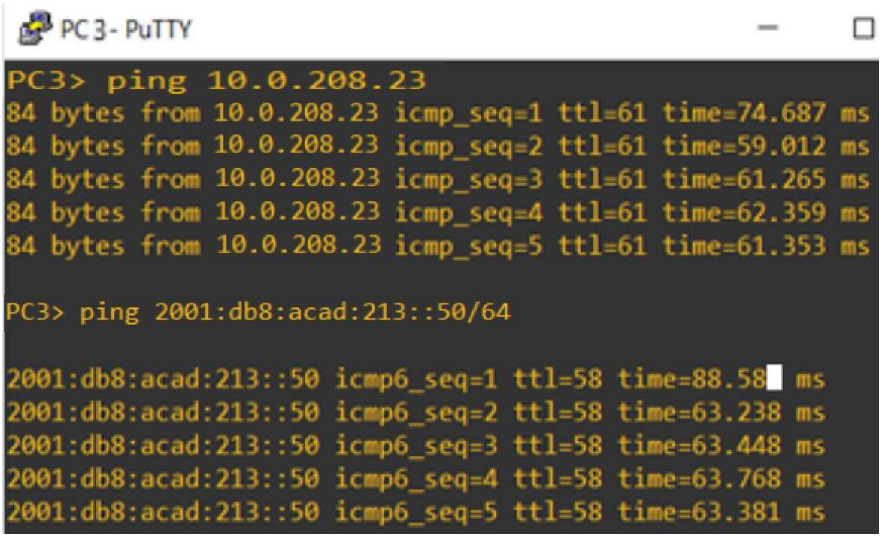
Figura 27. Ping de conectividad PC1 a PC2



Fuente: propia

Desde la pc3, verifique la conectividad ipv4 e ipv6 a la pc4.

Figura 28. Ping de conectividad PC3 a PC4



Fuente: propia

PARTE 4. CONFIGURE SEGURIDAD

Tabla 4. Configuración de Seguridad.

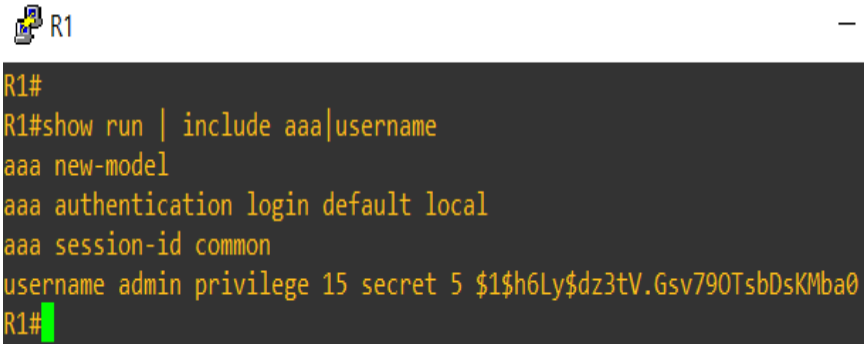
Tarea	Tarea	Especificación
4.1	En todos los dispositivos, modo EXE privilegiado seguro.	Configure un secreto de habilitación de la siguiente manera: • Tipo de algoritmo: SCRYPT • Contraseña: nombreestudianteXYZ.
4.2	En todos los dispositivos, cree una cuenta de usuario local.	Configurar un usuario local: • Nombre: administrador • Nivel de privilegio: 15 • Tipo de algoritmo: SCRYPT • Contraseña: nombrestudianteXYZ
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.

Fuente: propia

ROUTER R1

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario local admin
Username admin privilige 15 secret jojan232 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa autthentication login defaul local // activa autenticación en el equipo
exit // cierra la sesión del usuario actual

Figura 29. Configuración de Seguridad en Router R1

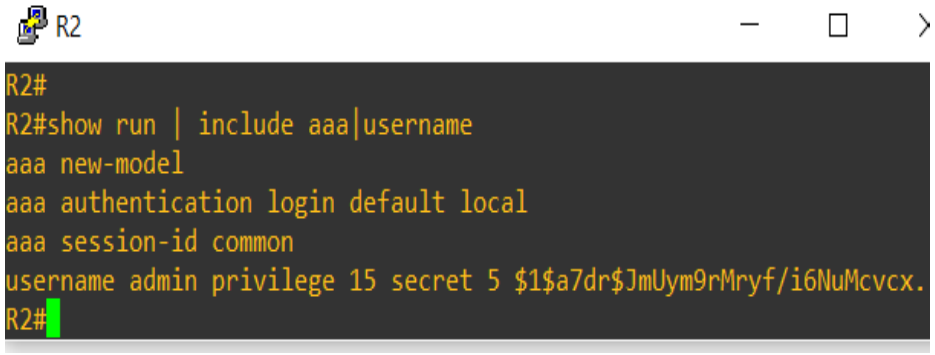


Fuente: propia

ROUTER R2

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario local admin
Username admin privilege 15 secret jojan232 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
exit // cierra la sesión del usuario actual

Figura 30. Configuración de Seguridad en Router R2

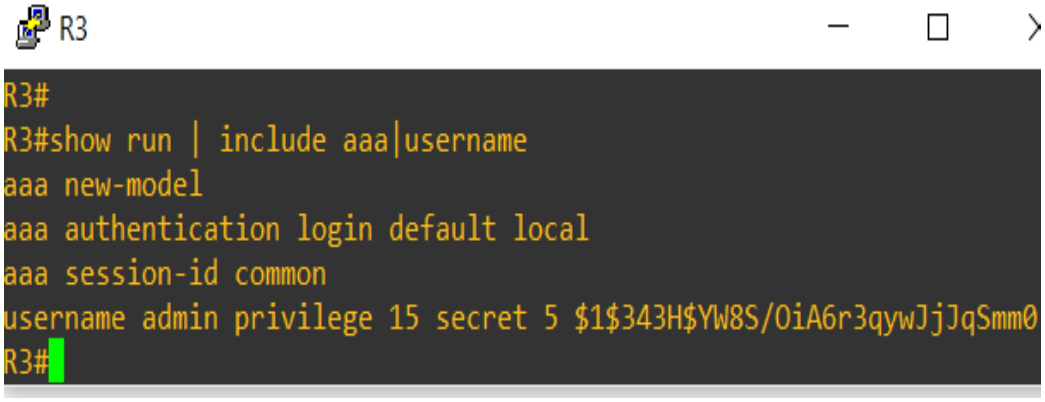


Fuente: propia

ROUTER R3

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario local admin
Username admin privilege 15 secret l jojan232 // crea usuario para nivel 15
aaa new-model // activa nuevo modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
exit // cierra la sesión del usuario actual

Figura 31. Configuración de Seguridad en Router R3

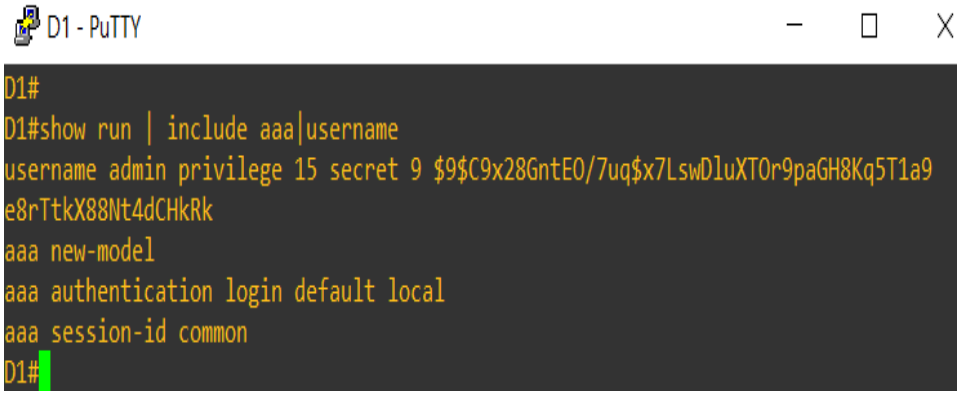


Fuente: propia

SWITCH D1

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario local admin
Username admin privilege 15 secret jojan232 // crea usuario para nivel 15
aaa new-model // modo de seguridad
aaa authentication login default local // autenticación en el equipo
end // cierra la sesión del usuario actual

Figura 32. Configuración de Seguridad en Switch D1

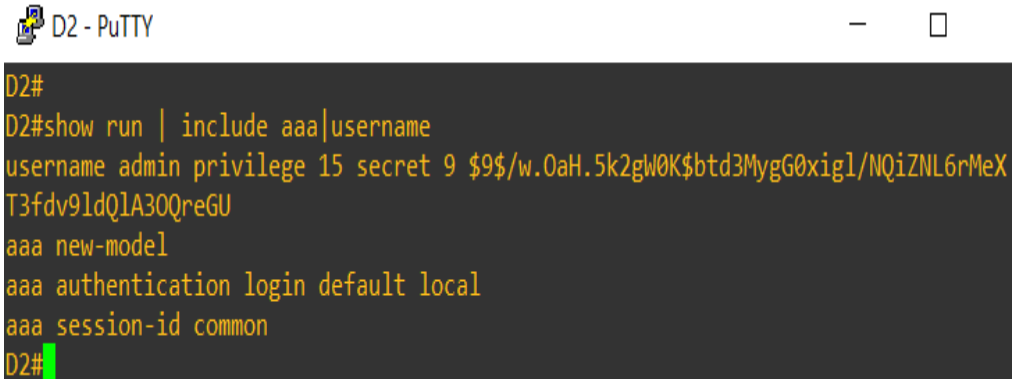


Fuente: propia

SWITCH D2

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario local admin
Username admin privilege 15 secret jojan232 // crea usuario para nivel 15
aaa new-model // modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
end // cierra la sesión del usuario actual

Figura 33. Configuración de Seguridad en Switch D2

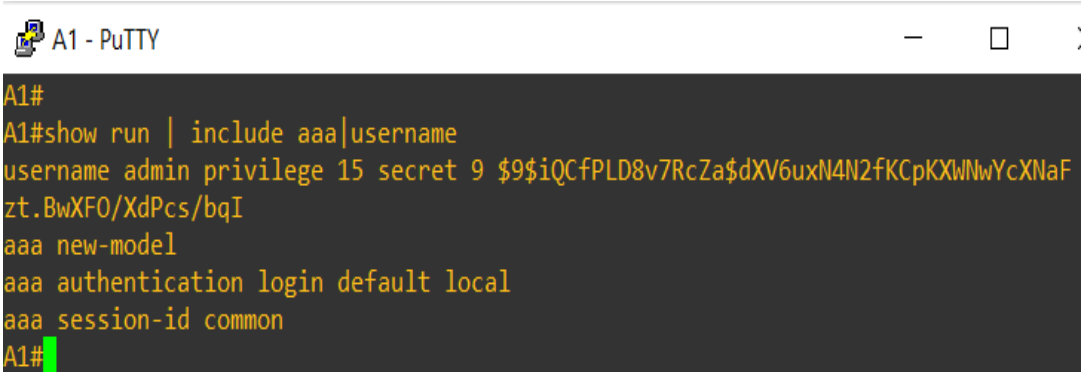


Fuente: propia

SWITCH A1

Configure terminal // modo de configuración
Service password-encryption // aplica un cifrado débil a todas las contraseñas sin cifrar
Enable secret l jojan232 // establece la contraseña
Username admin secret 0 jojan232 // crea usuario para nivel 15
Username admin privilege 15 secret jojan232 // modo de seguridad
aaa new-model // modo de seguridad
aaa authentication login default local // activa autenticación en el equipo
end

Figura 34. Configuración de Seguridad en Switch A1



Fuente: propia

CONCLUSIONES

Con el desarrollo del Diplomado De Profundización Cisco CCNP, Es importante entender que la estructuración de redes conmutadas mediante el uso del protocolo STP y la configuración de VLANs, permiten el desarrollo de una infraestructura de red jerárquica convergente. El protocolo STP (Spanning Tree Protocol) ayuda a evitar bucles de red y la configuración de VLANs (Virtual Local Area Networks) permite la segmentación de la red para mejorar la eficiencia y la seguridad.

Se logro interiorizar la configuración básica y avanzada de protocolos de enrutamiento permiten diseñar soluciones de red escalables para la implementación de servicios IP con calidad de servicio en ambientes de red empresariales LAN y WAN. La calidad de servicio (QoS) garantiza la entrega de tráfico prioritario y reduce la congestión de la red.

Se implemento la planificación de redes inalámbricas, de acceso remoto y sitio a sitio seguras mediante el análisis de escenarios simulados de infraestructuras de red empresariales, permite la aplicación de servicios de autenticación, roaming y localización. La autenticación garantiza la seguridad de la red, el roaming permite que los usuarios se muevan de un punto de acceso a otro sin perder la conexión, y la localización permite conocer la posición de los usuarios en la red.

Por último la implementación de redes empresariales con acceso seguro a través de la automatización y virtualización de la red, permite aplicar metodologías de solución de problemas en ambientes de red corporativos LAN y WAN. La automatización reduce los errores humanos y la virtualización permite crear redes virtuales que pueden ser configuradas, administradas y protegidas de manera más eficiente.

BIBLIOGRAFÍA

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. “CCNP and CCIE Enterprise Core ENCOR 350-401”. {En linea}. {25 de enero 2020}. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. Multicast. “CCNP and CCIE Enterprise Core ENCOR 350-401”. {En linea}. {25 de enero 2020}. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. QoS. “CCNP and CCIE Enterprise Core ENCOR 350-401”. {En linea}. {25 de enero 2020}. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA RIOS, Ramiro., GOOLEY, Jasón., HUCABY, David. IP Services. “CCNP and CCIE Enterprise Core ENCOR 350-401”. {En linea}. {25 de enero 2020}. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8