DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN MANUEL HOLGUÍN QUIRAMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

INGENIERÍA ELECTRÓNICA

SANTIAGO DE CALI

2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN MANUEL HOLGUÍN QUIRAMA

Diplomado de opción de grado presentado para optar al título de

INGENIERO ELECTRÓNICO

DIRECTOR:

MSc. GERARDO GRANADO ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

INGENIERÍA ELECTRÓNICA

SANTIAGO DE CALI

2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del jurado

_____

Firma del Jurado

SANTIAGO DE CALI, 03 de diciembre de 2021

AGRADECIMIENTOS

Dedico este trabajo a Dios, a mi familia y a las diferentes personas que a lo largo de este diplomado y de otros cursos en la UNAD me brindaron su apoyo para avanzar tanto a nivel profesional como personal encaminado a la consecución del objetivo principal que me permite aspirar al título de ingeniero electrónico.

Una mención especial a mis padres, mi esposa y mi hijo que son el impulso extra que me permite reivindicarme y tener esa energía necesaria para cumplir con las tareas propuestas y objetivos trazados.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ENRUTAMIENTO: Es el proceso de envío de paquetes en redes de comunicación con gran cantidad de conectividad entre los dispositivos que la conforman. Como punto fundamental este proceso optimiza e identifica la ruta mas óptima para llevar a cabo la comunicación. Este proceso genera tablas de enrutamiento y aplica parámetro como distancia administrativa, métrica, ancho de banda y uso de protocolos.

GATEWAY: Este concepto se aplica en comunicación enfocado a la frontera que permite o no la comunicación con otras redes y dispositivos. Se conoce también como puerta de enlace o pasarela y permite la interacción también de protocolos.

GNS3: Software especializado de uso libre para modelar redes de manera virtual mediante el uso de IOS de equipos CISCO que simulan su funcionamiento como si se trataran de equipos reales. Este software fue lanzado en 2008 desarrollado por GNS3, por otra parte, este software permite la interacción entre equipos reales y virtuales.

HOST: Es un equipo, ordenador o computador que funciona como punto de inicio o de fin del proceso de transferencia de datos. Estos equipos requieren de una configuración mínima de direccionamiento para permitir el intercambio de datos.

MASCARA DE RED: Este concepto se basa en una configuración a partir de bits para delimitar una red. Mediante la implementación de máscaras de red se pueden dividir en segmentos de una red o subredes lo cual hace parte fundamental del proceso de intercambio de paquetes entre dispositivos.

CONMUTACIÓN: Mediante la conmutación se establecen los caminos físicos entre dos puntos para el intercambio de información segmentando las redes y dividiéndolas en dominios de colisión aportando al desempeño óptimo de estas.

VIRTUAL MACHINE: Es un software que presta la función de simular un sistema operativo de un equipo de cómputo y que permite flexibilizar con diversos sistemas operativos en cuanto a versión o fabricantes. Esta instalación se realiza sobre un dispositivo físico que incluso permite la interacción entre el virtual y real.

RESUMEN

La actividad se basa principalmente en potencializar las características de los equipos que componen la topología de la red a través de los conceptos estudiados a lo largo del curso CCNP de CISCO mediante la implementación de comandos lógicos apoyados en el desarrollo en softwares especializados.

Para el desarrollo de las actividades se configuran dispositivos como conmutadores, enrutadores y ordenadores apoyados en los conceptos de redes integrando desempeño, seguridad, redundancia, direccionamiento, manejo de áreas de operación entre otros conceptos, los cuales contribuyen a aumentar el rendimiento y confiabilidad de redes. Este trabajo tiene como objetivo principal evidenciar las habilidades adquiridas a lo largo del diplomado CCNP para optar al título de Ingeniería Electrónica de la UNAD.

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

ABSTRACT

The activity is mainly based on enhancing the characteristics of the equipment that make up the network topology through the concepts studied throughout the CISCO CCNP course through the implementation of logical commands supported by the development of specialized software.

For the development of activities, the various devices such as switches, routers and computers are configured supported by the concepts of networks integrating performance, security, redundancy, addressing, management of operation areas among other concepts, which contribute to increase performance and reliability. of the networks. The main objective of this work is to demonstrate the skills acquired throughout the CCNP diploma to qualify for the title of Electronic Engineering from UNAD. In this, the development of the proposed activity and its results is reflected step by step.

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

INTRODUCCIÓN

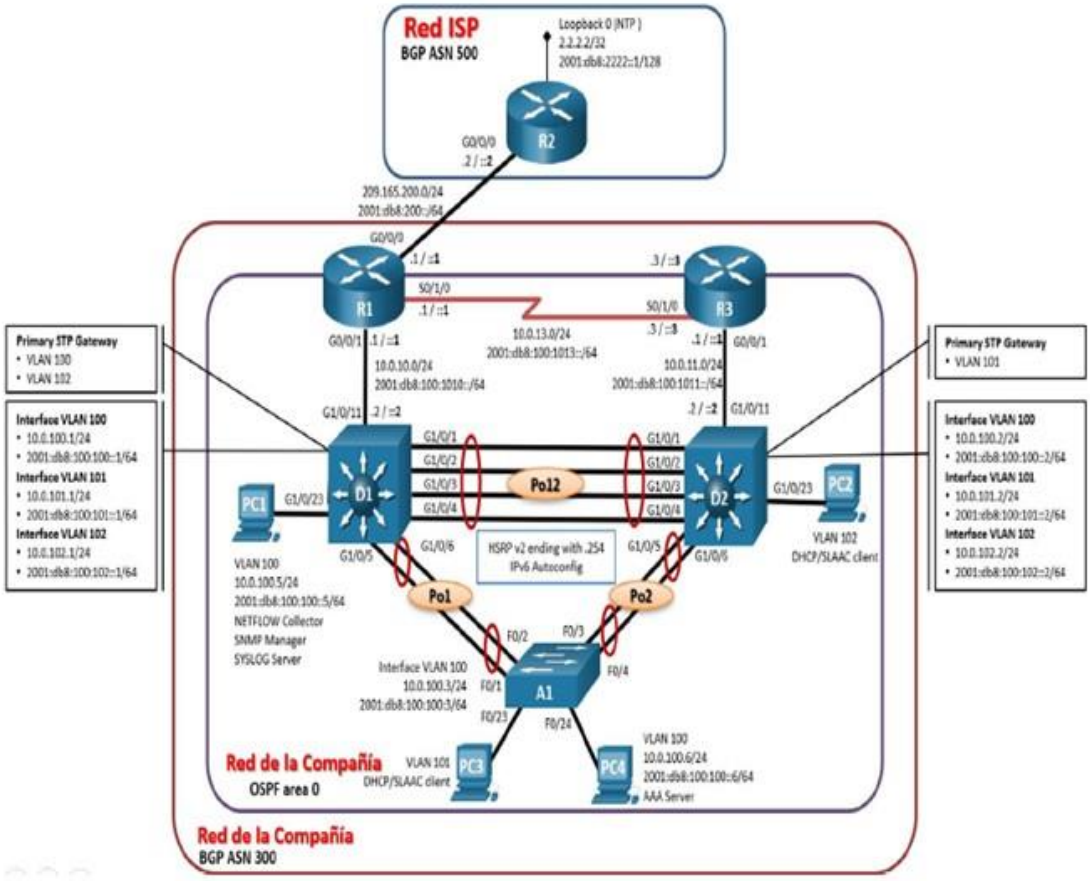
A continuación, se presenta la implementación y desarrollo sobre la topología de red propuesta en la cual se llevan a cabo los diferentes pasos de la actividad. En este documento se consignan los comandos utilizados para cada uno de los diferentes pasos propuestos, así como las evidencias tomadas a través de imágenes de las diferentes CLI de los equipos entre ellos, routers, switches y host.

Se realizan verificaciones del funcionamiento de las configuraciones implementadas y análisis de los conceptos estudiados a lo largo del diplomado CCNP de CISCO, entre los cuales se encuentran conceptos de enrutamiento en IP versión 4 e IP versión 6, segmentación de redes, creación de loopbacks, protocolos como STP, RSTP, HSRP, HSRP V2, OSPF V2, OSPFV3, MP-BGP, seguridad de equipos y redes avanzada para evitar suplantaciones y jaqueo de contraseñas, conceptos de administración, creación de túneles, entre otros.

DESARROLLO

1. Escenario Propuesto.

Figura 1. Topología de la Red



En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañia" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Figura 2. Escenario de simulación software GNS3

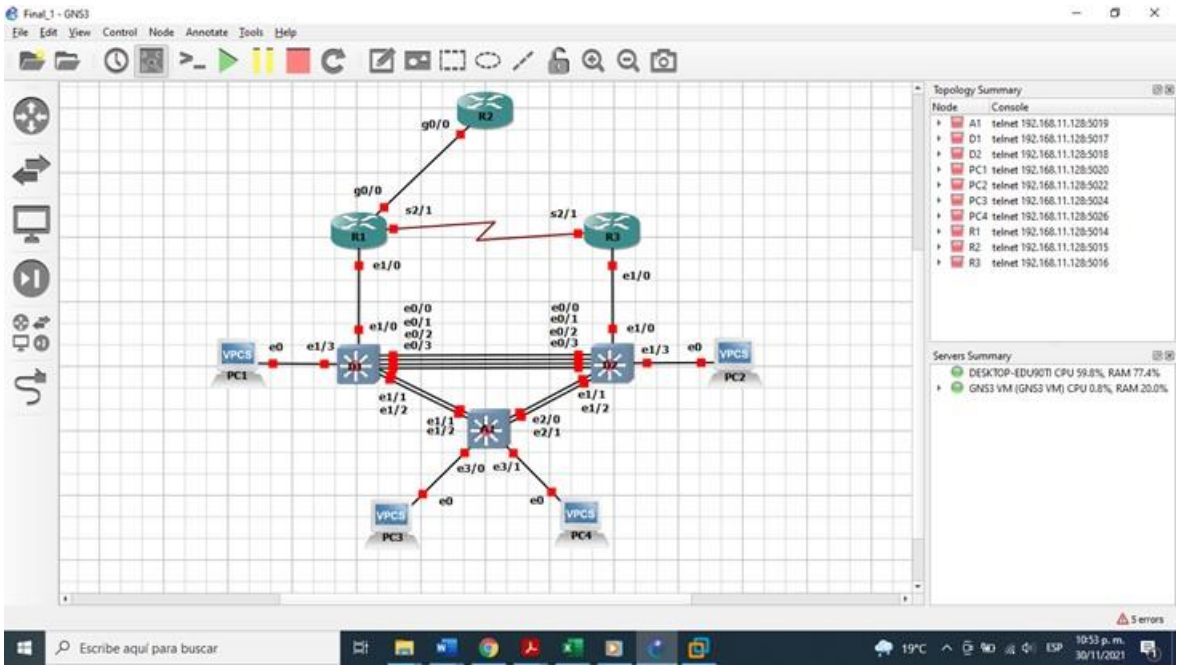


Tabla 1. Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4

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

2. Parte 1

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

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

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

Para esta etapa se emplea el software GNS3 y una Virtual Machine para soportar la ejecución adecuada de esta aplicación haciendo las veces de servidor donde se almacenan las diferentes imágenes de los equipos o similares compatibles antes mencionados. En la figura 1 se puede apreciar la topología de la red.

Paso 2: Configurar los parámetros básicos para cada dispositivo.

a. Mediante conexión de consola ingrese en cada dispositivo se acceden los diferentes dispositivos y se configuran los parámetros básicos de acuerdo con la información entregada en la tabla 1 de direccionamiento. A continuación, se presentan los parámetros configurados para los routers R1, R2 y R3, switches de capa 3 del modelo OSI TCP/IP D1 y D2, switche de capa 2 modelo OSI TCP/IP A1 y los diferentes PCs.

Router R1

hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.225 255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
interface g0/0/1
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.1 255.255.255.0

ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit

Router R2

hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit

Router R3

hostname R3
ipv6 unicast-routing

no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

Switch D1

hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100

name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit

interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit

Switch D2

hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0

logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local

ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit

Switch A1

hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0

exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
exit

b. Mediante el comando *copy running-config startup-config,* en el modo de configuración privilegiado se carga al archivo de inicio de cada dispositivo las configuraciones descritas en el literal a. del paso 1.
c. En los PC1 y PC4 de la topología de la red, se ingresa al modo consola y mediante el *comando IP 10.0.100.5 255.255.255.0 10.0.100.254* se

configura la IPv4 para PC1, para PC4 se ingresa el comando *IP 10.0.100.6 255.255.255.0 10.0.100.254*, el cual contiene la dirección IPv4 del host, la máscara de red y el gateway predeterminado.

3. Parte 2: Configurar la capa 2 de la red y el soporte de Host

Teniendo en cuenta lo solicitado en la parte 2 del documento final, se realiza la tabla 2 comandos parte 2 donde se definen los diferentes comandos utilizados para llevar a cabo las configuraciones solicitadas en esta parte del documento incluyendo verificaciones de comunicación a través de comandos de *ping* desde los diferentes PCs que componen la red.

Tabla 2. Tareas de configuración Parte 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: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • 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

Para el desarrollo de las actividades anteriores se presentan los comandos en la tabla 3 de comandos parte 2.

Tabla 3. Comandos Parte 2

Item		Comando	Funcionalidad
Parte 1	b	show running-config	Ver archivo de configuración
		copy running-config startup-config	Copiar archivo de configuración al archivo de inicio de SW
Parte 2	2.1	D1(config)#interface fastethernet 0/1 D1(config-if)#switchport mode trunk D1(config-if)#switchport trunk encapsulation dot1q	Configuración interfaces troncales IEEE 802.1Q
	2.2	D1(config-if)#switchport trunk native vlan *vlan-ID*	Configrar VLAN nativa en enlaces troncales
	2.3	D1(config)#spanning-tree mode rapid-pvst	Permite establecer el tipo de protocolo de árbol de expansión.
	2.4	D1(conf)#spanning-tree vlan ID root secondary	Establece la prioridad de puente en incrementos de 4096 (predeterminado = 32768).
	2.5	D1(config)#interface range fa 0/1 - 2	Especifica las interfaces que conforman el grupo EtherChannel
		D1(config-if-range)#interface port-channel 1 D1(config-if)#switchport trunk allowed vlan *vlan ID*	Asigna el ID del port channel que se está creando y asigna las VLAN que alojará el port-channel
	2.6	S1(config-if)#switchport mode access S1(config-if)#switchport access vlan *vlan ID*	Configuración de las interfaces como puertos de acceso y se asignan las VLAN para estas interfaces
	2.7	ip dhcp excluded-address 10.0.0.1 10.0.0.5 ip dhcp pool Central network 10.0.0.0 255.255.255.0 default-router 10.0.0.2 #show ip dhcp import	Mediante estos comandos se ecluyen los gruos de direcciones IP que no se desean asignar de manera automátca para evitar posibles conflictos. Se asigna la red de trabajo junto con la máscara de red, se nombra el servicio DHCP y se asigna una dirección al como puerta de enla o gateway. En los PCs 3 y 4 mediante el comando *IP show* se puede verificar la asignación dinámica.

La comprobación mediante el uso de *ping* entre los equipos propuestos en la tares 2.8 se trabajó desde consola en el software GNS3. A continuación se muestran las figuras 3, 4, 5 y 6 los comandos exitosos.

Figura 3 *Ping* desde PC1

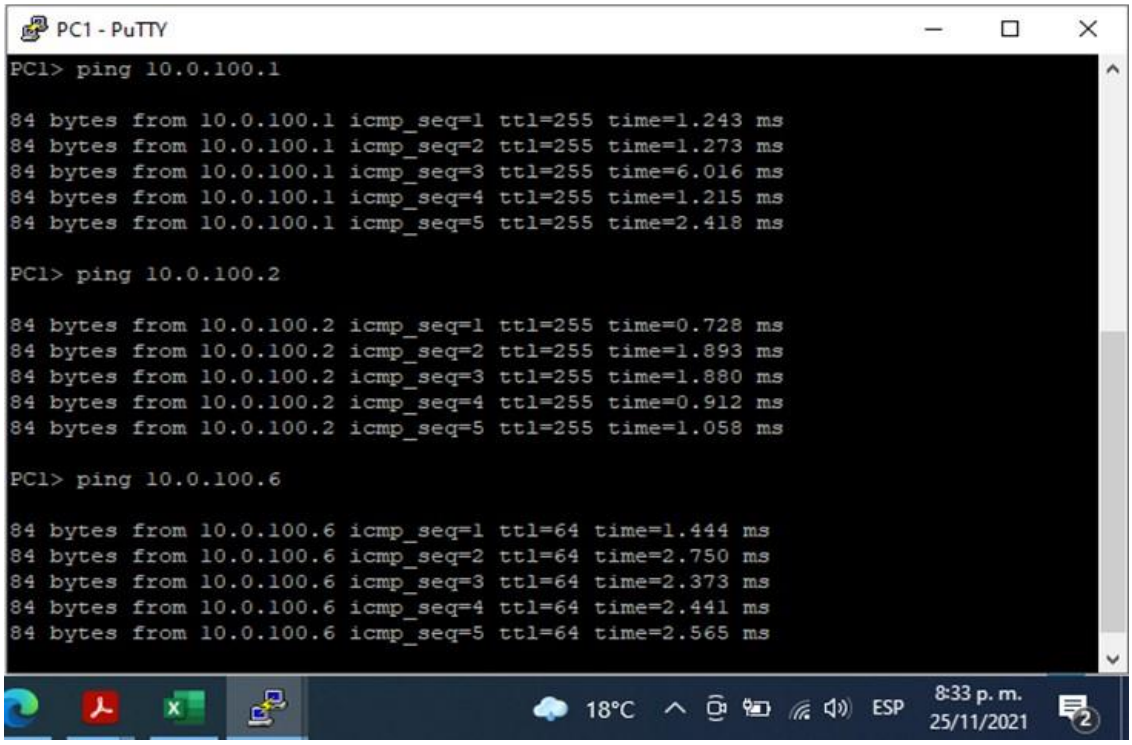


Figura 4 *Ping* desde PC2

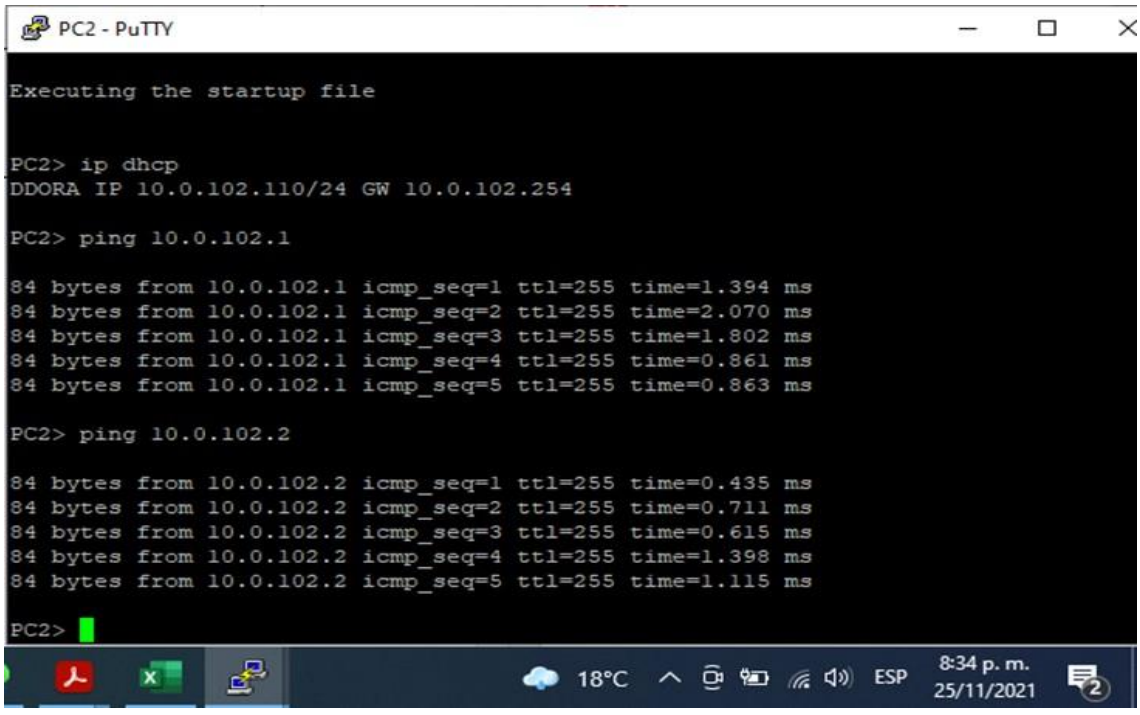


Figura 5 *Ping* desde PC3

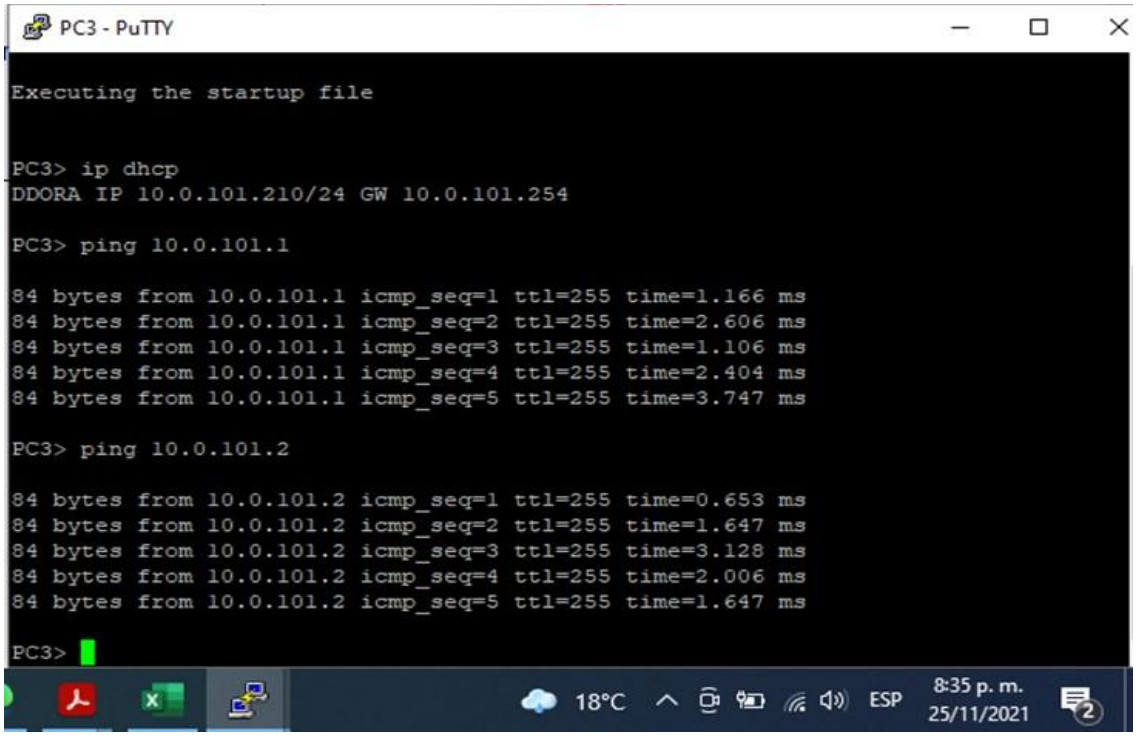
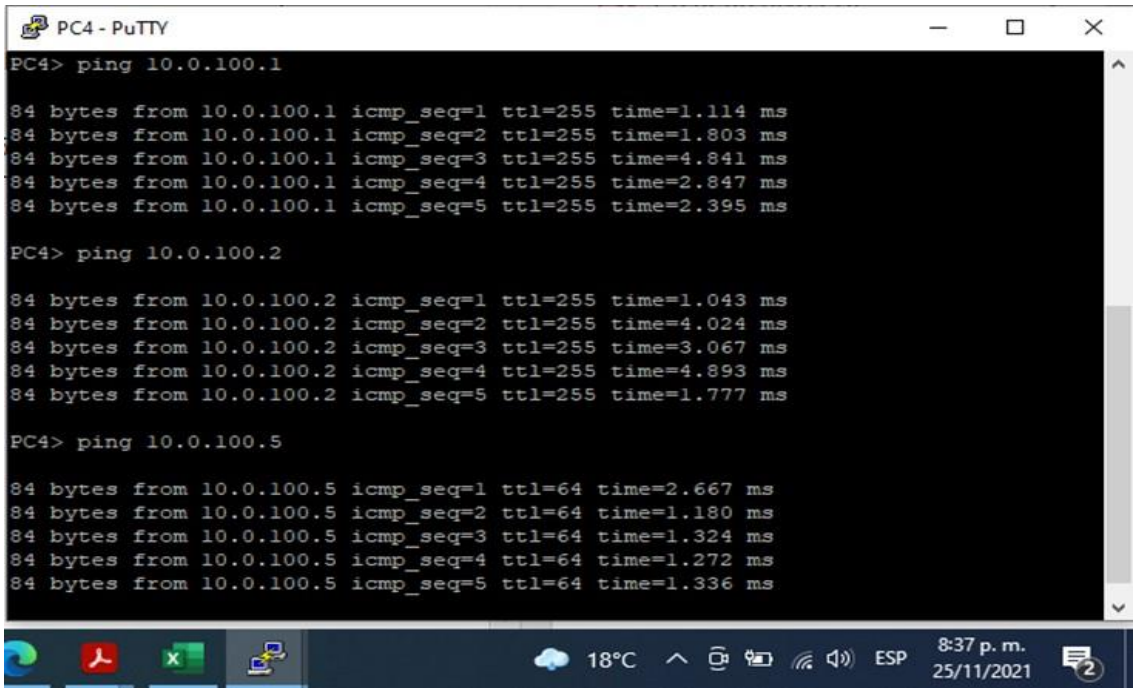


Figura 6 *Ping* desde PC4



4. Parte 3 Configurar los protocolos de enrutamiento

En la tabla 4 tarea parte 3 se describen los diferentes pasos a seguir para realizar la configuración de enrutamiento en la topología de red propuesta para el desarrollo de las tareas. Los comandos ejecutados en este punto se describen en la tabla 5 comandos parte 3.

Tabla 4. Tareas Parte 3

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	Use OSPF Process ID 4 y asigne los siguientes router-IDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • 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 Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID 6 y asigne los siguientes router-IDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • 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 MP-BGP.	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 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. 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 IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

Tabla 5. Comandos Parte 3.

Item		Comando	Funcionalidad
Parte 3	3.1	R1(config)# router ospf *ID* R1(config)# router-id xx.xx.xx.xx	comando en el modo de configuración global para habilitar OSPF
		R1(config-router)# network 192.168.1.0 0.0.0.255 area 0 R1(config-router)# network 192.168.12.0 0.0.0.3 area 0 R1(config-router)# network 192.168.13.0 0.0.0.3 area 0 R1(config-router)#passive-interface gx/x R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.13.3 R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.10.2 R1(config)#router ospf 4 R1(config-router)#default-information originate	Configure las instrucciones network para las redes en el R1. Utilice la ID de área 0. Use el comando router ospf y agregue las instrucciones network para las redes en el R2 y el R3. Se configuran las redes conectadas directamente al router Se puede ingresar la wild card o la mascara de red y el router la interpreta de igual manera Cuando el routing OSPF está configurado en el R2 y el R3, se muestran mensajes de adyacencia de vecino en el R1. R1# 00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to FULL, Loading Done R1# 00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to FULL, Loading Done R1#
	3.2	R1(config)#router ospfv3 *ID* R1(config-router)# router-id *xx.xx.xx.xx* R1(config-router)#exit R1(config)#interface *gx/x* R1(config-if)# ipv6 ospf *ID* area 0 R1(config)#router ospfv3 *ID* R1(config-router)#passive-interface *gx/x*	Configuración OSPFv3 El router ID debe ser de 32 bits Se configura OSPFv3 en cada interface

	3.3	R2(config)#ip route 0.0.0.0 0.0.0.0 loopbak 0 R2(config)# ipv6 unicast-routing R2(config) # ipv6 ::/0 loopbak 0 R2(config)# router bgp 500 R2(config-router)# bgp router-id 2.2.2.2 R2(config-router)# no bgp default ipv4-unicast R2(config-router)# neighbor 209.165.200.225 remote-as 300 R2(config-router)# neighbor 2001:db8:200::1 remote-as 300 R2(config-router)# address-family ipv4 R2(config-router-af)# network 2.2.2.0 mask 255.255.255.255 R2(config-router-af)# network 0.0.0.0 mask 0.0.0.0 R2(config-router-af)# neighbor 209.165.200.225 activate R2(config-router-af)# no neighbor 2001:db8:200::1 activate R2(config-router-af)# exit R2(config-router)# address-family ipv6 R2(config-router-af)# network 2001:db8:2222::/128 R2(config-router-af)# network ::/0 R2(config-router-af)# neighbor 2001:db8:200::2 activate R2(config-router-af)# exit	Configuración ruta estática predeterminada IPv4 e IPv6 Configuración MP-BGP
	3.4	R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.0 R1(config)# ipv6 unicast-routing R1(config) # ipv6 ::/0 2001:db8:100:: R1(config)# router bgp 300 R1(config-router)# bgp router-id 1.1.1.1 R1(config-router)# no bgp default ipv4-unicast R1(config-router)# neighbor 209.165.200.226 remote-as 500 R1(config-router)# neighbor 2001:db8:200::2 remote-as 500 R1(config-router)# address-family ipv4 R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0 R1(config-router-af)# neighbor 209.165.200.225 activate R1(config-router-af)# no neighbor 2001:db8:200::1 activate R1(config-router-af)# exit R1(config-router)# address-family ipv6 R1(config-router-af)# network 2001:db8:100::/48 R1(config-router-af)# neighbor 2001:db8:200::1 activate R1(config-router-af)# no neighbor 209.165.200.225 activate R1(config-router-af)# exit	Configuración ruta resúmen IPv4 e IPv6 Configuración MP-BGP desde R1

A continuación, se muestran las figuras 7 y 8 que contienen la evidencia de la configuración de OSPFv2 en R1 de acuerdo a lo solicitado para la parte 3 tarea 3.1 y 3.2 mediante el uso del comando *show ip protocol*.

Figura 7 Configuración OSPFv2 R1

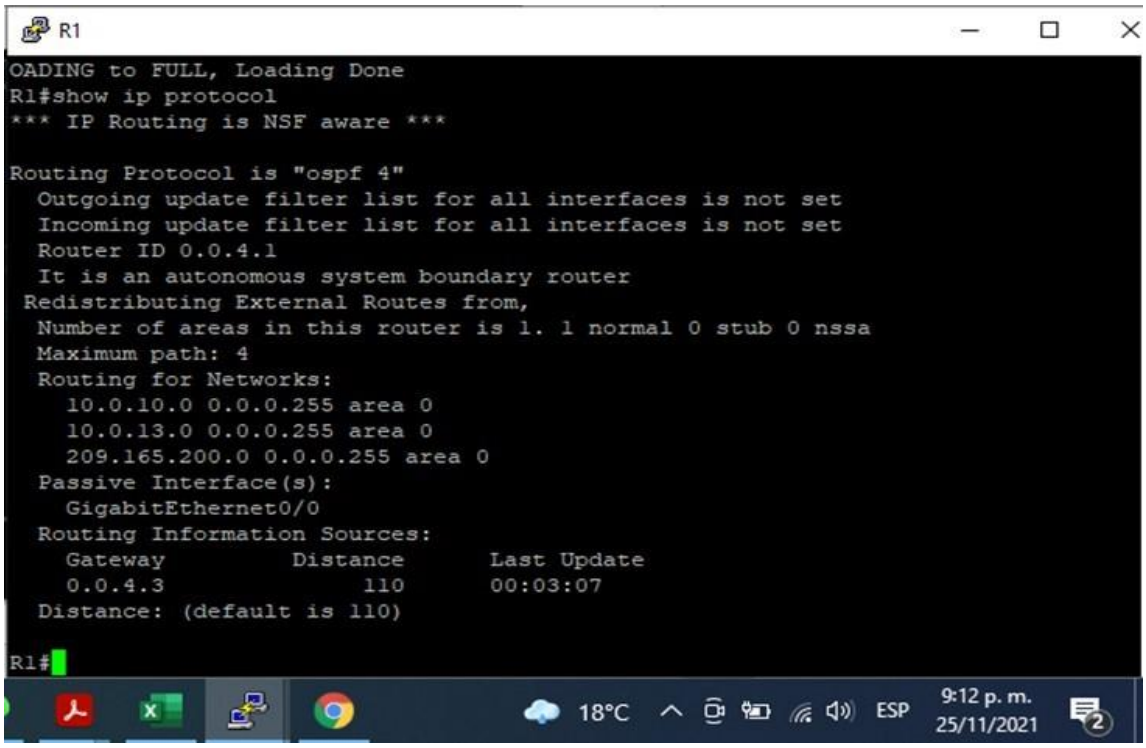
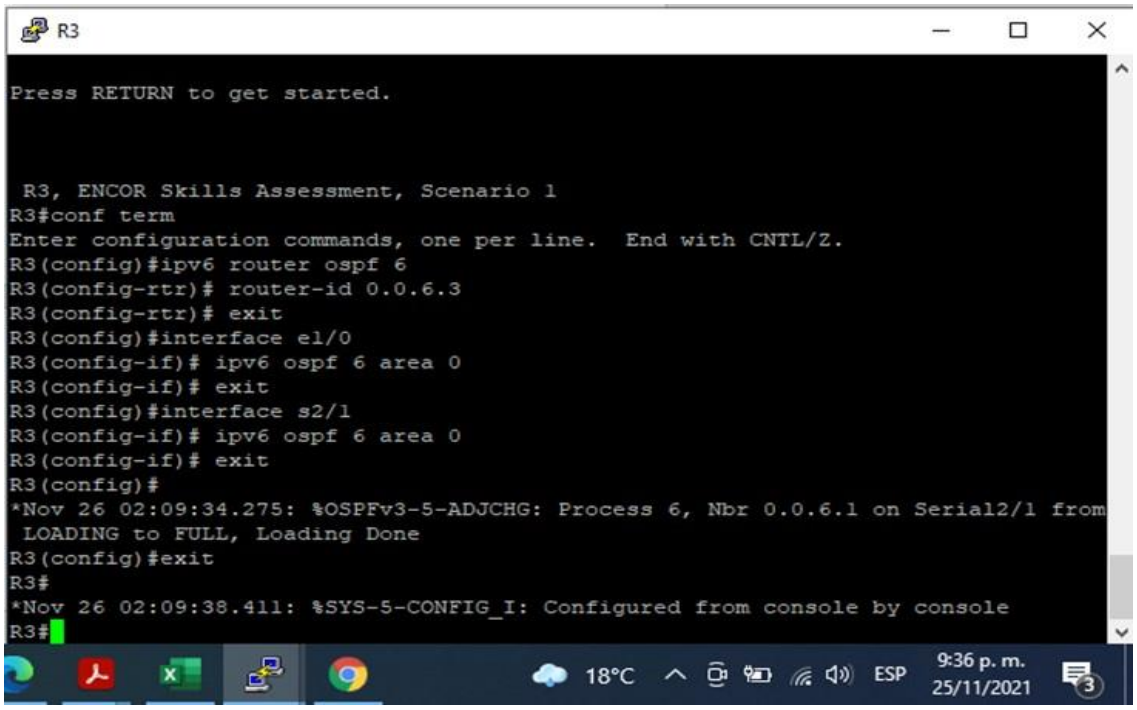


Figura 8 Configuración OSPFv2 R3



En la figura 8 se puede apreciar el mensaje en el que se información de arranque del enlace configurad a través de OSPF entre R1 y R3.

Dando continuidad al desarrollo de la tarea 3.3 y 3.4, en las figuras 9 y 10 se evidencia la implementación de MP-BGP para la “RED ISP”.

Figura 9 Configuración MP-BGP R2

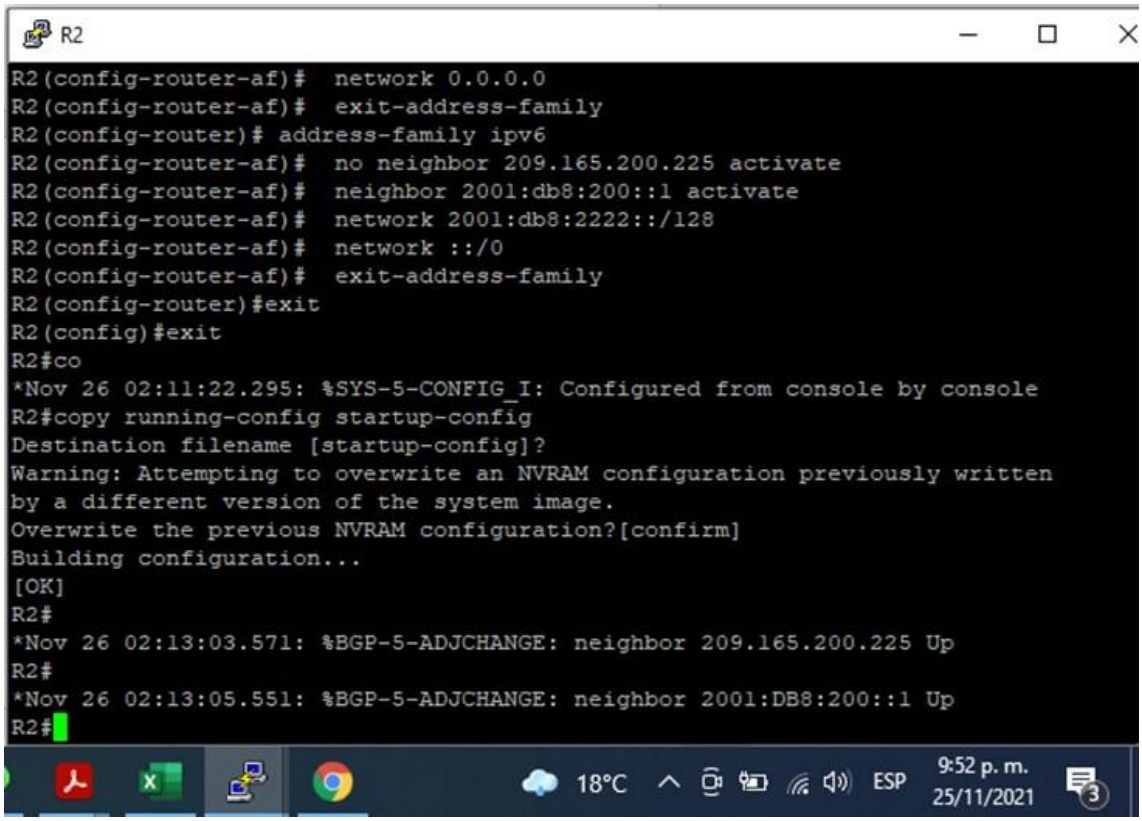
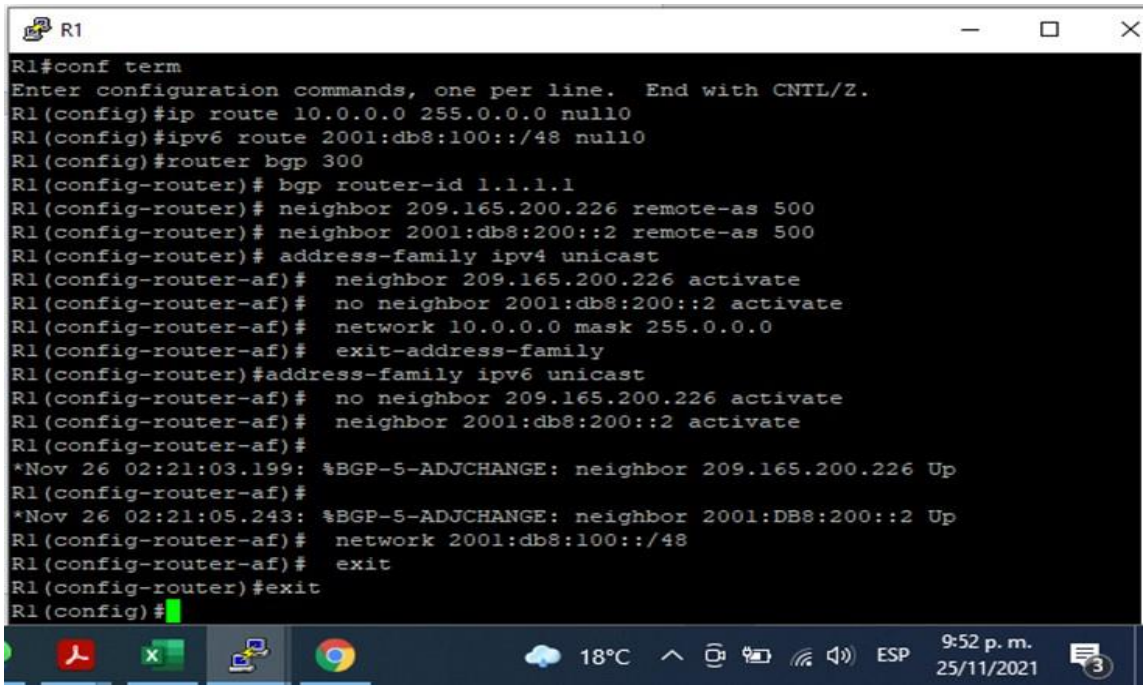


Figura 10 Configuración MP-BGP R1



5. Parte 4. Configurar la Redundancia del Primer Salto

Para el desarrollo de la parte 4, se presenta a continuación la tabla 6 Tarea Parte 4 donde se evidencia la actividad propuesta. En esta parte se trabajaron los comandos descritos en la tabla 7 Comandos parte 4, allí se puede evidenciar punto a punto los comandos requeridos al momento de implementar la configuración necesaria para HSRP versión 2.

Tabla 6. Tarea Parte 4

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.

Tabla 7. Comandos parte 4

Item	Comando	Funcionalidad

Parte 4	4.1	ip sla 4 icmp-echo 10.0.10.1 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 down 10 up 15	Creación de las IP SLAs con tiempos de implementación inmediata sin tiempo de finalización así como creación de IP SLAs objeto con tiempos de activación y desactivción realizando reportes a un dispositivo específico.
	4.2	ip sla 4 icmp-echo 10.0.11.1 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 down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit	Creación de IP SLAs para comprobar disponibilidad de interfaces con tiempos específicos de rateo.
	4.3	interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 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 10.0.101.254 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 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60 exit	Configuración HSRP vrsión 2 para la creación de clusters o grupos para enrutamiento de tráfico mediante la figura de Principal - Respaldo chequeando frecuentemente las interfaces programadas.

De acuerdo a lo solicitado en la tarea 4, se puede evidenciar en las figuras 11, 12 y 13 la implementación de las IP SLAs en los dispositivos D1 y D2, así como la activación del protocolo HSRP versión 2 en la topología de red propuesta mediante el uso del software de simulación GNS3.

Figura 11 IP-SLAs D1 interface e1/0 en R2

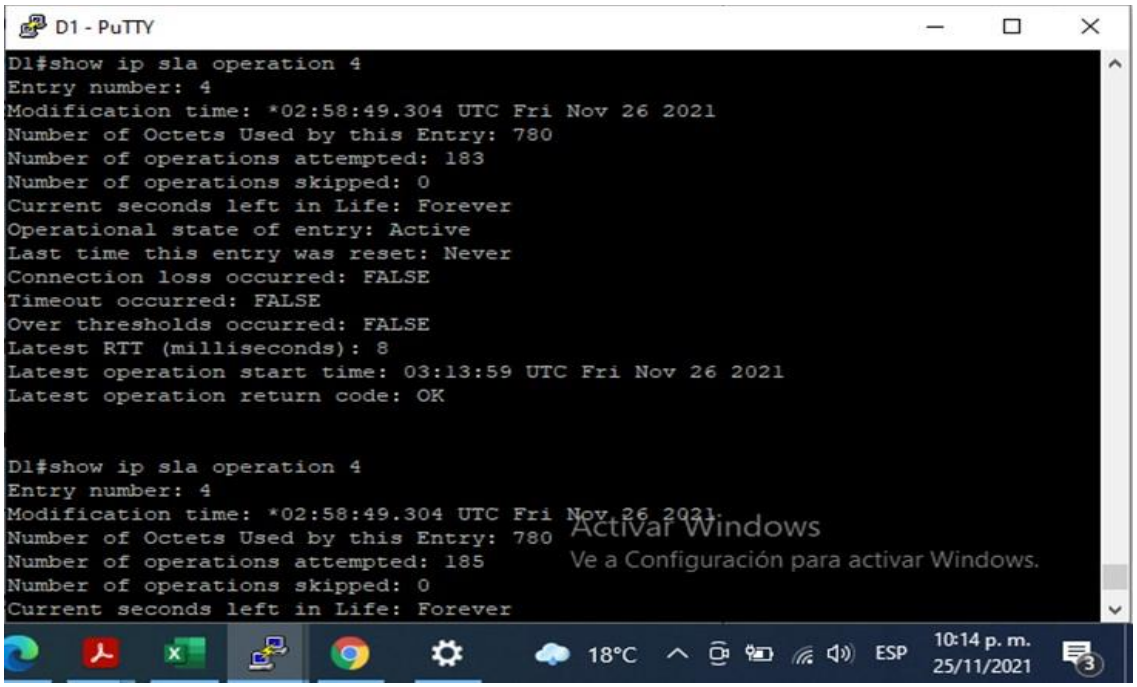


Figura 12 IP-SLAs D2 interface e1/0 en R3

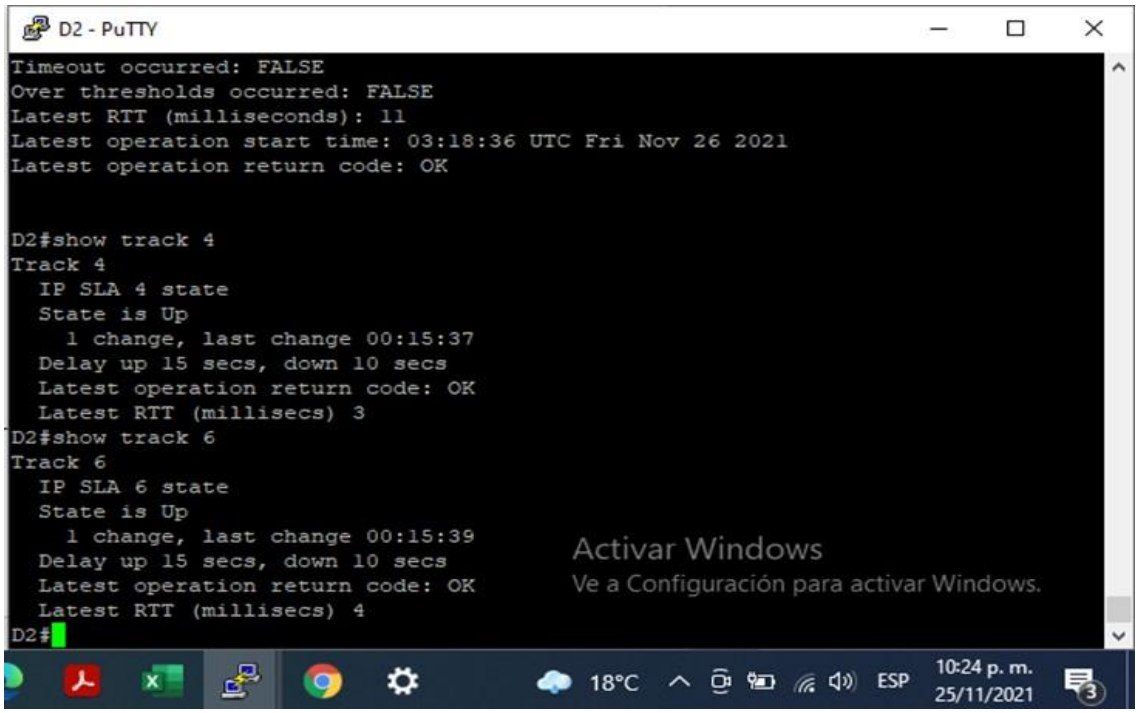
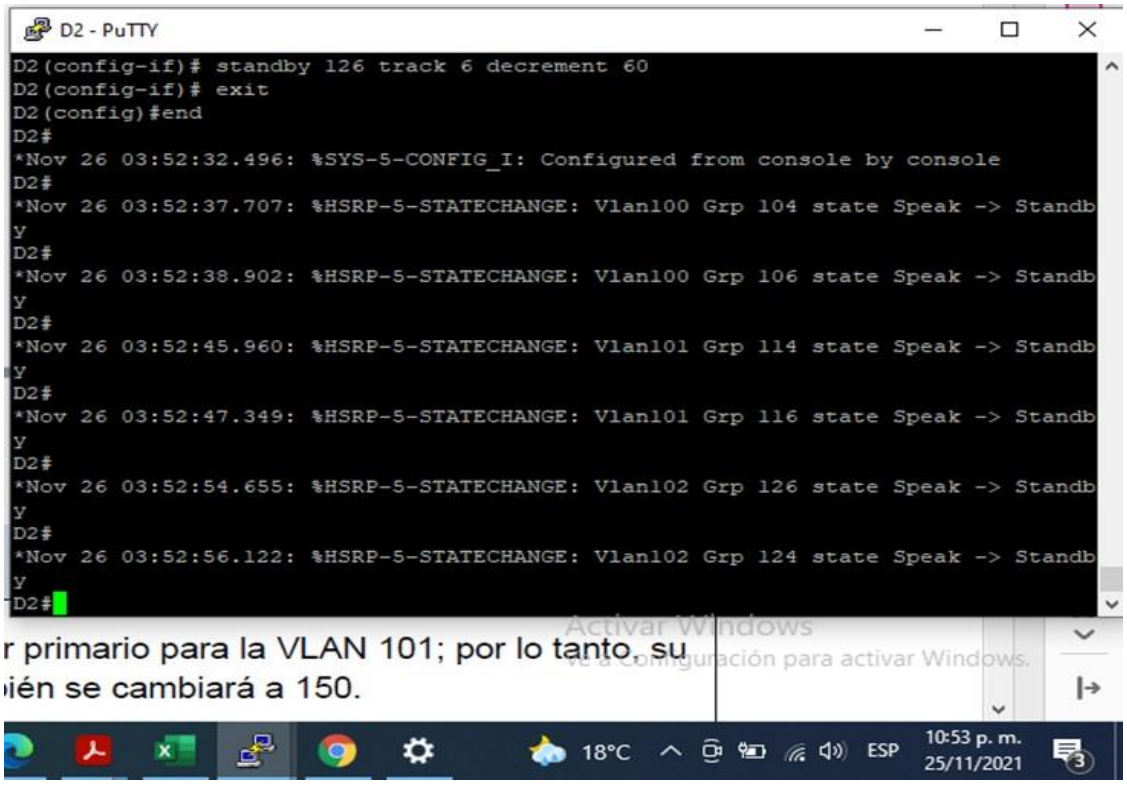


Figura 13 Configuración HSRP versión 2



6. Parte 5. Seguridad

En esta parte se revisan los conceptos relacionados con seguridad enfocados en prevenir modificaciones indeseadas en la red, uso y accesos indebidos, supervisión y administración. En esta parte se lleva a cabo el trabajo propuesto en la tarea 5 y que se encuentra descrito en la tabla 8 Tarea parte 5 mediante los comandos consignados en la tabla 9 Comandos parte 5.

Tabla 8. Tarea parte 5

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 lista de métodos de autenticación AAA	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.
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.

Tabla 9. Comandos parte 5.

Item		Comando	Funcionalidad
Parte 5	5.1	enable algorithm-type SCRYPT secret cisco12345cisco username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	
	5.2		
	5.3	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass exit aaa authentication login default group radius local	
	5.4		
	5.5		

Teniendo en cuenta lo solicitado en la parte 5 y mediante la implementación de los comandos recomendados, se llevan a cabo sobre la topología de la red propuesta y se adjuntan las siguientes evidencias de implementación y funcionamiento.

Figura 14 Implementación algoritmo tipo SCRYPT

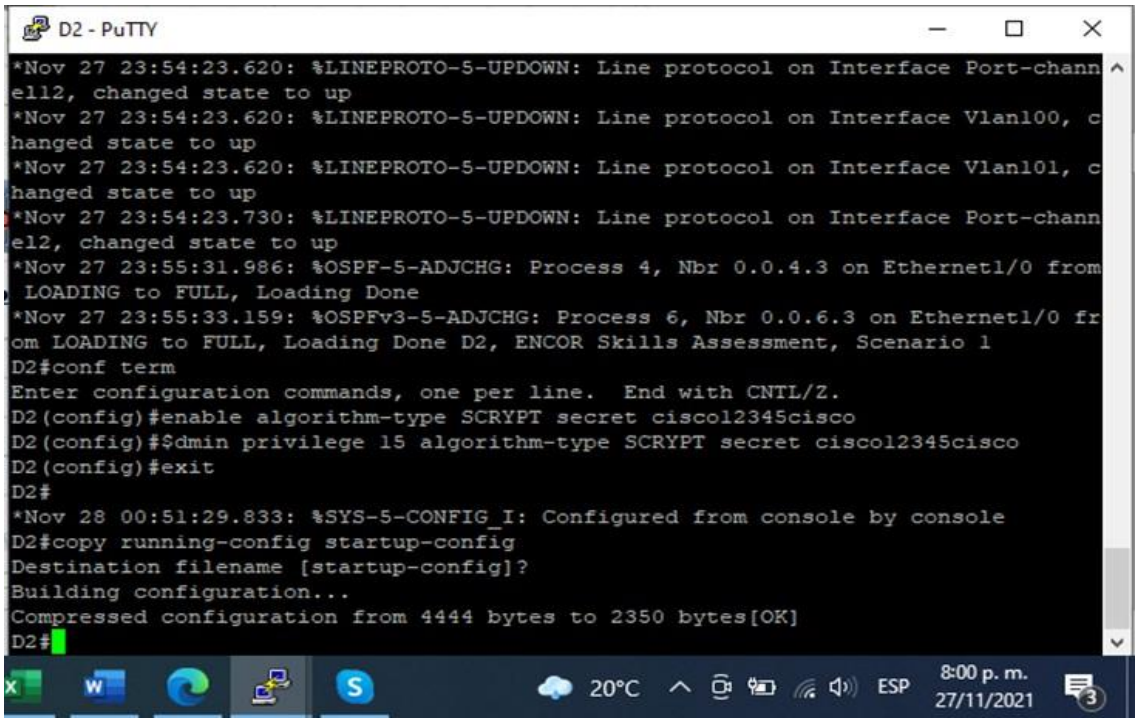
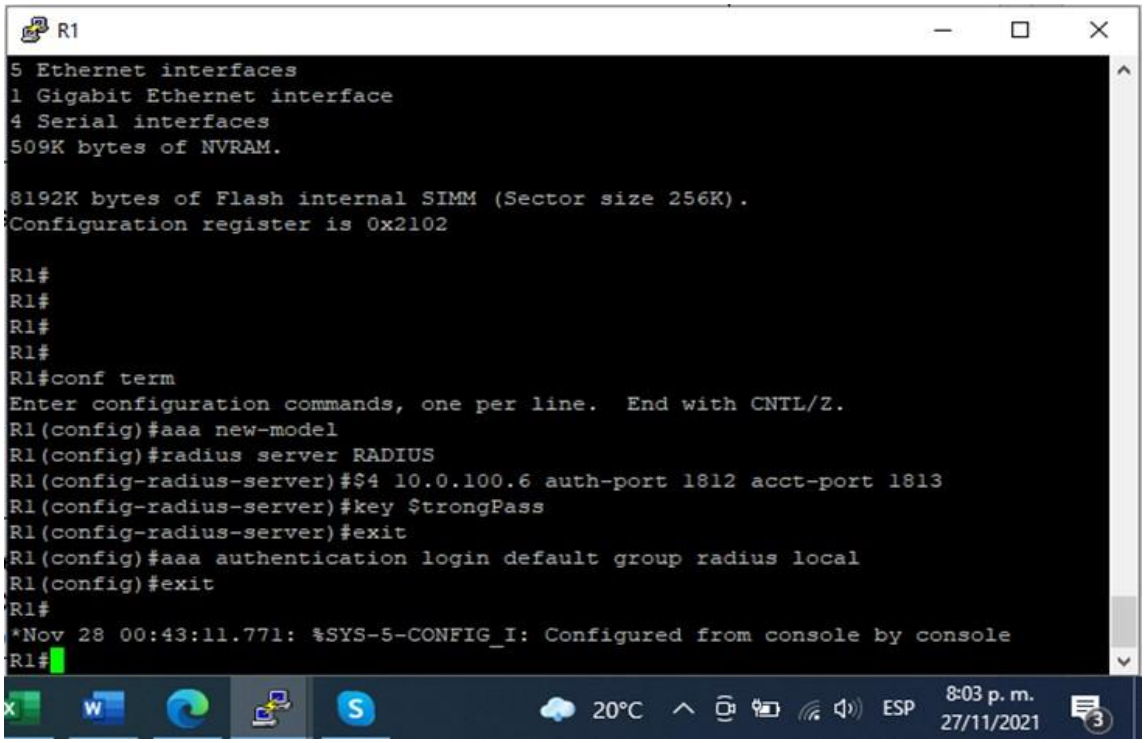


Figura 15 Servidor RADIUS y autenticación AAA



7. Parte 6. Configuración de las funciones de Administración de Red

En la tabla 10 Tarea parte 6 se evidencia lo solicitado como configuración de administración. Allí se encuentra lo relacionado con funciones como sincronización horaria por protocolo NTP, registros del sistema y SNMP. En la tabla 11 se presentan los comandos requeridos para la configuración esperada.

Tabla 10. Tarea parte 6

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.

Tabla 11. Comandos parte 6

Item		Comando	Funcionalidad
Parte 6	6.1	clock timezone utc -5 ntp master 3	Ajuste de hora y declaración de maestro.

	6.2	ntp server 2.2.2.2 logging trap warning logging host 10.0.100.5 logging on	Coonfiguración de NTP desde el maestro hacia los demás equipos
	6.3 6.4 6.5	ip access-list standard SNMP-NMS permit host 10.0.100.5 exit snmp-server contact Juan Holguin snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA snmp-server ifindex persist snmp-server enable traps bgp snmp-server enable traps config snmp-server enable traps ospf end	Configuración del protocolo de adminstración y registros del sistema.

A continuación, se presentan las evidencias de las configuraciones antes descritas.

Figura 16 Configuración horaria

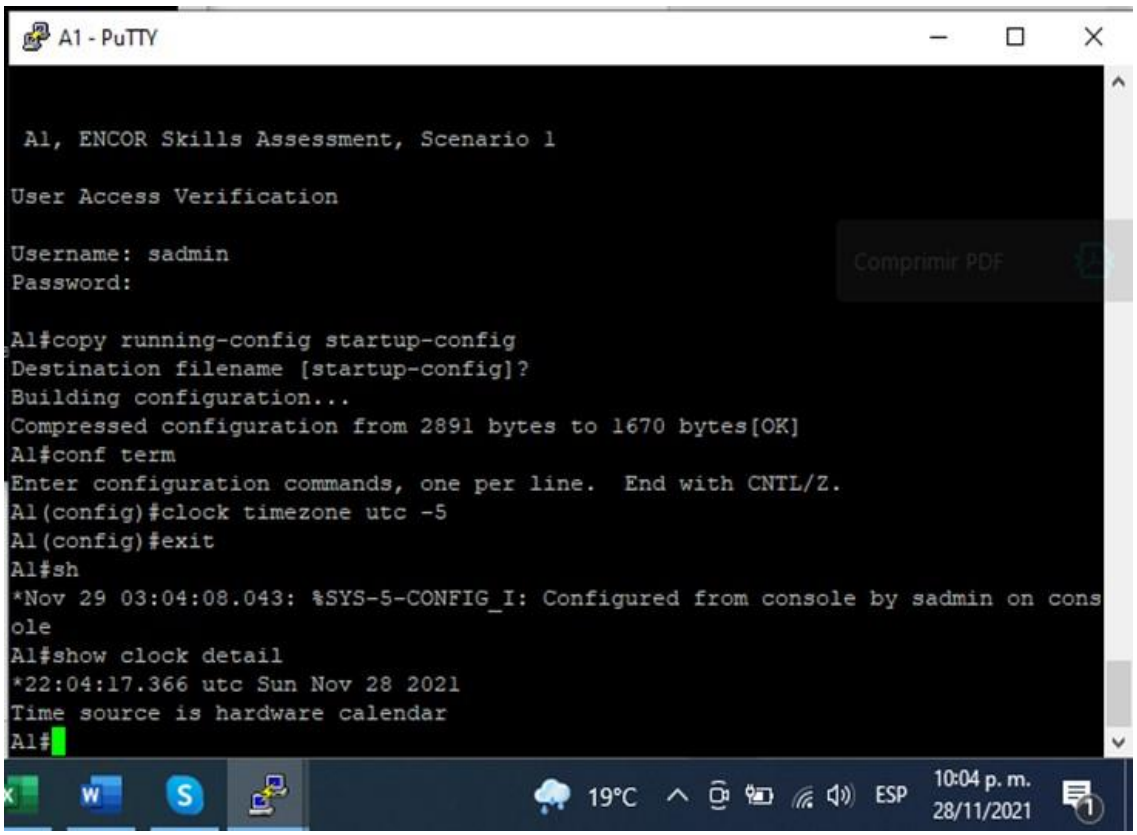


Figura 17 Configuración master NTP

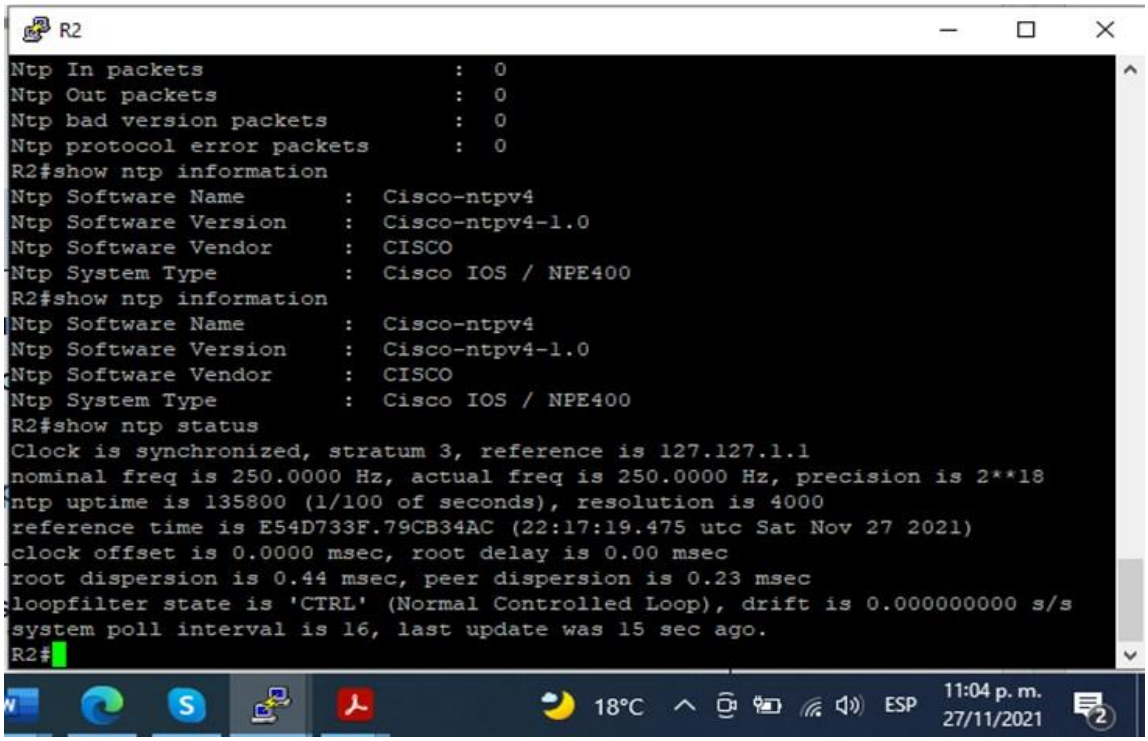
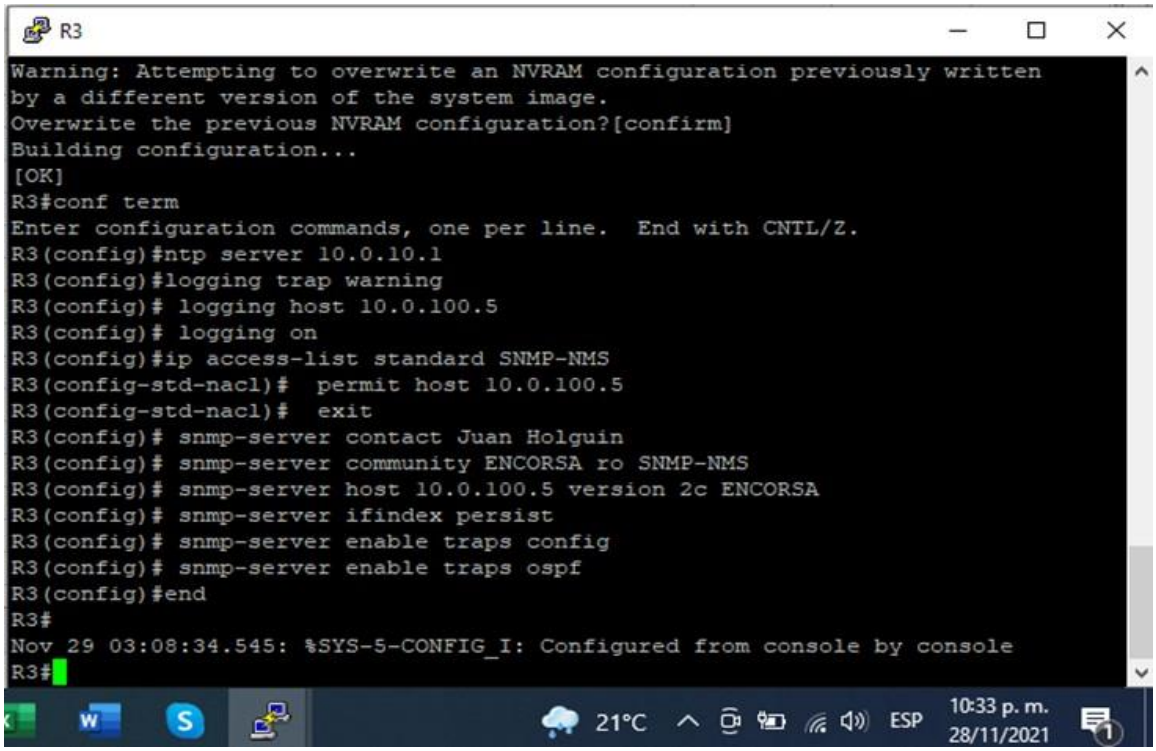


Figura 18 Especificaciones de SNMP versión 2



CONCLUSIONES

Mediante el uso de herramientas como LAN virtuales o VLAN, implementación de interfaces troncales y protocolos de enrutamiento (OSPF – BGP) se puede estructurar adecuadamente una red local que tiene interacción con otras redes externas, facilitando al administrador de la red LAN, la configuración de esta, obteniendo como resultado un impacto positivo en la disminución de errores, además garantizando un flujo de información continuo entre usuarios. Por otra parte, se cuenta con la posibilidad de tener canales redundantes en caso de falla de algún equipo que componga la red y que se habilite de manera automática disminuyendo la necesidad de intervención.

La seguridad es uno de los conceptos fundamentales de redes hoy en día y supone un desafío constante puesto que hay personas y organizaciones dedicadas a vulnerar este concepto, sin embargo, compañías como CISCO se encuentran a la vanguardia de esto y ofrecen en sus equipos y dispositivos controles para restringir estas prácticas y garantizar a nivel de las diferentes capas técnicas que contra resten estas prácticas.

Un tema fundamental sin lugar a dudas tanto para los administradores de redes como para los usuarios de las mismas es el impacto que puede llegar a tener la falta de conectividad. Técnicas y comandos como HSRP permiten manejar conceptos automáticos de redundancia mediante la verificación de redes e interfaces periódicamente, puesto que si se detecta un fallo en algún momento la red automáticamente debería enrutar el direccionamiento por una vía que se encuentra en standby garantizándole al usuario final la no interrupción del servicio.

El trabajo mediante la plataforma de CISCO permite desarrollar las habilidades obtenidas a lo largo del diplomado CCNP e implementarlas en equipos simulados muy similares a los equipos reales mediante el uso de los mismos comandos e interfaces de trabajo iguales a las de los equipos físicos, sin lugar a dudas un herramienta fundamental al momento de administrar y crear redes.

BIBLIOGRAFÍA

NOBOA MIRANDA, Diego. Manual de CISCO cuarta edición, McGraw Hill Interamericana. 2007. 698p.

ARIGANELLO, Ernesto. BARRIENTOS SEVILLA, Enrique. Redes CISCO CCNP a Fondo. Primera edición. RA-MA. 2015. 915p.