DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANTONIO SERRANO LUGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES
NEIVA (HUILA)
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANTONIO SERRANO LUGO

Diplomado de opción de grado presentado para optar el título de INGENIERO EN TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA EN TELECOMUNICACIONES
NEIVA (HUILA)
2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

NEIVA (HUILA), 26 de noviembre de 2021

AGRADECIMIENTOS

Me permito agradecer la tutoría del Director de diplomado Gerardo Granados persona encargada de aconsejar y dirigir el proceso de configuración de la topología asignada y explicaciones en las webs conferencias. De igual manera agradecer al Tutor Hector Julian Parra, el Ingeniero Pedro Torres y las personas encargadas de direccionar el proceso de aprendizaje.

Quiero agradecer a la Institución Educativa Superior Universidad Nacional Abierta y a Distancia UNAD por brindar los medios virtuales, las plataformas, los escritos y diferentes componentes necesarios para la realización del trabajo.

También me permito agradecer a mi familia el acompañamiento durante el proceso del diplomado de profundización cisco CCNP.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Dirección IP: es un código numérico que identifica a equipos o dispositivos de una red. Como un PC o tablet, un router, un servidor web, una impresora de red, un modem, etc. El nombre “IP” viene de las siglas de Internet Protocol. Porque se usa en redes que utilizan el “idioma” (protocolo) de Internet, ya sea una red privada o la propia Internet. La IP es el equivalente informático a la dirección de una casa.

VLAN: (Virtual LAN), o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3 como un router o una switch multicapa L3.

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

OSPF: Open Shortest Path First, Abrir el camino más corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Multicast/Unicast: Multicast se refiere a la entrega de datos de forma simultánea a un grupo de nodos receptores como destino, desde un emisor como origen. Por el contrario, en unicast un emisor se comunica con un único nodo receptor de destino. De tal manera que con unicast, si un emisor necesita comunicarse con 3 nodos receptores, tiene que establecer 3 canales de comunicación. En cambio, multicast permite crear un sólo canal de comunicación para los 3 nodos receptores.

RESUMEN

Se realiza la topología indicada por las guías, con la utilización en la simulación de la aplicación GNS3 y sus componentes descargados como imágenes Switch y Router.

Estas funciones se realizaron siguiendo las instrucciones según las guías, compuesto de dos momentos, siendo el primero un avance y este último el documento final. Además, cuenta con seis (6) puntos a desarrollar, de esta forma adquirir principalmente conocimientos de conmutación, enrutamiento de red, seguridad, administración entre otros.

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

ABSTRACT

The topology indicated by the guides is carried out, with the use in the simulation of the GNS3 application and its downloaded components such as Switch and Router images.

These functions were carried out following the instructions according to the guidelines, composed of two moments, the first being a preview and the latter the final document. In addition, it has six (6) points to develop, in this way to acquire mainly knowledge of switching, network routing, security, administration, among others.

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

INTRODUCCION

En el presente trabajo se propone reforzar los temas relacionados a las configuraciones principales mediante el uso de aplicaciones que simulen la topología de red, adquiriendo conocimientos para el uso en emprendimientos empresariales como personales.

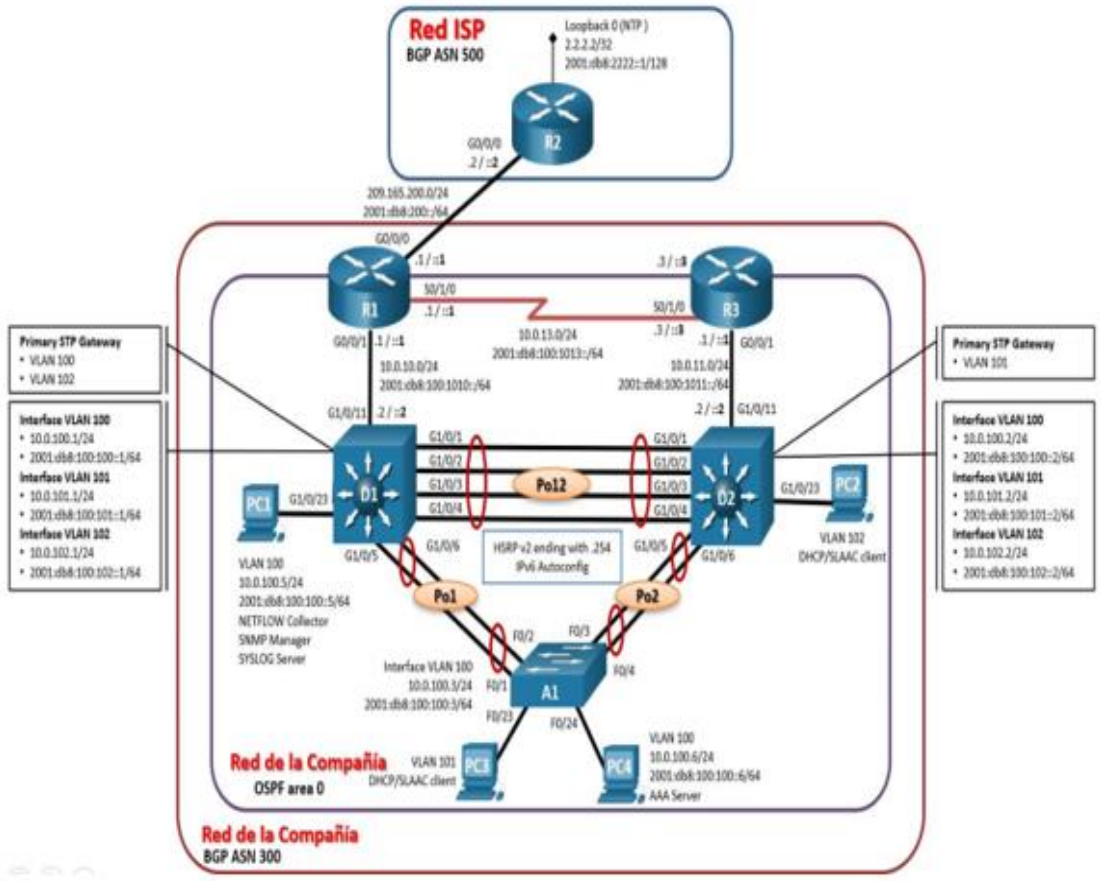
Se utiliza metodologías de simulación con aplicaciones como GNS3, PACKET TRACER para el desarrollo de topologías de red que en la vida real se pueden aplicar, como por ejemplo la seguridad informativa, protección de datos, entre otros.

Se tiene antecedentes prácticos para la configuración de redes determinados en cursos como CCNA (fundamentos de redes, principios de enrutamiento, LAN inalámbrica y acceso a la WAN). Estos refuerzos son aplicados actualmente con el diplomado de profundización CCNP.

Actualmente el presente documento está compuesto de dos momentos, el primero es un avance del documento y el segundo la entrega total dispuesta en las guías. Esta consiste en un registro detallado del paso a paso sobre la configuración básica de la red (enrutamiento), soporte de host, protocolos de enrutamiento como OSPF, redundancia, seguridad y administración de red. Con el fin de afianzar las habilidades educativas relacionadas a la topología de red.

DESARROLLO

Figura 1. Topología de Red



fuente: guías UNAD CCNP avance final

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	10.0.10.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2

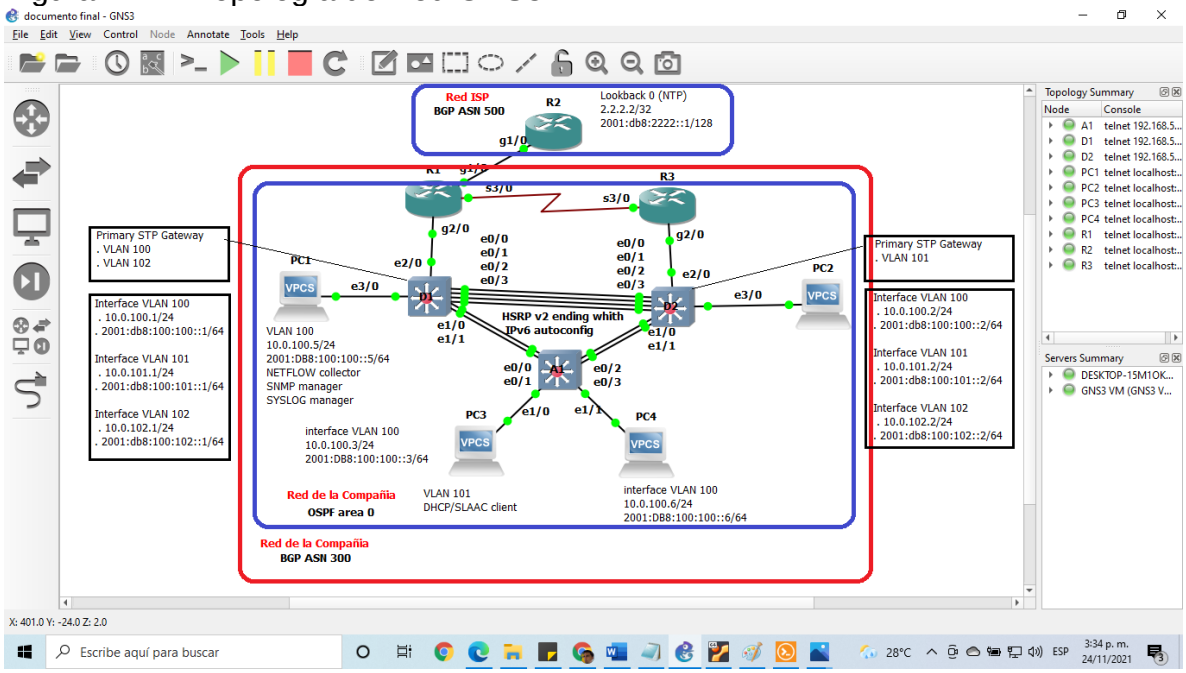
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente: guías UNAD CCNP avance final

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.

Figura 2. Topología de Red GNS3



Fuente: Aplicación GNS3 (Auditoria Propia)

Tabla 2. Tabla de Direccionamiento se cambian interfaces

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0****g1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1****g2/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0****s3/0	10.0.10.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0****g1/0	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****g2/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0****s3/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11***e2/0	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***e2/0	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

Fuente: guías UNAD CCNP avance final

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:

Router 1	
hostname R1	establecer el nombre actual
ipv6 unicast-routing	habilita el routing IPv6
no ip domain lookup	nombre a dirección basado en DNS del host
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	configuración de línea
line con 0	tiempo de espera inactivo
exec-timeout 0 0	desea enviar esta información a un servidor de syslog
logging synchronous	ingresamos la interfaz
exit	
interface g1/0	

ip address 209.165.200.225	se asignan las direcciones
255.255.255.224	se asignan las direcciones
ipv6 address fe80::1:1 link-local	se asignan las direcciones
ipv6 address 2001:db8:200::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface g2/0	ingresamos la interfaz
ip address 10.0.10.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::1:2 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1010::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface s3/0	ingresamos la interfaz
ip address 10.0.13.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::1:3 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1013::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	

Router 2

hostname R2	establecer el nombre actual
ipv6 unicast-routing	habilita el routing IPv6
no ip domain lookup	nombre a dirección basado en DNS del host
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	
line con 0	configuración de línea
exec-timeout 0 0	tiempo de espera inactivo
logging synchronous	desea enviar esta información a un servidor de syslog
exit	
interface g0/0/0	ingresamos la interfaz
ip address 209.165.200.226	se asignan las direcciones
255.255.255.224	se asignan las direcciones
ipv6 address fe80::2:1 link-local	se asignan las direcciones
ipv6 address 2001:db8:200::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface Loopback 0	ingresamos la interfaz loopback
ip address 2.2.2.2 255.255.255.255	se asignan las direcciones
ipv6 address fe80::2:3 link-local	se asignan las direcciones
ipv6 address 2001:db8:2222::1/128	se asignan las direcciones
no shutdown	se activa interfaz
exit	

Router 3

hostname R3	establecer el nombre actual
ipv6 unicast-routing	habilita el routing IPv6
no ip domain lookup	nombre a dirección basado en DNS del host
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	
line con 0	configuración de línea
exec-timeout 0 0	tiempo de espera inactivo
logging synchronous	desea enviar esta información a un servidor de syslog
exit	
interface g2/0	ingresamos la interfaz
ip address 10.0.11.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::3:2 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1011::1/64	se asignan las direcciones
no shutdown	se asignan las direcciones
exit	se activa interfaz
interface s3/0	ingresamos la interfaz
ip address 10.0.13.3 255.255.255.0	se asignan las direcciones
ipv6 address fe80::3:3 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1010::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	

Switch D1

hostname D1	establecer el nombre actual
ip routing	configurar tabla enrutamiento
ipv6 unicast-routing	habilita el routing IPv6
no ip domain lookup	nombre a dirección basado en DNS del host
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	
line con 0	configuración de línea
exec-timeout 0 0	tiempo de espera inactivo
logging synchronous	desea enviar esta información a un servidor de syslog
exit	
vlan 100	asignar el puerto a una VLAN
name Management	
exit	
vlan 101	asignar el puerto a una VLAN
name UserGroupA	
exit	
vlan 102	asignar el puerto a una VLAN
name UserGroupB	
exit	
vlan 999	asignar el puerto a una VLAN

name NATIVE	
exit	
interface e2/0	ingresamos la interfaz
no switchport	creación de las interfaces de la capa 3
ip address 10.0.10.2 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d1:1 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1010::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 100	ingresamos la interfaz vlan
ip address 10.0.100.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d1:2 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:100::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 101	ingresamos la interfaz vlan
ip address 10.0.101.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d1:3 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:101::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 102	ingresamos la interfaz vlan
ip address 10.0.102.1 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d1:4 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:102::1/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	excluir direcciones especificas
ip dhcp excluded-address 10.0.101.141 10.0.101.254	excluir direcciones especificas
ip dhcp excluded-address 10.0.102.1 10.0.102.109	excluir direcciones especificas
ip dhcp excluded-address 10.0.102.141 10.0.102.254	excluir direcciones especificas
ip dhcp pool VLAN-101	ingresa el router en el modo de
network 10.0.101.0 255.255.255.0	configuración dhcpv4
default-router 10.0.101.254	se establece una ruta predeterminada
exit	
ip dhcp pool VLAN-102	ingresa el router en el modo de
network 10.0.102.0 255.255.255.0	configuración dhcpv4
default-router 10.0.102.254	se establece una ruta predeterminada
exit	

Switch D2	
hostname D2	establecer el nombre actual
ip routing	configurar tabla enrutamiento
ipv6 unicast-routing	habilita el routing IPv6
no ip domain lookup	nombre a dirección basado en DNS del host
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	
line con 0	configuración de línea
exec-timeout 0 0	tiempo de espera inactivo
logging synchronous	desea enviar esta información a un servidor de syslog
exit	
vlan 100	asignar el puerto a una VLAN
name Management	
exit	
vlan 101	asignar el puerto a una VLAN
name UserGroupA	
exit	
vlan 102	asignar el puerto a una VLAN
name UserGroupB	
exit	
vlan 999	asignar el puerto a una VLAN
name NATIVE	
exit	
interface e2/0	ingresamos la interfaz
no switchport	creación de las interfaces de la capa 3
ip address 10.0.11.2 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d1:1 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:1011::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 100	ingresamos la interfaz vlan
ip address 10.0.100.2 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d2:2 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:100::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 101	ingresamos la interfaz vlan
ip address 10.0.101.2 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d2:3 link-local	se asignan las direcciones
ipv6 address 2001:db8:100:101::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface vlan 102	ingresamos la interfaz vlan
ip address 10.0.102.2 255.255.255.0	se asignan las direcciones
ipv6 address fe80::d2:4 link-local	se asignan las direcciones

ipv6 address 2001:db8:100:102::2/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.209	excluir direcciones especificas
ip dhcp excluded-address 10.0.101.241 10.0.101.254	excluir direcciones especificas
ip dhcp excluded-address 10.0.102.1 10.0.102.209	excluir direcciones especificas
ip dhcp excluded-address 10.0.102.241 10.0.102.254	excluir direcciones especificas
ip dhcp pool VLAN-101	ingresa el router en el modo de
network 10.0.101.0 255.255.255.0	configuración dhcpv4
default-router 10.0.101.254	se establece una ruta predeterminada
exit	
ip dhcp pool VLAN-102	ingresa el router en el modo de
network 10.0.102.0 255.255.255.0	configuración dhcpv4
default-router 10.0.102.254	se establece una ruta predeterminada
exit	

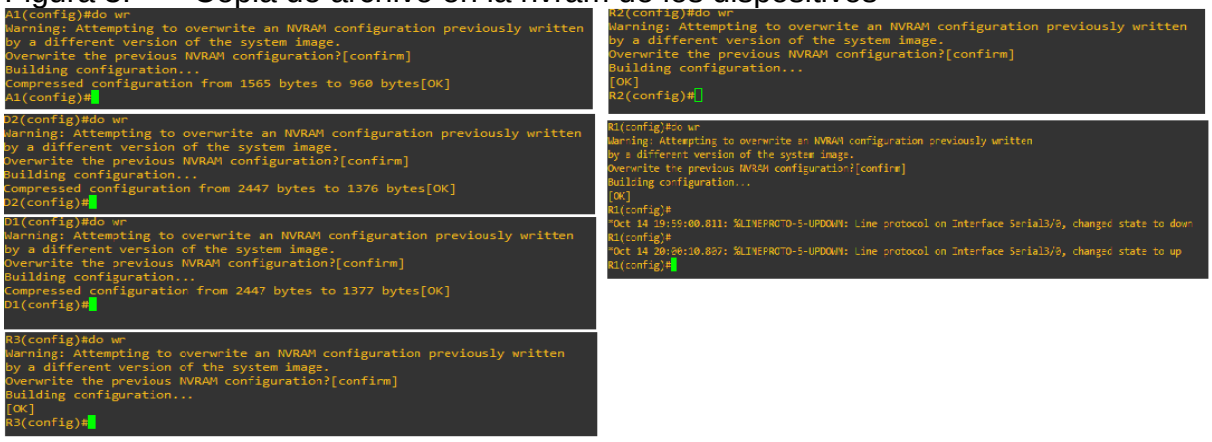
Switch A1

hostname A1	establecer el nombre actual
no ip domain lookup	nombre a dirección basado en DNS del
banner motd # A1, ENCOR Skills	host
Assessment, Scenario 1 #	
line con 0	configuración de línea
exec-timeout 0 0	tiempo de espera inactivo
logging synchronous	desea enviar esta información a un
exit	servidor de syslog
vlan 100	asignar el puerto a una VLAN
name Management	
exit	
vlan 101	asignar el puerto a una VLAN
name UserGroupA	
exit	
vlan 102	asignar el puerto a una VLAN
name UserGroupB	
exit	
vlan 999	asignar el puerto a una VLAN
name NATIVE	
exit	
interface vlan 100	asignar el puerto a una VLAN
ip address 10.0.100.3 255.255.255.0	se asignan las direcciones
ipv6 address fe80::a1:1 link-local	se asignan las direcciones

ipv6 address 2001:db8:100:100::3/64	se asignan las direcciones
no shutdown	se activa interfaz
exit	
interface range f0/5-22	ingresamos rango de interfaces
shutdown	se inactiva interfaz
exit	

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

Figura 3. Copia de archivo en la nvram de 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.

Figura 4. Configuración parámetros básicos PC1 IPv4 e IPv6

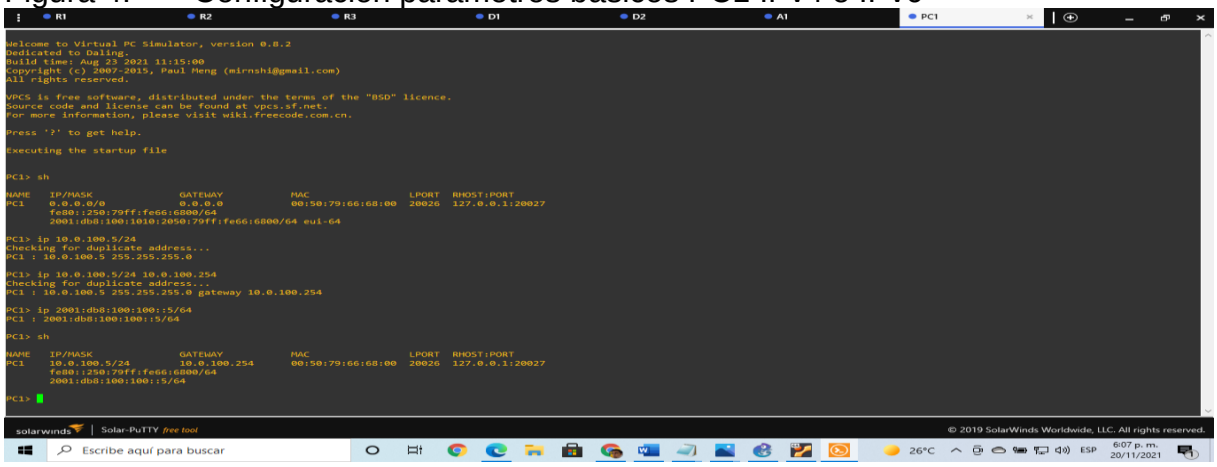
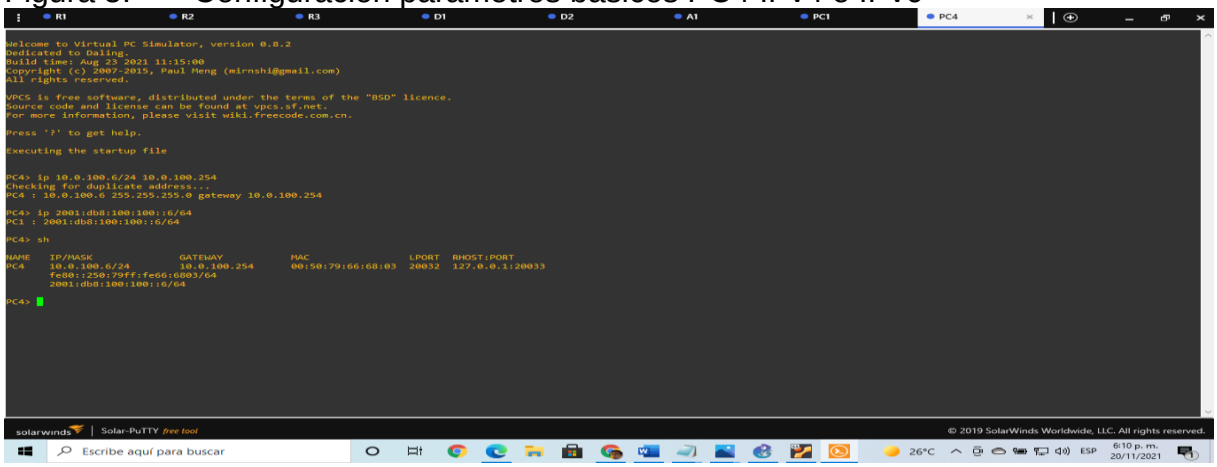


Figura 5. Configuración parámetros básicos PC4 IPv4 e IPv6



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 3. Configuraciones troncales, RSPT, Raíz root, Etherhetchannel LACP.

Tarea#	Tarea	Especificación
2,1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2,2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2,3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2,4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

2,5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2,6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

Switch D1

interface range g1/0/1-4	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del canal
channel-group 12 mode active	
no shutdown	se activa interfaz
exit	
interface range g1/0/5-6	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del canal
channel-group 1 mode active	
no shutdown	se activa interfaz
exit	
spanning-tree mode rapid-pvst	modo árbol de expansión
spanning-tree vlan 100,102 root primary	vlan primaria
spanning-tree vlan 101 root secondary	vlan secundaria
interface g1/0/23	Ingresamos rango de interfaces
switchport mode access	interfaz cambia al modo de acceso permanente
switchport access vlan 100	
spanning-tree portfast	acceso inmediato a la red de capa 2
no shutdown	se activa interfaz
exit	
end	

Switch D2

interface range e0/0-3	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del
channel-group 12 mode active	canal
no shutdown	se activa interfaz
exit	
interface range e1/0-1	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del
channel-group 2 mode active	canal
no shutdown	se activa interfaz
exit	
spanning-tree mode rapid-pvst	modo árbol de expansión
spanning-tree vlan 101 root primary	vlan primaria
spanning-tree vlan 100,102 root	vlans secundarias
secondary	
interface e3/0	ingresamos la interfaz
switchport mode access	interfaz cambia al modo de acceso
switchport access vlan 102	permanente
spanning-tree portfast	acceso inmediato a la red de capa 2
no shutdown	se activa interfaz
exit	
end	

Switch A1

spanning-tree mode rapid-pvst	modo de árbol de expansión
interface range e0/0-1	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del
channel-group 1 mode active	canal
no shutdown	se activa interfaz
exit	
interface range e0/2-3	Ingresamos rango de interfaces
switchport mode trunk	troncal de la interfaz
switchport trunk native vlan 999	especifica el número del grupo del
channel-group 2 mode active	canal
no shutdown	se activa interfaz
exit	
interface e1/0	ingresamos la interfaz
switchport mode access	interfaz cambia al modo de acceso
switchport access vlan 101	permanente
spanning-tree portfast	acceso inmediato a la red de capa 2
no shutdown	se activa interfaz

exit	
interface e1/1	ingresamos la interfaz
switchport mode access	interfaz cambia al modo de acceso
switchport access vlan 100	permanente
spanning-tree portfast	acceso inmediato a la red de capa 2
no shutdown	se activa interfaz
exit	
end	

Tabla 4. Verificación DHCP y ping

Tarea#	Tarea	Especificación
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 6. DHCP IPv4 PC2

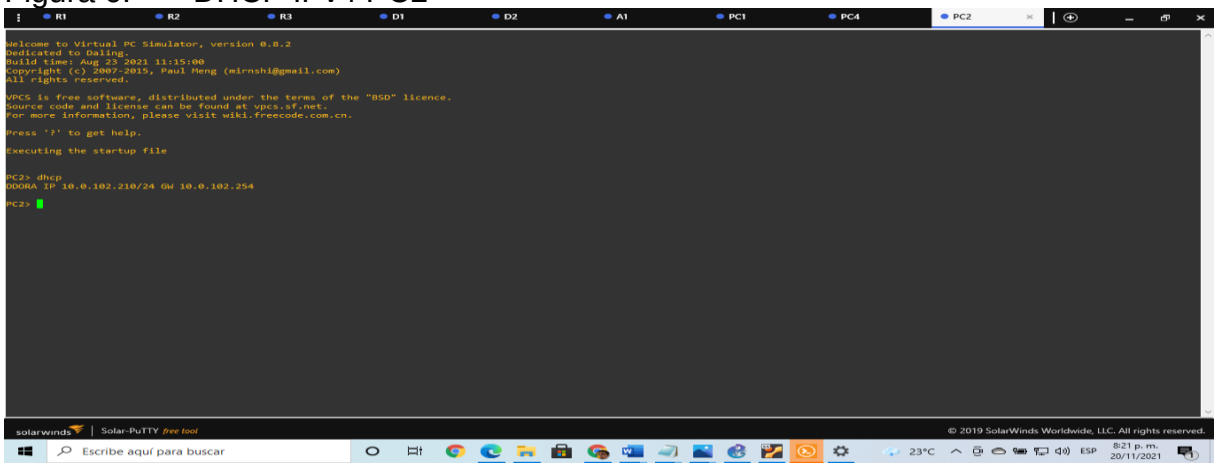


Figura 7. DHCP IPv4 PC3

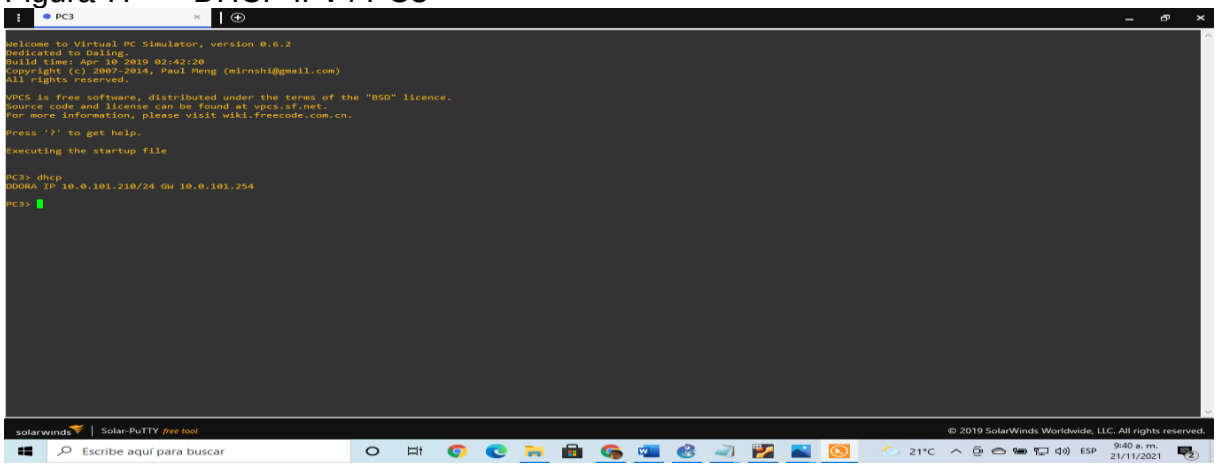


Figura 8. Ping PC1 a:

• D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6

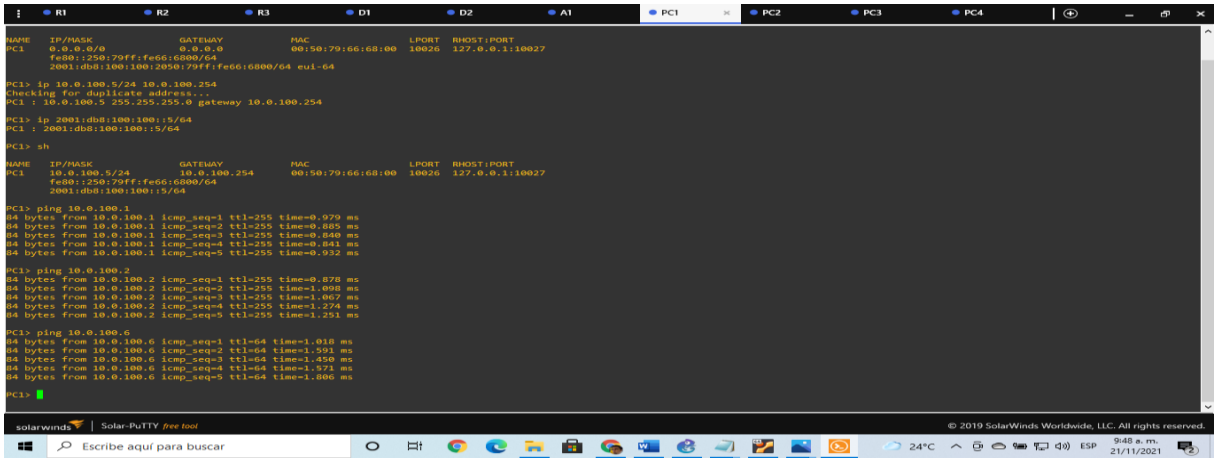


Figura 9. Ping PC2 a:

• D1: 10.0.102.1 • D2: 10.0.102.2

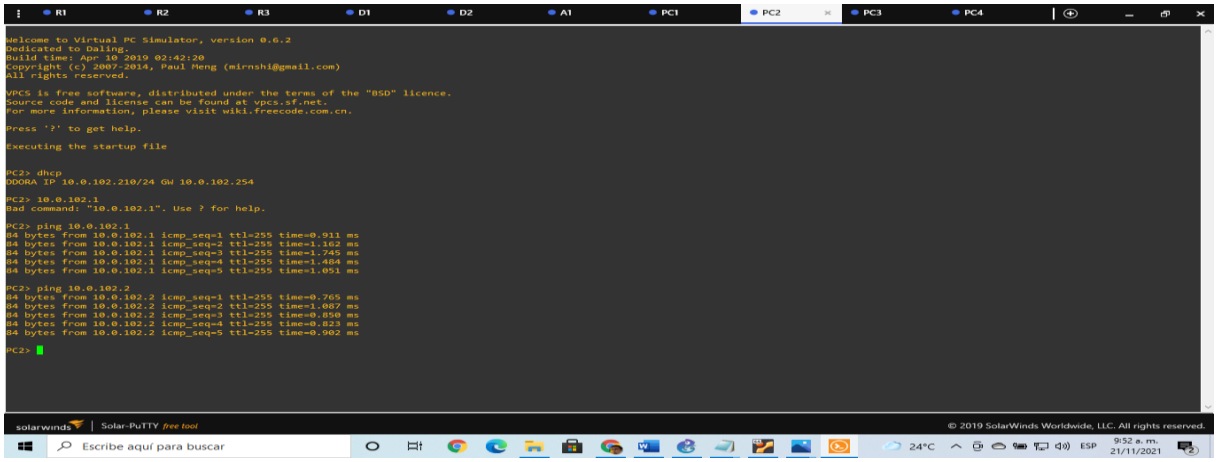


Figura 10. Ping PC3 a:
• D1: 10.0.101.1 • D2: 10.0.101.2

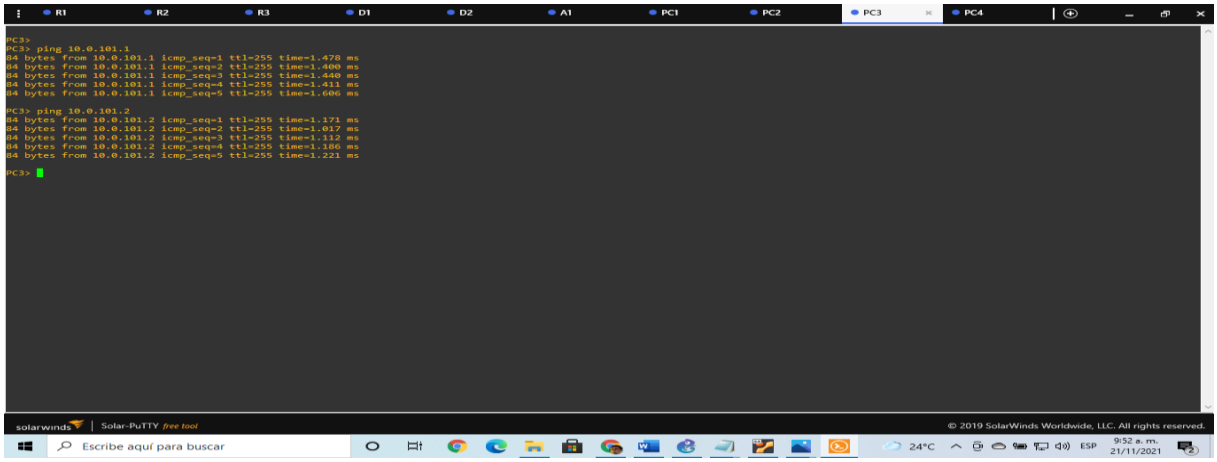
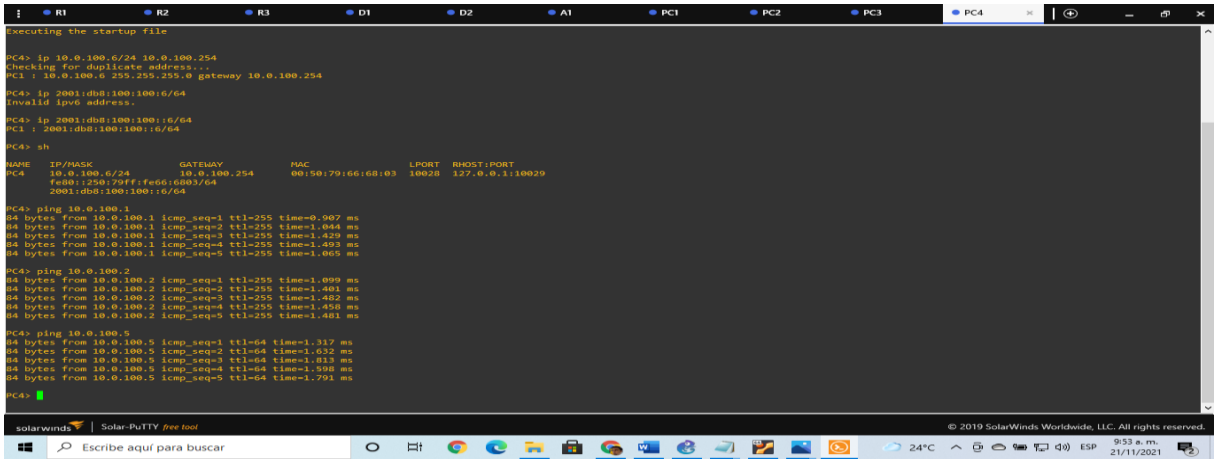


Figura 11. Ping PC4 a:
• D1: 10.0.100.1
• D2: 10.0.100.2
• PC1: 10.0.100.5



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 OSPFv2, OSPFv2 en Ipv4 e Ipv6

Tarea#	Tarea	Especificación
3,1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.	se OSPF Process ID 4 y asigne los siguientes routerIDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en 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 recibir direcciones IPv4 válidas.
3,2	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	se OSPF Process ID 6 y asigne los siguientes routerIDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en 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 MPBGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6

		con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3,4	En R1 en la "Red ISP", configure MPBGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

Router R1

router ospf 4	Enrutador ospf
router-id 0.0.4.1	Identificar router id
network 10.0.10.0 0.0.0.255 area 0	Interfaces que participan
network 10.0.13.0 0.0.0.255 area 0	Interfaces que participan
default-information originate	Propagación de una ruta estatica
exit	predeterminada
ipv6 router ospf 6	Los protocolos de routing IPv6 se
router-id 0.0.6.1	habilitan en una interfaz
default-information originate	Identificar router id
exit	Propagación de una ruta estatica
interface g2/0	ingresamos la interfaz
ipv6 ospf 6 area 0	
exit	
interface s3/0	ingresamos la interfaz

ipv6 ospf 6 area 0	
exit	
ip route 10.0.0.0 255.0.0.0 null0	
ipv6 route 2001:db8:100::/48 null0	
router bgp 300	Habilita el dominio BGP y define el
bgp router-id 1.1.1.1	número de sistema autónomo
neighbor 209.165.200.226 remote-as	Identificación route
500	número as del enrutador al que desea
neighbor 2001:db8:200::2 remote-as	conectarse con bgp
500	
address-family ipv4 unicast	configuración familia ipv4
neighbor 209.165.200.226 activate	activar vecino
no neighbor 2001:db8:200::2 activate	desactivar vecino
network 10.0.0.0 mask 255.0.0.0	
exit-address-family	salimos configuración familia ipv4
address-family ipv6 unicast	configuración familia ipv6
no neighbor 209.165.200.226 activate	
neighbor 2001:db8:200::2 activate	
network 2001:db8:100::/48	dirección y mascara
exit-address-family	salimos configuración familia ipv6

Router R2

ip route 0.0.0.0 0.0.0.0 loopback 0	
ipv6 route ::/0 loopback 0	
router bgp 500	número de sistema autónomo
bgp router-id 2.2.2.2	Identificación route
neighbor 209.165.200.225 remote-as	número as del enrutador al que desea
300	conectarse con bgp
neighbor 2001:db8:200::1 remote-as	número as del enrutador al que desea
300	conectarse con bgp
address-family ipv4	configuración familia ipv4
neighbor 209.165.200.225 activate	
no neighbor 2001:db8:200::1 activate	
network 2.2.2.2 mask 255.255.255.255	dirección y mascara
network 0.0.0.0	
exit-address-family	salimos configuración familia ipv4
address-family ipv6	configuración familia ipv6
no neighbor 209.165.200.225 activate	
neighbor 2001:db8:200::1 activate	dirección y mascara
network 2001:db8:2222::/128	
network ::/0	
exit-address-family	salimos configuración familia ipv6

Router R3

router ospf 4	Enrutador ospf
router-id 0.0.4.3	Identificar router id
network 10.0.11.0 0.0.0.255 area 0	dirección que participa
network 10.0.13.0 0.0.0.255 area 0	dirección que participa
exit	
ipv6 router ospf 6	
router-id 0.0.6.3	
exit	
interface g2/0	ingresamos la interfaz
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface s3/0	ingresamos la interfaz
ipv6 ospf 6 area 0	configuración área en ospf
exit	
end	

Switch D1

router ospf 4	Enrutador ospf
router-id 0.0.4.131	Identificar router id
network 10.0.100.0 0.0.0.255 area 0	dirección que participa
network 10.0.101.0 0.0.0.255 area 0	dirección que participa
network 10.0.102.0 0.0.0.255 area 0	dirección que participa
network 10.0.10.0 0.0.0.255 area 0	dirección que participa
passive-interface default	detiene el ruteo ospf
no passive-interface g1/0/11	permite comunicación ospf con la
exit	interfaz
ipv6 router ospf 6	Enrutador ospf
router-id 0.0.6.131	Identificar router id
passive-interface default	detiene el ruteo ospf
no passive-interface g1/0/11	permite comunicación ospf con la
exit	interfaz
interface e2/0	ingresamos la interfaz
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 100	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 101	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 102	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	

Switch D2	
router ospf 4	Enrutador ospf
router-id 0.0.4.132	Identificar router id
network 10.0.100.0 0.0.0.255 area 0	dirección que participa
network 10.0.101.0 0.0.0.255 area 0	dirección que participa
network 10.0.102.0 0.0.0.255 area 0	dirección que participa
network 10.0.11.0 0.0.0.255 area 0	dirección que participa
passive-interface default	detiene el ruteo ospf
no passive-interface e2/0	permite comunicación ospf con la
exit	interfaz
ipv6 router ospf 6	Enrutador ospf
router-id 0.0.6.132	Identificar router id
passive-interface default	detiene el ruteo ospf
no passive-interface g1/0/11	permite comunicación ospf con la
exit	interfaz
interface e2/0	ingresamos la interfaz
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 100	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 101	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	
interface vlan 102	ingresamos la interfaz vlan
ipv6 ospf 6 area 0	configuración área en ospf
exit	
end	

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”. Las tareas de configuración son las siguientes:

Tabla 6. Comandos (FHRP/SLA)

Tarea#	Tarea	Especificación
4,1	En D1, cree IP SLAs que prueben la	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

	accesibilidad de la interfaz R1 G0/0/1.	G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4,2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
	4,3 En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254.

		• Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. 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.

Switch D1	
ip sla 4	Monitoreo en un nodo en la red
icmp-echo 10.0.10.1	Ping, replica a esa dirección ipv4
frequency 5	
exit	
ip sla 6	Monitoreo en un nodo en la red
icmp-echo 2001:db8:100:1010::1	Ping, replica a esa dirección ipv4
frequency 5	
exit	
ip sla schedule 4 life forever start-time now	habilita el ip sla indica cuando y por cuanto tiempo estará activo
ip sla schedule 6 life-forever start-time now	habilita el ip sla indica cuando y por cuanto tiempo estará activo
track 4 ip sla 4	
delay down 10 up 15	retraso de 10 a 15
exit	
track 6 ip sla 6	
delay down 10 up 15	retraso de 10 a 15
exit	
interface vlan 100	ingresamos la interfaz vlan
standby version 2	configura el hsrp para usar la versión 2
standby 104 ip 10.0.100.254	
standby 104 priority 150	
standby 104 preempt	
standby 104 track 4 decrement 60	
standby 106 ipv6 autoconfig	
standby 106 priority 150	
standby 106 preempt	
standby 106 track 6 decrement 60	
exit	
interface vlan 101	ingresamos la interfaz vlan
standby version 2	configura el hsrp para usar la versión 2
standby 114 ip 10.0.101.254	
standby 114 preempt	
standby 114 track 4 decrement 60	
standby 116 ipv6 autoconfig	
standby 116 preempt	
standby 116 track 6 decrement 60	
exit	
interface vlan 102	ingresamos la interfaz vlan
standby version 2	configura el hsrp para usar la versión 2
standby 124 ip 10.0.102.254	
standby 124 priority 150	
standby 124 preempt	
standby 124 track 4 decrement 60	

standby 126 ipv6 autoconfig	
standby 126 priority 150	
standby 126 preempt	
standby 126 track 6 decrement 60	
exit	
end	

Switch D2	
ip sla 4	Monitoreo en un nodo en la red
icmp-echo 10.0.11.1	Ping, replica a esa dirección ipv4
frequency	
exit	
ip sla 6	Monitoreo en un nodo en la red
icmp-echo 2001:db8:100:1011::1	Ping, replica a esa dirección ipv4
frequency	
exit	
ip sla schedule 4 life forever start-time now	habilita el ip sla indica cuando y por cuanto tiempo estará activo
ip sla schedule 6 life forever start-time now	habilita el ip sla indica cuando y por cuanto tiempo estará activo
track 4 ip sla 4	
delay down 10 up 15	retraso de 10 a 15
exit	
track 6 ip sla 6	
delay down 10 up 15	retraso de 10 a 15
exit	
interface vlan 100	ingresamos la interfaz vlan
standby version 2	configura el hsrp para usar la versión 2
standby 104 ip 10.0.100.254	
standby 104 preempt	
standby 104 track 4 decrement 60	
standby 106 ipv6 autoconfig	
standby 106 preempt	
standby 106 track 6 decrement 60	
exit	
interface vlan 101	ingresamos la interfaz vlan
standby version 2	configura el hsrp para usar la versión 2
standby 114 ip 10.0.101.254	
standby 114 priority 150	
standby 114 preempt	
standby 114 track 4 decrement 60	
standby 116 ipv6 autoconfig	
standby 116 priority 150	
standby 116 preempt	

standby 116 track 6 decrement 60 exit interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60 exit end	 ingresamos la interfaz vlan configura el hsrp para usar la versión 2

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 7. Configuración seguridad

Tarea#	Tarea	Especificación
5,1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.
5,2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: sadmin • Nivel de privilegio 15 • Contraseña: cisco12345cisco
5,3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA
5,4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: $trongPass
5,5	En todos los dispositivos (excepto R2),	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto

	configure la lista de métodos de autenticación AAA	• Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5,6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

En todos los equipos:

enable algorithm-type SCRYPT secret cisco12345cisco username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	Configurar el tipo de algoritmo de una contraseña de usuario

en todos los equipos excepto R2:

aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass exit aaa authentication login default group radius local end	Configuración de autenticación protocolo de autenticación y autorización para aplicaciones de acceso a la red

Figura 12. Acceso de verificación cuenta encriptada SCRYPT

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 8. Configuraciones de administración de red

Tarea#	Tarea	Especificación
6,1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6,2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6,3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6,4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6,5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el community string en ENCORSA. • En R3, D1, y D2, habilite el envío de traps config y ospf. • En R1, habilite el envío de traps bgp, config, y ospf. • En A1, habilite el envío de traps config.

configuración reloj local UTC en todos los equipos

Router R2	
ntp master 3	reloj maestro ntp para sincronización
end	
Router R1	
ntp server 2.2.2.2	
logging trap warning	advertencia de registro
logging host 10.0.100.5	Ingreso sesión ip
logging on	activar sesión
ip access-list standard SNMP-NMS	acceso lista a protocolo de
permit host 10.0.100.5	administración
exit	
snmp-server contact Cisco Student	protocolo de administración cisco
snmp-server community ENCORSA ro SNMP-NMS	protocolo de administración comunidad
snmp-server host 10.0.100.5 version 2c ENCORSA	proporciona un valor de índice de
snmp-server ifindex persist	interfaz
snmp-server enable traps bgp	habilita el soporte
snmp-server enable traps config	de bgp para operaciones snm
snmp-server enable traps ospf	habilita el soporte
end	de ospf para operaciones snm
Router R3	
ntp server 10.0.10.1	
logging trap warning	advertencia de registro
logging host 10.0.100.5	Ingreso sesión ip
logging on	activar sesión
ip access-list standard SNMP-NMS	acceso lista a protocolo de
permit host 10.0.100.5	administración
exit	
snmp-server contact Cisco Student	protocolo de administración cisco
snmp-server community ENCORSA ro SNMP-NMS	protocolo de administración comunidad
snmp-server host 10.0.100.5 version 2c ENCORSA	proporciona un valor de índice de
snmp-server ifindex persist	interfaz
snmp-server enable traps config	habilita el soporte
snmp-server enable traps ospf	de bgp para operaciones snm
end	habilita el soporte
	de ospf para operaciones snm

Switch D1

ntp server 10.0.10.1	
logging trap warning	advertencia de registro
logging host 10.0.100.5	Ingreso sesión ip
logging on	activar sesión
ip access-list standard SNMP-NMS	acceso lista a protocolo de
permit host 10.0.100.5	administración
exit	
snmp-server contact Cisco Student	protocolo de administración cisco
snmp-server community ENCORSA ro SNMP-NMS	protocolo de administración comunidad
snmp-server host 10.0.100.5 version 2c ENCORSA	proporciona un valor de índice de
snmp-server ifindex persist	interfaz
snmp-server enable traps config	habilita el soporte
snmp-server enable traps ospf	de bgp para operaciones snm
end	habilita el soporte
	de ospf para operaciones snm

Switch D2

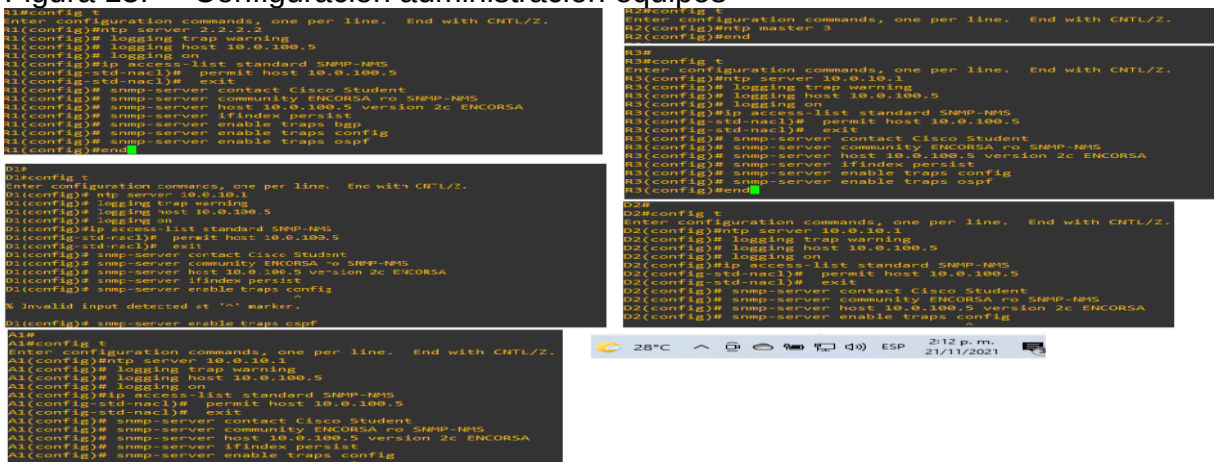
ntp server 10.0.10.1	
logging trap warning	advertencia de registro
logging host 10.0.100.5	Ingreso sesión ip
logging on	activar sesión
ip access-list standard SNMP-NMS	acceso lista a protocolo de
permit host 10.0.100.5	administración
exit	
snmp-server contact Cisco Student	protocolo de administración cisco
snmp-server community ENCORSA ro SNMP-NMS	protocolo de administración comunidad
snmp-server host 10.0.100.5 version 2c ENCORSA	habilitar las notificaciones
snmp-server enable traps config	de trampas snmp
snmp-server enable traps ospf	habilita el soporte
end	de ospf para operaciones snm

Switch A1

ntp server 10.0.10.1	
logging trap warning	advertencia de registro
logging host 10.0.100.5	Ingreso sesión ip
logging on	activar sesión
ip access-list standard SNMP-NMS	acceso lista a protocolo de
permit host 10.0.100.5	administración
exit	

snmp-server contact Cisco Student	protocolo de administración cisco
snmp-server community ENCORSA ro SNMP-NMS	protocolo de administración comunidad
snmp-server host 10.0.100.5 version 2c ENCORSA	proporciona un valor de índice de
snmp-server ifindex persist	interfaz
snmp-server enable traps config	habilitar las notificaciones
snmp-server enable traps ospf	de trampas snmp
end	habilita el soporte
	de ospf para operaciones snm

Figura 13. Configuración administración equipos



Evidencia de funcionamiento por medio del comando show

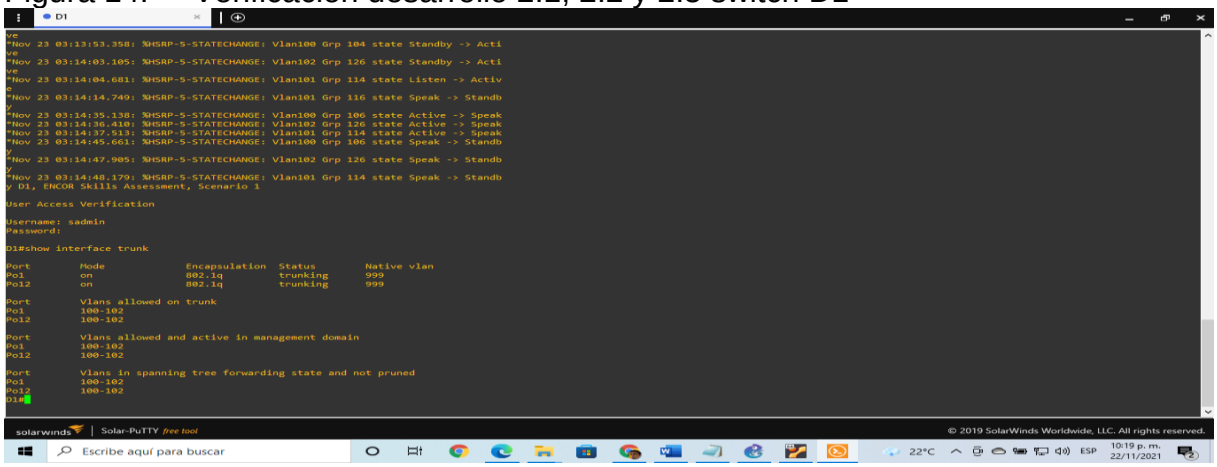
show interface trunk

se identifican múltiples elementos de la operación de los enlaces troncales, muestra el tronco de la interfaz.

Port Vlans allowed on trunk
Po1 1-4094
Po12 1-4094
Port Vlans allowed and active in management do
Po1 1,100-102,999
Po12 1,100-102,999

Port Vlans in spanning tree forwarding state a
Po1 1,100-102,999
Po12 1,100-102,999

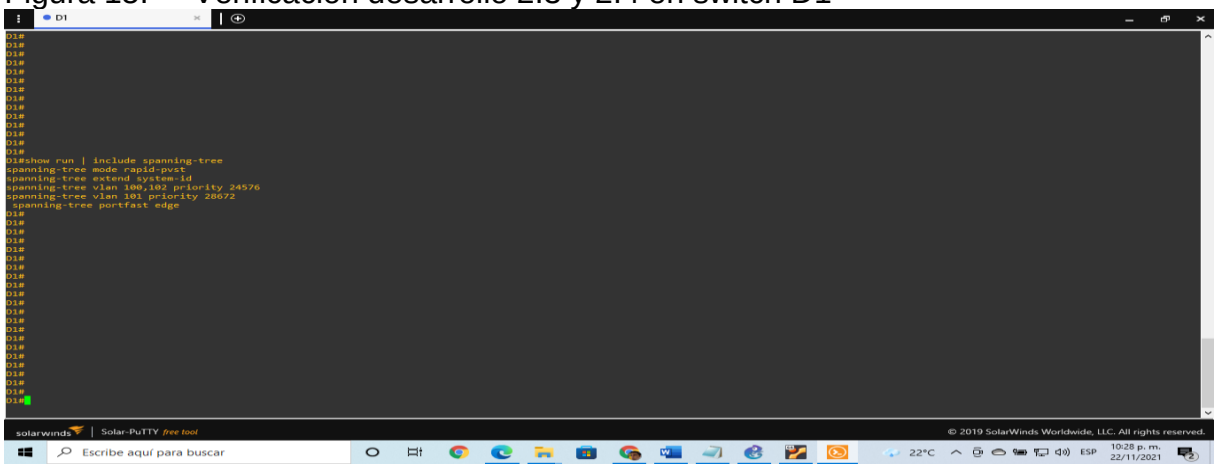
Figura 14. Verificación desarrollo 2.1, 2.2 y 2.5 switch D1



show run | include spanning-tree
comando que habilita el portfast en puertos operacionales como puertos de acceso

D1# show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast edge

Figura 15. Verificación desarrollo 2.3 y 2.4 en switch D1

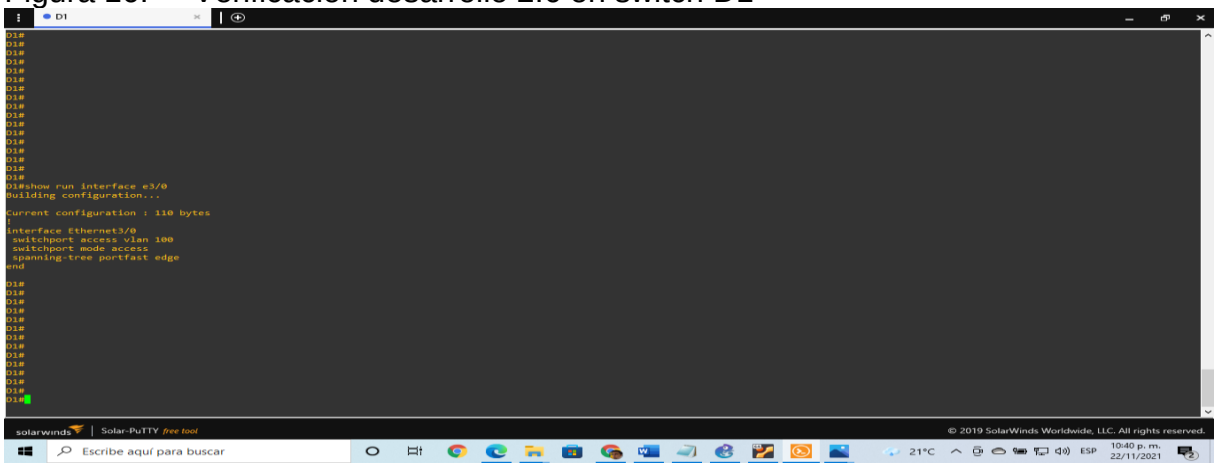


show run interface e3/0
Permite revisar el estado, configuración y estadísticas de todas o cada una de las interfaces del dispositivo individualmente

D1# show run interface e3/0
Building configuration...

Current configuration : 110 bytes
!
interface ethernet3/0
switchport access vlan 100
switchport mode access
spanning-tree portfast
end

Figura 16. Verificación desarrollo 2.6 en switch D1



show interfaces trunk
permite verificar múltiples elementos de la operación de los enlaces troncales

D2# show interfaces trunk

Port Mode Encapsulation Status
Po2 on 802.1q trunking
Po12 on 802.1q trunking

Port Vlans allowed on trunk
Po2 1-4094
Po12 1-4094

Port Vlans allowed and active in management do
Po2 1,100-102,999
Po12 1,100-102,999

Port Vlans in spanning tree forwarding state a
Po2 1,100-102,999
Po12 1,100-102,999

Figura 17. Verificación desarrollo 2.5 en switch D2

show run | section ^router ospf
permite verificar la configuración OSPF registrada en cada componente de la red

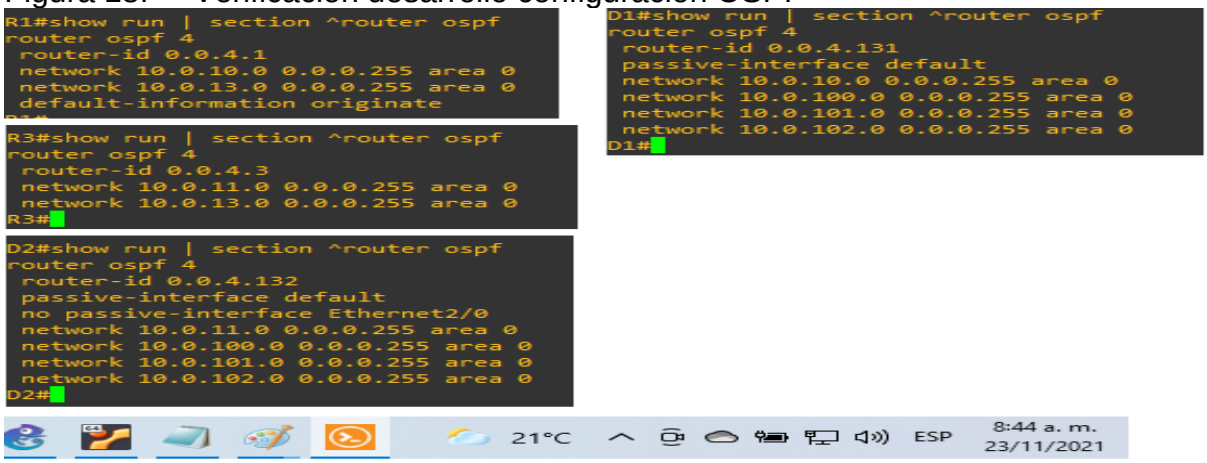
R1# show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate

R3# show run | section ^router ospf
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0

D1# show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
network 10.0.10.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0

D2# show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet2/0
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0

Figura 18. Verificación desarrollo configuración OSPF



show run | section ^ipv6 router
R1# show run | section ^ipv6
router ipv6 router ospf 6
router-id 0.0.6.1
default-information originate

show ipv6 ospf interface brief
permite verificar la configuración de interfaces OSPF habilitado

R1# show ipv6 ospf interface brief
Interface PID Area Intf ID Cost S
Se3/0 6 0 6 64 P2P 1/1
Gi2/0 6 0 5 1 DR 0/0

show run | section ^ipv6 router
R3# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.3

show ipv6 ospf interface brief
R3# show ipv6 ospf interface brief
Interface PID Area Intf ID Cost S
Se3/0 6 0 6 64 P2P 1/1
Gi2/0 6 0 5 1 DR 0/0

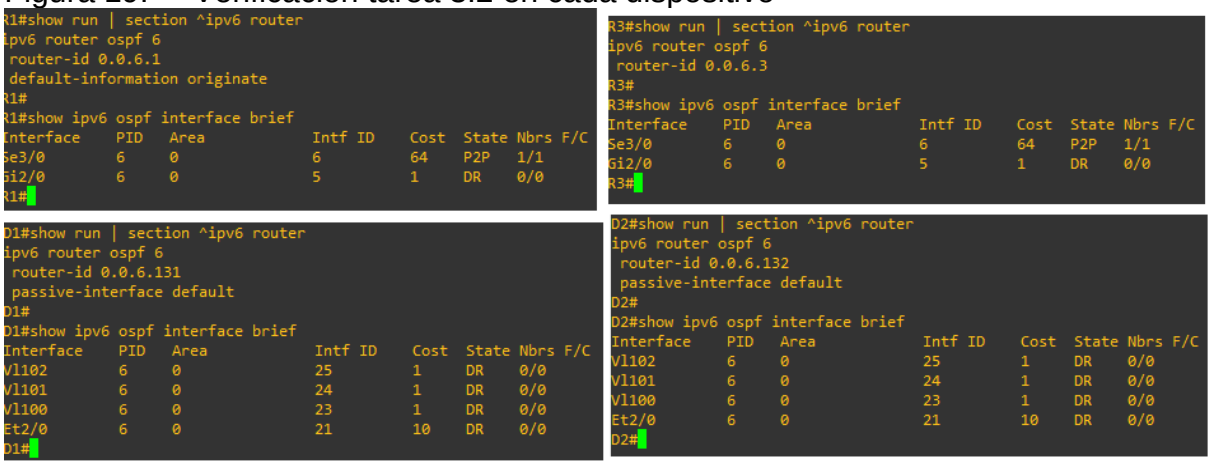
show run | section ^ipv6 router
D1# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default

show ipv6 ospf interface brief
D1# show ipv6 ospf interface brief
Interface PID Area Intf ID Cost S
Vl102 6 0 25 1 DR
Vl101 6 0 24 1 DR
Vl100 6 0 23 1 DR
Et2/0 6 0 21 1 B

show run | section ^ipv6 router
D2# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default

show ipv6 ospf interface brief
D2# show ipv6 ospf interface brief
Interface PID Area Intf ID Cost S
Vl102 6 0 25 1 DR
Vl101 6 0 24 1 DR
Vl100 6 0 23 1 DR
Et2/0 6 0 21 10 DR

Figura 19. Verificación tarea 3.2 en cada dispositivo



show run | section bgp

verificación de intercambio informativo entre dispositivos

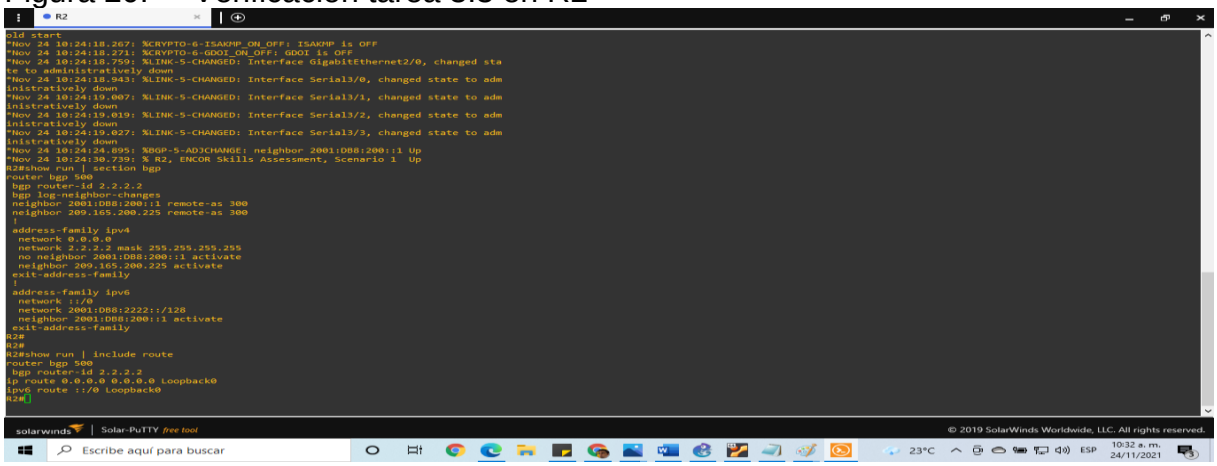
R2# show run | section router bgp
router bgp 500
bgp router-id 2.2.2.2
bgp log-neighbor-changes
neighbor 2001:DB8:200::1 remote-as 300
neighbor 209.165.200.225 remote-as 300
!
address-family ipv4
network 0.0.0.0
network 2.2.2.2 mask 255.255.255.255
no neighbor 2001:DB8:200::1 activate
neighbor 209.165.200.225 activate
exit-address-family
!
address-family ipv6
network ::/0
network 2001:DB8:2222::/128
neighbor 2001:DB8:200::1 activate
exit-address-family

show run | include route

R2# show run | include route
router bgp 500
bgp route-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0

ipv6 route ::/0 Loopback0

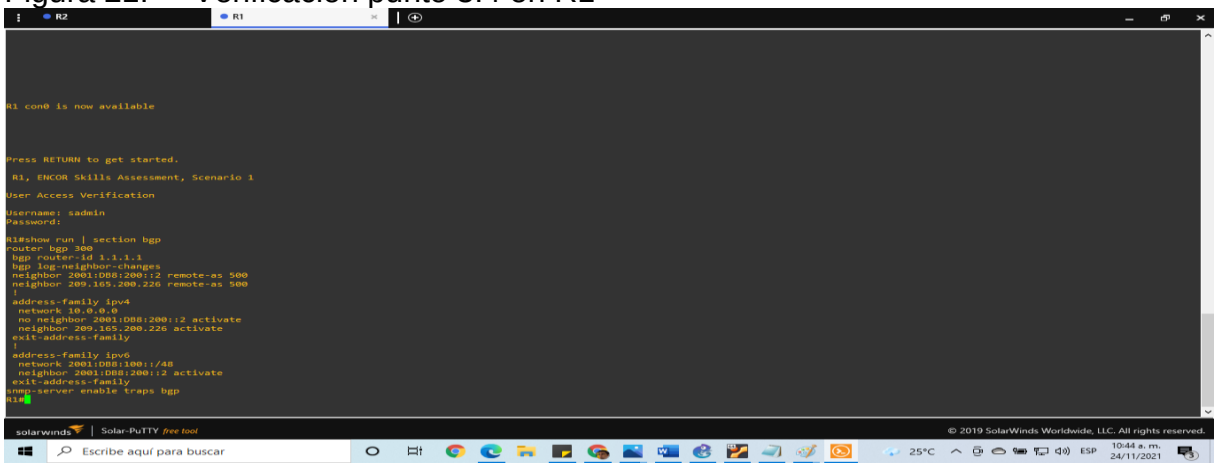
Figura 20. Verificación tarea 3.3 en R2



show run | section bgp

R1# show run | section bgp
router bgp 300
bgp router-id 1.1.1.1
bgp log-neighbor-changes
neighbor 2001:DB8:200::2 remote-as 500
neighbor 209.165.200.226 remote-as 500
!
address-family ipv4
network 10.0.0.0
no neighbor 2001:DB8:200::2 activate
neighbor 209.165.200.226 activate
exit-address-family
!
address-family ipv6
network 2001:DB8:100::/48
neighbor 2001:DB8:200::2 activate
exit-address-family

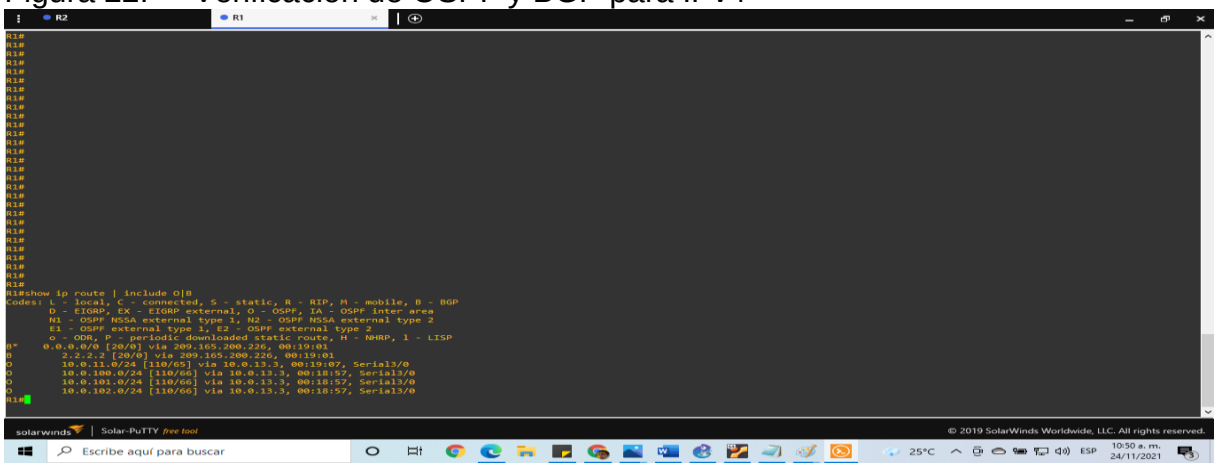
Figura 21. Verificación punto 3.4 en R1



show ip route | include O|B
verificación de OSPF y BGP para IPv4 funcionan correctamente

R1 # muestra la ruta IP | incluir O | B
Códigos: L - local, C - conectado, S - estático, R –
D - EIGRP, EX - EIGRP externo, O - OSPF, IA -
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA
E1 - OSPF externo tipo 1, E2 - OSPF externo ti
o - ODR, P - ruta estática descargada periódic
B * 0.0.0.0/0 [20/0] a través de 209.165.200.2,
B 2.2.2.2 [20/0] vía 209.165.200.2, 01:51:16
O 10.0.11.0/24 [110/65] a través de 10.0.13.3,
O 10.0.100.0/24 [110/66] a través de 10.0.10.2,
O 10.0.101.0/24 [110/66] a través de 10.0.10.2,
O 10.0.102.0/24 [110/66] a través de 10.0.10.2,

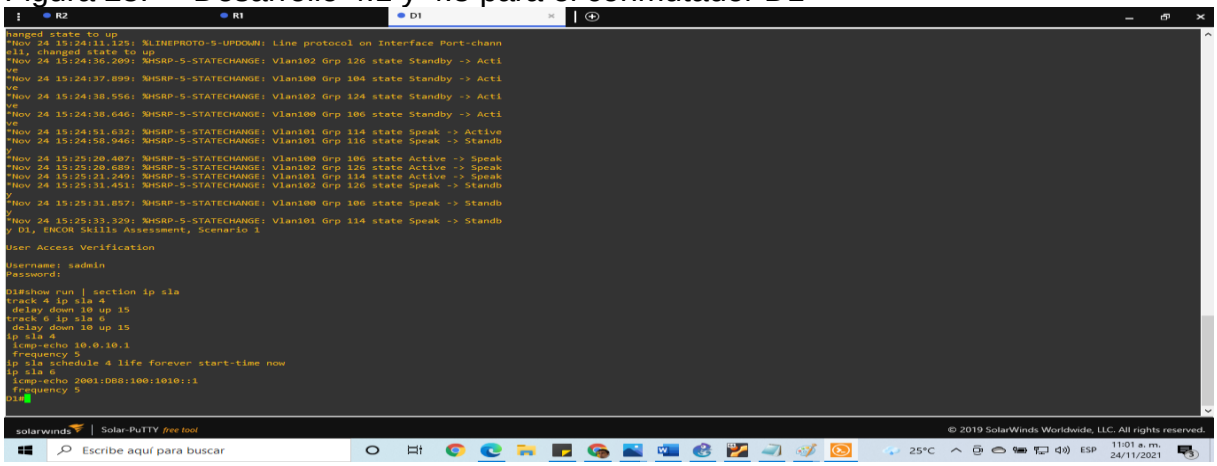
Figura 22. Verificación de OSPF y BGP para IPv4



show run | section ip sla
permite identificar el archivo de configuración activo en la RAM
se verifica desarrollo 4.1 y 4.3 para el conmutador D1

D1# show run | section ip sla
track 4 ip sla 4
delay down 10 up 15
track 6 ip sla 6
delay down 10 up 15
ip sla 4
icmp-echo 10.0.10.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1010::1
frequency 5

Figura 23. Desarrollo 4.1 y 4.3 para el conmutador D1

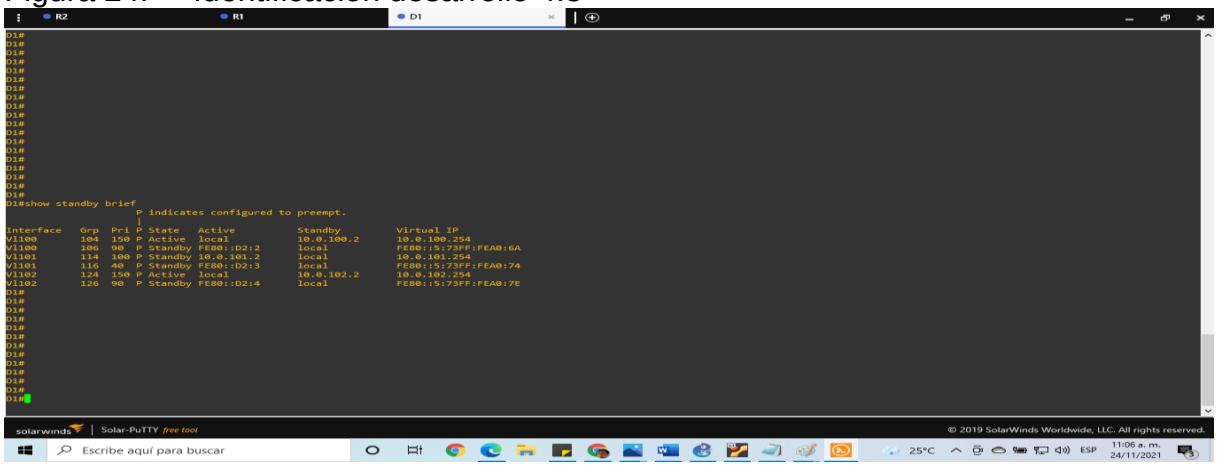


show standby brief
permite verificar el estado activo o pasivo en las direcciones IP virtuales

D1# show standby brief
P indicates configured to preemp
|
Interface Grp Pri P State Active Standb
Vl100 104 150 P Active local 10.0.100.2
Vl100 106 90 P Active local FE80::D2:2
Vl101 114 100 P Standby 10.0.101.2 local
Vl101 116 40 P Standby FE80::D2:3 local

Vl102 124 150 P Active local 10.0.102.2
Vl102 126 90 P Active local FE80::D2:4

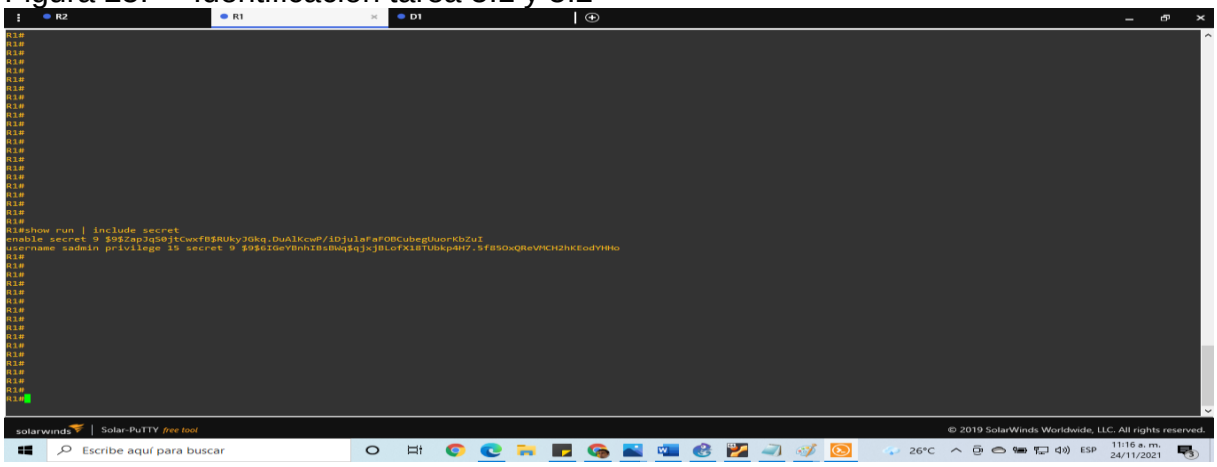
Figura 24. Identificación desarrollo 4.3



show run | include secret
confirmación de clave encriptada

R1# show run | include secret
enable secret 9 $9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu2
username sadmin privilege 15 secret 9 9XCO4pzqbRT.3

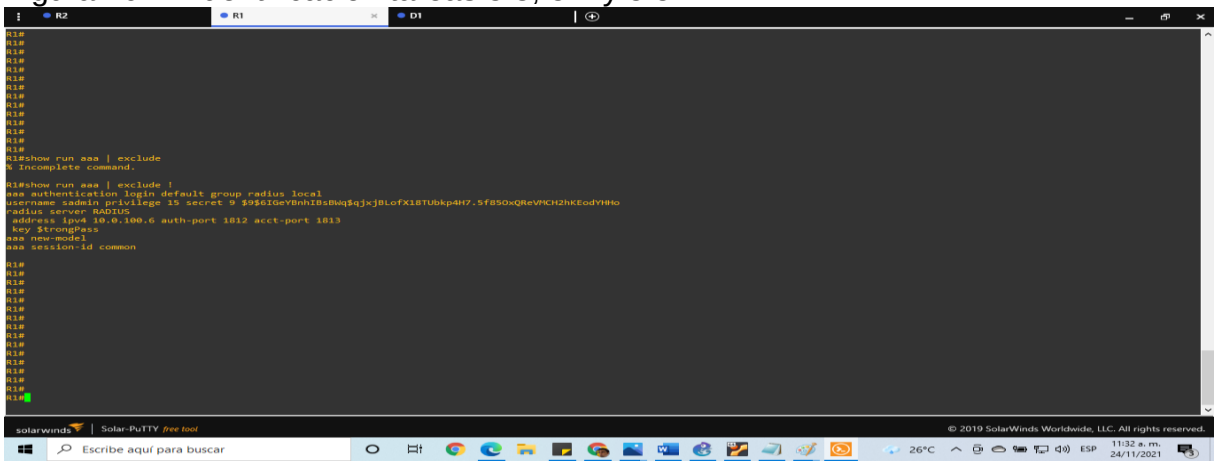
Figura 25. Identificación tarea 5.1 y 5.2



show run aaa | exclude !
confirmación de inicio de sesión con usuario sadmin y contraseña cisco12345cisco, se realiza inicio de sesión exitoso donde se verifica que AAA funciona correctamente

R1# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
aaa new-model
aaa session-id common

Figura 26. Identificación tareas 5.3, 5.4 y 5.5



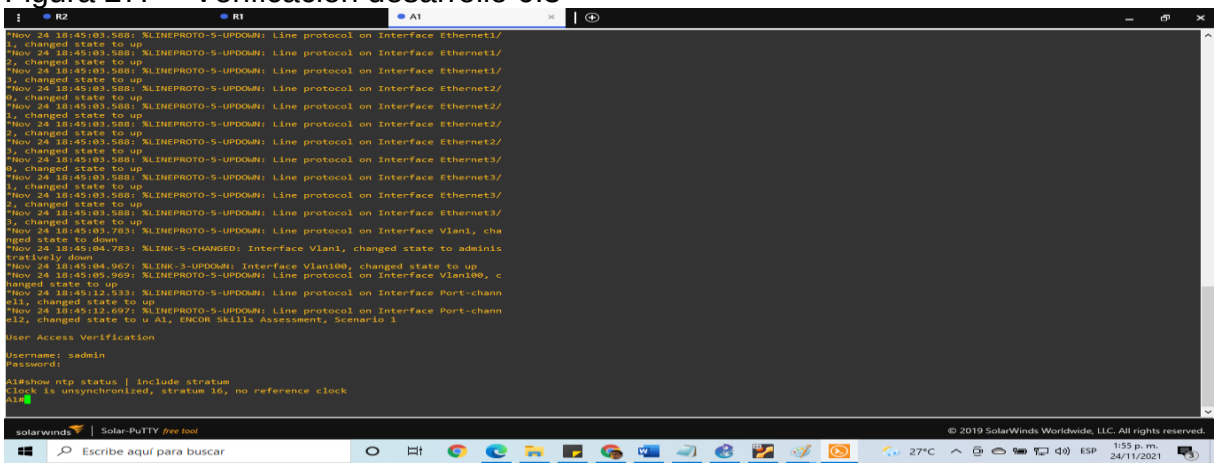
show run | incluir ntp
verificación de hora actual UTC correcta

R2 # show run | incluir ntp
ntp master 3

show ntp status | include stratum
permite verificar si NTP funciona, sincronización de tiempo y relojes y que estos se comuniquen exitosamente

A1# show ntp status | include stratum
Clock is synchronized, stratum 16

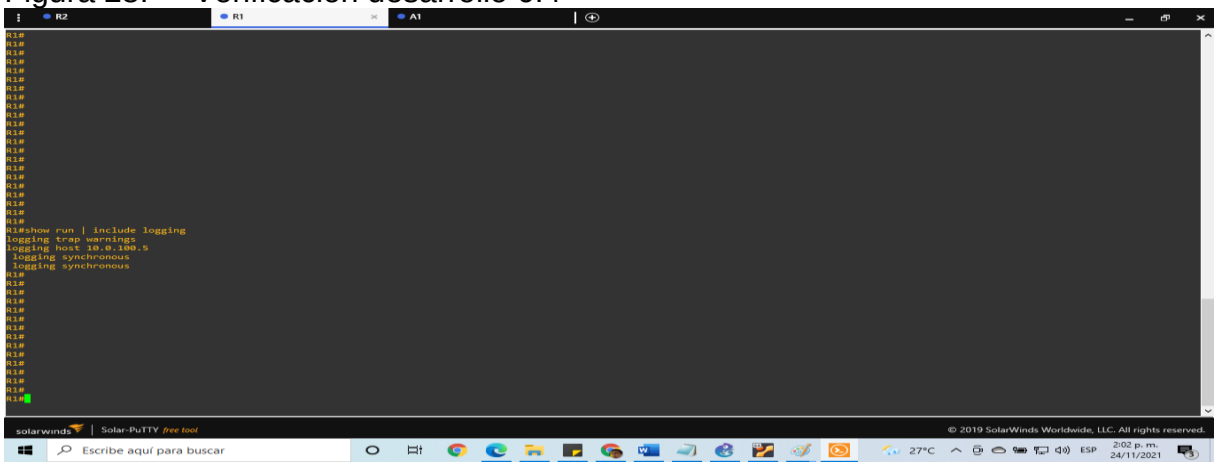
Figura 27. Verificación desarrollo 6.3



show run | include logging
confirmación comando de registro

R1# show run | include logging
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous

Figura 28. Verificación desarrollo 6.4

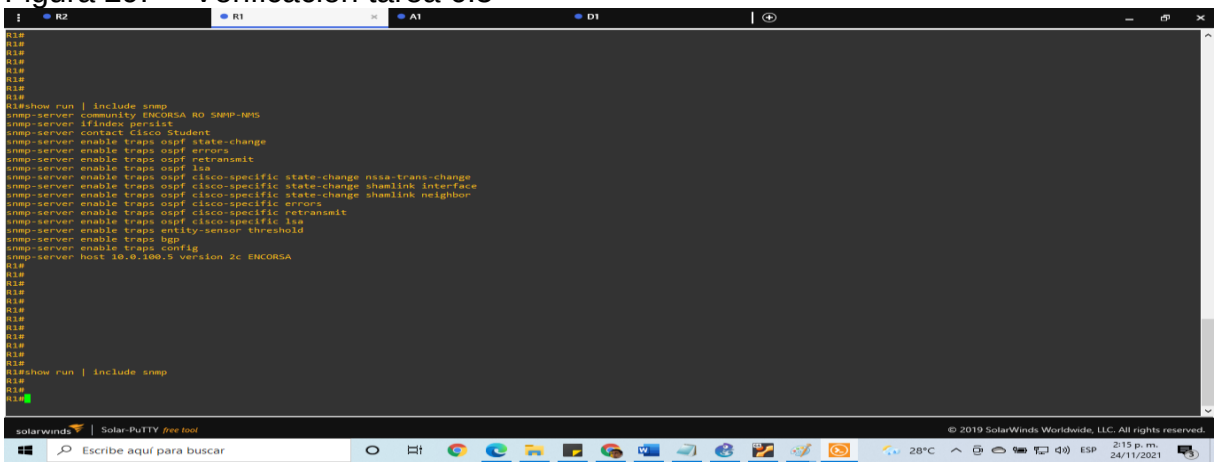


show run | include snmp
verifica la configuración de cadenas de la comunidad del protocolo simple de administración de redes

R1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS

snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-ch
snmp-server enable traps ospf cisco-specific state-ch
snmp-server enable traps ospf cisco-specific state-ch
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransm
snmp-server enable traps ospf cisco-specific lsa

Figura 29. Verificación tarea 6.5



CONCLUSIONES

Mediante el presente trabajo se busca obtener conocimientos prácticos para la creación, configuración y posterior uso de su servicio para las topologías de red, entender que componentes se necesitan para su viabilidad y eficacia en el momento de la ejecución. Desarrollando habilidades para el desarrollo integro y sistemático en las configuraciones de redes.

El presente trabajo cuenta con la formación de seis (6) puntos esenciales para el diseño de una topología de red, que cumpla con las siguientes condiciones: las configuraciones básicas de toda red como el enrutamiento e instalación de red DHCP y estáticas, cuenta con los parámetros necesarios como la seguridad computacional que hoy en día son primordiales para cualquier empresa proteger su base de datos e información que esta contenga.

Se organiza el documento con la transcripción de los comandos utilizados para su ejecución, acompañado de imágenes que permitan verificar su funcionamiento de forma correcta, de esta manera coordinar los procesos relacionados que se solicita en las guías.

La finalidad del trabajo para el diplomado CCNP es buscar que el estudiante indagué y defina mediante la investigación previa los elementos más relevantes en el momento de la ejecución para la administración de redes en cualquier tipo de escenario que incluya la configuración por medio de los comandos permitidos para este tipo de dispositivos.

BIBLIOGRAFIA

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

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

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

Wallace, K. (2015). CISCO Press (Ed). *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide*. https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl