

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANTONIO SERRANO LUGO

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE ANTONIO SERRANO LUGO

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

## NOTA DE ACEPTACION

## Firma del Presidente del Jurado

---

## Firma del Jurado

---

## Firma del Jurado

NEIVA (HUILA), 26 de noviembre de 2021

## **AGRADECIMIENTOS**

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

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

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

## **CONTENIDO**

NOTA DE ACEPTACION.....	3
AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS.....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCION.....	10
DESARROLLO .....	11
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos .	12
Paso 1: Cablear la red como se muestra en la topología.....	12
Paso 2: Configurar los parámetros básicos para cada dispositivo. ....	13
Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	20
Parte 3: Configurar los protocolos de enrutamiento.....	25
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy) .....	30
Parte 5: Seguridad.....	35
Parte 6: Configure las funciones de Administración de Red .....	37
CONCLUSIONES .....	54
BIBLIOGRAFIA.....	55

## LISTA DE TABLAS

Tabla 1.	Tabla de direccionamiento .....	11
Tabla 2.	Tabla de Direccionamiento se cambian interfaces .....	13
Tabla 3.	Configuraciones troncales, RSPT, Raíz root, Etherhetchannel LACP...	20
Tabla 4.	Verificación DHCP y ping .....	23
Tabla 5.	Configuración OSPFv2, OSPFv2 en Ipv4 e Ipv6 .....	26
Tabla 6.	Comandos (FHRP/SLA) .....	30
Tabla 7.	Configuración seguridad.....	35
Tabla 8.	Configuraciones de administración de red .....	37

## LISTA DE FIGURAS

Figura 1. Topología de Red .....	11
Figura 2. Topología de Red GNS3 .....	12
Figura 3. Copia de archivo en la nvram de los dispositivos .....	19
Figura 4. Configuración parámetros básicos PC1 IPv4 e IPv6 .....	19
Figura 5. Configuración parámetros básicos PC4 IPv4 e IPv6 .....	20
Figura 6. DHCP IPv4 PC2 .....	23
Figura 7. DHCP IPv4 PC3 .....	24
Figura 8. Ping PC1 .....	24
Figura 9. Ping PC2 .....	24
Figura 10.Ping PC3 .....	25
Figura 11.Ping PC4 .....	25
Figura 12.Acceso de verificación cuenta encriptada SCRYPT .....	36
Figura 13.Configuración administración equipos.....	40
Figura 14.Verificación desarrollo 2.1, 2.2 y 2.5 switch D1 .....	41
Figura 15.Verificación desarrollo 2.3 y 2.4 en switch D1 .....	41
Figura 16.Verificación desarrollo 2.6 en switch D1 .....	42
Figura 17.Verificación desarrollo 2.5 en switch D2.....	43
Figura 18.Verificación desarrollo configuración OSPF .....	44
Figura 19.Verificación tarea 3.2 en cada dispositivo .....	46
Figura 20.Verificación tarea 3.3 en R2 .....	47
Figura 21.Verificación punto 3.4 en R1 .....	48
Figura 22.Verificación de OSPF y BGP para IPv4.....	48
Figura 23.Desarrollo 4.1 y 4.3 para el commutador D1 .....	49
Figura 24.Identificación desarrollo 4.3.....	50
Figura 25.Identificación tarea 5.1 y 5.2.....	50
Figura 26.Identificación tareas 5.3, 5.4 y 5.5 .....	51
Figura 27.Verificación desarrollo 6.3 .....	52
Figura 28.Verificación desarrollo 6.4 .....	52
Figura 29.Verificación tarea 6.5.....	53

## GLOSARIO

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

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

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

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

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

## **RESUMEN**

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

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

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

## **ABSTRACT**

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

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

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

## **INTRODUCCION**

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

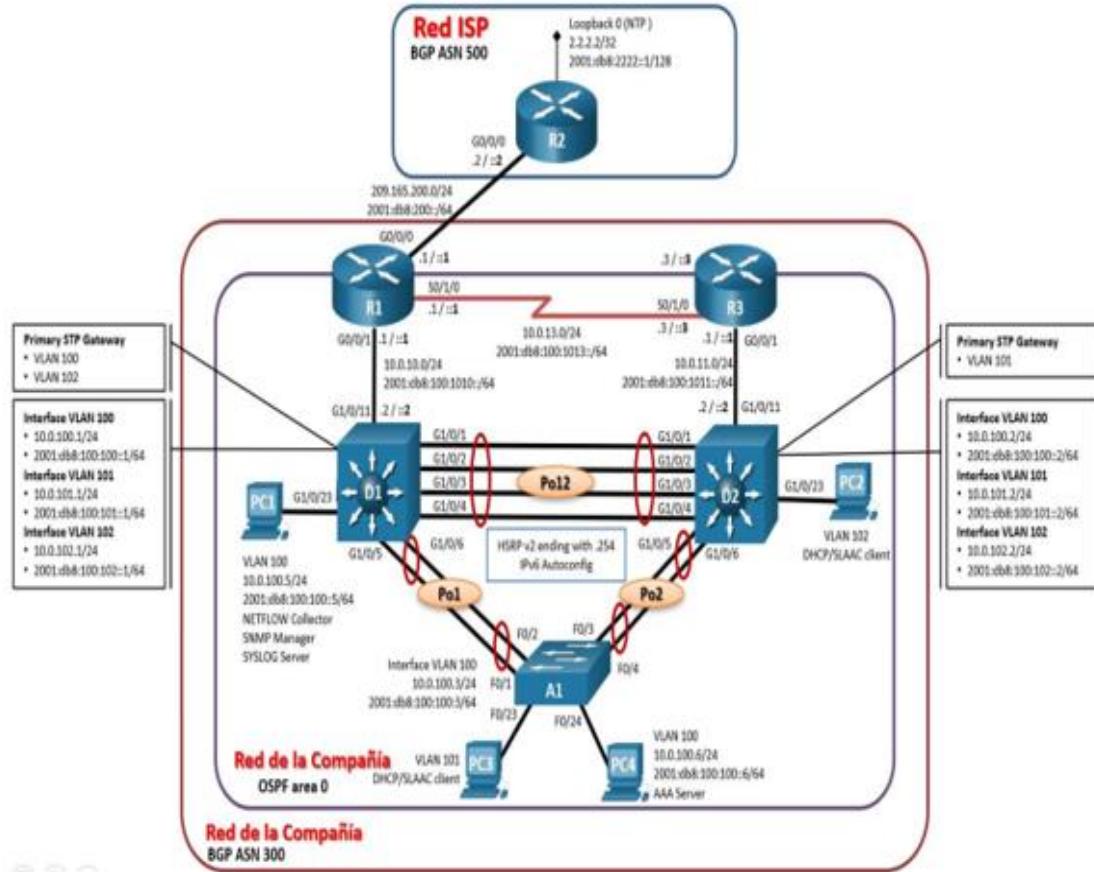
Se utiliza metodologías de simulación con aplicaciones como GNS3, PACKET TRACER para el desarrollo de topologías de red que en la vida real se pueden aplicar, como por ejemplo la seguridad informativa, protección de datos, entre otros.

