DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAVIER MAURICIO MONTENEGRO SANTIAGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
BOGOTA DC
2021

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAVIER MAURICIO MONTENEGRO SANTIAGO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
BOGOTA DC
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA DC, 29 de Noviembre de 2021

AGRADECIMIENTOS

Agradezco a Dios por la oportunidad que me ha dado en la vida por tener el gusto de adquirir conocimientos nuevos que me han permitido formarme como persona y como profesional. Agradezco a mi familia que siempre me ha apoyado para continuar con alcanzar mis metas y propósitos que siempre están ahí en cada momento ayudándome en cada instante. También a mis amigos y compañeros que siempre están colaborando con su apoyo incondicional.

Agradezco a mi esposa y a mi bb que están siempre apoyándome y fortaleciéndome cuando me encuentro cansado su apoyo no tiene precio y la sonrisa de mi bb me llena de fuerzas.

Agradezco a la Universidad a los tutores y a mi empresa por todo lo que me han brindado en este tiempo las cuales me han mostrado que todo es posible y que el conocimiento no tiene límite.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: Es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.

Las certificaciones cisco son reconocidas a nivel mundial como un estándar de la industria para diseño y soporte de redes, garantizando altos niveles de conocimientos y confiabilidad. Su línea de cursos va desde la tecnología más básica de redes hasta áreas especializadas y tecnología avanzada tales como seguridad, redes inalámbricas y telefonía IP. Como este proyecto que tiene certificaciones se validan los conocimientos y habilidades, proporcionando pruebas reales de logros profesionales incrementando las oportunidades de desarrollo y ascenso en la vida profesional. (https://www.netec.com/que-es-cisco)

CCNP: La Certificación Cisco Certified Network Professional (CCNP) te aprueba la habilidad para planificar, implementar, verificar y resolver problemas de redes locales. De igual forma te permite trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, wireless y video.

Las personas con al menos 1 año de experiencia en redes, que estén preparadas para avanzar en su carrera y trabajar de manera independiente en soluciones de redes complejas, son las más adecuadas para tomar una certificación CCNP. (https://www.netec.com/ccnp-routing-and-switching)

CONMUTACIÓN: La Conmutación se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido. (https://es.wikipedia.org/wiki/Conmutaci%C3%B3n_(redes_de_comunicaci%C3%B3n)

ELECTRÓNICA**:** Que es la electrónica, definición, concepto. Electrónica es la rama de la ciencia que se ocupa del estudio del flujo y control de electrones (electricidad) y del estudio de su comportamiento y efectos en aspiradoras, gases y semiconductores, y con dispositivos que utilizan dichos electrones.

Este control de electrones se realiza mediante dispositivos que resisten, transportan, seleccionan, dirigen, conmutan, almacenan, manipulan y explotan el electrón. (https://sivytec.com/electronica-definicion-concepto/)

RESUMEN

El proyecto del diplomado CCNP está formado con un alto contenido de información de redes que nos permitirán profundizar en los conceptos y conocimiento adquiridos en los módulos de CCNA en el programa de Ingenieria Electronica. Es muy importante aclarar que CCNP nos permitirá ampliar todos los conocimientos, conceptos, términos y configuraciones que se han visto desde CCNA de una manera más profesional y especializada.

El proyecto planteado tiene varios objetivos que al desarrollarlo nos permitirá ver cada paso en la estructura de una red. El conocimiento en Redes como lo plantea el diplomado en CISCO nos permitirá colocar en práctica con este proyecto cada tema visto a lo largo del aprendizaje.

Ahora bien al explorar los escenarios planteados podemos dividirlos en seis etapas que puedo clasificar primera la parte física de la topología con los dispositivos y conexiones. El segundo escenario es la implementación de la capa 2 de los switches para su enrutamiento donde los temas son más avanzado y bien estructurado porque podemos analizar que se involucran varios procesos para que la red tenga una convergencia apropiada. Por lo tanto se configurara en forma secuencial los siguientes procesos como son la configuración de la vlan nativa, la configuración de los puertos tanto troncales como de acceso, la activación del protocolo RSTP con la configuración del root- bridge, las activaciones de los canales para Etherchannel. Otro tercer escenario es la configuración de los router donde se configuran los protocolos que son necesarios para el desarrollo de la red como son OSPF y BGP. En la cuarta parte se configura HSRP Version 2 para proveer redundancia de primer salto donde IP SLA que es el acuerdo de nivel de servicio del Protocolo de Internet la cual es una herramienta integrada en el software Cisco IOS muy interesante para los profesionales de TI que permite el monitoreo continuo de la red para ayudar con la resolución de problemas. En la quinta parte de se desarrolla los mecanismos de seguridad AAA en los dispositivos de la topología.Y por ultimo analizaremos las funciones de administración de red donde aplicaremos NTP que nos permitirá sincronizar con la hora autorizada universal para observar un evento en la hora real y aplicaremos SYSLOG que almacenara las alarmas.Este proceso muy importante para ver los eventos y alarmas de la red sincronizadas para realizar soluciones exactas.Todos estos pasos están desarrollados en el simulador GNS3 y la maquina virtual, que desarrollara cada paso de manera casi real como si estuviéramos en un laboratorio con los dispositivos CISCO físicos.El diplomado en CCNP me ha permitido desarrollar una nueva capacidad de comprender mas a fondo conocimientos avanzados de un profesional TI con herramientas muy importantes para la resolución de problemas en las redes.

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

ABSTRACT

The CCNP diplomat project is formed with a high content of network information that will allow us to deepen the concepts and knowledge acquired in the CCNA modules in the Electronic Engineering program. It is very important to clarify that CCNP will allow us to expand all the knowledge, concepts, terms and configurations that have been seen from CCNA in a more professional and specialized way.
The proposed project has several objectives that when developing it will allow us to see each step in the structure of a network. Knowledge in Networks as proposed by the CISCO diploma will allow us to put into practice with this project each topic seen throughout the learning.
Now when exploring the proposed scenarios we can divide them into six stages that I can first classify the physical part of the topology with the devices and connections. The second scenario is the implementation of layer 2 of the switches for their routing where the topics are more advanced and well structured because we can analyze that several processes are involved so that the network has an appropriate convergence. Therefore, the following processes will be configured sequentially, such as the configuration of the native vlan, the configuration of both trunk and access ports, the activation of the RSTP protocol with the root-bridge configuration, the activations of the channels for Etherchannel. Another third scenario is the configuration of the routers where the protocols that are necessary for the development of the network such as OSPF and BGP are configured. In the fourth part, HSRP Version 2 is configured to provide first-hop redundancy where IP SLA, which is the Internet Protocol service level agreement, which is a tool integrated in Cisco IOS software, very interesting for IT professionals that allows continuous network monitoring to assist with troubleshooting. In the fifth part of the AAA security mechanisms in the devices of the topology are developed, and finally we will analyze the network administration functions where we will apply NTP that will allow us to synchronize with the universal authorized time to observe an event in real time and we will apply SYSLOG that will store the alarms. This very important process to see the events and alarms of the network synchronized to carry out exact solutions. All these steps are developed in the GNS3 simulator and the virtual machine, which will develop each step in an almost real way as if we were in a laboratory with physical CISCO devices. The CCNP diploma has allowed me to develop a new ability to understand more in-depth advanced knowledge of an IT professional with very important tools for solving problems in networks.

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

INTRODUCCION

El presente documento tiene como objetivo las pruebas de habilidades que refleja un caso de estudio en un entorno de red que nos permitirá profundizar y analizar la temática del Diplomado en CCNP para fortalecer las competencias en redes y telecomunicaciones que se necesitan como profesional en TI.La universidad nos ha brindado en los anteriores semestres todo el conocimiento en telecomunicaciones de CCNA que nos permite tener bases claras para realizar el diplomado. En este escenario propuesto en el diplomado nos permitirá el desarrollo de capacidades para administrar dispositivos de red, con el análisis de la arquitectura TCP/IP y ser capaz de usar recursos y herramientas de TI para establecer conectividad y solucionar y monitorear los inconvenientes presentados.

En el diplomado vamos adquirir la habilidad de trabajar con la herramienta de simulación GNS3 que trabaja con una maquina virtual que nos permite desarrollar la topología de red para realizar los análisis del los diferentes protocolos que nos permite el uso de los comandos de administración avanzados bajo el uso de protocolos de vector distancia (como OSPF) y estado de enlace y los protocolos de vector de ruta (como BGP).En el desarrollo del escenario vemos varias etapas en las cuales en la parte 2 nos va permitir aplicar las configuraciones de los switches D1, D2 y A1 .En este punto se configuraran las vlans Vlan100, Vlan101, Vlan102 y la Vlan999, también se habilitara el RSTP con la elección de del root bridge, se crearan los tres canales Etherchannel Po1, Po2 y Po12.

En la parte 3 se configurara los protocolos de enrutamiento de estado de enlace en R1, R2 y R3 para IPv4 e IPv6 con OSPF y en R2 se configurara MP-BGP. En esta parte los switches no admitieron OSPF v3. En la parte 4 se configurara la redundancia de primer salto HSRP v2 que nos permitirá un sistema de comunicaciones para detectar un fallo en la red de la manera mas rápida posible y que la red será capaz de recuperarse de la forma mas eficiente y efectiva. En la parte 5 que es de seguridad se protegerá el modo privilegiado usando el algoritmo de encripcion SCRYPT, también habilitar AAA y configurar servidor RADIUS.
En la parte 6 de la topología se configurara las funciones de Administracion de Red, se ajustara NTP maestro en R2, configurar Syslog, configurar SNMPv2.
Es muy importante el desarrollo de cada etapa donde podemos colocar en práctica todo el conocimiento adquirido en el diplomado, cada tema es muy interesante porque nos permite comprender la importancia de profundizar los conocimientos en administración de red.

1. ESCENARIO 1

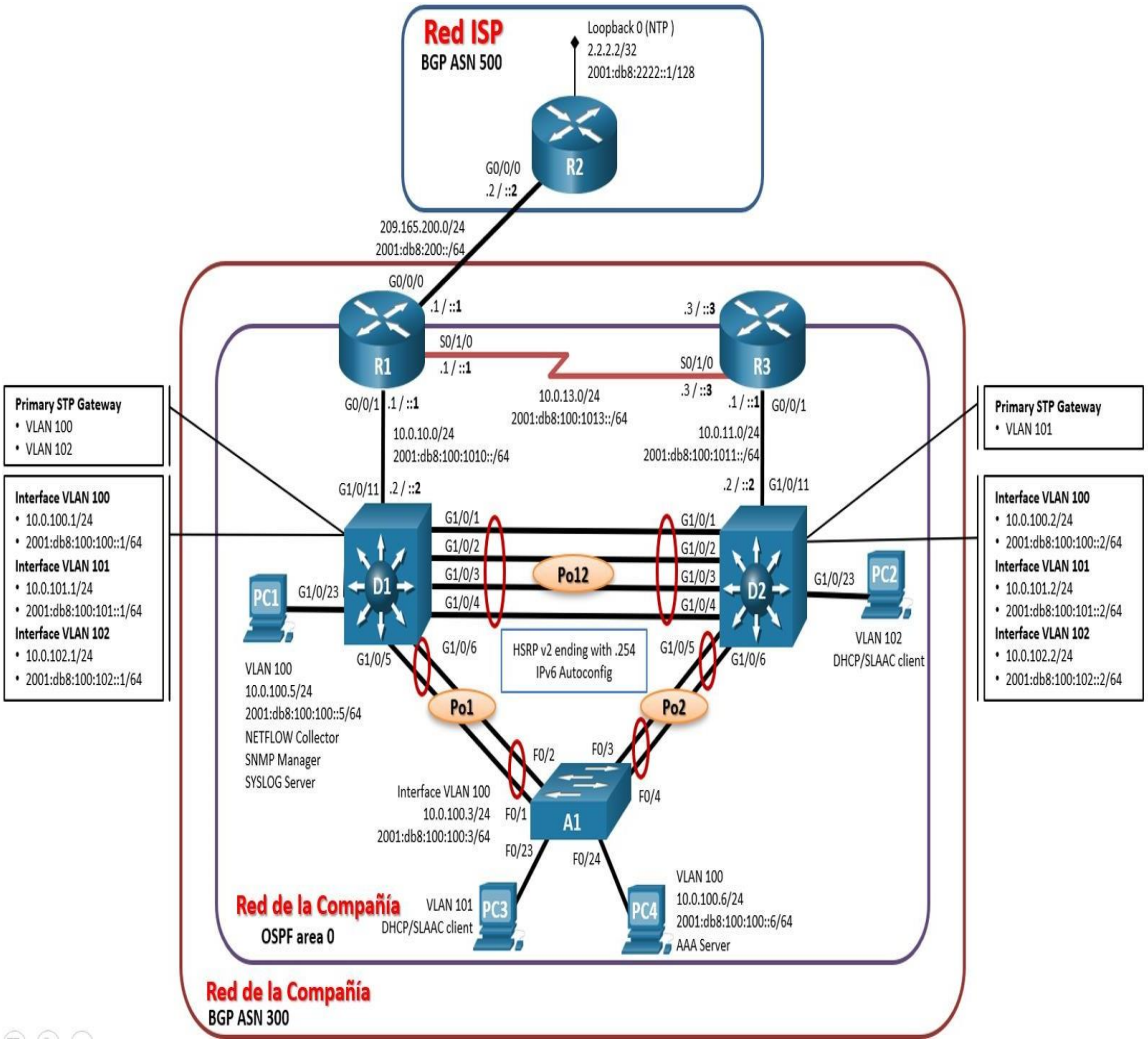

Figura 1. Escenario 1

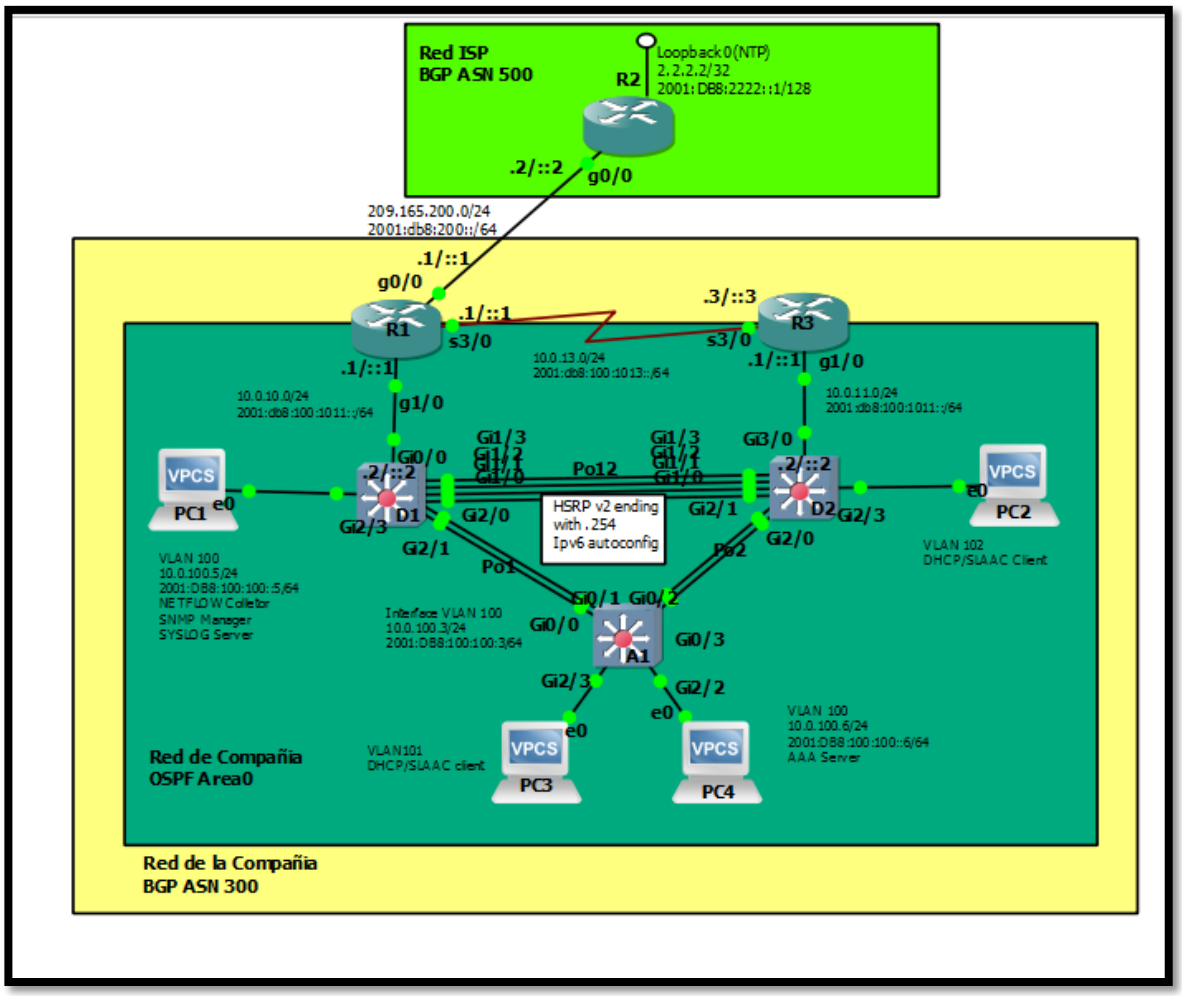

Figura 2. Escenario 1 en GNS3

Tabla 1. Direccionamiento en GNS3

Disp	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S3/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	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	G1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S3/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G0/1	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	G3/0	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

ESCENARIO 1

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.

DESARROLLO

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.

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:

Configurar los parámetros básicos para cada dispositivo

Router R1

```
Router>ena
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#banner motd # Realizado por Javier Montenegro UNAD CCNP #
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
R1(config-if)#ip address 209.165.200.255 255.255.255.254
Bad mask /31 for address 209.165.200.255
R1(config-if)#ex
```

```
R1(config)#interface g0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface g1/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config)#interface s3/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

Router R2

```
Router>ena
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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
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
R2(config)#
```

Router R3

```
Router>ena
Router#config 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 g1/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s3/0
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
```

Switch D1

```
Switch>ena
Switch#config 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 g0/1
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 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)#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-route 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 g0/1-3
D1(config-if-range)#shutdown
D1(config-if-range)#interface range g1/0/12-24
D1(config-if-range)#shutdown
D1(config-if-range)#interface range g1/1/1-4
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#interface vlan 999
```

D1(config-if)#ip address 10.0.99.10 255.255.255.0
D1(config-if)#ipv6 address
D1(config-if)#fe80::d1:3
link-local D1(config-if)#ipv6
address
D1(config-if)#2001:db8:100:99::1/64
D1(config-if)#no shutdown
D1(config-if)#exit

Switch D2

```
Switch>ena
Switch#config 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 g3/0
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-route 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 g0/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface g2/2
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range g3/1-3
D2(config-if-range)#shutdown
D2(config)#exit
D2(config)#interface vlan 999
D2(config-if)#ip address 10.0.99.11 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:99::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

Switch A1

```
Switch>ena
```

```
Switch#config t
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
enter
Switch>ena
Switch#config 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
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range g1/0-3
A1(config-if-range)#shutdown
A1(config)#interface range g2/0-1
A1(config-if-range)#shutdown
A1(config)#interface range g3/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#interface vlan 999
A1(config-if)#ip address 10.0.99.12 255.255.255.0
A1(config-if)#ipv6 address fe80::d1:5  link-local
```

```
A1(config-if)#ipv6 address 2001:db8:100:99::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
```

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

c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.(se configura PC4)

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

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

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces deinterconexión entre switches

Switch A1

```
A1(config)#interface range g1/0-3
A1(config-if-range)# switchport trunk encapsulation dot1q
A1(config-if-range)# switchport mode trunk
A1(config-if-range)# switchport trunk native vlan 999
A1(config-if-range)# no shutdown
A1(config-if-range)#interface vlan 999
A1(config-if)#no shutdown
A1(config-if)#interface range g2/3
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 100
A1(config-if-range)#interface range g2/2
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 101
A1(config-if-range)#exit
```

Switch D1

```
D1>ena
D1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface range G1/0-3,G2/0-1
D1(config-if-range)# switchport trunk encapsulation dot1q
D1(config-if-range)# switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)# no shutdown
D1(config-if-range)#interface vlan 999
D1(config-if)#no shutdown
D1(config-if)#interface range G2/3
D1(config-if-range)#switchport mode access
D1(config-if-range)#switchport access vlan 100
```

Switch D2

```
D2>ena
D2#conf term
```

Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#interface range G1/0-3,G2/0-1
D2(config-if-range)# switchport trunk encapsulation dot1q
D2(config-if-range)# switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)# no shutdown
D2(config-if-range)#interface vlan 999
D2(config-if)#no shutdown
D2(config-if)#
D2(config-if)#interface range G2/3
D2(config-if-range)#switchport mode access
D2(config-if-range)#switchport access vlan 102
D2(config-if-range)#switchport access vlan

2.2 Habilite enlaces trunk 802.1Q entre:

- D1 and D2
- D1 and A1D2 and A1

Switch D1
D1(config)#interface range G1/0-3,G2/0-1
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#exit

Switch D2
D2(config)#interface range G1/0-3,G2/0-1
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#exit

Switch A1
A1(config)#interface range g0/0-3
switchport trunk native vlan 999
A1(config-if-range)#switchport trunk allowed vlan 100
A1(config-if-range)#switchport trunk allowed vlan 101

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP) Use Rapid Spanning Tree (RSPT)

A1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree mode rapid-pvst

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.

Switch D1

```
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
```

Switch D2

```
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
```

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

Switch D1

```
D1(config)#interface range g1/0-3
D1(config-if-range)#shutdown
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#exit
D1(config)#interface port-channel 12
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#interface range g1/0-3
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range g2/0-1
D1(config-if-range)#shutdown
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#exit
D1(config)#interface range g2/0-1
D1(config-if-range)#shutdown
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#exit
D1(config)#interface port-channel 1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#exit
D1(config)#interface range g1/0-3
```

D1(config-if-range)#no shutdown
D1(config-if-range)#interface range g2/0-1
D1(config-if-range)#shutdown
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)# exit

Switch A1
A1(config)#interface range G0/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
A1(config-if-range)#exit
A1(config)#interface port-channel 2
A1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
A1(config-if)#swit
chport trunk native vlan 999
A1(config-if)#exit
A1(config)#interface range G0/0-1
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range G0/2-3
A1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
A1(config-if-range)#exit
A1(config)#interface port-channel 12
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#exit
A1(config)#interface range G0/0-1
A1(config-if-range)#shutdown
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#exit
A1(config)#interface port-channel 1
A1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#Interface GigabitEthernet0/1, A1(config-if)#exit
A1(config)#interface range G0/2-3
A1(config-if-range)#no shutdown

Switch D2
D2(config)#interface range g1/0-3
D2(config-if-range)#shutdown

```
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D2(config-if-range)#exit
D2(config)#interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)#interface range g1/0-3
D2(config-if-range)#no shutdown
D2(config-if-range)#interface range g2/0-1
D2(config-if-range)#shutdown
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#exit
D2(config)#interface port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)#interface range g2/0-1
D2(config-if-range)#no shutdown
D2(config-if-range)#interface range g1/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#exit
D2(config)#interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)#interface range g1/0-3
D2(config-if-range)#no shutdown
```

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).

Switch A1

```
A1(config)#interface range G2/3
A1(config-if-range)#switch mode access
A1(config-if-range)#switch access vlan 101
A1(config-if-range)# interface range G2/2
```

A1(config-if-range)#switch mode access
A1(config-if-range)#switch access vlan 100
A1(config-if-range)#exit

Switch D1
D1(config-if)#interface range G2/3
D1(config-if-range)#switch mode access
D1(config-if-range)#switch access vlan 100
D1(config-if-range)#interface range G2/2
D1(config-if-range)#switch mode access
D1(config-if-range)#switch access vlan 102
D1(config-if-range)#exit

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

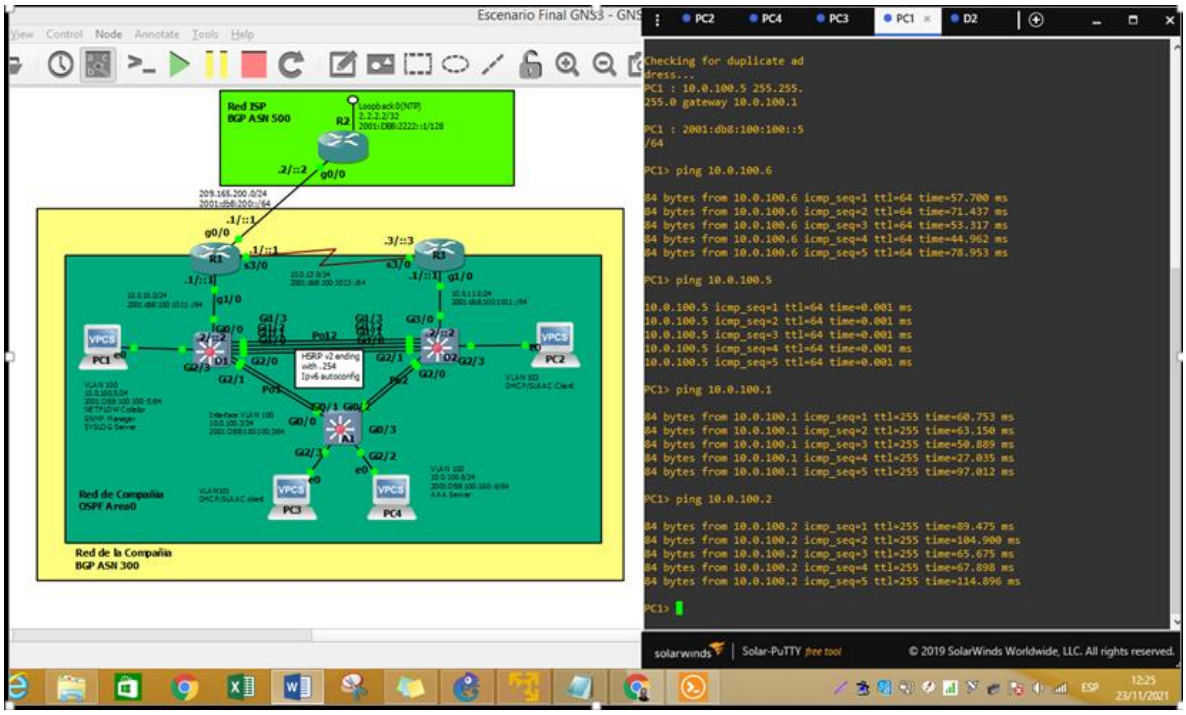

Figura 3. PC1 pings.

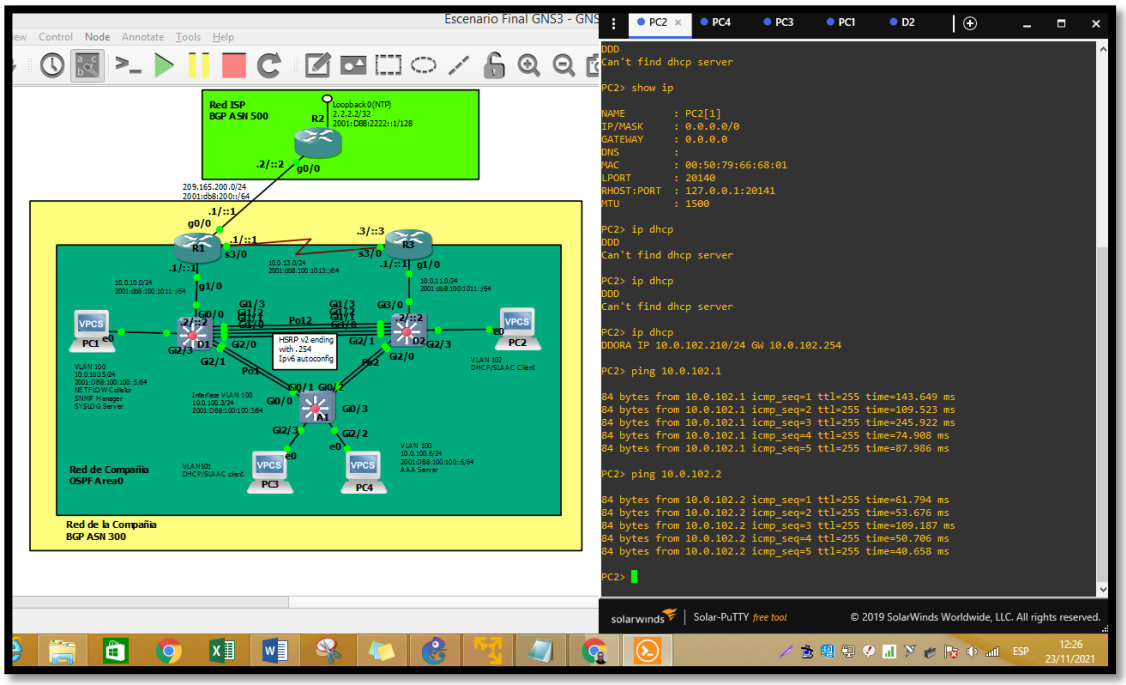

Figura 4. PC2 pings

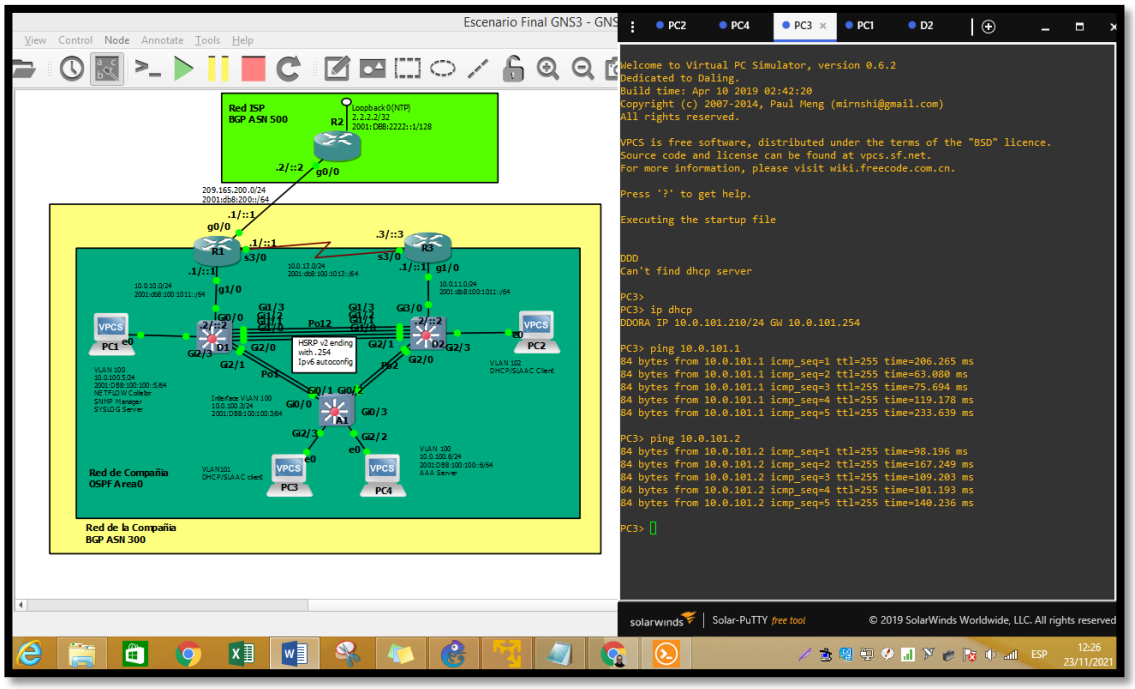

Figura 5. PC3 pings.

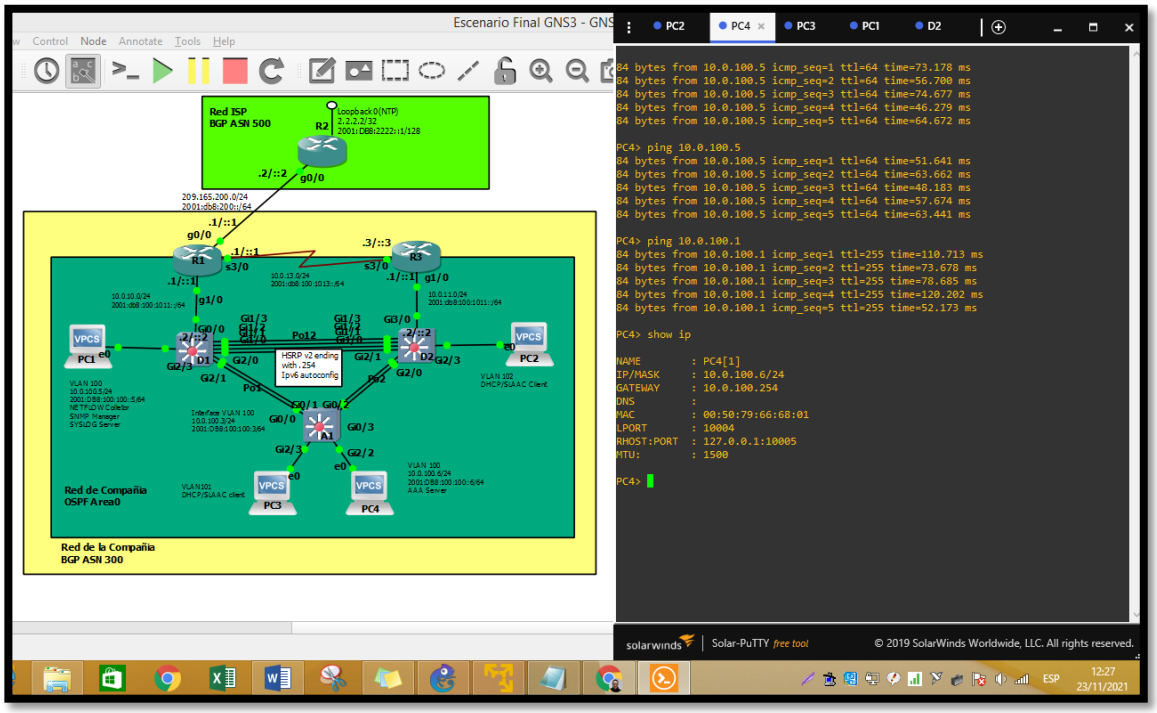

Figura 6. PC4 pings

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

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

Router R1

```
R1(config)#router ospf 4
R1(config-router)# router-id 0.0.4.1
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate
R1(config-router)# exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
```

Switch D2

```
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
D2(config-router)# network 10.0.100.0 0.0.0.255 area 0
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface g1/0/11
D2(config-router)# exit
```

Router R3

```
R3>ena
R3#conf term
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)# 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)# exit
*Nov 23 18:30:24.419: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial3/0
from LOADING to FULL, Loading Done
R3(config-router)# exit
```

Switch D1

```
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
D1(config-router)# network 10.0.100.0 0.0.0.255 area 0
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0
D1(config-router)# passive-interface default
D1(config-router)# no passive-interface g1/0/11
D1(config-router)# exit
```

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

3.2 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

Router R1

```
R1(config-router)# exit
R1(config)#ipv6 router ospf 6
```

```
R1(config-rtr)# router-id 0.0.6.1
R1(config-rtr)# default-information originate
R1(config-rtr)# exit
R1(config)#interface g1/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
R1(config)#interface s3/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
```

Switch D1

****Comando OSPF en swicth no lo soporta GNS3***

```
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
 no passive-interface g0/0
 exit
interface g0/0
 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
```

Router R3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)# router-id 0.0.6.3
R3(config-rtr)# exit
R3(config)#interface g1/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#interface s3/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
```

Switch D2

****Comando OSPF en swicth no lo soporta GNS3***

```
ipv6 router ospf 6
 router-id 0.0.6.132
 passive-interface default
 no passive-interface g3/0
 exit
interface g3/0
 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
```

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).

Router R2

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
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)#  neighbor 209.165.200.225 activate
R2(config-router-af)#  no neighbor 2001:db8:200::1 activate
```

```
R2(config-router-af)#  network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#  network 0.0.0.0
R2(config-router-af)#  exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)#  no neighbor 209.165.200.225 activate
R2(config-router-af)#  neighbor 2001:db8:200::1 activate
R2(config-router-af)#  network 2001:db8:2222::/128
R2(config-router-af)#  network ::/0
R2(config-router-af)#  exit-address-family
*Nov 23 18:28:25.875: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
R2(config-router-af)#  exit-address-family
*Nov 23 18:28:28.631: %BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up
R2(config-router-af)#  exit-address-family
```

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

Router R1

```
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
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)#  neighbor 209.165.200.226 activate
R1(config-router-af)#  no neighbor 2001:db8:200::2 activate
R1(config-router-af)#  network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#  exit-address-family
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)#  no neighbor 209.165.200.226 activate
R1(config-router-af)#  neighbor 2001:db8:200::2 activate
R1(config-router-af)#  network 2001:db8:100::/48
R1(config-router-af)#  exit-address-family
R1(config-router)#exit
```

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

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

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

Switch D1

```
D1(config)#ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
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
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#track 4 ip sla 4
D1(config-track)# delay down 10 up 15
D1(config-track)# exit
D1(config)#track 6 ip sla 6
D1(config-track)# delay down 10 up 15
D1(config-track)# exit
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 104 track 4 decrement 60
D1(config-if)# standby 106 ipv6
*Nov 23 20:31:36.096: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state
```

```
Standby -> Active autoconfig
D1(config-if)# standby 106 priority 150
D1(config-if)# standby 106 preempt
D1(config-if)# standby 106 track 6 decrement 60
D1(config-if)# exit
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
D1(config-if)# standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track
*Nov 23 20:34:26.650: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state
Standby -> Active6 decrement 60
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# standby ver
*Nov 23 20:34:43.961: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state
Standby -> Activesion 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
D1(config-if)# standby 126 ipv6 autoconfig
D1(config-if)# standby 126
*Nov 23 20:35:22.544: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state
Standby -> Activepriority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60
D1(config-if)# exit
D1(config)#end
```

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.

Switch D2

```
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency
% Incomplete command.
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)# frequency
% Incomplete command.
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
D2(config)#track 6 ip sla 6
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
*Nov 23 20:46:13.468: %TRACK-6-STATE: 4 ip sla 4 state Down -> Up
D2(config-track)# exit
```

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

Swicht D1

```
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 104 track 4 decrement 60
D1(config-if)# standby 106 ipv6
*Nov 23 20:31:36.096: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state
Standby -> Active autoconfig
D1(config-if)# standby 106 priority 150
D1(config-if)# standby 106 preempt
D1(config-if)# standby 106 track 6 decrement 60
D1(config)#interface vlan 101
D1(config-if)# standby version 2
D1(config-if)# standby 114 ip 10.0.101.254
D1(config-if)# standby 114 preempt
D1(config-if)# standby 114 track 4 decrement 60
D1(config-if)# standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track
*Nov 23 20:34:26.650: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state
Standby -> Active6 decrement 60
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# standby ver
*Nov 23 20:34:43.961: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state
Standby -> Activesion 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
D1(config-if)# standby 126 ipv6 autoconfig
D1(config-if)# standby 126
*Nov 23 20:35:22.544: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state
```

Standby -> Activepriority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60
D1(config-if)# exit
D1(config)#end

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

Switch D2
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 1

```
*Nov 23 21:10:21.665: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Speak
-> Standby06 track 6 decrement 60
*Nov 23 21:10:41.328: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak
-> Standby
D2(config-if)# exit
D2(config)#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 de
*Nov 23 20:49:57.936: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -
> Activecrement 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 tra
*Nov 23 20:50:34.947: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak
-> Active
*Nov 23 20:50:35.841: %IPV6_ND-4-DUPLICATE_OPTIMISTIC: Duplicate
address FE80::5:73FF:FEA0:74 on Vlan101ck 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 124 track 4 decrement 60
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
D2(config-if)# exit
D2(config)#end
```

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

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT. Contraseña: cisco12345cisco

Router R1
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
Router R3
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
Switch D1
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
Switch D2
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
Switch A1
A1(config)#enable algorithm-type SCRYPT secret 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

Router R1
R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
Router R3
R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
Switch D1
D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
Switch D2
D2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
Router R2
username : raduser privilege 15 algorithm-type SCRYPT secret upass123

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

Router R1
R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

R1(config-radius-server)# key $trongPass
R1(config-radius-server)# exit

Router R3
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass

Switch D1
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)# exit

Switch D2
D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)# key $trongPass
D2(config-radius-server)# exit

Switch A1
A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit

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.

Router R1
R1(config)#aaa authentication login default group radius local
R1(config)#endR1(config)#aaa new-model

Router R3
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#end

Switch D1
D1(config)#aaa authentication login default group radius local
D1(config)#

Switch D2
D2(config)#aaa authentication login default group radius local

D2(config)#end

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

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).Cierre e inicie sesión en todos los dispositivos (excepto R2 con el usuario: raduser y la contraseña: upass123.)En todos los dispositivos:

Nombre de usuario Local: sadmin
Nivel de privilegio 15
Contraseña: cisco12345cisco

Router R2
R2(config)#enable algorithm-type SCRYPT secret upass123
R2(config)#$duser privilege 15 algorithm-type SCRYPT secret upass123
R2(config)#aaa new-model
R2(config)#radius server RADIUS
R2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R2(config-radius-server)# key $trongPass
R2(config-radius-server)# exit
R2(config)#aaa authentication login default group radius local
R2(config)#end

Figura 7. Verificacion AAA R1

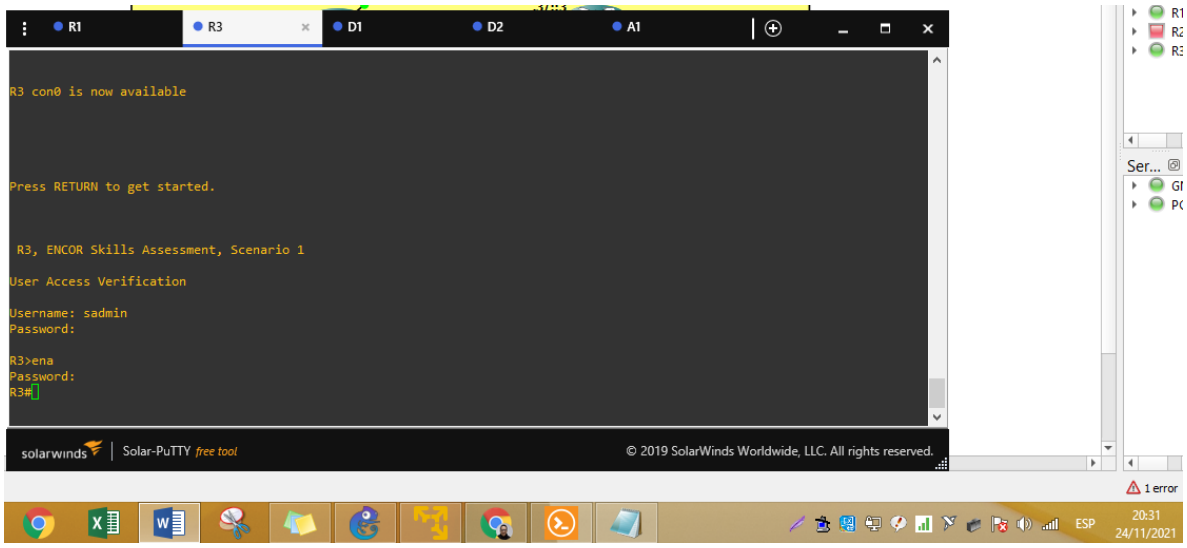

Figura 8. Verificacion AAA R3

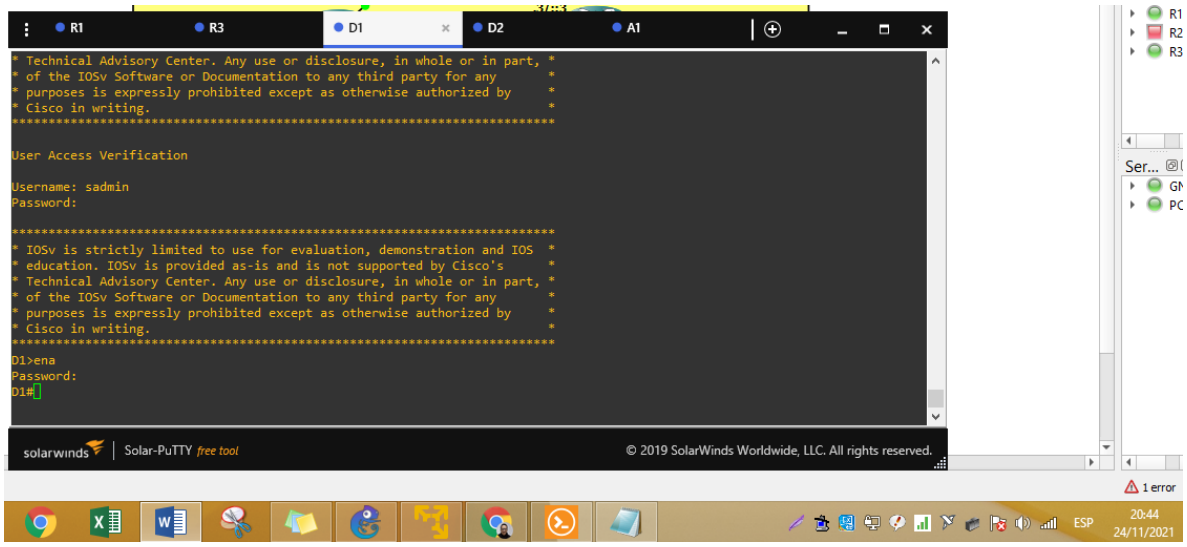

Figura 9. Verificacion AAA D1

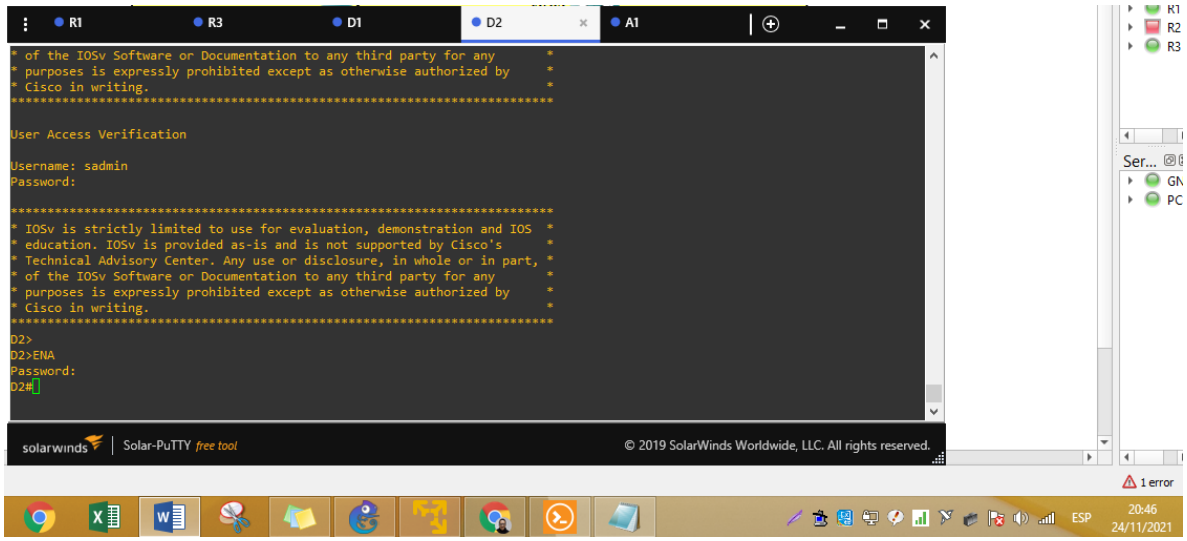

Figura 10. Verificacion AAA D2

Figura 11. Verificacion AAA A1

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:

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

[todos los dispositivos]
clock set 21:34:00 24 Nov 2021

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

Router R2
R2(config)#ntp master 3
R2(config)#end

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

Router R1
R1(config)#ntp server 2.2.2.2
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)# permit host 10.0.100.5
R1(config-std-nacl)# exit

Switch D2
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

Router R3
R3(config)#ntp server 10.0.10.1
R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
R3(config)# logging on

Switch A1

```
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
```

Switch D1

```
D1(config)#ntp server 10.0.10.1
D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
D1(config)# logging on
```

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

Router R1

```
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
//D2//
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#  permit host 10.0.100.5
D2(config-std-nacl)#  exit
% Invalid input detected at '^' marker.
D2(config)# snmp-server enable traps ospf
D2(config)#end
```

Router R3

```
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#  permit host 10.0.100.5
R3(config-std-nacl)#  exit
```

Switch A1

```
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#  permit host 10.0.100.5
A1(config-std-nacl)#  exit
```

Switch D1

```
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#  permit host 10.0.100.5
D1(config-std-nacl)#  exit
```

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

Router R1

```
R1(config)# snmp-server ifindex persist
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)#end
```

Switch D2

```
D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server enable traps config

D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps config
                          ^
% Invalid input detected at '^' marker.

D1(config)# snmp-server enable traps ospf
D1(config)#end
```

Router R3

```
R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end
```

Switch A1

```
A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)# snmp-server ifindex persist
A1(config)# snmp-server enable traps config
                           ^
% Invalid input detected at '^' marker.
A1(config)# snmp-server enable traps ospf
A1(config)#end
```

CONCLUSIONES

En el escenario propuesto se desarrollaron las seis partes de la actividad donde se pudo adquirir mucho conocimiento avanzado en administración y resolución de problemas en la redes. Un aspecto importante fue el uso del simulador GNS3 que es una herramienta.muy adecuada para crear un ambiente virtual con toda la estructura que el escenario CCNP demando, además que con la maquina virtual me enseño una nueva forma de realizar los laboratorios al implementar cada parte de la actividad.En el escenario se pueden concluir y analizar varios aspectos importantes en cada fase porque pudimos aplicar cada tema gradualmente en la topología propuesta de la red de la compañía.

La construcción de la topología en la primera parte nos lleva a implementar en GNS3 las imágenes y la IOS necesaria para obtener el switch y el router adecuador para montar el escenario.Al configurar los puertos como esta indicado en la actividad ya pudimos aplicar los protocolos que nos permitirian trabajar con los switches y los routers. En la actividad se configura en forma secuencial los siguientes procesos como son la configuración de la vlan nativa, la configuración de los puertos tanto troncales como de acceso, la activación del protocolo RSTP con la configuración del root- bridge, las activaciones de los canales para Etherchannel.Todos estos puntos importantes para realizar la primera convergencia de los switches con los pcs permitiendo que las vlans se pudieran comunicar e incluyendo la configuración de DHCP. En los routers se configuro OSPF v2 y v3 que me permitio trabajar para IPv4 y IPv6 en los routers R1 y R3.Ahora bien en R1 y R2 se configuro el protocolo BGP para el sistema autónomo 500 y 300.

En el punto numero cuatro se configuro IP SLA que es el acuerdo de nivel de servicio del Protocolo de Internet la cual es una herramienta integrada en el software Cisco IOS muy interesante para los profesionales de TI que permite el monitoreo continuo de varios aspectos de la red para ayudar con la resolución de problemas.En el punto cinco se pudo aplicar unos de los aspectos mas importantes en las redes el tema de seguridad. El colocar un nivel alto de seguridad nos da tranquilidad de que podemos estar sobre una red de confianza.

Y por ultimo configuramos las funciones de administración de red donde aplicaremos NTP que nos permitio sincronizar la hora autorizada universal para observar un evento en la hora real y activamos SYSLOG que es el encargado de almacenar las alarmas.Este proceso muy importante para ver los eventos y alarmas de la red sincronizadas para realizar soluciones exactas.

El escenario me permitio ahondar en cada fase realizar las investigaciones pertinentes para la actividad, fortaleciéndome como un profesional de TI viendo

aspectos muy importantes que me enseño el diplomado de profundización de CCNP porque gracias al simulador en GNS3 pude comprobar en la practica todo el conocimiento adquirido en el desarrollo del escenario.

BIBLIOGRÁFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

EDGEWORTH, Bradley. GARZA Ramiro., GOOLEY, Jason. HUCABY, David. “CISCO Press: Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 1072-1075. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

EDGEWORTH, Bradley, GARZA Ramiro., GOOLEY, Jason, HUCABY, David. “CISCO Press: VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 186-215. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: OSPF. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 353-367. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley. GARZA Ramiro., GOOLEY, Jason, HUCABY, David. “CISCO Press: Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 120-138. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 223-230. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: BGP. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 392-409. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley, GARZA Ramiro., GOOLEY, Jason, HUCABY, David. “CISCO Press: Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 810-839. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8