DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE LIBARDO GUEVARA PARRADO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE LIBARDO GUEVARA PARRADO

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*
ACACIAS
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

ACACIAS, 29 de noviembre de 2021

AGRADECIMIENTOS

Quiero agradecer a mi madre Alcira Parrado Alvares, mi padre Luis Alberto Guevara y a mi hermano William Ferney Guevara Parrado. Por todo el apoyo recibido de parte de ellos tanto en lo económico, emocional y motivacional, dado que han influenciado y permitido a lo largo de los años universitarios superar las diferentes dificultades para llegar así al desarrollo del presente documento.

También quiero agradecer al grupo de docentes de la Universidad Nacional Abierta y a Distancia (UNAD). quienes, a lo largo de los años estudiantiles con sus conocimeintos, habilidades y apoyo me permitieron superar las diferentes etapas y alcanzar los resultados esperados.

Por último, agradezco a los diferentes compañeros y amigos por el apoyo brindado a lo largo de las diferentes etapas académicas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

INTERFACES LOOPBACK: Es una interfaz de tipo virtual, la cual representa el mismo dispositivo mediante una creación de Software, esta se suele utilizar para transmitir datos con el propio host dirigiendo el tráfico hacia ellos mismos.

PROTOCOLO DE ENRUTAMIENTO: Es el protocolo secuencial el cual especifica la forma en la que los routers, se comunican permitiendo crear rutas dando dirección de tráfico para él envió de paquetes de información.

PROTOCOLO OSPF: Es un protocolo enlace-estado el cual fue creado para implementarlo en las redes con IP, basado en algoritmo con el camino más corto. Es decir que, por medio del algoritmo, se busca la ruta más corta en la comunicación.

PROTOCOLO EIGRP: Es un protocolo el cual está basado en CISCO, tipo vector distancia dual con un desarrollo algorítmico de actualizaciones difusas enviando información a los dispositivos routers de la misma área.

IPV4: Es un protocolo de internet de cuarta generación, el cual permite la conexión en red con un direccionamiento de 32 bits en 4 bloques de 3 caracteres cada uno.

IPV6: Es el protocolo actualizado del IPv4, el cual resuelve los inconvenientes de agotamiento de direcciones, teniendo como principio el internet sin límites.

TOPOLOGÍA DE RED: Es la forma en la que se realiza la organización de una red, teniendo en cuenta la forma en la que se diseña en plano físico.

ELECTRÓNICA: Es una rama de la física la cual se centra en la especialización de ingeniería, dedicada al estudio y creación de nuevas tecnologías y solución de problemas en relación con el flujo de cargas eléctricas en función a una acción.

RESUMEN

Por medio del desarrollo del escenario practico relacionado al diplomado de profundización CCNP CISCO, generando las habilidades necesarias para resolver situaciones relacionadas a la ingeniería electrónica para el manejo de redes locales y empresariales. Creando una topología de red, configurando ajustes básicos de los dispositivos presentes dando un direccionamiento de las interfaces, teniendo en cuenta que la red permita la accesibilidad completa entre los dispositivos y que el host tenga soporte en la puerta de enlace, validando las conexiones necesarias para dar solución a lo propuesto y obtener un correcto enrutamiento.

Se configuran los dispositivos en capa 2, configurando las interfaces como troncales y puentes raíz para que se pueda verificar la conmutación, se configuran parámetros de tipo OSPF y redundancia de primer salto para los hosts, al igual se configuran mecanismos de seguridad y funciones administrativas. se desarrolla la actividad en la herramienta GNS3 la cual tiene una interfaz que permite la emulación y configuración de dispositivos de redes virtuales y reales, utilizando 3 Routers, 3 switches y 4 PCs según la imagen dada de la topología de red del escenario, donde se configura cada dispositivo con el fin de que tenga estos los protocolos de enrutamientos adecuados para que la red tenga accesibilidad de extremo a otro, conmutando la configuración de los hosts y las puertas de enlace default Gateway, teniendo los protocolos configurados según la tabla de direccionamiento, teniendo así un correcto enrutamiento.

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

ABSTRACT

Through the development of the practical scenario related to the CCNP CISCO deepening diploma, generating the necessary skills to solve situations related to electronic engineering for the management of local and business networks. Creating a network topology, configuring basic settings of the devices present giving an addressing of the interfaces, taking into account that the network allows complete accessibility between the devices and that the host has support in the gateway, validating the necessary connections to give a solution to the proposal and obtain a correct routing.

Layer 2 devices are configured, configuring the interfaces as trunks and root bridges so that switching can be verified, OSPF type parameters and first-hop redundancy are configured for the hosts, as well as security mechanisms and administrative functions. The activity is carried out in the GNS3 tool, which has an interface that allows the emulation and configuration of virtual and real network devices, using 3 Routers, 3 switches and 4 PCs according to the given image of the network topology of the scenario, where configures each device so that it has the appropriate routing protocols so that the network has end-to-end accessibility, switching the configuration of the hosts and the default gateway, having the protocols configured according to the addressing table, thus having a correct routing.

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

INTRODUCCIÓN

En el presente documento se presenta el trabajo de Diplomado de profundización CISCO prueba de habilidades practicas CCNP. El cual permite fortalecer las habilidades y capacidades dando solución a diferentes situaciones presentes en las redes empresariales tipo LAN y WAN. El correcto desarrollo permite obtener el título de ingeniero, por medio del diplomado de profundización teniendo en cuenta los diferentes requisitos que se deben cumplir para ello. Dado que al terminar el diplomado se tendrán múltiples habilidades sobre el manejo de comandos IOS, dando así soluciones como profesional en redes escalables.

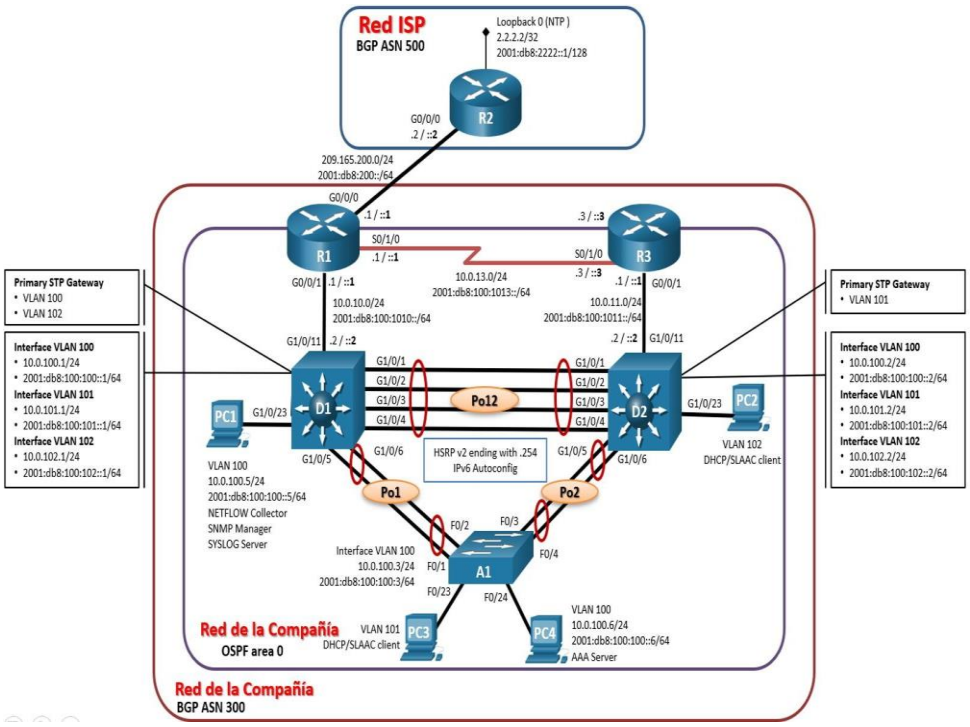
El documento presenta el desarrollo de 6 etapas practicas las cuales ponen a prueba las habilidades adquiridas de comprensión y desarrollo de situaciones relacionadas con el Networking. Se realiza la interacción virtual con los diferentes e-learning y software, desarrollando las temáticas relacionadas a las redes LAN y WAN como los protocolos de enrutamiento avanzados de Routing, en los protocolos EIGRP Y OSPF. Brindando soluciones en el ámbito de enrutamiento avanzado tenido en cuenta las configuraciones en capa 2, configuraciones básicas de direccionamiento de DHCP y SLAAC, al igual que mecanismos de seguridad a los dispositivos con el fin de que permita la autenticación de identidad a los usuarios, al igual que la implementación de funciones administrativas de red básicas.

Se desarrolla el laboratorio en la herramienta GNS3 de acuerdo con un escenario propuesto, utilizando 3 Routers, 3 switches y 4 PCs, contrayendo la topología de red, de acuerdo a una serie de pasos, configurando cronológicamente parámetros básicos de direccionamiento, con el fin de que se pueda tener una accesibilidad completa entre los hosts.

DESARROLLO

ESCENARIO PROPUESTO
Topología de la Red para trabajar según documento

Figura 1:Topología escenario 1



Fuente: Prueba de habilidades CCNP

Tabla 1:Tabla de 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/	EUI-64

			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

Fuente: Prueba de habilidades CCNP

Objetivos

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

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

Part 3: Configurar los protocolos de enrutamiento

Part 4: Configurar la redundancia del primer salto (**no se entrega aún)

Part 5: Configurar la seguridad (**no se entrega aún)

Part 6: Configurar las características de administración de red (** no se entrega aún)

Escenario

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.

Nota: Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global **sdm prefer dual-ipv4-and-ipv6 default**. Cambiar la plantilla

requerirá el reinicio del switch.

Recursos necesarios

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

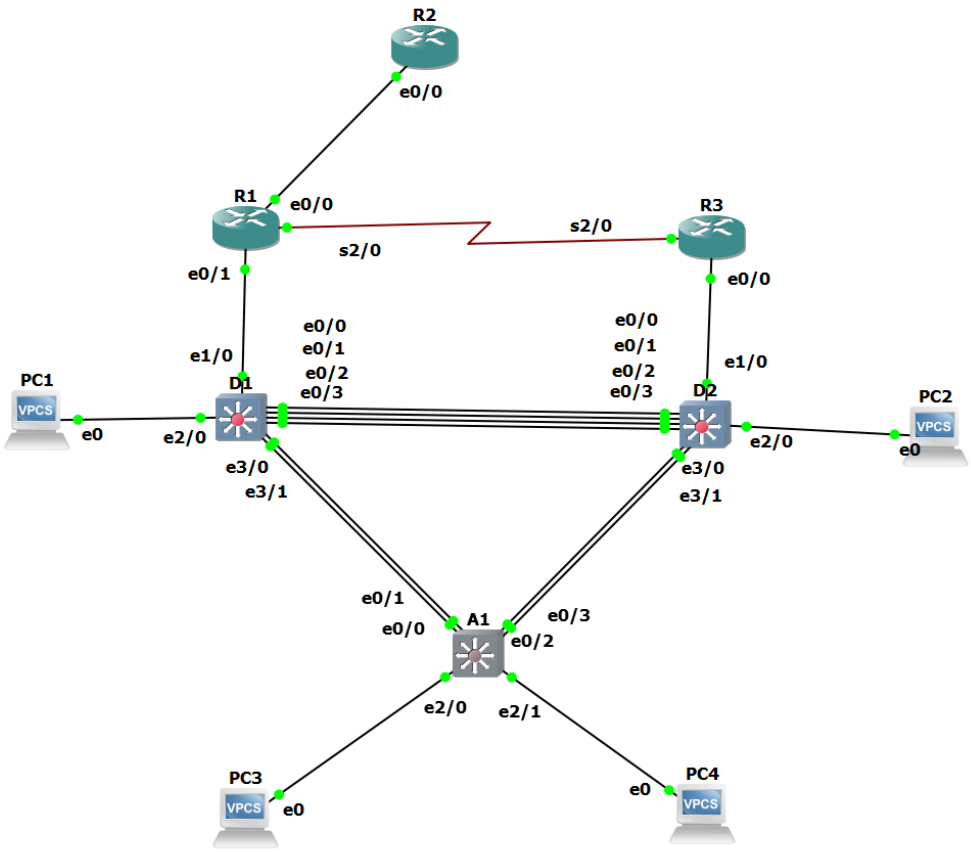
PARTE 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

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

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

Rta: Se realiza el cableado de los equipos según la topología requerida y con los cables necesarios

Figura 2:Topología solicitada, realizada en GNS3



PASO 2: Configurar los parámetros básicos para cada dispositivo.

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

Tabla 2: Configuración parámetros básicos dispositivos

Configuración parámetros básicos dispositivos	
R1	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de configuración (configure terminal).

	IOU5(config)#hostname R1 R1(config)#ipv6 unicast-routing R1(config)#no ip domain lookup R1(config)#banner motd # R1 Enter TEXT message. End with the character '#'. ENCOR Skills Assessment, Scenario 1 # R1(config)#line con 0 R1(config-line)#exec-timeout 0 0 R1(config-line)#logging synchronous R1(config-line)#exit R1(config)#interface e0/0 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 e0/1 R1(config-if)#ip address 10.0.10.1 255.255.255.0 R1(config-if)#ipv6 address fe80::1:2 link-local R1(config-if)#ipv6 address 2001:db8:100:1010::1/64 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface s2/0 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
R2	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de

	configuración (configure terminal). IOU4(config)#hostname R2 R2(config)#ipv6 unicast-routing R2(config)#no ip domain lookup R2(config)#banner motd # R2 Enter TEXT message. End with the character '#'. 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 e0/0 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
R3	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de configuración (configure terminal). IOU6(config)#hostname R3 R3(config)#ipv6 unicast-routing R3(config)#no ip domain lookup R3(config)#banner motd # R3

	Enter TEXT message. End with the character '#'. 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 e0/0 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)# R3(config)#interface s2/0 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
D1	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de configuración (configure terminal). IOU1(config)#hostname D1 D1(config)#ip routing D1(config)#ipv6 unicast-routing D1(config)#no ip domain lookup D1(config)#banner motd # D1 Enter TEXT message. End with the character '#'. 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 e1/0 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 *Nov 20 15:29:04.691: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up *Nov 20 15:29:05.697: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up D1(config)#interface vlan 100 D1(config-if)#ip address 10.0.100.1 255.255.255.0 D1(config-if)#ipv6 address fe80::d1:2 link-local D1(config-if)#ipv6 address 2001:db8:100:100::1/64 D1(config-if)#no shutdown D1(config-if)#exit

	D1(config)#interface vlan 101 D1(config-if)#ip address 10.0.101.1 255.255.255.0 D1(config-if)#ipv6 address fe80::d1:3 link-local D1(config-if)#ipv6 address 2001:db8:100:101::1/64 D1(config-if)#no shutdown D1(config-if)#exit D1(config)#interface vlan 102 D1(config-if)#ip address 10.0.102.1 255.255.255.0 D1(config-if)#ipv6 address fe80::d1:4 link-local D1(config-if)#ipv6 address 2001:db8:100:102::1/64 D1(config-if)#no shutdown D1(config-if)#exit D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109 D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254 D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109 D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254 D1(config)#ip dhcp pool VLAN-101 D1(dhcp-config)#network 10.0.101.0 255.255.255.0 D1(dhcp-config)#default-router 10.0.101.254 D1(dhcp-config)#exit D1(config)#ip dhcp pool VLAN-102 D1(dhcp-config)#network 10.0.102.0 255.255.255.0 D1(dhcp-config)#default-router 10.0.102.254 D1(dhcp-config)#exit
D2	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de configuración (configure terminal). IOU2(config)#hostname D2

	D2(config)#ip routing D2(config)#ipv6 unicast-routing D2(config)#no ip domain lookup D2(config)#banner motd # D2 Enter TEXT message. End with the character '#'. 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 e1/0 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-router 10.0.101.254 D2(dhcp-config)#exit D2(config)#ip dhcp pool VLAN-102 D2(dhcp-config)#network 10.0.102.0 255.255.255.0 D2(dhcp-config)#default-router 10.0.102.254 D2(dhcp-config)#exit

A1	Para realizar las configuraciones básicas de debe ingresar a la consola del dispositivo, luego ingresar al modo privilegiado (enable) y ya por último al modo de configuración (configure terminal). IOU3(config)#hostname A1 A1(config)#no ip domain lookup A1(config)#banner motd # A1 Enter TEXT message. End with the character '#'. 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

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.

Tabla 3: configuración direccionamientos host

direccionamiento de los host PC 1 y PC 4	
PC 1	PC 4
Comando enviado IP 10.0.100.5/24 10.0.100.254	Comando enviado IP 10.0.100.6/24 10.0.100.254

Fuente: Elaboración propia

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:

Tabla 4: Configurar la capa 2 de la red y el soporte de Host

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
	Código de configuración para las interfaces trunk 802.1Q D1(config)#Interface range e0/0-3 D1(config-if-range)#Switchport trunk encapsulation dot1q D1(config-if-range)#Switchport mode trunk D1(config-if-range)#exit D1(config)#Interface range e3/0-1	

<table>
<tr><td></td><td colspan="2">D1(config-if-range)#Switchport trunk encapsulation dot1q
D1(config-if-range)#Switchport mode trunk

D2(config)#Interface range e0/0-3
D2(config-if-range)#Switchport trunk encapsulation dot1q
D2(config-if-range)#Switchport mode trunk
D2(config-if-range)#exit
D2(config)#Interface range e3/0-1
D2(config-if-range)#Switchport trunk encapsulation dot1q
D2(config-if-range)#Switchport mode trunk
D2(config-if-range)#exit

A1(config)#Interface range e0/0-3
A1(config-if-range)#Switchport trunk encapsulation dot1q
A1(config-if-range)#Switchport mode trunk
A1(config-if-range)#exit</td></tr>
<tr><td rowspan="2">2.2</td><td>En todos los switches cambie la VLAN nativaen los enlaces troncales.</td><td>Use VLAN 999 como la VLAN nativa.</td></tr>
<tr><td colspan="2">Código de configuración para VLAN nativa

D1(config)#Interface range e0/0-3
D1(config-if-range)#Switchport trunk native vlan 999
D1(config-if-range)#exit
D1(config)#Interface range e3/0-1
D1(config-if-range)#Switchport trunk native vlan 999

D2(config)#Interface range e0/0-3
D2(config-if-range)#Switchport trunk native vlan 999
D2(config-if-range)#exit
D2(config)#Interface range e3/0-1
D2(config-if-range)#Switchport trunk native vlan 999

A1(config)#Interface range e0/0-3
A1(config-if-range)#Switchport trunk native vlan 999</td></tr>
<tr><td rowspan="2">2.3</td><td>En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)</td><td>Use Rapid Spanning Tree (RSPT).</td></tr>
<tr><td colspan="2">Configuración protocol Rapid Spanning-Tree (RSTP)</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">D1(config)#spanning-tree mode rapid-pvst

D2(config)#spanning-tree mode rapid-pvst</td></tr>
<tr><td rowspan="2">2.4</td><td>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 casode falla del puente raíz (root bridge).</td><td>Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.</td></tr>
<tr><td colspan="2">Código de configuración ingresado para los puentes raíz RSTP
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary

D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary</td></tr>
<tr><td>2.5</td><td>En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.</td><td>Use los siguientes números de canales:
• D1 a D2 – Port channel 12
• D1 a A1 – Port channel 1
• D2 a A1 – Port channel 2</td></tr>
<tr><td></td><td colspan="2">Configuracion EtherChannels LACP
D1(config)#interface range e0/0-3
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#exit
D1(config)#interface range e3/0-1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active

D2(config)#interface range e0/0-3</td></tr>
</table>

	D2(config-if-range)#channel-protocol lacp D2(config-if-range)#channel-group 12 mode active D2(config-if-range)#exit D2(config)#interface range e3/0-1 D2(config-if-range)#channel-protocol lacp D2(config-if-range)#channel-group 2 mode active A1(config)#interface range e0/0-1 A1(config-if-range)#channel-protocol lacp A1(config-if-range)#channel-group 1 mode active A1(config-if-range)#exit A1(config)#interface range e0/2-3 A1(config-if-range)#channel-protocol lacp A1(config-if-range)#channel-group 2 mode active	
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que seconectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, comose muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
	Configuración puertos de acceso del host D1(config)#interface e2/0 D1(config-if)#switchport mode access D1(config-if)# switchport access vlan 100 D1(config-if)# spanning-tree portfast D1(config-if)#no shutdown D2(config)#interface e2/0	

	D2(config-if)#switchport mode access D2(config-if)# switchport access vlan 102 D2(config-if)# spanning-tree portfast D2(config-if)# no shutdown D2(config-if)#exit A1(config)#interface e2/0 A1(config-if)#switchport mode access A1(config-if)# switchport access vlan 101 A1(config-if)# spanning-tree portfast A1(config-if)# no shutdown A1(config-if)# exit A1(config)#interface e2/1 A1(config-if)#switchport mode access A1(config-if)# switchport access vlan 100 A1(config-if)# spanning-tree portfast A1(config-if)#no shutdown A1(config-if)# exit	
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y debenrecibir 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

Desarrollo 2.7

Se verificación de los servicios DHCP IPv4.

Figura 3:Verificación DHCP PC2

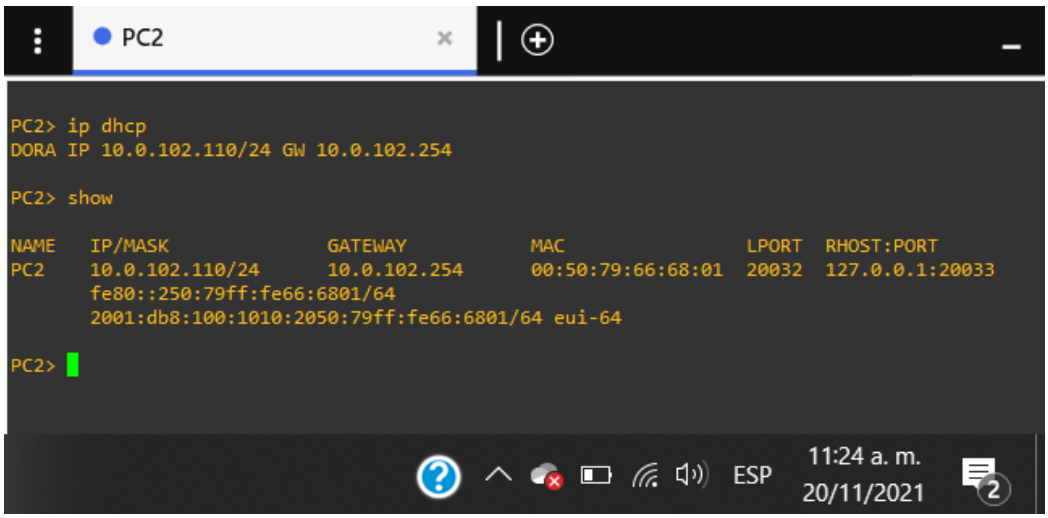
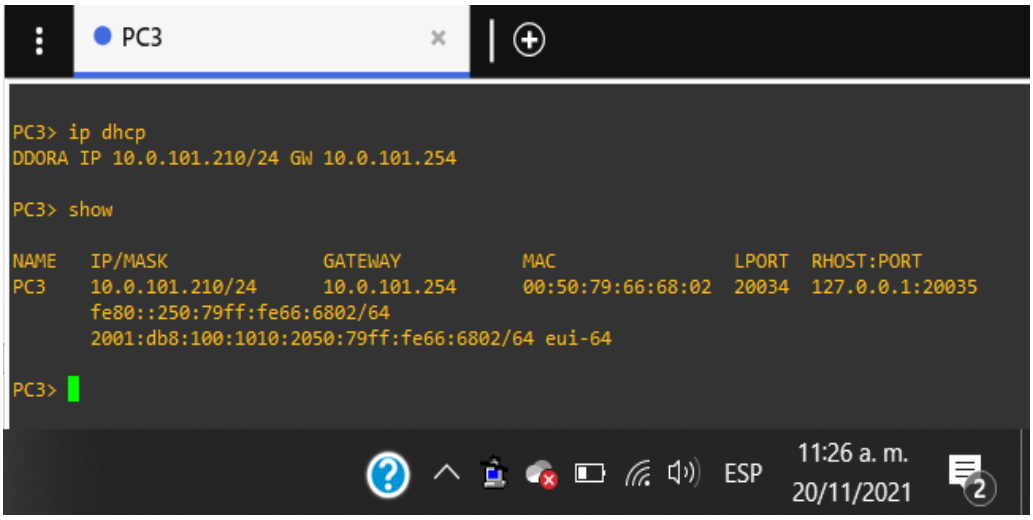


Figura 4:Verificación DHCP PC3



Desarrollo 2.8

Se verifica conectividad de la LAN local

Figura 5:Ping conectividad LAN desde PC1

Figura 6:Ping conectividad LAN desde PC2

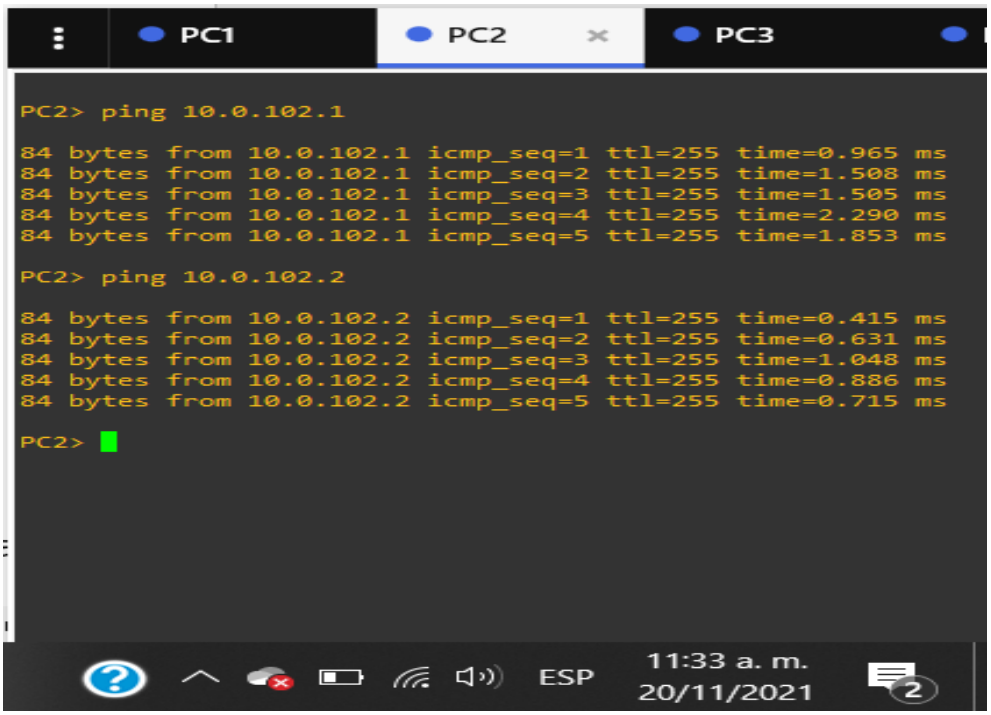


Figura 7:Ping conectividad LAN desde PC3

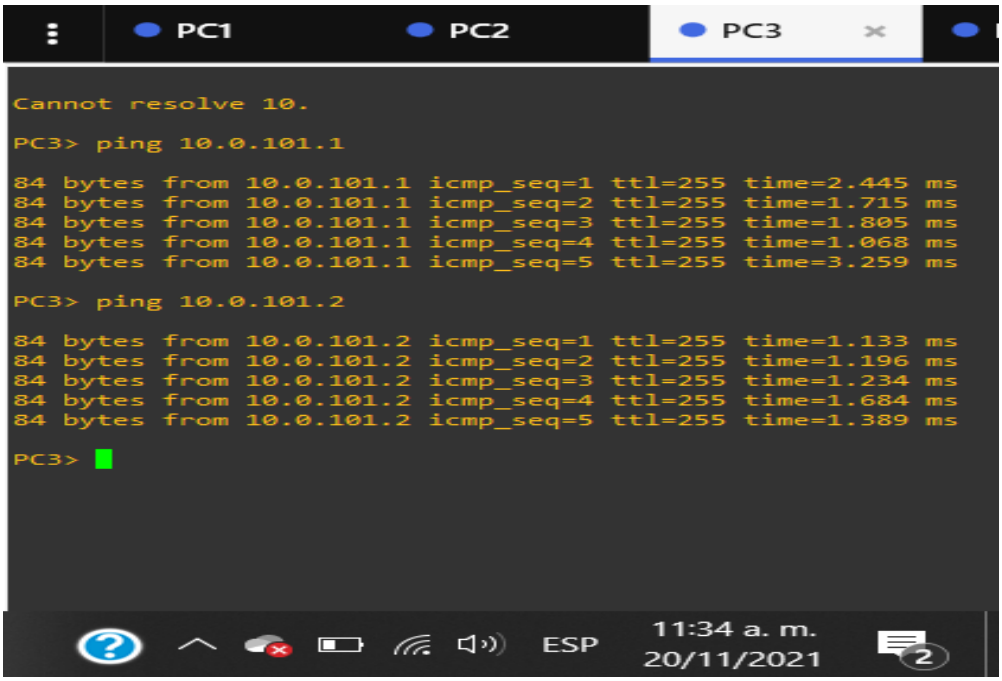


Figura 8:Ping conectividad LAN desde PC4

PARTE 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

Tabla 5:Configuración los protocolos de enrutamiento

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.

Se desarrolla la parte 3, por medio de los siguientes comandos

Tabla 6: Comandos y configuración realizada en la parte 3

Configuración protocolos de enrutamiento parte 3	
R1	Se realiza la configuración de OSPF con process

	ID 4. ID 6 asignando router-IDs Se realiza la configuración de interfaces Null 0 con rutas ipv4- ipv6 Se configura una relación vecino vecino IPv4 e IPv6 con R2 en ASN 300 R1(config)#ip route 0.0.0.0 0.0.0.0 e0/0 R1(config)#router ospf 4 R1(config-router)# router-id 0.0.4.1 R1(config-router)# network 10.0.10.0 0.0.0.255 area 0 R1(config-router)# network 10.0.13.0 0.0.0.255 area 0 R1(config-router)# default-information originate R1(config-router)#exit 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 e0/1 R1(config-if)#ipv6 ospf 6 area 0 R1(config-if)# exit R1(config)#interface s2/0 R1(config-if)# R1(config-if)# R1(config-if)#ipv6 ospf 6 area 0 R1(config-if)# exit R1(config)#ip route 10.0.0.0 255.0.0.0 null0 R1(config)#ipv6 route 2001:db8:100::/48 null0 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
R2	Se configuran rutas estáticas predeterminadas a través de la interfaz Loopback 0 Se configura una relación vecino vecino IPv4 e IPv6 con R2 en ASN 500 Se configura y habilita una relación de vecino IPv4 e IPv6 con R1 en ASN 300 R2(config)#ip route 0.0.0.0 0.0.0.0 e0/0 R2(config)#ipv6 route ::/0 e0/0 R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 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
R3	Se realiza la configuración de OSPF con process ID

	4. ID 6 asignando router-IDs 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 R3(config)#ipv6 router ospf 6 R3(config-rtr)# router-id 0.0.6.3 R3(config-rtr)# exit R3(config)#interface e0/0 R3(config-if)#ipv6 ospf 6 area 0 R3(config-if)# exit R3(config)#interface s2/0 R3(config-if)#ipv6 ospf 6 area 0 R3(config-if)# exit
D1	Se realiza la configuración de OSPF con process ID 4. ID 6 asignando router-IDs Se realiza la configuración para anunciar todas las redes directamente conectadas / VLANs en Área 0. Se configura para deshabilitar las publicaciones OSPFv3 menos e1/0 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 e1/0 D1(config-router)#exit D1(config)#ipv6 router ospf 6 D1(config-rtr)# router-id 0.0.6.131 D1(config-rtr)# passive-interface default D1(config-rtr)# no passive-interface e1/0 D1(config-rtr)#exit D1(config)#interface e1/0 D1(config-if)#ipv6 ospf 6 area 0

	D1(config-if)# exit D1(config)#interface vlan 100 D1(config-if)# ipv6 ospf 6 area 0 D1(config-if)# exit D1(config)#interface vlan 101 D1(config-if)# ipv6 ospf 6 area 0 D1(config-if)# exit D1(config)#interface vlan 102 D1(config-if)# ipv6 ospf 6 area 0 D1(config-if)# exit
D2	Se realiza la configuración de OSPF con process ID 4. ID 6 asignando router-IDs Se realiza la configuración para anunciar todas las redes directamente conectadas / VLANs en Área 0. Se configura para deshabilitar las publicaciones OSPFv3 menos e1/0 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 D2(config-router)# no passive-interface e1/0 D2(config-router)#exit D2(config)#ipv6 router ospf 6 D2(config-rtr)# router-id 0.0.6.132 D2(config-rtr)# passive-interface default D2(config-rtr)# no passive-interface D2(config-rtr)# no passive-interface e1/0 D2(config-rtr)#exit D2(config)#interface e1/0 D2(config-if)#ipv6 ospf 6 area 0 D2(config-if)# exit D2(config)#interface vlan 100 D2(config-if)# ipv6 ospf 6 area 0 D2(config-if)# exit D2(config)#interface vlan 101

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

Comprobación parte 3

Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Figura 9:Validación interfaz loopback desde D1

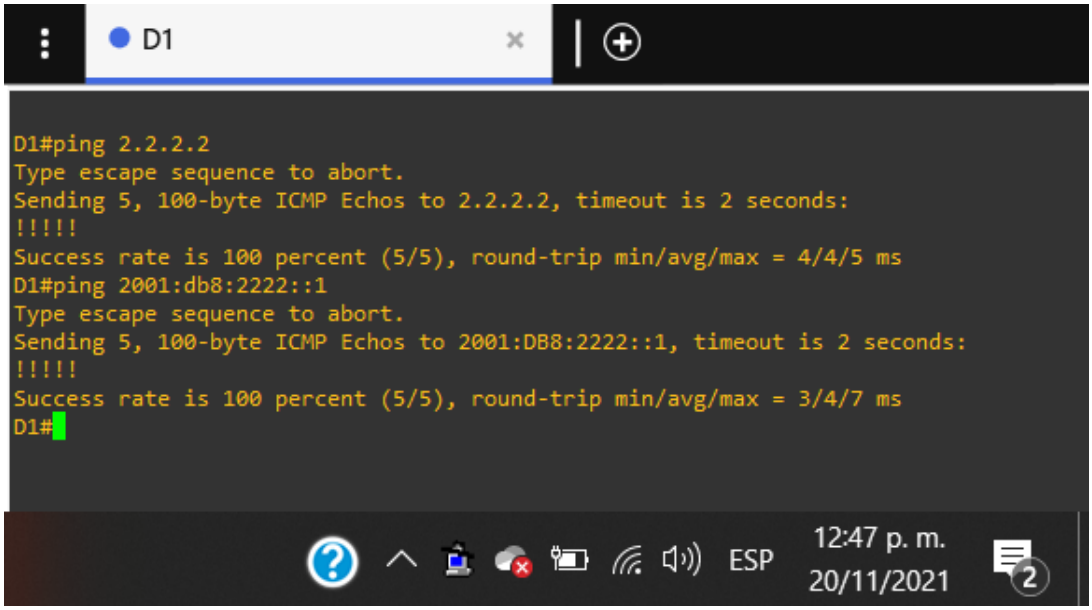


Figura 10:Validación interfaz loopback desde D2

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red dela Compañía”.

Las tareas de configuración son las siguientes:

Tabla 7:Configuracion redundancia primer salto

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 lotanto, 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.

	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, suprioridad 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.

Tabla 8: Comandos utilizados en la configuración, redundancia del primer salto

Configuración de la redundancia del Primer Salto (First Hop Redundancy) para D1 Y D2	
D1	Se crea dos IP SLAs con número 4 para IPv4 y 6 para IPv6 Se configura la SLA con el fin de valida la disponibilidad de la interfaz R1 e1/0 cada 5 segundos Se realiza la programación SLA para que esta se implemente de forma inmediata Se crea una IP SLA objeto para las IP SLA 4 y IP SLA 6 donde los objetos rastreados deben notificar a D1 el estado de la IP SLA cuando esta cambie Se realiza la configuración de HSRPv2 con IPv4 y IPv6 en las VLAN 100,101,102 D1(config)#ip sla 4 D1(config-ip-sla)# icmp-echo 10.0.11.1 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:db8:100:1011::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)#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 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 6 decrement 60 D1(config-if)# exit D1(config)#interface vlan 102 D1(config-if)# standby version 2 D1(config-if)# standby 124 ip 10.0.102.254 D1(config-if)# standby 124 priority 150 D1(config-if)# standby 124 preempt D1(config-if)# standby 124 track 4 decrement 60 D1(config-if)# standby 126 ipv6 autoconfig D1(config-if)# standby 126 priority 150 D1(config-if)# standby 126 preempt D1(config-if)# standby 126 track 6 decrement 60 D1(config-if)#exit
D2	Se crea dos Ip SLAs con nuemero 4 para IPv4 y 6 para IPv6 Se configura la SLA con el fin de valida la disponibilidad de la interfaz R3 e1/0 cada 5 segundos Se realiza la programación SLA para que esta se implemente de forma inmediata Se crea una IP SLA objeto para las IP SLA 4 y IP SLA 6 donde los objetos rastreados deben notificar a D2 el estado de la IP SLA cuando esta cambie Se realiza la configuración de HSRPv2 con IPv4 y IPv6 en las VLAN 100,101,102 D2(config)#ip sla 4 D2(config-ip-sla)# icmp-echo 10.0.11.1 D2(config-ip-sla-echo)# frequency 5 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 5 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 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 106 track 6 decrement 60 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 decrement 60 D2(config-if)# standby 116 ipv6 autoconfig D2(config-if)# standby 116 priority 150 D2(config-if)# standby 116 preempt D2(config-if)# standby 116 track 6 decrement 60 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

*Validación parte 4 r*edundancia del Primer Salto

Figura 11:Verificación redundancia en D1

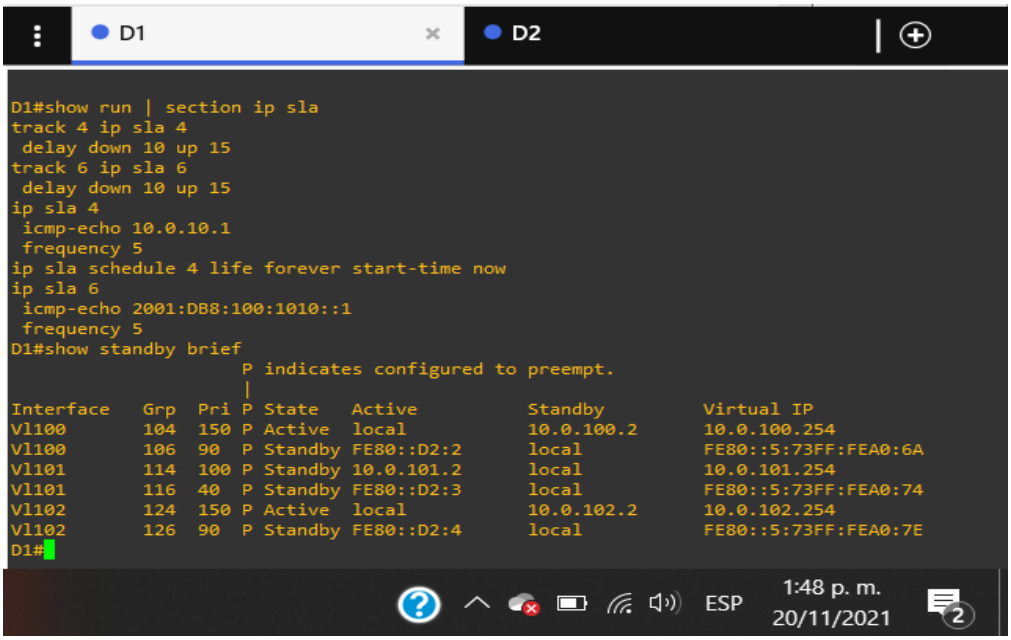
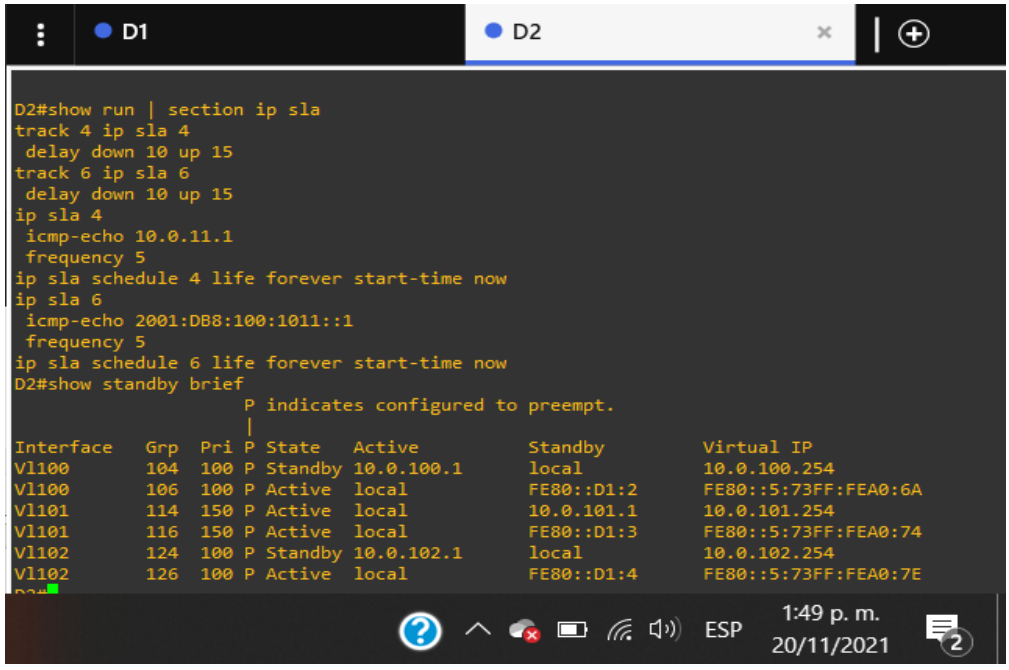


Figura 12:Verificación redundancia en D2



PARTE 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los

dispositivos de la topología. Las tareas de configuración son las siguientes:

Tabla 9: Desarrollo parte 5 seguridad de los dispositivos

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmode inscripción SCRYPT.	Contraseña: **cisco12345cisco**
	R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco	
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de inscripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
	R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco R2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco D2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	

	A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	
5.3	En todos los dispositivos (excepto R2),habilite AAA.	Habilite AAA.
	Se realiza la habilitación en los dispositivos AAA R1(config)#aaa new-model R2(config)#aaa new-model R3(config)#aaa new-model D1(config)#aaa new-model D2(config)#aaa new-model A1(config)#aaa new-model	
5.4	En todos los dispositivos (excepto R2),configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
	Configuración especificaciones del servidor RADIUS R1(config)#radius server RADIUS R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813 R1(config-radius-server)# key $trongPass R3(config)#radius server RADIUS R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813 R3(config-radius-server)# key $trongPass D1(config)#radius server RADIUS D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813	

	D1(config-radius-server)# key $trongPass D2(config)#radius server RADIUS D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813 D2(config-radius-server)# key $trongPass A1(config)#radius server RADIUS A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813 A1(config-radius-server)# key $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 servidoresRADIUS • De lo contrario, utilice la base de datos local.
	R1(config)#aaa authentication login default group radius local R3(config)#aaa authentication login default group radius local D1(config)#aaa authentication login default group radius local D2(config)#aaa authentication login default group radius local A1(config)#aaa authentication login default group radius local	
5.6	Verifique el servicio AAA en todos losdispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y la contraseña: **upass123**.

Verificación configuración realizada según los ítems dados en la parte 5

Figura 13:Verificación parte 5 en R1

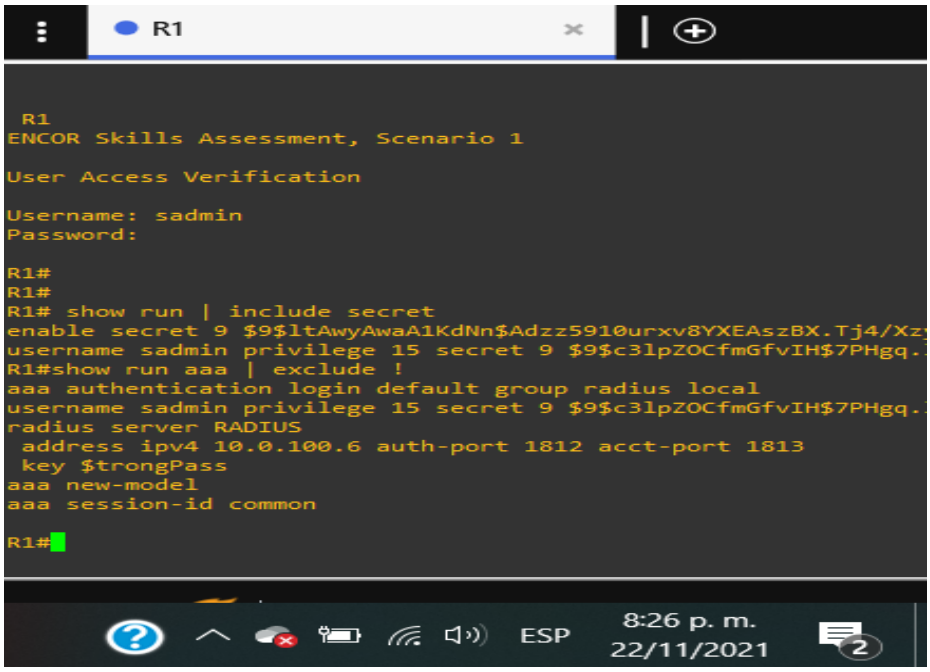


Figura 14:Verificación parte 5 en R3

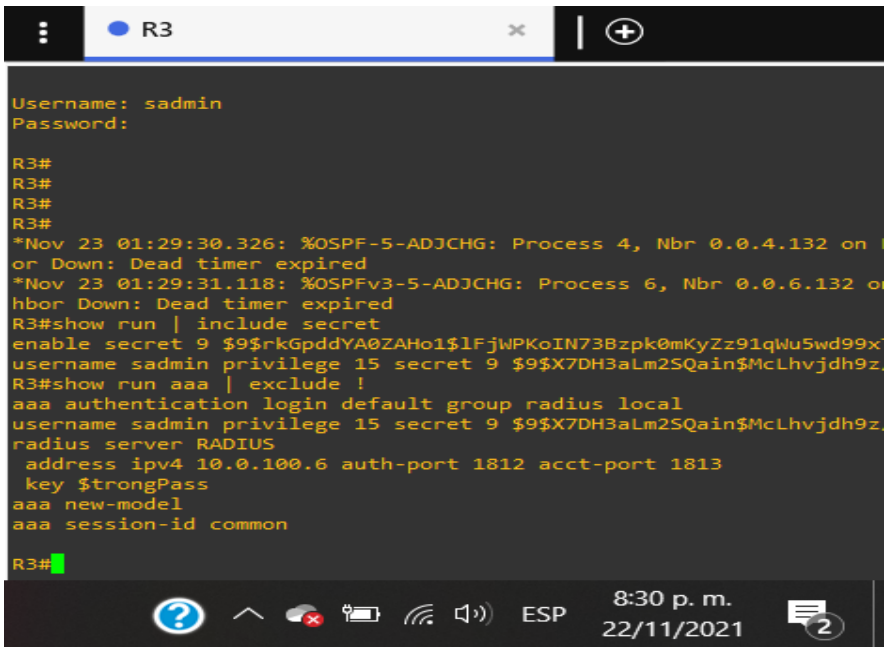


Figura 15:Verificación parte 5 en D1

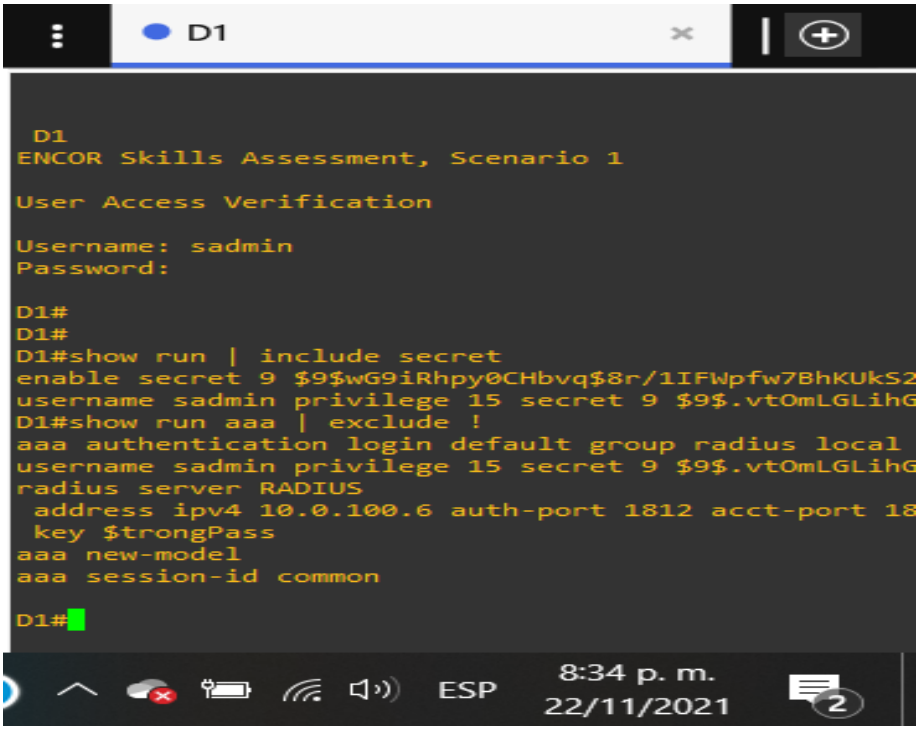


Figura 16:Verificación parte 5 en D2

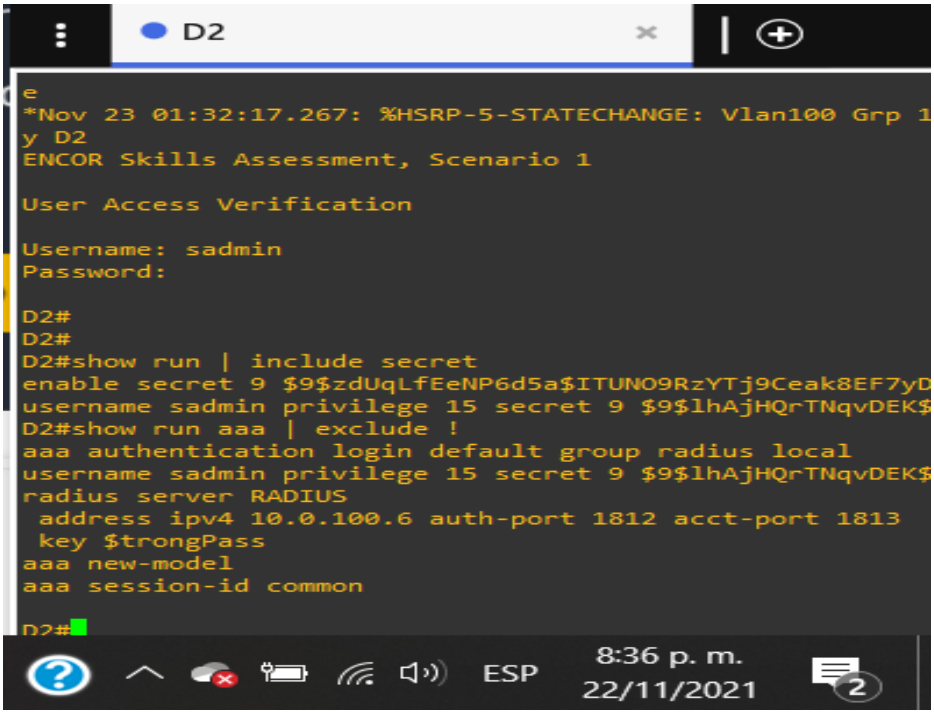
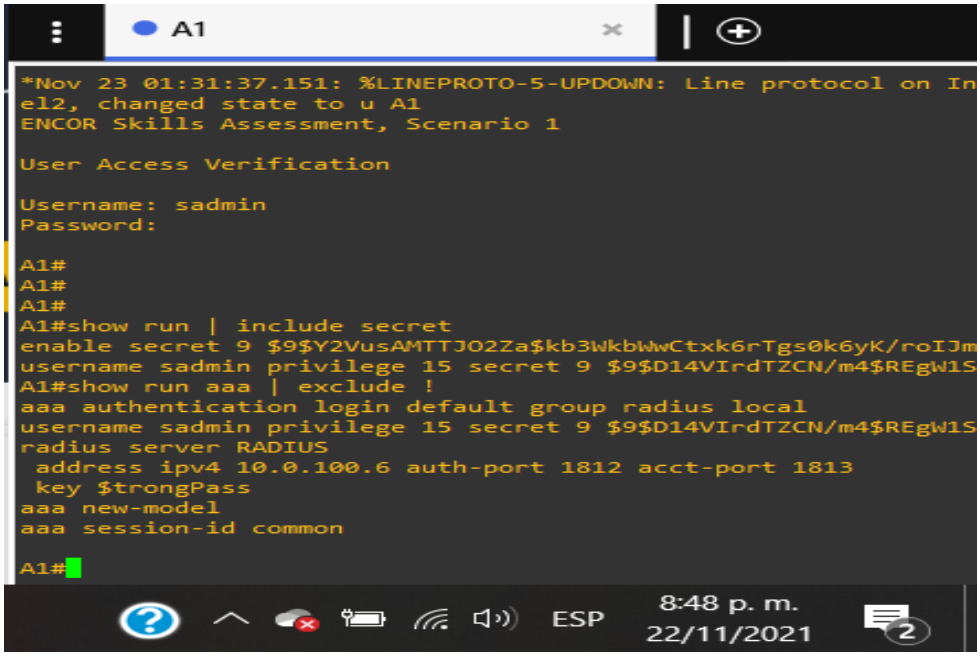


Figura 17:Verificación parte 5 en A1



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:

Tabla 10: Configure las funciones de administración Red

Tarea #	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel deestrato 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 losdispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos losdispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura(Read-Only). • Limite el acceso SNMP a la dirección IP de laPC1. • Configure el valor de contacto SNMP con sunombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

Desarrollo configuración parte 6

Tabla 11: Códigos utilizados en el desarrollo de los ítems para la parte 6

Configuración funciones de Administración de Red	
R2	El reloj UTC ya está configurado Para verificar el reloj envió el comando R2#show clock 02:47:13.783 UTC Tue Nov 23 2021 Se configura el NTP maestro de nivel 3 R2(config)#ntp master 3
R1	El reloj UTC ya está configurado Se realiza la configuración de NTP donde se sincronice con los otros equipos Se configura el Syslogs con un novel WARNING Se configuran los parámetros de SNMPv2 Código utilizado para dar solución a lo requerido 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 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 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)#exit
R3	El reloj UTC ya está configurado Se realiza la configuración de NTP donde se sincronice con los otros equipos Se configura el Syslogs con un novel WARNING Se configuran los parámetros de SNMPv2 Código utilizado para dar solución a lo requerido 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 R3(config)#ip access-list standard SNMP-NMS R3(config-std-nacl)# permit host 10.0.100.5 R3(config-std-nacl)#exit R3(config)#snmp-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)#exit
D1	El reloj UTC ya está configurado Se realiza la configuración de NTP donde se sincronice con los otros equipos Se configura el Syslogs con un novel WARNING Se configuran los parámetros de SNMPv2 Código utilizado para dar solución a lo requerido 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 D1(config)#ip access-list standard SNMP-NMS D1(config-std-nacl)# permit host 10.0.100.5 D1(config-std-nacl)#exit D1(config)#snmp-server contact Cisco 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 D1(config)#snmp-server enable traps ospf D1(config)#exit
D2	El reloj UTC ya está configurado Se realiza la configuración de NTP donde se sincronice con los otros equipos Se configura el Syslogs con un novel WARNING Se configuran los parámetros de SNMPv2 Código utilizado para dar solución a lo requerido D2#configure Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z.

	D2(config)#ntp server 10.0.10.1 D2(config)# logging trap warning D2(config)# logging host 10.0.100.5 D2(config)# logging on D2(config)#ip access-list standard SNMP-NMS D2(config-std-nacl)# permit host 10.0.100.5 D2(config-std-nacl)#exit 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 D2(config)# snmp-server enable traps ospf D2(config)#exit
A1	El reloj UTC ya está configurado Se realiza la configuración de NTP donde se sincronice con los otros equipos Se configura el Syslogs con un novel WARNING Se configuran los parámetros de SNMPv2 Código utilizado para dar solución a lo requerido A1(config)#ntp server 10.0.10.1 A1(config)# logging trap warning A1(config)# logging host 10.0.100.5 A1(config)# logging on A1(config)#ip access-list standard SNMP-NMS A1(config-std-nacl)# permit host 10.0.100.5 A1(config-std-nacl)#exit A1(config)#snmp-server contact Cisco 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 A1(config)# snmp-server enable traps ospf A1(config)#exit

CONCLUSIONES

Es de mencionar que para los laboratorios de CISCO, donde se requiera la utilización de varios dispositivos para simular topologías extensas o configurar en varis capas es mas eficiente el simulador GNS3 respecto al Packet Pracer , dada la interfaz de usuario, variedad de imágenes de dispositivos y la aceptación de diferentes comandos.

Es de resaltar que para las configuraciones cuando se requiera utilizar una interfaz como puerto troncal en un switch se debe enviar el comando para encapsular en Dot1Q, dado que si se activa el modo troncal antes de encapsular el sistema arroja un error y no nos permite realizar bien la configuración.

Cuando se realicen configuraciones de VLAN se debe verificar que estas estén asignadas a un puerto, con el fin de que cambien en el sistema al estado arriba, para que podamos tener un enrutamiento adecuado en la red.

Al configurar los dispositivos en capa 3 se tiene una mayor política de seguridad en la red dado que se configuran usuarios y mecanismo de autenticación permitiendo así tener un control de los dispositivos que quieran acceder a la red, con esto se mitigan las amenazas de seguridad y daños.

BIBLIOGRAFIA

CCNA3 - etherchannel - PAgP y LACP. (2016, 10 diciembre). [Vídeo]. YouTube. https://www.youtube.com/watch?v=7YTL9fH_BH4

Comparación del funcionamiento de la capa 2 en CatOs y cisco IOS system software en catalyst 6500/6000. (2021, 14 julio). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6000-series-switches/12155-101.html

Creación de VLAN de ethernet en switches catalyst. (2021, 14 julio). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/vlan/10023-3.html

Enlace del 802.1Q entre los switches de catalyst que funcionan con CatOS y el software del sistema del cisco IOS. (2018, 2 febrero). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/lan-switching/8021q/8760-67.html

J. (s. f.). Enrutamiento por internet. CCM. Recuperado 29 de noviembre de 2021, de https://es.ccm.net/contents/277-enrutamiento-por-internet

Juniper Networks. (s. f.). 404. Recuperado 29 de noviembre de 2021, de https://www.juniper.net/documentation/en_US/junose15.1/topics/example/simple/+mbgp-disable-default-address-family.html

NAT-PT estático por el ejemplo de la configuración del IPv6. (2020, 24 febrero). Cisco. Recuperado 29 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/113275-nat-ptv6.html

Sepúlveda, M. (2020, 13 diciembre). Configuración de VLANs y protocolo ruteo OSPF para el CCNA 200–301. eClassVirtual - Cursos Cisco en línea. Recuperado 29 de noviembre de 2021, de https://eclassvirtual.com/configuracion-de-vlans-y-protocolo-ruteo-ospf-para-el-ccna-200-301/