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

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

## DESARROLLO

Figura 1. Topología de Red



fuente: guías UNAD CCNP avance final

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.10.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2

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

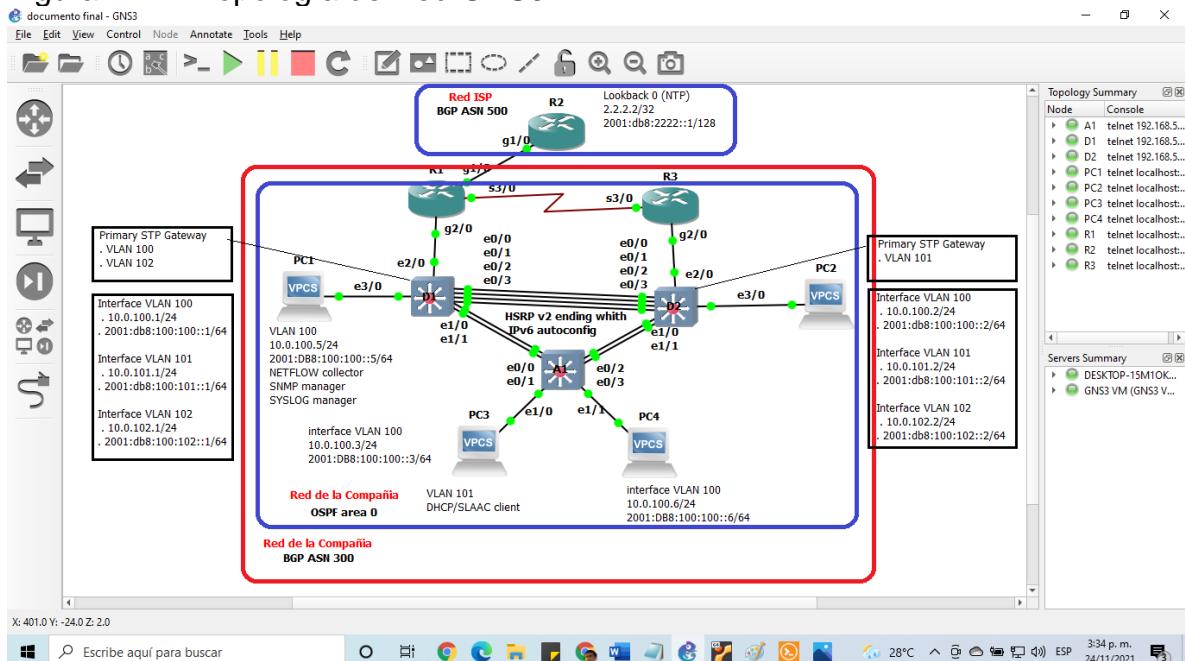
Fuente: guías UNAD CCNP avance final

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

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

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

Figura 2. Topología de Red GNS3



Fuente: Aplicación GNS3 (Auditoria Propia)

Tabla 2. Tabla de Direccionamiento se cambian interfaces

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0****g1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1****g2/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0****s3/0	10.0.10.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0****g1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1****g2/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0****s3/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11***e2/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11***e2/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente: guías UNAD CCNP avance final

Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

### Router 1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills
Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g1/0
```

establecer el nombre actual habilita el routing IPv6 nombre a dirección basado en DNS del host configuración de línea tiempo de espera inactivo desea enviar esta información a un servidor de syslog ingresamos la interfaz
--

```

ip address 209.165.200.225
255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
interface g2/0
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit

```

se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

## **Router 2**

```

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

```

establecer el nombre actual  
habilita el routing IPv6  
nombre a dirección basado en DNS del host

configuración de línea  
tiempo de espera inactivo  
desea enviar esta información a un  
servidor de syslog  
ingresamos la interfaz  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz loopback  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

**Router 3**

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills
Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g2/0
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

establecer el nombre actual  
habilita el routing IPv6  
nombre a dirección basado en DNS del host

configuración de línea  
tiempo de espera inactivo  
desea enviar esta información a un servidor de syslog  
ingresamos la interfaz  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz  
ingresamos la interfaz  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

**Switch D1**

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills
Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
```

establecer el nombre actual  
configurar tabla enrutamiento  
habilita el routing IPv6  
nombre a dirección basado en DNS del host

configuración de línea  
tiempo de espera inactivo  
desea enviar esta información a un servidor de syslog  
asignar el puerto a una VLAN

```

name NATIVE
exit
interface e2/0
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
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1
10.0.101.109
ip dhcp excluded-address
10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1
10.0.102.109
ip dhcp excluded-address
10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit

```

ingresamos la interfaz  
creación de las interfaces de la capa 3  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz vlan  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz vlan  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

ingresamos la interfaz vlan  
se asignan las direcciones  
se asignan las direcciones  
se asignan las direcciones  
se activa interfaz

excluir direcciones específicas

excluir direcciones específicas

excluir direcciones específicas

excluir direcciones específicas

ingresa el router en el modo de configuración dhcpcv4  
se establece una ruta predeterminada

ingresa el router en el modo de configuración dhcpcv4  
se establece una ruta predeterminada

**Switch D2**

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

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

### Switch A1

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

```

ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
exit

```

se asignan las direcciones  
se activa interfaz

ingresamos rango de interfaces  
se inactiva interfaz

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

Figura 3. Copia de archivo en la nvram de los dispositivos

```

R1(config)#do wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1965 bytes to 960 bytes[OK]
R1(config)#
R2(config)#do wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2(config)#
R1(config)#
R1(config)#
Oct 14 19:59:00.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to down
R1(config)#
Oct 14 20:00:10.857: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
R1(config)#
R1(config)#
R3(config)#
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3(config)#

```

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

Figura 4. Configuración parámetros básicos PC1 IPv4 e IPv6

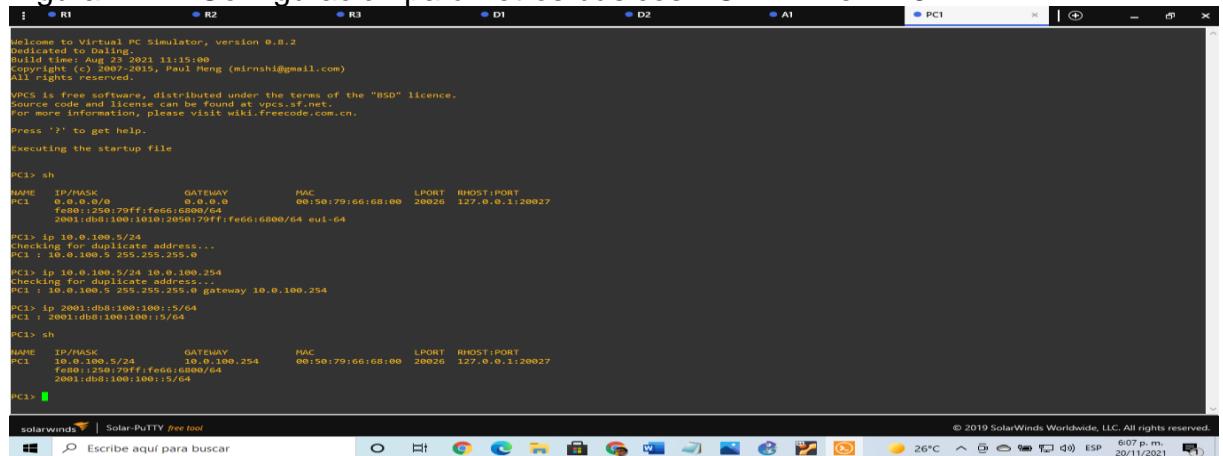


Figura 5. Configuración parámetros básicos PC4 IPv4 e IPv6

```

Welcome to Virtual PC Simulator, version 0.8.2
Copyright (c) 2015, Mirnshi (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.st.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC4> ip 2001:db8:100:100::6/64
PC3 : 2001:db8:100:100::6/64
PC4> sh
NAME      IP/MASK          GATEWAY        MAC           LPORT    RHOST:PORT
PC4      10.0.100.6/24     10.0.100.254   00:50:79:66:68:03  20032  127.0.0.1:20033
fe80::1250:79ff:fe66:6803%4
2001:db8:100:100::6/64
PC4>

```

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

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

Las tareas de configuración son las siguientes

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

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

2,5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"><li>• D1 a D2 – Port channel 12</li><li>• D1 a A1 – Port channel 1</li><li>• D2 a A1 – Port channel 2</li></ul>
2,6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

### Switch D1

```

interface range g1/0/1-4
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g1/0/5-6
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root
primary
spanning-tree vlan 101 root secondary
interface g1/0/23
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

