DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JAVIER ALONSO HURTADO PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JAVIER ALONSO HURTADO PEREZ

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2021

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá 29 de Noviembre de 2021

AGRADECIMIENTOS

Quiero dedicar este trabajo a mi familia ya que fueron ellos quienes desde el principio me animaron e impulsaron a retomar mis estudios universitarios, a creer de nuevo en que se pueden alcanzar los sueños y que con actitud, perseverancia, anhelo gratitud, humildad y confianza en Dios se pueden lograr los objetivos que uno se proponga en la vida, por lo tanto son ellos a quienes quiero hacer un pequeño reconocimiento pero con mucho amor por creer y confiar en mi, por alentarme en cada momento difícil donde estuve a punto de tirarlo todo debido a la carga laboral y educativa que muchas veces me agobiaba, por darme una palabra de aliento, por motivarme cada día y por impulsarme a seguir mis sueños a pesar de las adversidades y sacrificios, por entender cuando no podía jugar, dormir, salir o simplemente compartir con ellos, hoy siento que no los defraude y que todo ese sacrificio siempre valió la pena, que próximamente culminaremos juntos un sueño y una meta que nos trazamos y que gracias a ellos se hará realidad con la voluntad de Dios.

Por ultimo pero no menos importante quiero agradecer a mi gran universidad UNAD, a mis compañeros y en especial a mis Tutores, quienes también fueron parte fundamental en este proceso, por que fueron ellos quienes nos mostraron el camino y como debíamos seguirlo, nos guiaron, nos motivaron, muchos de ellos fueron amigos y maestros que nunca olvidare por que tuvieron conmigo métodos de enseñanza, paciencia, una cordial y amigable actitud siempre dispuesta a ayudar, entendiendo que no todos estamos en el mismo nivel educativo y que los años han hecho meya en nuestras mentes que nos dificultan el aprendizaje, pero que con su dedicación por la enseñanza y sus estudiantes nos permitieron retomar el camino y poder cumplir con los objetivos que cada semestre nos trazamos, gracias a todos ellos que hicieron parte de este sueño hoy cumplido.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

PROTOCOLO ENRUTAMIENTO: Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento

OSPF: es un protocolo de enrutamiento dinámico interior, usa un algoritmo de tipo Estado de Enlace Dijkstra para calcular la ruta idónea entre dos nodos en un sistema autónomo.

BGP es un protocolo de puerta de enlace (EGP) exterior que se utiliza para intercambiar información de encaminamiento entre enrutadores de diferentes sistemas autónomos.

HSRP: Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

SCRYPT: es una función de derivación de claves basada en contraseña, el algoritmo fue diseñado específicamente para que sea costoso realizar ataques de hardware personalizados a gran escala al requerir grandes cantidades de memoria.

NTP: Network Time Protocol es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

SNMP: Protocolo simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red

RADIUS: Remote Authentication Dial-In User Service es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

RESUMEN

Con la finalidad de desarrollar las habilidades adquiridas a lo largo del diplomado en cuanto a las tecnologías de redes de comunicaciones mas recientes , a continuación se detalla el desarrollo a nivel de configuración de un escenario propuesto el cual esta denotado como prueba de habilidades practicas CCNP, en donde se pretende realiza la configuración de diferentes protocolos de comunicación en capa dos y capa tres para dispositivos de red como switch y routers y de esta manera completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada y para que los protocolos configurados estén operativos de modo que se logre la convergencia en la red y cumplan con las especificaciones proporcionadas.

Palabras clave: CISCO, CCNP, conmutación, Enrutamiento, Redes, Electronica

ABSTRACT

In order to develop the skills acquired throughout the diploma in terms of the most recent communications network technologies, the development at the configuration level of a proposed scenario is detailed below, which is denoted as a test of practical CCNP skills, where it is intended to configure different communication protocols in layer two and layer three for network devices such as switches and routers and in this way complete the network configuration so that there is complete accessibility from one end to the other, so that the hosts are reliably supported by the default gateway and the configured protocols are operational so that convergence is achieved on the network and meets the specifications provided.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics

INTRODUCCION

En el campo de la ingeniería de telecomunicaciones es importante comprender todos los componentes que hacen posible la comunicación de extremo a extremo para la transferencia de datos, para poder comprender un campo tan amplio como lo son las comunicaciones existen diferentes áreas especificas en las cuales se puede indagar cara comprender al detalle lo que sucede al interior de los diferentes dispositivos que interactúan de manera directa o indirecta sobre esta comunicación, por lo tanto es indispensable hacer un acercamiento mas profundo sobre la configuración de estos dispositivos y poder de alguna manera modelar su comportamiento para un fin especifico de acuerdo a los requerimiento de una red en particular, por tal motivo en este documento se desarrollan una serie de tareas que tienen como finalidad modelar la red de manera que pueda lograse una convergencia entre los equipos intermedios de modo que se logre una comunicación exitosa entre los equipos de usuario final.

Para el desarrollo practico se ha propuesto un escenario de topología de red compuesto por switch capa 2, switch de capa 3, routers y equipos pc interconectados entre si con una topología redundante para lograr alta disponibilidad tanto para usuarios finales como para los diferentes protocolos que circulan en la red.

En esta topología se pueden encontrar protocolos de enrutamiento ya que simulara un escenario en el cual existe un protocolo de Gateway interior como lo es OSPF y un protocolo de Gateway exterior como lo es BGP, también se pretende desarrollar la configuración de switch y los diferentes protocolos de capa dos como Spanning-tree, Etherchannel, enlaces troncales creación de vlan entre otros y por ultimo se realizara una configuración de redundancia de primer salto, seguridad de contraseñas, seguridad de acceso, autenticación y configuración de protocolos de gestión de administración como lo es SNMP y Syslog.

DESARROLLO ESCENARIO PROPUESTO

ESCENARIO PROPUESTO

Topología de Red

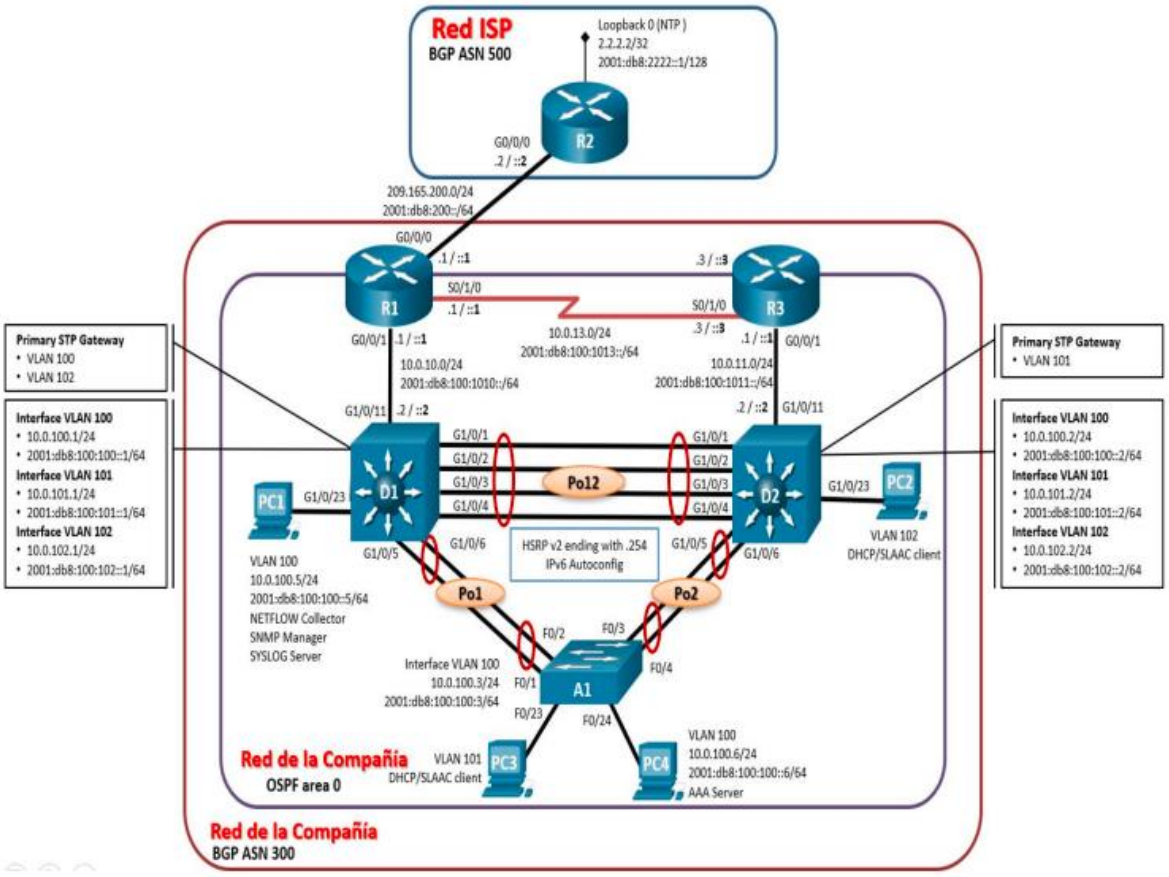

Ilustración 1Topologia propuesta

Tabla de direccionamiento

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
R1	G0/0/0	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	E0/3	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3

Tabla 1 Tabla de Direccionamiento R1

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
R2	G0/0/0	E0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	Lo0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3

Tabla 2 Tabla de Direccionamiento R2

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
R3	G0/0/1	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	E0/3	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3

Tabla 3 Tabla de Direccionamiento R3

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
D1	G1/0/11	E1/3	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	Int vlan 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	Int vlan 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	Int vlan 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4

Tabla 4 Tabla de Direccionamiento D1

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
D2	G1/0/11	E1/3	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	Int vlan 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	Int vlan 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	Int vlan 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4

Tabla 5 Tabla de Direccionamiento D2

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
A1	VLAN 100	Int vlan 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1

Tabla 6 Tabla de Direccionamiento A1

Dispositivo	Interfaz	Interfaz Simulador	Dir IPv4	Dir IPv6	IPv6 Link local
PC1	NIC	Ethernet	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	Ethernet	DHCP	SLAAC	EUI-64
PC3	NIC	Ethernet	DHCP	SLAAC	EUI-64
PC4	NIC	Ethernet	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Tabla 7 Tabla de Direccionamiento PCs

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.

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

Se realiza el montaje de la topología en el simulador GNS3 tal como se evidencia en la siguiente imagen.

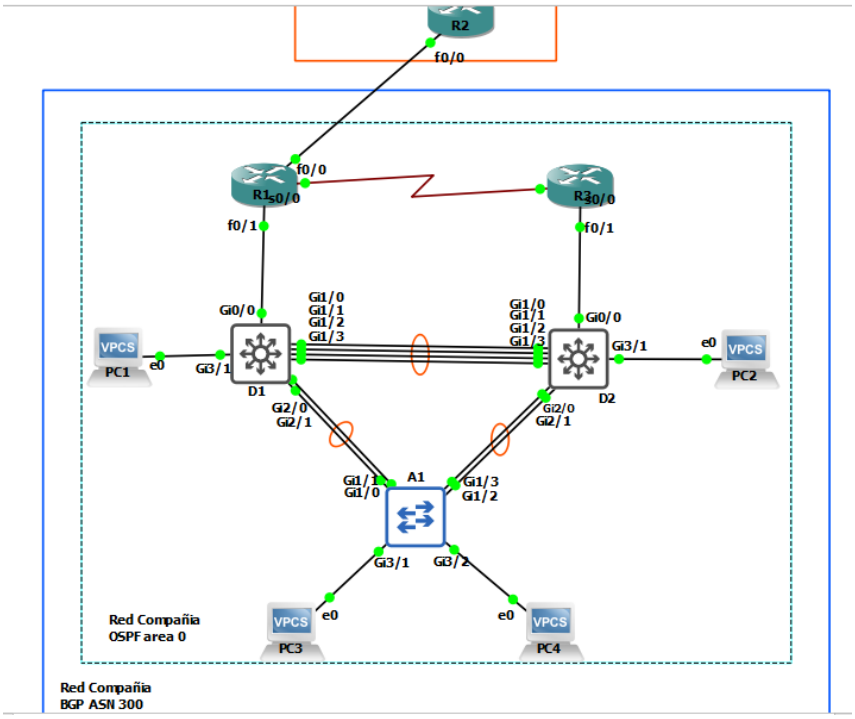

Ilustración 2 Montaje simulador GNS3

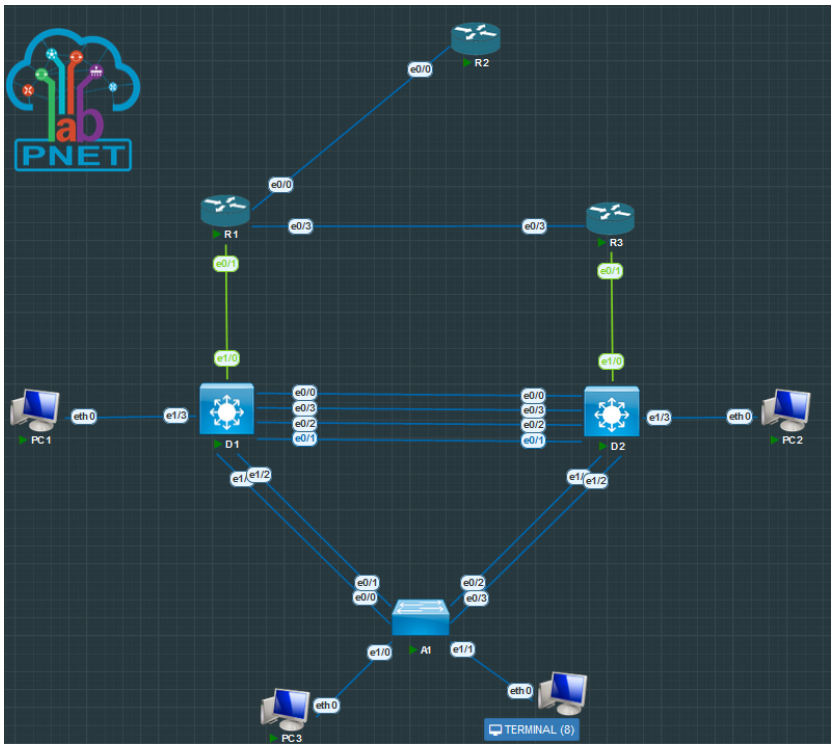

Ilustración 3 Montaje en simulador PNETLAB

Paso 2: Configurar los parámetros básicos para cada dispositivo.

