DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON ALEXANDER LUNA DURAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHON ALEXANDER LUNA DURAN

Diplomado de opción de grado presentado para optar el
título de INGENIERO ELECTRÓNICO.

DIRECTOR:
MSC. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá 25 de noviembre de 2021

CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

COMANDOS IOS: comandos que usa el software IOS de cisco para definir las funciones necesarias para el correcto funcionamiento de los dispositivos que componen la red.

INTERFAZ: elemento físico que permite la comunicación entre los diversos dispositivos que componen la red, permite el uso de los diferentes protocolos.

PROTOCOLO DE ENRUTAMIENTO: procesos basados en algoritmos que se encargan de administrar la actividad de la red, de forma que los paquetes de información lleguen a su destino de forma correcta, se selecciona la ruta más adecuada entre el origen y su destino para la circulación el paquete.

ROUTER: periférico que tiene la función de llevar conexión y proveer una ruta para el envío y recepción de los paquetes de datos entre los diferentes dispositivos que están conectados a la red e internet.

SWITCH: dispositivo que permite que los componentes de la red puedan comunicarse entre sí y compartir información, esto basado en el estándar técnico IEEE 802.3 conocido como ethernet.

TOPOLOGÍA DE RED: es la forma de distribuir y crear un arreglo para la interconexión entre los dispositivos que componen la red, existe la topología física la cual se refiere a los cableados y dispositivos físicos y la lógica que refiere a la forma de acceso de los dispositivos a la red.

VLAN: la red de área local virtual la es una red lógica independiente dentro de una red física compuesta de varios dispositivos, ayudan a disminuir el área lógica de la red y también pueden permitir o negar el acceso de las demás vlan que componen la red.

RESUMEN

La aplicación de las habilidades adquiridas durante el desarrollo de las actividades dentro de la plataforma Cisco, el diplomado CCNP y los cursos impartidos en la universidad, cobran una gran importancia en el momento de implementar soluciones a problemas reales. En un escenario planteado que requiere de un tipo de configuración especifico y tomando en cuenta los requerimientos de enrutamiento de los diferentes elementos que conforman la red, es necesario aplicar los conocimientos adquiridos durante el curso de la carrera de ingeniería electrónica y de esta forma realizar las pruebas pertinentes para verificar el correcto funcionamiento de los dispositivos ejecutando los comandos adecuados. El trabajo se desarrolló utilizando dos programas especializados para simular redes: Packet tracer y GN3S, buscando el software que permitiera implementar una solución aceptable, obtener una red conmutada que cumpla con los requisitos, lograr una buena simulación del escenario propuesto y obtener un mejor resultado, la utilización del software GN3S, el cual admite varios comandos que no es posible ejecutar en Packet tracer, permitió desarrollar la configuración del escenario de una manera más completa.

Palabras clave: Cisco, CCNP, conmutación, enrutamiento, redes, electrónica.

ABSTRACT

The use of the abilities acquired in the developing of the activities into the cisco platform, CCNP diplomat and the university courses, get a big importance at the moment of implementing solutions to real trouble. In a proposed scenario which requires a type of specific configuration and take in consideration the requirements of routing of the different elements that make up the net, it is necessary to apply the knowledge acquired during the curse of electronic engineering and in this mode perform the relevant test to check the right functioning of the devices running the right commands. This work was developed using two specialized software for net simulation: Packet tracer and GN3S, searching the software that allow the implementation of an acceptable solution, get a switched net that meets with the requirements, achieve a good simulation of the proposed scenario and get a better outcome, the utilization of GN3S software , which admits several commands that are not possible to be run in Packet tracer, allowed the developing of the scenario configuration in a more complete mode.

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

INTRODUCCION

En un escenario que simula una situación real donde se requiere dar conectividad a una serie de dispositivos y para poder tener la capacidad de dar solución a problemas de configuración de conexión, es necesario adquirir los conocimientos adecuados, saber los comandos que se pueden utilizar y cuál es su función, entender el funcionamiento de la red y como cualquier cambio puede afectar su correcto funcionamiento. El propósito del desarrollo del diplomado cisco CCNP es brindar las herramientas necesarias para poder afrontar un desafío de configurar una red propuesta, de manera correcta y funcional y que permita aplicar todos los conceptos aprendidos en el desarrollo del curso.

El escenario está compuesto de 5 partes, la primera parte de configuración inicial de los dispositivos que componen la red: switchwes, routers y PCs. En esta parte se configuran los parámetros básicos como lo son los nombres de dispositivos, las redes Vlan, configuración de las interfaces de los dispositivos y direcciones ip. En la segunda parte del escenario se configuran la capa 2 y soporte de host, se configuran enlaces troncales, vlan nativas, EtherChannel, protocolo RSTP y se verifica la interconectividad por medio de ping entre los dispositivos. La tercera parte del escenario comprende la configuración de los protocolos de enrutamiento OSPFv2 y OSPFv3 en ipv4 e ipv6 en los dispositivos que componen de la red y su consecuente verificación utilizando comandos ping.

En la parte cuatro que compone el escenario se configura el protocolo HSRPv2 y la redundancia del primer salto.Los diferentes mecanismos de seguridad donde se aplican conceptos como los algoritmos para la encriptación de contraseñas y la utilización del servidor RADIUS se desarrollan en la parte cinco del escenario. Finalmente en la parte 6 se configuran funciones que permiten una adecuada administración de la red como los protocolos SNMPv2 y NTP.

Cada parte del desarrollo de las diferentes actividades de configuración y pruebas de funcionamiento de los distintos dispositivos, son explicadas con el comentario de las diferentes partes de los códigos utilizados para la programación en la interfaz de línea de comandos CLI de cisco, esto para tener una mejor comprensión de los procedimientos realizados para poder cumplir con los requerimientos establecidos y tener una red funcional.

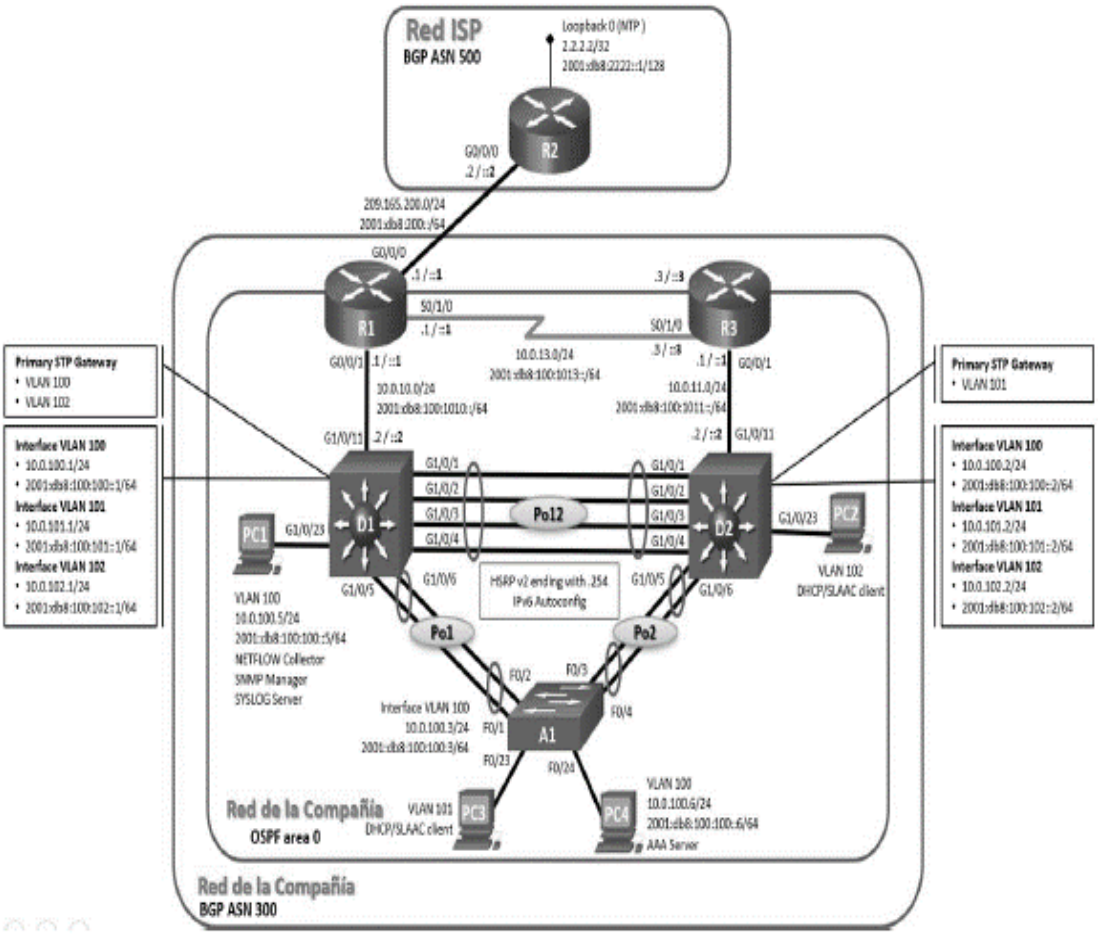
DESARROLLO

1. Escenario propuesto

A continuación se presenta la red propuesta para el desarrollo de la actividad.

En esta prueba de habilidades, debe 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 (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere. (Fuente: documento guía)

Figura 1: topología de red



Fuente: documento guía

Tabla 1: tabla de direccionamiento

Dispositivo	Interfaz	Dirección ipv4	Dirección ipv6	Link local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	G0/3	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	G0/3	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	Vlan 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	Vlan 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	Vlan 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	Vlan 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	Vlan 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	Vlan 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	Vlan 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

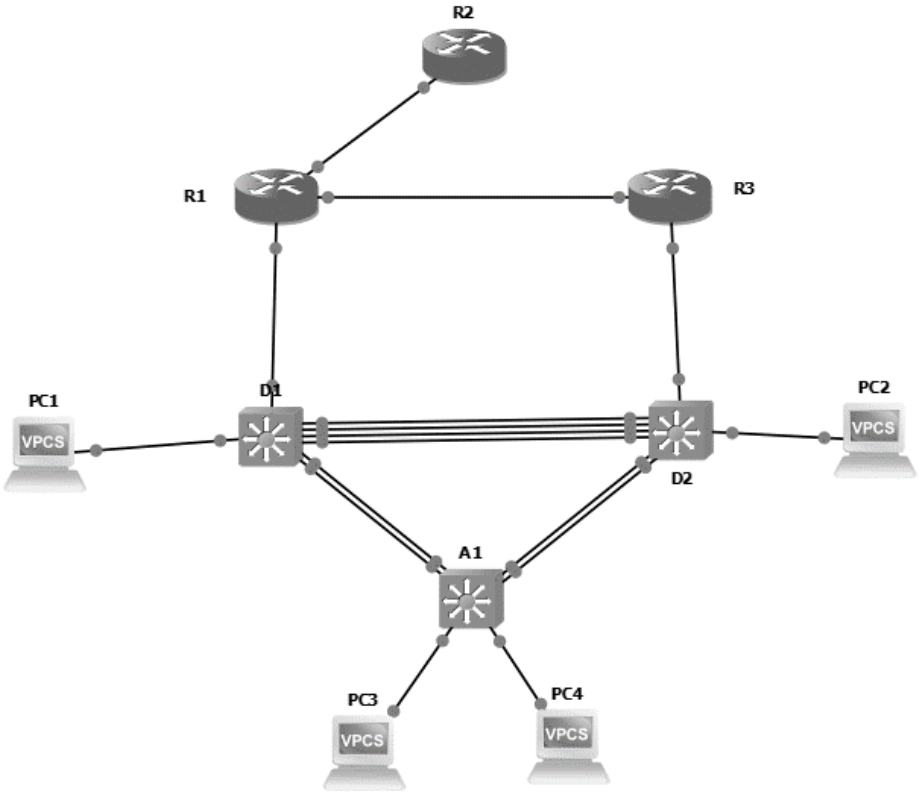
Fuente: documento guía

2. Configuración de parámetros en los dispositivos

2.1 Cableado de la red

Para la realización del escenario propuesto se usa el programa GN3S como se muestra en la figura.

Figura 2: cableado de la topología de red



Fuente: propia

2.2 Configuración de los dispositivos de red

La configuración de los distintos dispositivos que componen la red se realiza desde la interfaz de línea de comandos o CLI.

A continuación se realiza la configuración básica de los router, switches y pc que están relacionados en la topología teniendo en cuanta la tabla de enrutamiento. La explicación del código se realiza en la primera parte del código donde se configura el router 1. En los demás dispositivos se omite dicha explicación ya que se usan los mismos comandos, cuando son comandos distintos se realiza la explicación correspondiente.

2.2.1 Configuración de router R1

Router>enable
////acceso al modo administrador
Router#config t
///acceso a la configuración del router

```
Router(config)#hostname R1
    ///cambio de nombre del dispositivo
R1(config)#ipv6 unicast-routing
    ///comando para habilitar el enrutamiento de paquetes ipv6 en el router
R1(config)#banner motd #R1, ENCOR skills assessment, scenario 1#
    ///se configura un mensaje de aviso
R1(config)#line con 0
   ///ingreso al modo de configuración de línea
R1(config-line)#exec-timeout 0 0
   ///tiempo de espera inactivo en sesión remota
R1(config-line)#logging synchronous
  ///sincronización de mensajes con el ingreso de comandos en el prompt del so
R1(config-line)#exit
  ///retorno al modo anterior

R1(config)#interface g0/0
  ///selección de interfaz del router que se va a configurar
R1(config-if)#ip address 209.165.200.225 255.255.255.224
  ///configuración de dirección IP y mascara de la interfaz
R1(config-if)#ipv6 address fe80::1:1 link-local
  ///comando que facilita el reconocimiento por parte del router
R1(config-if)#ipv6 address 2001:db8:200::1/64
  ///configuración de la dirección ipv6
R1(config-if)#no shutdown
  ///habilitación de la interfaz
R1(config-if)#exit

R1(config)#interface g0/1
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 g0/3
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)#end

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

[OK]

2.2.2 Configuración de router R2

```
Router>enable
Router#config t
Router(config)#ipv6 unicast-routing
Router(config)#no ip domain lookup
Router(config)#banner motd #R2, encor skills assessment, scenario 1#
Router(config)#hostname R2
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit

R2(config)#interface g0/0
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:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.3 Configuración de router R3

```
Router>enable
Router#config t
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
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 g0/1
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-line)#exit

R3(config)#interface g0/3
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)#exit

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.4 Configuración de switch D1

```
Switch>enable
Switch#config t
Switch(config)#hostname D1
D1(config)#ip routing
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
///acceso a la vlan 100
D1(config-vlan)#name Management
///asignación de nombre a la vlan 100
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 g0/4
D1(config-if)#no switchport
  ///colocación de la interfaz en modo de capa 3
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit

D1(config)#interface vlan 100
  ///selección de interfaz vlan 100 en el switch
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
  ///excluye direcciones IP para la asignación de IP en los hosts
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
   ///crea un grupo de direcciones ip con el nombre designado
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
  ///habilitación del switch en modo de configuración de EIGRP
D1(dhcp-config)#default-router 10.0.101.254
  ///se establece el Gateway por donde ingresan los clientes al router
D1(dhcp-config)#exit
```

```
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit

D1(config)#interface range g1/0/7-10
D1(config-if-range)#shutdown
D1(config)#exit
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.5 Configuración de switch D2

```
Switch>enable
Switch#config t
Switch(config)#hostname D2
D2(config)#ip routing
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 g1/0
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
D2(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 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit

D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit

D2(config)#interface range g1/1-3, g2/2-3, g3/1-3
D2(config-if-range)#shutdown
```

```
D2(config)#end

D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.2.6 Configuración de switch A1

```
Switch>enable
Switch#config t
Switch(config)#hostname A1
A1(config)#no ip domain lookup
  ///desactivación de la búsqueda DNS
A1(config)#banner motd # A1, 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)#exit

A1(config)#interface range g0/0-3, g1/0-3, g3/0-1
```

A1(config-if-range)#shutdown
A1(config)#end

A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

3. Configuración de la capa 2 de la red y soporte de host.

3.1 Configuración de enlaces troncales y habilitación de protocolo RSTP

En este punto de la práctica se lleva a cabo la configuración de los enlaces troncales, los cuales son conexiones punto a punto entre los switches D1, D2 y A1 cuya función es transportar las VLAN configuradas en la parte inicial. Además se usa el etiquetado de trama con encapsulación 802.1Q. Como parte del desarrollo de esta parte de la práctica, también se habilita el protocolo RSTP el cual se usa para reducir el tiempo de convergencia en el momento de que existan cambios en la topología.

3.1.1 Configuración de enlaces troncales en D1 y habilitación de protocolo rapid spanning tree RSTP.

D1(config)#spanning-tree mode rapid-pvst
///se habilita ejecución del protocolo rstp en la vlan
D1(config)#interface range g0/1-3, g2/0-1
///en esta línea se escogen los rangos de interfaces para ser configuradas
D1(config-if-range)#switchport trunk encapsulation dot1q
///habilita el protocolo de encapsulación 802.1Q
D1(config-if-range)#switchport mode trunk
///configuración de un extremo de Puerto del switch como enlace troncal

3.1.2 Configuración de enlaces troncales en D2 y habilitación de protocolo rapid spanning tree RSTP.
.
D2(config)#spanning-tree mode rapid-pvst
D2(config)#interface range g0/0-3, g2/2-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk

3.1.3 Configuración de enlaces troncales en A1y habilitación de protocolo rapid spanning tree RSTP.

A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range g2/0-3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk

3.2 Cambio de VLAN nativa

Una vlan nativa es un identificador común para los enlaces troncales configurados en la parte anterior y es usada para dirigir el tráfico que no posee etiqueta. Cabe resaltar que esta vlan debe ser configurada igual en todos los extremos de los enlaces troncales, de lo contrario se genera un mensaje de error al no coincidir los nombres en los dispositivos.

3.2.1 Cambio de vlan nativa en D1

D1(config)#interface g0/0-3, g2/0-1
D1(config-if-range)#switchport trunk native vlan 999
///asignación de la interfaz vlan como nativa en los enlaces troncales
D1(config-if-range)#switchport trunk allowed vlan 999,100-102
///añade vlan que son permitidas para su tránsito en el enlace troncal

3.2.2 Cambio de vlan nativa en D2

D2(config)#interface g0/0-3, g2/0-1
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#switchport trunk allowed vlan 999,100-102

3.2.3 Cambio de vlan nativa en A1

A1(config)#interface
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#switchport trunk allowed vlan 999,100-102

3.3 Configuración de D1 y D2 como puente raíz.

Para el correcto funcionamiento del protocolo STP es necesario asignar un switch como root bridge o puente raíz, para lo cual se tiene en cuenta el valor de la prioridad del switch y su dirección MAC. A su vez es importante configurar un segundo switch como raíz secundario el cual soportara el tráfico en el caso de que el switch raíz primario falle.

D1(config)#spanning-tree vlan 100,102 root primary
///comando para designar las vlan en el switch como puente raíz primario

D1(config)#spanning-tree vlan 101 root secondary
///comando para designar las vlan en el switch como puente raíz secundario

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

3.4 Creación de EtherChannel LACP

Para lograr incrementar la velocidad nominal de los puertos físicos se realiza un agrupamiento lógico de varios enlaces ethernet correspondiente a dichos puertos. Esto se logra usando el EtherChannel con el cual se obtienen enlaces de alta velocidad. El protocolo LACP se usa como método de control para el grupo de puertos físicos y crea un único enlace lógico, además permite la negociación automática con los demás componentes de los enlaces. En esta parte de la práctica se crean los grupos 1,2 y 12 como EtherChannel LACP. Es necesario que las interfaces configuradas en cada switch coincidan con su par en el otro dispositivo para crear el grupo, de lo contrario aparece un mensaje de error. También es importante configurar los port channel como enlaces troncales para un correcto funcionamiento.

D1(config)#interface range g0/0-3
D1(config-if-range)#shutdown
///desactivación de la interfaz
D1(config-if-range)#channel-group 12 mode active
///creación de la interfaz port channel con el identificador 12 y activación como /// etherchannel LACP
D1(config-if-range)#no shutdown
///activación de la interfaz
D1(config-if-range)#interface port-channel 12
///selección de la interfaz port channel 12
D1(config-if)#switchport trunk encapsulation dot1q
///se activa el modo troncal en la interfaz y se habilita el estándar de ///encapsulación IEEE 8021q
D1(config-if)#switchport mode trunk
///configuración de un extremo de Puerto del switch como enlace troncal

D1(config)#interface range g2/0-1
D1(config-if-range)#shutdown
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#no shutdown
D1(config-if-range)#interface port-channel 1

```
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk

D2(config)#interface range g0/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk

D2(config)#interface range g2/0-1
D2(config-if-range)#shutdown
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#interface port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk

A1(config)#interface range g2/0-1
A1(config-if-range)#shutdown
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#interface port-channel 1
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk

A1(config)#interface range g2/2-3
A1(config-if-range)#shutdown
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#interface port-channel 2
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
```

3.5 Configuración de los puertos de acceso del host (host access port) en PC1, PC2, PC3 y PC4.

En esta parte se asigna un único puerto de acceso a las vlan, por este puerto existe tráfico sin etiqueta y permite únicamente el paso de la vlan seleccionada, esta asignación de puertos se usa en dispositivos finales en este caso son los PC que hacen parte de la topología.

```
D1(config)#interface g3/0
D1(config-if)#switchport mode access
   ///cambio de modo de acceso a la interfaz de forma permanente
D1(config-if)#switchport access vlan 100
  ///se asigna una vlan a la interfaz seleccionada por la cual solo transita dicha vlan

D2(config)#interface g3/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102

A1(config)#interface g3/2
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#interface g3/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
```

3.6 Verificación de dirección en PC2 y PC 3

Por medio del protocolo DHCP se establece la dirección IP de los dispositivos finales además de otras opciones de configuración. El servidor principal (switch D1 y D2) es el dispositivo que asigna la dirección IP por DHCP, estas direcciones IP son asignadas de acuerdo con los rangos de direcciones IP permitidas configuradas en la primera parte del ejercicio.

Figura 3: verificación de dirección ip en pc2

Fuente: propia

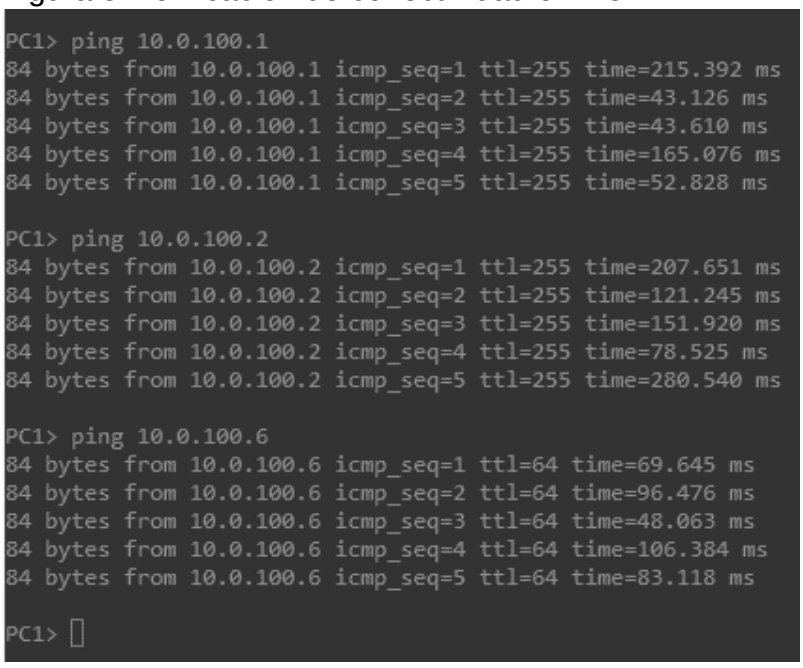
Figura 4: verificación de dirección ip en pc3

Fuente: propia

3.7 Verificar la conectividad en LAN local.

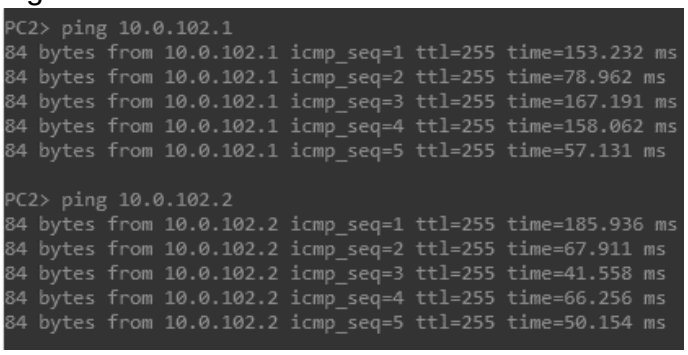
Para verificar la conectividad de la red se ejecuta el comando ping, con este comando se puede verificar el estado de los hosts remotos los cuales generan una respuesta. Así se puede diagnosticar si hay errores de conexión en la red. En la topología se realizan ping desde los PC hacia otros PC y los switches D1 y D2.

Figura 5: verificación de conectividad en PC1



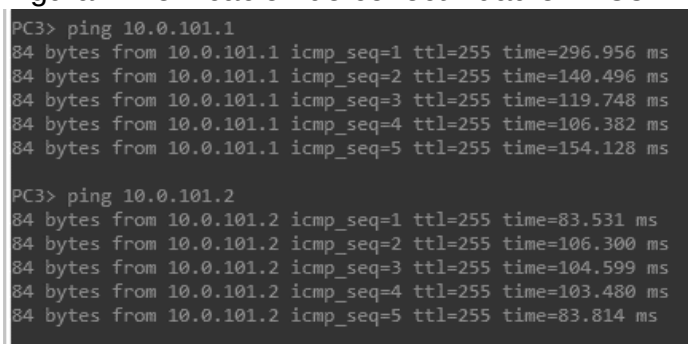
Fuente: propia

Figura 6: verificación de conectividad en PC2



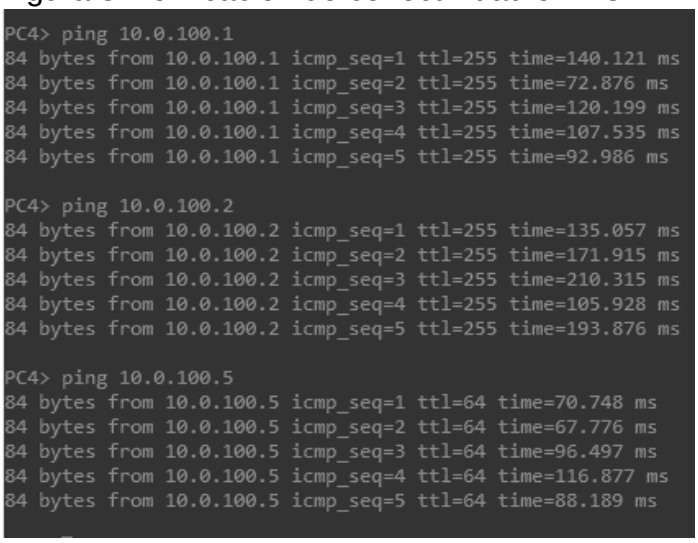
Fuente: propia

Figura 7: verificación de conectividad en PC3



Fuente: propia

Figura 8: verificación de conectividad en PC4



Fuente: propia

4. Configurar protocolos de enrutamiento

4.1 Configuración de OSPFv2 en R1, R3, D1 y D2

El protocolo OSPF es utilizado en redes amplias y complejas, el protocolo envía la información de su mascara de subred en las actualizaciones y utiliza un algoritmo que identifica la ruta más corta, calcula de forma más rápida los cambios en la topología para determinar estas rutas. Además agrega áreas que permiten la división del sistema y así disminuir el tráfico. Para las direcciones IPv4 se usa el protocolo OSPFv2. En esta parte del ejercicio además de la implementación del protocolo OSPFv2 también se configuran la ruta estática que hace que el router pueda acceder a cualquier red desconocida.

4.1.1 Configuración en R1

```
R1(config)#router ospf 4
     //activación del proceso OSPF en el router
R1(config-router)#router-id 0.0.4.1
   ///identificación del router representado como dirección ivpv4
R1(config-router)#log-adjacency-changes
   ///notifica a la consola cuando OSPF encuentra un vecino
R1(config-router)#no passive-interface g0/1
   ///permite que la interfaz cree adyacencia con un vecino
R1(config-router)#no passive-interface g0/3
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
   ///asigna el área 0 a la interfaz
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/0
   ///Evita que la interfaz genere adyacencia con un vecino
R1(config-router)#network 209.165.200.0 0.0.0.31 area 0
R1(config-router)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
   ///configuración de la ruta estática por defecto
R1(config)#router ospf 4
R1(config-router)#default-information originate
   ///propagación de la ruta estática por defecto a los demás dispositivos
```

4.1.2 Configuración en R3

```
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#log-adjacency-changes
R3(config-router)#no passive-interface g0/1
R3(config-router)#no passive-interface g0/3
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)# network 10.0.11.0 0.0.0.255 area 0
```

4.1.3 Configuración en D1

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#log-adjacency-changes
D1(config-router)#passive-interface default
   ///comando que evita que todas las interfaces reciban actualizaciones de
   ////enrutamiento
D1(config-router)#no passive-interface g1/0
```

```
D1(config-router)#network 10.0.100.0 0.0.0.255 area 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 10.0.10.0 0.0.0.255 area 0
```

4.1.4 Configuración en D2

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#log-adjacency-changes
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/0
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 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
```

4.2 Configuración OSPFv3 en R1, R3, D1 y D2

El protocolo OSPFv3 se usa para la configuración de estas características en direcciones IPv6, durante el desarrollo de la práctica no fue posible ejecutar varios de los comandos descritos en la configuración, al ingresarlos en el CLI arrojaron error de comando invalido. De igual forma se incluyó el desarrollo de la configuración de forma informativa y para aplicarla en otros escenarios.

```
R1(config)#ipv6 router ospf 6
    ///se agrega la interfaz ospf 6 al area 0
R1(config-rtr)#router-id 0.0.6.1
   ///identificación del switch representado como dirección ip
R1(config-rtr)#passive-interface g0/0
R1(config)#interface g0/1
R1(config-if)#ipv6 ospf 6 area 0
   ///se agrega la interfaz ospf 6 al area 0
R1(config-if)#exit

R1(config-if)#interface g0/3
R1(config-if)#ipv6 ospf 6 area 0
R1(config)#Ipv6 route ::/0 2001:db8:200::2
R1(config)#Ipv6 router ospf 6
R1(config)#Default-information originate

R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
```

```
R3(config)#interface g0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit

R3(config)#interface g0/3
R3(config-if)#ipv6 ospf 6 area 0

D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#no passive-interface g1/0
D1(config-if)#ipv6 ospf 6 area 0

D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface g0/0-3
D2(config-rtr)#passive-interface g2/0-1
D2(config-rtr)#passive-interface g3/0
D2(config-rtr)#exit

D2(config)#interface g1/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
```

4.4 En R2 en la “Red ISP”, configure MP-BGP

En la siguiente parte del desarrollo de la práctica se implementa el multiprotocolo BGP el cual permite transportar la información del enrutamiento y de familias de direcciones IP en las distintas capas que componen la red.

4.4.1 Configuración de ruta estática en R2

```
R2(config)#ipv6 route ::/0 loopback 0
```

///comando para asignar una ruta estática en ipv6
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
///comando para asignar una ruta estática en ipv4

4.4.2 Configuración de router bgp y vecino

A continuación se configuran los PeerBGP o vecinos, que son una relación entre 2 router con el fin de realizar el intercambio de información de protocolo BGP por medio de una conexión TCP. También se realiza la configuración para que los router funcionen dentro del mismo sistema autónomo AS.

R2(config)#router bgp 500
///selección del router bgp y su sistema autónomo AS
R2(config-router)#bgp router-id 2.2.2.2
///configuración de la dirección de acceso a router bgp con su número de
///asignación
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)#neighbor 209.165.200.225 remote-as 300
///se configuran los parámetros del router vecino y su sistema autónomo en ipv4
R2(config-router)# neighbor 2001:db8:200::1 remote as-300
///se configuran los parámetros del router vecino y su sistema autónomo en ipv6
R2(config-router)# address-family ipv4 unicast
///comando que habilita el intercambio de información de routing ipv4 con el
////vecino
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255
///configuración de ruta estática en ipv4
R2(config-router-af)# network 0.0.0.0 mask 0.0.0.0
R2(config-router-af)# exit-address-family
R2(config-router)# address-family ipv6 unicast
///comando que habilita el intercambio de información de routing ipv6 con el vecino
R2(config-router-af)# network 2001:db8:2222::1/128
R2(config-router-af)# network ::/0
///configuración de ruta estática en ipv6
R2(config-router-af)# exit-address-family

4.5 En R1 en la “Red ISP”, configure MP-BGP

En este aparte se configura la ruta estática resumida con la cual se reduce el número de entradas en la tabla de ruteo al resumir varias rutas estáticas en una sola.

R1(config)#ip route 10.0.0.0 255.255.255.0 null0
///configuración de ruta resumen en ipv4
R1(config)#ipv6 route 2001:db8:100::/48 null0
///configuración de ruta resumen en ipv6

```
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#address-family ipv4 unicast
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#no neighbor 2001:db8:200::2 activate
R1(config-router)#neighbor 209.165.200.226 activate
R1(config-router-af)# network 10.0.10.0 mask 255.255.255.0
R1(config-router-af)# exit-address-family

R1(config-router)# address-family ipv6 unicast
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#no neighbor 209.165.200.226 activate
R1(config-router)#neighbor 2001:db8:200::2 activate
R1(config-router-af)# network 2001:db8:200::/64
R1(config-router-af)# exit-address-family
```

5. Configuración de redundancia del primer salto

La red configurada debe tener la posibilidad de detectar una falla en poco tiempo además de ser capaz de recuperarse de la falla sin afectar el servicio. El protocolo HSRP se usa con el fin de que el sistema siga teniendo conmutación durante una falla en alguno de los componentes del primer salto, proporciona redundancia para los hosts. Mediante este protocolo configura un router principal y uno de reserva.

5.1 Configuración de redundancia del primer salto en D1

```
D1(config)#ip sla 4
   ///comando para monitorear un nodo de la red
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-interface g0/1
   ///se configura el funcionamiento del eco icmp con la interfaz como fuente
D1(config-ip-sla-echo)#frequency 5
   ///velocidad de repetición de la operación SLA
D1(config-ip-sla-echo)#exit

D1(config)#ip sla schedule 4 start-time now life forever
   ///define el momento de inicio del proceso y su duración, en este caso siempre
   ////activo
D1(config)#track 4 ip sla 4 state
    ////se crea un objeto con el fin de crear un rastreo del proceso
D1(config-track)#delay up 10 down 15
    ///configuración de tiempo de notificación del proceso sla
D1(config-track)#end
```

```
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1013::1 source-interface g0/1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit

D1(config)#ip sla schedule 6 start-time now life forever
D1(config)#track 6 ip sla 6 state
D1(config-track)#delay up 10 down 15
D1(config-track)#end
```

5.2 Configuración de redundancia de primer salto en D2

```
D2(config)#ip sla 4
D2(config-ip-sla)#Icmp-echo 10.0.11.1 source-interface g0/1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit

D2(config)#ip sla schedule 4 start-time now life forever
D2(config)#track 4 ip sla 4 state
D2(config-track)#delay up 10 down 15
D2(config-track)#end

D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-interface g0/1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit

D2(config)#ip sla schedule 6 start-time now life forever
D2(config)#track 6 ip sla 6 state
D2(config-track)#delay up 10 down 15
D2(config-track)#end
```

5.3 Configuración de HSRPv2 en D1

En el siguiente punto del desarrollo de la actividad se lleva a cabo la configuración de HSRPv2 en los dispositivos, este paso se realiza para que el router activo se encargue de todo el tráfico y el otro router se comporta como pasivo o en espera.

```
R1(config)# interface vlan 100
R1(config-if)# ip address 10.0.100.254 255.255.255.0
R1(config-if)# standby version 2
```
///inicio de la configuración de HSRP usando la versión 2

```
R1(config-if)# standby 104 priority 150
   ///en este comando se especifica el identificador del grupo de HSRP y la
   /// dirección IP que usan los router que conforman el grupo
R1(config-if)# standby 104 preempt
    ///establece el estado de router activo cuando se recupere de una falla
R1(config-if)# standby 104 track 4 decrement 60
   ///crea el objeto de rastreo y establece el decremento en la prioridad después de
  ////una falla
R1(config-if)# no shutdown

R1(config)# interface vlan 101
R1(config-if)# ip address 10.0.101.254 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 114 priority 0
R1(config-if)# standby 114 preempt
R1(config-if)# standby 114 track 4 decrement 60
R1(config-if)# no shutdown

R1(config)# interface vlan 102
R1(config-if)# ip address 10.0.102.254 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 124 priority 150
R1(config-if)# standby 124 preempt
R1(config-if)# standby 124 track 4 decrement 60
R1(config-if)# no shutdown

R1(config)# interface vlan 100
R1(config-if)# standby version 2
R1(config-if)# standby 106 ipv6 autoconfig
R1(config-if)# standby 106 priority 150
R1(config-if)# standby 106 preempt
R1(config-if)# standby 106 track 6 decrement 60
R1(config-if)# no shutdown

R1(config)# interface vlan 101
R1(config-if)# standby version 2
R1(config-if)# standby 116 ipv6 autoconfig
R1(config-if)# standby 116 priority 150
R1(config-if)# standby 116 preempt
R1(config-if)# standby 116 track 6 decrement 60
R1(config-if)# no shutdown
```

```
R1(config)# interface vlan 102
R1(config-if)# standby version 2
R1(config-if)# standby 126 ipv6 autoconfig
R1(config-if)# standby 126 priority 150
R1(config-if)# standby 126 preempt
R1(config-if)# standby 126 track 6 decrement 60
R1(config-if)# no shutdown
```

5.4 Configuración de HSRPv2 en D2

```
R2(config)# interface vlan 100
R2(config-if)# ip address 10.0.100.254 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 104 preempt
R2(config-if)# standby 104 track 4 decrement 60
R2(config-if)# no shutdown

R2(config)# interface vlan 101
R2(config-if)# ip address 10.0.101.254 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 114 priority 150
R2(config-if)# standby 114 preempt
R2(config-if)# standby 114 track 4 decrement 60
R2(config-if)# no shutdown

R2(config)# interface vlan 102
R2(config-if)# ip address 10.0.102.254 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 124 preempt
R2(config-if)# standby 124 track 4 decrement 60
R2(config-if)# no shutdown

R2(config)# interface vlan 100
R2(config-if)# standby version 2
R2(config-if)# standby 106 ipv6 autoconfig
R2(config-if)# standby 106 preempt
R2(config-if)# standby 106 track 6 decrement 60
R2(config-if)# no shutdown

R2(config)# interface vlan 101
```

```
R2(config-if)# standby version 2
R2(config-if)# standby 116 ipv6 autoconfig
R2(config-if)# standby 116 priority 150
R2(config-if)# standby 116 preempt
R2(config-if)# standby 116 track 6 decrement 60
R2(config-if)# no shutdown

R2(config)# interface vlan 102
R2(config-if)# standby version 2
R2(config-if)# standby 126 ipv6 autoconfig
R2(config-if)# standby 126 preempt
R2(config-if)# standby 126 track 6 decrement 60
R2(config-if)# no shutdown
```

6. Seguridad

6.1 Configuración de contraseña usuario exec privilegiado y cuenta scrypt en R1, R3, D1, D2 y A1.

Por medio de la utilización del algoritmo de encriptación scrypt de tipo 9, se protege el acceso al dispositivo encriptando la contraseña además de dar privilegio de usuario de nivel 15, en el caso de este ejercicio el cual da acceso a todos los comandos en la habilitación del router.

Todos los dispositivos a excepción de R2 usan los mismos comandos para la configuración requerida.

```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
   ////el uso de este comando permite habilitar la contraseña de tipo 9 que usa el
   ///algoritmo scrypt para encriptar la contraseña

R1(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
   ///ahora se le asigna privilegio nivel 15 al usuario sadmin además de encriptar la
   ///contraseña tipo 9
```

6.2 Habilitación de AAA en R1, R3, D1, D2 y A1

Para tener un control de seguridad y de acceso a los dispositivos de una red se configura el protocolo de autenticación AAA, con este protocolo se puede negar el acceso a usuarios que intentan tener acceso sin ser autorizados. También se puede hacer un seguimiento de las actividades de los usuarios que ingresan.

Todos los dispositivos a excepción de R2 usan los mismos comandos para la configuración requerida.

D1(config)#username raduser password upass123
///se configura un usuario y contraseña para poder acceder
D1(config)#aaa new-model
///habilitación del modo global del protocolo AAA

6.3 Configuración del servidor Radius en R1, R3, D1, D2 y A1

Radius es un protocolo de autenticación que se usa para poder gestionar el acceso de los usuarios a la red, este servidor verifica que los datos de ingreso sean correctos, si es válido la autenticación es completada por el servidor de lo contrario envía un mensaje de error. Para poder ingresar es necesario tener las credenciales de usuario y contraseña que se asignaron en el paso anterior.

Todos los dispositivos a excepción de R2 usan los mismos comandos para la configuración requerida.

D1(config)#radius server RADIUS
///se agrega el servidor Radius
D1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
///se configura la dirección ip del servidor, se configuran los puertos de acceso y
///autenticación del servidor
D1(config-radius-server)#key $trongPass
///se configura la contraseña de acceso al servidor

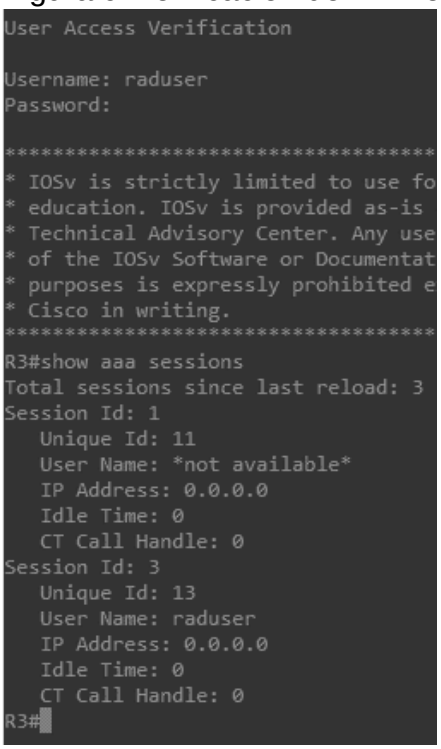
6.4 Configuración de métodos de autenticación AAA

En este aparte se establece los métodos de autenticación del protocolo AAA

A1(config)#aaa authentication login default enable
///se establece el método de acceso por defecto
A1(config)#aaa authentication login default group radius local
///con este comando se indica como primer método de autenticación el servidor
///RADIUS, si este no está disponible pasa al método de acceso secundario
///base de datos local.

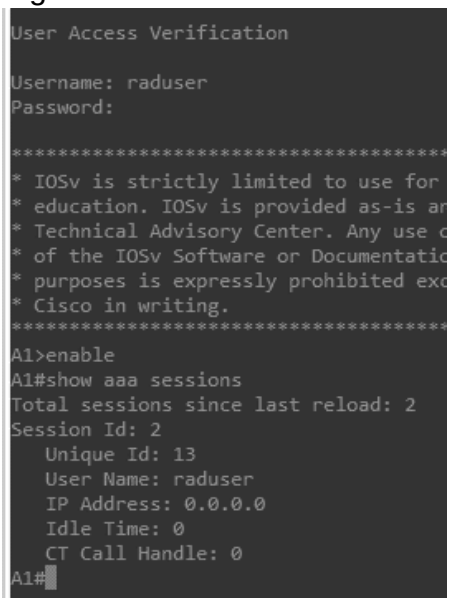
6.5 Verificación del servicio AAA

Figura 9: verificación de AAA en R3



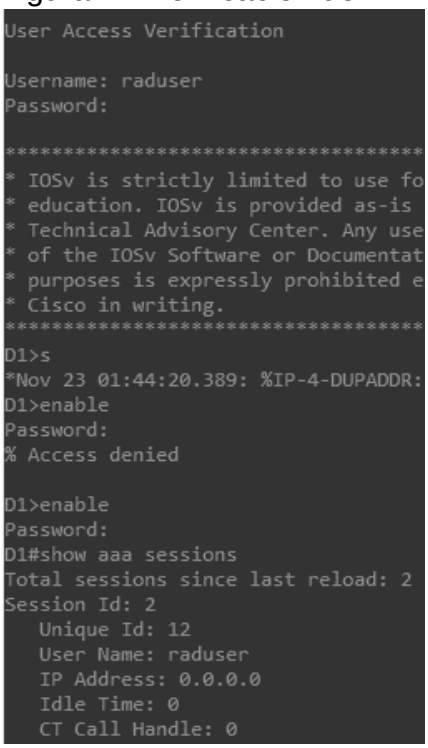
Fuente: propia

Figura 10: verificación de AAA en A1



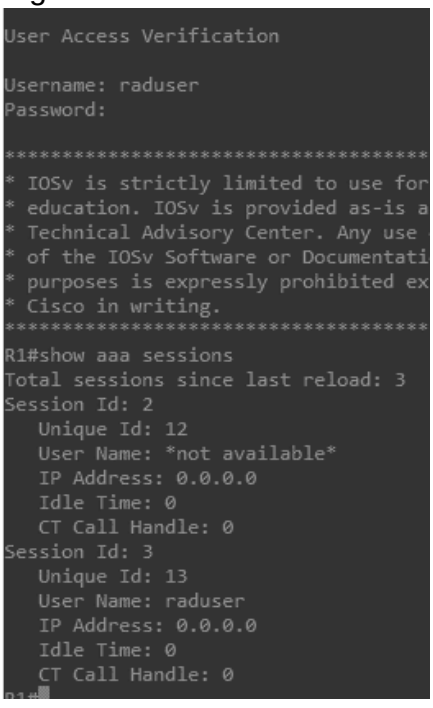
Fuente: propia.

Figura 11: verificación de AAA en D1



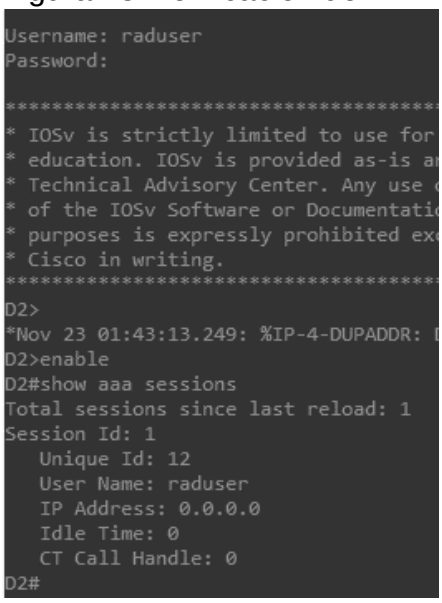
Fuente: propia.

Figura 12: verificación de AAA en R1



Fuente: propia

Figura 13: verificación de AAA en D2



7. Configuración de funciones de administración de la red

7.1 Configuración de reloj formato UTC

Para la configuración del reloj en hora local formato UTC se configura de modo manual.

En todos los dispositivos se configura la hora con el mismo método manual ya que presentan diferencias tanto en horas como en minutos, también es posible usar el comando *clock timezone UTC .*

R3#clock set 21:24:22 nov 22 2021
///configuración de hora y de fecha del dispositivo
R3#show clock detail
///se muestra la configuración actual del reloj
21:25:07.016 UTC Mon Nov 22 2021
Time source is user configuration
///el sistema indica la modificación del reloj por parte del usuario

7.2 Configuración de R2 como NTP maestro

Se configura el router como servidor maestro para sincronizar el tiempo entre todos los dispositivos para facilitar los eventos syslog, así se determina el momento en que sucede un evento.

R2#clock set 21:58:13 nov 22 2021
///configuración manual de la hora y la fecha
R2(config)#ntp master 3
///se configura el servidor como maestro estrato 3

7.3 Configuración de NTP en R1, R3, D1, D2 y A1

Se realiza la configuración del servidor NTP con la dirección IP de R2.

R1(config)#ntp server 209.165.200.226
///se configura el servidor con dirección de R2 como servidor de hora
R1(config)#ntp update-calendar
///se da el comando para actualizar el calendario
R1#show ntp associations
///con este comando se verifica la asociación entre el maestro y el dispositivo
///sincronizado

Luego se configuran los otros dispositivos tomando como maestro a R1:

R3(config)#ntp server 209.165.200.225
R3(config)#ntp update-calendar

D1(config)#ntp server 209.165.200.226
D1(config)#ntp update-calendar

D2(config)#ntp server 209.165.200.226
D2(config)#ntp update-calendar

A1(config)#ntp server 209.165.200.226
A1(config)#ntp update-calendar

7.4 Configuración de syslog en D1,D2,R1,R2,A1

Se configura el servicio para que los dispositivos envíen los mensajes al servidor con dirección 10.0.100.5.

Se utiliza el mismo comando en todos los dispositivos.

D2(config)#logging host 10.0.100.5
///comando para designar la dirección del host para recepción de logs
D2(config)#logging trap warning
///se configuran los logs de warning para ser recibidos en le host

7.5 Configuración de SNMPv2c

El protocolo SNMPv2 se configura con el fin de que el administrador de la red pueda tener control de la red, supervisarla, recibir los mensajes de error y de esta forma dar solución a los mismos.

Al realizar la configuración en los dispositivos switch D1, D2 y A1 no es posible seleccionar el trap config, no aparece en la lista de trap disponibles para los switches.

Configuración en R3,D1,D2

```
snmp-server community ENCORSA RO
   ////habilitación del protocolo snmp el string ENCORSA y el modo de solo lectura
snmp-server enable traps  ospf
  ///se habilitan las traps para la generación de informes en este caso ospf
snmp-server host 10.0.100.5 version 2c ENCORSA
  ///se designa el host destino de los logs y su dirección ip
snmp-server contact Jon Moon
  /// se habilita el valor de contacto
```

Configuración en R1

```
snmp-server community ENCORSA RO
snmp-server enable traps config ospf bgp
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server contact Jon Moon
```

Configuración en A1

```
snmp-server community ENCORSA RO
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server contact Jon Moon
```

CONCLUSIONES

Los conocimientos adquiridos durante el desarrollo del diplomado permitieron realizar la configuración de los diferentes pasos del escenario permitiendo elaborar una red que cumple con los requerimientos de conectividad y funcionalidad.

El uso de los diferentes programas disponibles para la práctica permitió evaluar cuál de los dos es el más apto para llevar a cabo la solución, el uso de GN3S permitió ejecutar la mayor variedad de comandos y pese a que no se pudo implementar al cien por ciento los comandos requeridos si se pudo desarrollar la mayor parte de la practica satisfactoriamente.

El desarrollo de la practica permitió ver un escenario que se asemeja mucho a una situación real, por lo tanto fue necesario la búsqueda y aplicación de diferentes soluciones a los requerimientos, con esto se adquirió solvencia en el manejo de las aplicaciones y su programación.

Por medio de la realización de pruebas de ensayo y error además de la verificación por códigos de línea de comando, como el comando ping o el comando show, se logró finalmente implementar los códigos necesarios para garantizar el correcto funcionamiento de la red.

BIBLIOGRAFIA

Bula J., (2018), Tutorial GNS3: Instalación y Configuración Básica, Telectronika. Recuperado de https://www.telectronika.com/tutoriales/gns3-tutorial-instalacion-configuracion/

Ccna desde cero. Recuperado de https://ccnadesdecero.es/

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

Hernández E., Imágenes Cisco en GNS3 para CCNP Enterprise. Recuperado de https://www.youtube.com/watch?v=GzxDzYn7ZBI&ab_channel=EdsonHernandez

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