```

Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

modo árbol de expansión  
vlan primaria  
  
vlan secundaria  
Ingresamos rango de interfaces  
interfaz cambia al modo de acceso permanente  
acceso inmediato a la red de capa 2  
se activa interfaz

### **Switch D2**

```
interface range e0/0-3
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range e1/0-1
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root
secondary
interface e3/0
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end
```

Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

modo árbol de expansión  
vlan primaria  
vlans secundarias

ingresamos la interfaz  
interfaz cambia al modo de acceso permanente  
acceso inmediato a la red de capa 2  
se activa interfaz

### **Switch A1**

```
spanning-tree mode rapid-pvst
interface range e0/0-1
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range e0/2-3
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface e1/0
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
```

modo de árbol de expansión  
Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

Ingresamos rango de interfaces troncal de la interfaz  
especifica el número del grupo del canal  
se activa interfaz

ingresamos la interfaz  
interfaz cambia al modo de acceso permanente  
acceso inmediato a la red de capa 2  
se activa interfaz

```

exit
interface e1/1
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

```

ingresamos la interfaz  
interfaz cambia al modo de acceso permanente  
acceso inmediato a la red de capa 2  
se activa interfaz

Tabla 4. Verificación DHCP y ping

Tarea#	Tarea	Especificación
2,7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2,8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC4: 10.0.100.6</li> </ul> <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC1: 10.0.100.5</li> </ul>

Figura 6. DHCP IPv4 PC2

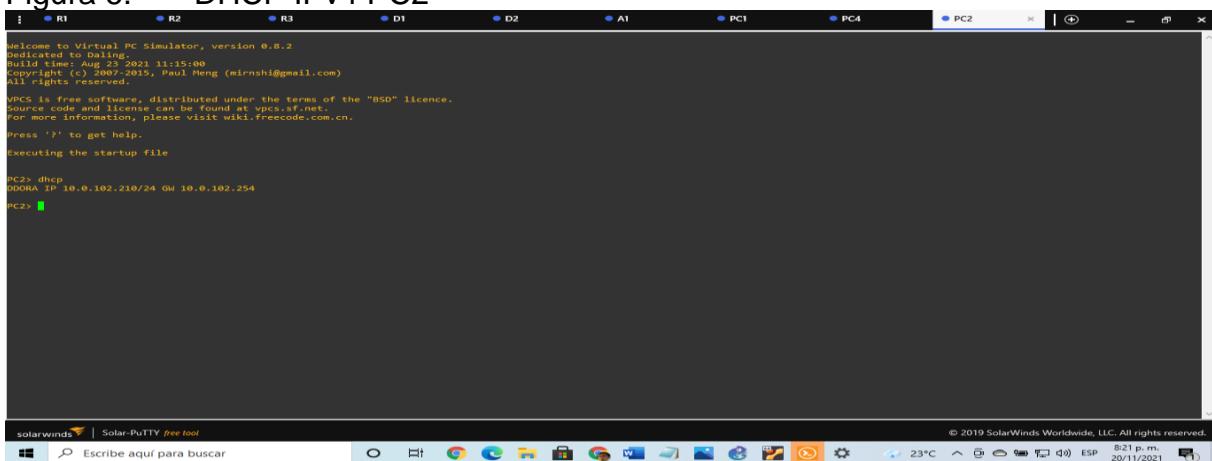


Figura 7. DHCP IPv4 PC3

```
Welcome to Virtual PC Simulator, version 0.6.2
Copyright (c) 2007-2014, 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 vpcss.vf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC3> dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254

PC3> 
```

Figura 8. Ping PC1 a:

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC4: 10.0.100.6

```
NAME IP/MAC GATEWAY MAC LPORT BOOST PORT
PC1 10.0.100.0/8 0.0.0.0 00:50:79:66:6B:00 10026 127.0.0.1:10027
2001:db8:100:100:2050:7fff:fe60:1000/64 eu1-64

PC1> ip 10.0.100.5/24 10.0.100.254
Gateway is 10.0.100.254...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
PC1 > 2001:db8:100:100::5/64
PC1 : 2001:db8:100:100::5/64

PC1> sh
NAME IP/MAC GATEWAY MAC LPORT BOOST PORT
PC1 10.0.100.5/24 10.0.100.254 00:50:79:66:6B:00 10026 127.0.0.1:10027
fe80::250:79ff:fe66:6B00/64
2001:db8:100:100::5/64

PC1> ping 10.0.100.0
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.979 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.885 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.849 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.911 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.932 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.970 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.090 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.067 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.274 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.291 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.010 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.591 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.592 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.571 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.806 ms

PC1> 
```

Figura 9. Ping PC2 a:

- D1: 10.0.102.1
- D2: 10.0.102.2

```
Welcome to Virtual PC Simulator, version 0.6.2
Copyright (c) 2007-2014, 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 vpcss.vf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254
Bad command: "10.0.102.1". Use ? for help.

PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.931 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.090 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=1.745 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.404 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.051 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.765 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=1.087 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=1.083 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.823 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.902 ms

PC2> 
```

Figura 10. Ping PC3 a:

- D1: 10.0.101.1
- D2: 10.0.101.2

The screenshot shows a SolarWinds Solar-PuTTY free tool window with multiple tabs at the top: R1, R2, R3, D1, D2, A1, PC1, PC2, PC3, and PC4. The PC3 tab is active, displaying ping results to 10.0.101.1 and 10.0.101.2. The results for 10.0.101.1 show 64 bytes sent with TTL=255 and times ranging from 1.476 ms to 1.600 ms. The results for 10.0.101.2 show 64 bytes sent with TTL=255 and times ranging from 1.171 ms to 1.221 ms. The command entered was 'ping 10.0.101.1'.

```
PC3> ping 10.0.101.1
64 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=1.476 ms
64 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=1.480 ms
64 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.440 ms
64 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.411 ms
64 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=1.600 ms

PC3> ping 10.0.101.2
64 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=1.171 ms
64 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=1.017 ms
64 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=1.180 ms
64 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=1.160 ms
64 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=1.221 ms

PC3>
```

Figura 11. Ping PC4 a:

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC1: 10.0.100.5

The screenshot shows a SolarWinds Solar-PuTTY free tool window with multiple tabs at the top: R1, R2, R3, D1, D2, A1, PC1, PC2, PC3, and PC4. The PC4 tab is active, displaying ping results to 10.0.100.1, 10.0.100.2, and 10.0.100.5. The results for 10.0.100.1 show 64 bytes sent with TTL=255 and times ranging from 0.907 ms to 1.065 ms. The results for 10.0.100.2 show 64 bytes sent with TTL=255 and times ranging from 1.099 ms to 1.481 ms. The results for 10.0.100.5 show 64 bytes sent with TTL=64 and times ranging from 1.017 ms to 1.598 ms. The command entered was 'ping 10.0.100.1'.

```
PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> ip 2001:db8:100:100::6/64
Invalid ipv6 address.

PC4> ip 2001:db8:100:100::1/64
PC1 : 2001:db8:100:100::1/64
PC1 : 2001:db8:100:100::1/64

PC4> sh
NAME          IP/MASK        GATEWAY      MAC           LPORT    RHOST:PORT
PC4  10.0.100.6/24  10.0.100.254  00:56:79:66:68:03  10028  127.0.0.1:10029
     2001:db8:100:100::6/64

PC4> ping 10.0.100.1
64 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.907 ms
64 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.041 ms
64 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.034 ms
64 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.429 ms
64 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.493 ms
64 bytes from 10.0.100.1 icmp_seq=6 ttl=255 time=1.065 ms

PC4> ping 10.0.100.2
64 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.099 ms
64 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.401 ms
64 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.454 ms
64 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.458 ms
64 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.481 ms

PC4> ping 10.0.100.5
64 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=1.017 ms
64 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=1.032 ms
64 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.013 ms
64 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.598 ms
64 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.793 ms

PC4>
```

### Parte 3: Configurar los protocolos de enrutamiento

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

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

Las tareas de configuración son las siguientes:

Tabla 5. Configuración OSPFv2, OSPFv2 en Ipv4 e Ipv6

Tarea#	Tarea	Especificación
3,1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.	<p>se OSPF Process ID 4 y asigne los siguientes routerIDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.4.1</li> <li>• R3: 0.0.4.3</li> <li>• D1: 0.0.4.131</li> <li>• D2: 0.0.4.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul> <p>recibir direcciones IPv4 válidas.</p>
3,2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>se OSPF Process ID 6 y asigne los siguientes routerIDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.6.1</li> <li>• R3: 0.0.6.3</li> <li>• D1: 0.0.6.131</li> <li>• D2: 0.0.6.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul>
3,3	En R2 en la “Red ISP”, configure MPBGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> <li>• Una ruta estática predeterminada IPv4.</li> <li>• Una ruta estática predeterminada IPv6.</li> </ul> <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</p>

		<p>con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/32).</li> <li>• La ruta por defecto (0.0.0.0/0).</li> </ul> <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/128).</li> <li>• La ruta por defecto (::/0).</li> </ul>
3,4	En R1 en la “Red ISP”, configure MPBGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> <li>• Una ruta resumen IPv4 para 10.0.0.0/8.</li> <li>• Una ruta resumen IPv6 para 2001:db8:100::/48.</li> </ul> <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"> <li>• Deshabilite la relación de vecino IPv6.</li> <li>• Habilite la relación de vecino IPv4.</li> <li>• Anuncie la red 10.0.0.0/8.</li> </ul> <p>En IPv6 address family:</p> <ul style="list-style-type: none"> <li>• Deshabilite la relación de vecino IPv4.</li> <li>• Habilite la relación de vecino IPv6.</li> <li>• Anuncie la red 2001:db8:100::/48.</li> </ul>

### Router R1

```

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
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface g2/0
ipv6 ospf 6 area 0
exit
interface s3/0

```

Enrutador ospf  
Identificar router id  
Interfaces que participan  
Interfaces que participan  
Propagación de una ruta estatica predeterminada  
Los protocolos de routing IPv6 se habilitan en una interfaz  
Identificar router id  
Propagación de una ruta estatica ingresamos la interfaz  
ingresamos la interfaz

```

ipv6 ospf 6 area 0
exit
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as
500
neighbor 2001:db8:200::2 remote-as
500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family

```

Habilita el dominio BGP y define el número de sistema autónomo  
Identificación route  
número as del enrutador al que desea conectarse con bgp

configuración familia ipv4  
activar vecino  
desactivar vecino

salimos configuración familia ipv4  
configuración familia ipv6

dirección y mascara  
salimos configuración familia ipv6

### **Router R2**

```

ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as
300
neighbor 2001:db8:200::1 remote-as
300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family

```

número de sistema autónomo  
Identificación route  
número as del enrutador al que desea conectarse con bgp  
número as del enrutador al que desea conectarse con bgp  
configuración familia ipv4

dirección y mascara

salimos configuración familia ipv4  
configuración familia ipv6

dirección y mascara

salimos configuración familia ipv6

### **Router R3**

```
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
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface g2/0
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
end
```

Enrutador ospf  
Identificar router id  
dirección que participa  
dirección que participa

ingresamos la interfaz  
configuración área en ospf

ingresamos la interfaz  
configuración área en ospf

### **Switch D1**

```
router ospf 4
router-id 0.0.4.131
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
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface g1/0/11
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface g1/0/11
exit
interface e2/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

Enrutador ospf  
Identificar router id  
dirección que participa  
dirección que participa  
dirección que participa  
dirección que participa  
detiene el ruteo ospf  
permite comunicación ospf con la  
interfaz

Enrutador ospf  
Identificar router id  
detiene el ruteo ospf  
permite comunicación ospf con la  
interfaz

ingresamos la interfaz  
configuración área en ospf

ingresamos la interfaz vlan  
configuración área en ospf

ingresamos la interfaz vlan  
configuración área en ospf

ingresamos la interfaz vlan  
configuración área en ospf

**Switch D2**

```
router ospf 4
router-id 0.0.4.132
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
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e2/0
exit
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g1/0/11
exit
interface e2/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Enrutador ospf  
Identificar router id  
dirección que participa  
dirección que participa  
dirección que participa  
dirección que participa  
detiene el ruteo ospf  
permite comunicación ospf con la  
interfaz  
Enrutador ospf  
Identificar router id  
detiene el ruteo ospf  
permite comunicación ospf con la  
interfaz  
ingresamos la interfaz  
configuración área en ospf  
ingresamos la interfaz vlan  
configuración área en ospf  
ingresamos la interfaz vlan  
configuración área en ospf  
ingresamos la interfaz vlan  
configuración área en ospf

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

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

Tabla 6. Comandos (FHRP/SLA)

Tarea#	Tarea	Especificación
4,1	En D1, cree IP SLAs que prueben la	Cree dos IP SLAs. <ul style="list-style-type: none"><li>• Use la SLA número 4 para IPv4.</li><li>• Use la SLA número 6 para IPv6.</li></ul> Las IP SLAs probarán la disponibilidad de la interfaz R1

	accesibilidad de la interfaz R1 G0/0/1.	G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. <ul style="list-style-type: none"><li>• Use el número de rastreo 4 para la IP SLA 4.</li><li>• Use el número de rastreo 6 para la IP SLA 6.</li></ul> Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4,2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. <ul style="list-style-type: none"><li>• Use la SLA número 4 para IPv4.</li><li>• Use la SLA número 6 para IPv6.</li></ul> 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. <ul style="list-style-type: none"><li>• Use el número de rastreo 4 para la IP SLA 4.</li><li>• Use el número de rastreo 6 para la SLA 6.</li></ul> Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4,3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: <ul style="list-style-type: none"><li>• Asigne la dirección IP virtual 10.0.100.254.</li><li>• Establezca la prioridad del grupo en 150.</li><li>• Habilite la preferencia (preemption).</li><li>• Rastree el objeto 4 y decremente en 60.</li></ul> Configure IPv4 HSRP grupo 114 para la VLAN 101: <ul style="list-style-type: none"><li>• Asigne la dirección IP virtual 10.0.101.254.</li><li>• Habilite la preferencia (preemption).</li><li>• Rastree el objeto 4 para disminuir en 60.</li></ul> Configure IPv4 HSRP grupo 124 para la VLAN 102: <ul style="list-style-type: none"><li>• Asigne la dirección IP virtual 10.0.102.254.</li></ul>

	<ul style="list-style-type: none"> <li>• Establezca la prioridad del grupo en 150.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando ipv6 autoconfig.</li> <li>• Establezca la prioridad del grupo en 150.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando ipv6 autoconfig.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Registre el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando ipv6 autoconfig.</li> <li>• Establezca la prioridad del grupo en 150.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60. D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</li> </ul> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual 10.0.100.254.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual 10.0.101.254.</li> <li>• Establezca la prioridad del grupo en 150.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual 10.0.102.254.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando ipv6 autoconfig.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando ipv6 autoconfig.</li> </ul>
--	---

**Switch D1**

```
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
  exit
ip sla 6
  icmp-echo 2001:db8:100:1010::1
  frequency 5
  exit
  ip sla schedule 4 life forever start-time now
  ip sla schedule 6 life-forever start-time now
  track 4 ip sla 4
    delay down 10 up 15
    exit
  track 6 ip sla 6
    delay down 10 up 15
    exit
  interface vlan 100
    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
    exit
  interface vlan 101
    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
    exit
  interface vlan 102
    standby version 2
    standby 124 ip 10.0.102.254
    standby 124 priority 150
    standby 124 preempt
    standby 124 track 4 decrement 60
```

Monitoreo en un nodo en la red  
Ping, replica a esa dirección ipv4

Monitoreo en un nodo en la red  
Ping, replica a esa dirección ipv4

habilita el ip sla indica cuando y por cuento tiempo estará activo

habilita el ip sla indica cuando y por cuento tiempo estará activo

retraso de 10 a 15

retraso de 10 a 15

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

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

### **Switch D2**

```
ip sla 4  
icmp-echo 10.0.11.1  
frequency  
exit  
ip sla 6  
icmp-echo 2001:db8:100:1011::1  
frequency  
exit  
ip sla schedule 4 life forever start-time  
now  
ip sla schedule 6 life forever start-time  
now  
track 4 ip sla 4  
delay down 10 up 15  
exit  
track 6 ip sla 6  
delay down 10 up 15  
exit  
interface vlan 100  
standby version 2  
standby 104 ip 10.0.100.254  
standby 104 preempt  
standby 104 track 4 decrement 60  
standby 106 ipv6 autoconfig  
standby 106 preempt  
standby 106 track 6 decrement 60  
exit  
interface vlan 101  
standby version 2  
standby 114 ip 10.0.101.254  
standby 114 priority 150  
standby 114 preempt  
standby 114 track 4 decrement 60  
standby 116 ipv6 autoconfig  
standby 116 priority 150  
standby 116 preempt
```

Monitoreo en un nodo en la red  
Ping, replica a esa dirección ipv4

Monitoreo en un nodo en la red  
Ping, replica a esa dirección ipv4

habilita el ip sla indica cuando y por  
cuanto tiempo estará activo  
habilita el ip sla indica cuando y por  
cuanto tiempo estará activo

retraso de 10 a 15

retraso de 10 a 15

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

```

standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

```

ingresamos la interfaz vlan  
configura el hsrp para usar la versión 2

## Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

Tabla 7. Configuración seguridad

Tarea#	Tarea	Especificación
5,1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.
5,2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"> <li>Nombre de usuario Local: admin</li> <li>Nivel de privilegio 15</li> <li>Contraseña: cisco12345cisco</li> </ul>
5,3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA
5,4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"> <li>Dirección IP del servidor RADIUS es 10.0.100.6.</li> <li>Puertos UDP del servidor RADIUS son 1812 y 1813.</li> <li>Contraseña: \$trongPass</li> </ul>
5,5	En todos los dispositivos (excepto R2),	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> <li>Use la lista de métodos por defecto</li> </ul>

	configure la lista de métodos de autenticación AAA	<ul style="list-style-type: none"> <li>• Valide contra el grupo de servidores RADIUS</li> <li>• De lo contrario, utilice la base de datos local.</li> </ul>
5,6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

### En todos los equipos:

```
enable algorithm-type SCRYPT
secret cisco12345cisco
username sadmin privilege 15
algorithm-type SCRYPT secret
cisco12345cisco
```

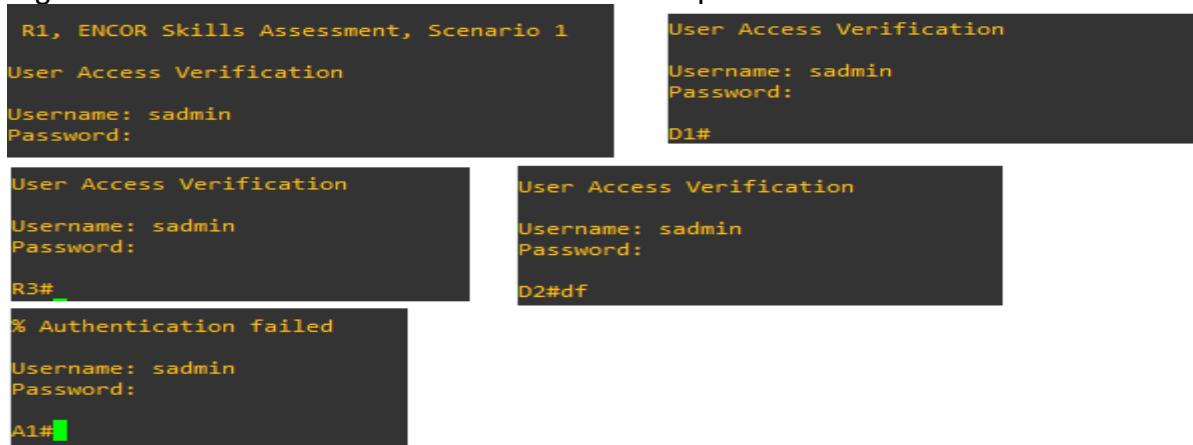
Configurar el tipo de algoritmo de una contraseña de usuario

### en todos los equipos excepto R2:

```
aaa new-model
radius server RADIUS
address ipv4 10.0.100.6 auth-port
1812 acct-port 1813
key $trongPass
exit
aaa authentication login default group
radius local
end
```

Configuración de autenticación protocolo de autenticación y autorización para aplicaciones de acceso a la red

Figura 12. Acceso de verificación cuenta encriptada SCRYPT



## Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tabla 8. Configuraciones de administración de red

Tarea#	Tarea	Especificación
6,1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6,2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6,3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"><li>• R1 debe sincronizar con R2.</li><li>• R3, D1 y A1 para sincronizar la hora con R1.</li><li>• D2 para sincronizar la hora con R3.</li></ul>
6,4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6,5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: <ul style="list-style-type: none"><li>• Unicamente se usará SNMP en modo lectura (Read-Only).</li><li>• Limite el acceso SNMP a la dirección IP de la PC1.</li><li>• Configure el valor de contacto SNMP con su nombre.</li><li>• Establezca el community string en ENCORSA.</li><li>• En R3, D1, y D2, habilite el envío de traps config y ospf.</li><li>• En R1, habilite el envío de traps bgp, config, y ospf.</li><li>• En A1, habilite el envío de traps config.</li></ul>

## **configuración reloj local UTC en todos los equipos**

### **Router R2**

```
ntp master 3  
end
```

reloj maestro ntp para sincronización

### **Router R1**

```
ntp server 2.2.2.2  
logging trap warning  
logging host 10.0.100.5  
logging on  
ip access-list standard SNMP-NMS  
permit host 10.0.100.5  
exit  
snmp-server contact Cisco Student  
snmp-server community ENCORSA ro  
SNMP-NMS  
snmp-server host 10.0.100.5 version  
2c ENCORSA  
snmp-server ifindex persist  
snmp-server enable traps bgp  
snmp-server enable traps config  
snmp-server enable traps ospf  
end
```

advertencia de registro

Ingreso sesión ip

activar sesión

acceso lista a protocolo de  
administración

protocolo de administración cisco

protocolo de administración comunidad

proporciona un valor de índice de  
interfaz

habilita el soporte

de bgp para operaciones snm

habilita el soporte

de ospf para operaciones snm

### **Router R3**

```
ntp server 10.0.10.1  
logging trap warning  
logging host 10.0.100.5  
logging on  
ip access-list standard SNMP-NMS  
permit host 10.0.100.5  
exit  
snmp-server contact Cisco Student  
snmp-server community ENCORSA ro  
SNMP-NMS  
snmp-server host 10.0.100.5 version  
2c ENCORSA  
snmp-server ifindex persist  
snmp-server enable traps config  
snmp-server enable traps ospf  
end
```

advertencia de registro

Ingreso sesión ip

activar sesión

acceso lista a protocolo de  
administración

protocolo de administración cisco

protocolo de administración comunidad

proporciona un valor de índice de  
interfaz

habilita el soporte

de bgp para operaciones snm

habilita el soporte

de ospf para operaciones snm

**Switch D1**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro
SNMP-NMS
snmp-server host 10.0.100.5 version
2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

advertencia de registro

Ingreso sesión ip

activar sesión

acceso lista a protocolo de administración

protocolo de administración cisco

protocolo de administración comunidad

proporciona un valor de índice de interfaz

habilita el soporte

de bgp para operaciones snm

habilita el soporte

de ospf para operaciones snm

**Switch D2**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro
SNMP-NMS
snmp-server host 10.0.100.5 version
2c ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf
end
```

advertencia de registro

Ingreso sesión ip

activar sesión

acceso lista a protocolo de administración

protocolo de administración cisco

protocolo de administración comunidad

habilitar las notificaciones

de trampas snmp

habilita el soporte

de ospf para operaciones snm

**Switch A1**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
```

advertencia de registro

Ingreso sesión ip

activar sesión

acceso lista a protocolo de administración

```

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

```

protocolo de administración cisco  
protocolo de administración comunidad

proporciona un valor de índice de interfaz  
habilitar las notificaciones de trampas snmp  
habilita el soporte de ospf para operaciones snm

Figura 13. Configuración administración equipos

```

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#snmp server 2.2.2.2
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)# ip access-list standard SNMP-NMS
R1(config)# permit host 10.0.100.5
R1(config)# exit
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server ifindex persist
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)#end

D1#config t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#snmp server 2.2.2.2
D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
D1(config)# ip access-list standard SNMP-NMS
D1(config)# permit host 10.0.100.5
D1(config)# exit
D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps config
N invalid input detected at '^' marker.
D1(config)# snmp-server enable traps ospf

A1#config t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#snmp server 2.2.2.2
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# ip access-list standard SNMP-NMS
A1(config)# permit host 10.0.100.5
A1(config)# exit
A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)# snmp-server ifindex persist
A1(config)# snmp-server enable traps config

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#snmp master 3
R2(config)#end

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#snmp server 2.2.2.2
R3(config)# logging trap warning
R3(config)# logging on
R3(config)# ip access-list standard SNMP-NMS
R3(config)# permit host 10.0.100.5
R3(config)# exit
R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end

D2#config t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#snmp server 2.2.2.2
D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5
D2(config)# ip access-list standard SNMP-NMS
D2(config)# permit host 10.0.100.5
D2(config)# exit
D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server enable traps config
D2(config)# snmp-server enable traps ospf
D2(config)#end

```

### Evidencia de funcionamiento por medio del comando show

#### show interface trunk

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

Port Vlans allowed on trunk

Po1 1-4094

Po12 1-4094

Port Vlans allowed and active in management do

Po1 1,100-102,999

Po12 1,100-102,999

Port Vlans in spanning tree forwarding state a

Po1 1,100-102,999

Po12 1,100-102,999

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

```
Nov 23 03:13:53.358: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Acti
ve
Nov 23 03:14:03.105: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Acti
ve
Nov 23 03:14:04.681: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Listen -> Activ
e
Nov 23 03:14:14.749: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standb
y
Nov 23 03:14:35.138: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Active -> Speak
Nov 23 03:14:36.410: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Active -> Speak
Nov 23 03:14:45.661: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standb
y
Nov 23 03:14:47.985: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standb
y
Nov 23 03:14:48.179: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standb
y
D1, ENCL: Skills Assessment, Scenario 1

User Access Verification

Username: admin
Password: 

D1#show interface trunk

Port      Mode          Encapsulation  Status      Native VLAN
P0/1    on           802.1q        trunking   999
P0/2    on           802.1q        trunking   999

Port      Vlans allowed on trunk
P0/1    100-102
P0/2    100-102

Port      Vlans allowed and active in management domain
P0/1    100-102
P0/2    100-102

Port      Vlans in spanning tree forwarding state and not pruned
P0/1    100-102
P0/2    100-102
D1#
```

**show run | include spanning-tree**

comando que habilita el portfast en puertos operacionales como puertos de acceso

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

Figura 15. Verificación desarrollo 2.3 y 2.4 en switch D1

## **show run interface e3/0**

Permite revisar el estado, configuración y estadísticas de todas o cada una de las interfaces del dispositivo individualmente

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

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

Figura 16. Verificación desarrollo 2.6 en switch D1

## **show interfaces trunk**

permite verificar múltiples elementos de la operación de los enlaces troncales

D2# show interfaces trunk

## Port Mode Encapsulation Status

## Po2 on 802.1q trunking

## Po12 on 802.1q trunking

Port Vlans allowed on trunk

Po2 1-4094

Po12 1-4094

Port Vlans allowed and active in management do

Po2 1.100-102.999

Po12 1.100-102.999

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

Figura 17. Verificación desarrollo 2.5 en switch D2

```

Nov 23 03:14:04.685: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Standby
Nov 23 03:14:11.718: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Speak -> Standby
Nov 23 03:14:11.774: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby
Nov 23 03:14:12.979: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby
Nov 23 03:14:16.176: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
Nov 23 03:14:35.135: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
Nov 23 03:14:36.409: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Active
Nov 23 03:14:37.510: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
Nov 23 03:14:40.664: %OSPF-5-ADICHG1: Process 4, Nbr 0.0.4.3 on Ethernet2/0 from
LOADING to FULL, Load D2, ENCR SKILLS ASSESSMENT, Scenario 1

User Access Verification
Username: admin
Password:
D2#show interfaces trunk
Port      Mode       Encapsulation  Status      Native vlan
Po2      on        802.1q         trunking   999
Po12     on        802.1q         trunking   999

port      Vlans allowed on trunk
Po2      100-102
Po12     1-4094

port      Vlans allowed and active in management domain
Po2      100-102
Po12     1,100-102,999

port      Vlans in spanning tree forwarding state and not pruned
Po2      100-102
Po12     1,100-102,999
D2#

```

### **show run | section ^router ospf**

permite verificar la configuración OSPF registrada en cada componente de la red

R1# show run | section ^router ospf

```

router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate

```

R3# show run | section ^router ospf

```

router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0

```

D1# show run | section ^router ospf

```

router ospf 4
router-id 0.0.4.131
passive-interface default
network 10.0.10.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0

```

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

Figura 18. Verificación desarrollo configuración OSPF

```
R1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.1
  network 10.0.10.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
  default-information originate
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  router-id 0.0.4.131
  passive-interface default
  network 10.0.10.0 0.0.0.255 area 0
  network 10.0.100.0 0.0.0.255 area 0
  network 10.0.101.0 0.0.0.255 area 0
  network 10.0.102.0 0.0.0.255 area 0
D1#
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
R3#
D2#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface Ethernet2/0
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.100.0 0.0.0.255 area 0
  network 10.0.101.0 0.0.0.255 area 0
  network 10.0.102.0 0.0.0.255 area 0
D2#
```

The terminal window includes a toolbar with icons for file operations, a weather icon showing 21°C, a battery icon, and a date/time stamp of 8:44 a.m. on 23/11/2021.

### **show run | section ^ipv6 router**

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

### **show ipv6 ospf interface brief**

permite verificar la configuración de interfaces OSPF habilitado

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

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

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

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

**show ipv6 ospf interface brief**  
D1# show ipv6 ospf interface brief  
Interface PID Area Intf ID Cost S  
VI102 6 0 25 1 DR  
VI101 6 0 24 1 DR  
VI100 6 0 23 1 DR  
Et2/0 6 0 21 1 B

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

**show ipv6 ospf interface brief**  
D2# show ipv6 ospf interface brief  
Interface PID Area Intf ID Cost S  
VI102 6 0 25 1 DR  
VI101 6 0 24 1 DR  
VI100 6 0 23 1 DR  
Et2/0 6 0 21 10 DR