Router R1

hostname R1	*asignación de nombre al router*
ipv6 unicast-routing	*Se habilita routing Ipv6*
no ip domain lookup	
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	*Aviso informativo cuando se accede al router*
line con 0	*línea de consola*
exec-timeout 0 0	*Tiempo salida 0*
logging synchronous	
exit	
interface e0/0	*Interface Ethernet 0/0*
descripción UpL_R2	*descripción de la interface*
ip address 209.165.200.225 255.255.255.224	*Se asigna direccionamiento ipv4*
ipv6 address fe80::1:1 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:200::1/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*

```
exit
interface e0/1                                  interface ethernet 0/1
description UpL_D1                              descripción de la interface
ip address 10.0.10.1 255.255.255.0              Se asigna direccionamiento ipv4
ipv6 address fe80::1:2 link-local               Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:100:1010::1/64            Se asigna direccionamiento ipv6
no shutdown                                     Se habilita la interface
exit
interface s1/0                                  interface serial 0/1
description UpL_R3                              descripción de la interface
ip address 10.0.13.1 255.255.255.0              Se asigna direccionamiento ipv4
ipv6 address fe80::1:3 link-local               Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:100:1013::1/64            Se asigna direccionamiento ipv6
no shutdown                                     Se habilita la interface
exit
```

Router R2

```
hostname R2                                     Asignacion de nombre al router
ipv6 unicast-routing                            Se habilita routing Ipv6
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #    Aviso informativo cuando
                                                           se accede al router
line con 0                                      línea de consola
exec-timeout 0 0                                Tiempo de salida 0
logging synchronous
exit
interface e0/0                                  interface ethernet 0/0
description UpL_R1                              descripción de la interface
ip address 209.165.200.226 255.255.255.224      Se asigna direccionamiento ipv4
ipv6 address fe80::2:1 link-local               Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:200::2/64                 Se asigna direccionamiento ipv6
no shutdown                                     Se habilita la interface
exit
interface Loopback 0                            interface loopback 0
ip address 2.2.2.2 255.255.255.255              Se asigna direccionamiento ipv4
ipv6 address fe80::2:3 link-local               Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:2222::1/128               Se asigna direccionamiento ipv6
no shutdown                                     Se habilita la interface
exit
```

Router R3

hostname R3	*Asignacion de nombre al router*
ipv6 unicast-routing	*Se habilita routing Ipv6*
no ip domain lookup	
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	*Aviso informativo cuando se accede al router*
line con 0	*línea de consola*
exec-timeout 0 0	*Tiempo de salida 0*
logging synchronous	
exit	
interface e0/1	*interface ethernet 0/*1
description UpL_D2	*descripción de la interface*
ip address 10.0.11.1 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::3:2 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:1011::1/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
interface s1/0	*interface ethernet 0/*1
description UpL_R1	*descripción de la interface*
ip address 10.0.13.3 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::3:3 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:1010::2/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	

Switch D1

hostname D1	*asignación de nombre al router*
ip routing	*Se habilita el enrutamiento*
ipv6 unicast-routing	*Se habilita routing Ipv6*
no ip domain lookup	
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	*Aviso informativo cuando se accede al router*
line con 0	*línea de consola*
exec-timeout 0 0	*Tiempo de salida 0*
logging synchronous	
exit	
vlan 100	*Crea vlan 100*
name Management	*Nombrar la vlan*
exit	
vlan 101	*Crea vlan 101*
name UserGroupA	*Nombrar la vlan*
exit	

vlan 102	*Crea vlan 102*
name UserGroupB	*Nombrar la vlan*
exit	
vlan 999	*Crea vlan 999*
name NATIVE	*Nombrar la vlan*
exit	
interface e1/0	*interface ethernet 1/*0
description UpL_ R1	*descripción de la interface*
no switchport	
ip address 10.0.10.2 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d1:1 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:1010::2/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
interface vlan 100	*ingresa a la interfaz vlan 100*
ip address 10.0.100.1 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d1:2 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:100::1/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
interface vlan 101	*ingresa a la interfaz vlan 101*
ip address 10.0.101.1 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d1:3 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:101::1/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
interface vlan 102	*ingresa a la interfaz vlan 101*
ip address 10.0.102.1 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d1:4 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:102::1/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	*excluye varios rangos de*
ip dhcp excluded-address 10.0.101.141 10.0.101.254	*direcciones de los pool DHCP*
ip dhcp excluded-address 10.0.102.1 10.0.102.109	
ip dhcp excluded-address 10.0.102.141 10.0.102.254	
ip dhcp pool VLAN-101	*Crear el pool DHCP para vlan 101*
network 10.0.101.0 255.255.255.0	*Asigna la red para el DHCP*
default-router 10.0.101.254	*Gateway de la red*
exit	
ip dhcp pool VLAN-102	*Crear el pool DHCP para vlan 101*
network 10.0.102.0 255.255.255.0	*Asigna la red para el DHCP*

default-router 10.0.102.254	*Gateway de la red*
exit	

Switch D2

hostname D2	*Asignacion de nombre al router*
ip routing	*Se habilita el enrutamiento*
ipv6 unicast-routing	*Se habilita routing Ipv6*
no ip domain lookup	
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	*Aviso informativo cuando se accede al router*
line con 0	*Linea de consola 0*
exec-timeout 0 0	Tiempo salida 0
logging synchronous	
exit	
vlan 100	*Crea la vlan 100*
name Management	*Asigna nombre a la vlan*
exit	
vlan 101	*Crea la vlan 101*
name UserGroupA	*Asigna nombre a la vlan*
exit	
vlan 102	*Crea la vlan 102*
name UserGroupB	*Asigna nombre a la vlan*
exit	
vlan 999	*Crea la vlan 999*
name NATIVE	*Asigna nombre a la vlan*
exit	
interface e1/0	Interface ethernet 1/0
description UpL_R3	Descripcion de la interface
no switchport	
ip address 10.0.11.2 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d1:1 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:1011::2/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	
interface vlan 100	*ingresa a la interfaz vlan 100*
ip address 10.0.100.2 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::d2:2 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:100::2/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	

```
interface vlan 101                                  ingresa a la interfaz vlan 101
ip address 10.0.101.2 255.255.255.0                 Se asigna direccionamiento ipv4
ipv6 address fe80::d2:3 link-local                  Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:100:101::2/64                 Se asigna direccionamiento ipv6
no shutdown                                         Se habilita la interface
exit
interface vlan 102                                  ingresa a la interfaz vlan 101
ip address 10.0.102.2 255.255.255.0                 Se asigna direccionamiento ipv4
ipv6 address fe80::d2:4 link-local                  Se asigna direccionamiento local ipv6
ipv6 address 2001:db8:100:102::2/64                 Se asigna direccionamiento ipv6
no shutdown                                         Se habilita la interface
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209    excluye varios rangos  de
ip dhcp excluded-address 10.0.101.241 10.0.101.254  direcciones de los pool DHCP
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101                               Crear el pool DHCP para vlan 101
network 10.0.101.0 255.255.255.0                    Asigna la red para el DHCP
default-router 10.0.101.254                         Gateway de la red
exit
ip dhcp pool VLAN-102                               Crear el pool DHCP para vlan 101
network 10.0.102.0 255.255.255.0                    Asigna la red para el DHCP
default-router 10.0.102.254                         Gateway de la red
exit
```

Switch A1

```
hostname A1                                                 Asignacion de nombre al router
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #     Aviso informativo cuando se
                                                                accede al router
line con 0                                                  Ingresa a línea de consola 0
exec-timeout 0 0                                            timeout en 0
logging synchronous
exit
vlan 100                                                    crea la vlan 100
name Management                                             Asigna nombre a la vlan
exit
vlan 101                                                    crea la vlan 101
name UserGroupA                                             Asigna nombre a la vlan
exit
vlan 102                                                    crea la vlan 102
```

name UserGroupB	*Asigna nombre a la vlan*
exit	
vlan 999	*crea la vlan 999*
name NATIVE	*Asigna nombre a la vlan*
exit	
interface vlan 100	Ingresa a la interfaz vlan 100
ip address 10.0.100.3 255.255.255.0	*Se asigna direccionamiento ipv4*
ipv6 address fe80::a1:1 link-local	*Se asigna direccionamiento local ipv6*
ipv6 address 2001:db8:100:100::3/64	*Se asigna direccionamiento ipv6*
no shutdown	*Se habilita la interface*
exit	

Parte 2: Configurar la capa 2 de la red y el soporte de Host

Tarea 2.1

En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Habilite enlaces trunk 802.1Q entre:

D1 and D2

D1 and A1

D2 and A1

Se ingresa a cada interfaz entre los switches solicitados y se configura el modo troncal y el tipo de encapsulación.

D1(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
exit
D1(config)#Interfaz range e1/1 – 2
Switchport encapsulation dot1q
Switchport mode trunk
exit

```
D1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      999
Po12        on               802.1q         trunking      999

Port        Vlans allowed on trunk
Po1         1-4094
Po12        1-4094

Port        Vlans allowed and active in management domain
Po1         1,100-102,999
Po12        1,100-102,999

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,100-102,999
Po12        1,100-102,999
```

Ilustración 4 D1 802.1q - Vlan nativa - trunk

D2
D2(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
exit
D2(config)#Interfaz range e1/1 – 2
Switchport encapsulation dot1q
Switchport mode trunk
Exit

```
D2#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Po2         on               802.1q         trunking      999
Po12        on               802.1q         trunking      999

Port        Vlans allowed on trunk
Po2         1-4094
Po12        1-4094

Port        Vlans allowed and active in management domain
Po2         1,100-102,999
Po12        1,100-102,999

Port        Vlans in spanning tree forwarding state and not pruned
Po2         1,100-102,999
Po12        1,100-102,999
```

Ilustración 5 D2 802.1q - Vlan nativa - trunk

A1
A1(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
exit

```
A1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      999
Po2         on               802.1q         trunking      999

Port        Vlans allowed on trunk
Po1         1-4094
Po2         1-4094

Port        Vlans allowed and active in management domain
Po1         1,100-102,999
Po2         1,100-102,999

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,100-102,999
Po2         none
```

Ilustración 6 A1 802.1q - Vlan nativa - trunk

Tarea 2.2
En todos los switches cambie la VLAN nativa en los enlaces troncales
Use VLAN 999 como la VLAN nativa.

Se procede a agregar a la configuración de los switch anteriormente descrita la línea Switchport trunk native vlan 999

D1(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
Switchport trunk native vlan 999
exit
D1(config)#Interfaz range e1/1 – 2

Switchport encapsulation dot1q
Switchport mode trunk
Switchport trunk native vlan 999
exit

D2(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
Switchport trunk native vlan 999
exit
D2(config)#Interfaz range e1/1 – 2
Switchport encapsulation dot1q
Switchport mode trunk
Switchport trunk native vlan 999
Exit

A1(config)#Interfaz range e0/0 – 3
Switchport encapsulation dot1q
Switchport mode trunk
Switchport trunk native vlan 999
exit

Tarea 2.3
En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)
Use Rapid Spanning Tree (RSPT).

Se ingresa a cada switch y se habilita el mode RSTP con el comando spanning-tree mode rapid-pvst

D1(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree mode rapid-pvst
A1(config)#spanning-tree mode rapid-pvst

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

Ilustración 7 D1 Rapid Spanning-tree

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

Ilustración 8 D2 Rapid Spanning-tree

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

Ilustración 9 A1 Rapid Spanning-tree

Tarea 2.4

En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

Se ingresa al switch D1 y se configura en modo primario para las vlan 100 y 102 y como respaldo para la vlan 101, de igual manera al switch D2 como primario para la vlan 101 pero también como respaldo para las vlan 100 y 102.

D1(config)#spanning-tree vlan 100, 102 root primary
D1(config)#spanning-tree vlan 101 root secondary

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
```

Ilustración 10 D1 Spanning-tree root primary

D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100, 102 root secondary

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
```

Ilustración 11 D2 Spanning-tree root secondary

Tarea 2.5

En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

Use los siguientes números de canales:
D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2

Se debe ingresar al grupo de interfaces que conformaran el etherchanel y asignarlos a un grupo de portchanel según solicitud, habilitando con el comando active el modo LACP

D1(config)#int range ethernet 0/0 – 3
Channel-group 12 mode active
D1(config)#int range ethernet 1/1 – 2
Channel-group 1 mode active

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
```

Ilustración 12 D1 Port-channel 1 y 12

D2(config)#int range ethernet 0/0 – 3
Channel-group 12 mode active
D2(config)#int range ethernet 1/1 – 2
Channel-group 1 mode active

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
```

Ilustración 13 D2 Port-channel 2 y 12

A1(config)#int range ethernet 0/0 – 1
Channel-group 1 mode active

A1(config)#int range ethernet 0/2 – 3
Channel-group 2 mode active

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
```

Ilustración 14 A1 Port-channel 1 y 2

Tarea 2.6
En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.
Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

En el puerto donde se conecta el host se debe configurar en modo acceso, con acceso a la vlan indicada y habilitando el modo de reenvío de spannin-tree

D1(config)# interface Ethernet1/3
description PC_1
switchport mode Access
switchport access vlan 100
spanning-tree portfast edge

```
interface Ethernet1/3
 description PC_1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
 spanning-tree bpduguard enable
end

D1#
```

Ilustración 15 D1 Interfaz PC1

D2(config)# interface Ethernet1/3
description PC_2
switchport mode Access
switchport access vlan 102
spanning-tree portfast edge

```
interface Ethernet1/3
 description PC_1
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
 spanning-tree bpduguard enable
end

D2#
```

Ilustración 16 D2 Interfaz PC2

A1(config)# interface Ethernet1/0
description PC_3
switchport mode Access
switchport access vlan 101
spanning-tree portfast edge

A1(config)# interface Ethernet1/1
description PC_4
switchport mode Access
switchport access vlan 100
spanning-tree portfast edge

```
interface Ethernet1/0
 description PC_3
 switchport access vlan 101
 switchport mode access
 spanning-tree bpduguard enable
end

A1#sh run int Et1/1
Building configuration...

Current configuration : 155 bytes
!
interface Ethernet1/1
 description PC_4
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
end

A1#
```

Ilustración 17 A1 Interfaz PC3 y PC4

Tarea 2.7

Verifique los servicios DHCP IPv4.
PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

Se ingresa a los PC2 y PC3, se valida que ip tienen asignada, si no tienen con el comando ip dhcp obtendrían una por DHCP

PC3>ip dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254

PC2>ip dhcp
DDORA IP 10.0.102.110/24 GW 10.0.102.254

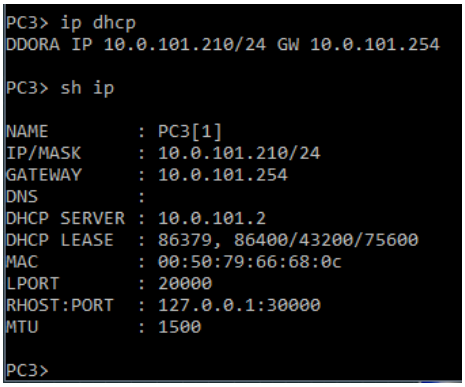

Ilustración 18 IP DHCP PC3

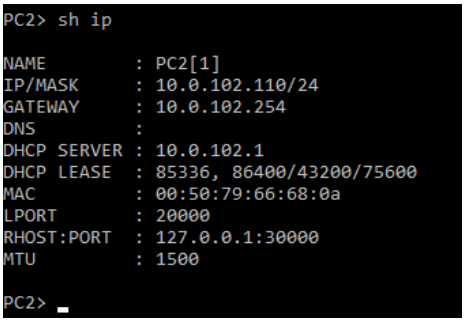

Ilustración 19 IP DHCP PC2

Tarea 2.8
Verifique la conectividad de la LAN local
PC1 debería hacer ping con éxito a:
D1: 10.0.100.1
D2: 10.0.100.2
PC4: 10.0.100.6

```
PC1> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.428 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.707 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.098 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.477 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.519 ms

PC1> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=2.392 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.018 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.992 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.134 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.989 ms

PC1> ping 10.0.100.6

84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=4.813 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.154 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.186 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.257 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.332 ms
```

Ilustración 20 Ping desde PC1

PC2 debería hacer ping con éxito a:
D1: 10.0.102.1
D2: 10.0.102.2

```
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.291 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=2.604 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=2.134 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.116 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.301 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.546 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=1.197 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.711 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.742 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=1.439 ms
```

Ilustración 21 Ping desde PC2

PC3 debería hacer ping con éxito a:
D1: 10.0.101.1
D2: 10.0.101.2

```
PC3> ping 10.0.101.1

84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.795 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.952 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.006 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.600 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.852 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=4.853 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=1.301 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=3.820 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=1.311 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=1.577 ms
```

Ilustración 22 Ping desde PC3

PC4 debería hacer ping con éxito a:
D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5

```
PC4> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=67.127 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.033 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.871 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=20.141 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=2.202 ms

PC4> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=4.199 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=25.551 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=2.102 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=2.671 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=2.413 ms

PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.946 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=1.120 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.264 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.503 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.304 ms
```

Ilustración 23 Ping desde PC4

Parte 3: Configurar los protocolos de enrutamiento

Tarea 3.1
En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single área OSPFv2 en area 0.
Use OSPF Process ID 4 y asigne los siguientes routerIDs:
R1: 0.0.4.1
R3: 0.0.4.3
D1: 0.0.4.131
D2: 0.0.4.132
En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.
En R1, no publique la red R1 – R2.
En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en:
D1: todas las interfaces excepto G1/0/11
D2: todas las interfaces excepto G1/0/11

Se debe habilitar el enrutamiento OSPF, colocar el router-id correspondiente, se anuncian las rutas conectadas directamente, en el área 0, se deshabilitan la interfaces que no deben procesar paquetes OSPF.

R1(config)# router ospf 4
router-id 0.0.4.1
network 10.0.13.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0

```
R1#sh run | section router ospf
router ospfv3 6
 router-id 0.0.6.1
 !
 address-family ipv6 unicast
 exit-address-family
router ospf 4
 router-id 0.0.4.1
 network 10.0.10.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.255 area 0
R1#
```

Ilustración 24 R1 configuracion OSPF y OSPFv3

R3(config)# router ospf 4
router-id 0.0.4.3
network 10.0.13.0 0.0.0.255 area 0

network 10.0.11.0 0.0.0.255 area 0

```
R3#sh run | sec
R3#sh run | section router ospf
router ospfv3 6
 router-id 0.0.6.3
 !
 address-family ipv6 unicast
  router-id 0.0.6.3
 exit-address-family
router ospf 4
 router-id 0.0.4.3
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.255 area 0
```

Ilustración 25 R3 configuracion OSPF y OSPFv3

D1(config)# router ospf 4
router-id 0.0.4.131
network 0.0.0.0 0.0.0.0 area 0
passive-interface po12
passive-interface po1
passive-interface e1/3

