DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP.

ROSA LILIANA GETIAL FLOREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
LA HORMIGA
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP.

ROSA LILIANA GETIAL FLOREZ

Diplomado de opción de grado presentado para
optar el título de INGENIERO ELECTRONICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
LA HORMIGA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

HORMIGA, 5 de diciembre 2021

AGRADECIMIENTOS

Agradezco a Dios por permitirme llegar hasta este punto, también a mi pareja porque es el que me permitió tener esta hermosa oportunidad de estudiar, a los instructores, por tener tanta paciencia con nosotros los estudiantes, agradezco a esta institución, por ofrecer esta modalidad a distancia ya que gracias a ustedes logre superarme sin desplazarme a otro lugar.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Dirección IP pública: es el que enruta el tráfico de Internet. Esto se utiliza en Internet y los proveedores de servicios de Internet (ISP) lo entregan a sus clientes.

Dirección IP privada: es una dirección que sirve para el tráfico interno dentro de la LAN. Las direcciones privadas no se pueden enrutar a través de Internet.

El Protocolo de configuración dinámica de host (DHCP): es un protocolo de capa de aplicación que se utiliza para distribuir varios parámetros de configuración de red a dispositivos en una red TCP / IP, direcciones IP, máscaras de subred, puertas de enlace predeterminadas, servidores DNS, etc.

OSPF (Open Shortest Path First): es un protocolo de enrutamiento de estado de enlace. Debido a que es un estándar abierto, lo implementan una variedad de proveedores de red.

IPv4 o Protocolo de Internet versión 4: la dirección es una cadena de números de 32 bits separados por puntos. Identifica de forma única una interfaz de red en un dispositivo.

RESUMEN

En este documento se plasma conocimiento como opción de grado, mostrando otros beneficios que ofrece mi carrera de electrónica, para evidenciar parte de lo adquirido en el aprendizaje de CISCO y CCNP aplicando diferentes maneras de enrutamiento a través del uso de comandos para cada parte y punto.

Así es como se logra de manera correcta resolver el escenario planteado, siguiendo el orden y reconociendo que comandos se aplican para que cada configuración tenga lo necesario, donde el objetivo principal es que la red tenga comunicación en todos los dispositivos.

Palabras Clave: CISCO, CCNP, Enrutamiento, Red, Electrónica.

ABSTRACT

In this document, knowledge is reflected as a degree option, showing other benefits that my electronics career offers, to show part of what I acquired in learning CISCO and CCNP applying different ways of routing through the use of commands for each part and point.

This is how it is achieved in a correct way to solve the proposed scenario, following the order and recognizing which commands are applied so that each configuration has what is necessary, where the main objective is that the network has communication in all the devices.

Keywords: CISCO, CCNP, Routing, Network, Electronics.

INTRODUCCIÓN

El siguiente trabajo se realizó para demostrar todas las habilidades que ha adquirido durante esta etapa de estudio demostrando en este documento una de habilidades enfatizadas hacia las redes de comunicación.

Aquí encontraran seis partes de un diseño donde se realizó la respectiva configuración para que exista una accesibilidad de un dispositivo a otro. Inicialmente construí la red solicitada después comencé a configurar ajustes básicos de cada dispositivo como lo es el direccionamiento de las interfaces para que dos de los computadores puedan recibir direccionamiento de DHCP y los otros dos reciban SLAAC.

Para la siguiente parte se configura los protocolos de enrutamiento IPv4 e IPv6. Además, también se configuro HSRP versión 2 en los switchs, se crea un mecanismo de seguridad mediante usuario y contraseña. Finalmente se configuro varias cosas relacionadas con la administración de red como la hora actual o el nombre del contacto.

DESARROLLO

ESCENARIO PROPUESTO

Figura 1. Topología de red propuesta.

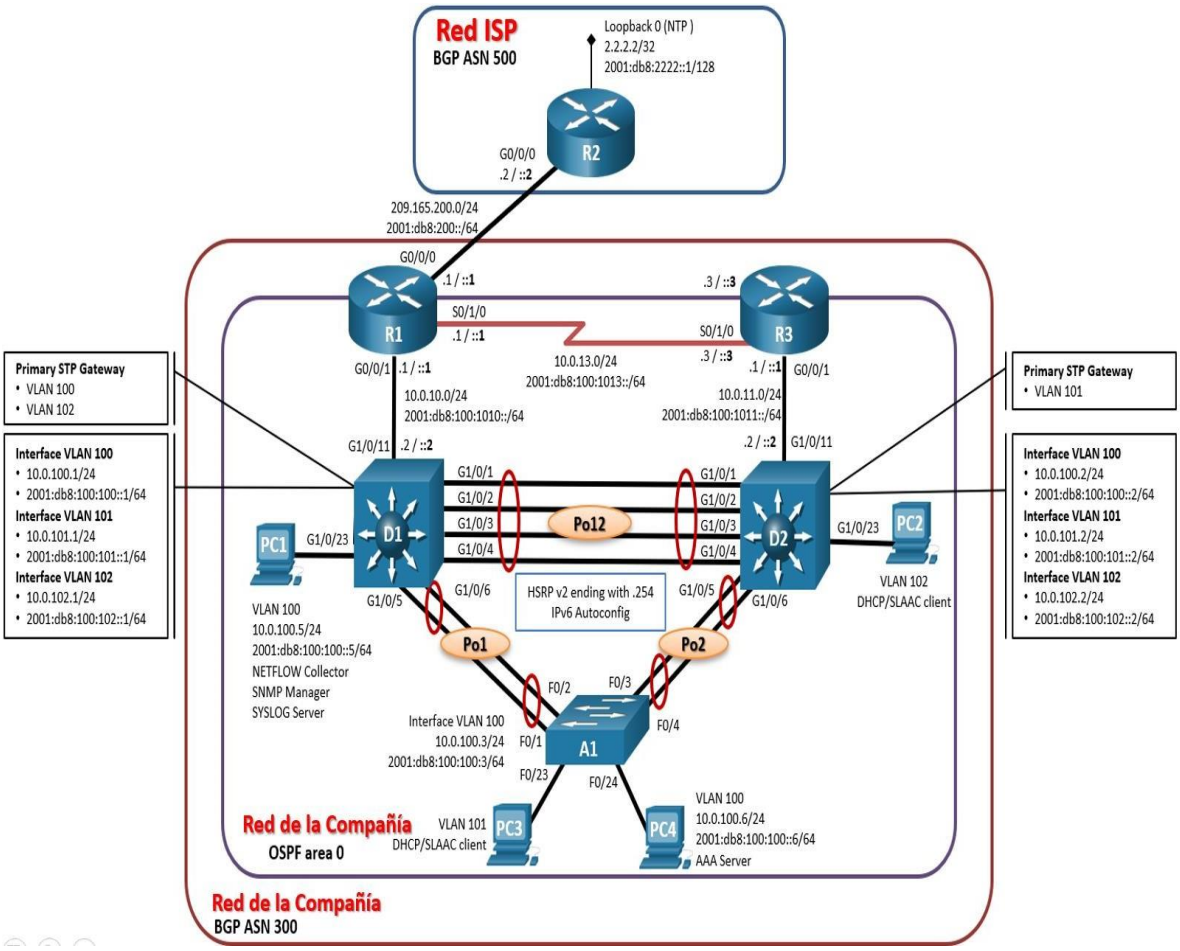


Tabla 1. Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	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	G1/0/11	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

PARTE 1

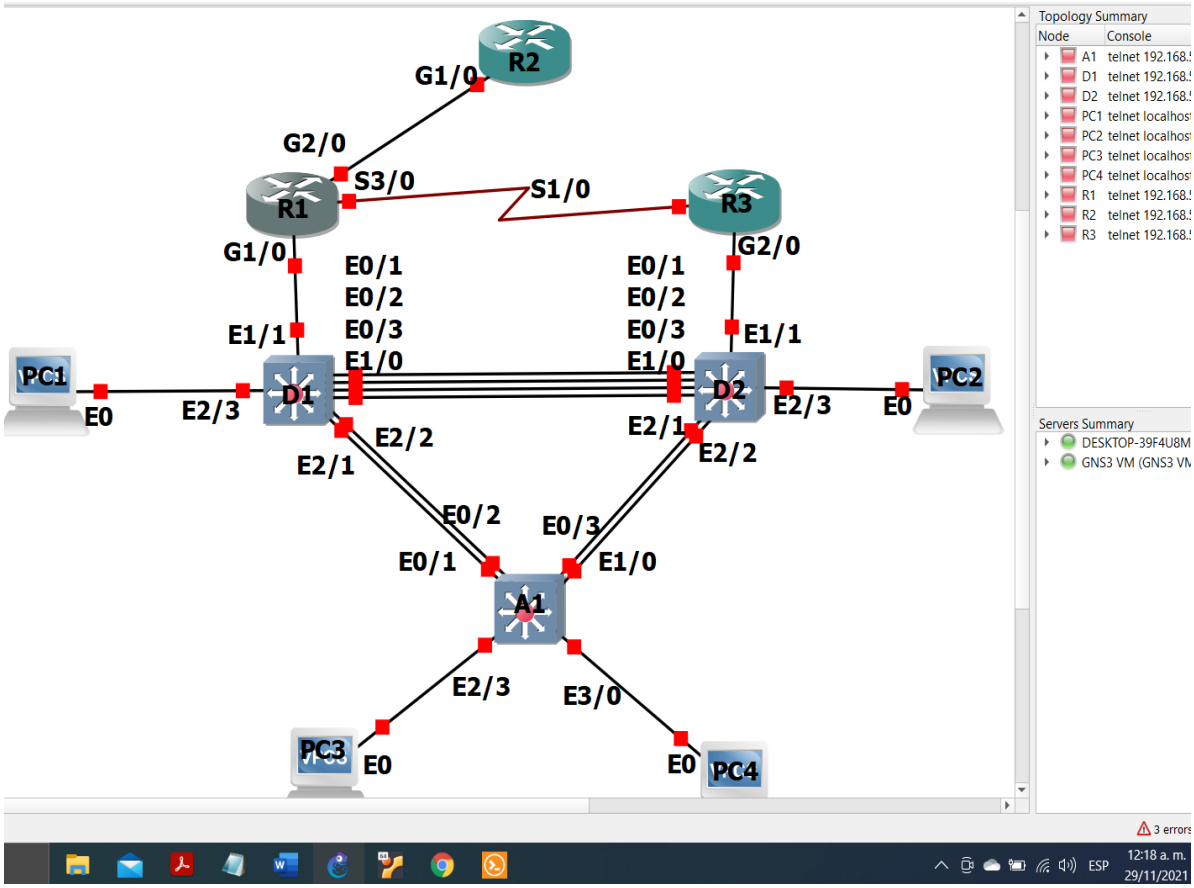
Construir la red y configurar.

Paso 1.

Cablear la red como se muestra en la topología.

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según era necesario.

Figura 2. Mi topología que realice en GNS3.



Paso 2.

Configurar los parámetros básicos.

a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación

Parte a.

Se adjunta código de las configuraciones básicas e iniciales que hice en cada dispositivo de comunicación como lo es el nombre del dispositivo y configuraciones de interfaz de acuerdo a su direccionamiento correspondiente esto lo realicé en los 3 routers y 3 switchs.

ROUTER R1

```
R1#enable
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
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 g2/0
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 g1/0
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 s3/0
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
```

ROUTER 2

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(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 g1/0
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-if)#interface loopback 0
R2(config-if)#
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)#exit
R2(config)#
```

ROUTER 3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(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 g2/0
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-if)#exit
R3(config)#interface s1/0
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)#exit
changed state to up
R3(config)#
```

SWITCH D1

```
D1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D1(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
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 e1/1
D1(config-if)#no switchport
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
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(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
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 e0/0-3,e1/0,e1/2-3,e2/0-3,e3/0-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
```

SWITCH D2

```
D2#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D2(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 e1/1
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::d1:4 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 e0/0-3,e1/0,e1/2-3,e2/0-3,e3/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
```

SWITCH A1

```
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#hostname A1
A1(config)#ip routing
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
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 e1/1-3,e2/0-3,e3/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
```

Parte b.

b. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.

Tabla 2. Se guarda la configuración realizada.

El comando que se empleó.	Función.
copy running-config startup	Con el comando **copy running-config startup** en R1, R2, R3, A1, D1 y D2 guardo la configuración.

Parte c.

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.

Aquí realizo una asignación de ip según la tabla de direcciones:

Tabla 3. Asignación de ip en PC1.

Dispositivo.	**Interfaz.**	**Dirección IPv4.**	**Dirección IPv6.**	**IPv6 Link-Local.**
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC1> **ip 10.0.100.5/24** Checking for duplicate address... PC1 : 10.0.100.5 255.255.255.0				
Solo agregue la palabra **ip** más la dirección que deseo asignar la cual fue **10.0.100.5/24**.				

Tabla 4. Asignación de ip en PC4.

Dispositivo.	**Interfaz.**	**Dirección IPv4.**	**Dirección IPv6.**	**IPv6 Link-Local.**
PC4	NIC	10.0.100.6/24	2001:db8:100:100::5/64	EUI-64
PC4> **ip 10.0.100.6/24** Checking for duplicate address... PC1 : 10.0.100.6 255.255.255.0				
Solo agregue la palabra **ip** más la dirección que deseo asignar la cual fue **10.0.100.6/24**.				

Parte 2.

Configurar la capa 2 de la red y el soporte de Host.

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switchs debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 5. Tareas 2.1, 2,2 y 2,3.

Tarea .	Tarea.	Especificación.
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces deinterconexión entre switches.	Habilite los enlaces troncales de 802.1Q entre: D1 con D2, D1 con d A1 y D2 con A1.
Switch D1.	interface range e0/1-3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk interface range e2/1-2 switchport trunk encapsulation dot1q switchport mode trunk	Habilite los enlaces troncales 802.1Q entre: D1 con D2 y D1 con A1.

Switch D2.	interface range e0/1-3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk interface range e2/1-2 switchport trunk encapsulation dot1q switchport mode trunk	Habilite los enlaces troncales 802.1Q entre: D1 con D2 y D2 con A1.
Switch A1.	interface range e0/1-2 switchport trunk encapsulation dot1q switchport mode trunk interface range e0/3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk	Habilite los enlaces troncales 802.1Q entre: A1 con D1 y A1 con D2.
2.2	En todos los switches cambie la VLAN nativaen los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
Switchs D1, D2 y A1.	switchport trunk native vlan 999	Use VLAN 999 como la VLAN nativa en todos los switchs.

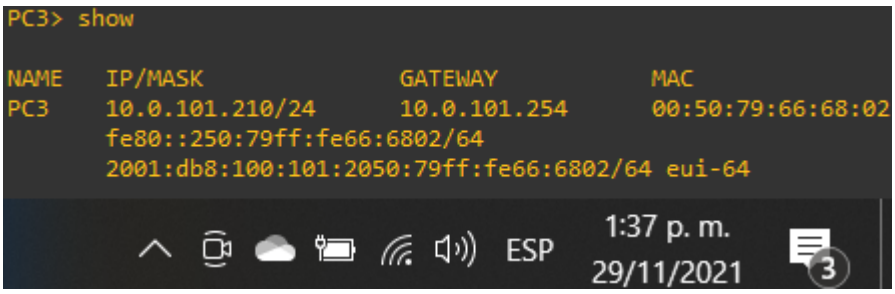
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use el protocol Rapid Spanning Tree (RSPT).
Switch D1 y D2.	spanning-tree mode rapid-pvst spanning-tree portfast	habilite el protocolo RSPTen los switchs D1 y D2.
Switch A1	spanning-tree portfast	habilite el protocolo RSPT en el switch A1.

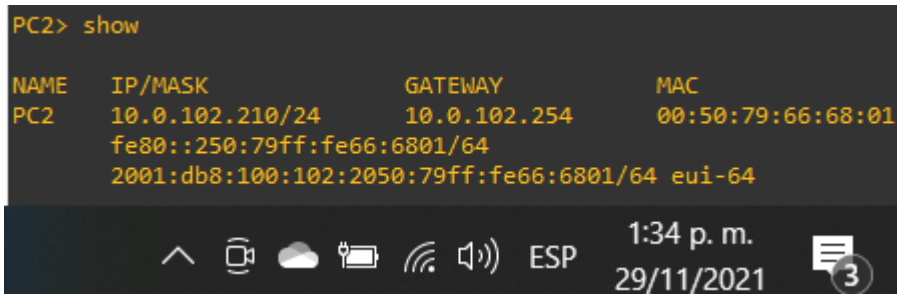
Tabla 6. Tareas 2.4, 2.5, 2.6, 2.7 y 2.8.

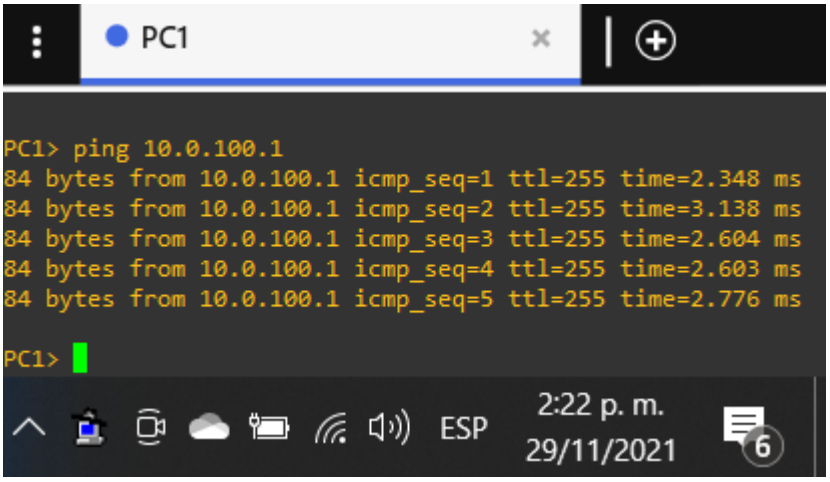
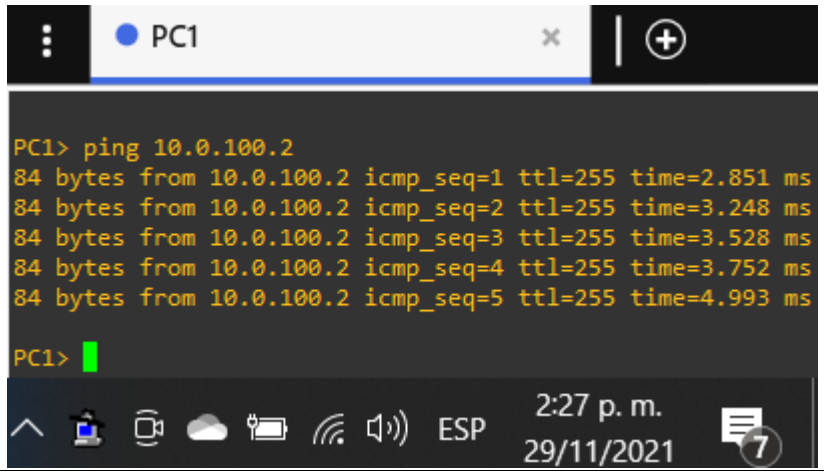
Tarea.	Tarea.	Especificación.
2.4	En D1 y D2, configure los puentes raíz RSTP(root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en casode falla del puente raíz (root bridge).	Configure D1 y D2 como raíz para las VLAN apropiadas, con prioridades deapoyo mutuo en caso de falla del switch.
Switch D1.	spanning-tree vlan 100,102 root primary spanning-tree vlan 101 root secondary	Configure D1 como raíz para las VLAN apropiadas, con prioridades deapoyo mutuo en caso de falla del switch.
Switch D2.	spanning-tree vlan 101 root primary spanning-tree vlan 100,102 root secondary	Configure D2 como raíz para las VLAN apropiadas, con prioridades deapoyo mutuo en caso de falla del switch.

2.5	En todos los switches, cree los canales LACP como se muestra en el diagrama detopología.	Use los siguientes números de canales: en D1 a D2 el canal 12, en D1 a A1 el canal 1, en D2 a A1 el canal 2.
Switch D1.	channel-group 12 mode active channel-group 1 mode active	En todos los switchs, cree LACP. De D1 a D2 el canal 12. De D1 a A1 el canal 1.
Switch D2.	channel-group 12 mode active channel-group 2 mode active	En todos los switchs, cree el canal LACP. De D1 a D2 el canal 12. De D2 a A1 el canal 2.
Switch A1.	channel-group 1 mode active channel-group 2 mode active	En todos los switchs, cree el canal LACP. De D1 a A1 el canal 1. De D2 a A1 el canal 2.

2.6	En todos los switches, configure los puertos de acceso del host que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.
En D1.	interface e2/3 switchport mode Access switchport access vlan 100 spanning-tree portfast no shutdown exit	Configuración de VLAN para la interfaz PC1.
En D2.	Interface e2/3 switchport mode Access switchport access vlan 102 spanning-tree portfast no shutdown exit	Configuración de VLAN para la interfaz PC2.
En D3.	interface e2/3 switchport mode access switchport access vlan 101 spanning-tree portfast no shutdown exit	Configuración de VLAN para la interfaz PC3 y PC4.

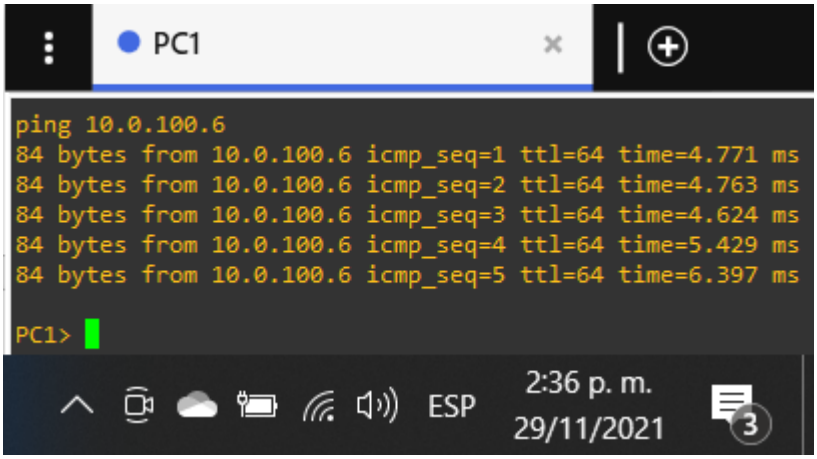
	interface e3/0 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end	
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y debenrecibir direcciones IPv4 válidas.
PC3	PC3> ip dhcp DDORA IP 10.0.101.210/24 GW 10.0.101.254	Primero configure PC3 con dirección IPv4 de DHCP.
Evidencia de que en PC3 verifique los servicios DHCP IPv4.		
Figura 3. Evidencia en PC3. 		

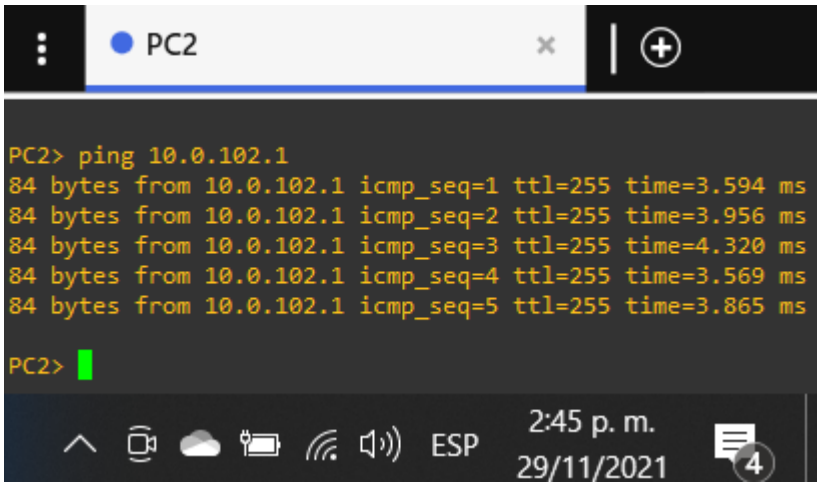
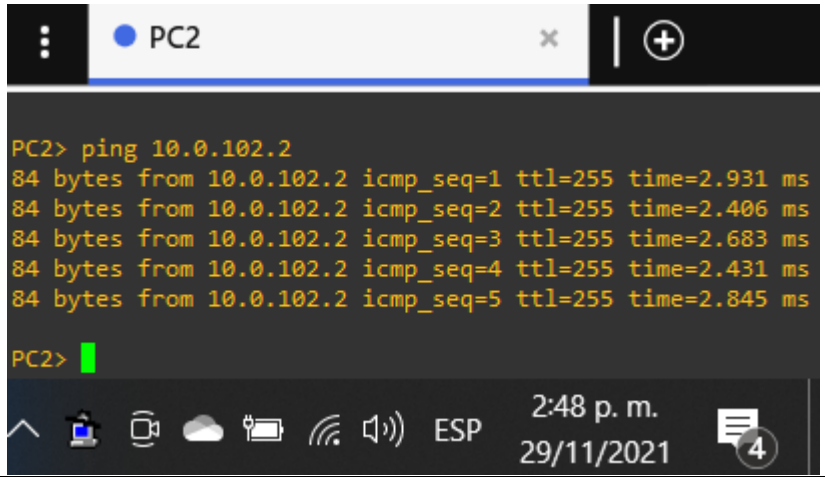
<table>
<tr><td>PC2</td><td>PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254</td><td>Primero configure PC2 con dirección IPv4 de DHCP.</td></tr>
<tr><td colspan="3">Evidencia de que en PC2 verifique los servicios DHCP IPv4</td></tr>
<tr><td colspan="3">Figura 4. Evidencia en PC2.
 
</td></tr>
<tr><td>2.8</td><td>Verifique la conectividad de la LAN local.</td><td>PC1 debería hacer ping con éxito a: D1, D2 y PC4.</td></tr>
<tr><td></td><td colspan="2">Verifique la conectividad de la LAN local al hacer Ping desde PC1 a D1: ping 10.0.100.1.</td></tr>
</table>

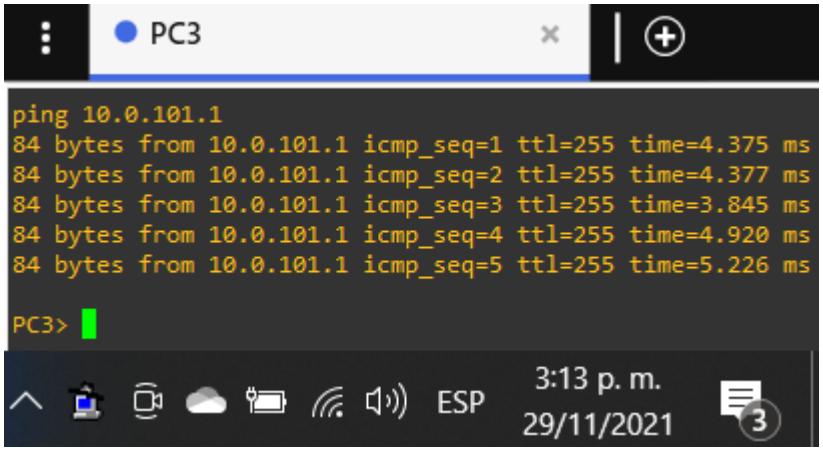
PC1	Figura 5. Ping desde PC1 a D1. 
PC1	Verifique la conectividad de la LAN local al hacer Ping desde PC1 a D2: ping 10.0.100.2. Figura 6. Ping desde PC1 a D2. 

<table>
<tr><td>PC1</td><td colspan="2">Verifique la conectividad de la LAN local al hacer Ping desde PC1 a PC4: ping 10.0.100.6.

Figura 7. Ping desde PC1 a PC4.

 
</td></tr>
<tr><td>PC2</td><td>Verifique la conectividad de la LAN local.</td><td>PC2 debería hacer ping con éxito a:
• D1: 10.0.102.1
• D2: 10.0.102.2</td></tr>
</table>

PC2	Verifique la conectividad de la LAN local al hacer Ping desde PC2 a D1: ping 10.0.102.1. Figura 8. Ping desde PC2 a D1. 
PC2	Verifique la conectividad de la LAN local al hacer Ping desde PC2 a D2: ping 10.0.102.2. Figura 9. Ping desde PC2 a D2. 

PC3	Verifique la conectividad de la LAN local.	PC3 debería hacer ping con éxito a: D1 y a D2.
PC3	Verifique la conectividad de la LAN local al hacer Ping desde PC3 a D1: ping 10.0.101.1. Figura 10. Ping desde PC3 a D1. 	
PC3	Verifique la conectividad de la LAN local al hacer Ping desde PC3 a D2: ping 10.0.101.2.	

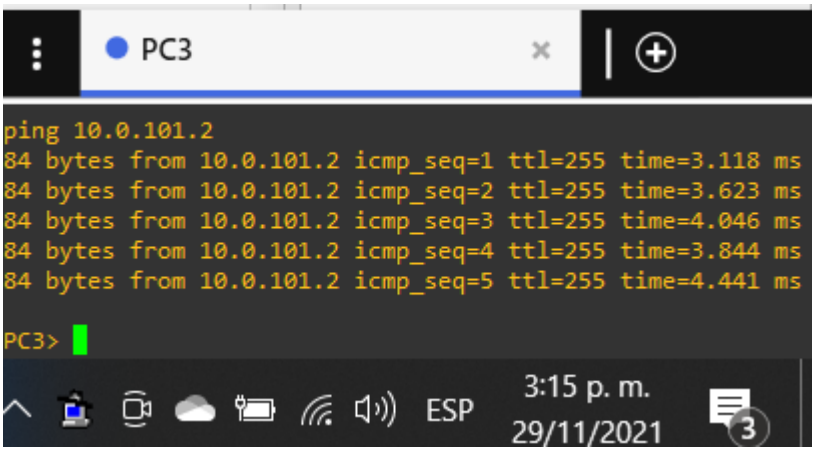
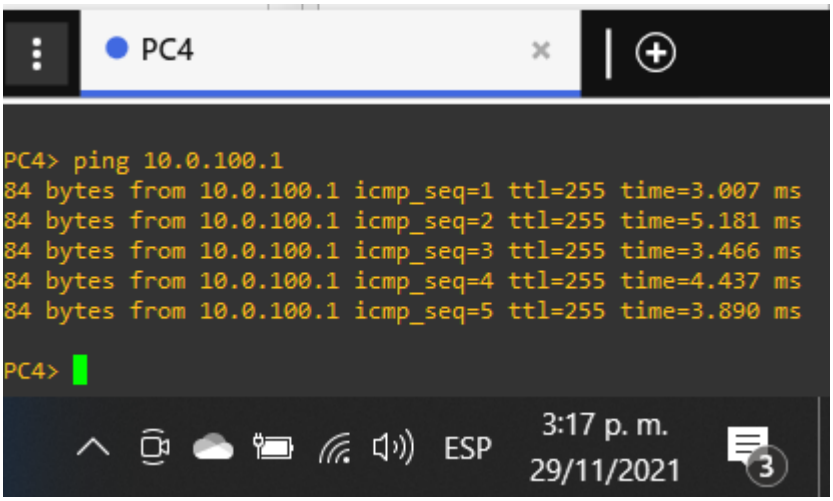
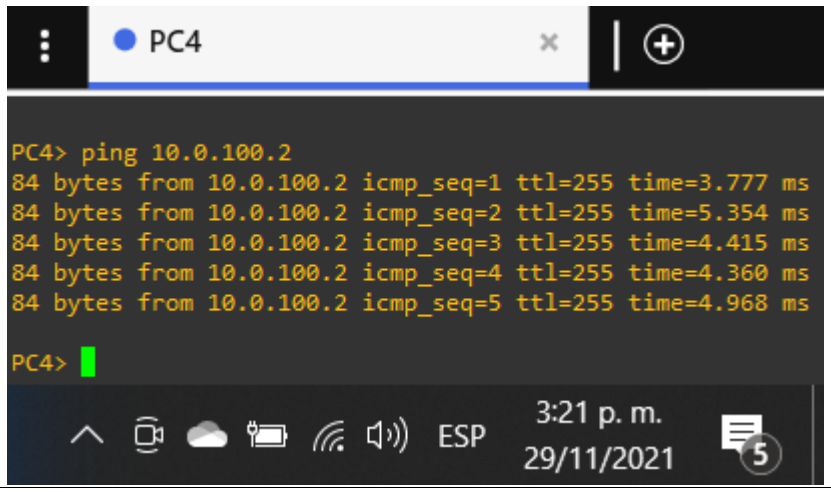
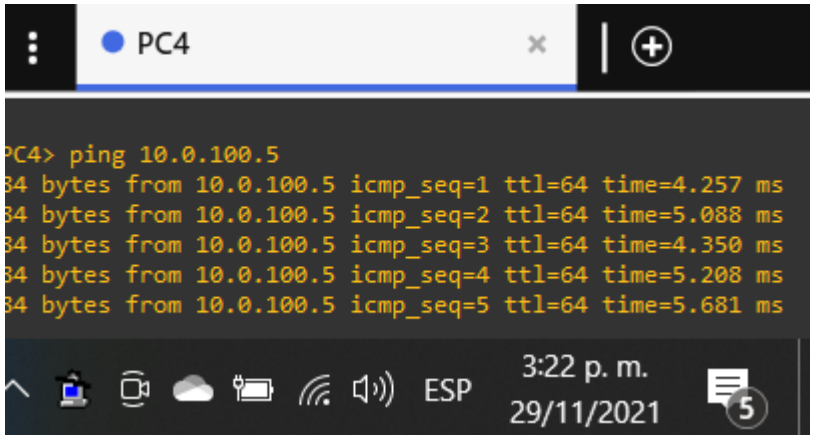
<table>
<tr><td></td><td colspan="2">Figura 11. Ping desde PC3 a D2.
 
</td></tr>
<tr><td>PC4</td><td>Verifique la conectividad de la LAN local.</td><td>PC4 debería hacer ping con éxito a:
D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5</td></tr>
<tr><td>PC4</td><td colspan="2">Verifique la conectividad de la LAN local al hacer Ping desde PC4 a D1: ping 10.0.100.1.</td></tr>
</table>

	Figura 12. Ping desde PC4 a D1. 
PC4	Verifique la conectividad de la LAN local al hacer Ping desde PC4 a D2: ping 10.0.100.2. Figura 13. Ping desde PC4 a D2. 

PC4	Verifique la conectividad de la LAN local al hacer Ping desde PC4 a PC1: ping 10.0.100.5 Figura 14. Ping desde PC4 a PC1. 

Resumen de códigos para la parte 2.

SWITCH D1

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface range e0/1-3, e1/0
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range e2/1-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface e2/3
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on Ethernet2/3 but will only
 have effect when the interface is in a non-trunking mode.
D1(config-if)#no shutdown
D1(config-if)#exit
```

SWITCH D2

```
D2#
D2#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#interface range e0/1-3, e1/0
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D2(config-if-range)#
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface range e2/1-2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#!
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#!
D2(config)#interface e2/3
D2(config-if)#switchport mode Access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on Ethernet2/3 but will only
 have effect when the interface is in a non-trunking mode.
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#end
```

SWITCH A1

```
A1#
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range e0/3, e1/0
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface e2/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface e3/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#end
```

Parte 3.

Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Comandos utilizados en esta parte 3.

Tabla 7. Tarea 3.1.

Tarea.	Tarea.	Especificación.
3.1	Comandos para las configuraciones solicitadas:	Configure OSPFv2 en area 0.
R1	enable conf term router ospf 4 router-id 0.0.4.1 do show ip route connected network 10.0.10.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0 default-information originate exit	En R1, use OSPF con ID 4 quedando así en R1 0.0.4.1.

R3	enable conf term router ospf 4 router-id 0.0.4.3 do show ip route connected network 10.0.11.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0 default-information originate exit	En R3, use OSPF con ID **4** quedando así en R3 0.0.4.3.
D1	config t router ospf 4 router-id 0.0.4.131 do show ip route connected network 10.0.10.0 0.0.0.255 area 0 network 10.0.100.0 0.0.0.255 area 0 network 10.0.101.0 0.0.0.255 area 0 network 10.0.102.0 0.0.0.255 area 0 passive-interface default no passive-interface e1/1	En D1, use OSPF con ID **4** quedando así en D1 0.0.4.131. En D1, anuncie todas las redes directamente conectadas en área 0. En D1 deshabilite las publicaciones OSPFv2 excepto e1/1.

D2	config t router ospf 4 router-id 0.0.4.132 do show ip route connected network 10.0.100.0 0.0.0.255 area 0 network 10.0.101.0 0.0.0.255 area 0 network 10.0.102.0 0.0.0.255 area 0 network 10.0.11.0 0.0.0.255 area 0 passive-interface default no passive-interface e1/1	En D2, use OSPF con ID **4** quedando así en D2 0.0.4.132. En D2, anuncie todas las redes directamente conectadas en área 0. En D2 deshabilite las publicaciones OSPFv2 excepto e1/1.

Tabla 8.Tarea 3.2.

Tarea.	Tarea.	Especificación.
3.2	Comandos para las configuraciones solicitadas:	Configure classic single-area OSPFv3 en area 0.
R1	en conf term ipv6 unicast-routing router ospf 6 router-id 0.0.6.1 default-information originate exit int g1/0 ipv6 ospf 6 area 0 exit int s3/0 ipv6 ospf 6 area 0 exit	Habilita globalmente IPv6. En R1, use OSPF con ID 6 quedando así en R1 0.0.6.1. En R1 anuncie todas las redes directamente conectadas en área 0.
R3	en conf term ipv6 unicast-routing router ospf 6 router-id 0.0.6.3 exit interface g2/0 ipv6 ospf 6 area 0	Habilita globalmente IPv6. En R3, use OSPF con ID 6 quedando así en R3 0.0.6.3.

	exit int s1/0 ipv6 ospf 6 area 0 exit	En R3, anuncie todas las redes directamente conectadas en área 0.
D1	config t router ospf 6 router-id 0.0.6.131 exit interface e1/1 ipv6 ospf 6 area 0 inter vlan100 ipv6 ospf 6 area 0 inter vlan101 ipv6 ospf 6 area 0 inter vlan102 ipv6 ospf 6 area 0	En D1, use OSPF con ID 6 quedando así en D1 0.0.6.131. En D1, anuncie todas las redes directamente conectadas en área 0. En D1 deshabilite las publicaciones OSPFv3 excepto e1/1.
D2	config t router ospf 6 router-id 0.0.6.132 exit interface e1/1 ipv6 router ospf 6 area 0 ipv6 ospf 6 area 0 interface vlan100 ipv6 ospf 6 area 0	En D2, use OSPF con ID 6 quedando así en D2 0.0.6.132. En D2, anuncie todas las redes directamente conectadas en área 0.

	interface vlan101 ipv6 ospf 6 area 0 interface vlan102 ipv6 ospf 6 area 0 exit	En D2 deshabilite las publicaciones OSPFv3 excepto e1/1.

Tabla 9. Tareas 3.3 y 3.4.

Tarea.	Tarea.	Especificación.
3.3	Comandos para las configuraciones solicitadas:	En R2 en la “Red ISP”, configure MP-BGP.
En R2.	ip route 0.0.0.0 0.0.0.0 loopback 0	Interfaz Loopback 0 para dos rutas estáticas.
	ipv6 route ::/0 loopback 0	
	router bgp 500	Configuración de BGP ASN **500.**
	bgp router-id 2.2.2.2	Use el id 2.2.2.2.
	neighbor 209.165.200.225 remote-as 300	
	neighbor 2001:db8:200::1 remote-as 300	Es una ruta estática predeterminada IPv4 en ASN 300.
	address-family ipv4 unicast	
	network 2.2.2.2 mask 255.255.255.255	Se usa otra ruta estática predeterminada IPv6 en ASN 300.
	network 0.0.0.0 mask 0.0.0.0	
	address-family ipv6 unicast	En IPv4 se anuncia la red familia. La red loopback 0 quedaría así; la dirección IPv4 2.2.2.2/32 y la ruta por defecto.
	network 2001:db8:200::1/128	
	network ::/0	En IPv6 anuncia la red familia loopback 0 quedaría así; la dirección IPv6/128 y la ruta por defecto.

3.4	Comandos para las configuraciones solicitadas:	En R1 en la “Red ISP”, configure MP como BGP.
R1	ip route 10.0.0.0 255.255.255.0 null 0 router bgp 300 bgp router-id 1.1.1.1 neighbor 209.165.200.226 remote-as 500 address-family ipv4 unicast address-family ipv6 unicast network 2001:db8:200::1/128	Configuración de la ruta resumen estáticas a la interfaz NULL 0. Configuración en BGP ASN así **300.** Use el id 1.1.1.1 en el router. Configuración de una relación de vecino IPv4 e IPv6 con R2 en ASN 500. Habilite la relación de vecino IPv4. Habilite la relación de vecino IPv6. Anuncie la red.

Parte 4.

Configurar la Redundancia del Primer Salto. En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los host en la “Red de la Compañía”.

Tabla 10. Tareas 4.1 y 4.2.

Tarea.	Tarea.	Especificación.
4.1	Comandos para las configuraciones solicitadas.	En D1, cree IP SLAS que prueben la accesibilidad dela interfaz R1 G1/0.
D1	configure terminal ip sla 4 icmp-echo 10.0.10.1 frequency 5 exit ip sla schedule 4 start-time now life forever	Define el numero de la “sesión” del SLA que es 4 para IPv4. Cree una IP SLA **4** para IPv4. Cada cuanto tiempo se va a enviar el mensaje. Habilita la SLA para que se ejecute indefinidamente. Se conoce la disponibilidad de “objetos”.

	track 4 ip sla 4 state delay up 10 down 15 exit ip sla 6 icmp-echo 2001:db8:100:1010::1 frequency 5 exit ip sla schedule 4 life forever start-time now ip sla schedule 6 life forever start-time now track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit	Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos. Cree una IP SLA **6** para IPv6. Cada cuanto tiempo se va a enviar el mensaje. Habilito la SLA **4** para IPv4 para indicar que empiece. Habilito la SLA **6** para IPv6 para indicar que empiece. Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	Comandos para las configuraciones solicitadas.	En D2, cree IP SLAS que prueben la accesibilidad dela interfaz R3 G2/0.

D2		Define numero de la “sesión” del SLA que es 4 para IPv4.
	conf term ip sla 4 icmp-echo 10.0.11.1 frequency 5 exit	Cree una IP SLA **4** para IPv4. Cada cuanto tiempo se va a enviar el mensaje.
	ip sla 6 icmp-echo 2001:db8:100:1010::1 frequency 5 exit	Cree una IP SLA **6** para IPv6. Cada cuanto tiempo se va a enviar el mensaje.
	ip sla schedule 4 life forever start-time now	Habilito la SLA **4** para IPv4 para indicar que empiece.
	ip sla schedule 6 life forever start-time now	Habilito la SLA **6** para IPv6 para indicar que empiece.
	track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit	Conoce la disponibilidad de “objetos”. Los objetos rastreados deben notificar a D2 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Tabla 11. Tarea 4.3.

Tarea.	Especificación.
4.3	En D1 configure HSRPv2.
interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 priority 150 standby 104 preempt standby 104 track 4 decrement 60	Configuración de HSRP como versión 2. Configuración de IPv4 en HSRP como grupo **104** para la VLAN 100. Su prioridad también se cambiará a 150.
interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 preempt standby 114 track 4 decrement 60	Configuración de IPv4 en HSRP como grupo **114** para la VLAN 101.
interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 priority 150 standby 124 preempt standby 124 track 4 decrement 60	Configuración de IPv4 en HSRP como grupo **124** para la VLAN 102.

standby 106 ipv6 autoconfig standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 60	Configuración de IPv6 en HSRP como grupo **106** para la VLAN 100.
standby 116 ipv6 autoconfig standby 116 preempt standby 116 track 6 decrement 60	Configuración de IPv6 en HSRP como grupo **116** para la VLAN 101.
standby 126 ipv6 autoconfig standby 126 priority 150 standby 126 preempt standby 126 track 6 decrement 60	Configure IPv6 HSRP grupo **126** para la VLAN 102.

Tabla 12. Tarea 4.4.

Tarea.	**Especificación.**
4.4. Comandos.	En D2, configure HSRPv2.
interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 track 4 decrement 60	Configuración de HSRP como versión 2. Configuración de IPv4 en HSRP como grupo **104** para la VLAN 100.
interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 priority 150 standby 114 preempt	Configuración de IPv4 en HSRP como grupo **114** para la VLAN 101.
interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60	Configuración de IPv4 en HSRP como grupo **124** para la VLAN 102.

standby 106 ipv6 autoconfig standby 106 preempt standby 106 track 6 decrement 60	Configuración de IPv6 en HSRP como grupo **106** para la VLAN 100.
standby 116 ipv6 autoconfig standby 116 priority 150 standby 116 preempt standby 116 track 6 decrement 60	Configure de IPv6 en HSRP como grupo **116** para la VLAN 101.
standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60	Configuración de IPv6 en HSRP grupo **126** para la VLAN 102.

Parte 5.

Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración se encuentran en la siguiente tabla.

Tabla 13. Tareas 5.1, 5.2, 5.3, 5.4, 5.5 y 5.6.

Tarea.	Tarea.	Especificación.
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmode SCRYPT.	Contraseña: **cisco12345cisco**
R1	conf term enable password cisco12345cisco service password-encryption	Asigno contraseña. Protejo el EXEC privilegiado.
R3	conf term enable password cisco12345cisco service password-encryption	Asigno contraseña. Protejo el EXEC privilegiado.

D1	conf term enable password cisco12345cisco service password-encryption	Asigno contraseña. Protejo el EXEC privilegiado.
D2	conf term enable password cisco12345cisco service password-encryption	Asigno contraseña. Protejo el EXEC privilegiado.
A1	conf term enable password cisco12345cisco service password-encryption	Asigno contraseña. Protejo el EXEC privilegiado.
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de SCRYPT.	Detalles de la cuenta encriptada SCRYPT así: nombre de usuario local como: **sadmin,** nivel de privilegio **15** y contraseña: **cisco12345cisco.**

R1	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nombre de usuario local como: **sadmin.** Nivel de privilegio **15.** Contraseña: **cisco12345cisco.**
R3	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nombre de usuario local como: **sadmin.** Nivel de privilegio **15.** Contraseña: **cisco12345cisco.**
D1	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nombre de usuario local como: **sadmin.** Nivel de privilegio **15.** Contraseña: **cisco12345cisco.**

D2	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nombre de usuario local como: **sadmin.** Nivel de privilegio **15.** Contraseña: **cisco12345cisco.**
A1	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nombre de usuario local como: **sadmin.** Nivel de privilegio **15.** Contraseña: **cisco12345cisco.**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.

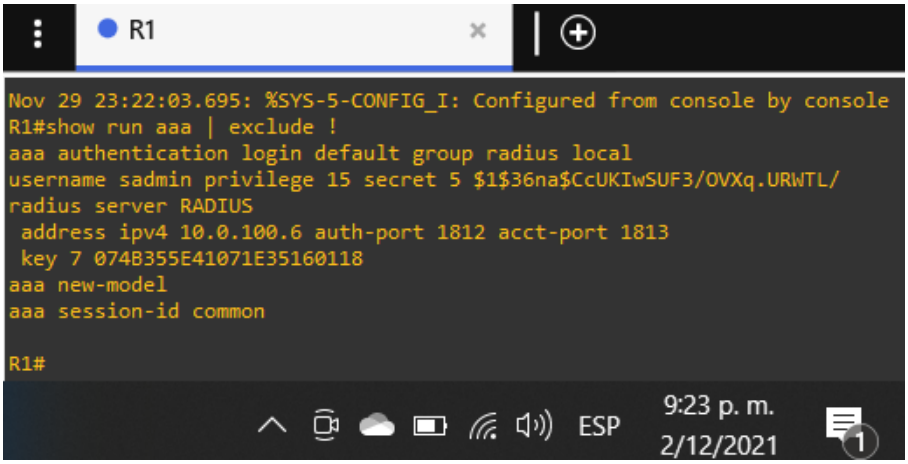
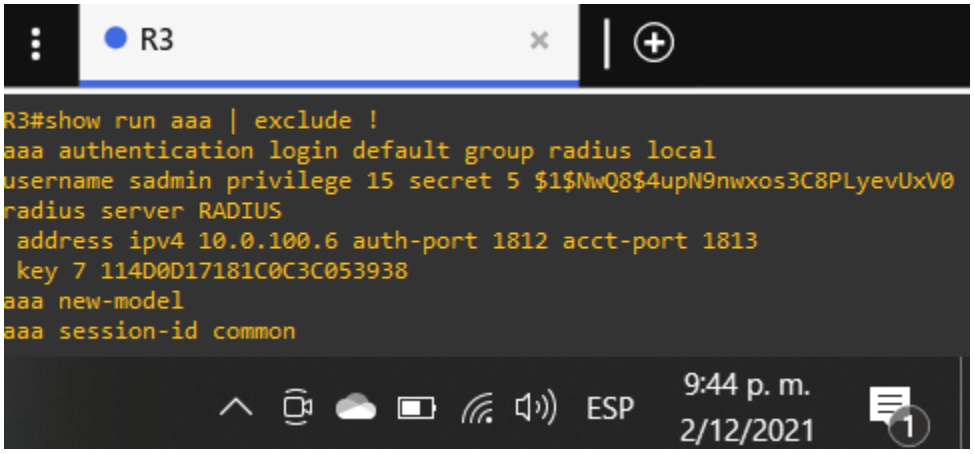
R1	aaa new-model	Este es el comando para habilitar AAA en R1.
R3	aaa new-model	Este es el comando para habilitar AAA en R3.
D1	aaa new-model	Este es el comando para habilitar AAA en D1.
D2	aaa new-model	Este es el comando para habilitar AAA en D2.
A1	aaa new-model	Este es el comando para habilitar AAA en A1.

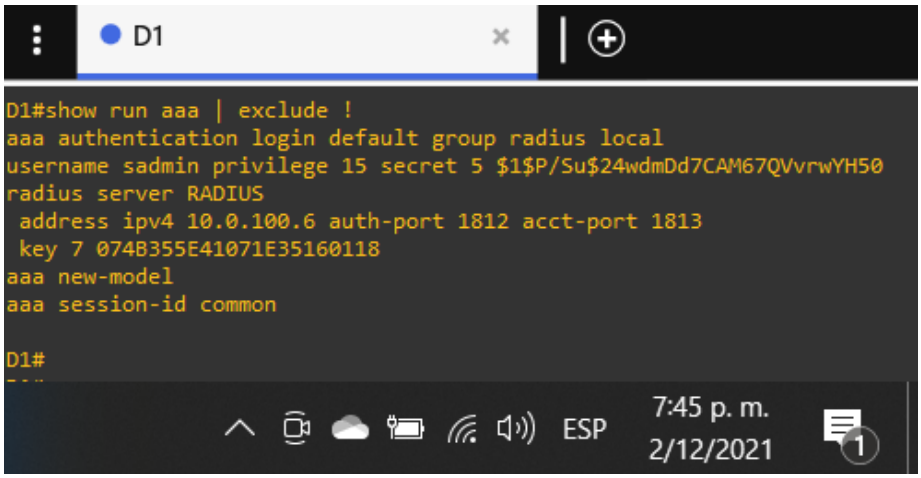
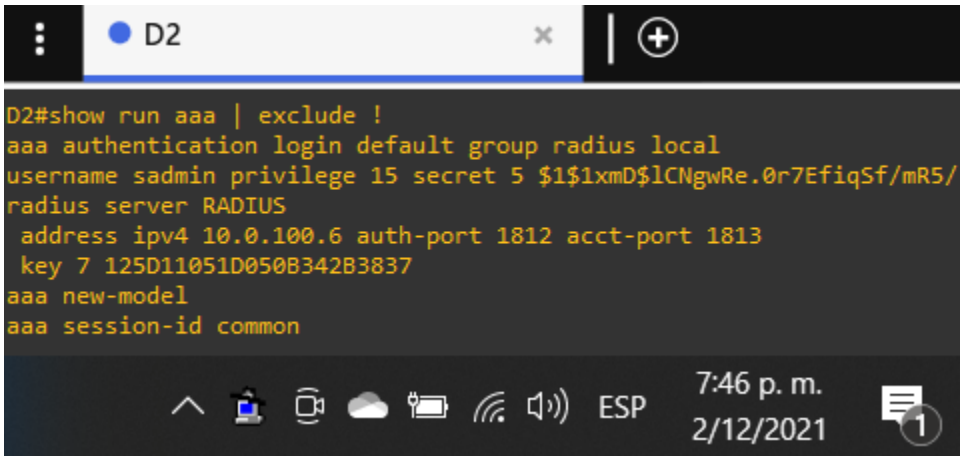
5.4	En todos los dispositivos, configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS: con dirección IP del servidor RADIUS es10.0.100.6, puertos UDP del servidor RADIUS son1812, 1813 y contraseña: **$trongPass.**
R1	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Nombre del servidor RADIUS. Se crea un grupo de servidores con miembros del servidor RADIUS, cada uno con la misma dirección IP pero con puertos de autenticación y contabilidad únicos. Contraseña: **$trongPass.**
R3	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Nombre del servidor RADIUS. Se crea un grupo de servidores con miembros del servidor RADIUS, cada uno con la misma dirección IP pero con puertos de autenticación y contabilidad únicos. Contraseña: **$trongPass.**

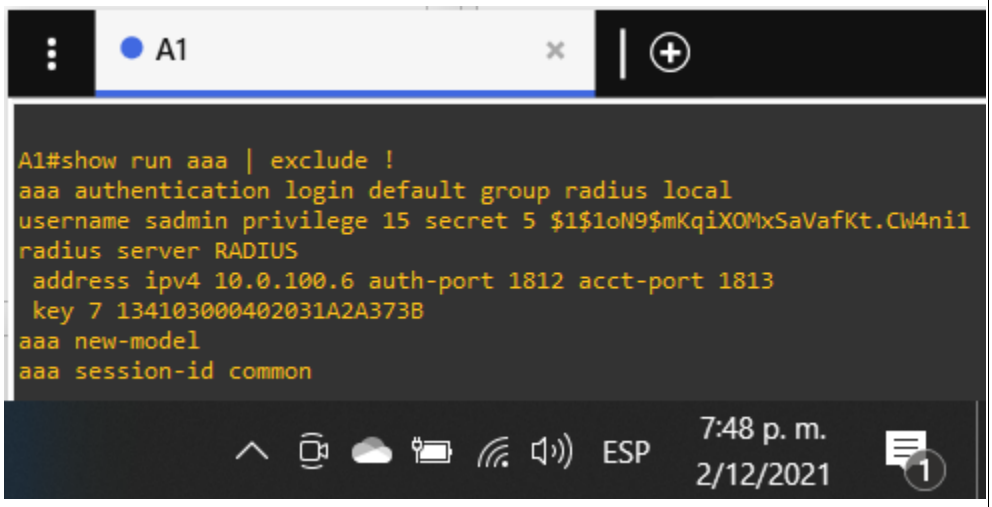
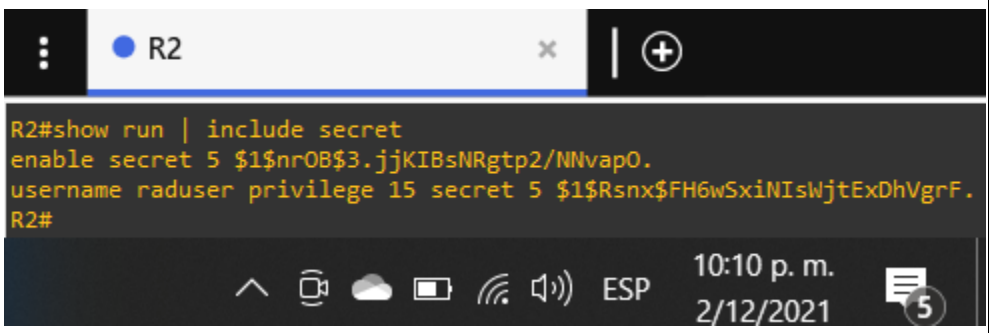
D1	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Nombre del servidor RADIUS. Se crea un grupo de servidores con miembros del servidor RADIUS, cada uno con la misma dirección IP pero con puertos de autenticación y contabilidad únicos. Contraseña: **$trongPass.**
D2	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Nombre del servidor RADIUS. crear un grupo de servidores con miembros del servidor RADIUS, cada uno con la misma dirección IP pero con puertos de autenticación y contabilidad únicos. Contraseña: **$trongPass.**
A1	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Nombre del servidor RADIUS. crear un grupo de servidores con miembros del servidor RADIUS, cada uno con la misma dirección IP pero con puertos de autenticación y contabilidad únicos.

		Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: use la lista de métodos por defecto, valide contra el grupo de servidores RADIUS o de lo contrario, utilice la base de datos local.
R1	config t aaa authentication login default group radius local end	Método de autenticación de EXEC. Utilice la base de datos local.
R3	config t aaa authentication login default group radius local end	Método de autenticación de EXEC. Utilice la base de datos local.

D1	config t aaa authentication login default group radius local end	Método de autenticación de EXEC. Utilice la base de datos local.
D2	config t aaa authentication login default group radius local end	Método de autenticación de EXEC. Utilice la base de datos local.
A1	config t aaa authentication login default group radius local end	Método de autenticación de EXEC. Utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos.	Cierre e inicie sesión en todos los dispositivos.

R1	Figura 15. Verifique el servicio AAA en R1. 
R3	Figura 16. Verifique el servicio AAA en R3. 

D1	Figura 17. Verifique el servicio AAA en D1. 
D2	Figura 18. Verifique el servicio AAA en D2. 

A1	Figura 19. Verifique el servicio AAA. 
R2	Aquí solo verifico el usuario y contraseña ya que lo demás no se aplicó. Figura 20. Verificación en R2. 

Parte 6.

Configure las funciones de Administración de Red.

En esta parte, debe configurar varias funciones de administración de red.

Tabla 14.Tareas 6.1 y 6.2.

Tarea.	Tarea.	Especificación.
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
R1	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.
R2	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.

R3	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.
D1	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.
D2	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.
A1	show clock clock set 26:00:00 1 Dec 2021	Muestra la configuración del reloj y establece la configuración del reloj del software.
6.2	Configure R2 como un NTPmaestro.	Configurar R2 como NTP maestro en el nivel deestrato 3.
R2	ntp master 3	NTP maestro en el nivel de estrato 3.

Tabla 15. Tareas 6.3, 6.4 y 6.5.

Tarea.	Tarea.	Especificación.
6.3	Configure NTP en R1, R3, D1, D2,y A1.	Configure NTP de la siguiente manera: R1 debe sincronizar con R2, por otra parte, R3, D1 y A1 con R1 y finalmente D2 con R3.
R1	ntp server 2.2.2.2	R1 debe sincronizar con R2.
R3	ntp server 10.0.10.1	R3 para sincronizar la hora con R1.
D1	ntp server 10.0.10.1	D1 para sincronizar la hora con R1.
D2	ntp server 10.0.10.1	D2 para sincronizar la hora con R3.
A1	ntp server 10.0.10.1	A1 para sincronizar la hora con R1.

6.4	Configure SYSLOG en todos los dispositivos excepto R2.	SYSLOGS deben enviarse a la PC1 en 10.0.100.5 enel nivel WARNING.
R1	logging trap warning logging host 10.0.100.5 logging on	Envía todos los mensajes con advertencia enel nivel WARNING. SYSLOGS deben enviarse a la PC1 en 10.0.100.5. Al iniciar sección puede enviar mensajes de SYSLOG.
R3	logging trap warning logging host 10.0.100.5 logging on	Envía todos los mensajes con advertencia enel nivel WARNING. SYSLOGS deben enviarse a la PC1 en 10.0.100.5. Al iniciar sección puede enviar mensajes de SYSLOG.

D1	logging trap warning logging host 10.0.100.5 logging on	Envía todos los mensajes con advertencia enel nivel WARNING. SYSLOGS deben enviarse a la PC1 en 10.0.100.5. Al iniciar sección puede enviar mensajes de SYSLOG.
D2	logging trap warning logging host 10.0.100.5 logging on	Envía todos los mensajes con advertencia enel nivel WARNING. SYSLOGS deben enviarse a la PC1 en 10.0.100.5. Al iniciar sección puede enviar mensajes de SYSLOG.

A1	logging trap warning logging host 10.0.100.5 logging on	Envía todos los mensajes con advertencia enel nivel WARNING. SYSLOGS deben enviarse a la PC1 en 10.0.100.5. Al iniciar sección puede enviar mensajes de SYSLOG.
6.5	Configure SNMPv2c en todos losdispositivos excepto R2.	Especificaciones de SNMPv2: únicamente se usará SNMP en modo lectura, limite el acceso SNMP a la dirección IP de laPC1, configure el valor de contacto SNMP con sunombre, establezca *COMMUNITY STRING* en **ENCORSA.**

R1	ip access-list standard SNMP-NMS permit host 10.0.100.5 exit snmp-server contact Cisco RosaG snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 versión 2c ENCORSA snmp-server ifindex persist snmp-server enable traps bgp snmp-server enable traps config snmp-server enable traps ospf end	Creé una ACL para permitir el tráfico SNMP. Definí el destino. Escribí mi nombre como contacto. Habilite la cadena de comunidad de sólo lectura. Configure SNMPV2C. Habilite globalmente la persistencia de IFINDEX de SNMP. Habilite el envío de *TRAPS BGP.* Habilite el envío de *TRAPS CONFIG.* Habilite el envío de *TRAPS OSPF*.

R3	ip access-list standard SNMP-NMS	Creé una ACL para permitir el tráfico SNMP.
	permit host 10.0.100.5	
	exit	Definí el destino.
	snmp-server contact RosaG	Escribí mi nombre como contacto.
	snmp-server community ENCORSA ro SNMP-NMS	Habilite la cadena de comunidad de sólo lectura.
	snmp-server host 10.0.100.5 version 2c ENCORSA	
	snmp-server ifindex persist	Configure SNMPV2C.
	snmp-server enable traps config	
	snmp-server enable traps ospf	Habilite globalmente la persistencia de IFINDEX de SNMP.
		Habilite el envío de *TRAPS CONFIG.*
		Habilite el envío de *TRAPS OSPF.*

D1	ip access-list standard SNMP-NMS permit host 10.0.100.5 exit snmp-server contact Cisco RosaG snmp-server host 10.0.100.5 version 2c ENCORSA snmp-server ifindex persist snmp-server enable traps config snmp-server enable traps ospf	Creé una ACL para permitir el tráfico SNMP. Definí el destino. Escribí mi nombre como contacto. Habilite la cadena de comunidad de sólo lectura. Configure SNMPV2C. Para habilitar globalmente la persistencia de IFINDEX de SNMP. Habilite el envío de *TRAPS CONFIG.* Habilite el envío de *TRAPS OSPF.*

D2	ip access-list standard SNMP-NMS	Creé una ACL para permitir el tráfico SNMP.
	permit host 10.0.100.5	Definí el destino.
	exit	
	snmp-server contact RosaG	Escribí mi nombre como contacto.
	snmp-server community ENCORSA ro SNMP-NMS	Habilite la cadena de comunidad de sólo lectura.
	snmp-server host 10.0.100.5 version 2c ENCORSA	
	snmp-server enable traps config	Configure SNMPv2c.
	snmp-server enable traps ospf	
		Para habilitar globalmente la persistencia de IFINDEX de SNMP.
		Habilite el envío de *TRAPS CONFIG.*
		Habilite el envío de *TRAPS OSPF.*

A1		Creé una ACL para permitir el tráfico SNMP.
	ip access-list standard SNMP-NMS permit host 10.0.100.5 exit	Definí el destino.
	snmp-server contact RosaG	Escribí mi nombre como contacto.
	snmp-server community ENCORSA ro SNMP-NMS	Habilite la cadena de comunidad de sólo lectura.
	snmp-server host 10.0.100.5 version 2c ENCORSA	Configure SNMPV2C.
	snmp-server ifindex persist	Habilite globalmente la persistencia de IFINDEX de SNMP.
	snmp-server enable traps config	Habilite el envío de *TRAPS CONFIG.*
	snmp-server enable traps ospf	Habilite el envío de *TRAPS OSPF.*

CONCLUSIONES

Entendí que para realizar un escenario como el propuesto en este documento se requieren unas características de hardware muy buenas en el computador tanto en procesador como de RAM en caso contrario no va funcionar y por supuesto no se lograría completar este tipo de informes.

Adquirí más información de GNS3 como el hecho de que se deba virtualizar para poder configurar cada dispositivo es algo que requiere más tiempo porque en GNS3 toca agregarle todo dispositivo de comunicación como lo es; un switch de capa 3 o un router para que este nos acepte los comandos necesarios.

Practique diferentes comandos tanto de configuración como de verificación en todos los componentes de esta red como en el router, en el switch y en los computadores.

Identifique que, si bien GNS3 requiere más tiempo inicialmente, después ofrece más alternativas que Cisco Packet Tracer, porque en GNS3 se puede cargar hasta un sistema operativo como Windows, Linux entre otros S.O. en un computador logrando así tener más opciones de configuración.

BIBLIOGRÁFIA

PARRA H. (2021). Web CCNP unidades 8, 9 y 10. Recuperado de https://drive.google.com/file/d/1aHYc08lI27zbypmCBn-r1v_q1WsKE1xs/view

STUDY-CCNA.COM. (2021). Configure el enrutador Cisco como servidor DHCP. Recuperado de https://study-ccna.com/configure-cisco-router-as-dhcp-server/

STUDY-CCNA.COM. (2021). Descripción general de OSPF. Recuperado de https://study-ccna.com/ospf-overview/

STUDY-CCNA.COM. (2021). ¿Qué es la dirección IPv4 y cuál es su función en la red? Recuperado de https://study-ccna.com/what-is-ipv4-address/

STUDY-CCNA.COM. (2021). ¿Qué es la dirección IPv4 y cuál es su función en la red? Tipos de direcciones IPv4. Dirección IP pública. Recuperado de https://study-ccna.com/what-is-ipv4-address/

STUDY-CCNA.COM. (2021). ¿Qué es la dirección IPv4 y cuál es su función en la red? Tipos de direcciones IPv4. Dirección IP privada. pública. Recuperado de https://study-ccna.com/what-is-ipv4-address/