

**SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO**

WESTHLY JOSE SARABIA CARRILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE TELECOMUNICACIONES*
VALLEDUPAR
2021

**SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO**

WESTHLY JOSE SARABIA CARRILLO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *TELECOMUNICACIONES*
VALLEDUPAR
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

VALLEDUPAR, 14 de noviembre de 2021

AGRADECIMIENTO

Tras un largo periodo académico, de muchas noches largas y traspasadas conjuntas, el día de hoy presento mis más sinceros agradecimientos para finalizar de manera satisfactoria mi trabajo de grado. Al nivel personal y académico ha sido una etapa de aprendizaje muy fructuoso, por tal motivo quiero agradecer a toda mi familia, quienes en los momentos más difíciles me han brindado ayuda y apoyo emocional incondicional, para culminar con éxito esta etapa académica.

Además, me gustaría agradecer a mis tutores y directores de cursos, porque me han ayudado en la resolución de problemas que se han presentado alrededor de esta etapa ofreciéndome herramientas necesarias para completar mi proyecto, con su dedicación, paciencia y compromiso, ayudándome hacer una mejor persona a la que inicio los estudios en la Universidad Nacional Abierta y a Distancia.

CONTENIDO

AGRADECIMIENTO.....	4
CONTENIDO.....	5
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN	9
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO.....	11
ESCENARIO 1	11
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES	12
PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST	19
PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO	23
PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO (FIRST HOP REDUNDANCY).....	28
PARTE 5: SEGURIDAD - En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.....	33
PARTE 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED.....	35
CONCLUSIÓN	40
BIBLIOGRAFIA	41

LISTA DE FIGURAS

Figura 1. Escenario 1	11
Figura 2. Simulación en GNS3 del escenario 1	12
Figura 3. Asignación de direcciones IP al PC 1 y PC4.....	18
Figura 4. Verificación de los clientes DHCP en PC2 y PC3	21
Figura 5. Verificación de conectividad PC1	21
Figura 6. Verificación de conectividad PC2.....	21
Figura 7. Verificación de conectividad PC3.....	22
Figura 8. Verificación de conectividad PC4.....	23
Figura 9. Configuración ospfv3 R1	24
Figura 10. Configuración ospfv3 R1	25
Figura 11. Configuración ospfv3 R1	25
Figura 12. Configuración ospfv3 R1	25
Figura 13. Configuración del área 0 en R3.....	25
Figura 14. Configuración del área 0 en R1.....	25
Figura 15: configuración y verificación del reloj local	36
Figura 16: configuración y verificación del server NTP en R1	36
Figura 17: configuración y verificación del server NTP en R3.....	36
Figura 18: configuración y verificación del server NTP en D1	36
Figura 19: configuración y verificación del server NTP en A1	37
Figura 20: configuración y verificación del server NTP en D2.....	37

GLOSARIO

DHCP: El Servidor DHCP, de sus siglas en ingles Dynamic Host configuration Protocol, es un servidor de Red el cual permite una asignación automática de direcciones IP, gateways predeterminadas, así como otros parámetros de red que necesiten los clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red. Tomado de: (*Glosario- Qué es DHCP y Para qué Sirve*, s. f.)

OSPF: Open Shortest Path First (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo. Tomado de: (Fernández, s. f.).

MP-BGP: El MP-BGP es un BGP extendido que permite que el BGP lleve la información de ruteo para el IPv6, el VPNv4, y otros de los protocolos de capa de la Red múltiple. El MP-BGP permite que usted tenga una topología del Unicast Routing diferente de una topología del ruteo multicast, que ayuda a controlar la red y los recursos. Tomado de (*Ejemplo de Configuración MP-EBGP*, s. f.).

IP SLA: Un IP SLA o Internet Protocol Service Level Agreement, es una función que te permite monitorear la conectividad por red de uno o múltiples nodos donde sea que estos se encuentren (y sean alcanzables). Tomado de (Gabriel, 2020)

HSRPv2: es un protocolo exclusivo de Cisco diseñado para permitir la conmutación por falla transparente de un dispositivo IPv4 de primer salto, aumenta la cantidad de grupos admitidos. La versión 1 de HSRP admite los números de grupo de 0 a 255. La versión 2 de HSRP admite los números de grupo de 0 a 4095 e incorpora la compatibilidad para autenticación MD5. Tomado de («HSRP Protocolo de Routing de reserva activa», s. f.)

Encriptación Script: provienen de un gran vector de cadenas de bits pseudoaleatorias que se generan como parte del algoritmo. Una vez que se genera el vector, se accede a sus elementos en un orden pseudoaleatorio y se combinan para producir la clave derivada. Tomado de (*Algoritmo Script: programador de clics*, s. f.)

AAA: La arquitectura AAA permite el acceso de los usuarios legítimos a los activos conectados a la red e impide el acceso no autorizado. Tomado de (*Uso de seguridad AAA para la administración de equipos de Conectividad*, s. f.).

IOS: Cisco IOS es el software utilizado en la gran mayoría de routers y switches de Cisco Systems. IOS es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo multitarea. Tomado de («Cisco IOS», 2020)

RESUMEN

En el informe que se presenta, la aplicación de un escenario en donde es solucionado con conocimientos adquiridos a través del diplomado de CISCO prueba de habilidades practicas CCNP, en ello se involucra un entorno empresarial, y la configuración de dispositivos de redes mediante los lineamientos de enrutamiento y conmutación, tales como las familias OSPF, DHCP, NTP entre otros, y el uso del servidor RADIUS y su autenticación aaa. Se llevará acabo el estudio de la parte electrónica de los dispositivos, ya que algunos no podrán realizar algunos comandos necesarios para el total desarrollo del escenario. Este informe se divide por parte, en donde describe que se realizara en cada parte, proporcionando con más claridad la utilización de comandos y la descripción de cada uno.

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

ABSTRACT

In the report that is presented, the application of a scenario where it is solved with knowledge acquired through the CISCO diploma test of practical skills CCNP, in which a business environment is involved, and the configuration of networking devices through the guidelines of routing and switching, such as the OSPF, DHCP, NTP families among others, and the use of the RADIUS server and its aaa authentication. The study of the electronic part of the devices will be carried out since some will not be able to carry out some commands necessary for the total development of the scenario. This report is divided by part, where it describes what will be done in each part, it contains more clarity on the use of commands and the description of each one.

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

INTRODUCCIÓN

En la actualidad el mundo se mueve alrededor de las tecnologías y prácticamente todo esta conectado, ya sea a internet o a una red privada, de igual forma las telecomunicaciones han dado un gran giro en el siglo XXI y según los acontecimientos más comunes evolucionara. Existen redes LAN, WAN PAN entre otras, y una es más grande que la otra, esto quiere decir implica una distancia mayor entre dispositivos, en esta ocasión se trabajara y explicara como se crea una red WAN de una empresa, llevando consigo los protocolos de seguridad, enrutamiento, conmutación y autenticación para que sea una red fiable. Siendo así, existen 6 partes en donde se divide este informe.

En nuestra parte uno se presentará la realización de la topología indicada, y la configuración básica de los dispositivos, de igualmente con sus respectivas configuraciones en las interfaces. En la parte 2, se llevará a cabo la configuración de la capa 2 de los dispositivos de red y el soporte de host, en donde se incluirán, la configuración y asignación de vlan, los enlaces troncales, implementación de protocolos RSTP, servicios de DHCP, creación de puertos de canales, y asignación de root primarios en los dispositivos. En la parte 3, se procederá a configurar los protocolos de enrutamientos, tales como OSPF con la asignación de área correspondiente y MP-BGP.

Entrando en la parte 4, se configurará la redundancia del primer salto IP SLA, Usando dos SLA una para las direcciones ipv4 y la otra para direcciones ipv6, de igual forma también se configurará los servicios de HSRPv2 en los dispositivos D1 y D2, con la implementación necesaria. Siguiendo a la parte 5, se procede a configuración de la seguridad de los dispositivos, en donde habilitamos el servicio aaa, y a su vez configurando el servidor RADIUS. En la parte 6, se procede a configurar las funciones administrativas de red, en donde se lleva a cabo la configuración de la hora de los dispositivos, el servidor NTP, el servidor Syslog y el servicio de SNMPv2c exceptuando el router R2.

DESARROLLO

ESCENARIO 1

Topología de la Red:

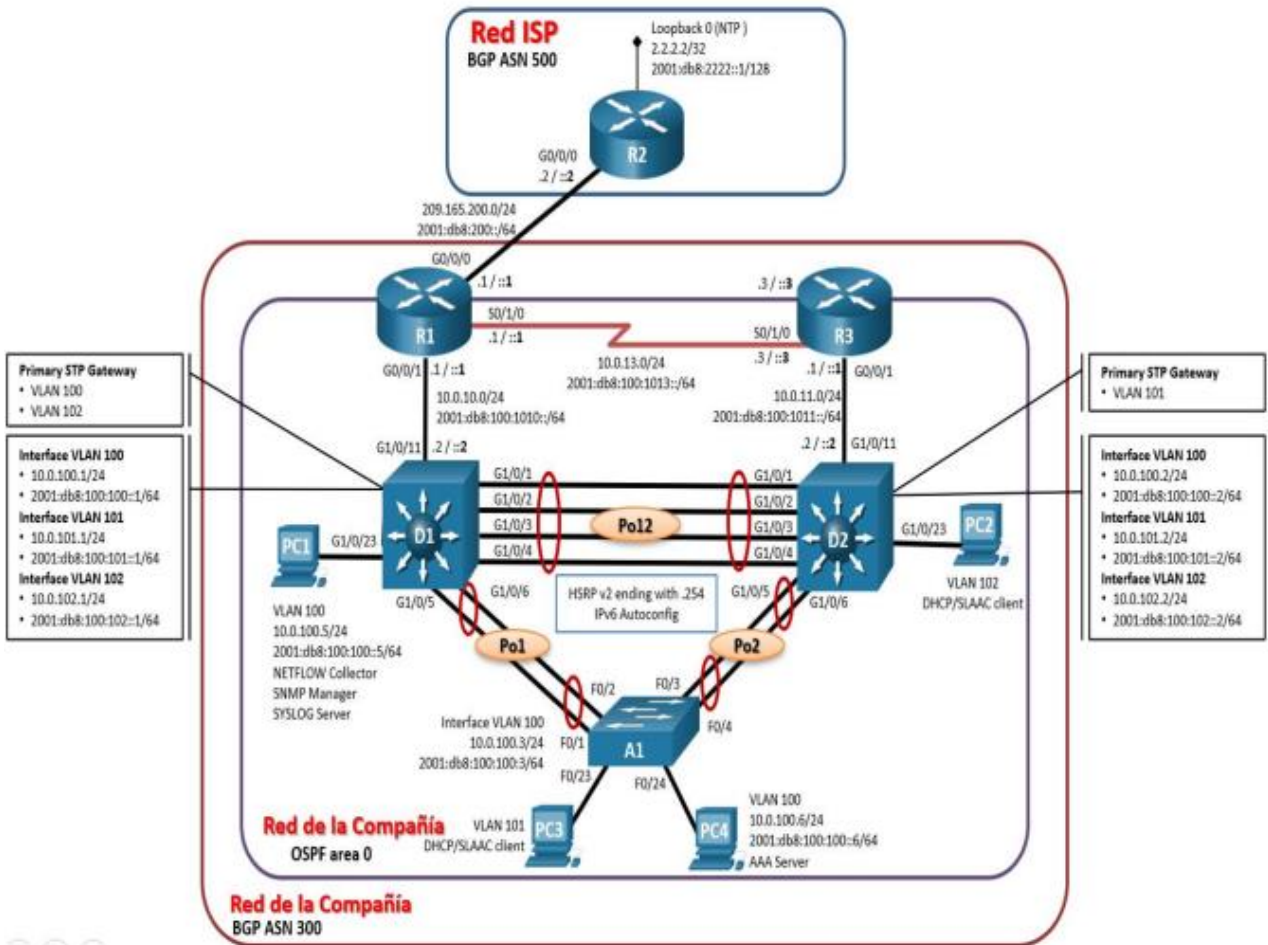


Figura 1. Escenario 1

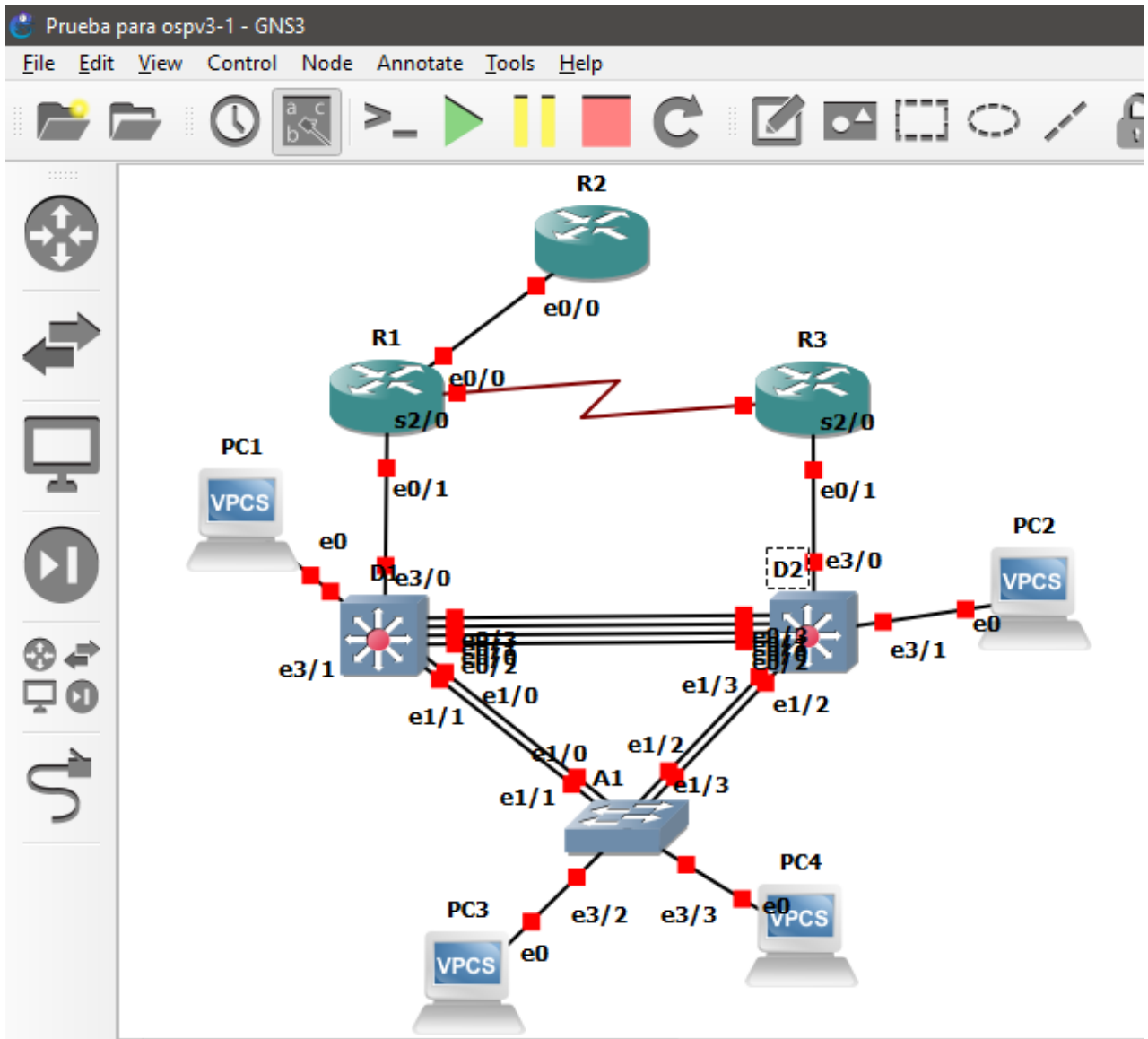


Figura 2. Simulación en GNS3 del escenario 1

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES

Configurar los parámetros básicos para cada dispositivo.

- Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos.

Router R1

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)# ipv6 unicast-routing
R1(config)-# no ip domain lookup
R1(config)-# banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)-# line con 0
R1(config-line)# exec-timeout 0 0
R1(config-line)# logging synchronous
R1(config-line)#exit
R1(config)-#interface e0/0
R1(config-if)-# ip address 209.165.200.225 255.255.255.224
R1(config-if)-# ipv6 address fe80::1:1 link-local
R1(config-if)-# ipv6 address 2001:db8:200::1/64
R1(config-if)-# no shutdown
R1(config-if)-#exit
R1(config)-#interface e0/1
R1(config-if)-# ip address 10.0.10.1 255.255.255.0
R1(config-if)-# ipv6 address fe80::1:2 link-local
R1(config-if)-# ipv6 address 2001:db8:100:1010::1/64
R1(config-if)-# no shutdown
R1(config-if)-#exit
R1(config)-#interface s2/0
R1(config-if)-# ip address 10.0.13.1 255.255.255.0
R1(config-if)-# ipv6 address fe80::1:3 link-local
R1(config-if)-# ipv6 address 2001:db8:100:1013::1/64
R1(config-if)-# no shutdown
R1(config-if)-#exit
R1(config)-#end
Router#copy running-config startup-config
```

Router R2

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)# ipv6 unicast-routing
R2(config)-# no ip domain lookup
R2(config)-# banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)-# line con 0
R2(config-line)# exec-timeout 0 0
R2(config-line)# logging synchronous
```

```
R2(config-line)#exit
R2(config)#interface e0/0
R2(config-if)# ip address 209.165.200.226 255.255.255.224
R2(config-if)# ipv6 address fe80::2:1 link-local
R2(config-if)# ipv6 address 2001:db8:200::2/64
R2(config-if)# no shutdown
R2(config-if)#exit
R2(config)#interface Loopback 0
R2(config-if)# ip address 2.2.2.2 255.255.255.255
R2(config-if)# ipv6 address fe80::2:3 link-local
R2(config-if)# ipv6 address 2001:db8:2222::1/128
R2(config-if)# no shutdown
R2(config-if)#end
R2#copy running-config startup-config
```

Router R3

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)# ipv6 unicast-routing
R3(config)# no ip domain lookup
R3(config)# banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)# line con 0
R3(config-line)# exec-timeout 0 0
R3(config-line)# logging synchronous
R3(config-line)#exit
R3(config)#interface e0/0
R3(config-if)# ip address 10.0.11.1 255.255.255.0
R3(config-if)# ipv6 address fe80::3:2 link-local
R3(config-if)# ipv6 address 2001:db8:100:1011::1/64
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)#interface s2/0
R3(config-if)# ip address 10.0.13.3 255.255.255.0
R3(config-if)# ipv6 address fe80::3:3 link-local
R3(config-if)# ipv6 address 2001:db8:100:1010::2/64
R3(config-if)# no shutdown
R3(config-if)#end
R2#copy running-config startup-config
```

Switch D1

```
IOU1>
IOU1>enable
IOU1#configure terminal
```

```

IOU1 (config)#hostname D1
D1(config)# ipv6 unicast-routing
D1(config)-# no ip domain lookup
D1(config)-# banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)-# line con 0
D1(config-line)# exec-timeout 0 0
D1(config-line)# logging synchronous
D1(config-line)#exit
D1(config)-#vlan 100
D1(config-vlan)-#name Management
D1(config-vlan)-#exit
D1(config)-#vlan 101
D1(config-vlan)-#name UserGroupA
D1(config-vlan)-#exit
D1(config)-#vlan 102
D1(config-vlan)-#name UsergroupB
D1(config-vlan)-#exit
D1(config)-#vlan 999
D1(config-vlan)-#name Native
D1(config-vlan)-#exit
D1(config)-#interface e3/0
D1(config-if)-#no switchport
D1(config-if)-# ip address 10.0.100.1 255.255.255.0
D1(config-if)-# ipv6 address fe80::d1:2 link-local
D1(config-if)-# ipv6 address 2001:db8:100:100::1/64
D1(config-if)-# no shutdown
D1(config-if)-#exit
D1(config)-#interface vlan 101
D1(config-if)-# ip address 10.0.101.1 255.255.255.0
D1(config-if)-# ipv6 address fe80::d1:3 link-local
D1(config-if)-# ipv6 address 2001:db8:100:101::1/64
D1(config-if)-# no shutdown
D1(config-if)-#exit
D1(config)-#interface vlan 102
D1(config-if)-# ip address 10.0.102.1 255.255.255.0
D1(config-if)-# ipv6 address fe80::d1:4 link-local
D1(config-if)-# ipv6 address 2001:db8:100:102::1/64
D1(config-if)-# no shutdown
D1(config-if)-#exit
D1(config)-#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)-#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)-#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)-#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)-#ip dhcp pool VLAN-101
D1(dhcpo-config)-#network 10.0.101.0 255.255.255.0
D1(dhcpo-config)-#default-router 10.0.101.254
D1(dhcpo-config)-#exit

```

```
D1(config)-#ip dhcp pool VLAN-102
D1(dhcpo-config)-#network 10.0.102.0 255.255.255.0
D1(dhcpo-config)-#default-router 10.0.102.254
D1(dhcpo-config)-#end
D1#copy running-config startup-config
```

Switch D2

```
IOU1>
IOU1>enable
IOU1#configure terminal
IOU1 (config)#hostname D2
D2(config)# ipv6 unicast-routing
D2(config)-# no ip domain lookup
D2(config)-# banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)-# line con 0
D2(config-line)# exec-timeout 0 0
D2(config-line)# logging synchronous
D2(config-line)#exit
D2(config)-#vlan 100
D2(config-vlan)-#name Management
D2(config-vlan)-#exit
D2(config)-#vlan 101
D2(config-vlan)-#name UserGroupA
D2(config-vlan)-#exit
D2(config)-#vlan 102
D2(config-vlan)-#name UsergroupB
D2(config-vlan)-#exit
D2(config)-#vlan 999
D2(config-vlan)-#name Native
D2(config-vlan)-#exit
D2(config)-#interface e3/0
D2(config-if)-#no switchport
D2(config-if)-# ip address 10.0.11.2 255.255.255.0
D2(config-if)-# ipv6 address fe80::d1:1 link-local
D2(config-if)-# ipv6 address 2001:db8:100:1011::2/64
D2(config-if)-# no shutdown
D2(config-if)-#exit
D2(config)-#interface vlan 100
D2(config-if)-# ip address 10.0.100.2 255.255.255.0
D2(config-if)-# ipv6 address fe80::d2:2 link-local
D2(config-if)-# ipv6 address 2001:db8:100:100::2/64
D2(config-if)-# no shutdown
D2(config-if)-#exit
D2(config)-#interface vlan 101
D2(config-if)-# ip address 10.0.101.2 255.255.255.0
D2(config-if)-# ipv6 address fe80::d2:3 link-local
```

```

D2(config-if)-# ipv6 address 2001:db8:100:101::2/64
D2(config-if)-# no shutdown
D(config-if)-#exit
D2(config)-#interface vlan 102
D2(config-if)-# ip address 10.0.102.2 255.255.255.0
D2(config-if)-# ipv6 address fe80::d2:4 link-local
D2(config-if)-# ipv6 address 2001:db8:100:102::2/64
D2(config-if)-# no shutdown
D2(config-if)-#exit
D2(config)-#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)-#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)-#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D2(config)-#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)-#ip dhcp pool VLAN-101
D2(dhcpo-config)-#network 10.0.101.0 255.255.255.0
D2(dhcpo-config)-#default-router 10.0.101.254
D2(dhcpo-config)-#exit
D2(config)-#ip dhcp pool VLAN-102
D2(dhcpo-config)-#network 10.0.102.0 255.255.255.0
D2(dhcpo-config)-#default-router 10.0.102.254
D2(dhcpo-config)-#end
D2#copy running-config startup-config

```

Switch A1

```

IOU1>
IOU1>enable
IOU1#configure terminal
IOU1 (config)#hostname A1
A1(config)# ipv6 unicast-routing
A1(config)-# no ip domain lookup
A1(config)-# banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
A1(config)-# line con 0
A1(config-line)# exec-timeout 0 0
A1(config-line)# logging synchronous
A1(config-line)#exit
A1(config)-#vlan 100
A1(config-vlan)-#name Management
A1(config-vlan)-#exit
A1(config)-#vlan 101
A1(config-vlan)-#name UserGroupA
A1(config-vlan)-#exit
A1(config)-#vlan 102
A1(config-vlan)-#name UsergroupB
A1(config-vlan)-#exit
A1(config)-#vlan 999
A1(config-vlan)-#name Native

```



```

A1(config-vlan)-#exit
A1(config)-#interface vlan 100
A1(config-if)-# ip address 10.0.100.3 255.255.255.0
A1(config-if)-# ipv6 address fe80::a1:1 link-local
A1(config-if)-# ipv6 address 2001:db8:100:100::3/64
A1(config-if)-# no shutdown
A1(config-if)-#end
A1#copy running-config startup-config

```

- b. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos
- c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

```

PC1> ip 10.0.100.5/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show ipv6

NAME                : PC1[1]
LINK-LOCAL SCOPE    : fe80::250:79ff:fe66:6800/64
GLOBAL SCOPE        : 2001:db8:100:100::5/64
ROUTER LINK-LAYER   : aa:bb:cc:80:05:00
MAC                 : 00:50:79:66:68:00
LPORT               : 10004
RHOST:PORT          : 127.0.0.1:10005
MTU                 : 1500

PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> save
Saving startup configuration to startup.vpc
. done

PC4> show ipv6

NAME                : PC4[1]
LINK-LOCAL SCOPE    : fe80::250:79ff:fe66:6802/64
GLOBAL SCOPE        : 2001:db8:100:100::6/64
ROUTER LINK-LAYER   : aa:bb:cc:80:05:00
MAC                 : 00:50:79:66:68:02
LPORT               : 10008
RHOST:PORT          : 127.0.0.1:10009
MTU                 : 1500

```

Figura 3. Asignación de direcciones IP al PC 1 y PC4

PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST

2.1 Habilite enlaces trunk 802.1Q entre:

D1 and D2: D1(config-if)#interface range Ethernet0/0-3 (iniciamos configuración de las interfaces por rangos)

D1(config-if-range)#switchport trunk encapsulation dot1q (*cambiamos el tipo de encapsulación de las interfaces*)

D1(config-if-range)#switchport mode trunk (*activamos los puertos troncales en las interfaces*)

D1 and A1: D1(config)#interface rang e1/0-1

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

D2 and A1: D1(config)#interface rang e1/2-3

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

2.2 Use Vlan 999 como la VLAN nativa

D1(config-if-range)#interface range Ethernet0/0-3 (*iniciamos configuración de las interfaces por rangos*)

D1(config-if-range)#sw trunk native vlan 999 (*Usamos la VLAN 999 como vlan nativa*)

D1(config-if-range)#interface range Ethernet1/0-1

D1(config-if-range)#sw trunk native vlan 999

D2(config-if-range)#inte rang e0/0-3

D2(config-if-range)#sw trunk native vlan 999

D2(config-if-range)#inte rang e1/2-3

D2(config-if-range)#sw trunk native vlan 999

2.3 Use Rapid Spanning Tree (RSPT) en todos los swiches

D1(config)#spanning-tree mode rap (*se habilita el protocolo RSPT*)

D2(config)#spanning-tree mode rap

A1(config)#spanning-tree mode rap

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.

D1(config)#spanning-tree vlan 100 root primary (*Se configura la vlan 100 como root primaria*)

D1(config)#spanning-tree vlan 102 root primary (*Se configura la vlan 102 como root primaria*)

D2(config)#spanning-tree vlan 101 root primary (*Se configura la vlan 101 como root primaria*)

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

D1 a D2 – Port channel 12

```
D1(config)#inter range e0/0-3 (iniciamos configuración de las interfaces por rangos)
D1(config-if-range)#channel-protocol lacp (se activa el protocolo LACP)
D1(config-if-range)#channel-group 12 mode active (Se crea el grupo canal 12 y se active)
```

D1 a A1 – Port channel 1

```
D1(config)#inter range e1/0-1
D1(config-if-range)#channel-protocol lacp (se activa el protocolo LACP)
D1(config-if-range)#channel-group 1 mode active (Se crea el grupo canal 1 y se active)
```

D2 a A1 – Port channel 2

```
D2(config)#inter range e1/2-3
D2(config-if-range)#channel-protocol lacp (se activa el protocolo LACP)
D2(config-if-range)#channel-group 2 mode active (Se crea el grupo canal 2 y se active)
```

- 2.6 Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología

```
D1(config)#inter e3/1 (Se ingresa a la interface)
D1(config-if)#sw mode access (se active el modo de acceso)
D1(config-if)#sw access vlan 100 (Se asigna la VLAN 100 a la interface)
D1(config-if)#no shutdown (se enciende la interface)
```

```
D2(config)#inter e3/1
D2(config-if)#sw mode access (se active el modo de acceso)
D2(config-if)#sw access vlan 102 (Se asigna la VLAN 102 a la interface)
D2(config-if)#no shutdown
```

```
A1(config)#inter e3/2
A1(config-if)#sw mode access (se active el modo de acceso)
A1(config-if)#sw access vlan 101 (Se asigna la VLAN 101 a la interface)
A1(config-if)#no shutdown
A1(config-if)#inter e3/3
A1(config-if)#sw mode access (se active el modo de acceso)
A1(config-if)#sw access vlan 100 (Se asigna la VLAN 100 a la interface)
A1(config-if)#no shutdown
```

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

```
PC3> ip dhcp
DORRA IP 10.0.101.210/24 GW 10.0.101.254

PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254
```

2.8 Verificación de la conectividad LAN local

Figura 4. Verificación de los clientes DHCP en PC2 y PC3

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC4: 10.0.100.6

```
ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.400 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.701 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.706 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.741 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.811 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.951 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.898 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.948 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.047 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.978 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=14.784 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=18.566 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=16.501 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=14.396 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=12.488 ms
```

Figura 5. Verificación de conectividad PC1

PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

D2: 10.0.102.2

```
ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.765 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.051 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.802 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.941 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.870 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.438 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.905 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.920 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.761 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.979 ms
```

Figura 6. Verificación de conectividad 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=701.520 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=314.851 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=258.782 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=214.320 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=150.744 ms

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=806.762 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=168.096 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=223.004 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=73.274 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=649.338 ms
```

Figura 7. Verificación de conectividad 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=15.997 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=13.415 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=19.316 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=14.428 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=15.216 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=23.103 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=19.982 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=24.819 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=21.009 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=19.075 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=18.055 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=13.472 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=13.393 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=14.889 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=20.207 ms

```

Figura 8. Verificación de conectividad PC4

PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO

- 3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en área 0. Use OSPF Process ID **4** y asigne los siguientes routerIDs

R1: 0.0.4.1

R1(config)#router ospf 4 (se activa el proceso OSPF con ID 4)

R1(config-router)#router-id 0.0.4.1 (se le asigna el router-id)

R3: 0.0.4.3

R3(config)#router ospf 4 (se activa el proceso OSPF con ID 4)

R3(config-router)#router-id 0.0.4.3 (se le asigna el router-id)

D1: 0.0.4.131

D1(config)#router ospf 4 (se activa el proceso OSPF con ID 4)

D1(config-router)#router-id 0.0.4.131 (se le asigna el router-id)

D2: 0.0.4.132

D2(config)#router ospf 4 (se activa el proceso OSPF con ID 4)

D2(config-router)#router-id 0.0.4.132 (se le asigna el router-id)

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

```
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 (Se anuncian las redes conectadas
y se incluyen en el área 0)
```

```
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.100.1 0.0.0.0 area 0
D1(config-router)#network 10.0.101.1 0.0.0.0 area 0
D1(config-router)#network 10.0.102.1 0.0.0.0 area 0
```

```
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.100.2 0.0.0.0 area 0
D2(config-router)#network 10.0.101.2 0.0.0.0 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.2 0.0.0.0 area 0
```

```
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.10.1 0.0.0.255 area 0
R1(config-router)#network 209.165.200.224 0.0.0.34 area 0
R1(config-router)#network 209.165.200.225 0.0.0.0 area 0
```

```
R2(config-router)#network 10.0.11.0 0.0.0.255 area 0
R2(config-router)#network 10.0.11.1 0.0.0.0 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.3 0.0.0.0 area 0
```

En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

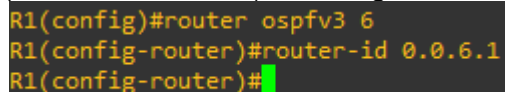
```
R1(config-router)#default-information originate (propaga la ruta por defecto)
```

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en área 0.

Use OSPF Process ID **6** y asigne los siguientes routerIDs:

- R1: 0.0.6.1

```
R1(config)#router ospfv3 6 (se active el proceso OSPFv6 con ID de proceso 6
R1(config-router)#router-id 0.0.6.1 (Se le asigna el router-id)
```



```
R1(config)#router ospfv3 6
R1(config-router)#router-id 0.0.6.1
R1(config-router)#
```

Figura 9. Configuración ospfv3 R1

- R3: 0.0.6.3

```
R3(config)#router ospfv3 6 (se active el proceso OSPFv6 con ID de proceso 6
```

R3(config-router)#router-id 0.0.6.3 (Se le asigna el router-id)

```
R3(config)#router ospfv3 6
R3(config-router)#router-id 0.0.6.3
R3(config-router)#
```

Figura 10. Configuración ospfv3 R1

- D1: 0.0.6.131

D1(config)#router ospfv3 6 (se active el proceso OSPFv6 con ID de proceso 6)
D1(config-router)#router-id 0.0.6.131 (Se le asigna el router-id)

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

Figura 11. Configuración ospfv3 R1

- D2: 0.0.6.132

D2(config)#router ospfv3 6 (se active el proceso OSPFv6 con ID de proceso 6)
D2(config-router)#router-id 0.0.6.132 (Se le asigna el router-id)

```
D2(config)#router ospfv3 6
D2(config-router)#router-id 0.0.6.132
D2(config-router)#
```

Figura 12. Configuración ospfv3 R1

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

R3(config)#inte e0/0 (se ingresa a la interface)
R3(config-if)#ipv6 ospf area 0 (se asigna el proceso ID 6 y el área 0 a la interface)

```
R3(config)#inte e0/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
```

Figura 13. Configuración del área 0 en R3

R1(config)#inte e0/1 (se ingresa a la interface)
R1(config-if)#ipv6 ospf area 0 (se asigna el proceso ID 6 y el área 0 a la interface)

```
R1(config)#inter e0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#
```

Figura 14. Configuración del área 0 en R1

D1(config)#int vlan 100 (Se ingresa a la vlan 100)
D1(config-if)#ipv6 ospf 6 area 0 (Se le asigna el proceso ID 6 y el área 0)


```
D1(config)#int vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config)#int vlan 102
D1(config-if)#ipv6 ospf 6 area 0
```

```
D2(config)#int vlan 100 (Se ingresa a la vlan 100)
D2(config-if)#ipv6 ospf 6 area 0 (Se le asigna el proceso ID 6 y el área 0)
D2(config)#int vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config)#int vlan 102
D2(config-if)#ipv6 ospf 6 area 0
```

- En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

```
R1(config-rtr)#default-information originate (Se propaga la ruta por defecto en R1)
R2(config-rtr)#default-information originate (Se propaga la ruta por defecto en R2)
```

Deshabilite las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto G1/0/11

```
D1(config-rtr)#passive-interface e0/0 (Se deshabilita las publicaciones OSPFv3 en la inter)
D1(config-rtr)#passive-interface e0/1
D1(config-rtr)#passive-interface e0/2
D1(config-rtr)#passive-interface e0/3
D1(config-rtr)#passive-interface e1/0
D1(config-rtr)#passive-interface e1/1
D1(config-rtr)#passive-interface e3/1
```

- D2: todas las interfaces excepto G1/0/11

```
D1(config-rtr)#passive-interface e0/0 (Se deshabilita las publicaciones OSPFv3 en la inter)
D1(config-rtr)#passive-interface e0/1
D1(config-rtr)#passive-interface e0/2
D1(config-rtr)#passive-interface e0/3
D1(config-rtr)#passive-interface e1/2
D1(config-rtr)#passive-interface e1/3
D1(config-rtr)#passive-interface e3/1
D1(config-rtr)#passive-interface e3/2
D1(config-rtr)#passive-interface e3/3
D1(config-rtr)#exit
```

3.3 En R2 en la “Red ISP”, configure MPBGP.

Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.

```
R2(config)#router bgp 500 (Se crea el proceso BGP para el sistema autónomo 500
ASN500)
```

```
R2(config-router)#bgp router-id 2.2.2.2 (Identificación del router para BGP)
```

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.
R2(config-router)#address-family ipv4 unicast

R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255 (se anuncia de loopback ipv4 2.2.2.2)
- Una ruta estática predeterminada IPv6.
R2(config-router)#address-family ipv6 unicast (agrega las direcciones ipv6 unicast)
R2(config-router-af)#neighbor :: activate (Anuncio de ruta por defecto ipv6 0)

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).

R2(config-router-af)#neighbor 0.0.0.0 activate (se anuncia de ruta por defecto ipv4 0)
R2(config-router)#neighbor 209.165.200.1 remote-as 300 (Configuración de vecindad ipv4 con R1 en ASN300)

En IPv6 address family, anuncie:

- La red Loopback 0 IPv4 (/128).
- La ruta por defecto (::/0).

R2(config-router)#neighbor 2001:db8:200::1 remote-as 300 (Configuración de vecindad ipv6 con R1 en ASN300)
R2(config-router-af)#network 2001:db8:2222::1/128 (se anuncia de loopback ipv6 2001:db8:2.2.2.2::1/128)

3.4 En R1 en la “Red ISP”, configure MPBGP.

R1(config)#router bgp 300 (Se crea el proceso BGP para el sistema autónomo 500 ASN500)

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.

R1(config-router)#bgp router-id 1.1.1.1 (Identificación del router para BGP)

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

R1(config-router)#neighbor 209.165.200.2 remote-as 500 (Configuración de vecindad ipv4 con R1 en ASN500)

- Deshabilite la relación de vecino IPv6.
R1(config-router-af)#no neighbor 2001:db8:200::2 activate (*Configuración de vecindad ipv6 con R1 en ASN500*)
- Habilite la relación de vecino IPv4.
R1(config-router-af)#neighbor 209.165.200.2 activate (*Se habilita vecindad ipv4*)
- Anuncie la red 10.0.0.0/8.
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0 (*Se anuncia red 10.0.0.0*)

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.
R1(config-router-af)#no neighbor 2001:db8:200::2 activate (*Se deshabilita vecindad ipv6*)
- Habilite la relación de vecino IPv6.
R1(config-router-af)#neighbor 2001:db8:200::2 activate (*Se habilita vecindad ipv6*)
- Anuncie la red 2001:db8:100::/48.
R1(config-router-af)#network 2001:db8:100::/48 (*Se anuncia la red*)

PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO (FIRST HOP REDUNDANCY)

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.

D1(config)#ip sla 4 (*Se crea la ip sla 4*)
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-ip 10.0.10.2 (*se estable el origen y destino de la interface e0/1*)

D1(config)#ip sla schedule 4 life forever start-time now (*SLA programado para implementación inmediata sin tiempo de finalización*)

```
D1(config)#ip sla 6 (Se crea la ip sla 6)
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1/64 source-ip 2001:db8:100:1010::2 (se
estable el origen y destino de la interface e0/1)
```

```
D1(config)#ip sla schedule 6 life forever start-time now (SLA programado para
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)#track 4 ip sla 4 (Se crea el track 4 para el ip sla 4)
D1(config-track)#delay up 10 down 15 (cambio de down a up 10 y de up a down 15)
D1(config)#track 6 ip sla 6 (Se crea el track 6 para el ip sla 6)
D1(config-track)#delay up 10 down 15 (cambio de down a up 10 y de up a down 15)
```

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.

Programa la SLA para una implementación inmediata sin tiempo de finalización.

```
D2(config)#ip sla 4 (Se crea la ip sla 4)
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-ip 10.0.11.2 (se estable el origen y destino
de la interface e0/1)
```

```
D2(config)#ip sla schedule 4 life forever start-time now (SLA programado para
implementación inmediata sin tiempo de finalización)
```

```
D2(config)#ip sla 6 (Se crea la ip sla 6)
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-ip 2001:db8:100:1011::2 (se
estable el origen y destino de la interface e0/1)
```

```
D2(config)#ip sla schedule 6 life forever start-time now (SLA programado para
```

implementación inmediata sin tiempo de finalización)

Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.

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)#track 4 ip sla 4 (Se crea el track 4 para el ip sla 4)
D2(config-track)#delay up 10 down 15 (cambio de down a up 10 y de up a down 15)
D2(config)#track 6 ip sla 6 (Se crea el track 6 para el ip sla 6)
D2(config-track)#delay up 10 down 15 (cambio de down a up 10 y de up a down 15)
```

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.

```
D1(config)#inter vlan 100 (ingresamos a la vlan 100)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 104 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtua)
D1(config-if)#standby 104 priority 150 (establecemos la prioridad del grupo)
D1(config-if)#standby 104 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 104 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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.
- ```
D1(config)#inter vlan 101 (ingresamos a la vlan 101)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 114 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtual)
D1(config-if)#standby 114 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 114 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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.
- ```
D1(config)#inter vlan 102 (ingresamos a la vlan 102)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 124 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtual)
D1(config-if)#standby 124 priority 150 (establecemos la prioridad del grupo)
D1(config-if)#standby 124 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 124 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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.
- ```
D1(config)#inter vlan 100 (ingresamos a la vlan 100)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 106 ipv6 autoconfig (creamos el grupo y activamos autoconfig ipv6)
D1(config-if)#standby 106 priority 150 (establecemos la prioridad del grupo)
D1(config-if)#standby 106 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 106 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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.
- ```
D1(config)#inter vlan 101 (ingresamos a la vlan 101)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 116 ipv6 autoconfig (creamos el grupo y activamos autoconfig ipv6)
D1(config-if)#standby 106 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 106 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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)#inter vlan 102 (ingresamos a la vlan 102)
D1(config-if)#standby version 2 (activamos HSRPv2)
D1(config-if)#standby 126 ipv6 autoconfig (creamos el grupo y activamos autoconfig ipv6)
D1(config-if)#standby 126 priority 150 (establecemos la prioridad del grupo)
D1(config-if)#standby 126 preempt (habilitamos la preferencia preemption)
D1(config-if)#standby 126 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D1(config-if)#
```

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.

```
D2(config)#inter vlan 100 (ingresamos a la vlan 100)
D2(config-if)#standby version 2 (activamos HSRPv2)
D2(config-if)#standby 104 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtua)
D2(config-if)#standby 104 preempt (habilitamos la preferencia preemption)
D2(config-if)#standby 104 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D2(config-if)#
```

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.

```
D2(config)#inter vlan 101 (ingresamos a la vlan 101)
D2(config-if)#standby version 2 (activamos HSRPv2)
D2(config-if)#standby 114 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtua)
D2(config-if)#standby 126 priority 150 (establecemos la prioridad del grupo)
D2(config-if)#standby 114 preempt (habilitamos la preferencia preemption)
D2(config-if)#standby 114 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D2(config-if)#
```

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.

```
D2(config)#inter vlan 102 (ingresamos a la vlan 102)
D2(config-if)#standby version 2 (activamos HSRPv2)
D2(config-if)#standby 124 ip 10.0.100.254 (creamos el grupo y asignamos la ip virtua)
D2(config-if)#standby 124 priority 150 (establecemos la prioridad del grupo)
D2(config-if)#standby 124 preempt (habilitamos la preferencia preemption)
D2(config-if)#standby 124 track 4 decrement 60 (rastreamos el objeto 4 y decrem. en 60)
D2(config-if)#
```

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.

D2(config)#inter vlan 100 (*ingresamos a la vlan 100*)

D2(config-if)#standby version 2 (*activamos HSRPv2*)

D2(config-if)#standby 106 ipv6 autoconfig (*creamos el grupo y activamos autoconfig ipv6*)

D2(config-if)#standby 106 preempt (*habilitamos la preferencia preemption*)

D2(config-if)#standby 106 track 4 decrement 60 (*rastreamos el objeto 4 y decrem. en 60*)

D2(config-if)#

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.

D2(config)#inter vlan 101 (*ingresamos a la vlan 101*)

D2(config-if)#standby version 2 (*activamos HSRPv2*)

D2(config-if)#standby 116 ipv6 autoconfig (*creamos el grupo y activamos autoconfig ipv6*)

D2(config-if)#standby 116 priority 150 (*establecemos la prioridad del grupo*)

D2(config-if)#standby 116 preempt (*habilitamos la preferencia preemption*)

D2(config-if)#standby 116 track 4 decrement 60 (*rastreamos el objeto 4 y decrem. en 60*)

D2(config-if)#

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)#inter vlan 102 (*ingresamos a la vlan 102*)

D2(config-if)#standby version 2 (*activamos HSRPv2*)

D2(config-if)#standby 126 ipv6 autoconfig (*creamos el grupo y activamos autoconfig ipv6*)

D2(config-if)#standby 126 preempt (*habilitamos la preferencia preemption*)

D2(config-if)#standby 126 track 4 decrement 60 (*rastreamos el objeto 4 y decrem. en 60*)

D2(config-if)#

PARTE 5: SEGURIDAD - EN ESTA PARTE DEBE CONFIGURAR VARIOS MECANISMOS DE SEGURIDAD EN LOS DISPOSITIVOS DE LA TOPOLOGÍA.

- 5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

R1(config)#enable algorithm-type scrypt secret cisco12345cisco (*activamos el algoritmo de encriptación SCRYPT*)

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

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

- 5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

R1(config)#username sadmin privilege 15 pass cisco12345cisco (*creamos un usuario y lo protegemos con contraseña*)

R2(config)#username sadmin privilege 15 pass cisco12345cisco

R3(config)#username sadmin privilege 15 pass cisco12345cisco

D1(config)#username sadmin privilege 15 pass cisco12345cisco

D2(config)#username sadmin privilege 15 pass cisco12345cisco

A1(config)#username sadmin privilege 15 pass cisco12345cisco

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

D2(config)#aaa new-model (*habilita el protocolo AAA*)

D1(config)#aaa new-model

A1(config)#aaa new-model

R1(config)#aaa new-model

R3(config)#aaa new-model

5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

```
R3(config)#radius-server host 10.0.100.6 acct-port 1812 key $strongPass (se especifica la
direccion ip del servidor RADIUS el puerto a utilizar y la contraseña)
R1(config)#radius-server host 10.0.100.6 acct-port 1812 key $strongPass
D1(config)#radius-server host 10.0.100.6 acct-port 1812 key $strongPass
D2(config)#radius-server host 10.0.100.6 acct-port 1812 key $strongPass
A1(config)#radius-server host 10.0.100.6 acct-port 1812 key $strongPass
```

```
A1(config)#radius-server host 10.0.100.6 acct-port 1813 key $strongPass (se especifica la
direccion ip del servidor RADIUS el puerto a utilizar y la contraseña)
D1(config)#radius-server host 10.0.100.6 acct-port 1813 key $strongPass
D2(config)#radius-server host 10.0.100.6 acct-port 1813 key $strongPass
R1(config)#radius-server host 10.0.100.6 acct-port 1813 key $strongPass
R3(config)#radius-server host 10.0.100.6 acct-port 1813 key $strongPass
```

5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

```
R3(config)#aaa authentication login default group radius local (se autentica el servidor
RAIDUS mediante la lista por defecto y con el grupo de servidores radius)
R1(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
```

PARTE 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED

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

```
A1(config)#clock timezone AR -5 (se configura la UTC con el horario de Colombia UTC -5)
D1(config)#clock timezone AR -5
D2(config)#clock timezone AR -5
R1(config)#clock timezone AR -5
R2(config)#clock timezone AR -5
R3(config)#clock timezone AR -5
```

```
D1(config)#clock timezone AR -5
D1(config)#do show clock
*08:30:14.891 AR Sat Nov 6 2021
D1(config)#

D2(config)#clock timezone AR -5
D2(config)#do show clock
*08:32:08.894 AR Sat Nov 6 2021

A1(config)#clock timezone AR -5
A1(config)#do show clock
*08:33:43.877 AR Sat Nov 6 2021
A1(config)#
```

```

R3(config)#do show clock
*08:35:38.604 valle Sat Nov 6 2021
R3(config)#

R1(config)#do show clock
*08:36:39.478 valle Sat Nov 6 2021
R1(config)#

R2(config)#do show clock
*08:37:32.860 valle Sat Nov 6 2021
R2(config)#

```

Figura 15: configuración y verificación del reloj local

6.2 Configure R2 como un NTP maestro 3.
R2(config)#ntp master 3 (Se configura a R2 como maestro 3)

6.3 Configure NTP en R1, R3, D1, D2, y A1.

Configure NTP de la siguiente manera:

- R1 debe sincronizar con R2.

R1(config)#ntp server 209.165.200.226 (conectando al servidor NTP en R2)

```

R1(config)#ntp server 209.165.200.226
R1(config)#end
R1#
*Nov 6 13:48:20.304: %SYS-5-CONFIG_I:
R1#show clock detail
*08:48:29.389 valle Sat Nov 6 2021
Time source is NTP
R1#

```

Figura 16: configuración y verificación del server NTP en R1

- R3, D1 y A1 para sincronizar la hora con R1.

R3(config)#ntp server 10.0.13.3 (conectando al servidor NTP en R1)

```

R3(config)#ntp server 10.0.13.3
R3(config)#do show clock detail
*08:50:25.362 valle Sat Nov 6 2021
Time source is NTP
R3(config)#

```

Figura 17: configuración y verificación del server NTP en R3

D1(config)#ntp server 10.0.10.1 (conectando al servidor NTP en R1)

```

D1(config)#ntp server 10.0.10.1
D1(config)#do show clock detail
^
% Invalid input detected at '^' m

D1(config)#do show clock detail
*08:51:52.069 AR Sat Nov 6 2021
Time source is NTP
D1(config)#

```

Figura 18: configuración y verificación del server NTP en D1

A1(config)#ntp server 10.0.10.1 *(conectando al servidor NTP en R1)*

```
A1(config)#ntp server 10.0.10.1
A1(config)#do show clock detail
*08:53:30.092 AR Sat Nov 6 2021
Time source is NTP
A1(config)#
```

Figura 19: configuración y verificación del server NTP en A1

- D2 para sincronizar la hora con R3.

D2(config)#ntp server 10.0.11.1 *(conectando al servidor NTP en R3)*

```
D2(config)#ntp server 10.0.11.1
D2(config)#do show clock detail
*08:54:35.039 AR Sat Nov 6 2021
Time source is NTP
D2(config)#
```

Figura 20: configuración y verificación del server NTP en D2

6.4 Configure Syslog en todos los dispositivos excepto R2

R1(config)#logging 10.0.100.5 *(se configura syslog para que se enviado a PC1)*

R1(config)#logging trap warning *(Se configura los mensajes syslog en el nivel warning)*

R3(config)#logging 10.0.100.5

R3(config)#logging trap warning

D1(config)#logging 10.0.100.5

D1(config)#logging trap warning

D2(config)#logging 10.0.100.5

D2(config)#logging trap warning

A1(config)#logging 10.0.100.5

A1(config)#logging trap warning

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

- Únicamente 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.

```
R1(config)#snmp-server community string ro ENCORSA (activamos SNMP en modo lectura y creamos el Grupo ENCORSA)
R1(config)#snmp-server contact WesthlySarabia (activamos el valor de contacto para el SNMP, en este caso será mi nombre)
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA (se active el snmp versión 2 e identificamos el server host, en este caso será PC1)
R1(config)#ip access-list standard ENCORSA (damos acceso a la lista de la comunidad ENCORSA)
R1(config-std-nacl)#permit 10.0.100.5 (Se permite el acceso solo al PC1)
```

```
R3(config)#snmp-server community string ro ENCORSA
R3(config)#snmp-server contact WesthlySarabia
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#ip access-list standard ENCORSA
R3(config-std-nacl)#permit 10.0.100.5
```

```
D1(config)#snmp-server community string ro ENCORSA
D1(config)#snmp-server contact WesthlySarabia
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#ip access-list standard ENCORSA
D1(config-std-nacl)#permit 10.0.100.5
```

```
D2(config)#snmp-server community string ro ENCORSA
D2(config)#snmp-server contact WesthlySarabia
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#ip access-list standard ENCORSA
D2(config-std-nacl)#permit 10.0.100.5
```

```
A1(config)#snmp-server community string ro ENCORSA
A1(config)#snmp-server contact WesthlySarabia
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#ip access-list standard ENCORSA
A1(config-std-nacl)#permit 10.0.100.5
```

- En R3, D1, y D2, habilite el envío de traps config y ospf.

```
D2(config)#snmp-server enable traps ospf (se habilita el envio de traps ospf)  
D2(config)#snmp-server enable traps config (Se habilita el envio de traps config)
```

```
D1(config)#snmp-server enable traps ospf  
D1(config)#snmp-server enable traps config
```

```
R3(config)#snmp-server enable traps ospf  
R3(config)#snmp-server enable traps config
```

- En R1, habilite el envío de traps bgp, config, y ospf.

```
R1(config)#snmp-server enable traps ospf (se habilita el envio de traps ospf)  
R1(config)#snmp-server enable traps config (Se habilita el envio de traps config)  
R1(config)#snmp-server enable traps bgp (se habilita el envio de traps bgp)
```

- En A1, habilite el envío de traps config.

```
R1(config)#snmp-server enable traps config
```

CONCLUSIÓN

Alrededor del desarrollo del escenario 1, se encontraron varios errores, de tal forma que fue pertinente darle solución para así continuar con el desarrollo de este. Se opto por investigar los comandos faltantes y a su vez retroalimentar en algunas temáticas que se han dado al inicio del curso.

Se dio con éxito el desarrollo de la primera etapa del proyecto aplicado, configurando las plataformas a través del software GNS3, y comprobando con veracidad la conmutación entre los switches, usando protocolos como lo es la STP mediante la configuración de VLANs en un entorno corporativo.

Se comprendió el modo de operación de las subredes mostrando y resaltando los beneficios de la administración de broadcast independientes en los diferentes escenarios al interior de una red independiente jerárquica. Esta configuración se llevó a cabo por comando IOS investigados y obtenidos en las practicas con anterioridad, con los direccionamientos tanto IPv4 y IPV6, añadiendo los protocolos, DHCP, OSPF, EIGRP y BGP, logrando dar soluciones en una red escalable mediante el uso de los principios de enrutamiento en ambientes como la LAN y WAN.

De manera que se presente caída de las puertas de enlaces, como contingencia se configuro IP SLA y HSRPv2, para proveer redundancia de primer salto para los hosts de la red de compañía. La seguridad de nuestra red se completó debido a procedimientos requeridos en donde nos ayuda a la protección de información y de terceros ajenos a la empresa, no obstante, es preferible realizar test y configuraciones futuras para su mejoramiento. A través de la parte administrativa de la red, se establecieron servidores NTP y Syslog, con la garantía de proporcionar mayor seguridad, y conectividad entre la red WAN, autenticando con el servicio de aaa, mediante el servidor RADIUS, de igual forma, se habilito los mensajes warning, solo al PC1, para poder tener un mejor control de lo que se esta realizando en tiempo real, dando soluciones de manera efectiva aun problema si se presenta

BIBLIOGRAFIA

Algoritmo Scrypt: Programador de clics. (s. f.). Recuperado 11 de noviembre de 2021, de <https://programmerclick.com/article/9326915661/>

Cisco IOS. (2020). En *Wikipedia, la enciclopedia libre*.
<https://es.wikipedia.org/w/index.php?title=Cisco IOS&oldid=130949606>

Gabriel, E. (2020, agosto 24). Como configurar IP SLA tracking. *Estudia Redes*.
<https://estudiaredes.com/cisco/como-configurar-ip-sla-tracking/>

Ejemplo de configuración MP-EBGP. (s. f.). 6.

Fernández, R. P. (s. f.). *Enrutamiento dinámico OSPF con Packet Tracer*. Recuperado 11 de noviembre de 2021, de <https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer>

Glosario- Qué es DHCP y Para qué Sirve. (s. f.). Netec. Recuperado 11 de noviembre de 2021, de <https://www.netec.com/que-es-dhcp-y-para-que-sirve>

HSRP Protocolo de Routing de reserva activa. (s. f.). *HSRP Protocolo de Routing de reserva activa*. Recuperado 11 de noviembre de 2021, de <http://myblogiovanniperez.blogspot.com/2018/07/hsrp-protocolo-de-routing-de-reserva.html>

Uso de seguridad AAA para la administración de equipos de Conectividad. (s. f.). Recuperado 11 de noviembre de 2021, de <https://www.perlesystems.es/supportfiles/aaa-security.shtml>