```
D1#sh run | section router ospf
router ospfv3 6
 !
 address-family ipv6 unicast
  router-id 0.0.6.131
 exit-address-family
router ospf 4
 router-id 0.0.4.131
 passive-interface Ethernet1/3
 passive-interface Port-channel1
 passive-interface Port-channel12
 network 0.0.0.0 255.255.255.255 area 0
```

Ilustración 26 D1 configuracion OSPF y OSPFv3

D2(config)# router ospf 4
router-id 0.0.4.132
network 0.0.0.0 0.0.0.0 area 0
passive-interface po12
passive-interface po1
passive-interface e1/3

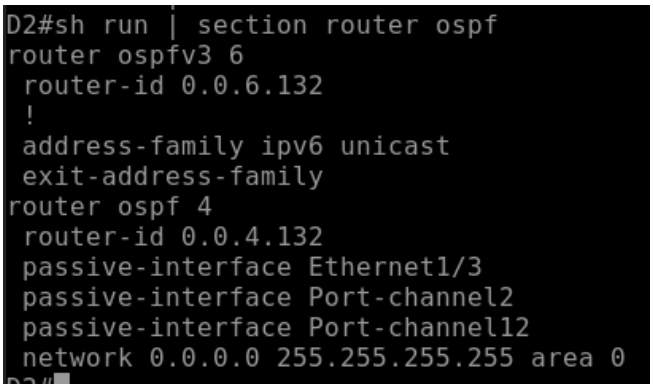

Ilustración 27 D2 configuracion OSPF y OSPFv3

Tarea 3.2
En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.
Use OSPF Process ID 6 y asigne los siguientes routerIDs:
R1: 0.0.6.1
R3: 0.0.6.3
D1: 0.0.6.131
D2: 0.0.6.132
En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.
En R1, no publique la red R1 – R2.
En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en:
Se debe habilitar el enrutamiento OSPF para ipv6, colocar el router-id correspondiente, se anuncian las rutas conectadas directamente, en el área 0, se deshabilitan la interfaces que no deben procesar paquetes OSPF.

R1(config)# router ospfv3 6
router-id 0.0.6.1
R1(config)# Interface e0/3
ospfv3 6 ipv6 area 0
R1(config)# Interface e0/1
ospfv3 6 ipv6 area 0

R3(config)# router ospfv3 6
router-id 0.0.6.3
R3(config)# Interface e0/3
ospfv3 6 ipv6 area 0
R1(config)# Interface e0/1
ospfv3 6 ipv6 area 0

```
D1(config)# router  ospfv3 6
router-id 0.0.6.131

Interface e0/1
ospfv3 6 ipv6 area 0

interface vlan 100
ospfv3 6 ipv6 area 0

interface vlan 101
ospfv3 6 ipv6 area 0

interface vlan 102
ospfv3 6 ipv6 area 0

interface po12
passive-interface
interface po1
passive-interface
interface e1/3
passive-interface


D2(config)# router  ospfv3 6
router-id 0.0.6.132
interface po12
passive-interface
interface po1
passive-interface
interface e1/3
passive-interface

Interface e0/1
ospfv3 6 ipv6 area 0

interface vlan 100
ospfv3 6 ipv6 area 0

interface vlan 101
ospfv3 6 ipv6 area 0

interface vlan 102
```

ospfv3 6 ipv6 area 0

Tarea 3.3
En R2 en la “Red ISP”, configure MP-BGP.
Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
Una ruta estática predeterminada IPv4.
Una ruta estática predeterminada IPv6.
Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.
Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.
En IPv4 address family, anuncie:
La red Loopback 0 IPv4 (/32).
La ruta por defecto (0.0.0.0/0).
En IPv6 address family, anuncie:
La red Loopback 0 IPv4 (/128).
La ruta por defecto (::/0)

R2(config)#ip route 0.0.0.0 0.0.0.0
R2(config)#ipv6 route ::/0

R2(config)# router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
address family ipv4
network 2.2.2.2 255.255.255.255
network 0.0.0.0 mask 0.0.0.0
default information-originate
neighbor 209.165.200.225 activate
address family ipv6
network 2001:db8:2222::1/128
network ::/0
default information-originate

```
R2#sh run | sec
R2#sh run | section router bgp
router bgp 500
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 209.165.200.225 remote-as 300
 !
 address-family ipv4
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  neighbor 209.165.200.225 activate
  default-information originate
 exit-address-family
 !
 address-family ipv6
  default-information originate
  network ::/0
  network 2001:DB8:2222::1/128
 exit-address-family
```

Ilustración 28 R2 Configuracion BGP

Tarea 3.4
En R1 en la “Red ISP”, configure MP-BGP.
Configure dos rutas resumen estáticas a la interfaz Null 0:
Una ruta resumen IPv4 para 10.0.0.0/8.
Una ruta resumen IPv6 para 2001:db8:100::/48.
Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.
Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.
En IPv4 address family:
Deshabilite la relación de vecino IPv6.
Habilite la relación de vecino IPv4.
Anuncie la red 10.0.0.0/8.
En IPv6 address family:
Deshabilite la relación de vecino IPv4.
Habilite la relación de vecino IPv6.
Anuncie la red 2001:db8:100::/48.

R1(config)#ip route 0.0.0.0 0.0.0.0
R1(config)#ipv6 route ::/0

R1(config)# router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
address family ipv4
network 10.0.0.0 mask 255.0.0.0

neighbor 209.165.200.226 activate
address family ipv6
Network 2001:db8:100::/48

```
R1#sh run | section router bgp
router bgp 300
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 209.165.200.226 remote-as 500
 !
 address-family ipv4
  network 10.0.0.0
  neighbor 209.165.200.226 activate
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8:100::/48
 exit-address-family
```

Ilustración 29 R1 Configuracion BGP

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

Tarea 4.1
En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.
Cree dos IP SLAs.
Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6.
Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.
Programe la SLA para una implementación inmediata sin tiempo de finalización.
Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la IP SLA 6.
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D1(config)# ip sla 4
icmp-echo 10.0.10.1 source-interface e1/0
frequency 5
exit
D1(config)# ip sla schedule 4 start-time now life forever

D1(config)# ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
D1(config)# ip sla schedule 6 start-time now life forever

D1(config)# track 4 ip sla 4
delay down 10 up 15

D1(config)# track 6 ip sla 6
delay down 10 up 15
```

```
D1#sh run | section ip sla
track 4 ip sla 4
 delay down 15 up 10
track 6 ip sla 6
 delay down 15 up 10
ip sla 4
 icmp-echo 10.0.10.1 source-interface Ethernet1/0
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1010::1
 frequency 5
ip sla schedule 6 life forever start-time now
```

Ilustración 30 D1 SLA - Track

Tarea 4.2
En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.
Cree IP SLAs.
Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6.
Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.
Programe la SLA para una implementación inmediata sin tiempo de finalización.
Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la SLA 6.
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D2(config)# ip sla 4
icmp-echo 10.0.11.1 source-interface e1/0
frequency 5
exit
D2(config)# ip sla schedule 4 start-time now life forever

D2(config)# ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
D2(config)# ip sla schedule 6 start-time now life forever


D2(config)# track 4 ip sla 4
delay down 10 up 15

D2(config)# track 6 ip sla 6
delay down 10 up 15
```

```
D2#sh run | section ip sla
track 4 ip sla 4
 delay down 10 up 15
track 6 ip sla 6
 delay down 10 up 15
ip sla 4
 icmp-echo 10.0.11.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5
ip sla schedule 6 life forever start-time now
```

Ilustración 31 D2 SLA - Track

Tarea 4.3

En D1 configure HSRPv2.

D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decremente en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Registre el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 6 y decremente en 60.

