DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

WINEN JAVIER MEJIA MEJIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

INGENIERÍA ELECTRÓNICA

ARMENIA

2022

DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

WINEN JAVIER MEJIA MEJIA

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

DIRECTOR:

JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

INGENIERÍA ELECTRÓNICA

ARMENIA

2022

NOTA DE ACEPTACION

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

ARMENIA, 17 de noviembre de 2022

AGRADECIMIENTOS

Tengo la satisfacción de poder agradecer a mi madre, por ser la fuerza impulsora para continuar día a día, su apoyo incondicional en cada etapa de mi formación profesional me permite hoy alcanzar una nueva meta, también dejo unas líneas a mi padre por estar siempre acompañándome desde la distancia como animador incansable y por ser un ejemplo como trabajador dedicado y honesto.

Para mis familiares, amigos y compañeros que siempre se han un preocupado por mí y han estado alentando este proceso educativo con “pequeñas” palabras y grandes gestos, un gracias infinito.

Por último, agradezco, a todos los tutores que participaron en mi proceso de aprendizaje y a todos los funcionarios UNAD que siempre estuvieron dispuestos al asesoramiento y guía para culminar de la mejor manera este logro personal.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: Es la tecnología que permite crear una LAN virtual (VLAN), que es una red superpuesta lógica que agrupa un subconjunto de dispositivos que comparten una LAN física, aislando el tráfico para cada grupo.

LACP: Protocolo de control de agregación de enlaces (Link Aggregation Control Protocol), LACP forma parte de una selección de IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automáticamente mediante el envío de paquetes LACP al peer.

RSTP: (Rapid spanning tree protocol) es un protocolo que detecta y evita bucles dentro de la red, gestionando enlaces redundantes, este fue desarrollado para mejorar el funcionamiento del protocolo STP. RSTP trae varias mejoras con respecto a STP, principalmente en lo que tiene que ver con los tiempos de convergencia, además mejora la ruta desde el switch que no es raíz al switch raíz, remplaza al puerto raíz cuando este entra en fallo, habilitando automáticamente el puerto alternativo

OSPF: Es un protocolo de enrutamiento que basa su funcionamiento en permitir elegir la ruta más corta disponible para la comunicación, esto se mantiene aun cuando se presenta un cambio físico en la topología de la red.

BGP: (Border Gateway Protocol) es un protocolo de puerta de enlace exterior (EGP) estandarizado diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos (AS). La información de enrutamiento del BGP incluye la ruta completa a cada destino. El BGP utiliza la información de enrutamiento para mantener una base de datos de información de accesibilidad de red, que intercambia con otros sistemas de la misma característica.

RESUMEN

En la actualidad las necesidades en cuanto a conectividad para el intercambio rápido y constante de información exigen el diseño de redes escalables y de conmutación con un cierto nivel de seguridad, por esto se hace necesario la implementación de tecnologías y uso de protocolos de conmutación mejorados que permitan comunicaciones efectivas a través de las redes de datos, haciendo estas más eficientes y estableciendo alternativas a problemas de interconectividad. Mediante el diplomado CCNP (Cisco Certified Network Professional) se ha logrado desarrolla en el futuro ingeniero la capacidad de diseñar, efectuar implementación, verificar funcionamiento optimo y solucionar los posibles problemas que se puedan presentar en las redes empresariales.

Durante el desarrollo del diplomado se utilizaron los softwares Packet Tracer y GNS3 que permiten simular los múltiples conceptos vistos, ofreciendo la posibilidad de realizar desde la configuración básica de router y swiches como la implementación de los protocolos específicos de enrutamiento como EIGRP, OSPF, BGP, HSRP versión 2, protocolos como NTP, implementación de VLANs y troncales, Spanning Tree, RSTP, LACP, etc.

ABSTRACT

At present, the needs in terms of connectivity for the rapid and constant exchange of information require the design of scalable and switching networks with a certain level of security, for this reason it is necessary to implement technologies and use of improved switching protocols that allow communications to through data networks, making them more efficient and establishing alternatives to interconnectivity problems. Through the CCNP (Cisco Certified Network Professional) diploma, future engineers have developed the ability to design, carry out implementation, verify optimal operation and solve possible problems that may arise in business networks.

During the development of the diploma, the Packet Tracer and GNS3 software was used, which allows simulating the multiple concepts seen, offering the possibility of performing from the basic configuration of the router and switches as well as the implementation of specific routing protocols such as EIGRP, OSPF,

BGP, HSRP version 2, protocols such as NTP, implementation of VLANs and trunks, Spanning Tree, RSTP, LACP, etc.

INTRODUCCION

El objetivo del presente informe es detallar el proceso de aprendizaje y las actividades realizadas durante el diplomado CCNP (Cisco Certified Network Professional), donde se ha logrado fortalecer las capacidades generales del profesional en redes de datos, tales como la habilidad de administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI y la arquitectura TCP/IP y la posibilidad de aplicar recursos y herramientas que permiten el soporte técnico de las redes de datos y el establecimiento de alternativas a problemas de conectividad.

También se han fortalecido los conocimientos necesarios para la implementación adecuada de niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de las redes empresariales, aplicando tanto destrezas de software como de hardware que permitan asegurar la información transferida frente a cualquier ataque que se pueda presentar desde el interior o exterior de la red.

Adicionalmente se trabajaron técnicas y estrategias para el diseño de redes que puedan ser escalables a futuro, buscando siempre optimizar el rendimiento de estas e incorporar adecuadamente la aplicación de tecnologías y protocolos como: VLAN, RSTP, Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP), Protocolos de enrutamiento como EIGRP, OSPF, BGP, etc.

DESARROLLO

SCENARIO 1

Next is the configuration of the network so that there is full end-to-end accessibility, so that the hosts have reliable default gateway support, and so that the management protocols are operational within the company network. The routers used in the labs are Cisco 7200 routers. The switches used are Cisco Catalyst L2 switches.

Resources used

3 routers (Cisco 7200).

3 switches (Cisco IOU L2).

4 PCs (VPCS of GNS3)

Topology

Figure 1. Network topology.

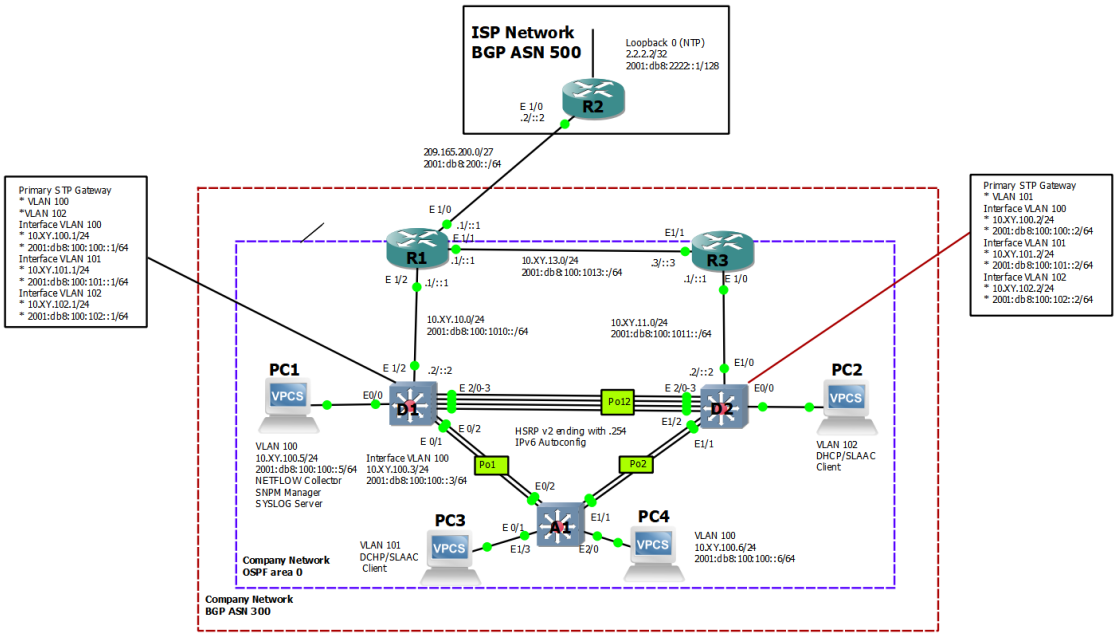


Table 1. Addressing Table.

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.48.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10. 48.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	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	E1/0	10.48.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.48.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.48.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.48.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.48.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.48.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.48.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.48.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.48.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.48.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.48.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.48.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.48.100.6/24	2001:db8:100:100::6/64	EUI-64

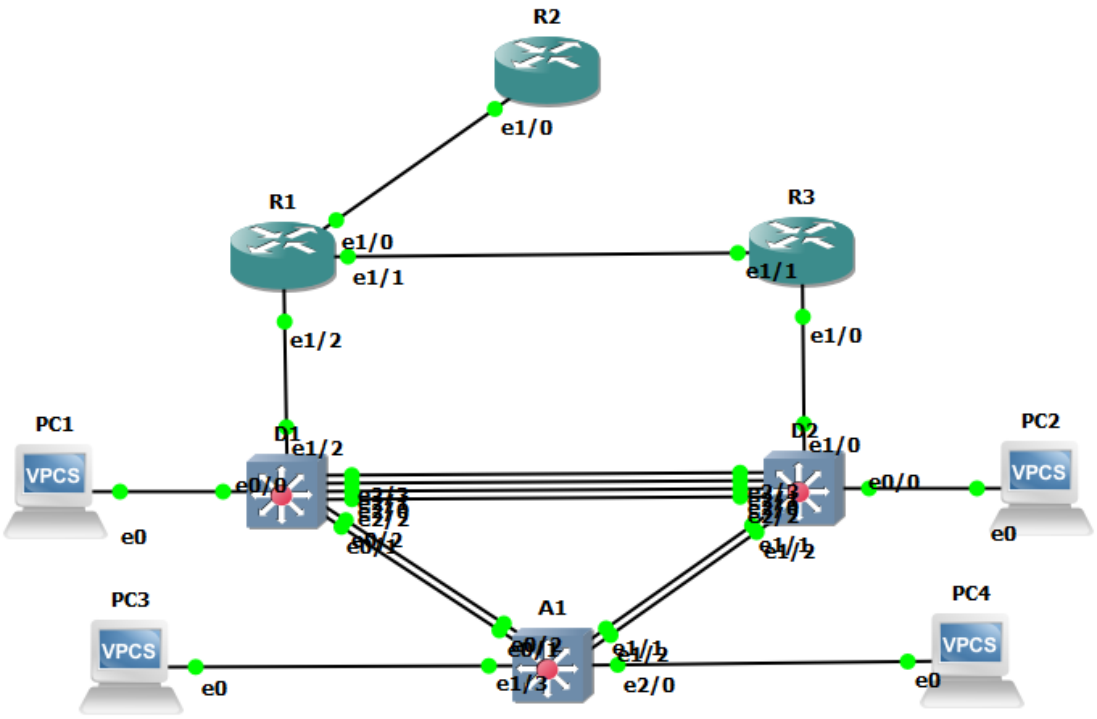
Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

The network topology configuration is done and the basic settings and interface addressing have been applied.

Step 1: Cable the network as shown in the topology.

The network is wired as shown in the topology the devices were connected as shown in the topology diagram.

Figure 2. Network topology implemented in GNS3.



Step 2: Configure basic settings for each device.

Global configuration mode was entered through the console to apply the required basic settings. The configuration codes used for each device are described below.

Router R1

R1#config terminal

R1(config)#hostname R1

R1(config)#ipv6 unicast-routing

R1(config)#no ip domain lookup

R1(config)#banner motd # R1, ENCOR Skills Assessment#

R1(config)#line con 0

R1(config-line)# exec-timeout 0 0

R1(config-line)# logging synchronous

R1(config-line)# exit

R1(config)#interface e1/0

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 e1/2

R1(config-if)# ip address 10.48.10.1 255.255.255.0

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 e1/1

R1(config-if)# ip address 10.48.13.1 255.255.255.0

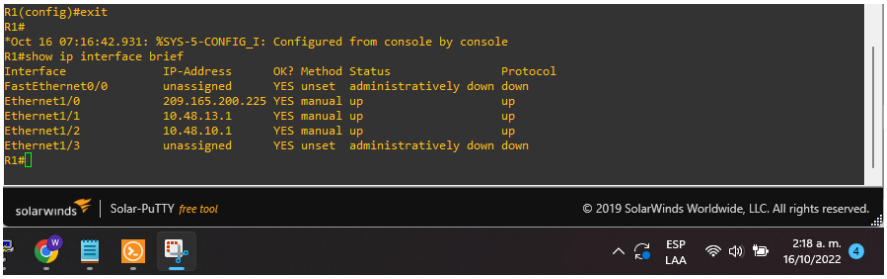
R1(config-if)# ipv6 address fe80::1:3 link-local

R1(config-if)# ipv6 address 2001:db8:100:1013::1/64

R1(config-if)# no shutdown

R1(config-if)# exit

Figure 3. Command "show ip interface brief" R1.



Router 2

R2(config)#hostname R2

R2(config)#ipv6 unicast-routing

R2(config)#no ip domain lookup

R2(config)#banner motd # R2, ENCOR Skills Assessment#

R2(config)#line con 0

R2(config-line)# exec-timeout 0 0

R2(config-line)# logging synchronous

R2(config-line)#exit

R2(config)#interface e1/0

R2(config-if)# ip address 209.165.200.226 255.255.255.224

R2(config-if)# ipv6 address fe80::2:1 link-local

R2(config-if)# ipv6 address 2001:db8:200::2/64

R2(config-if)# no shutdown

R2(config-if)# exit

R2(config)#interface Loopback 0

R2(config-if)# ip address 2.2.2.2 255.255.255.255

R2(config-if)# ipv6 address fe80::2:3 link-local

R2(config-if)# ipv6 address 2001:db8:2222::1/128

R2(config-if)# no shutdown

R2(config-if)# exit

**Oct 16 07:23:31.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up*

R2(config-if)# exit

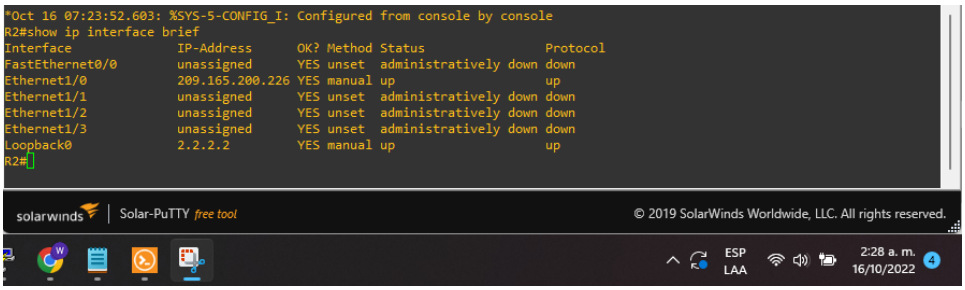
**Oct 16 07:23:33.095: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up*

**Oct 16 07:23:34.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up*

R2(config-if)# exit

R2(config)#exit

Figure 4. Command "show ip interface brief" R2.



Router 3

R3(config)#hostname R3

R3(config)#ipv6 unicast-routing

R3(config)#no ip domain lookup

R3(config)#banner motd # R3, ENCOR Skills Assessment#

R3(config)#line con 0

R3(config-line)# exec-timeout 0 0

R3(config-line)# logging synchronous

R3(config-line)# exit

R3(config)#interface e1/0

R3(config-if)# ip address 10.48.11.1 255.255.255.0

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 e1/1

R3(config-if)# ip address 10.48.13.3 255.255.255.0

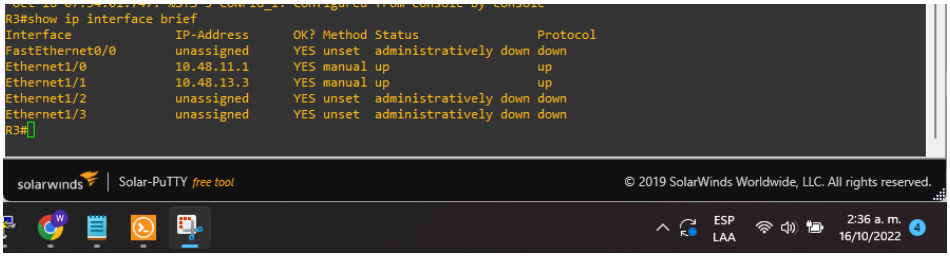
R3(config-if)# ipv6 address fe80::3:3 link-local

R3(config-if)# ipv6 address 2001:db8:100:1010::2/64

R3(config-if)# no shutdown

R3(config-if)# exit

Figure 5. Command "show ip interface brief" R3.



Switch D1

D1(config)#hostname D1

D1(config)#ip routing

D1(config)#ipv6 unicast-routing

D1(config)#no ip domain lookup

D1(config)#banner motd # D1, ENCOR Skills Assessment#

D1(config)#line con 0

D1(config-line)# exec-timeout 0 0

D1(config-line)# logging synchronous

D1(config-line)# exit

D1(config)#vlan 100

D1(config-vlan)# name Management

D1(config-vlan)# exit

D1(config)#vlan 101

D1(config-vlan)# name UserGroupA

D1(config-vlan)# exit

D1(config)#vlan 102

D1(config-vlan)# name UserGroupB

D1(config-vlan)# exit

D1(config)#vlan 999

D1(config-vlan)# name NATIVE

D1(config-vlan)# exit

D1(config)#interface e1/2

D1(config-if)# no switchport

D1(config-if)# ip address 10.48.10.2 255.255.255.0

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 10.48.100.1 255.255.255.0

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 10.48.101.1 255.255.255.0

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 10.48.102.1 255.255.255.0

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 10.48.101.1 10.48.101.109

D1(config)#ip dhcp excluded-address 10.48.101.141 10.48.101.254

D1(config)#ip dhcp excluded-address 10.48.102.1 10.48.102.109

D1(config)#ip dhcp excluded-address 10.48.102.141 10.48.102.254

D1(config)#ip dhcp pool VLAN-101

D1(dhcp-config)# network 10.48.101.0 255.255.255.0

D1(dhcp-config)# default-router 10.48.101.254

D1(dhcp-config)# exit

D1(config)#ip dhcp pool VLAN-102

D1(dhcp-config)# network 10.48.102.0 255.255.255.0

D1(dhcp-config)# default-router 10.48.102.254

D1(dhcp-config)# exit

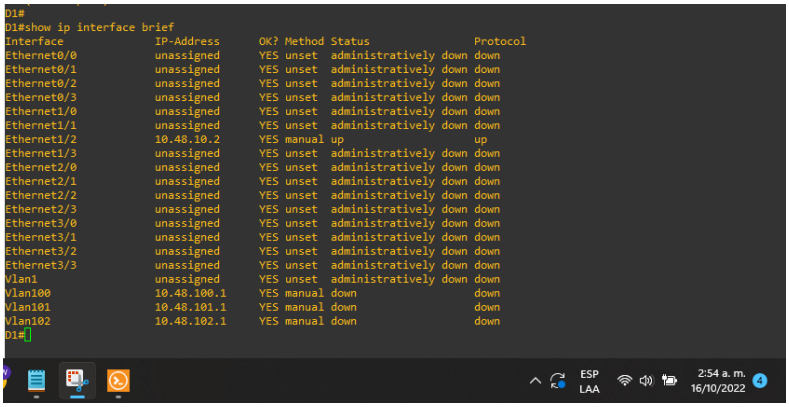
D1(config)#interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3

D1(config-if-range)# shutdown

D1(config-if-range)# exit

D1(config)#

Figure 6. Command "show ip interface brief" Switch D1.



Switch D2

D2#CONFIG TERMINAL

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

D2(config)#hostname D2

D2(config)#ip routing

D2(config)#ipv6 unicast-routing

D2(config)#no ip domain lookup

D2(config)#banner motd # D2, ENCOR Skills Assessment#

D2(config)#line con 0

D2(config-line)# exec-timeout 0 0

D2(config-line)# logging synchronous

D2(config-line)# exit

D2(config)#vlan 100

D2(config-vlan)# name Management

D2(config-vlan)# exit

D2(config)#vlan 101

D2(config-vlan)# name UserGroupA

D2(config-vlan)# exit

D2(config)#vlan 102

D2(config-vlan)# name UserGroupB

D2(config-vlan)# exit

D2(config)#vlan 999

D2(config-vlan)# name NATIVE

D2(config-vlan)# exit

D2(config)#interface e1/0

D2(config-if)# no switchport

D2(config-if)# ip address 10.48.11.2 255.255.255.0

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 10.48.100.2 255.255.255.0

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 10.48.101.2 255.255.255.0

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 10.48.102.2 255.255.255.0

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 10.48.101.1 10.48.101.209

D2(config)#ip dhcp excluded-address 10.48.101.241 10.48.101.254

D2(config)#ip dhcp excluded-address 10.48.102.1 10.48.102.209

D2(config)#ip dhcp excluded-address 10.48.102.241 10.48.102.254

D2(config)#ip dhcp pool VLAN-101

D2(dhcp-config)# network 10.48.101.0 255.255.255.0

D2(dhcp-config)# default-router 48.0.101.254

D2(dhcp-config)# exit

D2(config)#ip dhcp pool VLAN-102

D2(dhcp-config)# network 10.48.102.0 255.255.255.0

D2(dhcp-config)# default-router 10.93.102.254

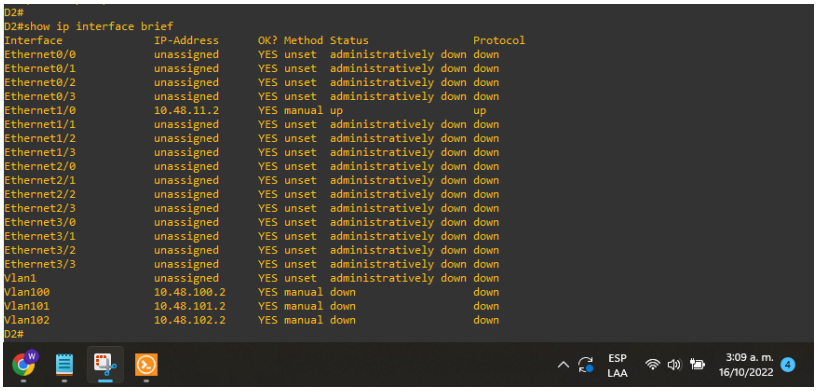
D2(dhcp-config)# exit

D2(config)#interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3

D2(config-if-range)# shutdown

D2(config-if-range)# exit

Figure 7. Command "show ip interface brief" Switch D2.



Switch A1

A1(config)#

A1(config)#hostname A1

A1(config)#no ip domain lookup

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

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 10.48.100.3 255.255.255.0

A1(config-if)# ipv6 address fe80::a1:1 link-local

A1(config-if)# ipv6 address 2001:db8:100:100::3/64

A1(config-if)# no shutdown

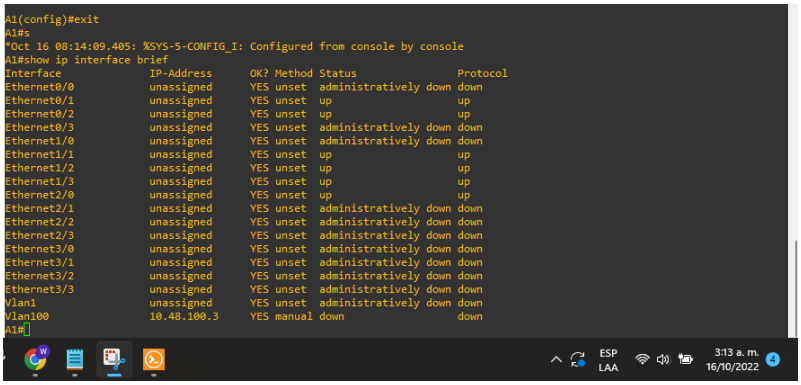
A1(config-if)# exit

A1(config)#interface range e0/0,e0/3,e1/0,e2/1-3,e3/0-3

A1(config-if-range)# shutdown

A1(config-if-range)# exit

Figure 8. Command “show ip interface brief” Switch A1.



Save the running configuration to startup-config on all devices.

R/ apply the command (copy running-config startup-config) to all devices copy running-config startup-config

Part 2: Configure the Layer 2 Network and Host Support

In this part, the complement to the configuration of the layer 2 network and configuration of the basic host support is developed. all switches are configured to be able to communicate with each other, for PC2 and PC3 DHCP and SLAAC addressing are enabled, for PC1 and PC2 static addressing is assigned.

Table 2. Implemented Configuration Tasks

Task#	***Task***	***Specification***	***Points***
2.1	On all switches, configure IEEE 802.1Q trunk interfaces on interconnecting switch links	Enable 802.1Q trunk links between: • *D1 and D2* • *D1 and A1* • *D2 and A1*	*6*
2.2	*On all switches, change the native VLAN on trunk links.*	*Use VLAN 999 as the native VLAN.*	*6*
2.3	*On all switches, enable the Rapid Spanning-Tree Protocol.*	*Use Rapid Spanning Tree.*	*3*
2.4	*On D1 and D2, configure the appropriate RSTP root bridges based on the information in the topology diagram.* *D1 and D2 must provide backup in case of root bridge failure.*	*Configure D1 and D2 as root for the appropriate VLANs with mutually supporting priorities in case of switch failure.*	*2*
2.5	*On all switches, create LACP EtherChannels as shown in the topology diagram.*	*Use the following channel numbers:* • *D1 to D2 – Port channel 12* • *D1 to A1 – Port channel 1* • *D2 to A1 – Port channel 2*	*3*

Task#	Task	Specification	Points
2.6	*On all switches, configure host access ports connecting to PC1, PC2, PC3, and PC4.*	*Configure access ports with appropriate VLAN settings as shown in the topology diagram.* *Host ports should transition immediately to forwarding state.*	*4*
2.7	*Verify IPv4 DHCP services.*	*PC2 and PC3 are DHCP clients and should be receiving valid IPv4 addresses.*	*1*
2.8	*Verify local LAN connectivity.*	PC1 should successfully ping: • *D1: 10.48.100.1* • *D2: 10.48.100.2* • *PC4: 10.48.100.6* PC2 should successfully ping: • *D1: 10.48.102.1* • *D2: 10.48.102.2* PC3 should successfully ping: • *D1: 10.48.101.1* • *D2: 10.48.101.2* PC4 should successfully ping: • *D1: 10.48.100.1* • *D2: 10.48.100.2* • *PC1: 10.48.100.5*	*1*

Task 2.1: Enable 802.1Q trunk links between (D1 and D2; D1 and A1; D2 and A1)

SW D1

config terminal

interface range e2/0-3,e0/1-2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

SW D2

config terminal

interface range e2/0-3,e1/1-2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

SW A1

config terminal

interface range e0/1-2,e1/1-2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

Task 2.2: VLAN 999 as the native VLAN

SW D1

config terminal
interface range e2/0-3,e0/1-2
switchport trunk native vlan 999
exit

SW D2

config terminal
interface range e2/0-3,e1/1-2
switchport trunk native vlan 999
exit

SW A1

config terminal
interface range e0/1-2,e1/1-2
switchport trunk native vlan 999
exit

Task 2.3: Use Rapid Spanning Tree and Task 2.4 Configure D1 and D2 as root for the appropriate VLANs with mutually supporting priorities in case of switch failure.

SW D1

config term

spanning-tree mode rapid-pvst

spanning-tree vlan 100,102 root primary

spanning-tree vlan 101 root secondary

exit

SW D2

config terminal

spanning-tree mode rapid-pvst

spanning-tree vlan 101 root primary

spanning-tree vlan 100,102 root secondary

exit

SW A1

config termial

spanning-tree mode rapid-pvst

exit

Task 2.5: create LACP EtherChannels, Use the following channel numbers, D1 to D2 – Port channel 12, D1 to A1 – Port channel 1, D2 to A1 – Port channel 2

SW D1

config term
interface range e2/0-3
channel-group 12 mode active
no shutdown
exit
interface range e0/1-2
channel-group 1 mode active
no shutdown
exit

SW D2

config terminal
interface range e2/0-3
channel-group 12 mode active
no shutdown
exit
interface range e1/1-2
channel-group 2 mode active
no shutdown
exit

SW A1

config terminal
interface range e1/1-2
channel-group 2 mode active
no shutdown
exit
interface range e0/1-2
channel-group 1 mode active
no shutdown
exit

Task 2.6: configure host access ports connecting to PC1, PC2, PC3, and PC4

SW D1

config terminal
interface e0/0
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit

SW D2

Config terminal
interface e0/0
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit

SW A1

Config terminal
interface e1/3
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface e2/0
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit

Task 2.7: Verify IPv4 DHCP services PC2 and PC3

Figure 9. DHCP PC2.

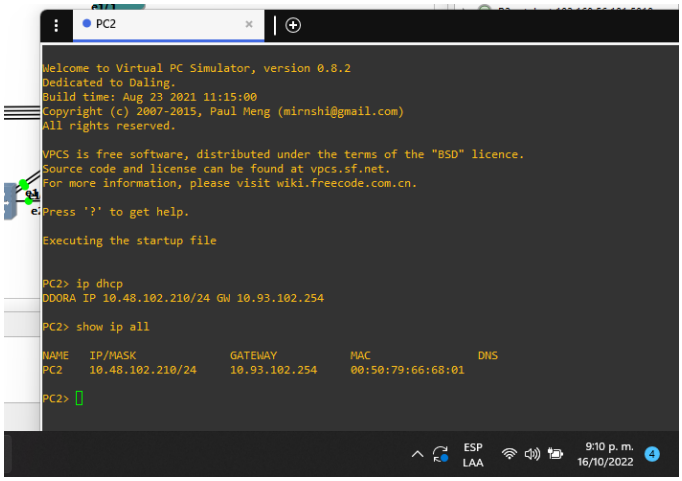
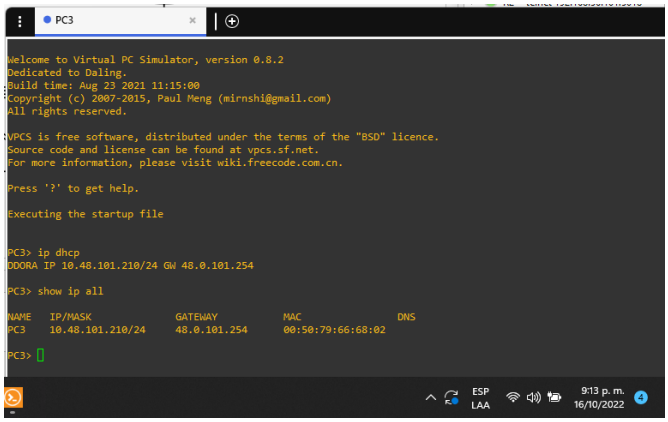


Figure 10. DHCP PC3.



PC2 and PC3 are receiving the DHCP service, it is evident that valid IPv4 addresses are obtained

Task 2.8: Verify local LAN connectivity.

Figure 11. Ping from PC1.

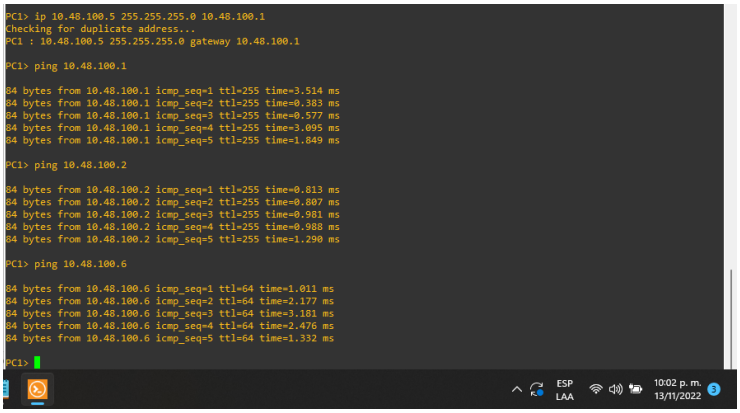


Figure 12. Ping from PC2.

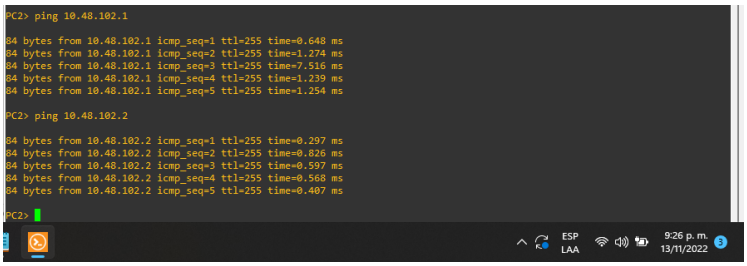


Figure 13. Ping from PC3.

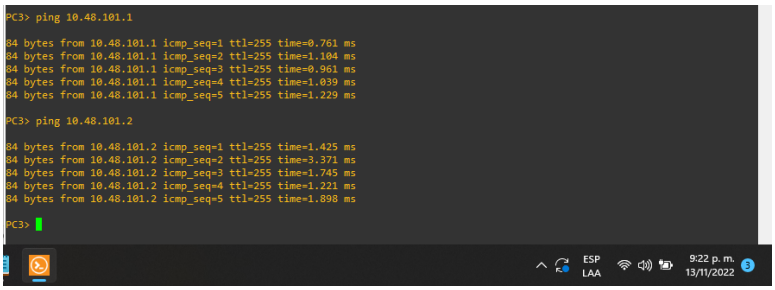
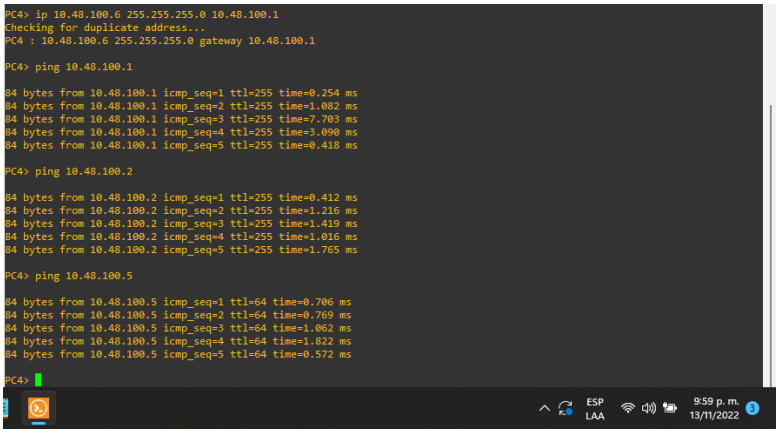


Figure 13. Ping from PC4.



SCENARIO 2*:* Continuation of the Scenario 1

Part 3: Configure Routing Protocols

In this part, the configurations required to activate the IPv4 and IPv6 routing protocols were made, so that the network is completely convergent.

Table 3. Configuration Tasks for part 3

Task#	***Task***	***Specification***	***Points***
3.1	*On the "Company Network" (i.e., R1, R3, D1, and D2), configure single-area OSPFv2 in area 0.*	Use OSPF Process ID **4** and assign the following router-IDs: • *R1: 0.0.4.1* • *R3: 0.0.4.3* • *D1: 0.0.4.131* • *D2: 0.0.4.132* On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0. • *On R1, do not advertise the R1 – R2 network.* • *On R1, propagate a default route. Note that the default route will be provided by BGP.* Disable OSPFv2 advertisements on: • *D1: All interfaces except E1/2* • *D2: All interfaces except E1/0*	*8*

Task#	Task	Specification	Points
3.2	*On the "Company Network" (i.e., R1, R3, D1, and D2), configure classic single-area OSPFv3 in area 0.*	Use OSPF Process ID **6** and assign the following router-IDs: • *R1: 0.0.6.1* • *R3: 0.0.6.3* • *D1: 0.0.6.131* • *D2: 0.0.6.132* On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0. • *On R1, do not advertise the R1 – R2 network.* • *On R1, propagate a default route. Note that the default route will be provided by BGP.* Disable OSPFv3 advertisements on: • *D1: All interfaces except E1/2* • *D2: All interfaces except E1/0*	*8*

Task#	Task	Specification	Points
3.3	*On R2 in the "ISP Network", configure MP-BGP.*	*Configure two default static routes via interface Loopback 0:* • *An IPv4 default static route.* • *An IPv6 default static route.* *Configure R2 in BGP ASN **500** and use the router-id 2.2.2.2.* *Configure and enable an IPv4 and IPv6 neighbor relationship with R1 in ASN 300.* *In IPv4 address family, advertise:* • *The Loopback 0 IPv4 network (/32).* • *The default route (0.0.0.0/0).* *In IPv6 address family, advertise:* • *The Loopback 0 IPv4 network (/128).* • *The default route (::/0).*	*4*

Task#	Task	Specification	Points
3.4	*On R1 in the "ISP Network", configure MP-BGP.*	Configure two static summary routes to interface Null 0: • *A summary IPv4 route for 10.48.0.0/8.* • *A summary IPv6 route for 2001:db8:100::/48.* Configure R1 in BGP ASN **300** and use the router-id 1.1.1.1. Configure an IPv4 and IPv6 neighbor relationship with R2 in ASN 500. In IPv4 address family: • *Disable the IPv6 neighbor relationship.* • *Enable the IPv4 neighbor relationship.* • *Advertise the 10.48.0.0/8 network.* In IPv6 address family: • *Disable the IPv4 neighbor relationship.* • *Enable the IPv6 neighbor relationship.* • *Advertise the 2001:db8:100::/48 network.*	*4*

***Task* 3.1*: C*onfig single-area OSPFv2 in area 0 *o*n the R1, R3, D1, and D2**

Router R1

config terminal

router ospf 4

router-id 0.0.4.1

network 10.48.10.0 0.0.0.255 area 0

network 10.48.13.0 0.0.0.255 area 0

default-information originate

exit

Router R3

router ospf 4

router-id 0.0.4.3

network 10.48.11.0 0.0.0.255 area 0

network 10.48.13.0 0.0.0.255 area 0

exit

SW D1

router ospf 4

router-id 0.0.4.131

network 10.48.100.0 0.0.0.255 area 0

network 10.48.101.0 0.0.0.255 area 0

network 10.48.102.0 0.0.0.255 area 0

network 10.48.10.0 0.0.0.255 area 0

passive-interface default

no passive-interface e1/2

exit

SW D2

router ospf 4

router-id 0.0.4.132

network 10.48.11.0 0.0.0.255 area 0

network 10.48.100.0 0.0.0.255 area 0

network 10.48.101.0 0.0.0.255 area 0

network 10.48.102.0 0.0.0.255 area 0

passive-interface default

no passive-interface e1/0

exit

***Task* 3.2*: C*onfig classic single-area OSPFv3 in area 0 *o*n the R1, R3, D1, and D2**

Router R1

ipv6 router ospf 6

router-id 0.0.6.1

default-information originate

exit

interface e1/2

ipv6 ospf 6 area 0

exit

interface e1/1

```
ipv6 ospf 6 area 0
exit
```

Router R3

```
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
exit
```

SW D1

```
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e1/2
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
```

```
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

SW D2

```
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface e1/0
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Figure 14. Config OSFPv2 and OSFPv3 in area 0 for R3.

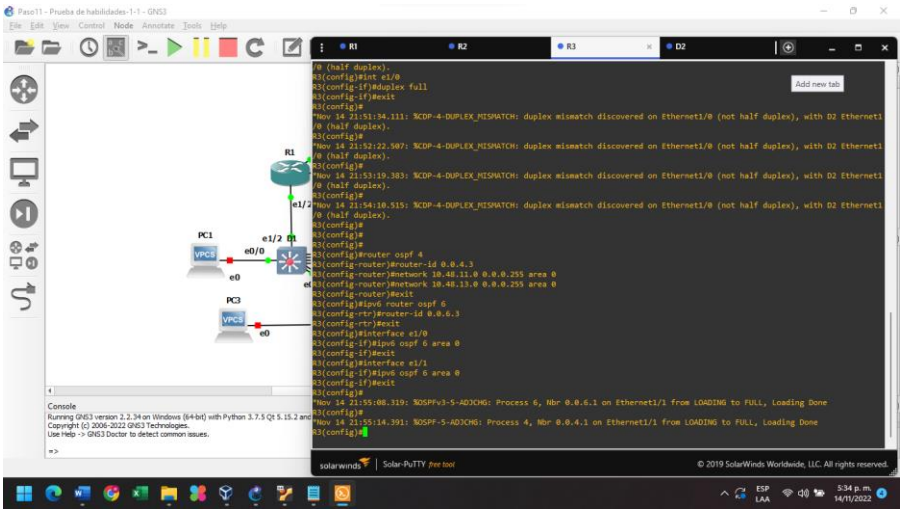
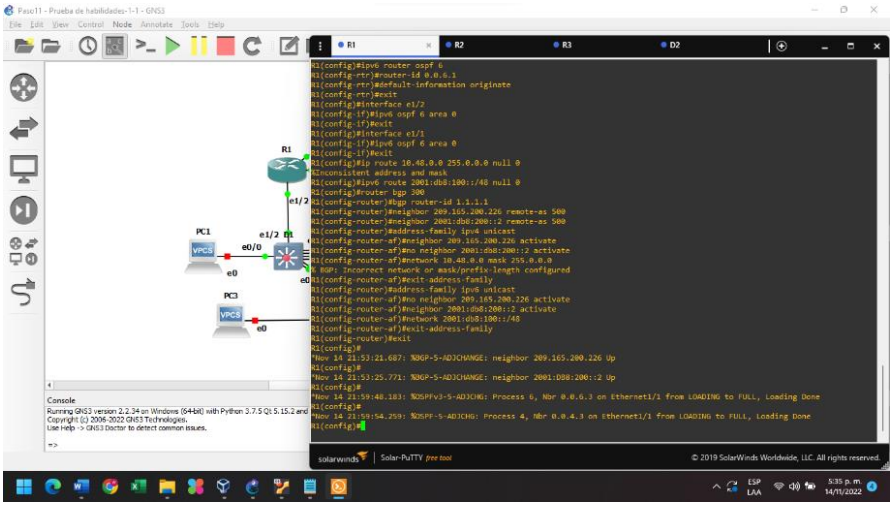


Figure 15. Config OSFPv2 and OSFPv3 in area 0 for R1.

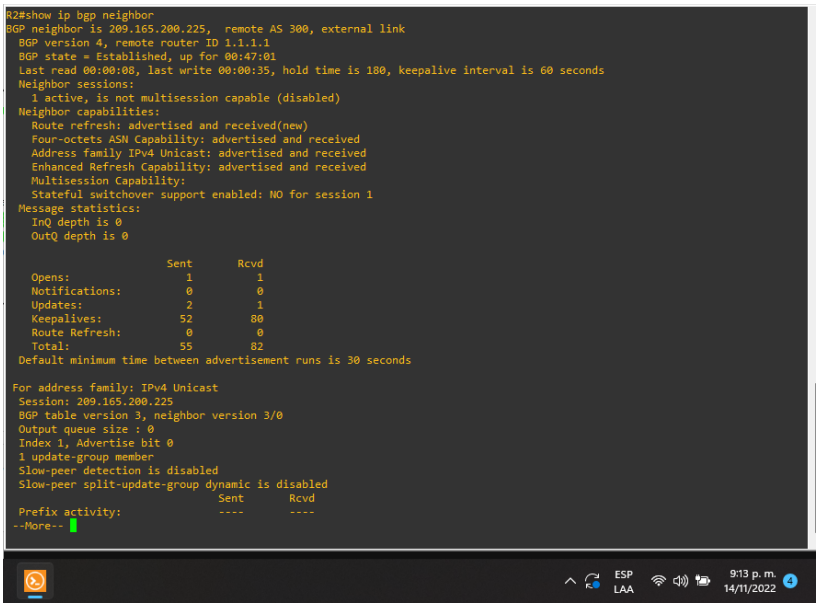


Task 3.3: Config MP-BGP on R2 in the “ISP Network”

Router R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::1/128
network ::/0
exit-address-family
```

Figure 16. "show ip bgp neighbor" command to verify on R2



Task 3.4: Config MP-BGP on R1 in the “ISP Network”

Router R1

ip route 10.48.0.0 255.0.0.0 null 0

ipv6 route 2001:db8:100::/48 null 0

router bgp 300

bgp router-id 1.1.1.1

neighbor 209.165.200.226 remote-as 500

neighbor 2001:db8:200::2 remote-as 500

address-family ipv4 unicast

neighbor 209.165.200.226 activate

no neighbor 2001:db8:200::2 activate

network 10.48.0.0 mask 255.0.0.0

exit-address-family

address-family ipv6 unicast

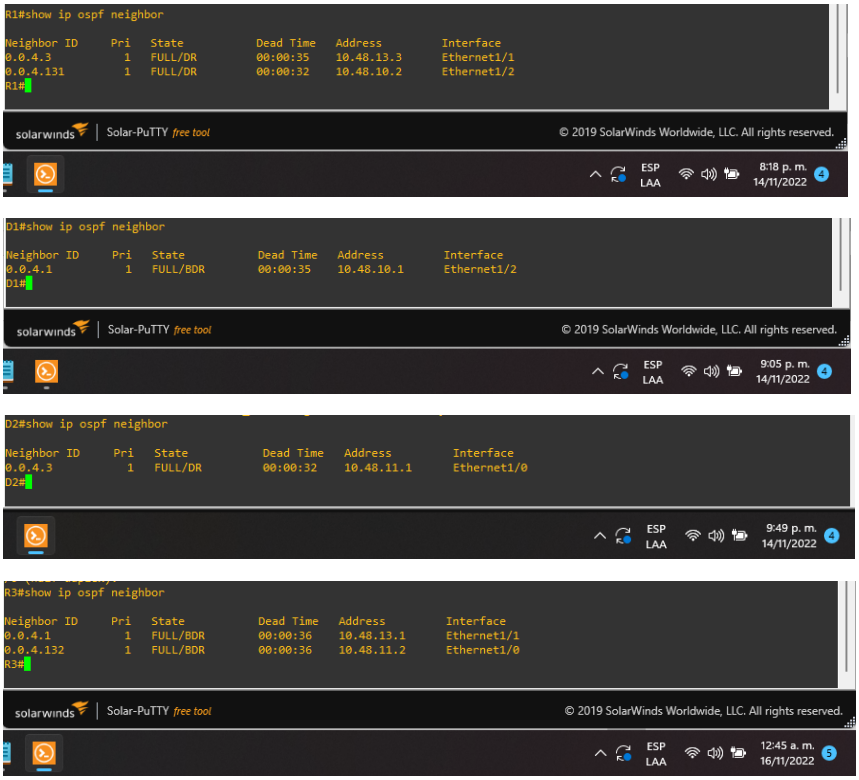
no neighbor 209.165.200.226 activate

neighbor 2001:db8:200::2 activate

network 2001:db8:100::/48

exit-address-family

Figure 17. "show ip ospf neighbor" command to verify correct configuration on R1, R3, D1 and D2.



Part 4: Configure First Hop Redundancy

This part applies the settings to enable HSRP version 2 which provides first hop redundancy for hosts in enterprise networks.

Table 4. Implemented Configuration for Tasks part 4

Task#	***Task***	***Specification***	***Points***
4.1	*On D1, create IP SLAs that test the reachability of R1 interface E1/2.*	*Create two IP SLAs.* • *Use SLA number **4** for IPv4.* • *Use SLA number **6** for IPv6.* *The IP SLAs will test availability of R1 E1/2 interface every 5 seconds.* *Schedule the SLA for immediate implementation with no end time.* *Create an IP SLA object for IP SLA 4 and one for IP SLA 6.* • *Use track number **4** for IP SLA 4.* • *Use track number **6** for IP SLA 6.* *The tracked objects should notify D1 if the IP SLA state changes from down to up after 10 seconds, or from up to down after 15 seconds.*	*2*

Task#	Task	Specification	Points
4.2	*On D2, create IP SLAs that test the reachability of R3 interface E1/0.*	*Create two IP SLAs.* • *Use SLA number **4** for IPv4.* • *Use SLA number **6** for IPv6.* *The IP SLAs will test availability of R3 E1/0 interface every 5 seconds.* *Schedule the SLA for immediate implementation with no end time.* *Create an IP SLA object for IP SLA 4 and one for IP SLA 6.* • *Use track number **4** for IP SLA 4.* • *Use track number **6** for IP SLA 6.* *The tracked objects should notify D1 if the IP SLA state changes from down to up after 10 seconds, or from up to down after 15 seconds.*	*2*

Task#	Task	Specification	Points
4.3	*On D1, configure HSRPv2.*	D1 is the primary router for VLANs 100 and 102; therefore, their priority will also be changed to 150. Configure HSRP version 2. *Configure IPv4 HSRP group **104** for VLAN 100:* • *Assign the virtual IP address **10. 48.100.254**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 4 and decrement by 60.* Configure IPv4 HSRP group **114** for VLAN 101: • *Assign the virtual IP address **10. 48.101.254**.* • *Enable preemption.* • *Track object 4 to decrement by 60.* Configure IPv4 HSRP group **124** for VLAN 102: • *Assign the virtual IP address **10. 48.102.254**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 4 to decrement by 60.* Configure IPv6 HSRP group **106** for VLAN 100: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 6 and decrement by 60.* Configure IPv6 HSRP group **116** for VLAN 101: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Enable preemption.* • *Track object 6 and decrement by 60.* Configure IPv6 HSRP group **126** for VLAN 102: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 6 and decrement by 60.*	*8*

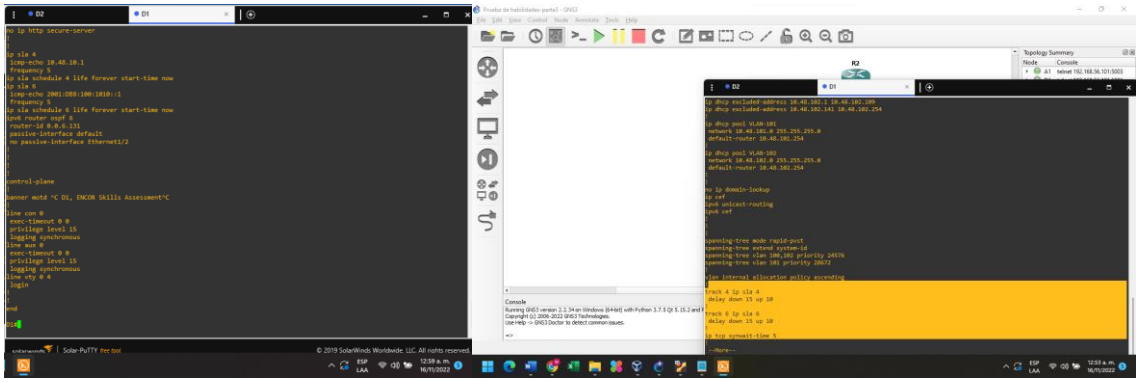
Task#	Task	Specification	Points
	On D2, configure HSRPv2.	D2 is the primary router for VLAN 101; therefore, the priority will also be changed to 150. Configure HSRP version 2. Configure IPv4 HSRP group **104** for VLAN 100: • *Assign the virtual IP address **10. 48.100.254**.* • *Enable preemption.* • *Track object 4 and decrement by 60.* Configure IPv4 HSRP group **114** for VLAN 101: • *Assign the virtual IP address **10. 48.101.254**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 4 to decrement by 60.* Configure IPv4 HSRP group **124** for VLAN 102: • *Assign the virtual IP address **10. 48.102.254**.* • *Enable preemption.* • *Track object 4 to decrement by 60.* Configure IPv6 HSRP group **106** for VLAN 100: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Enable preemption.* • *Track object 6 and decrement by 60.* Configure IPv6 HSRP group **116** for VLAN 101: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Set the group priority to **150**.* • *Enable preemption.* • *Track object 6 and decrement by 60.* Configure IPv6 HSRP group **126** for VLAN 102: • *Assign the virtual IP address using **ipv6 autoconfig**.* • *Enable preemption.* • *Track object 6 and decrement by 60.*	

Task 4.1: On D1, create IP SLAs that test the reachability of R1 interface E1/2.

SW D1

```
ip sla 4
icmp-echo 10.48.10.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay up 10 down 15
exit
track 6 ip sla 6
delay up 10 down 15
exit
```

Figure 18. Verification of creation of IP SLAs in D1



Task 4.2: On D2, create IP SLAs that test the reachability of R3 interface E1/0.

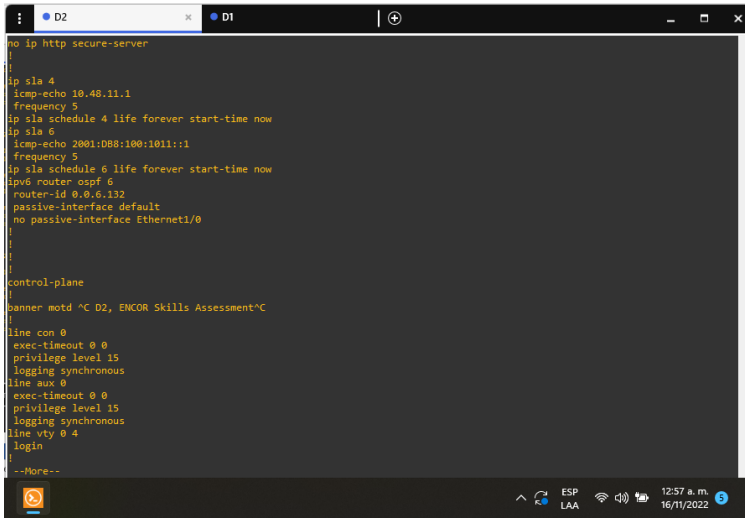
SW D2

```
ip sla 4
icmp-echo 10.48.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay up 10 down 15
exit
track 6 ip sla 6
```

delay up 10 down 15

exit

Figure 19. Verification of creation of IP SLAs in D2



Task 4.3: On D1 and D2, configure HSRPv2.

SW D1

interface vlan 100

standby version 2

standby 104 ip 10.48.100.254

standby 104 priority 150

standby 104 preempt

standby 104 track 4 decrement 60

standby 106 ipv6 autoconfig

standby 106 priority 150

```
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.48.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.48.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Figure 20. Checking the HSRPv2 configuration for D1

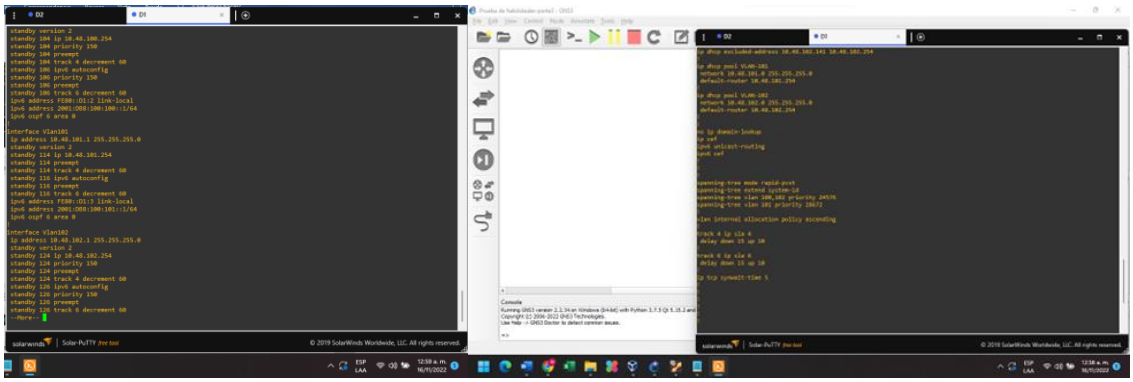
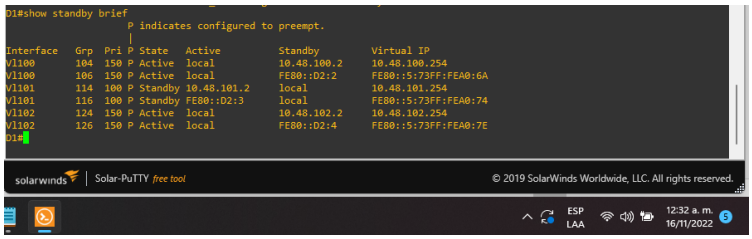


Figure 21. "show standby brief" command for D1



SW D2

interface vlan 100

standby version 2

standby 104 ip 10.48.100.254

standby 104 preempt

standby 104 track 4 decrement 60

standby 106 ipv6 autoconfig

standby 106 preempt

```
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.48.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.48.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Figure 22. Checking the HSRPv2 configuration for D2

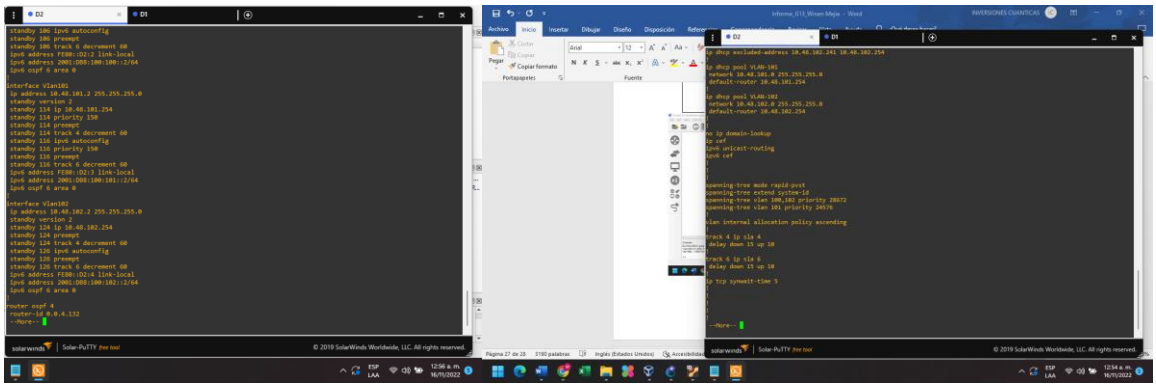
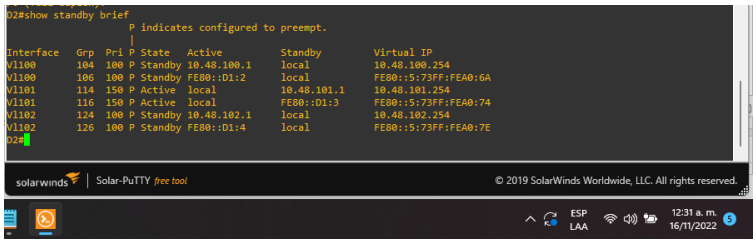


Figure 23. "show standby brief" command for D1



CONCLUSIONES

El desarrollo de las distintas prácticas de aprendizaje durante el diplomado CCNP de Cisco, reforzo las capacidades en la configuración básica de router y switch, permitió adquirir habilidades en el diseño y estructuración de redes conmutadas mediante el uso de los protocolos como STP y RSTP, también se pusieron en práctica los conocimientos en la configuración de VLANs y su enrutamiento.

Otros de los aprendizajes adquiridos, es la capacidad de implementar y diseñar soluciones de redes empresariales escalables mediante la configuración básica y avanzada de protocolos de enrutamiento como OSPF, BGP y HSRP

Por último, se comprendieron las distintas maneras de solucionar errores que se pueden presentar durante la configuración e implementación de una red de datos aplicando adecuadamente comandos para el diagnóstico en ambientes de red corporativos LAN y WAN

BIBLIOGRAFÍA

English, J. (2022). What is a VLAN (virtual LAN). What is network virtualization? Everything you need to know (Article). Disponible en: https://www.techtarget.com/searchnetworking/definition/virtual-LAN

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

Edgeworth, B. Garza Rios, B. Gooley, J. Hucaby, D. (2020). CISCO Press (Ed). OSPFv3. CCNP and CCIE Enterprise Core ENCOR 350-401.Disponible en: 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.Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

Flor, P. (2022). Introducción al protocolo BGP [OVI]. Disponible en: https://repository.unad.edu.co/handle/10596/49573

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

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