

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DARWIN DURAN MYLES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
LA DORADA
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DARWIN DURAN MYLES

Diplomado de opción de grado presentado para optar el título de INGENIERÍA
ELECTRÓNICA

DIRECTOR:
Msc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
LA DORADA
2021

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN	8
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO	11
1. ESCENARIO 1	11
CONCLUSIONES	65
BIBLIOGRAFÍA	66
ANEXO 1. CONFIGURACION DE LOS DISPOSITIVOS	67

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento para la topología.	11
Tabla 2. Asignación de actividades 2.1.....	23
Tabla 3. Asignación de actividades 2.2.....	24
Tabla 4. Asignación de actividades 2.3.....	25
Tabla 5. Asignación de actividades 2.4.....	25
Tabla 6. Asignación de actividades 2.5.....	26
Tabla 7. Asignación de actividades 2.6.....	27
Tabla 8. Asignación de actividades 2.7.....	28
Tabla 9. Asignación de actividades 2.8.....	30
Tabla 10. Asignación de actividades 3.1.....	35
Tabla 11. Asignación de actividades 3.2.....	37
Tabla 12. Asignación de actividades 3.3.....	40
Tabla 13. Asignación de actividades 3.4.....	42
Tabla 14. Asignación de actividades 4.1.....	44
Tabla 15. Asignación de actividades 4.2.....	45
Tabla 16. Asignación de actividades 4.3.....	47
Tabla 17. Asignación de actividades 5.1.....	51
Tabla 18. Asignación de actividades 5.2.....	52
Tabla 19. Asignación de actividades 5.3.....	54
Tabla 20. Asignación de actividades 5.4.....	54
Tabla 21. Asignación de actividades 5.5.....	56
Tabla 22. Asignación de actividades 5.6.....	57
Tabla 23. Asignación de actividades 6.1.....	57
Tabla 24. Asignación de actividades 6.2.....	58
Tabla 25. Asignación de actividades 6.3.....	59
Tabla 26. Asignación de actividades 6.4.....	60
Tabla 27. Asignación de actividades 6.5.....	61

LISTA DE FIGURAS

Figura 1. Topología que representa el escenario 1.....	11
Figura 2. Verificación de los servicios DHCP IPv4 en PC2.....	29
Figura 3. Verificación de los servicios DHCP IPv4 en PC3.....	30
Figura 4. Prueba de ping desde PC1 a D1, D2 y PC4.....	31
Figura 5. Prueba de ping desde PC2 a D1 y D2.....	32
Figura 6. Prueba de ping desde PC3 a D1 y D2.....	33
Figura 7. Prueba de ping desde PC4 a D1, D2 y PC1.....	34

GLOSARIO

BGP: Protocolo de puerta de enlace fronteriza. Protocolo de enrutamiento entre dominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP. Está definido por RFC 1163.

NTP: Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

OSPF: Primero, abra el camino más corto. Algoritmo de enrutamiento IGP jerárquico de estado de enlace propuesto como sucesor de RIP en la comunidad de Internet. Las características de OSPF incluyen enrutamiento de menor costo, enrutamiento de múltiples rutas y equilibrio de carga. OSPF se derivó de una versión anterior del protocolo IS-IS.

VLAN: LAN virtual. Grupo de dispositivos en una o más LAN que están configurados (usando software de administración) para que puedan comunicarse como si estuvieran conectados al mismo cable, cuando en realidad están ubicados en varios segmentos de LAN diferentes. Debido a que las VLAN se basan en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

STP: Par trenzado blindado. Medio de cableado de dos pares utilizado en una variedad de implementaciones de red. El cableado STP tiene una capa de aislamiento blindado para reducir la EMI.

RESUMEN

En esta prueba de habilidades, se realiza la configuración completa de la red permitiendo que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace preterminada y para que los protocolos OSPF y BGP configurados estén operativos dentro de la parte correspondiente a la “Red de la Compañía” en la topología. Estos cambios en las configuraciones son verificados de acuerdo a las especificaciones dadas, cumpliendo cada uno de los detalles y asegurando que los dispositivos funcionen como es requerido.

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

ABSTRACT

In this skills test, the complete network configuration is performed allowing for complete end-to-end accessibility, for hosts to have reliable support of the default gateway, and for configured OSPF and BGP protocols to be operating within the part corresponding to the "Company Network" in the topology. These changes in the configurations are verified according to the given specifications, fulfilling each one of the details and ensuring that the devices work as required.

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

INTRODUCCIÓN

La evaluación denominada “DOCUMENTO FINAL”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, como estudiante se debe realizar una serie de tareas asignadas en el escenario propuesto, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

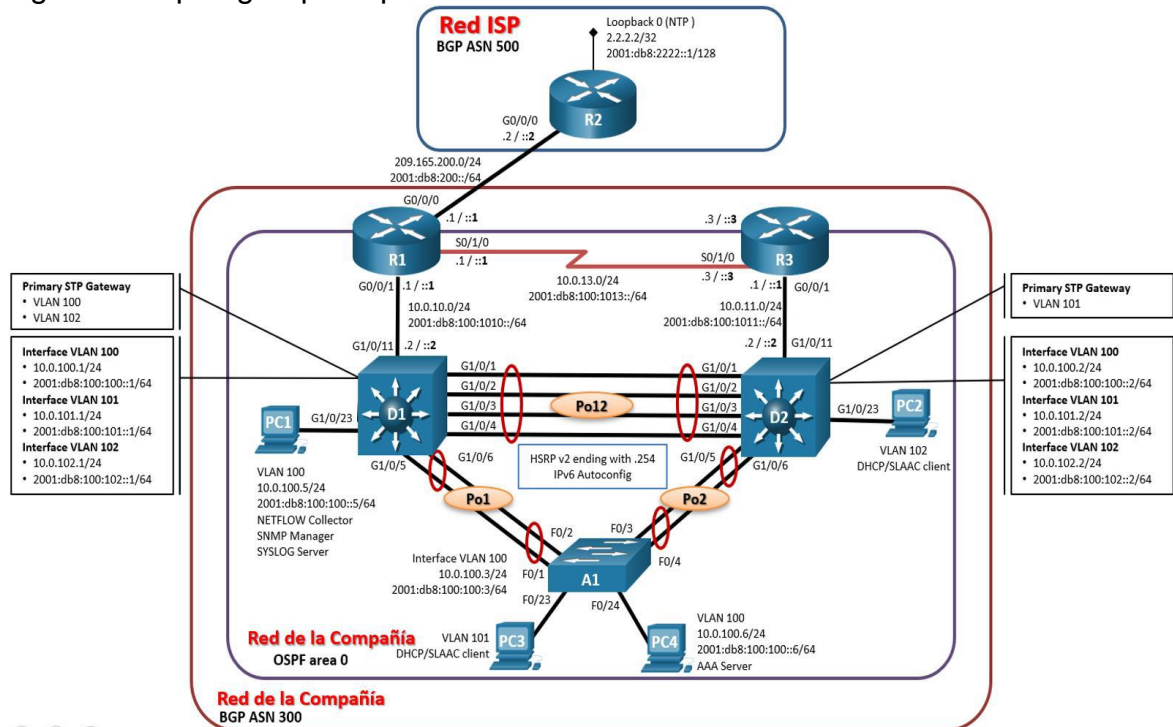
Finalmente se realiza la configuración de cada uno de los dispositivos, se presenta la información detallada y se anexa la configuración realizada.

DESARROLLO

1. ESCENARIO 1

Teniendo en la cuenta la siguiente imagen:

Figura 1. Topología que representa el escenario 1.



Fuente: Autor

1.1. Tabla de direccionamiento

Tabla 1. Tabla de direccionamiento para la topología.

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
	Loopback 0	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::1/6 4	fe80::d1: 2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/6 4	fe80::d1: 3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/6 4	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::2/6 4	fe80::d2: 2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/6 4	fe80::d2: 3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/6 4	fe80::d2: 4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/6 4	fe80::a1: 1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/6 4	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::6/6 4	EUI-64

Fuente: Autor.

1.2. 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)

1.3. 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 Compañía" 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 Catalyst 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.

1.4. 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

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

1.5.1. 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.

1.5.2. Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Router R1

hostname R1	Se asigna el nombre de host
ipv6 unicast-routing para ipv6	Se habilita el enrutamiento
no ip domain lookup ip de dominio	Se desactiva la búsqueda de
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0 de la consola	Se accede a la configuración
exec-timeout 0 0 la consola	Se habilita la desconexión de
logging synchronous sincronico	Se habilita el logeo
exit	
interface g0/0 gigabitEthernet	Se accede a la interface
ip address 209.165.200.225 255.255.255.224	Se configura la dirección ip
ipv6 address fe80::1:1 link-local local	Se configura la dirección link
ipv6 address 2001:db8:200::1/64	Se configura la dirección ipv6
no shutdown gigabitEthernet	Se enciende la interfaz
exit	
interface g2/0	Se accede a la interface
ip address 10.0.10.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::1:2 link-local local	Se configura la dirección link
ipv6 address 2001:db8:100:1010::1/64	Se configura la dirección ipv6

no shutdown	Se enciende la interfaz
exit	
interface s1/0	Se accede a la interface
serial	
ip address 10.0.13.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::1:3 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:1013::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Router R2

hostname R2	Se asigna el nombre de host
ipv6 unicast-routing	Se habilita el enrutamiento
para ipv6	
no ip domain lookup	Se desactiva la búsqueda de
ip de dominio	
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración
de la consola	
exec-timeout 0 0	Se habilita la desconexión de
la consola	
logging synchronous	Se habilita el logeo
sincronico	
exit	
interface g0/0	Se accede a la interface
gigabitEthernet	
ip address 209.165.200.226 255.255.255.224	Se configura la dirección ip
ipv6 address fe80::2:1 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:200::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface Loopback 0	Se accede a la interface
Loopback	
ip address 2.2.2.2 255.255.255.255	Se configura la dirección ip
ipv6 address fe80::2:3 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:2222::1/128	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Router R3

hostname R3	Se asigna el nombre de host
ipv6 unicast-routing para ipv6	Se habilita el enrutamiento
no ip domain lookup ip de dominio	Se desactiva la búsqueda de
banner motd # R3, ENCOR Skills Assessment, Scenario 1 # line con 0 de la consola	Se asigna un mensaje Se accede a la configuración
exec-timeout 0 0 la consola	Se habilita la desconexión de
logging synchronous sincronico	Se habilita el logueo
exit	
interface g2/0	Se accede a la interface
gigabitEthernet	
ip address 10.0.11.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::3:2 link-local local	Se configura la dirección link
ipv6 address 2001:db8:100:1011::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface s1/0	Se accede a la interface
serial	
ip address 10.0.13.3 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::3:3 link-local local	Se configura la dirección link
ipv6 address 2001:db8:100:1010::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Switch D1

hostname D1	Se asigna el nombre de host
ip routing	Se habilita el enrutamiento
ipv4	
ipv6 unicast-routing para ipv6	Se habilita el enrutamiento
no ip domain lookup ip de dominio	Se desactiva la búsqueda de
banner motd # D1, ENCOR Skills Assessment, Scenario 1 # line con 0 de la consola	Se asigna un mensaje Se accede a la configuración

exec-timeout 0 0	Se habilita la desconexión de
la consola	
logging synchronous	Se habilita el logueo
sincronico	
exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la
vlan	
exit	
vlan 101	Se configura la vlan
name UserGroupA	Se configura el nombre de la
vlan	
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la
vlan	
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la
vlan	
exit	
interface e2/0	Se accede a la interface
Ethernet	
no switchport	
ip address 10.0.10.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:1 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:1010::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 100	Se accede a la interface Vlan
ip address 10.0.100.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:2 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:100::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 101	Se accede a la interface Vlan
ip address 10.0.101.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:3 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:101::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 102	Se accede a la interface Vlan

ip address 10.0.102.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:4 link-local local	Se configura la dirección link local
ipv6 address 2001:db8:100:102::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.101.141 10.0.101.254	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.102.1 10.0.102.109	Se excluyen direcciones de la VLAN-102
ip dhcp excluded-address 10.0.102.141 10.0.102.254	Se excluyen direcciones de la VLAN-102
ip dhcp pool VLAN-101	Se crea un pool de
direcciones ip	
network 10.0.101.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.101.254	Se define la puerta de enlace
exit	
ip dhcp pool VLAN-102	Se crea un pool de
direcciones ip	
network 10.0.102.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.102.254	Se define la puerta de enlace
exit	
interface range e0/0-3, e1/0-3, e2/1	Se selecciona el rango de
interfaces que no se utilizarán	
shutdown	Se apagan las interfaces
exit	

Switch D2

hostname D2	Se asigna el nombre de host
ip routing	Se habilita el enrutamiento
ipv4	
ipv6 unicast-routing	Se habilita el enrutamiento
para ipv6	
no ip domain lookup	Se desactiva la búsqueda de
ip de dominio	
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración
de la consola	
exec-timeout 0 0	Se habilita la desconexión de
la consola	
logging synchronous	Se habilita el logueo
sincronico	

exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la
vlan	
exit	
vlan 101	Se configura la vlan
name UserGroupA	Se configura el nombre de la
vlan	
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la
vlan	
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la
vlan	
exit	
interface e2/0	Se accede a la interface
Ethernet	
no switchport	Se configura como un puerto
de capa 3	
ip address 10.0.11.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:1 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:1011::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 100	Se accede a la interface Vlan
ip address 10.0.100.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d2:2 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:100::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 101	Se accede a la interface Vlan
ip address 10.0.101.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d2:3 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:101::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 102	Se accede a la interface Vlan
ip address 10.0.102.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d2:4 link-local	Se configura la dirección link
local	

ipv6 address 2001:db8:100:102::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.209	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.101.241 10.0.101.254	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.102.1 10.0.102.209	Se excluyen direcciones de la VLAN-102
ip dhcp excluded-address 10.0.102.241 10.0.102.254	Se excluyen direcciones de la VLAN-102
ip dhcp pool VLAN-101	Se crea un pool de direcciones ip
network 10.0.101.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.101.254	Se define la puerta de enlace
exit	
ip dhcp pool VLAN-102	Se crea un pool de direcciones ip
network 10.0.102.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.102.254	Se define la puerta de enlace
exit	
interface range e0/0-3, e1/0-3, e2/1	Se selecciona el rango de interfaces que no se utilizarán
shutdown	Se apagan las interfaces
exit	

Switch A1

hostname A1	Se asigna el nombre de host
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje de la consola
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconexión de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la vlan
exit	
vlan 101	Se configura la vlan

name UserGroupA	Se configura el nombre de la
vlan	
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la
vlan	
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la
vlan	
exit	
interface vlan 100	Se accede a la interface
Ethernet	
ip address 10.0.100.3 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::a1:1 link-local	Se configura la dirección link
local	
ipv6 address 2001:db8:100:100::3/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface range e1/2-3	Se selecciona el rango de
interfaces que no se utilizarán	
shutdown	Se apagan las interfaces
exit	

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

Router R1

R1#copy ru st config R1#	Copia el archivo running
--------------------------------	--------------------------

Router R2

R2#copy ru st config R2#	Copia el archivo running
--------------------------------	--------------------------

Router R3

R3#copy ru st config R3#	Copia el archivo running
--------------------------------	--------------------------

Switch D1

D1#copy ru st
config
D1#

Copia el archivo running

Switch D2

D2#copy ru st
config
D2#

Copia el archivo running

Switch A1

A1#copy ru st
config
A1#

Copia el archivo running

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.

Host PC1

PC1> ip 10.0.100.5 255.255.255.0 10.0.100.254 Se configura el
direccionamiento en el VPC
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> ip 2001:db8:100:100::5/64 Se configura el
direccionamiento IPV6 en el VPC
PC1 : 2001:db8:100:100::5/64

PC1>

Host PC4

PC4> ip 10.0.100.6 255.255.255.0 10.0.100.254 Se configura el
direccionamiento en el VPC
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> ip 2001:db8:100:100::6/64 Se configura el
direccionamiento IPV6 en el VPC
PC1 : 2001:db8:100:100::6/64

PC4>

1.6. 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 debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 2. Asignación de actividades 2.1.

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: <ul style="list-style-type: none">• D1 and D2• D1 and A1• D2 and A1

Fuente: Autor.

Switch D1

D1#configure terminal

D1(config)# interface range e0/0-3, e1/0-1 Se seleccionan las interfaces troncales

D1(config-if-range)#switchport trunk encapsulation dot1q Se habilita la encapsulación dot1q en el puerto

D1(config-if-range)#switchport mode trunk Se habilita el puerto en modo troncal

D1(config-if-range)#no shutdown Se enciende la interfaz

D1(config-if-range)#

Switch D2

D2#configure terminal

D2(config)#interface range e0/0-3, e1/0-1 Se seleccionan las interfaces troncales

D2(config-if-range)#switchport trunk encapsulation dot1q Se habilita la encapsulación dot1q en el puerto

D2(config-if-range)#switchport mode trunk Se habilita el puerto en modo troncal

D2(config-if-range)#no shutdown Se enciende la interfaz

Tabla 4. Asignación de actividades 2.3.

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

Fuente: Autor.

Switch D1

D1(config)#spanning-tree mode rapid-pvst
Tree en el switch

Se habilita Rapid Spanning

Switch D2

D2(config)#spanning-tree mode rapid-pvst
Tree en el switch

Se habilita Rapid Spanning

Switch A1

A1(config)#spanning-tree mode rapid-pvst
Tree en el switch

Se habilita Rapid Spanning

Tabla 5. Asignación de actividades 2.4.

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.
-----	--	--

Fuente: Autor.

Switch D1

D1(config)#spanning-tree vlan 100,102 root primary RSTP

Se configura el puente raíz

D1(config)#spanning-tree vlan 101 root secondary respaldo

Se configura el puente de

Switch D2

D2(config)#spanning-tree vlan 101 root primary RSTP Se configura el puente raíz

D2(config)#spanning-tree vlan 100,102 root secondary de respaldo Se configura el puente de respaldo

Tabla 6. Asignación de actividades 2.5.

2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
-----	---	---

Fuente: Autor.

Switch D1

D1(config)#interface range e0/0-3 Se seleccionan las interfaces

D1(config-if-range)#channel-group 12 mode active Se configura el canal del grupo y en modo activo

D1(config-if-range)#exit

D1(config)#interface range e1/0-1 Se seleccionan las interfaces

D1(config-if-range)#channel-group 1 mode active Se configura el canal del grupo y en modo activo

D1(config-if-range)#exit

Switch D2

D2(config)#interface range e0/0-3 Se seleccionan las interfaces

D2(config-if-range)#channel-group 12 mode active Se configura el canal del grupo y en modo activo

D2(config-if-range)#exit

D2(config)#interface range e1/0-1 Se seleccionan las interfaces

D2(config-if-range)#channel-group 2 mode active Se configura el canal del grupo y en modo activo

D2(config-if-range)#exit

Switch A1

A1(config)#interface range e0/0-1	Se seleccionan las interfaces
A1(config-if-range)#channel-group 1 mode active grupo y en modo activo	Se configura el canal del grupo y en modo activo
A1(config-if-range)#exit	
A1(config)#interface range e0/2-3	Se seleccionan las interfaces
A1(config-if-range)#channel-group 2 mode active grupo y en modo activo	Se configura el canal del grupo y en modo activo
A1(config-if-range)#exit	

Tabla 7. Asignación de actividades 2.6.

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).
-----	---	---

Fuente: Autor.

Switch D1

D1(config)#interface e2/1	Se selecciona la interfaz
D1(config-if)#switchport mode Access acceso	Se configura en modo de acceso
D1(config-if)#switchport access vlan 100	Se asigna la vlan al puerto
D1(config-if)#spanning-tree portfast	Se habilita portfast
D1(config-if)#no shutdown	Se enciende la interfaz
D1(config-if)#exit	

Switch D2

D2(config)#interface e2/1	Se selecciona la interfaz
D2(config-if)#switchport mode Access acceso	Se configura en modo de acceso
D2(config-if)#switchport access vlan 102	Se asigna la vlan al puerto

D2(config-if)#spanning-tree portfast	Se habilita portfast
D2(config-if)#no shutdown	Se enciende la interfaz
D2(config-if)#exit	

Switch A1

A1(config)#interface e1/0	Se selecciona la interfaz
A1(config-if)#switchport mode Access	Se configura en modo de acceso
A1(config-if)#switchport access vlan 101	Se asigna la vlan al puerto
A1(config-if)#spanning-tree portfast	Se habilita portfast
A1(config-if)#no shutdown	Se enciende la interfaz
A1(config-if)#exit	
A1(config)#interface e1/1	Se selecciona la interfaz
A1(config-if)#switchport mode Access	Se configura en modo de acceso
A1(config-if)#switchport access vlan 100	Se asigna la vlan al puerto
A1(config-if)#spanning-tree portfast	Se habilita portfast
A1(config-if)#no shutdown	Se enciende la interfaz
A1(config-if)#exit	

Tabla 8. Asignación de actividades 2.7.

2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
-----	------------------------------------	---

Fuente: Autor.

Host PC2

PC2> ip dhcp DHCP DDORA IP 10.0.102.210/24 GW 10.0.102.254 PC2>	Se configura ipv4 por
--	-----------------------

Figura 2. Verificación de los servicios DHCP IPv4 en PC2.

```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> clear ipv6
IPv6 address/mask and router link-layer address cleared

PC2> ip auto
GLOBAL SCOPE      : 2001:db8:100:102:2050:79ff:fe66:6801/64
ROUTER LINK-LAYER : aa:bb:cc:80:01:00

PC2> █
```

Fuente: Autor.

Host PC3

```
PC3> ip dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254      Se configura ipv4 por DHCP
PC3>
```

Figura 3. Verificación de los servicios DHCP IPv4 en PC3.



Fuente: Autor.

Tabla 9. Asignación de actividades 2.8.

2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.101.1
-----	---	--

		<ul style="list-style-type: none"> • D2: 10.0.101.2 <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5
--	--	---

Fuente: Autor.

Prueba ping PC1

Figura 4. Prueba de ping desde PC1 a D1, D2 y PC4.

```

PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.215 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.340 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.292 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.340 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.339 ms
^[A
PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.223 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.402 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.507 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.391 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.441 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.215 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=0.361 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.402 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.332 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.418 ms

PC1> █

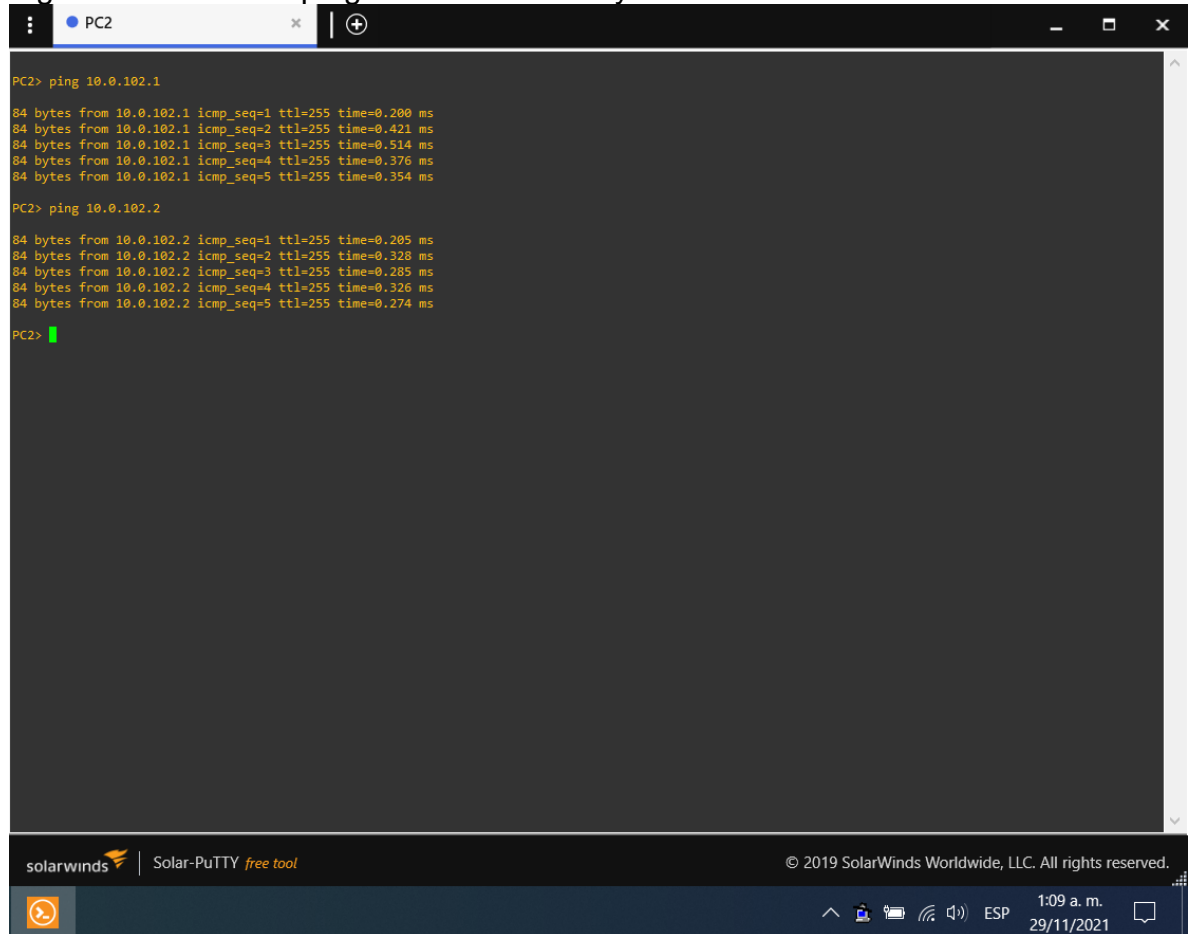
```

The screenshot shows a PuTTY terminal window titled 'PC1'. The terminal output displays the results of three ping tests performed from PC1. The first test is to 10.0.100.1, the second to 10.0.100.2, and the third to 10.0.100.6. Each test shows five successful responses with varying round-trip times. The terminal interface includes a status bar at the bottom with 'solarwinds Solar-PuTTY free tool' and a system tray showing the time as 1:07 a.m. on 29/11/2021.

Fuente: Autor.

Prueba ping PC2

Figura 5. Prueba de ping desde PC2 a D1 y D2.



```
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.200 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.421 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.514 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.376 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.354 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.205 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.328 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.285 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.326 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.274 ms

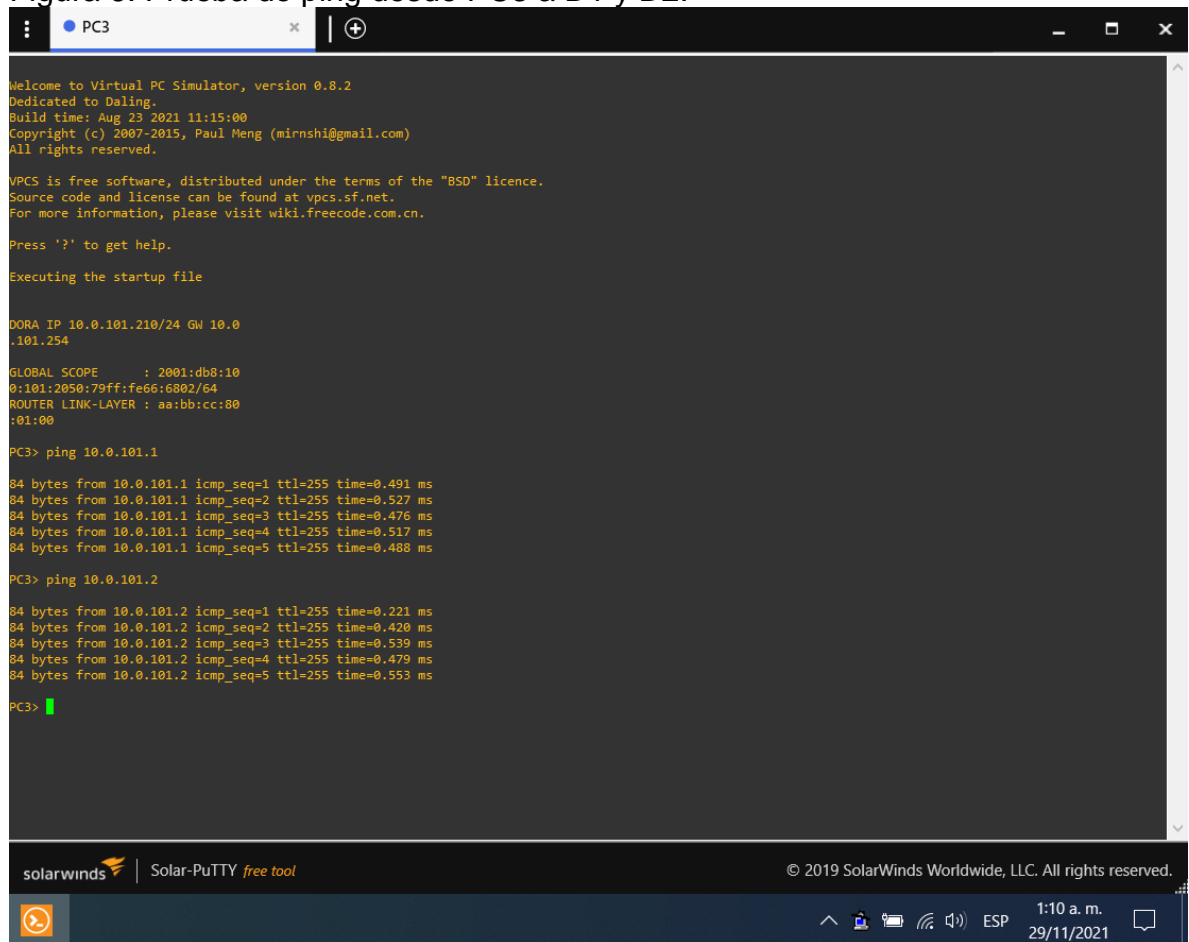
PC2> █
```

solarwinds | Solar-PuTTY *free tool* © 2019 SolarWinds Worldwide, LLC. All rights reserved. 1:09 a. m. 29/11/2021

Fuente: Autor.

Prueba ping PC3

Figura 6. Prueba de ping desde PC3 a D1 y D2.



```
PC3
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

DORA IP 10.0.101.210/24 GW 10.0
.101.254

GLOBAL SCOPE      : 2001:db8:10
0:101:2050:79ff:fe66:6802/64
ROUTER LINK-LAYER : aa:bb:cc:80
:01:00

PC3> ping 10.0.101.1

84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.491 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.527 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=0.476 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=0.517 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.488 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.221 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.420 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=0.539 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.479 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.553 ms

PC3> █
```

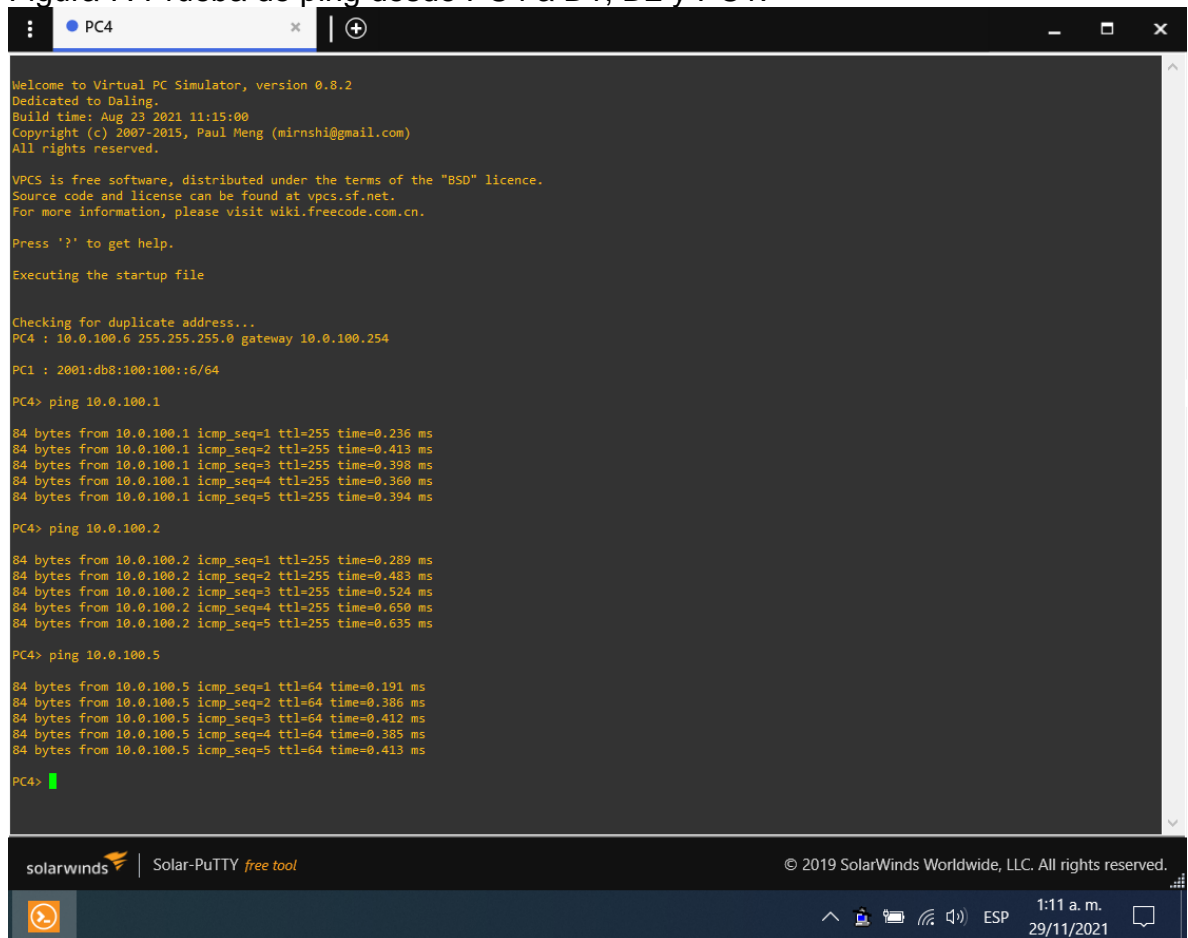
solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

1:10 a. m. 29/11/2021

Fuente: Autor.

Prueba ping PC4

Figura 7. Prueba de ping desde PC4 a D1, D2 y PC1.



```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC1 : 2001:db8:100:100::6/64

PC4> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.236 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.413 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.398 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.360 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.394 ms

PC4> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.289 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.483 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.524 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.650 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.635 ms

PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.191 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.386 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.412 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.385 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.413 ms

PC4> █
```

Fuente: Autor.

1.7. 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 10. Asignación de actividades 3.1.

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	<p>Use OSPF Process ID 4 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • 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. <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

Fuente: Autor.

Router R1

R1#configure terminal	
R1(config)#router ospf 4	Se habilita OSPF con su indicador
R1(config-router)#router-id 0.0.4.1	Se configura el identificador
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0	Se configura las redes y su área

R1(config-router)#network 10.0.13.0 0.0.0.255 area 0 Se configura las redes y su área
R1(config-router)#default-information originate Se genera una ruta predetermina
R1(config-router)#exit
R1(config)#

Router R3

R3#configure terminal
R3(config)#router ospf 4 Se habilita OSPF con su indicador
R3(config-router)#router-id 0.0.4.3 Se configura el identificador
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0 Se configura las redes y su área
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0 Se configura las redes y su área
R3(config-router)#exit
R3(config)#

Switch D1

D1#configure terminal
D1(config)#router ospf 4 Se habilita OSPF con su indicador
D1(config-router)#router-id 0.0.4.131 Se configura el identificador
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#passive-interface default Se configuran las interfaces como pasivas
D1(config-router)#no passive-interface e2/0 Se excluye la interfaz de estar pasiva
D1(config-router)#exit

Switch D2

D2#configure terminal	
D2(config)#router ospf 4	Se habilita OSPF con su indicador
D2(config-router)#router-id 0.0.4.132	Se configura el identificador
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0	Se configura las redes y su área
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0	Se configura las redes y su área
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0	Se configura las redes y su área
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0	Se configura las redes y su área
D2(config-router)#passive-interface default	Se configuran las interfaces como pasivas
D2(config-router)#no passive-interface e2/0	Se excluye la interfaz de estar pasiva
D2(config-router)#exit	

Tabla 11. Asignación de actividades 3.2.

3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>Use OSPF Process ID 6 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none">• R1: 0.0.6.1• R3: 0.0.6.3• D1: 0.0.6.131• D2: 0.0.6.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none">• En R1, no publique la red R1 – R2.• On R1, propague una ruta por defecto. <p>Note que la ruta por defecto deberá ser provista por BGP.</p>
-----	--	--

		<p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
--	--	--

Fuente: Autor

Router R1

R1(config)#ipv6 router ospf 6
indicador

Se habilita OSPF con su

R1(config-rtr)#router-id 0.0.6.1

Se configura el identificador

R1(config-rtr)#default-information originate
predetermina

Se genera una ruta

R1(config-rtr)#exit

R1(config)#interface gi2/0

Se accede a la interfaz

R1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área

Se habilita OSPFv6 en la

R1(config-if)#exit

R1(config)#interface se1/0

Se accede a la interfaz

R1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área

Se habilita OSPFv6 en la

R1(config-if)#exit

Router R3

R3(config)#ipv6 router ospf 6
indicador

Se habilita OSPF con su

R3(config-rtr)#router-id 0.0.6.3

Se configura el identificador

R3(config-rtr)#exit

R3(config)#interface gi2/0

Se accede a la interfaz

R3(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área

Se habilita OSPFv6 en la

R3(config-if)#exit

R3(config)#interface se1/0
R3(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área
R3(config-if)#exit

Se accede a la interfaz
Se habilita OSPFv6 en la

Switch D1

D1(config)#ipv6 router ospf 6
indicador
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
como pasivas
D1(config-rtr)#no passive-interface e2/0
estar pasiva
D1(config-rtr)#exit
D1(config)#interface e2/0
D1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
interfaz y se configura el área
D1(config-if)#exit
D1(config)#

Se habilita OSPF con su
Se configura el identificador
Se configuran las interfaces
Se excluye la interfaz de
Se accede a la interfaz
Se habilita OSPFv6 en la
Se accede a la interfaz
Se habilita OSPFv6 en la
Se accede a la interfaz
Se habilita OSPFv6 en la
Se accede a la interfaz
Se habilita OSPFv6 en la

Switch D2

D2(config)#ipv6 router ospf 6
indicador
D2(config-rtr)#router-id 0.0.6.132

Se habilita OSPF con su
Se configura el identificador

D2(config-rtr)#passive-interface default como pasivas	Se configuran las interfaces
D2(config-rtr)#no passive-interface e2/0 estar pasiva	Se excluye la interfaz de
D2(config-rtr)#exit	
D2(config)#interface e2/0	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 100	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 101	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 102	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#	

Tabla 12. Asignación de actividades 3.3.

3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p>
-----	--	---

		<p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
--	--	---

Fuente: Autor.

Router R2

R2#configure terminal

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 Se configura una ruta predeterminada con interfaz de salida loopback

R2(config)#ipv6 route ::/0 loopback 0 Se configura una ruta IPv6 predeterminada con interfaz de salida loopback

R2(config)#router bgp 500 Se configura bgp 500

R2(config-router)# bgp router-id 2.2.2.2 Se asigna un identificador bgp

R2(config-router)# neighbor 209.165.200.225 remote-as 300 Se configura la relación con R1 en ASN 300

R2(config-router)# neighbor 2001:db8:200::1 remote-as 300 Se configura la relación con R1 en ASN 300

R2(config-router)# address-family ipv4

R2(config-router-af)# neighbor 209.165.200.225 activate Se configura la relación con el vecino activa

R2(config-router-af)# no neighbor 2001:db8:200::1 activate Se excluye la dirección IPv6

R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255 Se configura la relación con la interface loopback de R2

R2(config-router-af)# network 0.0.0.0 Redes predeterminadas

R2(config-router-af)# exit-address-family

R2(config-router)# address-family ipv6

R2(config-router-af)# no neighbor 209.165.200.225 activate Se configura la relación con el vecino activa

R2(config-router-af)# neighbor 2001:db8:200::1 activate Se incluye la dirección IPv6

R2(config-router-af)# network 2001:db8:2222::/128 Se excluye la dirección IPv6

R2(config-router-af)# network ::/0 Redes predeterminadas

R2(config-router-af)# exit-address-family

R2(config-router)#

Tabla 13. Asignación de actividades 3.4.

3.4	En R1 en la “Red ISP”, configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • • Una ruta resumen IPv4 para 10.0.0.0/8. • • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • • Deshabilite la relación de vecino IPv6. • • Habilite la relación de vecino IPv4. • • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • • Deshabilite la relación de vecino IPv4. • • Habilite la relación de vecino IPv6. • • Anuncie la red 2001:db8:100::/48.
-----	--	--

Fuente: Autor.

Router R1

R1(config)#ip route 10.0.0.0 255.0.0.0 null0	Se configura una ruta
predeterminada con interfaz de salida	
R1(config)#ipv6 route 2001:db8:100::/48 null0	Se configura una ruta IPv6
predeterminada con interfaz de salida	
R1(config)#router bgp 300	Se configura bgp 300
R1(config-router)# bgp router-id 1.1.1.1	Se asigna un identificador
bgp	
R1(config-router)# neighbor 209.165.200.226 remote-as 500	Se configura la
relación con R2 en ASN 500	
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500	Se configura la
relación con R2 en ASN 500	
R1(config-router)# address-family ipv4 unicast	
R1(config-router-af)# neighbor 209.165.200.226 activate	Se configura la
relación con el vecino activa	
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	Se deshabilita la
relación con el vecino activa	
R1(config-router-af)# neighbor 2001:db8:200::2 activate	Se configura la
relación con el vecino activa	
R1(config-router-af)# network 2001:db8:100::/48	Se configura la dirección ipv6
R1(config-router-af)# exit-address-family	
R1(config-router)#exit	
R1(config)#	

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

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

Tabla 14. Asignación de actividades 4.1.

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>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.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>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.</p>

Fuente: Autor.

Configuración en D1.

D1#configure terminal	
D1(config)#ip sla 4	Se configura sla
D1(config-ip-sla)#icmp-echo 10.0.10.1 probar	Se configura la interfaz a probar
D1(config-ip-sla-echo)#frequency 5	Se configura la frecuencia
D1(config-ip-sla-echo)#exit	
D1(config)#ip sla 6	Se configura sla
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 probar	Se configura la interfaz a probar
D1(config-ip-sla-echo)#frequency 5	Se configura la frecuencia
D1(config-ip-sla-echo)#exit	
D1(config)#ip sla schedule 4 life forever start-time now del sla	Se activa la operación del sla
D1(config)#ip sla schedule 6 life forever start-time now del sla	Se activa la operación del sla

D1(config)#track 4 ip sla 4 de estado de IP SLA	Se configura un verificador
D1(config-track)#delay down 10 up 15 después de 10 segundos, o de Up a Down después de 15 segundos	Cambia de Down a Up
D1(config-track)#exit	
D1(config)#track 6 ip sla 6 de estado de IP SLA	Se configura un verificador
D1(config-track)#delay down 10 up 15 después de 10 segundos, o de Up a Down después de 15 segundos	Cambia de Down a Up
D1(config-track)#exit	
D1(config)#	

Tabla 15. Asignación de actividades 4.2.

4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>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.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>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.</p>
-----	--	--

Fuente: Autor.

Configuración en D2.

D2#configure terminal	
D2(config)#ip sla 4	Se configura sla
D2(config-ip-sla)#icmp-echo 10.0.11.1 probar	Se configura la interfaz a
D2(config-ip-sla-echo)#frequency 5	Se configura la frecuencia

D2(config-ip-sla-echo)#exit	
D2(config)#ip sla 6	Se configura sla
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1	Se configura la
interfaz a probar	
D2(config-ip-sla-echo)#frequency 5	Se configura la frecuencia
D2(config-ip-sla-echo)#exit	
D2(config)#ip sla schedule 4 life forever start-time now	Se activa la operación
del sla	
D2(config)#ip sla schedule 6 life forever start-time now	Se activa la operación
del sla	
D2(config)#track 4 ip sla 4	Se configura un verificador
de estado de IP SLA	
D2(config-track)#delay down 10 up 15	Cambia de Down a Up
después de 10 segundos, o de Up a Down después de 15 segundos	
D2(config-track)#exit	
D2(config)#track 6 ip sla 6	Se configura un verificador
de estado de IP SLA	
D2(config-track)#delay down 10 up 15	Cambia de Down a Up
después de 10 segundos, o de Up a Down después de 15 segundos	
D2(config-track)#exit	
D2(config)#	

Tabla 16. Asignación de actividades 4.3.

4.3	En D1 configure HSRPv2.	<p>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.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • • 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. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • • Asigne la dirección IP virtual 10.0.101.254. • • Habilite la preferencia (preemption). • • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • • 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. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • • 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. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • • Asigne la dirección IP virtual usando ipv6 autoconfig. • • Habilite la preferencia (preemption). • • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • • Asigne la dirección IP virtual usando ipv6 autoconfig.
-----	-------------------------	---

		<ul style="list-style-type: none"> • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.
	<p>En D2, configure HSRPv2.</p>	<p>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:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

		<p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.
--	--	--

Configuración en D1.

D1(config)#interface vlan 100	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 104 ip 10.0.100.254	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 104 priority 150	Se establece la prioridad del grupo en 150
D1(config-if)#standby 104 preempt	Se habilita la preferencia
D1(config-if)#standby 104 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#standby 106 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 106 priority 150	Se establece la prioridad del grupo en 150
D1(config-if)#standby 106 preempt	Se habilita la preferencia
D1(config-if)#standby 106 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#exit	
D1(config)#interface vlan 101	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 114 ip 10.0.101.254	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 114 preempt	Se habilita la preferencia

D1(config-if)#standby 114 track 4 decrement 60 decrementa en 60	Se rastrea el objeto y
D1(config-if)#standby 116 ipv6 autoconfig virtual para el respectivo grupo	Se asigna la dirección IP
D1(config-if)#standby 116 preempt	Se habilita la preferencia
D1(config-if)#standby 116 track 6 decrement 60 decrementa en 60	Se rastrea el objeto y
D1(config-if)#exit	
D1(config)#interface vlan 102	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 124 ip 10.0.102.254 virtual para el respectivo grupo	Se asigna la dirección IP
D1(config-if)#standby 124 priority 150 grupo	Se configura la prioridad del
D1(config-if)#standby 124 preempt	Se habilita la preferencia
D1(config-if)#standby 124 track 4 decrement 60 decrementa en 60	Se rastrea el objeto y
D1(config-if)#standby 126 ipv6 autoconfig virtual para el respectivo grupo	Se asigna la dirección IP
D1(config-if)#standby 126 priority 150 grupo	Se configura la prioridad del
D1(config-if)#standby 126 preempt	Se habilita la preferencia
D1(config-if)#standby 126 track 6 decrement 60 decrementa en 60	Se rastrea el objeto y
D1(config-if)#exit	

Configuración en D2.

D2(config)#interface vlan 100	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2
D2(config-if)# standby 104 ip 10.0.100.254 virtual para el respectivo grupo	Se asigna la dirección IP
D2(config-if)# standby 104 preempt	Se habilita la preferencia
D2(config-if)# standby 104 track 4 decrement 60 decrementa en 60	Se rastrea el objeto y
D2(config-if)# standby 106 ipv6 autoconfig virtual para el respectivo grupo	Se asigna la dirección IP
D2(config-if)# standby 106 preempt	Se habilita la preferencia
D2(config-if)# standby 106 track 6 decrement 60 decrementa en 60	Se rastrea el objeto y
D2(config-if)# exit	
D2(config)#interface vlan 101	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2
D2(config-if)# standby 114 ip 10.0.101.254 virtual para el respectivo grupo	Se asigna la dirección IP

D2(config-if)# standby 114 priority 150 grupo en 150	Se establece la prioridad del grupo en 150
D2(config-if)# standby 114 preempt	Se habilita la preferencia
D2(config-if)# standby 114 track 4 decrement 60 decrementa en 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# standby 116 ipv6 autoconfig virtual para el respectivo grupo	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 116 priority 150 grupo en 150	Se establece la prioridad del grupo en 150
D2(config-if)# standby 116 preempt	Se habilita la preferencia
D2(config-if)# standby 116 track 6 decrement 60 decrementa en 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# exit	
D2(config)#interface vlan 102	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2
D2(config-if)# standby 124 ip 10.0.102.254 virtual para el respectivo grupo	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 124 preempt	Se habilita la preferencia
D2(config-if)# standby 124 track 4 decrement 60 decrementa en 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# standby 126 ipv6 autoconfig virtual para el respectivo grupo	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 126 preempt	Se habilita la preferencia
D2(config-if)# standby 126 track 6 decrement 60 decrementa en 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# exit	

1.9. 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 17. Asignación de actividades 5.1.

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco

Fuente: Autor.

Configuración en R1.

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Configuración en R2.

R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Configuración en R3.

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Configuración en D1.

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Configuración en D2.

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Configuración en A1.

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT

Tabla 18. Asignación de actividades 5.2.

5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: sadmin • Nivel de privilegio 15 • Contraseña: cisco12345cisco
-----	--	--

Fuente: Autor.

Configuración en R1.

```
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Configuración en R2.

```
R2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Configuración en R3.

```
R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Configuración en D1.

```
D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Configuración en D2.

```
D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Configuración en A1.

```
A1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret
cisco12345cisco Se crea un usuario
local protegido con el algoritmo de encriptación SCRYPT
```

Tabla 19. Asignación de actividades 5.3.

5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
-----	---	---------------

Fuente: Autor.

Configuración en R1.

R1(config)#aaa new-model Se habilita AAA

Configuración en R3.

R3(config)#aaa new-model Se habilita AAA

Configuración en D1.

D1(config)#aaa new-model Se habilita AAA

Configuración en D2.

D2(config)#aaa new-model Se habilita AAA

Configuración en A1.

A1(config)#aaa new-model Se habilita AAA

Tabla 20. Asignación de actividades 5.4.

5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"> • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: \$strongPass
-----	---	--

Fuente: Autor.

D1(config)#aaa authentication login default group radius local Se configura la lista de métodos de autenticación AAA

Configuración en D2.

D2(config)#aaa authentication login default group radius local Se configura la lista de métodos de autenticación AAA

Configuración en A1.

A1(config)#aaa authentication login default group radius local Se configura la lista de métodos de autenticación AAA

Tabla 22. Asignación de actividades 5.6.

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 .
-----	--	--

Fuente: Autor.

1.10. 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 23. Asignación de actividades 6.1.

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.

Fuente: Autor.

Configuración en R1.

R1(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Configuración en R2.

R2(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Configuración en R3.

R3(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Configuración en D1.

D1(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Configuración en D2.

D2(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Configuración en A1.

A1(config)#clock timezone utc -5
la hora UTC actual

Se configura el reloj a

Tabla 24. Asignación de actividades 6.2.

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

Fuente: Autor.

Configuración en R2.

R2(config)#ntp master 3
NTP maestro

Se configura como

Tabla 25. Asignación de actividades 6.3.

6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none">• R1 debe sincronizar con R2.• R3, D1 y A1 para sincronizar la hora con R1.• D2 para sincronizar la hora con R3.
-----	--	--

Fuente: Autor.

Configuración en R1.

R1(config)#ntp server 2.2.2.2

Se sincroniza NTP

Configuración en R3.

R3(config)#ntp server 10.0.10.1

Se sincroniza NTP

Configuración en D1.

D1(config)#ntp server 10.0.10.1

Se sincroniza NTP

Configuración en D2.

D2(config)#ntp server 10.0.10.1

Se sincroniza NTP

Configuración en A1.

A1(config)#ntp server 10.0.10.1

Se sincroniza NTP

Tabla 26. Asignación de actividades 6.4.

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.
-----	---	--

Fuente: Autor.

Configuración en R1.

R1(config)#logging trap warning Syslog de peligro	Se configura el
R1(config)#logging host 10.0.100.5 del syslog a la PC1	Se configura el envío
R1(config)#logging on	Se habilita el syslog

Configuración en R3.

R3(config)#logging trap warning Syslog de peligro	Se configura el
R3(config)#logging host 10.0.100.5 del syslog a la PC1	Se configura el envío
R3(config)#logging on	Se habilita el syslog

Configuración en D1.

D1(config)#logging trap warning Syslog de peligro	Se configura el
D1(config)#logging host 10.0.100.5 del syslog a la PC1	Se configura el envío
D1(config)#logging on	Se habilita el syslog

Configuración en D2.

D2(config)#logging trap warning Syslog de peligro	Se configura el
D2(config)#logging host 10.0.100.5 del syslog a la PC1	Se configura el envío
D2(config)#logging on	Se habilita el syslog

Configuración en A1.

A1(config)#logging trap warning Syslog de peligro	Se configura el
A1(config)#logging host 10.0.100.5 del syslog a la PC1	Se configura el envío
A1(config)#logging on	Se habilita el syslog

Tabla 27. Asignación de actividades 6.5.

6.5	Configure SNMPv2c en todos los dispositivos excepto R2	<p>Especificaciones de SNMPv2:</p> <ul style="list-style-type: none"> • Únicamente 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 <i>community string</i> en ENCORSA. • En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>. • En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>. • En A1, habilite el envío de <i>traps config</i>.
-----	--	---

Fuente: Autor.

Configuración en R1.

R1(config)#ip access-list standard SNMP de acceso estándar	Se configura una lista
R1(config-std-nacl)#permit host 10.0.100.5 dirección del PC1	Se permite SNMP a la
R1(config-std-nacl)#exit	
R1(config)#snmp-server contact Darwin Duran contacto SNMP	Se configura el valor de

R1(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
R1(config)# snmp-server ifindex persist	Se habilita la persistencia de index
R1(config)# snmp-server enable traps bgp	Se habilita el envío de traps bgp
R1(config)# snmp-server enable traps config	Se habilita el envío de traps config
R1(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

Configuración en R3.

R3(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
R3(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
R3(config-std-nacl)#exit	
R3(config)#snmp-server contact Darwin Duran	Se configura el valor de contacto SNMP
R3(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
R3(config)# snmp-server ifindex persist	
R3(config)# snmp-server enable traps config	
R3(config)# snmp-server enable traps ospf	
R3(config)#	

Configuración en D1.

D1(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
D1(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
D1(config-std-nacl)#exit	

D1(config)#snmp-server contact Darwin Duran	Se configura el valor de contacto SNMP
D1(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
D1(config)# snmp-server ifindex persist	Se habilita la persistencia de index
D1(config)# snmp-server enable traps config	Este comando no es soportado por la imagen utilizada
D1(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

Configuración en D2.

D2(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
D2(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
D2(config-std-nacl)# exit	
D2(config)#snmp-server contact Darwin Duran	Se configura el valor de contacto SNMP
D2(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
D2(config)# snmp-server enable traps config	Este comando no es soportado por la imagen utilizada
D2(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

Configuración en A1.

A1(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
A1(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
A1(config-std-nacl)# exit	

A1(config)#snmp-server contact Darwin Duran contacto SNMP	Se configura el valor de
A1(config)#snmp-server community ENCORSA ro SNMP	Se configura el
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la
A1(config)# snmp-server ifindex persist	Se habilita la
A1(config)# snmp-server enable traps config	Este comando no es
A1(config)# snmp-server enable traps ospf	Se habilita el envío

CONCLUSIONES

Con el desarrollo del presente trabajo se llevaron a cabo una serie de implementaciones donde se ponen a prueba los conceptos adquiridos en el transcurso del diplomado, yendo primeramente de la interpretación de la topología, saber que dispositivos utilizar, que herramienta de simulación adecuar y que imágenes son apropiadas para el desarrollo de la actividad. Es de anotar que el uso de imágenes tipo Dynamips, IOU, QEMU y la utilización de la máquina virtual para poder emular estos dispositivos fue algo bastante complejo, la activación, el uso de scripts y demás fueron cosas que complicaron el desarrollo de la actividad.

Luego de solucionar esto y verificar que las imágenes utilizadas cumplieran casi el 100% de la actividad, se procede a aplicar los direccionamientos, la creación de vlans en los switches de capa 3 y la utilización de DHCP que venía previamente establecida al comienzo de la actividad.

Solamente con el hecho de tener inconvenientes al principio de la prueba da a entender que este mundo de las redes es muy amplio, que no está demás reforzar sobre los conceptos adquiridos y por qué no, pensar a en un futuro poder ejercer como administrador de redes en una gran compañía.

BIBLIOGRAFÍA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1lhgTCtKY-7F5KIRC3>

ANEXO 1. CONFIGURACION DE LOS DISPOSITIVOS

Configuración de R1

```
!  
  
!  
upgrade fpd auto  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
enable secret 9  
$9$s5Lc1cRQOU7ghR$mzHW5f7zFGsr0Z14ja5e3NtSQpB9utcoBrVxMXNA2DM  
!  
aaa new-model  
!  
!  
aaa authentication login default group radius local  
!  
!  
!  
!  
aaa session-id common  
clock timezone utc -5 0  
no ip icmp rate-limit unreachable  
!  
!  
!  
!
```

```
!  
!  
no ip domain lookup  
ip cef  
ipv6 unicast-routing  
ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
username sadmin privilege 15 secret 9  
$9$G46BZy3y46kz0a$nSCrIESAmamf.ttWJvw5yh5en6LVONzFM171kEPJIAs  
!  
redundancy  
!  
!  
ip tcp synwait-time 5  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
no ip address  
shutdown  
duplex auto  
!
```

```

interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.224
duplex full
speed 1000
media-type gbic
negotiation auto
ipv6 address FE80::1:1 link-local
ipv6 address 2001:DB8:200::1/64
!
interface Serial1/0
ip address 10.0.13.1 255.255.255.0
ipv6 address FE80::1:3 link-local
ipv6 address 2001:DB8:100:1013::1/64
ipv6 ospf 6 area 0
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface GigabitEthernet2/0
ip address 10.0.10.1 255.255.255.0
negotiation auto
ipv6 address FE80::1:2 link-local
ipv6 address 2001:DB8:100:1010::1/64
ipv6 ospf 6 area 0
!
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
!
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    no neighbor 2001:DB8:200::2 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
  !
  ip forward-protocol nd
  no ip http server
  no ip http secure-server
  !
  !
  ip route 10.0.0.0 255.0.0.0 Null0
  !
  ip access-list standard SNMP
    permit 10.0.100.5
  !
  logging trap warnings
  logging host 10.0.100.5
  no cdp log mismatch duplex
  ipv6 route 2001:DB8:100::/48 Null0
  ipv6 router ospf 6
    router-id 0.0.6.1
    default-information originate
  !
  !

```

```

snmp-server community ENCORSA RO SNMP
snmp-server ifindex persist
snmp-server contact Darwin Duran
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-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
!
!
!
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
  shutdown
!
banner motd _____R1, ENCOR Skills Assessment, Scenario
1 _____
!

```

```
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  transport input all
!
ntp server 2.2.2.2
!
end
```

Configuración de R2

```
!

!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$YZDvjq1M5JzjRh$PYMqAIUVVSoeCd.Ml.5OctHnDLhPhnzmRUNjCVP28xg
!
no aaa new-model
clock timezone utc -5 0
```

```
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
username sadmin privilege 15 secret 9
$9$pmMTseVXWdaa24$Gtg3bey0tLmJ0bYnHj2v7K6LLsEQU3BodiXca/McGbs
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
```

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
ipv6 address FE80::2:3 link-local
ipv6 address 2001:DB8:2222::1/128
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 209.165.200.226 255.255.255.224
duplex full
speed 1000
media-type gbic
negotiation auto
ipv6 address FE80::2:1 link-local
ipv6 address 2001:DB8:200::2/64
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
```

```

interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
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
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
no cdp log mismatch duplex
ipv6 route ::/0 Loopback0
!
!
!
control-plane
!
!

```

```
!  
mgcp profile default  
!  
!  
!  
gatekeeper  
shutdown  
!  
banner motd _____ R2, ENCOR Skills Assessment, Scenario  
1 _____  
!  
line con 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
stopbits 1  
line aux 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
stopbits 1  
line vty 0 4  
login  
transport input all  
!  
ntp master 3  
!  
end
```

Configuración de R3

```
!  
  
!  
upgrade fpd auto  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption
```

```
!  
hostname R3  
!  
boot-start-marker  
boot-end-marker  
!  
!  
enable secret 9  
$9$tyJiQtYaNnIBlh$BYbqmQSY6oSo23qU9zRQPc1rQVNWWiz3hPWa0QyNnbl  
!  
aaa new-model  
!  
!  
aaa authentication login default group radius local  
!  
!  
!  
!  
!  
aaa session-id common  
clock timezone utc -5 0  
no ip icmp rate-limit unreachable  
!  
!  
!  
!  
!  
!  
no ip domain lookup  
ip cef  
ipv6 unicast-routing  
ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!
```

```
!  
!  
!  
!  
username sadmin privilege 15 secret 9  
$9$LKkMXRmz9G5CJ4$4.RJn1YrhvgZK3b4WIEdRS/04FhR0AuSp31.AeoYMFc  
!  
redundancy  
!  
!  
ip tcp synwait-time 5  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
no ip address  
shutdown  
duplex auto  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex full  
speed 1000  
media-type gbic  
negotiation auto  
!  
interface Serial1/0  
ip address 10.0.13.3 255.255.255.0  
ipv6 address FE80::3:3 link-local  
ipv6 address 2001:DB8:100:1010::2/64  
ipv6 ospf 6 area 0
```

```
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface GigabitEthernet2/0
ip address 10.0.11.1 255.255.255.0
negotiation auto
ipv6 address FE80::3:2 link-local
ipv6 address 2001:DB8:100:1011::1/64
ipv6 ospf 6 area 0
!
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
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ip access-list standard SNMP
permit 10.0.100.5
!
logging trap warnings
```

```
logging host 10.0.100.5
no cdp log mismatch duplex
ipv6 router ospf 6
  router-id 0.0.6.3
!
!
snmp-server community ENCORSA RO SNMP
snmp-server ifindex persist
snmp-server contact Darwin Duran
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-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
!
!
!
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
```

```
shutdown
!
banner motd _____ R3, ENCOR Skills Assessment, Scenario
1 _____
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  transport input all
!
ntp server 10.0.10.1
!
end
```

Configuración de D1

```
!
! Last configuration change at 22:38:47 utc Mon Nov 29 2021
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname D1
!
boot-start-marker
boot-end-marker
!
```

```

!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 9
$9$ozgHrs/0GBLRdp$2/AEItiDR4TVWBH/I7mbkPBXFIZMBn.msKCHtqRV2Ts
!
username sadmin privilege 15 secret 9
$9$MdwU/9yIOqGTfZ$.va8RA8ZrSCCq6CCFrOE4f1VoM3d7HjklmPjyL4cQ2
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
!
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
!
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef

```

```
!  
!  
!  
!  
!  
ipv6 unicast-routing  
ipv6 cef  
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree vlan 100,102 priority 24576  
spanning-tree vlan 101 priority 28672  
!  
vlan internal allocation policy ascending  
!  
track 4 ip sla 4  
  delay down 10 up 15  
!  
track 6 ip sla 6  
  delay down 10 up 15  
!  
ip tcp synwait-time 5  
!  
!  
!  
!  
interface Port-channel1  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Port-channel12  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Ethernet0/0  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999
```

```
switchport mode trunk
channel-group 12 mode active
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 1 mode active
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 1 mode active
!
interface Ethernet1/2
shutdown
!
interface Ethernet1/3
shutdown
!
```

```

interface Ethernet2/0
  no switchport
  ip address 10.0.10.2 255.255.255.0
  ipv6 address FE80::D1:1 link-local
  ipv6 address 2001:DB8:100:1010::2/64
  ipv6 ospf 6 area 0
!
interface Ethernet2/1
  switchport access vlan 100
  switchport mode access
  spanning-tree portfast edge
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan100
  ip address 10.0.100.1 255.255.255.0
  standby version 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
  ipv6 address FE80::D1:2 link-local
  ipv6 address 2001:DB8:100:100::1/64
  ipv6 ospf 6 area 0
!
interface Vlan101
  ip address 10.0.101.1 255.255.255.0
  standby version 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
ipv6 address FE80::D1:3 link-local
ipv6 address 2001:DB8:100:101::1/64
ipv6 ospf 6 area 0
!
interface Vlan102
ip address 10.0.102.1 255.255.255.0
standby version 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
ipv6 address FE80::D1:4 link-local
ipv6 address 2001:DB8:100:102::1/64
ipv6 ospf 6 area 0
!
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet2/0
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
!
ip forward-protocol nd
!
!
no ip http server
!
ip access-list standard SNMP

```

```

permit 10.0.100.5
!
!
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
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet2/0
!
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Darwin Duran
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-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
!
!
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $strongPass

```

```
!  
!  
control-plane  
!  
banner motd _____ D1, ENCOR Skills Assessment, Scenario  
1 _____  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
!  
ntp server 10.0.10.1  
!  
end
```

Configuración de D2

```
!  
! Last configuration change at 22:38:47 utc Mon Nov 29 2021  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname D2  
!  
boot-start-marker  
boot-end-marker  
!  
!
```

```

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 9
$9$shC3/HSnNI1CXJ$2t/d1eQtQi5l56gyAWo8iiQnH22J4z6/QnDADqYEh7s
!
username sadmin privilege 15 secret 9
$9$86YZINZIKoyBJ3$i03LLGSvd14NVKatilCbSHEFzIqB3qHUGR7FUwnU9S2
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
!
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
!
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef
!

```

```
!  
!  
!  
!  
ipv6 unicast-routing  
ipv6 cef  
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree vlan 100,102 priority 28672  
spanning-tree vlan 101 priority 24576  
!  
vlan internal allocation policy ascending  
!  
track 4 ip sla 4  
  delay down 10 up 15  
!  
track 6 ip sla 6  
  delay down 10 up 15  
!  
ip tcp synwait-time 5  
!  
!  
!  
!  
interface Port-channel2  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Port-channel12  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Ethernet0/0  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk
```

```
channel-group 12 mode active
!  
interface Ethernet0/1  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport mode trunk  
channel-group 12 mode active  
!  
interface Ethernet0/2  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport mode trunk  
channel-group 12 mode active  
!  
interface Ethernet0/3  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport mode trunk  
channel-group 12 mode active  
!  
interface Ethernet1/0  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport mode trunk  
channel-group 2 mode active  
!  
interface Ethernet1/1  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport mode trunk  
channel-group 2 mode active  
!  
interface Ethernet1/2  
shutdown  
!  
interface Ethernet1/3  
shutdown  
!  
interface Ethernet2/0
```

```

no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address FE80::D1:1 link-local
ipv6 address 2001:DB8:100:1011::2/64
ipv6 ospf 6 area 0
!
interface Ethernet2/1
switchport access vlan 102
switchport mode access
spanning-tree portfast edge
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 10.0.100.2 255.255.255.0
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
ipv6 address FE80::D2:2 link-local
ipv6 address 2001:DB8:100:100::2/64
ipv6 ospf 6 area 0
!
interface Vlan101
ip address 10.0.101.2 255.255.255.0
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60

```

```

standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
ipv6 address FE80::D2:3 link-local
ipv6 address 2001:DB8:100:101::2/64
ipv6 ospf 6 area 0
!
interface Vlan102
ip address 10.0.102.2 255.255.255.0
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
ipv6 address FE80::D2:4 link-local
ipv6 address 2001:DB8:100:102::2/64
ipv6 ospf 6 area 0
!
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
!
ip forward-protocol nd
!
!
no ip http server
!
ip access-list standard SNMP
permit 10.0.100.5
!
!

```

```
ip sla 4
  icmp-echo 10.0.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet2/0
!
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Darwin Duran
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-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
!
!
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
!
!
control-plane
!
```

```
banner motd _____ D2, ENCOR Skills Assessment, Scenario
1 _____
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
!
ntp server 10.0.10.1
!
end
```

Configuración de A1

```
!
! Last configuration change at 22:38:46 utc Mon Nov 29 2021
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname A1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
```

```
enable secret 9
$9$w/WHFV9YJi8HMZ$bLxA8Qnr2HE7Yc8D8O8jiGSzba52fZ4M9ILx2oaANvM
!
username sadmin privilege 15 secret 9
$9$tqwf2WhRBMPvYZ$q4kpXVg71CxOgdBcz5PJllicJmsc784J40t1qNMEIXk
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
!
!
!
!
!
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
```

```
!  
interface Port-channel1  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Port-channel2  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
!  
interface Ethernet0/0  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface Ethernet0/1  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface Ethernet0/2  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
  channel-group 2 mode active  
!  
interface Ethernet0/3  
  switchport trunk encapsulation dot1q  
  switchport trunk native vlan 999  
  switchport mode trunk  
  channel-group 2 mode active  
!  
interface Ethernet1/0  
  switchport access vlan 101  
  switchport mode access  
  spanning-tree portfast edge
```

```

!
interface Ethernet1/1
  switchport access vlan 100
  switchport mode access
  spanning-tree portfast edge
!
interface Ethernet1/2
  shutdown
!
interface Ethernet1/3
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan100
  ip address 10.0.100.3 255.255.255.0
  ipv6 address FE80::A1:1 link-local
  ipv6 address 2001:DB8:100:100::3/64
!
ip forward-protocol nd
!
!
no ip http server
!
ip access-list standard SNMP
  permit 10.0.100.5
!
!
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Darwin Duran
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-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
!
!
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
!
!
control-plane
!
banner motd _____ A1, ENCOR Skills Assessment, Scenario
1 _____
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
!
ntp server 10.0.10.1
!
end

```