```
D1(config)# int vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60

D1(config)# int vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60

D1(config)# int vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60

D1(config)# int vlan 100
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60

D1(config)# int vlan 101
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60

D1(config)# int vlan 102
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
```

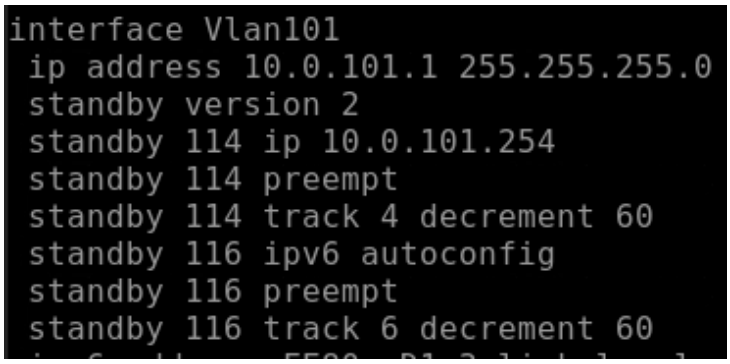

Ilustración 32 D1 HSRP

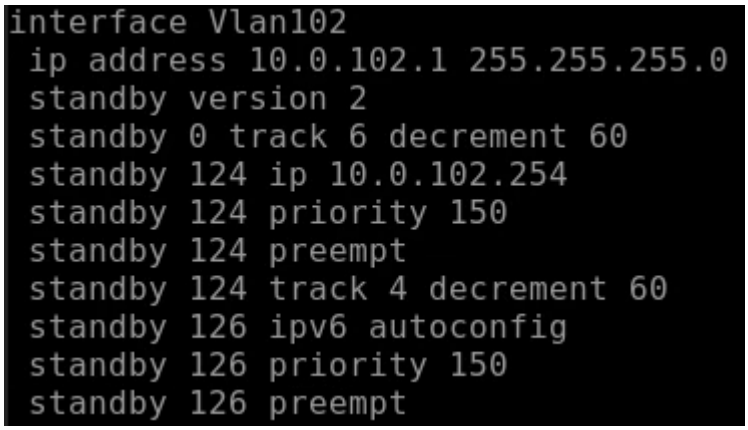

Ilustración 33 D1 HSRP .

Tarea 4.4
En D2, configure HSRPv2.
D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100:
Asigne la dirección IP virtual 10.0.100.254.
Habilite la preferencia (preemption).
Rastree el objeto 4 y decremente en 60.
Configure IPv4 HSRP grupo 114 para la VLAN 101:
Asigne la dirección IP virtual 10.0.101.254.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.
Configure IPv4 HSRP grupo 124 para la VLAN 102:
Asigne la dirección IP virtual 10.0.102.254.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.
Configure IPv6 HSRP grupo 106 para la VLAN 100:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.
Configure IPv6 HSRP grupo 116 para la VLAN 101:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 6 para disminuir en 60.
Configure IPv6 HSRP grupo 126 para la VLAN 102:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Habilite la preferencia (preemption).
Rastree el objeto 6 para disminuir en 60

D2(config)# int vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60

D2(config)# int vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60

D2(config)# int vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60

D2(config)# int vlan 100
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60

D2(config)# int vlan 101
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60

D2(config)# int vlan 102

standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60

```
interface Vlan101
 ip address 10.0.101.2 255.255.255.0
 standby version 2
 standby 114 ip 10.0.101.254
 standby 114 priority 150
 standby 114 preempt
 standby 114 track 4 decrement 60
 standby 116 ipv6 autoconfig
 standby 116 priority 150
 standby 116 preempt
 standby 116 track 6 decrement 60
```

Ilustración 34 D2 HSRP

```
interface Vlan102
 ip address 10.0.102.2 255.255.255.0
 standby version 2
 standby 0 track 4 decrement 60
 standby 124 ip 10.0.102.254
 standby 124 preempt
 standby 126 ipv6 autoconfig
 standby 126 preempt
 standby 126 track 6 decrement 60
```

Ilustración 35 D1 HSRP .

Parte 5: Seguridad

Tarea 5.1
En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.
Contraseña: cisco12345cisco

```
R1(config)# enable algorithm-type scrypt secret cisco12345cisco

R2(config)# enable algorithm-type scrypt secret cisco12345cisco

R3(config)# enable algorithm-type scrypt secret cisco12345cisco

D1(config)# enable algorithm-type scrypt secret cisco12345cisco

D2(config)# enable algorithm-type scrypt secret cisco12345cisco

A1(config)# enable algorithm-type scrypt secret cisco12345cisco
```

Tarea 5.2
En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.
Detalles de la cuenta encriptada SCRYPT:
Nombre de usuario Local: sadmin
Nivel de privilegio 15
Contraseña: cisco12345cisco

```
R1(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco

R2(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco

R3(config)# username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco

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

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

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

Tarea 5.3
En todos los dispositivos (excepto R2), habilite AAA.
Habilite AAA

R1(config)# aaa new-model

R3(config)# aaa new-model

D1(config)# aaa new-model

D2(config)# aaa new-model

A1(config)# aaa new-model

```
enable secret 9 $9$IRGbf60q2cmkkd$V4xAQ4qbAnYwuFWXMQpTXRIluh4e4I1kzkZsu/VNkH6
!
username sadmin privilege 15 secret 9 $9$TnYJV9Lm5ssGu7$AzX9fWmsyN5sFRsUgH3NgfDMqw7iE/hIgMCts8HLqE6
aaa new-model
!
!
!
!
!
!
!
!
aaa session-id common
clock timezone UTC -5 0
```

Ilustración 36 RO Username - enable - AAA -

```
enable secret 9 $9$C7Ib9UcZFG2JlH$2MLT9kwkXNn2W00PMWxvyc2y81EX/Gp7iq0Qr9WNGkI
!
username sadmin privilege 15 secret 9 $9$I3G9B.MGAkgf01$6FvNdk2aNENvGhfNZiE/6pXQwj72Wt96juAIyNLX9x6
aaa new-model
!
!
!
!
!
!
!
!
aaa session-id common
clock timezone UTC -5 0
```

Ilustración 37 Sw RO Username - enable - AAA

Tarea 5.4
En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.
Especificaciones del servidor RADIUS.:
Dirección IP del servidor RADIUS es 10.0.100.6.
Puertos UDP del servidor RADIUS son 1812 y 1813.
Contraseña: $trongPass

R1(config)# radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass

R3(config)# radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass

D1(config)# radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass

D2(config)# radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass

A1(config)# radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass

Tarea 5.5
En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA
Especificaciones de autenticación AAA:
Use la lista de métodos por defecto
Valide contra el grupo de servidores RADIUS
De lo contrario, utilice la base de datos local.

R1(config)# aaa authentication login default group radius local

R3(config)# aaa authentication login default group radius local

D1(config)# aaa authentication login default group radius local

D2(config)# aaa authentication login default group radius local

A1(config)# aaa authentication login default group radius local

Tarea 5.6

Verifique el servicio AAA en todos los dispositivos (except R2).
Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

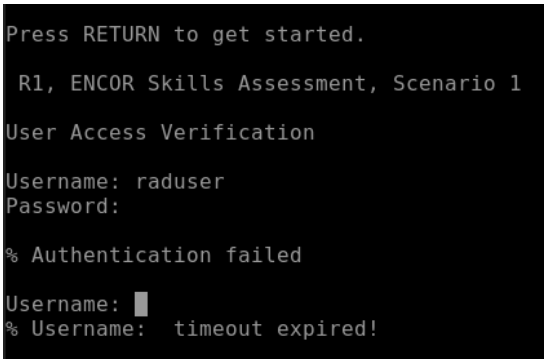

Ilustración 38 Acceso R1usuario raduser

Nota: A pesar de que en cada dispositivo se configuro el usuario y password no es posible que el sw solicite usuario luego del reinicio del equipo

Ilustración 39Configuracion de username

Parte 6: Configure las funciones de Administración de Red

Tarea 6.1
En todos los dispositivos, configure el reloj local a la hora UTC actual.
Configure el reloj local a la hora UTC actual.

R1(config)# clock timezone UTC -5

R2(config)# clock timezone UTC -5

R3(config)# clock timezone UTC -5

D1(config)# clock timezone UTC -5

D2(config)# clock timezone UTC -5

A1(config)# clock timezone UTC -5

Tarea 6.2
Configure R2 como un NTP maestro.
Configurar R2 como NTP maestro en el nivel de estrato 3

R2(config)# ntp master 3

Tarea 6.3
Configure NTP en R1, R3, D1, D2, y A1.
Configure NTP de la siguiente manera:
R1 debe sincronizar con R2.
R3, D1 y A1 para sincronizar la hora con R1.
D2 para sincronizar la hora con R3.

R1(config)# ntp server 209.165.200.226

R3(config)# ntp server 10.0.13.1

D1(config)# ntp server 10.0.10.1

D2(config)# ntp server 10.0.11.1

A1(config)# ntp server 10.0.10.1

Tarea 6.4
Configure Syslog en todos los dispositivos excepto R2
Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

R1(config)# logging 10.0.100.5
logging trap warnings

R3(config)# logging 10.0.100.5
logging trap warnings

D1(config)# logging 10.0.100.5
logging trap warnings

D2(config)# logging 10.0.100.5
logging trap warnings

A1(config)# logging 10.0.100.5
logging trap warnings

Tarea 6.5
Configure SNMPv2c en todos los dispositivos excepto R2
Especificaciones de SNMPv2:
Unicamente se usará SNMP en modo lectura (Read-Only).
Limite el acceso SNMP a la dirección IP de la PC1.
Configure el valor de contacto SNMP con su nombre.
Establezca el community string en ENCORSA.
En R3, D1, y D2, habilite el envío de traps config y ospf.
En R1, habilite el envío de traps bgp, config, y ospf.
En A1, habilite el envío de traps config.

R1(config)# ip access-list standard SNMP
permit host 10.0.100.5
snmp-server contact Javier_Hurtado_Perez
snmp-server community ENCORSA ro SNMP
snmp-server host 10.0.100.5 version 2 ENCORSA
snmp-server enable traps bgp
snmp-server enable traps ospf

R3(config)# ip access-list standard SNMP
permit host 10.0.100.5

snmp-server contact Javier_Hurtado_Perez
snmp-server community ENCORSA ro SNMP
snmp-server host 10.0.100.5 version 2 ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf

D1(config)# ip access-list standard SNMP
permit host 10.0.100.5
snmp-server contact Javier_Hurtado_Perez
snmp-server community ENCORSA ro SNMP
snmp-server host 10.0.100.5 version 2 ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf

D2(config)# ip access-list standard SNMP
permit host 10.0.100.5
snmp-server contact Javier_Hurtado_Perez
snmp-server community ENCORSA ro SNMP
snmp-server host 10.0.100.5 version 2 ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf

A1(config)# ip access-list standard SNMP
permit host 10.0.100.5
snmp-server contact Javier_Hurtado_Perez
snmp-server community ENCORSA ro SNMP
snmp-server host 10.0.100.5 version 2 ENCORSA
snmp-server enable traps

```
!
logging trap warnings
logging host 10.0.100.5
ipv6 route 2001:DB8:100::/48 Null0
ipv6 ioam timestamp
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Javier_Hurtado_Perez
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bgp
snmp-server host 10.0.100.5 version 2c ENCORSA
!
```

Ilustración 40 R1 SNMP y Traps

```
logging trap warnings
logging host 10.0.100.5
ipv6 ioam timestamp
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Javier_Hurtado_Perez
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
!
```

Ilustración 41 R3 SNMP y Traps

```
ip access-list standard SNMP
 permit 10.0.100.5
!
!
ip sla 4
 icmp-echo 10.0.10.1 source-interface Ethernet1/0
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1010::1
 frequency 5
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Javier_Hurtado_Perez
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
```

Ilustración 42 D1 SNMP y Traps

```
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ip access-list standard SNMP
 permit 10.0.100.5
!
!
ip sla 4
 icmp-echo 10.0.11.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Javier_Hurtado_Perez
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
```

Ilustración 43 D2 SNMP y Traps

```
!
ip access-list standard SNMP
 permit 10.0.100.5
!
!
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Javier_Hurtado_Perez
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
```

Ilustración 44 A1 SNMP y Traps

CONCLUSIONES

Es muy enriquecedor este proceso de implementación de un escenario en el cual se puedan poner en practica las habilidades adquiridas a lo largo del curso en simuladores de redes lo que nos da un acercamiento a la configuración de dispositivos reales ya que se maneja el mismo software que encontraremos en estos dispositivos y así podemos afianzar el manejo de los diferentes comandos sobre el software.

Es muy importante complementar los conocimientos previamente adquiridos a lo largo de la experiencia y el desarrollo de los cursos anteriores de CCNA y poder complementarlos con el temario visto en CCNP nos permite una proyección mucho mas avanzada en el dominio de los temas mucho mas complejos que puedan presentarse en el campo profesional.

Realizar el desarrollo parctico del escenario propuesto fue una experiencia significativa puesto que nos enfrenta a topologías mas complejas que se encuentran en muchas compañías que cuentan con este tipo de dispositivos los cuales tienen una configuración mas compleja y requiere del conocimiento de los diferentes conceptos y protocolos para una correcta aplicación de los mismos en torno a un requerimiento especifico que pueda tener la compañía.

Por medio de este trabajo se pudo poner en practica lo aprendido durante el diplomado CCNP y se lograron desarrollar diferentes habilidades en la configuración tanto de switch como de routers y los diferentes protocolos que pueden aplicarse a cada uno de estos dispositivos para que cumplan un fin especifico dentro de nuestra red y así brindar un soporte confiable convergente y de alta disponibilidad para lograr así un optimo desempeño de la red en el momento de una implementación real.

BIBLIOGRAFIA

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

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

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

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

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC