DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FERNEY JESUS COMEZAQUIRA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FERNEYJESUS COMEZAQUIRA

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 ELECTRÓNICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ,29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

SWITCH: son piezas de construcción claves para cualquier red, conectan varios dispositivos como computadoras, access points inalámbricos, impresoras y servidores en la misma red de un edificio o campus. Permite a los dispositivos conectados compartir información y comunicasen entre sí.

PROTOCOLO DE ENRUTAMIENTO: los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otro router con el fin de compartir información de enrutamiento dicha información se usa para construir y mantener las tablas de enrutamiento. Un protocolo de enrutamiento es la aplicación de un algoritmo de enrutamiento en el software o hardware.

VLAN: (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

BGP: Protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicios registrados en internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

HOST: servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas. Al igual que cualquier computadora conectada a internet, debe tener una dirección o número IP y un nombre.

RESUMEN

El presente trabajo comprende el desarrollo de la prueba de habilidades del curso diplomado de profundización CCNP de cisco, para la carrera ingeniería electrónica. Nos permite a los estudiantes estar capacitados, para las soluciones que impliquen la instalación, configuración, administración de redes mediante la topología planteada en el desarrollo de los diferentes puntos tratamos temas de gran ayuda para nuestra vida laboral como profesionales al momento de enfrentar problemas relacionados con las redes.

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

ABSTRACT

The present work includes the development of the skills test of the cisco CCNP deepening diploma course, for the electronic engineering career. It allows us students to be trained, for solutions that involve the installation, configuration, administration of networks through the topology raised in the development of the different points, we deal with topics of great help for our working life as professionals when facing problems related to the networks.

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

INTRODUCCIÓN

para un ingeniero electrónico es vital obtener conocimientos, habilidades y acertado desempeño en el campo de las redes de comunicación como sistema eficaz para diferentes aplicaciones actuales en las industrias. A través del desarrollo del diplomado de CCNP de CISCO se obtendrán conocimientos en el área de enrutamiento de protocolos tales como el OSPF, BGP entre otros. Además del enrutamiento de VLAN y la configuración de la seguridad de la plataforma de comunicación. La estrategia del trabajo está compuesta de un escenario y radica en la solución de ejercicios donde se aplicará los conocimientos de enrutamiento por medio de herramientas de simulación como packet tracer, GNS3 o Smartlab. Su objetivo es comprender la arquitectura y el control de la red de rango medio y enfatizar en el protocolo de enrutamiento y su optimización mediante configuración.

En el escenario propuesto configuraremos la topología de red desde 0 desarrollaremos los 6 puntos propuestos con su respectivo ítem de tareas.

DESARROLLO

Escenario

Imagen 1. Escenario propuesto

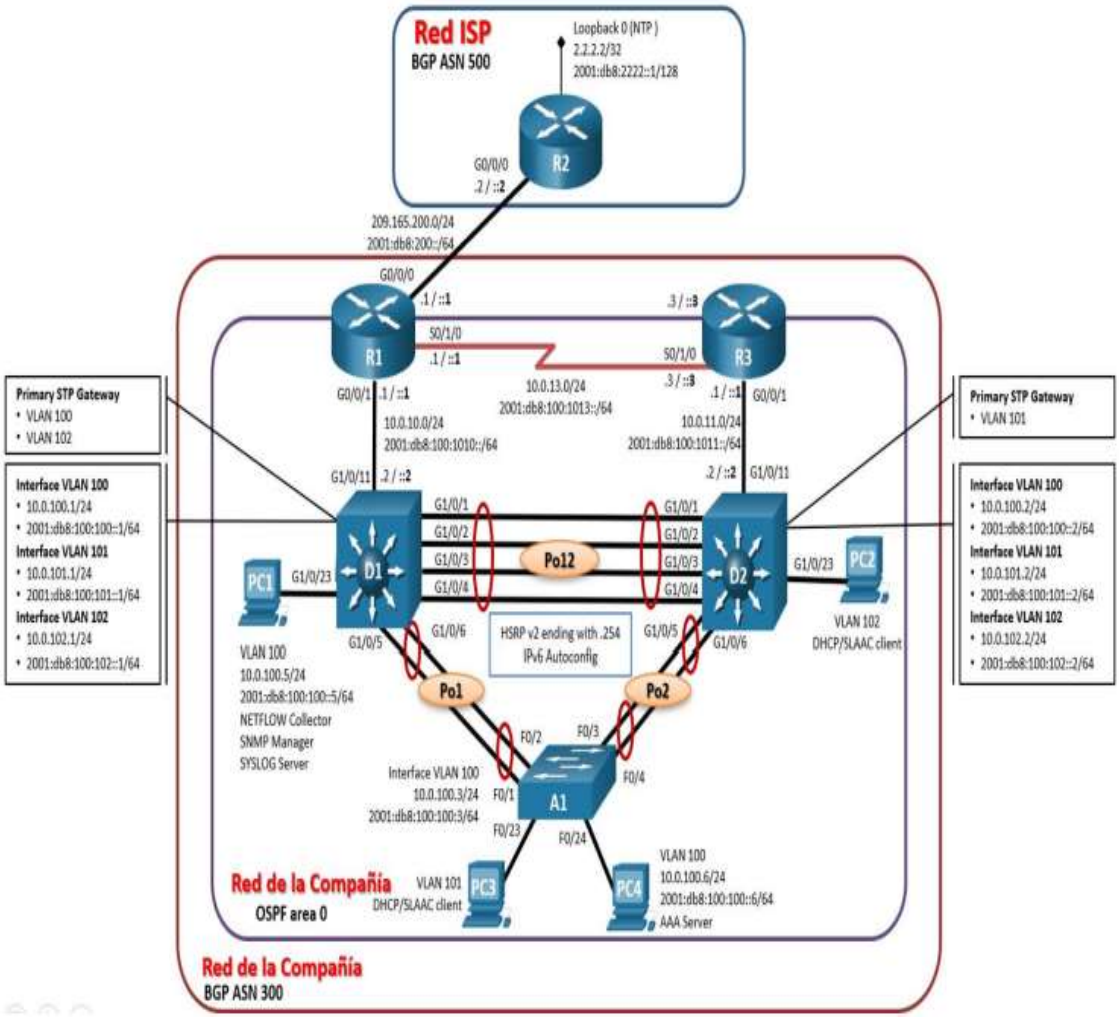


Tabla 1. Direccionamiento escenario propuesto

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

Recursos necesarios

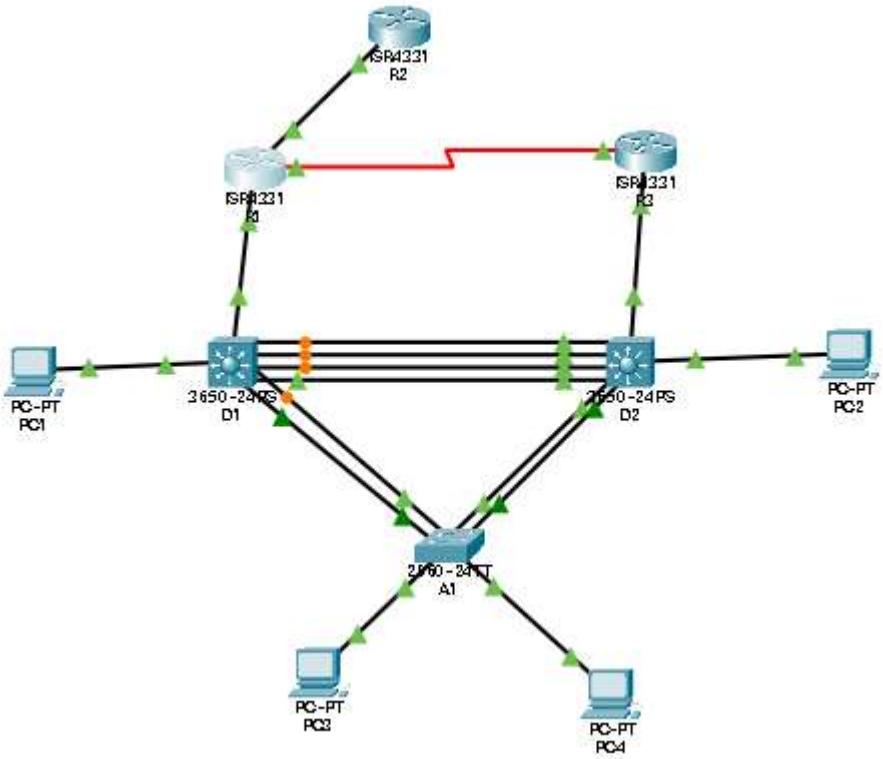
3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
4 PCs (utilice el programa de emulación de terminal)
Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
Los cables Ethernet y seriales van como se muestra en la topología

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

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

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

Imagen 2. Simulación tipología



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Router R1

Router>enable /se ingresa a modo privilegiado
Router#confi t /se ingresa a modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1 /se asigna nombre al router R1
R1(config)#ipv6 unicast-routing / tipo de dirección ipv6
R1(config)#no ip domain lookup /evitar retrasos al ingresar un comando mal escrito
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 g0/0/0
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 g0/0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0

```
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown

R1(config-if)#exit
R1(config)#interface s0/1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#
R1#
```

Router R2

```
Press RETURN to get started!



Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#hostname R2
R2(config)#ipv6 unicast-routing
```

```
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g0/0/0
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)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

R2(config-if)#exit
R2(config)#interface Loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up

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 R3

```
Router>enable
Router#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface g0/0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown

R3(config-if)#exit
R3(config)#interface s0/1/0
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
R3(config-if)#exit
R3(config)#
```

R3(config)#

Switch D1

Press RETURN to get started!

Switch>enable
Switch#confi 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
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 g1/0/11
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 g1/0/1-10, g1/0/12-24, g1/1/1-4
interface range not validated - command rejected
D1(config)#shutdown
^
D1(config)#exit
D1#
```

Switch D2

```
Press RETURN to get started!


Switch>enable
Switch#confi 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(config)#interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
interface range not validated - command rejected
D2(config)#shutdown
D2(config)#exit

D2(config)#exit
D2#
```

Switch A1

```
Switch>enable
Switch#confi t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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-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
^
% Invalid input detected at '^' marker.
```

```
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
^
% Invalid input detected at '^' marker.
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range f0/5-22
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#

A1(config)#
A1(config)#
```

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

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

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

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

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

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

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

c. Configure el direccionamiento de los hosts 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.

Podemos evidenciar la puerta de enlace predeterminada en los pc1 y pc4

Imagen 3. Verificación puerta de enlace

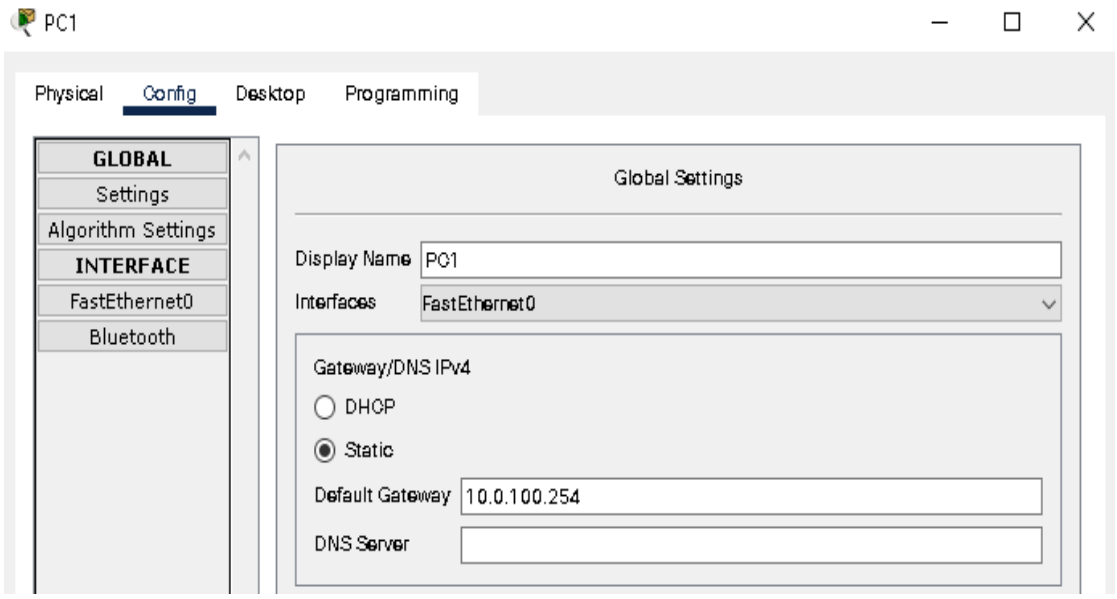
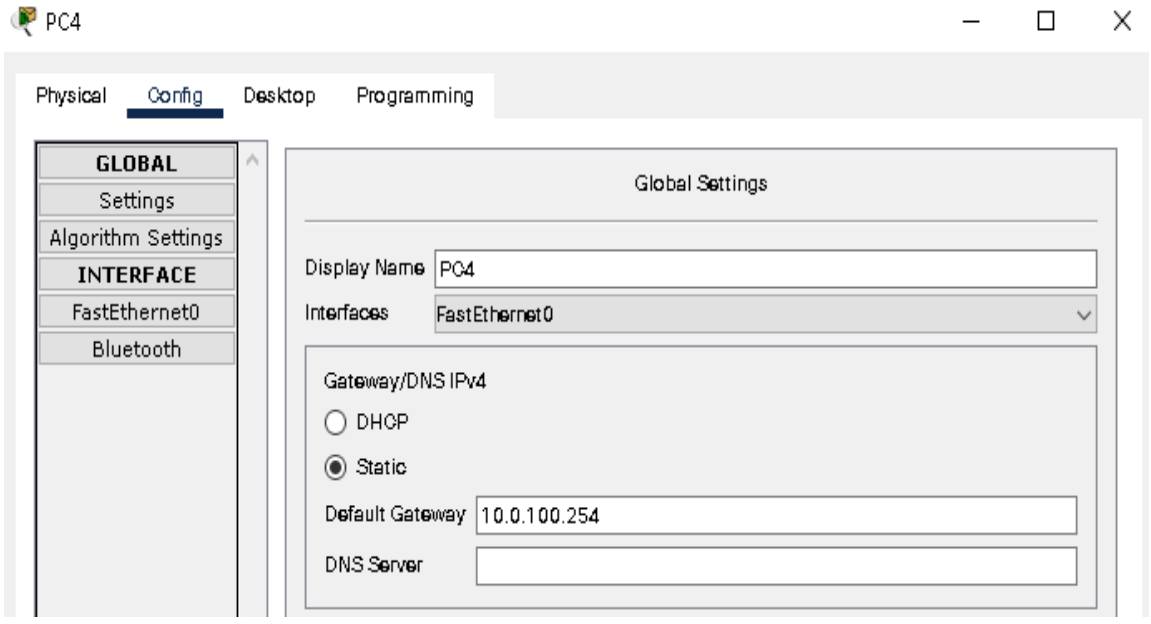


Imagen 4. Verificación puerta de enlace pc4



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 debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC. Las tareas de configuración son las siguientes:

Tabla 2. Configuración capa 2

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: •D1andD2 •D1andA1 • 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: • 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: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Tarea 2.1

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

Para esta solución se debe configurar la encapsulación que hace referencia a 802.1Q la cual es dot1q se utiliza el siguiente código en cada conexión

D1#sh int gig1/0/1 switchport
Name: Gig1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001

Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

D1#sh int gig1/0/5 switchport
Name: Gig1/0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All

D2#sh int gig1/0/6 switchport
Name: Gig1/0/6
Switchport: Enabled

Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All

Tarea 2.2

En todos los switches cambie la VLAN nativa en los enlaces troncales.

D1

100 VLA100 active
101 VLA101 active
102 VLA102 active
999 NATIVE active

1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

D2

100 Management active
101 UserGroupA active
102 UserGroupB active
999 NATIVE active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

Tarea 2.3

En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP se configura el protocolo Rapid Spanning Tree (RSPT).

D1

D1#sh spanning-tree
VLAN0001
Spanning tree enabled protocol rstp

Root ID Priority 32769
Address 0001.639B.EC56
Cost 19
Port 5(GigabitEthernet1/0/5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

D2

D2#sh spanning-tree
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 32769
Address 0001.639B.EC56
Cost 19
Port 5(GigabitEthernet1/0/5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

A1

A1#sh spanning-tree
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 32769
Address 0001.639B.EC56
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Tarea 2.4

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

A continuación, podemos ver que el switch D1 es el principal en la vlan100 y 102 en caso de falla del puente raíz

D1

VLAN0100
Spanning tree enabled protocol rstp
Root ID Priority 24676
Address 00D0.9711.32C9
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24676 (priority 24576 sys-id-ext 100)
Address 00D0.9711.32C9
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

VLAN0102
Spanning tree enabled protocol rstp
Root ID Priority 24678
Address 00D0.9711.32C9
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24678 (priority 24576 sys-id-ext 102)
Address 00D0.9711.32C9
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

A continuación, podemos ver que el switch D2 es el principal en la vlan101 en caso de falla del puente raíz

D2

VLAN0101
Spanning tree enabled protocol rstp
Root ID Priority 24677
Address 0004.9AA6.9D2C
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24677 (priority 24576 sys-id-ext 101)
Address 0004.9AA6.9D2C
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Tarea 2.5

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

A continuación podemos ver la configuración de EtherChannels LACP

D2

D2#sh etherchannel
Channel-group listing:

Group: 2

Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP

Group: 12

Group state = L2
Ports: 4 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP

A1

A1#sh etherchannel
Channel-group listing:

Group: 1

Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP

Group: 2

Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP

D1

D1#sh etherchannel
Channel-group listing:

Group: 1

Group state = L2
Ports: 2 Maxports = 16

Port-channels: 1 Max Port-channels = 16
Protocol: LACP

Group: 12

Group state = L2
Ports: 4 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
D1#

Tarea 2.6

En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

A1 PC3 Y PC4

100 VLAN100 active Fa0/7, Fa0/24
101 UserGroupA active Fa0/23
102 UserGroupB active
999 NATIVE active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
D1 PC1

D1(config-if)#int gig1/0/23
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan100

D1#sh vlan brief

100 VLA100 active Gig1/0/23
101 VLA101 active

D2 A PC2

D2#sh vlan brief

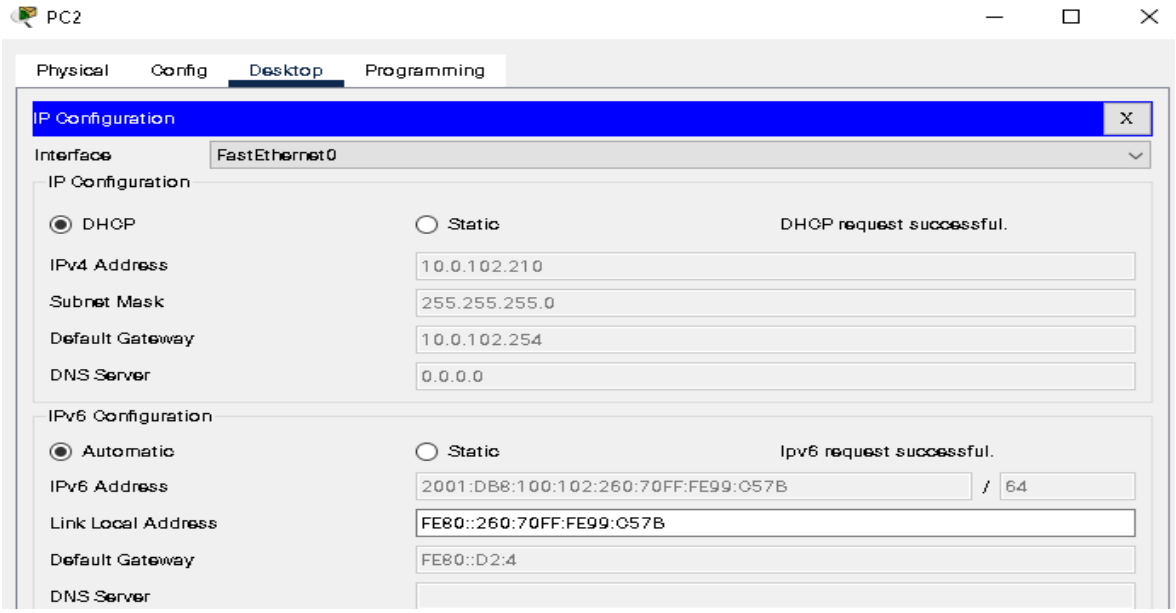
100 Management active
101 UserGroupA active
102 UserGroupB active Gig1/0/23
999 NATIVE active

Tarea 2.7

Verifique los servicios DHCP IPv4.

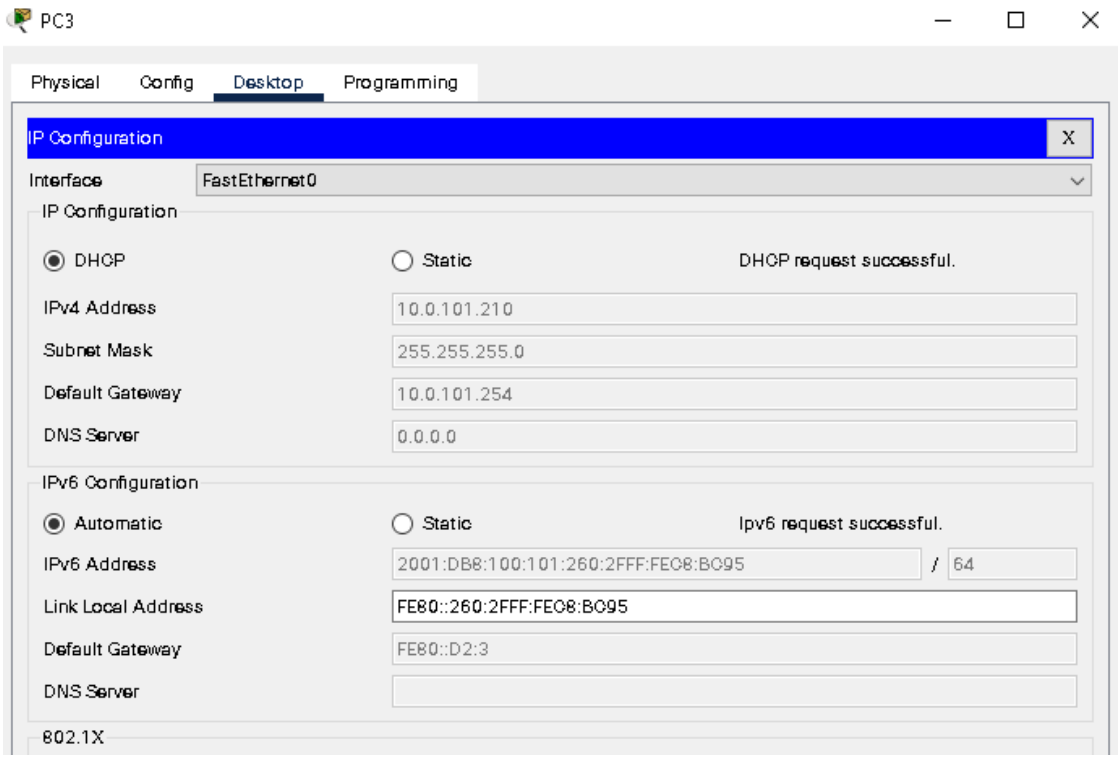
Verificamos en pc2

Imagen 5. DHCP IPv4 en pc2



Verificamos en PC3

Imagen 6. DHCP IPv4 en pc3



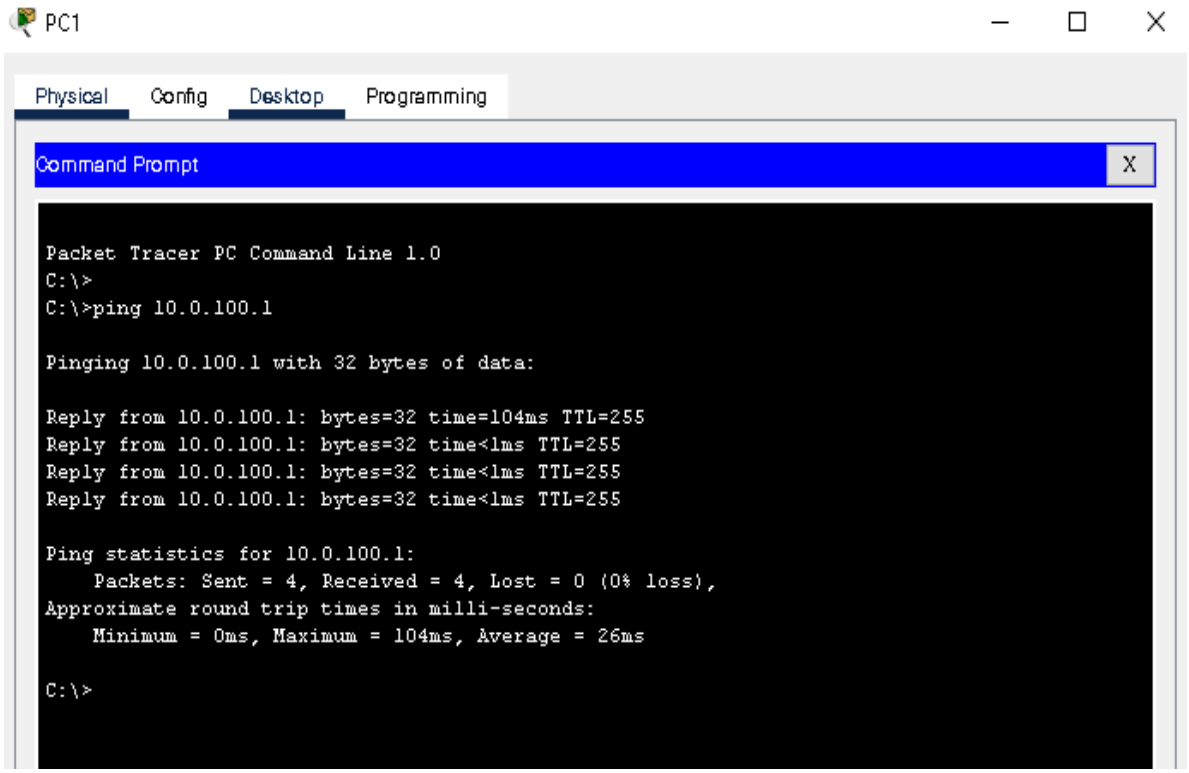
Tarea 2.8

Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

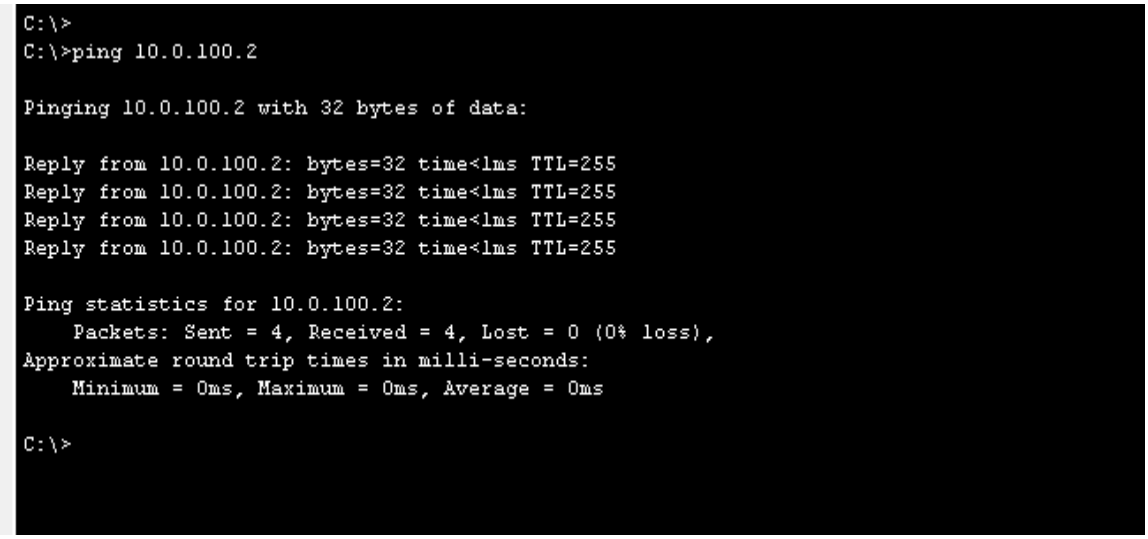
• D1: 10.0.100.1

Imagen 7. Ping pc1 y D1



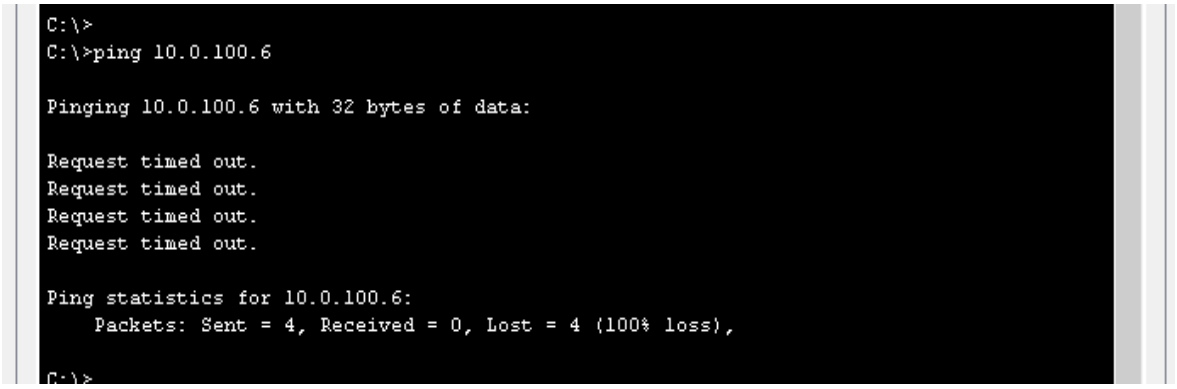
• D2: 10.0.100.2

Imagen 8. Ping entre pc1 y D2



• PC4: 10.0.100.6

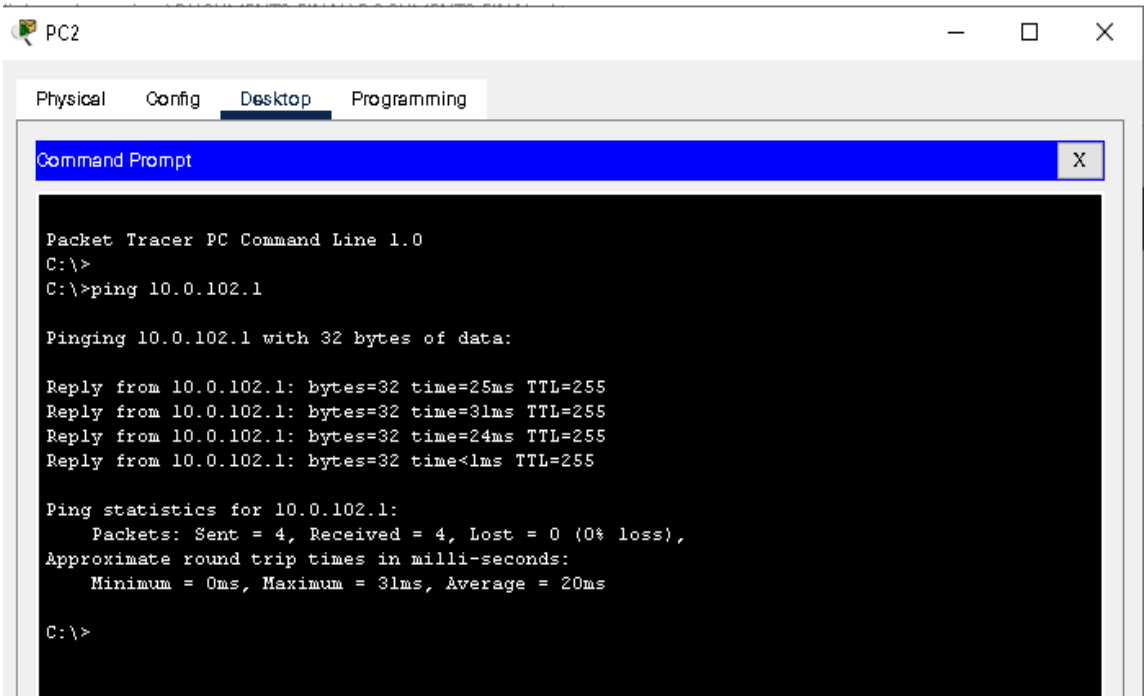
Imagen 9. Ping entre pc1 y pc4



PC2 debería hacer ping con éxito a:

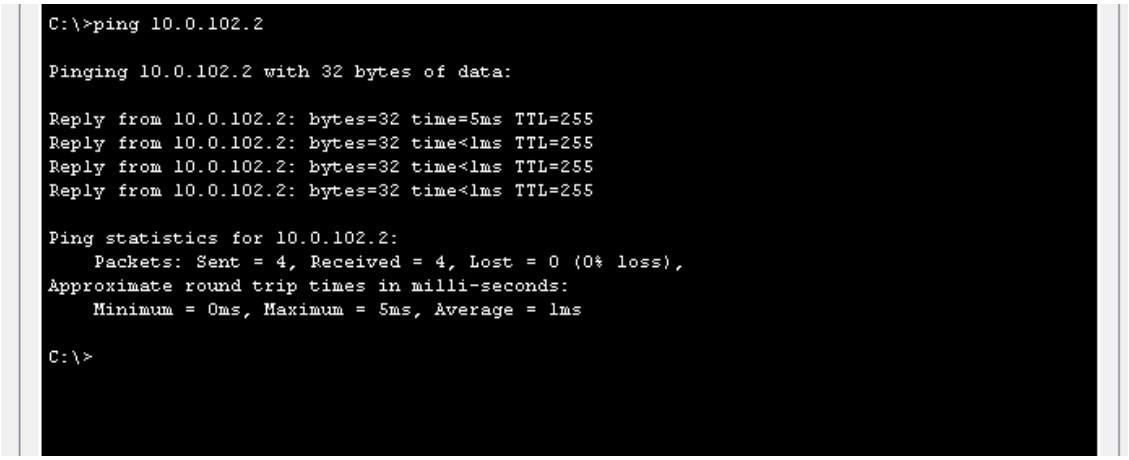
• D1: 10.0.102.1

Imagen 10. Ping entre pc2 y D1



• D2: 10.0.102.2

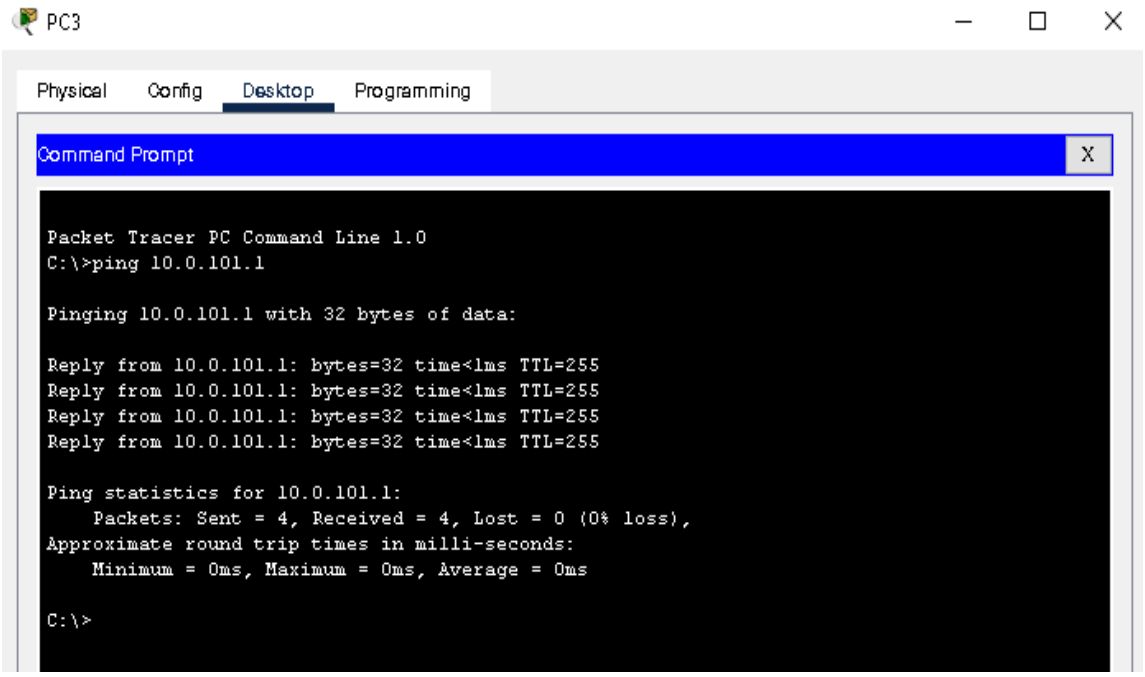
Imagen 11. Ping entre pc2 y D2



PC3 debería hacer ping con éxito a:

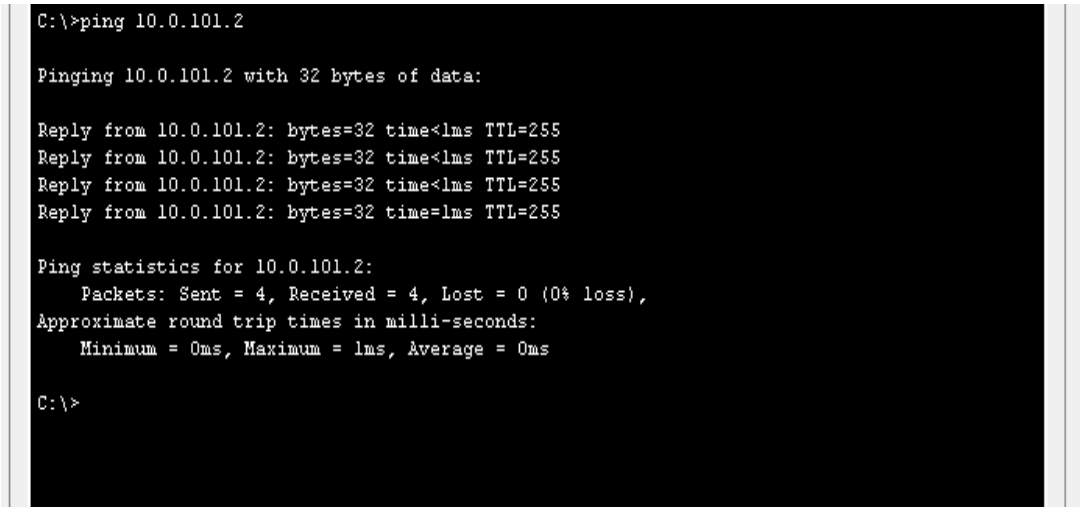
• D1: 10.0.101.1

Imagen 12. Ping entre pc3 y D1



• D2: 10.0.101.2

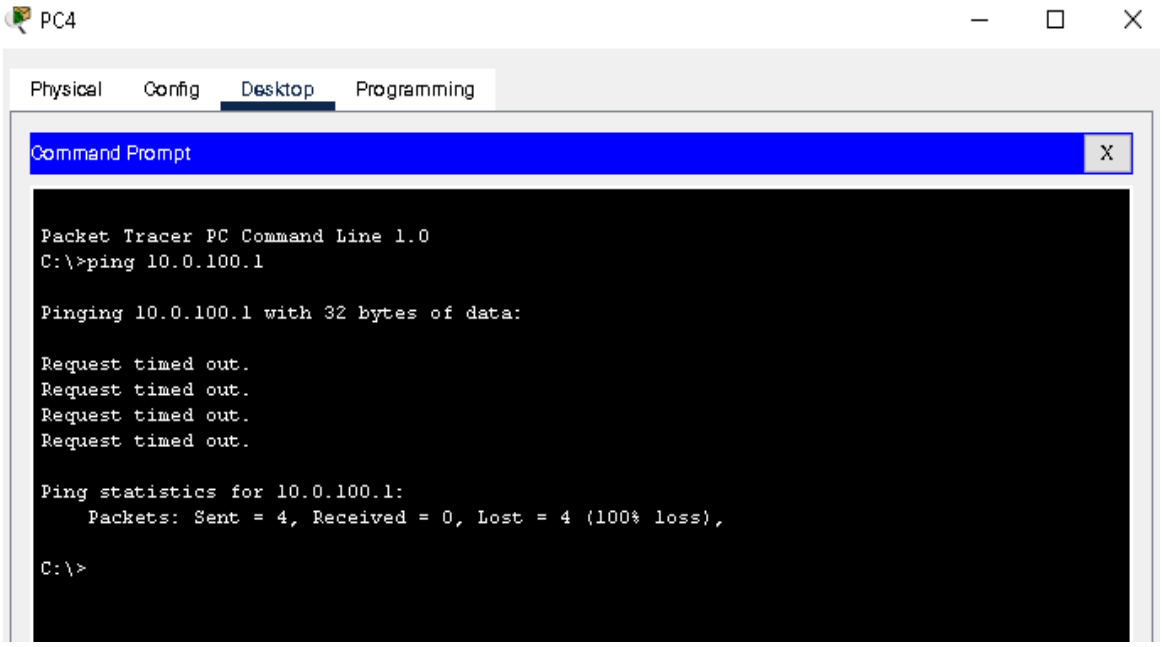
Imagen 13. Ping entre pc3 y D2



PC4 debería hacer ping con éxito a:

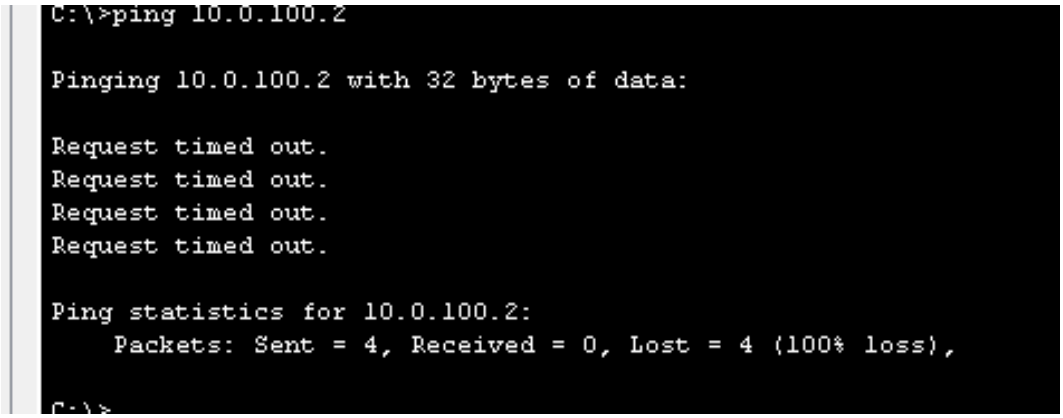
• D1: 10.0.100.1

Imagen 14. Ping entre pc4 y D1



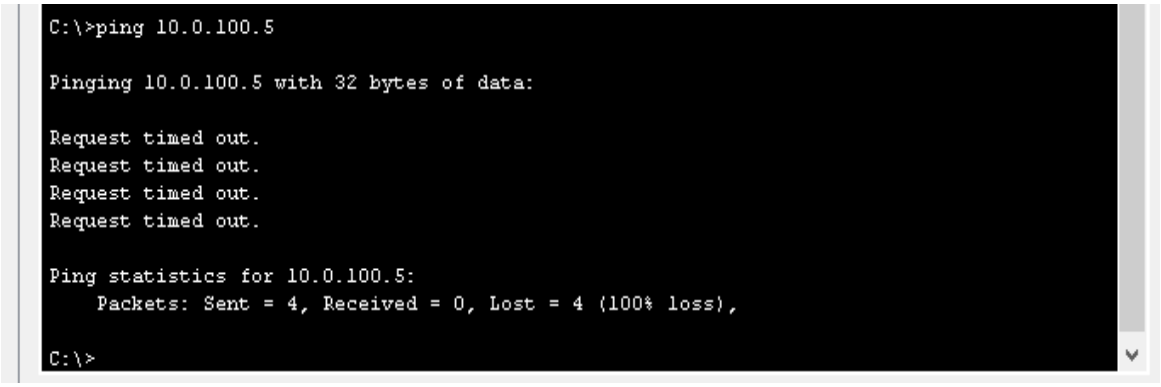
• D2: 10.0.100.2

Imagen 15. Ping entre pc4 y D2



• PC1: 10.0.100.5

Imagen 16. Ping entre pc4 y pc1



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:

Tabla 3. configuración protocolos de enrutamiento

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 routerIDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Área 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.	R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0. Use OSPF Process ID 6 y asigne los siguientes routerIDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Área 0. • 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: • 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 MPBGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la "Red ISP", configure MPBGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family:

		• Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6maddress family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48

Tarea 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:

• R1: 0.0.4.1

Anuncie todas las redes directamente conectadas / VLANs en Area 0.

R1> en

R1#confi t

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

R1(config)#router ospf 4

R1(config-router)#

R1(config-router)#router-id 0.0.4.1

R1(config-router)#do show ip route connected

C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1

C 10.0.13.0/24 is directly connected, Serial0/1/0

C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1
L 10.0.10.1/32 is directly connected, GigabitEthernet0/0/1
C 10.0.13.0/24 is directly connected, Serial0/1/0
L 10.0.13.1/32 is directly connected, Serial0/1/0
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0
S* 0.0.0.0/0 is directly connected, GigabitEthernet0/0/0

• R3: 0.0.4.3

R3>en
R3#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#do show ip route connected
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)#
00:10:44: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial0/1/0 from LOADING to FULL, Loading Done

R3(config-router)#end

Neighbor ID Pri State Dead Time Address Interface
0.0.4.1 0 FULL/ - 00:00:39 10.0.13.1 Serial0/1/0
R3#

D1>en
D1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#do show ip route connected
C 10.0.10.0/24 is directly connected, GigabitEthernet1/0/11
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0

D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#
00:50:42: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on GigabitEthernet1/0/11 from FULL to DOWN, Neighbor Down: Interface down or detached
D1(config-router)#no passive-interface g1/0/11
D1(config-router)#
00:51:27: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on GigabitEthernet1/0/11 from LOADING to FULL, Loading Done

Se deshabilitan las publicaciones OSPFv2 en el swiche D1

D2>en
D2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#do show ip route connected
D2(config-router)#do show ip route connected
C 10.0.11.0/24 is directly connected, GigabitEthernet1/0/11
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0

D2(config-router)#passive-interface default
D2(config-router)#
01:12:11: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on GigabitEthernet1/0/11 from FULL to DOWN, Neighbor Down: Interface down or detached
D2(config-router)#no passive-interface g1/0/11
D2(config-router)#
01:12:57: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on GigabitEthernet1/0/11 from LOADING to FULL, Loading Done

Se deshabilitan las publicaciones OSPFv2 en el swiche D2

Tarea 3.2

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

Utilizamos ahora la configuración para ipv6

R1>en
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 6 / configuramos ospf en ipv6
R1(config-rtr)#router-id 0.0.6.1 / asignamos id
R1(config-rtr)#default-information originate / declaramos informacion predeterminada
R1(config-rtr)#exit / salimos del modo configuracion

R1(config)#int gig0/0/1 / declaramos la interfaz que vamos a configurar
R1(config-if)#ipv6 ospf 6 area 0 /asignamos area 0 en ipv6
R1(config-if)#exit /salimos del modo configuración
R1(config)#int s0/1/0 /declaramos la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0 / asignamos area 0 en ipv6
R1(config-if)#
R1(config-if)#end /terminamos con la configuración

Aplicamos el código anterior para la configuración para R3, D1, D2

```
R3>en
R3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface gig0/0/1
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
R3(config)#
```

01:37:34: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial0/1/0 from LOADING to FULL, Loading Done

```
D1>en
D1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
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 g1/0/11
D1(config-rtr)#exit
D1(config)# interface g1/0/11
D1(config-if-range)#ipv6 ospf  6 area 0
D1(config-if)#exit
D1(config)# interface vlan 100
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)# interface vlan 101
D1(config)#ipv6 ospf 6 area 0
D1(config-if)# exit

D1(config)#int  vlan 102
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config-if)#end


D2>en
D2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
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)#exit
D2(config)#int g1/0/11
D2(config-if)#ipv6 ospf  6 area 0
D2(config)#exit
D2(config)#interface vlan 100
D2(config)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config)#ipv6 ospf 6 area 0
D2(config-if)# exit

D2(config)#interface vlan 102
D2(config)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#end
```

Tarea 3.3

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

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

- Una ruta estática predeterminada IPv4.
- Una ruta estática predeterminada IPv6.

Utilizaremos el siguiente código

R2>enable / se ingresa al modo privilegiado
R2#configure terminal /se ingresa a configurar el terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 /Llamamos la interfaz a configurar loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)# ipv6 route ::/0 loopback 0 /Establecemos los parámetros a configurar con ip y mascara de red, como indica la topología
R2(config)#

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

Configuramos las redes directamente conectadas en el R2 usando el siguiente código

R2#confi t / Configuramos terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 500 /Establecemos el router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2 /Asignamos el id 2.2.2.2

Se configuro y se habilitó una relación de vecino IPv4 y IPv6 con R1 en ASN 300

R2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 500 / se establece el router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2 /Asignamos el id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300 /Definimos la relación vecino ipv4
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300 /Definimos la relación vecino ipv6

En IPv4 address family, anuncie:
La red Loopback 0 IPv4 (/32).
La ruta por defecto (0.0.0.0/0).

R2(config-router)# address-family ipv4 / configuramos 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)#network 0.0.0.0 / ruta por defecto
R2(config-router)#exit-address-family /salimos de la configuracion de 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::1/128
R2(config-router)# network ::/0
R2(config-router)#exit-address-family
```

Tarea 3.4

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

Configure dos rutas resumen estáticas a la interfaz Null 0:
Una ruta resumen IPv4 para 10.0.0.0/8.
Una ruta resumen IPv6 para 2001:db8:100::/48.

```
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 10.0.0.0 255.255.255.255 null0
R1(config)#ip route 2001:db8:100::/48 null0
```

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

```
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
```

R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1

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

R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)# neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500

En IPv4 address family:

Deshabilite la relación de vecino IPv6.
Habilite la relación de vecino IPv4.
Anuncie la red 10.0.0.0/8

R1(config-router)#address-family ipv4 unicast
R1(config-router)#neighbor 209.165.200.226 activate
R2(config-router)#exit-address-family
R1(config-router)# no neighbor 2001:db8:200::2 activate

R2(config-router)#network 10.0.0.0 mask 255.0.0.0
R2(config-router)#exit-address-family

En IPv6 address family:

Deshabilite la relación de vecino IPv4.

Habilite la relación de vecino IPv6.

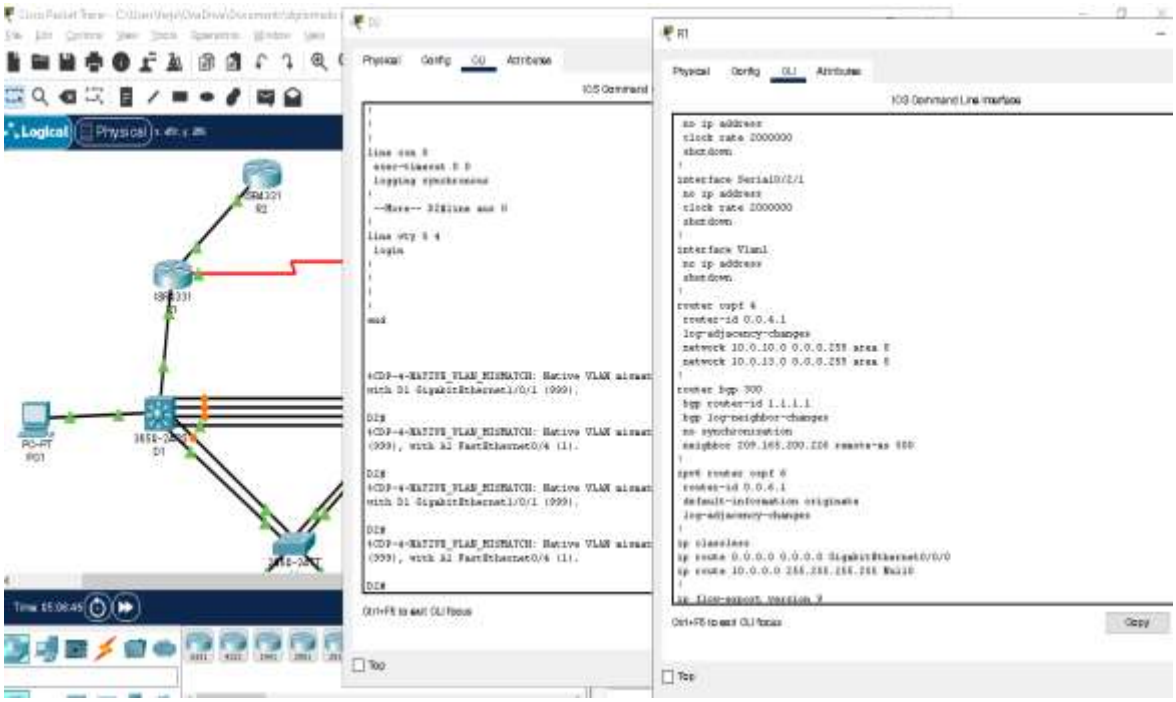
Anuncie la red 2001:db8:100::/48.

R1(config-router)#address-family ipv6 unicast

R1(config-router)#no neighbor 209.165.200.226 activate
R1(config-router)#neighbor 2001:db8:200::2 activate
R1(config-router)#network 2001:db8:100::/48
R1(config-router)#exit-addres-family

Validamos la tarea 3

Imagen 17. Configuración parte 3



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 hosts en la “Red de la Compañía”. Las tareas de configuración son las siguientes

Tabla 4. First Hop Redundancy

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. • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos Programe la SLA para una implementación inmediata sin tiempo de finalización Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de

		Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6 Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.3	En D1 configure HSRPv2	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..

		Configure HSRP version 2 Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100:

		• Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.
4.4	En D2, configure HSRPv2	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2.

		Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60 Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig.

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

Tarea 4.1

Cree dos IP SLAs.

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

D1>en / Ingresamos a modo global
D1#confi t / Ingresamos a la configuración del dispositivo
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#
D1(config)#ip sla 4 / Arroja un error al momento de ingresar el comando
D1(config-ip-sla)# icmp-echo 10.0.10.1 /Indicamos la dirección a configurar

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

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

Con el mismo código configuramos la 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

Programe la SLA para una implementación inmediata sin tiempo de finalización se define el inicio y que se mantenga implementada

D1(config-ip-sla)# ip sla schedule 4 life forever start-time now
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
D1(config-ip-sla-track)# delay down 10 up 15
D1(config-ip-sla-track)#exit
D1(config-ip-sla)# track 6 ip sla 6
D1(config-ip-sla-track)# delay down 10 up 15
D1(config-ip-sla-track)#exit

Se adjunta el código de configuración, pero en el switch de packet tracer no recibió varios comandos

Tarea 4.2

En este punto se configura con el mismo código del punto anterior en el switch D2

Cree IP SLAs.
Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6

D2>en /Se ingresa al modo global
D2#conf term /Se ingresa a la configuración del dispositivo
D2(config)# ip sla 4 / Arroja un error al momento de ingresar el comando
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 R3 G0/0/1 cada 5 segundos.

D2(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit

Realizamos la misma configuración 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

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

se define el inicio y que se mantenga implementada.

D2(config-ip-sla)# ip sla schedule 4 life forever start-time now
D2(config-ip-sla)# ip sla schedule 6 life-forever start-time now

Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.

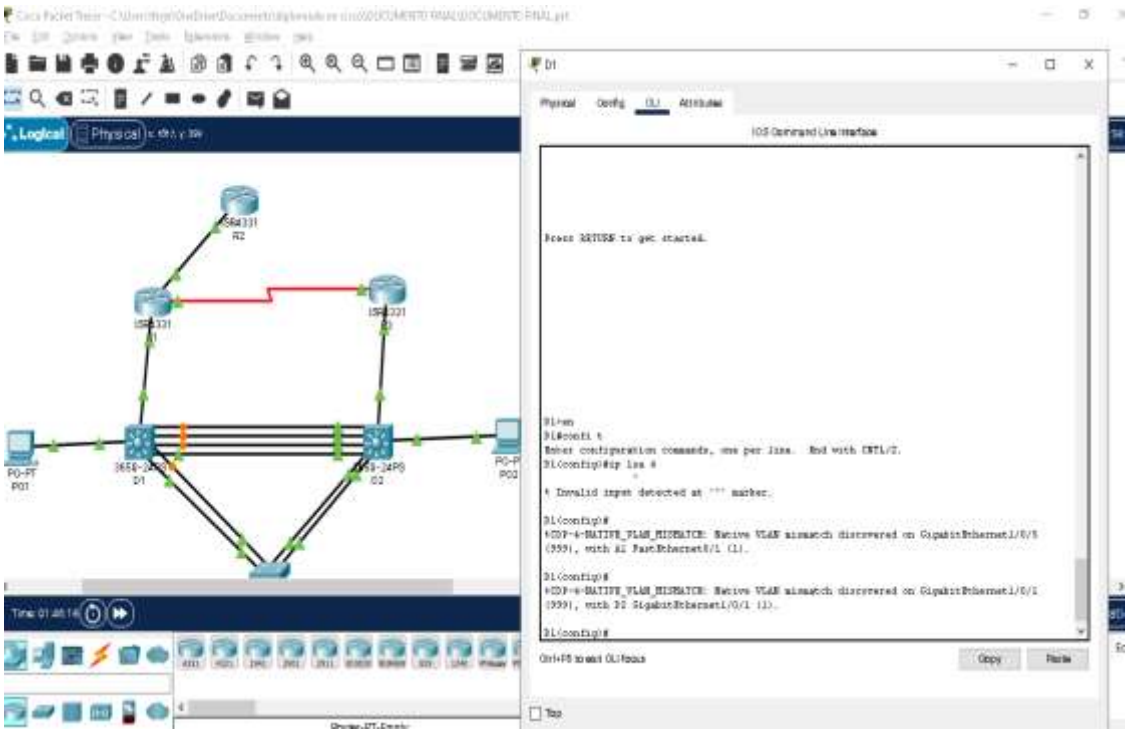
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

D2(config-ip-sla)# track 4 ip sla 4 / Permite actualizar el estatus de los cambios en la conexión o configuración.
D2(config-ip-sla-track)# delay down 10 up 15 / Declara el tiempo en el que actualiza los cambios
D2(config-ip-sla-track)#exit
D2(config-ip-sla)# track 6 ip sla 6
D2(config-ip-sla-track)# delay down 10 up 15
D2(config-ip-sla-track)#exit

Nota: para la tarea 4.1 y 4.2 no reconoce los comandos como se muestra en loa siguiente figura para realizar esta configuración debería implementarse en un ambiente real con los servidores físicos

Imagen 18. Configuración tarea 4.1 y 4.2



Tarea 4.3

En D1 configure HSRPv2

D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decremente en 60.

Utilizaremos la siguiente configuración

D1(config)#interface vlan 100 / ingreso a la vlan a configurar
D1(config-if)#standby version 2 /configuro HSRP en la vlan
D1(config-if)#standby 104 ip 10.0.100.254 /asigno la ip virtual
D1(config-if)#standby 104 priority 150 /se establece prioridad en 150
D1(config-if)#standby 104 preempt /configuro como preferencia
D1(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.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Se utiliza el código del paso anterior, y se configura la vlan

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.

Se utiliza el código del paso anterior, y se configura la vlan 102, se cambia la IP virtual

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

Configure IPv6 HSRP grupo 106 para la VLAN 100:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 6 y decremente en 60.

Para este paso continuamos utilizando el código de configuración anterior y se cambia a ipv6, se cambia la VLAN y la IP virtual

```
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(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.
Habilite la preferencia (preemption).
Registre el objeto 6 y decremente en 60

Continuamos con los mismos pasos de configuración cambiando el grupo y la VLAN y no establecemos prioridad:

D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track 6 decrement 60
Configure IPv6 HSRP grupo 126 para la VLAN 102:

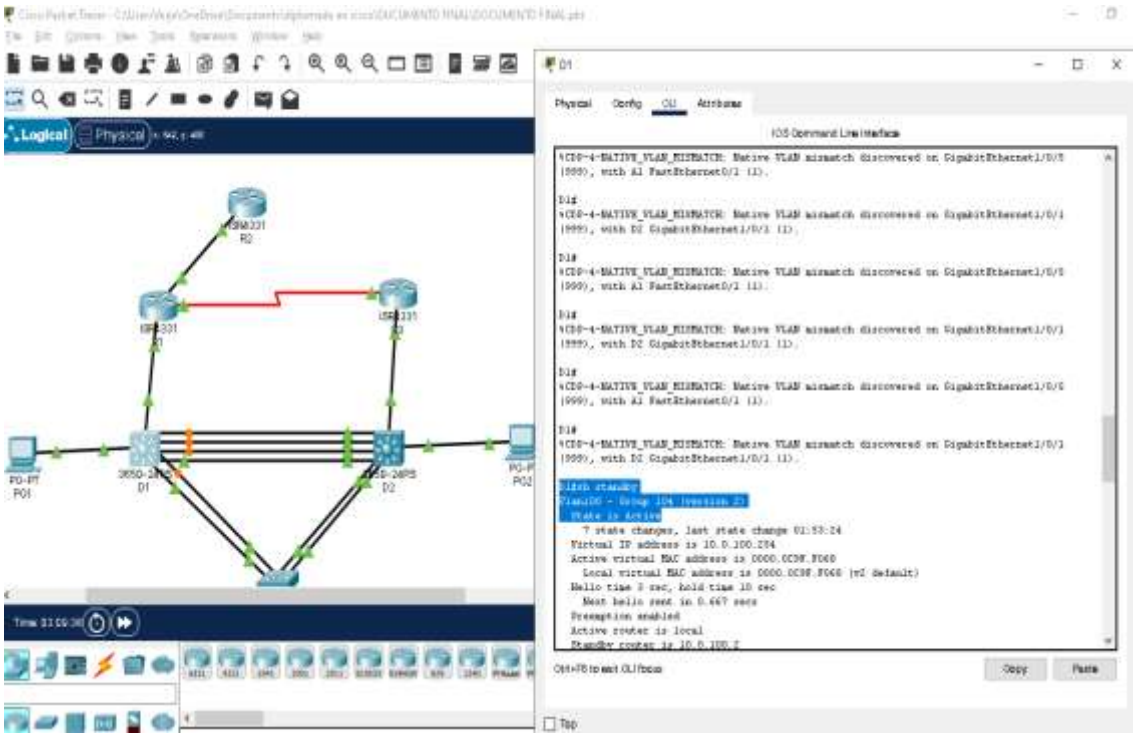
Asigne la dirección IP virtual usando ipv6 autoconfig.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 6 y decremente en 60.

Continuamos con los mismos pasos de configuración cambiando el grupo y la VLAN y establecemos prioridad

D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)# standby 126 priority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60

Se verifica la conectividad con el comando D1#sh standby

Imagen 19. Verificación tarea 4.3



Tarea 4.4

En D2, configure HSRPv2

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

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:
Asigne la dirección IP virtual 10.0.100.254.
Habilite la preferencia (preemption).

Rastree el objeto 4 y decremente en 60.

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.

Utilizamos los códigos del paso anterior cambiando la VLAN, la IP virtual y el grupo. Establecemos la prioridad 150:

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
D2(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.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Continuamos con la serie de códigos utilizados en el paso anterior cambiando la VLAN y la IP virtual en este paso no establecemos 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
```

A continuación copiamos el código, pero ahora se configura la ipv6

Configure IPv6 HSRP grupo 106 para la VLAN 100
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).
Rastree el objeto 6 para disminuir en 60.

```
D2(config-if)#standby 116 ipv6 autoconfig
 D2(config-if)# standby 116 priority 150
 D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60
```

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60

Continuamos con los códigos de configuración se cambia la VLAN y grupo:

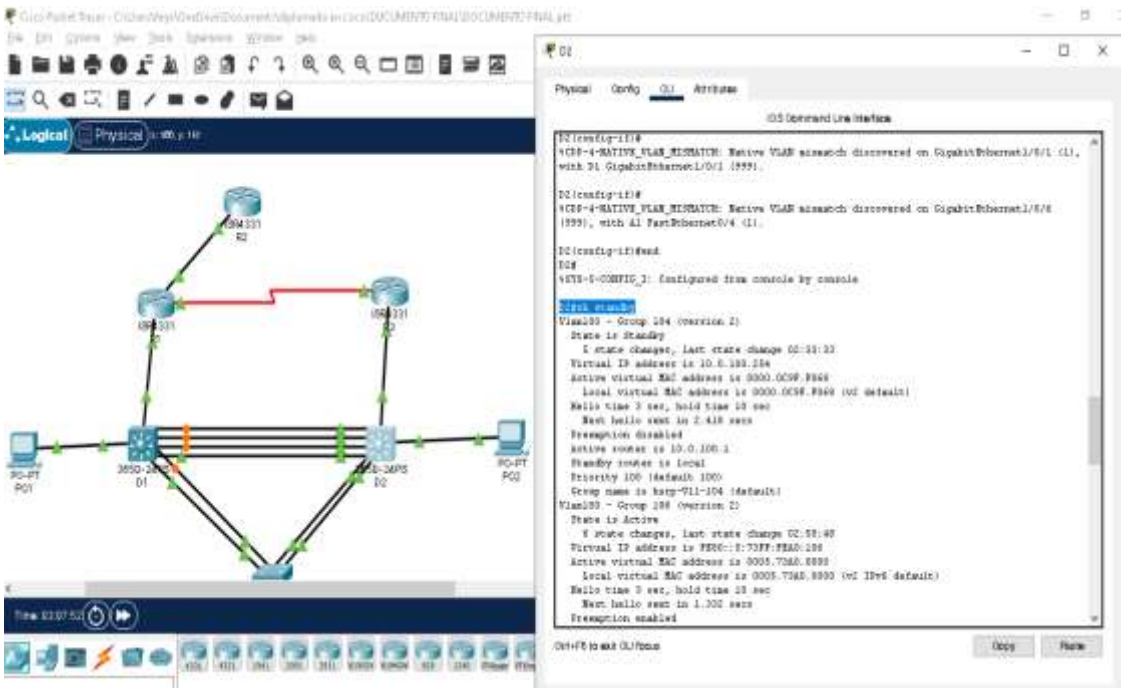
D2(config-if)#standby 126 ipv6 autoconfig

D2(config-if)# standby 126 preempt

D2(config-if)# standby 126 track 6 decrement 60

Verificamos con el comando D2#sh standby

Imagen 20. Verificación tarea 4.4



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:

Tabla 5. Configuración de seguridad

Tarea #	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: sadmin • Nivel de privilegio 15 • Contraseña: cisco12345cisco
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto

	lista de métodos de autenticación AAA	• Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
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, 5.2 y 5.3

En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

Con la contraseña **cisco12345cisco**

Detalles de la cuenta encriptada SCRYPT:
Nombre de usuario Local: sadmin
Nivel de privilegio 15
Contraseña: cisco12345cisco

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

Para esta configuración de seguridad se debe ingresar a cada dispositivo el código a continuación

R2>
R2>en / Se ingresa a modo privilegiado
R2#confi t / Se ingresa a configurar terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable password cisco12345cisco /Se asigna contraseña a modo privilegiado
R2(config)#service password-encryption / Se encripta la contraseña
R2(config)#exit / Se sale del modo configuración
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret level 15 cisco12345cisco / Se crea sesión privilegio 15
R2(config)#username sadmin privilege 15 secret cisco12345cisco / Se crea usuario y contraseña encriptada para el usuario.
R2(config)#end / Configuración de la consola

R1>en
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
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 el modelo AAA

R3>en
R3#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable password cisco12345cisco
R3(config)#service password-encryption
R3(config)#enable secret level 15 cisco12345cisco
R3(config)#username sadmin privilege 15 secret cisco12345cisco
R3(config)#aaa new-model

D1>en
D1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
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
D1(config)#

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

Tarea 5.4, 5.5, 5.6

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
Valide contra el grupo de servidores RADIUS
De lo contrario, utilice la base de datos local.

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

Configuramos para todos los dispositivos el siguiente código excepto R2

R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model / Llamamos el modelo a configurar
R1(config)#radius server RADIUS / Se indica el servidor a configurar Radius
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 /se asigna la dirección ip y puertos del servidor Radius

R1(config-radius-server)#key $trongPass / se asigna la contraseña $trongPass

R3#confi t
Enter configuration commands, one per line. End with CNTL/Z.
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
R3(config)#aaa authentication login default group radius local
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $trongPass 99
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local D2(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 $trongPass
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 $trongPass

A1(config-radius-server)#exit

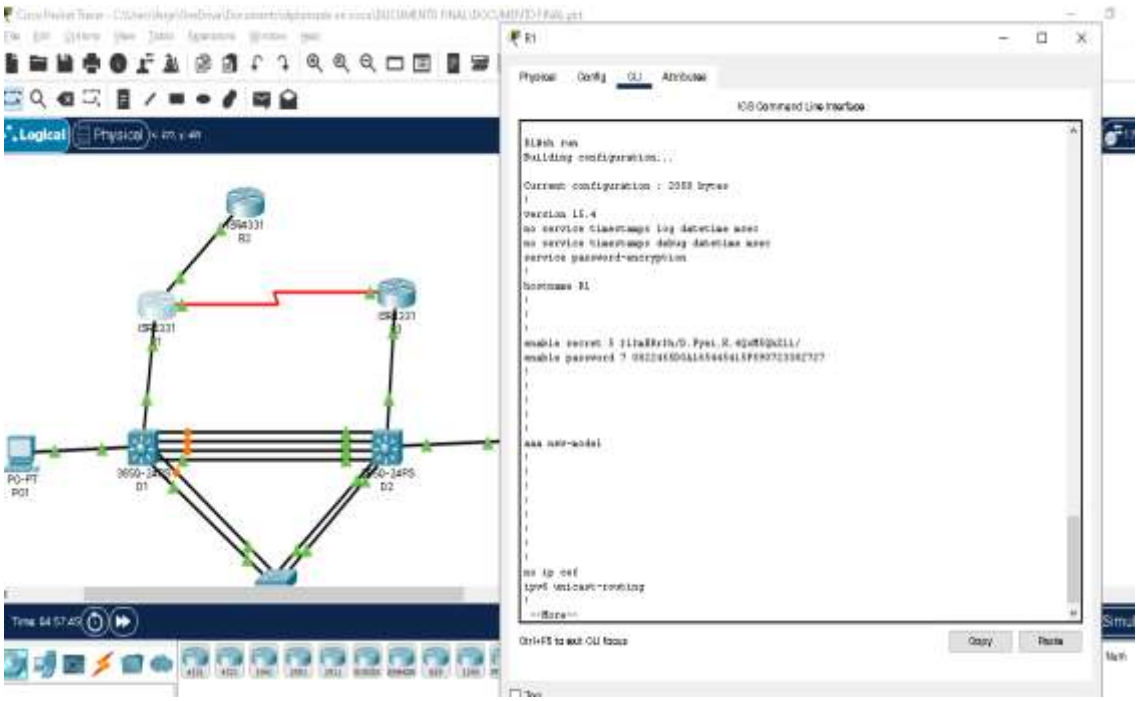
A1(config)#aaa authentication login default group radius local

A1(config)#end

Nota: En algunos dispositivos D1,D2,A1 no fue posible realizar la configuración ya que arroja error la configuración de packet tracer, pero son los códigos para utilizar en un escenario real no simulado

Verificamos la seguridad

Imagen 21. Verificación de seguridad



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:

Tabla 6. Configuración administración de red

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: • 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	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el community string en ENCORSA.

		• En R3, D1, y D2, habilite el envío de traps config y ospf. • En R1, habilite el envío de traps bgp, config, y ospf. • En A1, habilite el envío de traps config

Tarea 6.1

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

Para esto validamos en los dispositivos la hora configurada con el código:

R1#sh clock
*5:15:48.476 UTC Mon Mar 1 1993

R3#sh clock
*5:18:52.742 UTC Mon Mar 1 1993

Como se evidencia la hora no corresponde a la hora actual se configura con el código:
Procedemos a configurarla

R1#clock set 11:00:00 29 Nov 2021

Lo configuramos en todos los dispositivos

R2#clock set 11:03:00 29 Nov 2021

R3#clock set 11:04:00 29 Nov 2021

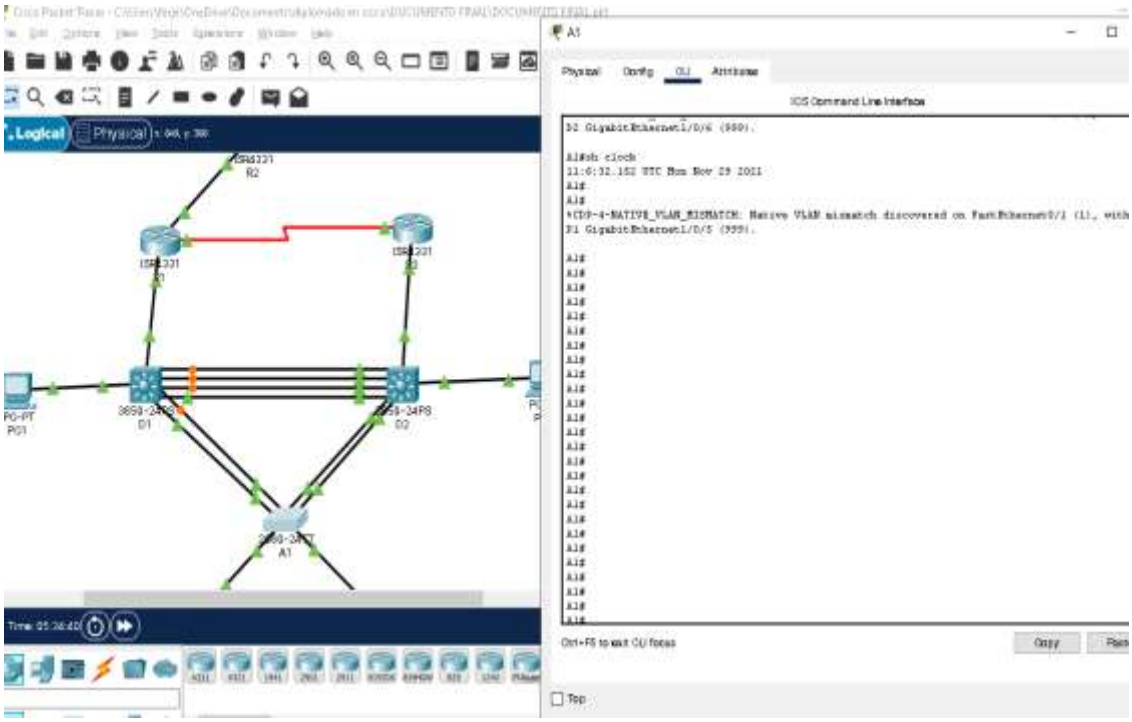
D1#clock set 11:06:00 29 Nov 2021

D2#clock set 11:08:00 29 Nov 2021

A1#clock set 11:05:00 29 Nov 2021

Verificamos la hora y fecha configuradas

Imagen 22. Verificación de hora y fecha



Tarea 6.2

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

Utilizaremos el siguiente comando

R2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3 /se configure NTP maestro en el nivel de estrato 3

Tareas 6.3, 6.4 y 6.5

Configure NTP de la siguiente manera:

R1 debe sincronizar con R2.
R3, D1 y A1 para sincronizar la hora con R1.
D2 para sincronizar la hora con R3.

Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

Especificaciones de SNMPv2:

Únicamente se usará SNMP en modo lectura (Read-Only).
Limite el acceso SNMP a la dirección IP de la PC1.
Configure el valor de contacto SNMP con su nombre.
Establezca el community string en ENCORSA.
En R3, D1, y D2, habilite el envío de traps config y ospf.
En R1, habilite el envío de traps bgp, config, y ospf.
En A1, habilite el envío de traps config.

Utilizaremos el siguiente código

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 103
R1(config)#ip access-list standard SNMP-NMS / se cinfigura SNMP lectura
R1(config-std-nacl)#permit host 10.0.100.5 / se declara límite de acceso
R1(config-std-nacl)#exit R1(config- snmp)#snmp-server contact Cisco ferneC / valor de contacto SNP R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS /se establece
R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA /se declara el host
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 él envió de traps osfp
R1(config- snmp)#end /se finaliza la configuración

Se configura el código anterior en los demás dispositivos

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 ferneyC
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 ferneyC
D1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config- snmp)#snmp-server ifindex persist
D1(config- snmp)#snmp-server enable traps config
D1(config- snmp)#snmp-server enable traps ospf

D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS 104
D2(config-std-nacl)#permit host 10.0.100.5
D2(config)#snmp-server contact Cisco ferneyC
D2(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
D2(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config- snmp)# snmp-server enable traps config
D2(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 ferneyC

A1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS

A1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA

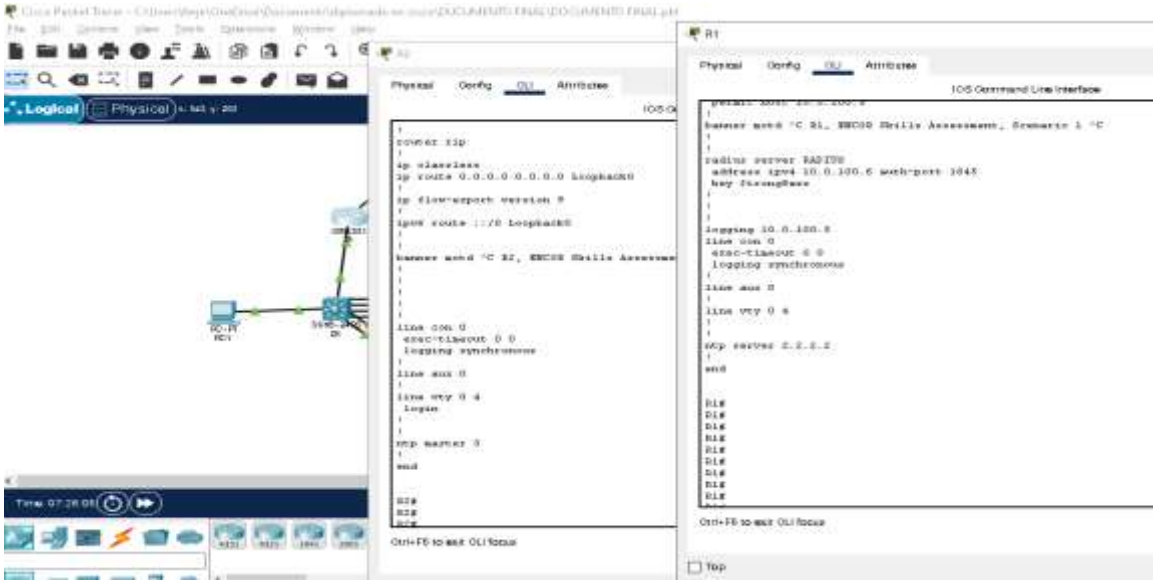
A1(config- snmp)#snmp-server ifindex persist

A1(config- snmp)#snmp-server enable traps config

A1(config- snmp)#snmp-server enable traps ospf

Nota: en los dispositivos configurados se relaciona la configuración correcta de comandos, pero packet tracer no funciona la simulación de snmp-server. A continuación, adjunto la verificación del mismo.

Imagen 23. Verificación de snmp-server



CONCLUSIONES

La realización de este documento final plasma los conocimientos adquiridos mediante las unidades del curso de profundización ciscoCCNP, y se pone en práctica mediante el escenario aquí previamente desarrollado brindando como resultado competencias significativas en áreas de las redes de comunicaciones y sus diversas aplicaciones y configuraciones.

Se resalta la practicidad del software de desarrollo como lo son packet tracer o GNS3 los cuales de forma didáctica permite la configuración de equipos con los mismos resultados de aprendizaje de una forma física con la ventaja de aprendizaje del error sin exponer los equipos al daño físico y observando el transito correcto de su comunicación y posible error en su mala configuración.

Mediante el desarrollo practico del escenario o ejercicios propuestos y realizados en los entornos y software de desarrollo como packet tracer, se obtienen habilidades para la correcta configuración de equipos de enrutamiento utilizando protocolos como el OSPF y demás comandos para su correcta configuración.

BIBLIOGRAFÍA

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **OSPF v3**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

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

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