

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ESTUDIANTE:
FRAY DAVID DELGADO BEDOYA
71367577

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ESTUDIANTE:
FRAY DAVID DELGADO BEDOYA
71367577

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del jurado

Firma del jurado

BOGOTA, 28 de noviembre de 2021

Contenido

LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN	8
INTRODUCCION	9
DESARROLLO	10
ESCENARIO PROPUESTO	10
CONCLUSIONES	33
BILIOGRAFÍA	53

LISTA DE TABLAS

Tabla 1. Direccionamiento de topología de red propuesta.....	10
Tabla 2. Configuración de interfaces troncales en los Switch	24
Tabla 3. Configuración de VLAN 999 como nativa en los switch	24
Tabla 4. Habilitación del protocolo RSTP en todos los Switch	24

LISTA DE FIGURAS

Figure 1. Topología de la red propuesta	10
Figure 2. Topología de la red propuesta en Packet Tracer	12
Figure 3. Configuración básica Router 1	14
Figure 4. Configuración básica Router 2	15
Figure 5. Configuración básica Router 3	16
Figure 6. Actualización firmware de switch A1	20
Figure 7. Direccionamiento IPv4 e IPv6 en PC1 y PC4	24
Figura 8. Habilitación de protocolo RSTP en Switch A1	25
Figura 9. Verificación DHCP en PC2... ..	27
Figura 10. Ping desde PC1 hacia D1, D2 y PC4... ..	27
Figura 11. Ping desde PC4 hacia D1, D2, y PC1... ..	28
Figura 12. Ping desde PC3 hacia D1 y D3.....	28
Figura 13. Ping desde PC2 hacia D1 y D2.....	29

GLOSARIO

PROTOCOLO DE CONFIGURACIÓN DE HOST DINÁMICO (DHCP): Es un protocolo administrador de red usado en Protocolo de Internet (IP) para asignar automáticamente las direcciones IP y otros parámetros de comunicación.

HSRP VERSIÓN 2: Es un protocolo de redundancia patentado por cisco, para establecer una puerta de enlace a prueba de fallos.

IP ACUERDO DE NIVEL DE SERVICIO: Por sus siglas SLA, es un método activo de monitoreo y reportar confiablemente el rendimiento en una Red.

CAPA 2 DE RED: Proporciona tránsito de datos confiables a través de un enlace físico, conocida como capa de enlace de datos.

ROUTER: Es un dispositivo de red que envía paquetes de datos entre computadores dentro de una red

SWITCH CAPA 3: Es un dispositivo que funciona como switch y router a la vez, y conmuta paquetes con la supervisión de sus direcciones IP y sus direcciones MAC.

CCNP: Se refiere a la certificación de Cisco para profesionales de TI con al menos un año de experiencia en redes profesionales.

RESUMEN

En el presente informe se aborda el estudio y el desarrollo de la prueba de habilidades practicas CCNP del diplomado de profundización cisco. En el informe se realiza la implementación de la red propuesta, se configura los parámetros básicos de los dispositivos y el soporte de Host, se configura los protocolos de enrutamiento y la redundancia de primer salto, finalmente se configura la seguridad y las características de administración de la red para dar solución al escenario propuesto documentando, explicando en detalle con su respectiva línea de comandos o códigos utilizados para la configuración.

Palabras clave.

CISCO, CCNP, VLAN, Protocolo, redes, EIGRP, Switches, Routers.

ABSTRACT

This report addresses the study and development of the CCNP practical skills test for the Cisco in-depth diploma. The report performs the implementation of the proposed network, configures the basic parameters of the devices and Host support, configures the routing protocols and first-hop redundancy, finally configures the security and management characteristics of the network to solve the proposed scenario by documenting, explaining in detail with their respective command line or codes used for configuration.

Keywords

CISCO, CCNP, VLAN, Protocol, networks, EIGRP, Switches, Routers.

INTRODUCCION

Las empresas cuentan con una estructura organizada para todo el tráfico de datos para diferentes topologías, con la finalidad de que de la comunicación entre diferentes elementos dentro de una red, que manejan una información a través de los dispositivos, viaje de manera favorable hacia el destino final.

En el presente trabajo se aborda el diseño e implementación de un escenario donde se realiza la configuración de una topología de red planteada, así como su caracterización y configuración desde la capa 2. Además de construir la red, se realiza la configuración básica de cada dispositivo y el direccionamiento de las interfaces, se realiza la configuración capa 2 de la red y protocolos de enrutamiento, también se realiza la configuración de redundancia de primer salto y configuración de la seguridad de la red.

DESARROLLO

ESCENARIO PROPUESTO

A continuación se muestra en la figura 1, la topología de la red propuesta para su estudio, configuración e implementación.

Figure 1. Topología de la red propuesta

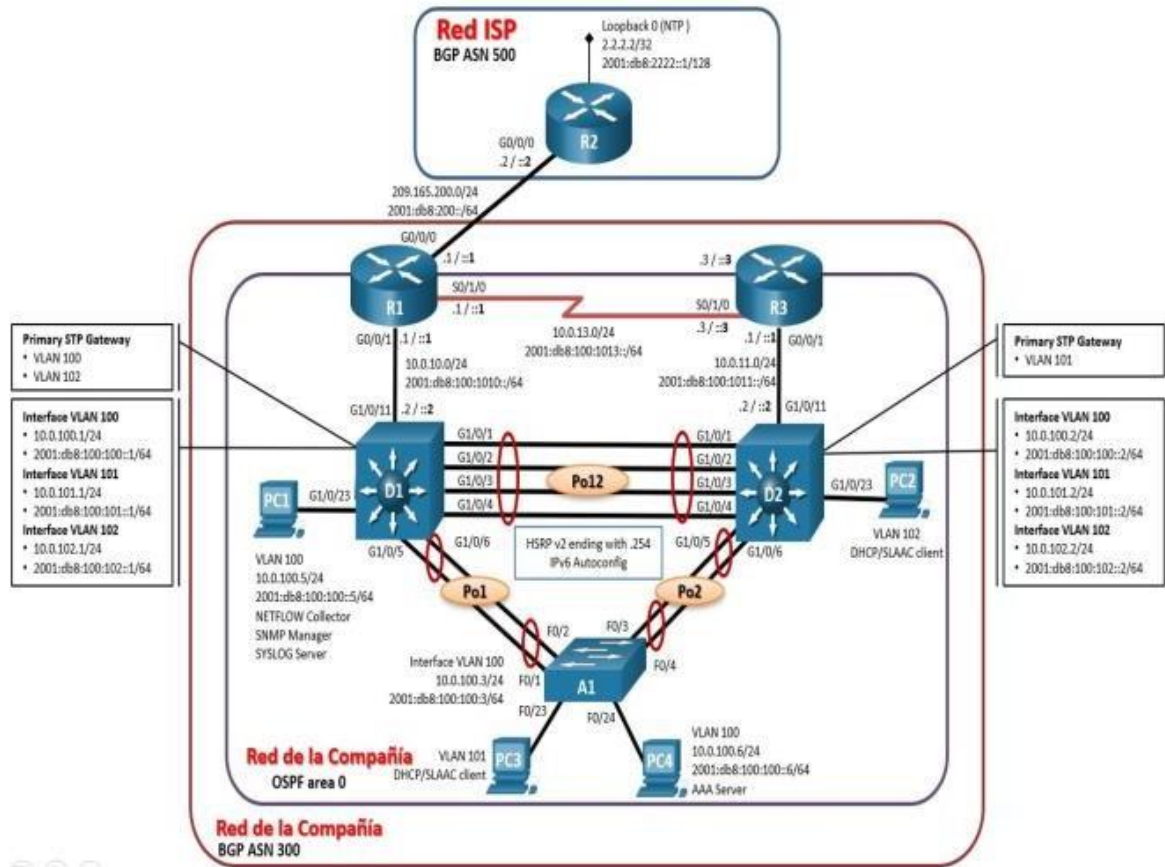


Tabla 1. Direccionamiento de topología de red propuesta

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
	Loopback 0	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

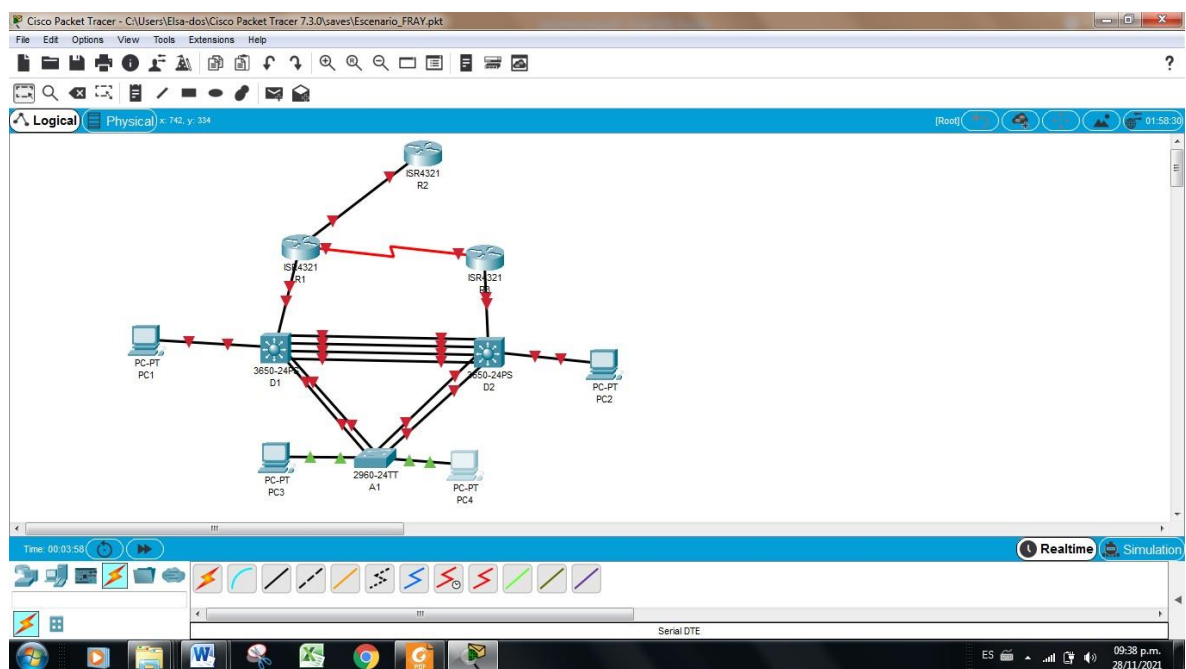
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2: 3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2: 4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1: 1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

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 sea necesario.

Figure 2. Topología de la red propuesta en Packet Tracer



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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:

```
Router>en //Ingresa al modo privilegiado
Router#conf t //ingresa al modo configuración
Router(config)#hostname R1 //Asigna nombre a Router
R1(config)#ipv6 unicast-routing //enrutamiento ipv6
R1(config)#no ip domain lookup //retarda los comandos mal tipeados
R1(config)#banner mot #R1, ENCOR Skills Assessment, Scenario 1 #
//Descripcion R1
R1(config)#line con 0 //Configuracion de linea
R1(config-line)#exec-timeout 0 0 //Tiempo ilimitado
R1(config-line)#logging synchronous //Depuracion de mensajes
R1(config-line)#exit //Sale de modo de configuracion
R1(config)#int g0/0/0 //Ingresa a interfaz giga 0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224 //Asigna direccion IP
R1(config-if)#ipv6 address fe80::1:1 link-local //Asigma IP version 6
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shut down //Activa interfaz

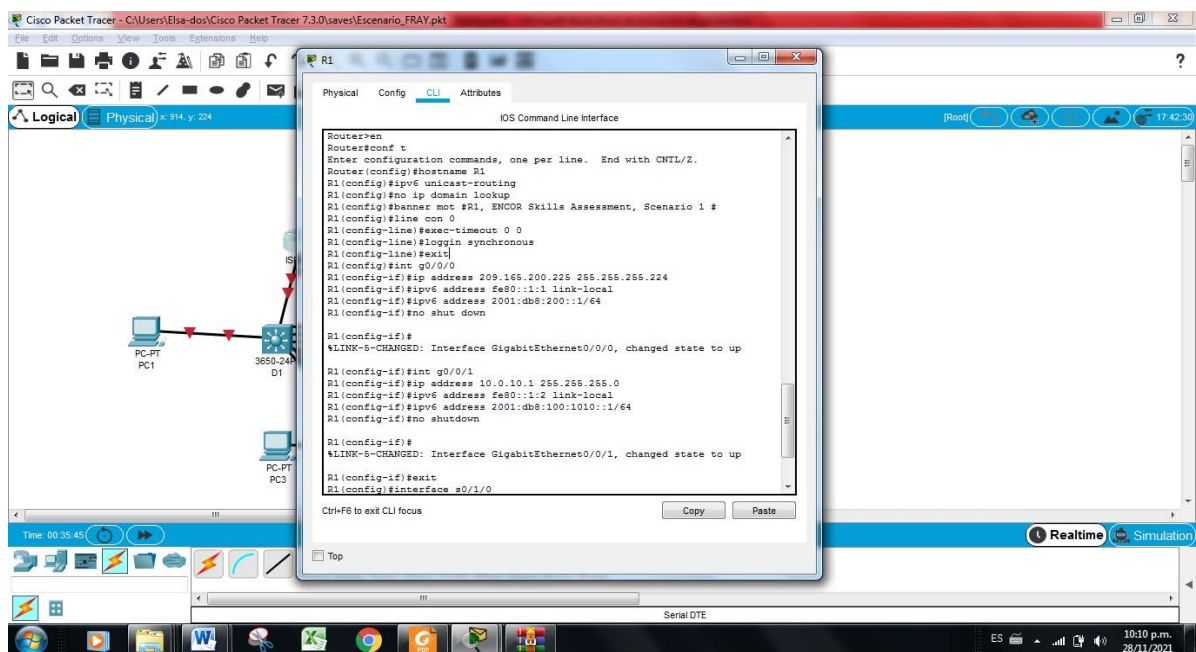
R1(config-if)#int g0/0/1 //ingresa a interfaz g0/0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0 //configure direccion ip
R1(config-if)#ipv6 address fe80::1:2 link-local //configure link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64 //asigna direccion IPv6
R1(config-if)#no shutdown //activa la interfaz
R1(config-if)#exit //sale modo configuracion
R1(config)#interface s0/1/0 //ingresa a interfaz s0/1/0
```

```

R1(config-if)#ip address 10.0.13.1 255.255.255.0 //configure direccion IPv4
R1(config-if)#ipv6 address fe80::1:3 link-local //configura link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64 //configura direccion IPv6
R1(config-if)#no shutdown //activa la interfaz
R1(config-if)#exit //sale modo configuracion

```

Figure 3. Configuración básica Router 1



Ahora realizamos la configuración básica para R2

```

Router>en //Ingresa al modo privilegiado
Router#conf t //ingresa al modo configuración
Router(config)#hostname R2 //Asigna nombre a Router
R2(config)#ipv6 unicast-routing //Permite enrutamiento ipv6
R2(config)#no ip domain lookup //retarda los comandos mal tipeados
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 # //Mensaje R2
R2(config)#line con 0 //Configuracion de linea
R2(config-line)#exec-timeout 0 0 //tiempo ilimitado
R2(config-line)#logging synchronous //Depuración de mensajes
R2(config-line)#exit //sale modo configuracion

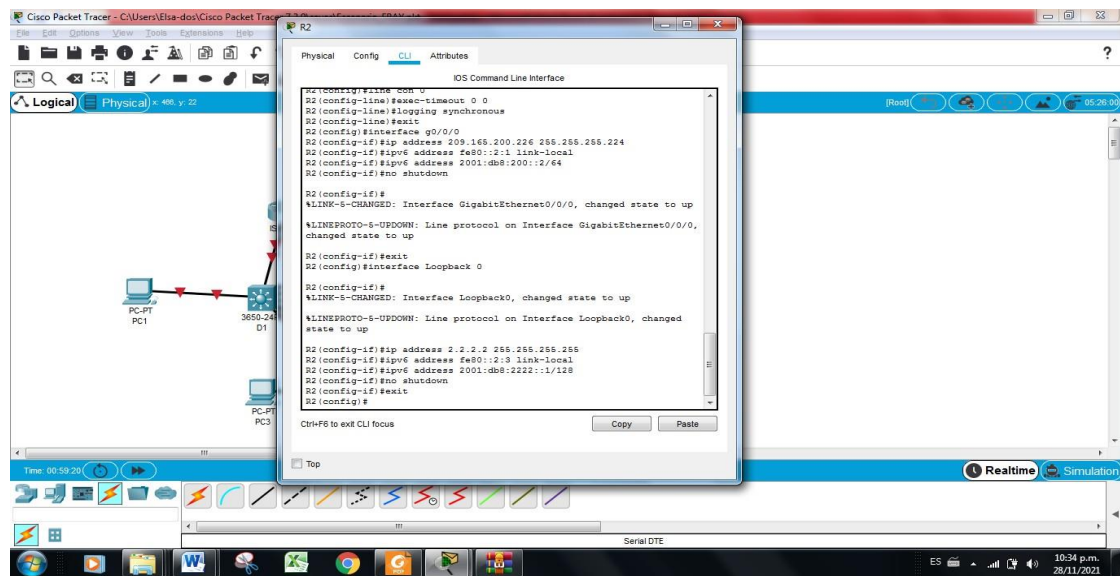
```

```

R2(config)#interface g0/0/0 //ingresa a interfaz g0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224 //Asigna direccion ipv4
R2(config-if)#ipv6 address fe80::2:1 link-local //configura link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64//Configura IPv6
R2(config-if)#no shutdown //Activa Interfaz
R2(config-if)#exit //Sale modo configuracion
R2(config)#interface Loopback 0 //ingresa interfaz loopback
R2(config-if)#ip address 2.2.2.2 255.255.255.255 //Asigna direccion IP
R2(config-if)#ipv6 address fe80::2:3 link-local //configure direccion IPv6
R2(config-if)#ipv6 address 2001:db8:2222::1/128 //configura direccion IPv6
R2(config-if)#no shutdown //Activa interfaz
R2(config-if)#exit //Sale de modo de configuración

```

Figure 4. Configuración básica Router 2



Continuamos la configuración básica con R3

```

Router>en //Ingresa al modo privilegiado
Router#conf t //ingresa al modo configuración
Router(config)#hostname R3 //Asigna nombre a Router
R3(config)#ipv6 unicast-routing //Permite enrutamiento ipv6
R3(config)#no ip domain lookup //retarda los comandos mal tipeados

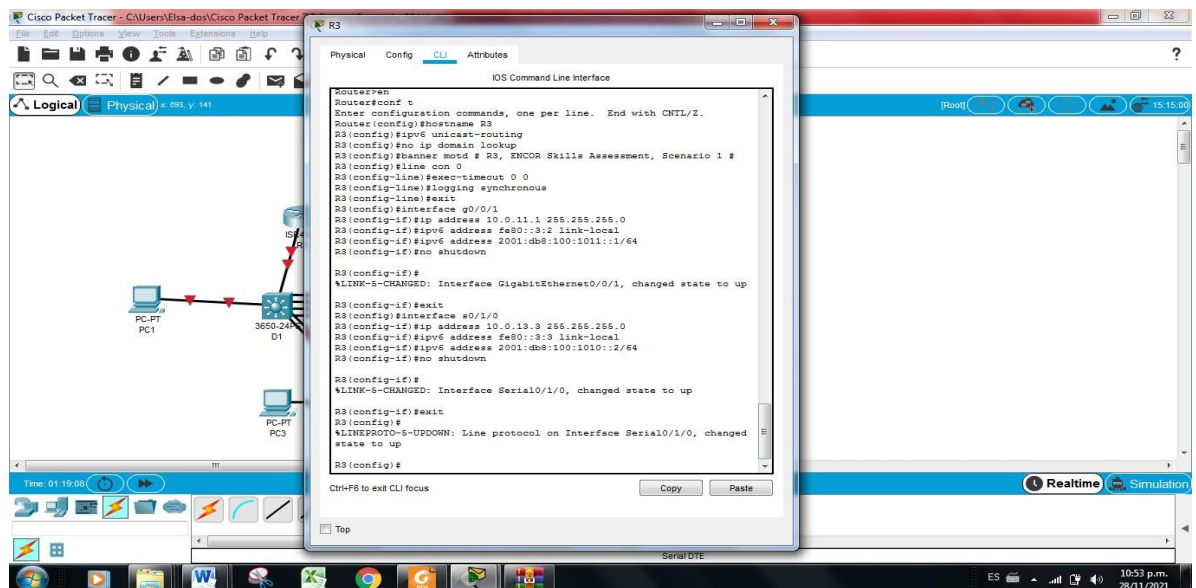
```

```

R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 # //Mensaje
R3
R3(config)#line con 0 //Configuracion de linea
R3(config-line)#exec-timeout 0 0 //tiempo ilimitado
R3(config-line)#logging synchronous //Depuración de mensajes
R3(config-line)#exit //sale modo configuracion
R3(config)#interface g0/0/1 //ingresa a interfaz g0/0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0 //Asigna direccion ipv4
R3(config-if)#ipv6 address fe80::3:2 link-local //configura link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64 //Configura IPv6
R3(config-if)#no shutdown //Activa Interfaz
R3(config-if)#exit //Sale modo configuracion
R3(config)#interface s0/1/0 //ingresa Serial 0/1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0 //Asigna direccion ipv4
R3(config-if)#ipv6 address fe80::3:3 link-local //configura link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64 //Configura IPv6
R3(config-if)#no shutdown //Activa Interfaz
R3(config-if)#exit //Sale modo configuracion

```

Figure 5. Configuración básica Router 3



Configuracion D1

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

```
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 //Crea VLAN 100
D1(config-vlan)#name Management //asigna nombre a la vlan
D1(config-vlan)#exit
D1(config)#vlan 101 //crea vlan 101
D1(config-vlan)#name UserGroupA //nombra vlan 101
D1(config-vlan)#exit
D1(config)#vlan 102 //Cra vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999 //crea vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface g1/0/11
D1(config-if)#no switchport //usa interfaces en
capa 3
D1(config-if)#ip address 10.0.10.2 255.255.255.0 //asigna direccion IP
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-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-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 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)#
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 //crea un conjunto de ip's
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 g1/0/1-10, g1/0/12-24, g1/1/1-4
D1(config)#shutdown

```

Configuracion D1

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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 g1/0/11
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
```

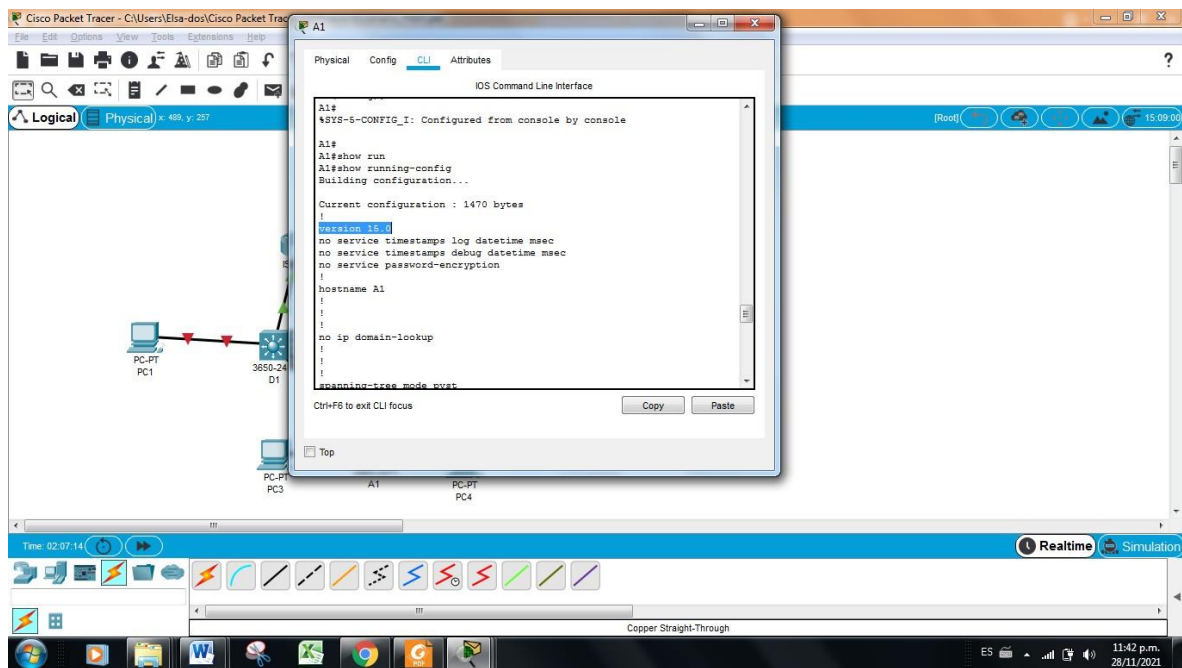
```

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(dhcp-config)#exit
D2(config)#interface range g1/0/1-10
D2(config-if-range)#shutdown
D2(config-if-range)#
D2(config-if-range)#interface range g1/0/12-24
D2(config-if-range)#shutdown
D2(config-if-range)#interface range g1/1/1-4
D2(config-if-range)#shutdown

```

Dado que el switch A1 no reconocía algunos comandos como **ipv6 address** se hizo necesaria una actualización del IOS a la versión 15.0 como se muestra en la figura 6. El procedimiento fue copiar desde el servidor al switch A1 el firmware *c2960-lanbasek9-mz.150-2.SE4.bin*

Figure 6. Actualización firmware de switch A1



Configuracion A1

A1>en

A1#conf t

A1(config)#sdm prefer dual-ipv4-and-ipv6 default //Permite direccionamiento IPv6 e IPv4

A1(config)#exit

A1#reload

A1(config)# hostname A1

A1(config)# no ip domain lookup

A1(config)# banner motd # A1, ENCOR Skills Assessment, Scenario 1 #

A1(config)# line con 0

A1(config)# exec-timeout 0 0

A1(config)# logging synchronous

A1(config)#exit

A1(config)#vlan 100 //Se crea VLAN 100

A1(config-vlan)# name Management //Asigna nombre a vlan 101

A1(config-vlan)# exit

A1(config)#vlan 101 //Se crea VLAN 101

A1(config-vlan)# name UserGroupA //Asigna nombre a vlan 101

```
A1(config-vlan)# exit
A1(config)#vlan 102 //se crea vlan 102
A1(config-vlan)# name UserGroupB //Asigna nombre a vlan 102
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 sh
A1(config-if)#no shutdown
A1(config-if)#exit
```

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

```
R1>en
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2>en
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

```
D1>en
```

```
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

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

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

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

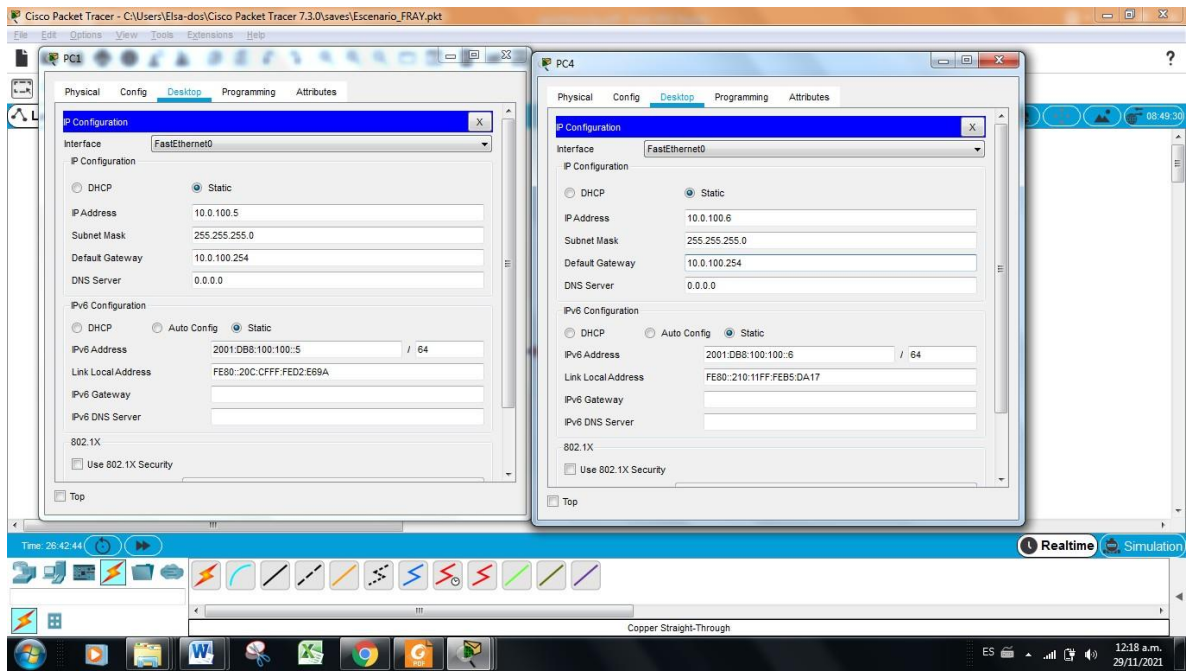


Figure 7. Direccionamiento IPv4 e IPv6 en PC1 y PC4

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 switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el

		diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

A continuación se detalla la explicación para cada tarea planteada en la parte 2

Tabla 2. Configuración de interfaces troncales en los switch

Comentarios	Solución	Descripción Tarea 2.1
Ingresar rango de interfaz g/1/0/1-4 Encapsulación de protocolo 802.1Q Se define modo Trunk	D1(config-if)#int range g1/0/1-4 D1(config-if-range)#switchport trunk encapsulation dot1q D1(config-if-range)#switchport mode trunk	Habilitación de enlace trunk 802.1Q entre D1 y D2
Ingresar rango de interfaz g/1/0/5-6	D1(config-if-range)#int range g1/0/5-6	Habilitación de

Encapsulación protocolo 802.1Q Se define modo Trunk	D1(config-if-range)#switchport trunk encapsulation dot1q D1(config-if-range)#switchport mode trunk	enlace trunk 802.1Q entre D1 y A1
Ingresa rango interfaz g/1/0/5-6 Encapsulación protocolo 802.1Q Se define modo Trunk	D2(config)#int range g1/0/5-6 D2(config-if-range)#switchport trunk encapsulation dot1q D2(config-if-range)#switchport mode trunk D2(config-if-range)#	Habilitación de enlace trunk 802.1Q entre D2 y A1

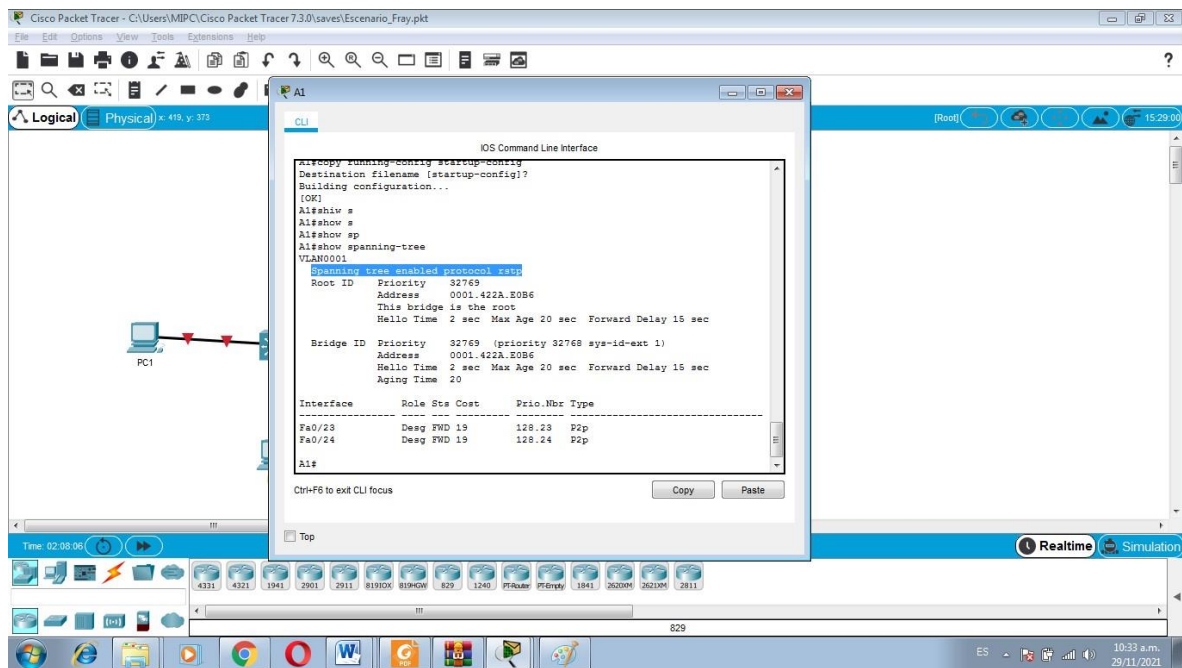
Tabla 3. Configuración de vlan 999 como nativa en los switch

Comentarios	Solución Tarea 2.2
Ingresa rango interfaz g/1/0/1-6 Define vlan 999 como interfaz nativa	D1(config-if)#int range g1/0/1-6 D1(config-if-range)# switchport trunk native vlan 999
Ingresa rango interfaz g/1/0/1-6 Define vlan 999 como interfaz nativa	D2(config-if-range)# int range g1/0/1-6 D2(config-if-range)# switchport trunk native vlan 999
Ingresa rango interfaz fa0/1-4 Define vlan 999 como interfaz nativa	A1(config)#int range fa0/1-4 A1(config-if-range)# switchport trunk native vlan 999

Tabla 4. Habilitación del protocolo RSTP en todos los switch

Comentarios	Solución Tarea 2.3
Habilitación de protocolo RSTP	D1(config)#spanning-tree mode rapid-pvs
Habilitación de protocolo RSTP	D2(config)#spanning-tree mode rapid-pvs
Habilitación de protocolo RSTP	A1(config)#spanning-tree mode rapid-pvs

Figura 8. Habilitación de protocolo RSTP en switch A1



Tarea 2.4

Configuración de los puentes raíz RSTP en D1 y D2

D1(config)#spanning-tree vlan 100,102 root primary //Prioridad primaria Vlan 100-102

D1(config)#spanning-tree vlan 101 root secondary //Prioridad Secundaria Vlan 101

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

D2(config)#spanning-tree vlan 101 root primary

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

Tarea 2.5

Creación de EtherChannels LACP en todos los switch

Entre D1 y D2 Port Channel 12

D1(config)#interface range g1/0/1-4 //ingresa a rango interfaz

D1(config-if-range)#channel-protocol lacp //Se selecciona protocolo LACP

D1(config-if-range)#channel-group 12 mode active //Asigna nombre de grupo

D1(config-if-range)#no shutdown //Activa interfaz

```
D2(config)#interface range g1/0/1-4 //Ingresa a rango interfaz
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown //Activa interfaz
```

Entre D2 y A1 Port Channel 2

```
D2(config)#interface range g1/0/1-6
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
```

```
A1(config)#interface range f0/3-4
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active
```

Entre D1 y A1 Port Channel 1

```
D1(config)#interface range g1/0/5-6
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
```

```
A1(config)#interface range f0/1-2
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode active
```

Tarea 2.6

Configuración de los puertos de accesos a las vlan adecuada

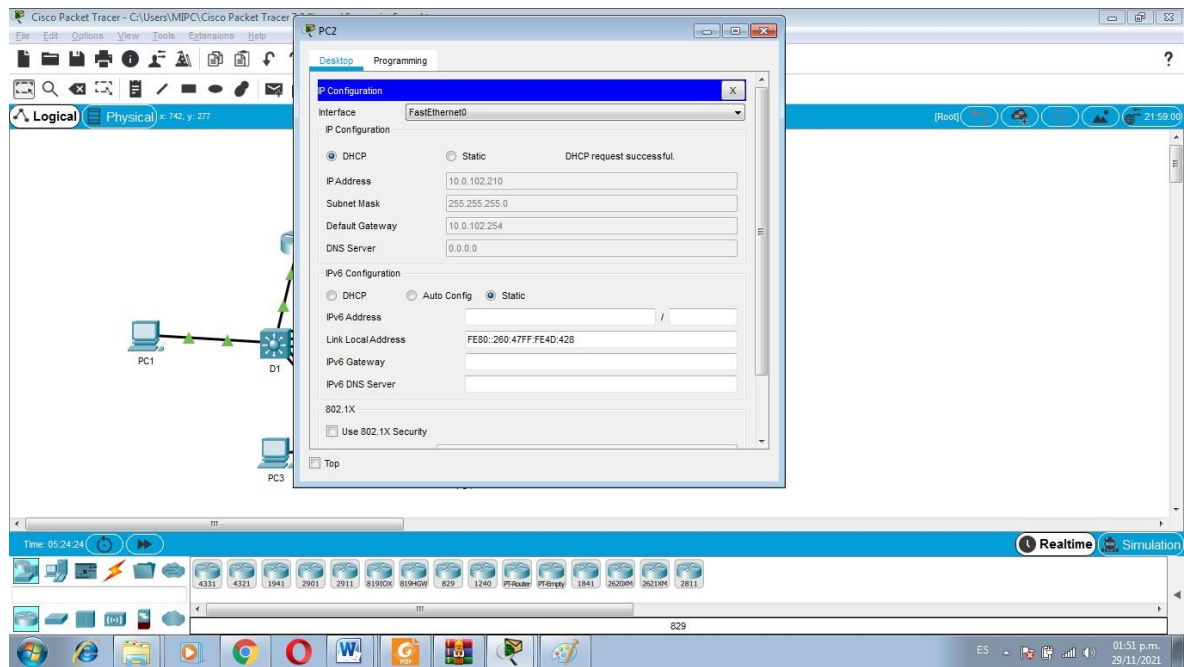
```
D1(config)#int g1/0/23
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
```

```
A1(config)#interface f0/23
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#exit
A1(config)#interface f0/24
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
```

```
D2(config)#int g1/0/23
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
```

Tarea 2.7 Verificación del Servicio DHCP

Figura 9. Verificación DHCP en PC2



Tarea 2.8. Verifica la conectividad de la LAN local

Figura 10. Ping desde PC1 a D1, D2 y PC4

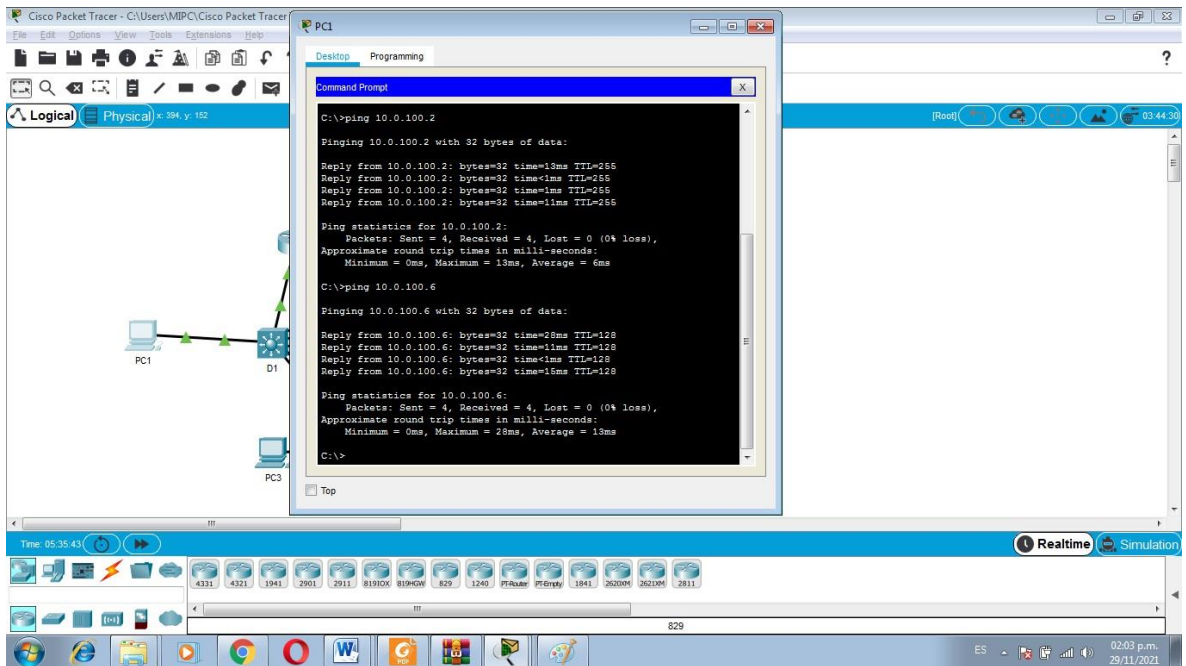


Figura 11. Ping desde PC4 hasta D1,D2 y PC1

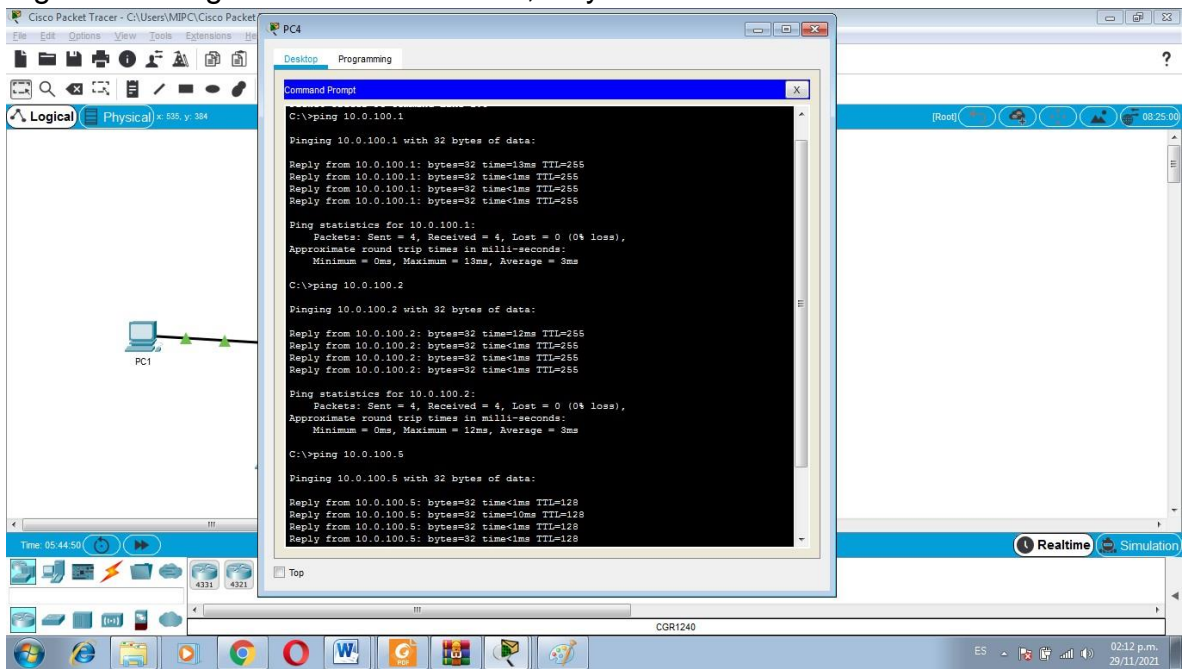


Figura 12. Ping desde PC3 hasta D1 y D2

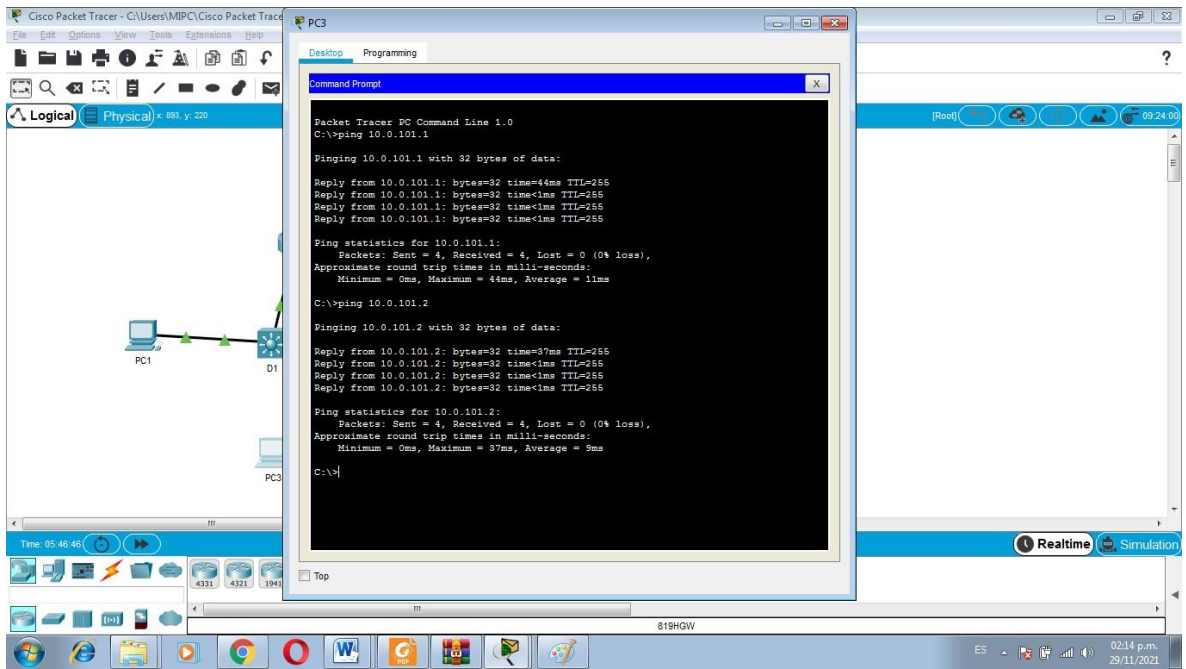
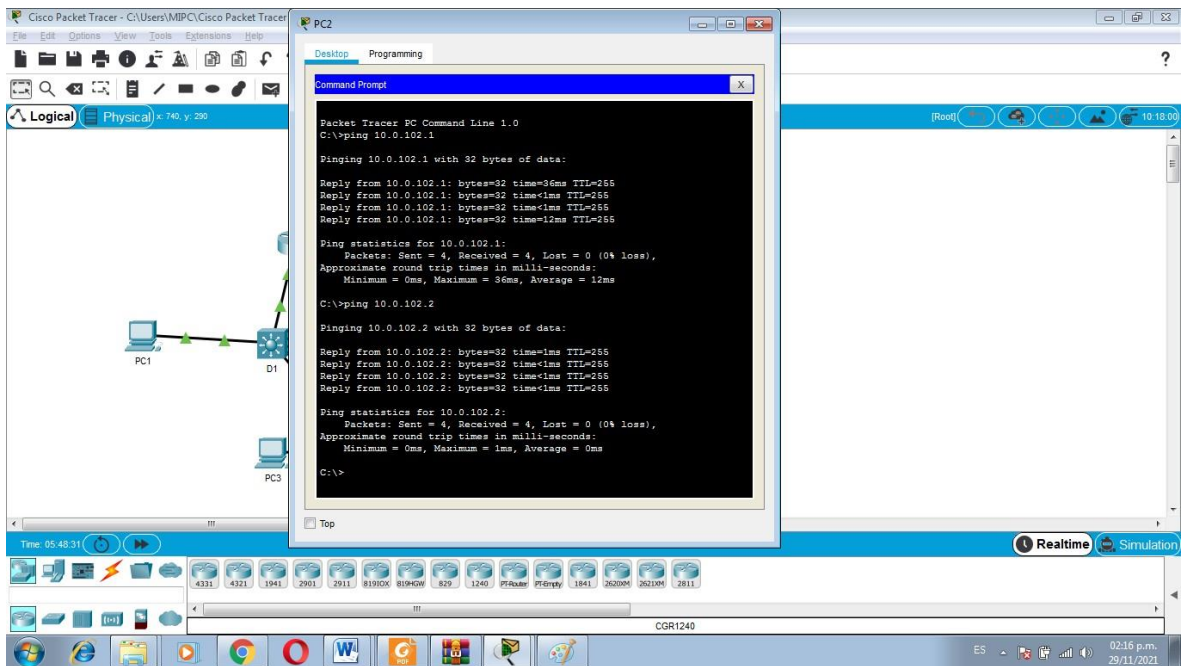


Figura 13. Ping desde PC2 hasta D1 y D2



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

Las tareas de configuración son las siguientes:

Tarea #	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single área OSPFv2 en área 0.	Use OSPF Process ID 4 y asigne los siguientes router IDs: <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID 6 y asigne los siguientes router IDs: <ul style="list-style-type: none"> • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la “Red ISP”, configure MP	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

	BGP.	<ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MP BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48

Tarea 3.1 configure classic single-area OSPFv3 en area 0.

```
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
```

```
R3(config)#router ospf 4 //Habilita enrutamiento OSPF
R3(config-router)#router-id 0.0.4.3 //Asigna un ID
```

```
R3(config-router)#do show ip route connected //Muestra las redes conectadas
C 10.0.11.0/24 is directly connected, GigabitEthernet0/0/1
C 10.0.13.0/24 is directly connected, Serial0/1/0
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#
```

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
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
D1(config-router)#passive-interface default
```

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
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
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/0/11
```

Tarea 3.2 Configuración de OSPv3 en área 0

```
R1(config)#ipv6 router ospf 6 //Habilita OSPF en IPV6
R1(config-rtr)#router-id 0.0.6.1 //Se asigna una identificación
R1(config-rtr)#default-information originate //Información predeterminada
R1(config-rtr)#exit //Sale modo OSPF
R1(config)#int g0/0/1 //Ingresa a interfaz g0/0/1
R1(config-if)#ipv6 ospf 6 area 0 //Se asigna Area 0 en IPv6
R1(config-if)#exit
R1(config)#int s0/1/0 //Ingresa a interfaz Serial0/1/0
R1(config-if)#ipv6 ospf 6 area 0 //Se asigna Area 0 en IPv6
```

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface g0/0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#int s0/1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
```

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface gigabitEthernet 1/0/11
D1(config-rtr)#exit
D1(config)# interface g1/0/11
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#
```

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface g1/0/11
D2(config-rtr)#exit
D2(config)#int range g1/0/11
D2(config-if-range)#ipv6 ospf 6 area 0
D2(config-if-range)#exit
D2(config)#int g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#
```

Tarea 3.3

```
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 // interfaz a conf. Loopback 0
R2(config-if)# ipv6 route ::/0 loopback 0 //parámetros a configurar con ip y
mascara de red
```

Configuración de BGP

```
R2(config-router)#router bgp 500 //router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2 //se asigna el id 2.2.2.2
Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.
R2(config-router)#neighbor 209.165.200.225 remote-as 300
//define la relación vecino ipv4
R2(config-router)#neighbor 2001:db8:200::1/64 remote-as 300
//define la relación vecino ipv6
```

En IPv4 address family, anuncie:

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0). 82

```
R2(config-router)#address-family ipv4 //configurar la familia
ipv4
R2(config-router)# neighbor 209.165.200.225 activate //red loopback
R2(config-router)# no neighbor 2001:db8:200::1 activate //red loopback
R2(config-router)# network 2.2.2.2 mask 255.255.255.255 //red y mascara
R2(config-router)#neighbor 0.0.0.0/0 // ruta por defecto
R2(config-router)# exit-address-family //Sale configuración familia
```

En IPv6 address family, anuncie:

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

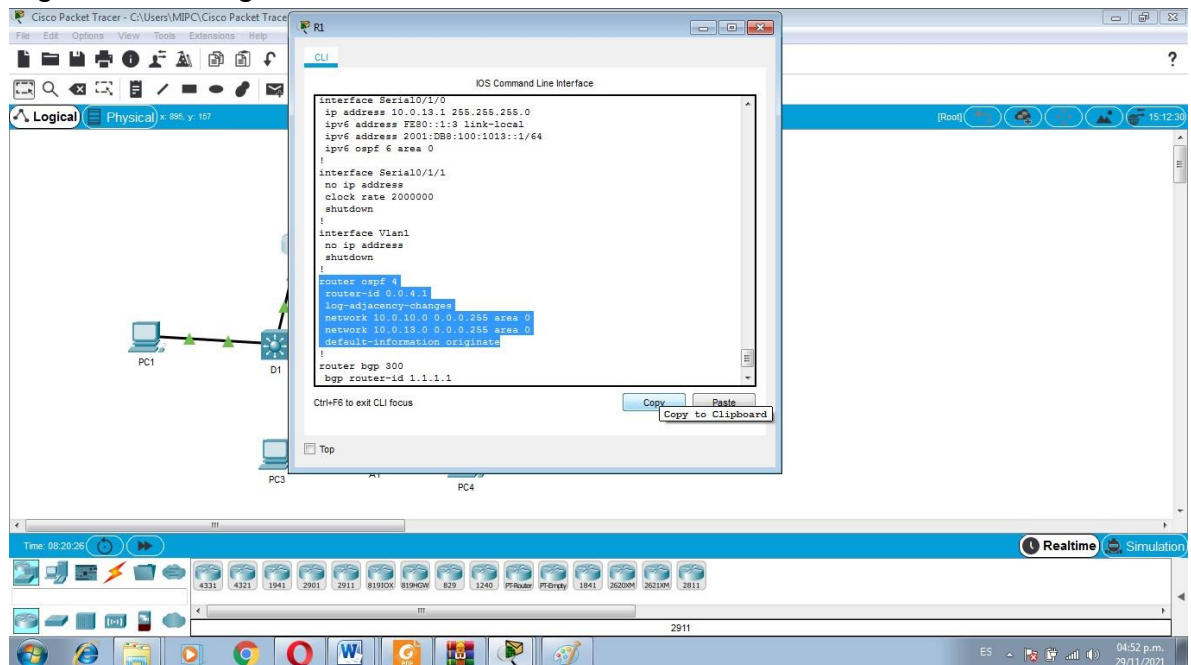
```
R2(config-router)#address-family ipv6
R2(config-router)# no neighbor 209.165.200.225 activate
R2(config-router)# neighbor 2001:db8:200::1 activate
R2(config-router)# network 2001:db8:2222::/128
R2(config-router)# network ::/0
R2(config-router)# exit-address-family
```

Tarea 3.4

```
R1#conf term //configuración de terminal
R1(config)#ip route 10.0.0.0 255.255.255.255 null0 //configura interfaz null ipv4
R1(config)#ip route 2001:db8:100::/48 null0 // interfaz null opv6
```

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.
R1#conf term / se ingresa a la configuración de terminal
R1(config)#router bgp 300 / se asigna bgp y ns 300
R1(config-router)#bgp router-id 1.1.1.1 //Asigna id del router
Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.
R1(config-router)#neighbor 209.165.200.226 remote-as 500
//se define la relación vecino ipv4
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
//se define la relación vecino ipv6

Figura 14. Configuración en R1



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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los host en la “Red de la Compañía”. Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6.

		<p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	<p>En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.</p>	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p>

		<ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN</p>

		<p>102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.
--	--	--

Tarea 4.1

Para la solución de esta se implementa el siguiente código:

Cree dos IP SLAs.

- Use la SLA número 4 para IPv4.
- Use la SLA número 6 para IPv6.

```
D1(config)# ip sla 4 //Nombra el seguidor del servidor a configurar
```

```
D1(config-ip-sla)# icmp-echo 10.0.10.1 //se indica la ip a configurar
```

```
D1(config-ip-sla-echo)# frequency 5
```

```
D1(config-ip-sla-echo)# exit
```

Se realiza el mismo código para Ipv6

```
D1(config)# ip sla 6
```

```
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
```

```
D1(config-ip-sla-echo)# frequency 5
```

```
D1(config-ip-sla-echo)# exit
```

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

```
D1(config-ip-sla)# ip sla schedule 4 life forever start-time now /se define el inicio y que se mantenga implementada.
```

```
D1(config-ip-sla)# ip sla schedule 6 life-forever start-time now
```

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la IP SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down

a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D1(config-ip-sla)# track 4 ip sla 4 //actualiza el estatus de los cambios en la conexión o configuracion.
```

```
D1(config-ip-sla-track)# delay down 10 up 15 //Declara el tiempo en el que actualiza los cambios o notifica
```

Tarea 4.2

- Use la SLA número 4 para IPv4.
- Use la SLA número 6 para IPv6.

```
D2(config)# ip sla 4 //Asigna nombre el seguidor del servidor a configurar
```

```
D2(config-ip-sla)# icmp-echo 10.0.11.1 // se indica la ip a configurar
```

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

```
D2(config-ip-sla-echo)# frequency 5
```

```
D1(config-ip-sla-echo)# exit
```

Se realiza el mismo código para Ipv6

```
D2(config)# ip sla 6
```

```
D2(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
```

```
D2(config-ip-sla-echo)# frequency 5
```

```
D2(config-ip-sla-echo)# exit
```

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

```
D2(config-ip-sla)# ip sla schedule 4 life forever start-time now /se define el inicio y que se mantenga implementada.
```

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

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la IP SLA 6.

Tarea 4.3

Como D1 es el router primario para las VLANs 100 y 102; entonces también lo es su prioridad.

Se cambiará a 150. Configure HSRP versión 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

```
D1(config)#interface vlan 100 / se ingresa a la vlan a configurar
```

```
D1(config-if)#standby version 2 /se configura HSRP en la vlan
```

```
D1(config-if)#standby 104 ip 10.0.100.254 /se asigna la ip virtual
```

```
D1(config-if)#standby 104 priority 150 /se establece prioridad en 150
```

```
D1(config-if)#standby 104 preempt /se configura como preferencia
```

```
D1(config-if)#standby 104 track 4 decrement 60
```

//Configuración de rastreo del objeto y decremento 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

```
D1(config)#interface vlan 101
```

```
D1(config-if)# standby version 2
```

```
D1(config-if)# standby 114 ip 10.0.101.254
```

```
D1(config-if)# standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
Configure IPv4 HSRP grupo 124 para la VLAN 102:
```

- Asigne la dirección IP virtual 10.0.102.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Tarea 4.4

En D2, configure HSRPv2.

se usó el mismo código de la tarea 4.3 y realizamos los cambios de vlan e ip según corresponda:

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

```
D2(config)#interface vlan 100 / se ingresa a la vlan a configurar
```

```
D2(config-if)# standby version 2 /se configura HSRP en la vlan
```

```
D2(config-if)# standby 104 ip 10.0.100.254 /se asigna la ip virtual
```

```
D2(config-if)# standby 104 track 4 decrement 60
```

//se configura el rastreo del objeto y decremento 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Estableciendo la prioridad 150. Utilizamos los códigos del paso inmediatamente anterior cambiando la vlan, la ip virtual y el grupo

```
D2(config-if)#interface vlan 101
```

```
D2(config-if)# standby version 2
```

```
D2(config-if)# standby 114 ip 10.0.101.254
```

```
D2(config-if)# standby 114 priority 150
```

```
D2(config-if)# standby 114 preempt
```

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.
- Habilite la preferencia (preemption).

- Rastree el objeto 4 para disminuir en 60.

Continuamos con la serie de codigos utilizados en el paso anterior cambiando la vlan y la ip virtual en este paso no se establece prioridad:

D2(config-if)#interface vlan 102

D2(config-if)# standby version 2

D2(config-if)# standby 124 ip 10.0.102.254

D2(config-if)# standby 124 preempt

D2(config-if)#standby 124 track 4 decrement 60

De acá en adelante se replica el código, pero ahora se configura la ipv6:

Configure IPv6 HSRP grupo 106 para la VLAN 100:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

D2(config-if)#standby 106 ipv6 autoconfig

D2(config-if)# standby 106 preempt

D2(config-if)# standby 106 track 6 decrement 60

Configure IPv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).

Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

Tarea	Tare	Es
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: sadmin • Nivel de privilegio 15
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos	Especificaciones del

	(excepto R2), configure las especificaciones del servidor RADIUS.	servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor
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
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123 .

Tarea 5.1

Detalles de la cuenta encriptada SCRYPT:

- Nombre de usuario Local: sadmin
- Nivel de privilegio 15
- Contraseña: cisco12345cisco
- Habilite AAA (no en R2).

```
R2(config)#enable password cisco12345cisco //Contraseña Modo Privilegiado
R2(config)#service password-encryption //Encriptación de contraseña
R2(config)#exit //Sale de modo de configuración
```

```
R2#conf t
R2(config)#enable secret level 15 cisco12345cisco //Nivel privilegiado 15
R2(config)#username sadmin privilege 15 secret cisco12345cisco
//Contraseña encriptada y creación de usuario
R2(config)#
```

```
R1(config)#enable password cisco12345cisco
R1(config)#service password-encryption
```

```
R1(config)#enable secret level 15 cisco12345cisco
R1(config)#username sadmin privilege 15 secret cisco12345cisco
R1(config)#aaa new-model //Se declara model aaa
R1(config)#
```

```
D1(config)#enable password cisco12345cisco
D1(config)#service password-encryption
D1(config)#enable secret level 15 cisco12345cisco
D1(config)#username sadmin privilege 15 secret cisco12345cisco
D1(config)#aaa new-model
```

```
D2(config)#enable password cisco12345cisco
D2(config)#service password-encryption
D2(config)#enable secret level 15 cisco12345cisco
D2(config)#username sadmin privilege 15 secret cisco12345cisco
D2(config)#aaa new-model
```

Nota: La configuración, instrucciones y procedimiento realizado para dar cumplimiento a la tarea 5.1 también cubren la solución a la tarea 5.2 y 5.3

Especificaciones del servidor RADIUS:

- Dirección IP del servidor RADIUS es 10.0.100.6.
- Puertos UDP del servidor RADIUS son 1812 y 1813.
- Contraseña: \$trongPass

Especificaciones de autenticación AAA:

- Use la lista de métodos por defecto
- Valde contra el grupo de servidores RADIUS
- De lo contrario, utilice la base de datos local.

```
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
//Asigna Direccion IP y puertos del servidor RADIUS
R1(config-radius-server)#key $trongPass //Se asigna contraseña
R1(config-radius-server)#
```

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

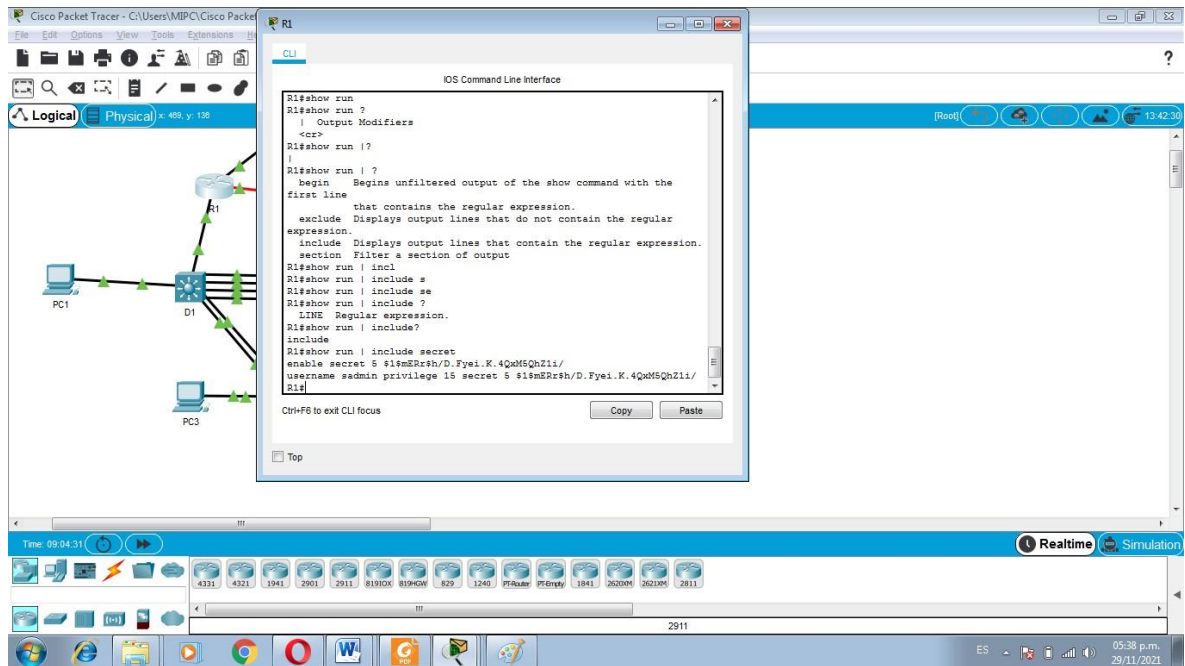
Warning: Address not yet configured.

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

```
D1(config)#aaa new-model  
D1(config)#radius server RADIUS  
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
D1(config-radius-server)#key $strongPass  
D1(config-radius-server)#exit  
D1(config)#aaa authentication login default group radius local  
D1(config)#end
```

```
A1(config)#aaa new-model  
A1(config)#radius server RADIUS  
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
A1(config-radius-server)#key $strongPass  
A1(config-radius-server)#exit  
A1(config)#aaa authentication login default group radius local  
A1(config)#end
```

Figura 15. Configuración de seguridad en R1



Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

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.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel

		WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	<p>Especificaciones de SNMPv2:</p> <ul style="list-style-type: none"> • Únicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el <i>community string</i> en ENCORSA. • En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>. • En R1, habilite el envío de <i>traps bgp, config, y ospf</i>. • En A1, habilite el envío de <i>traps config</i>

Tarea 6.1

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

R1#clock set 05:24:00 29 Nov 2021 //Configura fecha y hora actual

R2#clock set 05:24:00 29 Nov 2021

R3#clock set 05:24:00 29 Nov 2021

D1#clock set 05:24:00 29 Nov 2021

A1#clock set 05:24:00 29 Nov 2021

D2#clock set 05:24:00 29 Nov 2021

Tarea 6.2

Configurar R2 como NTP maestro en el nivel de estrato 3.

```
R2(config)#ntp master 3
```

Tarea 6.3, 6.4 y 6.5

```
R1(config)#ntp server 2.2.2.2           // se configura NTP
R1(config)#logging trap warning        // Syslogs en nivel warning
R1(config)#logging host 10.0.100.5    // enviarse a la PC1 en 10.0.100.5
R1(config)#logging on                  //se cambia a estado encendido

R1(config)#ip access-list standard SNMP-NMS //configura SNMP lectura
R1(config-std-nacl)#permit host 10.0.100.5 //declara límite de acceso
R1(config-std-nacl)#exit
R1(config- snmp)#snmp-server contact Cisco frayD // valor de contacto SNP
R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA

R1(config- snmp)#snmp-server ifindex persist /se habilita el envío de traps
R1(config- snmp)#snmp-server enable traps bgp /se habilita el envío de traps bgp
R1(config- snmp)#snmp-server enable traps config /se habilita traps
R1(config- snmp)# snmp-server enable traps ospf

//se habilita el envió de traps osfp
R1(config- snmp)#end /se finaliza la configuración
```

```
R3(config)#logging host 10.0.100.5
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config- snmp)#snmp-server contact Cisco gustavoR
R3(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R3(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
```

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

```
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco gustavoR
D1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSAs
D1(config- snmp)#snmp-server ifindex persist
D1(config- snmp)#snmp-server enable traps config
D1(config- snmp)#snmp-server enable traps ospf
```

```
A1(config)#ntp server 10.0.10.1
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)#logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco gustavoR
A1(config- snmp)#snmp-server community ENCORSAs ro SNMP-NMS
A1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSAs
A1(config- snmp)#snmp-server ifindex persist
A1(config- snmp)#snmp-server enable traps config
A1(config- snmp)#snmp-server enable traps ospf
```

CONCLUSIONES

Con el desarrollo de esta prueba de habilidades del diplomado CCNP se logró realizar la configuración y diseño de un escenario propuesto de donde realizo satisfactoriamente su caracterización y configuración desde la capa 2. Además se construyó la red, se realizó la configuración básica de cada dispositivo y el direccionamiento de las interfaces, se realizó la configuración capa 2 de la red y protocolos de enrutamiento, también se realizó la configuración de redundancia de primer salto y configuración de la seguridad de la red.

En otro sentido se implementó los protocolos de enrutamiento de la red, configurando OSPF tanto para ipv4 como ipv6, enrutando por familias y áreas de red. Finalmente se establece la comunicación de la red y subredes del escenario

BILIOGRAFÍA

CISCO. (s.f.) Cómo comprender VLAN Trunk Protocol (VTP) . Recuperado de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf

CISCO. (2020). Configure InverVLAN Routing on Layer 3 Switches. Recuperado de <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

AREAIP. (s.f.). Comandos Ethernetchannel o Portchannel con LACP y PAGP. Recuperado de http://areaip.blogspot.com/2016/09/comandos-ethernetchannel-o-portchannel_24.html

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de <https://1drv.ms/b/s!AqIGq5JUgUBthFt77ehzL5qp0OKD>

Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>