Figura 19. Verificación tarea 3.2 en cada dispositivo

R1#show run   section ^ipv6 router ipv6 router ospf 6 router-id 0.0.6.1 default-information originate R1# R1#show ipv6 ospf interface brief Interface PID Area Intf ID Cost State Nbrs F/C Se3/0 6 0 6 64 P2P 1/1 Gi2/0 6 0 5 1 DR 0/0 R1#	R3#show run   section ^ipv6 router ipv6 router ospf 6 router-id 0.0.6.3 R3# R3#show ipv6 ospf interface brief Interface PID Area Intf ID Cost State Nbrs F/C Se3/0 6 0 6 64 P2P 1/1 Gi2/0 6 0 5 1 DR 0/0 R3#
D1#show run   section ^ipv6 router ipv6 router ospf 6 router-id 0.0.6.131 passive-interface default D1# D1#show ipv6 ospf interface brief Interface PID Area Intf ID Cost State Nbrs F/C Vl102 6 0 25 1 DR 0/0 Vl101 6 0 24 1 DR 0/0 Vl100 6 0 23 1 DR 0/0 Et2/0 6 0 21 10 DR 0/0 D1#	D2#show run   section ^ipv6 router ipv6 router ospf 6 router-id 0.0.6.132 passive-interface default D2# D2#show ipv6 ospf interface brief Interface PID Area Intf ID Cost State Nbrs F/C Vl102 6 0 25 1 DR 0/0 Vl101 6 0 24 1 DR 0/0 Vl100 6 0 23 1 DR 0/0 Et2/0 6 0 21 10 DR 0/0 D2#

### **show run | section bgp**

verificación de intercambio informativo entre dispositivos

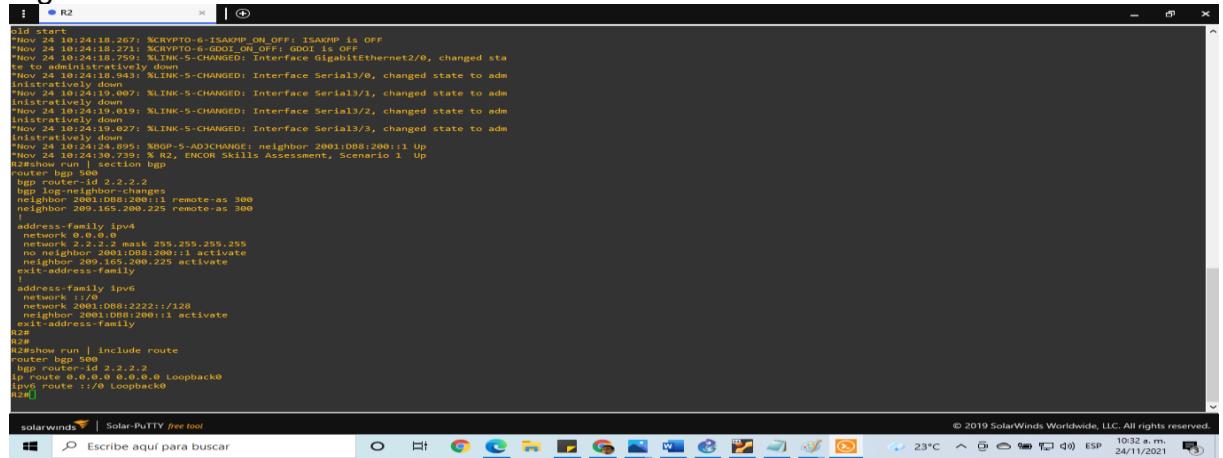
```
R2# show run | section router bgp
router bgp 500
bgp router-id 2.2.2.2
bgp log-neighbor-changes
neighbor 2001:DB8:200::1 remote-as 300
neighbor 209.165.200.225 remote-as 300
!
address-family ipv4
network 0.0.0.0
network 2.2.2.2 mask 255.255.255.255
no neighbor 2001:DB8:200::1 activate
neighbor 209.165.200.225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

### **show run | include route**

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

ipv6 route ::/0 Loopback0

Figura 20. Verificación tarea 3.3 en R2



The screenshot shows a SolarWinds Putty window titled "R2". The terminal session displays the following configuration commands:

```
old start
Nov 24 10:24:18.267: %CRYPTO-5-G001: DR OFF, GD01 Is OFF
Nov 24 10:24:18.271: %CRYPTO-5-G002: DR OFF, GD02 Is OFF
Nov 24 10:24:18.759: %LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to up
to administratively down
Nov 24 10:24:18.763: %LINK-5-CHANGED: Interface Serial3/0, changed state to adm
inistratively down
Nov 24 10:24:18.767: %LINK-5-CHANGED: Interface Serial3/1, changed state to adm
inistratively down
Nov 24 10:24:19.019: %LINK-5-CHANGED: Interface Serial3/2, changed state to adm
inistratively down
Nov 24 10:24:19.027: %LINK-5-CHANGED: Interface Serial3/3, changed state to adm
inistratively down
Nov 24 10:24:19.029: %NGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
Nov 24 10:24:19.739: % R2, ENCOR Skills Assessment, Scenario 1 Up
R2# show run | section bgp
router bgp 500
bgp router-id 2.2.2.2
bgp log-neighbor-changes
neighbor 2001:DB8:200::1 remote-as 300
neighbor 209.165.200.225 remote-as 300
!
address-family ipv4
network 0.0.0.0 0.0.0.0 mask 255.255.255.255
no neighbor 2001:DB8:200::1 activate
no neighbor 209.165.200.225 activate
exit-address-family
R2#
R2# show run | include route
route 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Loopback0
ip route ::/0 Loopback0
R2#
```

The status bar at the bottom right indicates the date and time: 24/11/2021, 10:32 a. m.

### show run | section bgp

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

Figura 21. Verificación punto 3.4 en R1

```
R1 con0 is now available

Press RETURN to get started.

R1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: admin
Password: 
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 209.108.200.12 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 0.0.0.0 0.0.0.0
    neighbor 209.108.200.12 activate
    neighbor 209.165.200.226 activate
    exit-address-family
  !
  address-family ipv6
    network :: 0::0
    neighbor 209.108.200.12/48
    neighbor 209.165.200.226/48
    exit-address-family
  !
  timer server enable traps bgp
R1#
```

**show ip route | include O|B**

verificación de OSPF y BGP para IPv4 funcionan correctamente

R1 # muestra la ruta IP | incluir O | B

Códigos: L - local, C - conectado, S - estático, R -

D - EIGRP, EX - EIGRP externo, O - OSPF, IA -

N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA

E1 - OSPF externo tipo 1, E2 - OSPF externo ti

o - ODR, P - ruta estática descargada periódic

B \* 0.0.0.0/0 [20/0] a través de 209.165.200.2,

B 2.2.2.2 [20/0] vía 209.165.200.2, 01:51:16

O 10.0.11.0/24 [110/65] a través de 10.0.13.3,

O 10.0.100.0/24 [110/66] a través de 10.0.10.2,

O 10.0.101.0/24 [110/66] a través de 10.0.10.2,

O 10.0.102.0/24 [110/66] a través de 10.0.10.2,

Figura 22. Verificación de OSPF y BGP para IPv4

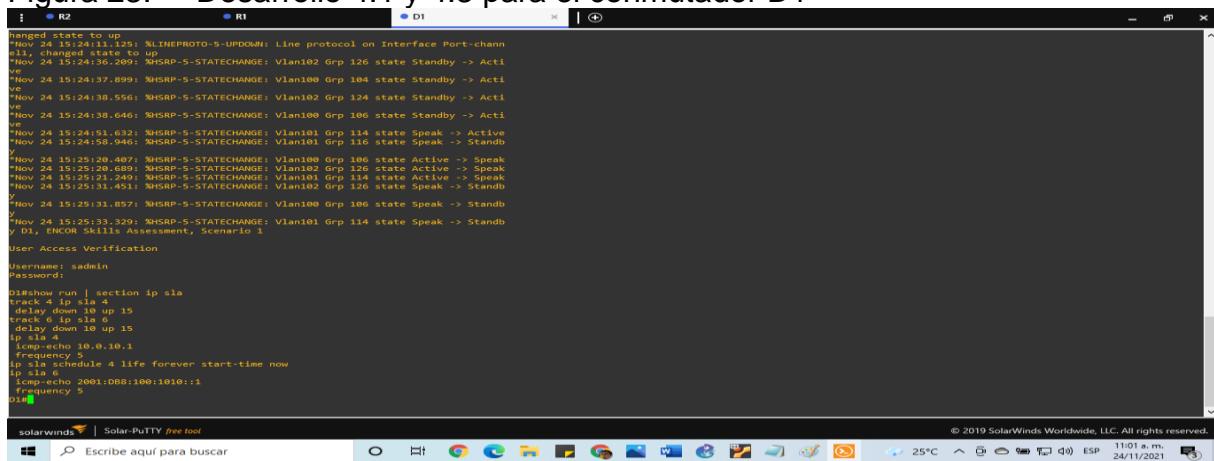
```
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP
O* 0.0.0.0/0 [20/0]
B 2.2.2.2 [20/0] via 209.165.200.226, 00:19:01
O 10.0.11.0/24 [110/65] via 10.0.13.3, 00:19:07, Serial3/0
O 10.0.100.0/24 [110/66] via 10.0.10.2, 00:18:57, Serial3/0
O 10.0.101.0/24 [110/66] via 10.0.13.3, 00:18:57, Serial3/0
O 10.0.102.0/24 [110/66] via 10.0.13.3, 00:18:57, Serial3/0
R1#
```

## **show run | section ip sla**

permite identificar el archivo de configuración activo en la RAM  
se verifica desarrollo 4.1 y 4.3 para el commutador D1

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

Figura 23. Desarrollo 4.1 y 4.3 para el commutador D1



The screenshot shows a terminal window titled "SolarWinds Solar-PuTTY free tool". The command entered is "D1# show run | section ip sla". The output displays the configuration for IP SLA tracks 4 and 6, including their schedules and echo destinations. The session title bar also shows "R2", "R1", and "D1". The bottom status bar indicates the date and time as "24/11/2021 11:01 a.m.", the location as "Barcelona, Spain", and the temperature as "25°C".

```
R2 R1 D1
Rangeto up
Nov 24 15:24:11.125: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel
changed state to up
Nov 24 15:24:13.209: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Acti
ve
Nov 24 15:24:13.899: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Acti
ve
Nov 24 15:24:13.899: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby -> Acti
ve
Nov 24 15:24:13.899: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby -> Acti
ve
Nov 24 15:24:13.899: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Acti
ve
Nov 24 15:24:13.899: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby -> Acti
ve
Nov 24 15:24:38.646: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Acti
ve
Nov 24 15:24:51.632: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Active
Nov 24 15:24:58.946: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standb
y
Nov 24 15:25:20.407: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Active -> Speak
Nov 24 15:25:20.407: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Active -> Speak
Nov 24 15:25:20.407: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Speak
Nov 24 15:25:31.451: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standb
y
Nov 24 15:25:31.857: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standb
y
Nov 24 15:25:33.529: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standb
y
01 ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: admin
Password:
D1# show run | section ip sla
track 4 ip sla 4
delay down 10 up 15
track 6 ip sla 6
delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
D1#
```

## **show standby brief**

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

```
D1# show standby brief
```

P indicates configured to preemp

|

```
Interface Grp Pri P State Active Standb
VI100 104 150 P Active local 10.0.100.2
VI100 106 90 P Active local FE80::D2:2
VI101 114 100 P Standby 10.0.101.2 local
VI101 116 40 P Standby FE80::D2:3 local
```

VI102 124 150 P Active local 10.0.102.2  
VI102 126 90 P Active local FE80::D2:4

Figura 24. Identificación desarrollo 4.3

```
R1# show standby brief
  * indicates configured to preempt.

Interface  Opr  Pri  P state  Active   Standby          Virtual IP
VI100    100  90  P Active  local   10.0.100.2      10.0.100.254
VI100    100  90  P Standby FE80::D2:4      local   FE80::15:73FF:FEA0:16A
VI101    114  100  P Standby 10.0.101.2      local   10.0.101.254
VI101    114  100  P Standby 10.0.101.13     local   FE80::15:73FF:FEA0:174
VI102    124  150  P Active  local   10.0.102.2      10.0.102.254
VI102    126  90  P Standby FE80::D2:4      local   FE80::15:73FF:FEA0:7E
R1#
```

**show run | include secret**  
confirmación de clave encriptada

R1# show run | include secret  
enable secret 9 \$9\$0C3pnVdgrhnY9\$uzGA.WZfcLg5lhuyJu2  
username sadmin privilege 15 secret 9 \$9\$XCO4pzqbRT.3

Figura 25. Identificación tarea 5.1 y 5.2

```
R1# show run | include secret
enable secret 9 $9$0C3pnVdgrhnY9$uzGA.WZfcLg5lhuyJu2
username sadmin privilege 15 secret 9 $9$XCO4pzqbRT.3
R1#
```

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

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

Figura 26. Identificación tareas 5.3, 5.4 y 5.5

The screenshot shows a Windows desktop environment with three terminal windows open in SolarWinds Putty. The title bar for each window indicates the device name: R2, R1, and D1. The R1 window displays the configuration command and its output:

```
R1# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$0IoyBnhIBsbhqq$qjxjBLofX18TUbkp4H7..5f85OxQReVnCH2hkEodVn#o
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
aaa new-model
aaa session-id common
```

### **show run | incluir ntp**

verificación de hora actual UTC correcta

```
R2 # show run | incluir ntp
ntp master 3
```

### **show ntp status | include stratum**

permite verificar si NTP funciona, sincronización de tiempo y relojes y que estos se comuniquen exitosamente

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

Figura 27. Verificación desarrollo 6.3

The screenshot shows a SolarWinds Putty window titled 'R1' with three tabs: R2, R1, and A1. The R1 tab displays a log of system events from November 24, 2018. The log includes entries for interface states (Ethernet1/1, Ethernet1/2, Ethernet2/1, Ethernet2/2, Ethernet3/1, Ethernet3/2, Vlan1, Vlan100), protocol states (XLINEPROTO-5-UPDOWN), and configuration changes (XLINK-5-CHANGED). It also shows user access verification for 'admin'. The bottom of the window shows a command-line prompt and a SolarWinds toolbar.

```
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/1 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/2 changed state to up
Nov 24 18:45:03.508: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Nov 24 18:45:04.783: %LINK-5-CHANGED: Interface Vlan1, changed state to adminis trative down
Nov 24 18:45:04.967: %LINK-3-UPDOWN: Interface Vlan100, changed state to up
Nov 24 18:45:05.969: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, c hanged state to up
Nov 24 18:45:12.697: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann el1, changed state to up
Nov 24 18:45:12.697: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann el2, changed state to up
User Access Verification
Username: admin
password:
Allow ntp status | include stratum
Clock is unsynchronized; Stratum 16, no reference clock
A1#
```

solarwinds Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 27°C 1:55 p. m. 24/11/2021

**show run | include logging**  
confirmación comando de registro

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

Figura 28. Verificación desarrollo 6.4

The screenshot shows a SolarWinds Putty window titled 'R1' with three tabs: R2, R1, and A1. The R1 tab displays a log of system events from November 24, 2018. The log includes entries for interface states (Ethernet1/1, Ethernet1/2, Ethernet2/1, Ethernet2/2, Ethernet3/1, Ethernet3/2, Vlan1, Vlan100), protocol states (XLINEPROTO-5-UPDOWN), and configuration changes (XLINK-5-CHANGED). It also shows user access verification for 'admin'. The bottom of the window shows a command-line prompt and a SolarWinds toolbar.

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

solarwinds Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved. 27°C 2:02 p. m. 24/11/2021

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

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

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

### Figura 29. Verificación tarea 6.5

## **CONCLUSIONES**

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

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

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

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

## BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). *EIGRP. CCNP and CCIE Enterprise Core ENCOR 350-401.* <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300- 115. <https://1drv.ms/b/s!AmIjYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. <https://1drv.ms/b/s!AmIjYeiNT1InMfy2rhPZHwEoWx>

Wallace, K. (2015). CISCO Press (Ed). *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide.* <https://1drv.ms/b/s!AqIGg5JUqUBthFx8WOxiq6LPJppl>