

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSÉ DAVID RESTREPO GÓMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
MANIZALES  
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSÉ DAVID RESTREPO GÓMEZ

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
MANIZALES  
2021

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Manizales, 10 de noviembre de 2021

## **AGRADECIMIENTOS**

Doy gracias en primera instancia a Dios que durante cada día me llena más de vida, anhelos, sueños, energía y vigor para salir adelante. A mi mamá Gloria Stella Gómez que desde el cielo debe sentirse muy orgullosa de mí de haber culminado una segunda carrera y no darme por vencido nunca, además de que siempre me inculcó de terminar todo lo que se empieza, no dejar todo para última hora y de ser una gran persona. A mi padre Omar Restrepo Alzate por su apoyo para sacar esta profesión adelante y acompañarme en los momentos difíciles. A mi pareja por estar siempre conmigo y alentándome a salir adelante a cada momento. Finalmente, a la UNAD por ser mi segunda casa, a los tutores que desde primer semestre me acompañaron con sus valiosos conocimientos y asesorías para sacar adelante cada una de las asignaturas.

## CONTENIDO

Agradecimientos .....	4
Contenido .....	5
Lista de tablas .....	6
Lista de figuras .....	7
Glosario .....	8
Resumen .....	9
Abstract .....	9
Introducción .....	10
Desarrollo .....	11
1. Escenario propuesto .....	11
Conclusiones .....	54
Bibliografía .....	55

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	11
Tabla 2. Tareas a realizar de 2.1 a 2.8 .....	20
Tabla 3. Tareas a realizar de 3.1 a 3.4 .....	26
Tabla 4. Tareas a realizar de 4.1 a 4.3 .....	38
Tabla 5. Tareas a realizar de 5.1 a 5.6 .....	43
Tabla 6. Tareas a realizar de 6.1 a 6.2 .....	47

## LISTA DE FIGURAS

Figura 1. Topología de red (escenario propuesto)	11
Figura 2. Montaje de la topología de red en GNS3	12
Figura 3. Verificación D1 Port mediante show interfaces trunk	24
Figura 4. Verificación D1 mediante show run   include spanning-tree	24
Figura 5. Verificación D1 mediante show run int g2/3	24
Figura 6. Verificación A1 Port mediante show int trunk	25
Figura 7. Verificación A1 mediante show run int g2/3	25
Figura 8. Verificación A1 mediante show run int g3/0	25
Figura 9. Verificación R1 mediante show ip ospf neighbor	33
Figura 10. Verificación D1 mediante show ip ospf neighbor	33
Figura 11. Verificación R1 mediante show ip ospf neighbor 2 vecinos	33
Figura 12. Verificación vecino en D1 mediante show ip ospf neighbor	34
Figura 13. Verificación en R3 mediante show ip ospf neighbor	34
Figura 14. Verificación vecino D2 mediante show ip ospf neighbor	34
Figura 15. Verificación R1 mediante comando show ip bgp neighbor	35
Figura 16. Verificación R1 conexiones mediante show ip route	35
Figura 17. Verificación de R1 bgp, ospf mediante show ipv6 route	36
Figura 18. Verificación R2 rutas estáticas, bgp mediante show ip route	36
Figura 19. Verificación de R2 ruta estática, bgp mediante show ipv6 route	37
Figura 20. Verificación de R3 ospf, conexiones, mediante show ip route	37
Figura 21. Verificación R3 conexiones, local, mediante show ipv6 route	37
Figura 22. Verificación en D1 mediante show standby brief	42
Figura 23. Verificación en D2 mediante show standby brief	42
Figura 24. Verificación en R1 de la autenticación de seguridad	46
Figura 25. Comprobación en D1 de la autenticación de la seguridad	47
Figura 26. Verificación en D2 mediante snmp-server enable traps ?	51
Figura 27. Verificación en R1 mediante show run   include snmp	52
Figura 28. Verificación en D1 mediante show run   include snmp	53
Figura 29. Topología finalizada	53

## GLOSARIO

**Conmutación:** Se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

**DHCP:** Es un servidor de Red el cual permite una asignación automática de direcciones IP, gateways predeterminadas, así como otros parámetros de red que necesiten los clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red.

**Dirección IP:** Es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (Internet Protocol) o que corresponde al nivel de red del modelo TCP/IP.

**Dirección loopback:** Es una dirección ip (también conocida como localhost) reservada específicamente para probar el funcionamiento de TCP/IP en un dispositivo. Una dirección loopback se necesita para realizar tareas de diagnóstico de una conexión de red, en principio, requieren siempre de 2 terminales: un transmisor y un receptor.

**Router:** Son aquellos que guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

**SCRIPT:** Son fragmentos de código que se utilizan para dar forma a herramientas tanto en Internet como en el sector de la informática en general. Son una parte crucial del software, ya que se trata precisamente del código que conforma a una aplicación en su totalidad o a una de sus funciones.

**SLAs:** Se trata de un contrato firmado entre las partes involucradas en una negociación que determina cuáles son las responsabilidades de cada uno en relación a los servicios contratados.

**Switch:** 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.

**VLANs:** Aquel que nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soporten VLANs para segmentar adecuadamente la red.

## **RESUMEN**

En esta prueba de habilidades del diplomado de profundización CISCO CCNP se debe realizar la respectiva configuración electrónica de la red para que haya una accesibilidad completa de la conmutación esto con el fin de que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) del enrutamiento y para que los protocolos configurados estén operando correctamente dentro de la parte correspondiente a la red de topología propuesta.

La prueba de habilidades permitirá trabajar en seis puntos básicos, en cada uno se desarrollará la construcción de la red y la respectiva configuración de los dispositivos básicos. Posteriormente, se deben configurar las capas de redes y realizar un soporte de Host. Cuando se haga esta parte se debe configurar los protocolos de enrutamiento tanto de IPv4 e IPv6, y pasada esta parte se procede a realizar la configuración del HSRP versión 2 para poder proveer redundancia de primer salto para los Host de la red de la compañía. Finalmente, se le dar seguridad a los diferentes dispositivos de la topología, esto con el fin de poder administrar de manera correcta la red.

Palabras clave: CCNP, CISCO, Conmutación, Enrutamiento, Electrónica, HSRP, IPv4, IPv6, Redes

## **ABSTRACT**

In this skills test of the CISCO CCNP in-depth diploma, the respective electronic configuration of the network must be carried out so that there is complete accessibility of the switching, so that the hosts have a reliable support of the default gateway (default gateway) of the routing and so that the configured protocols are operating correctly within the part corresponding to the proposed topology network.

The skills test will allow working on six basic points, in each one the construction of the network and the respective configuration of the basic devices will be developed. Subsequently, the network layers must be configured and Host support performed. When this part is done, the routing protocols for both IPv4 and IPv6 must be configured, and after this part, the HSRP version 2 configuration is carried out in order to provide first-hop redundancy for the Hosts of the company network. Finally, the different devices in the topology will be given security, this in order to be able to correctly manage the network.

Keywords: CCNP, CISCO, Electronics, HSRP, IPv4, IPv6, Networking, Switching, Routing

## INTRODUCCIÓN

El diplomado de profundización Cisco CCNP corresponde al curso Cisco Enterprise Network Core Technologies (CCNP ENCOR v8) ofrecido a nivel mundial por Cisco Networking Academy, y que sirve como requisito de grado para optar por el título de ingeniero. El Diplomado Cisco CCNP permite desarrollar la capacidad de planificación, implementación, verificación en la solución de problemas de redes empresariales locales y de área amplia y trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, redes inalámbricas y calidad de servicio (QoS). Las temáticas para el desarrollo del diplomado están distribuidas en cuatro grandes ejes que son el Switching, Routing, Wireless y finamente Enterprise.

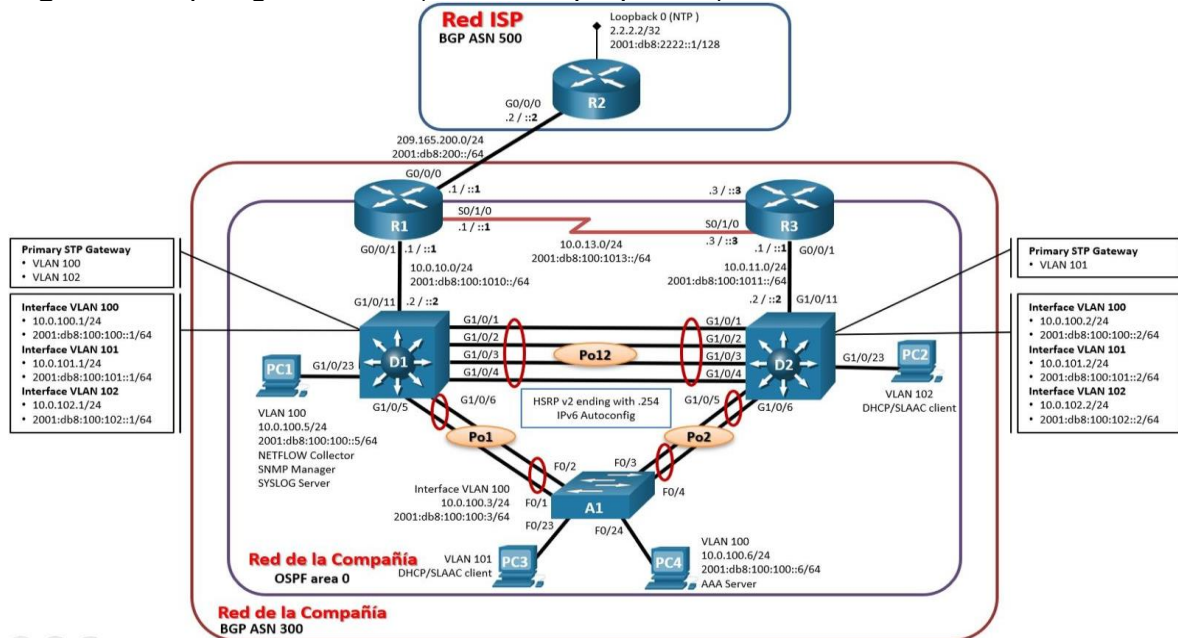
Dentro del desarrollo del diplomado se deberá trabajar en la creación de una red empresarial eficaz y escalable en la que se permita instalar, configurar, supervisar y solucionar problemas en los equipos pertenecientes a la infraestructura de una red multipropósito y multiplataforma.

Para poder llevar a cabo todo esto se contará con un escenario propuesto y una topología de red que tiene asignada su respectiva tabla de direccionamiento y para ello se deberá alcanzar una serie de objetivos para dar solución a este escenario. Estos objetivos radican en construir la red y configurar los ajustes básicos de cada dispositivo, la configuración de la capa 2 de red y soporte Host, configurar protocolos de enrutamiento, configuración de la redundancia del primer salto, además la configuración de seguridad y finalmente la configuración de las características de administración de red.

## DESARROLLO

### ESCENARIO PROPUESTO

**Figura 1:** Topología de Red (escenario propuesto)



Fuente: Rúbrica de evaluación UNAD

### TABLA DE DIRECCIONAMIENTO

**Tabla 1:** Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
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
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a:1
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
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

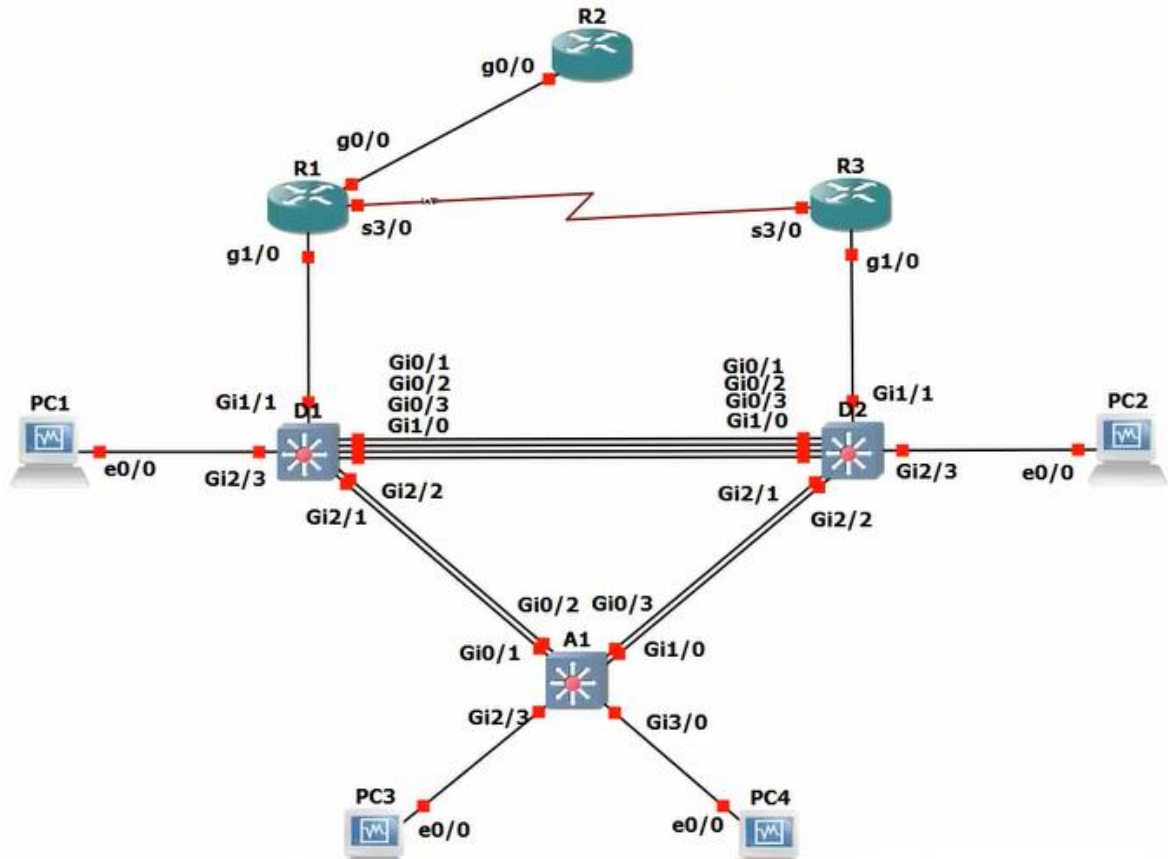
Fuente: Rúbrica de evaluación UNAD

**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:** Montaje de la topología de red en GNS3



**Fuente:** Autor

**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.
- b. Copie el archivo running-config al archivo startup-config en todos los dispositivos.
- c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

## **Router 1 (R1)**

```
R1#config terminal "Ingreso a modo de configuración"
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1 "Asignar nombre"
R1(config)#ipv6 unicast-routing "Se habilita routing IPv6 en el router"
R1(config)#no ip domain lookup "Desactivar búsqueda de DNS"
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0 "Ingreso configuración consola"
R1(config-line)#exec-timeout 0 0 "Establecer tiempo de inactividad en 0"
R1(config-line)#logging synchronous "Evitar el desplazamiento del comando"
R1(config-line)#exit
R1(config)#interface g0/0 "Asignar interfaces"
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown "Habilita interfaz"
R1(config-if)#exit
R1(config)#interface g1/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0 "Se asigna dirección ip"
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown "Habilita la interfaz"
R1(config-if)#exit
R1(config)#interface s3/0 "Asigna Interface serial"
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local "Muestra dirección link"
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown "Habilita interfaz"
R1(config-if)#exit "Salida"
R1(config)#
```

## **Router 2 (R2)**

```
R2#config terminal "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2 "Asignar nombre"
R2(config)#ipv6 unicast-routing "Se habilita routing IPv6 en el router"
R2(config)#no ip domain lookup "Desactiva nombre a dirección de dispositivo"
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0 "Ingreso configuración consola"
R2(config-line)#exec-timeout 0 0 "Establecer tiempo de inactividad en 0"
R2(config-line)#logging synchronous "Evitar el desplazamiento del comando"
R2(config-line)#exit
R2(config)#interface g0/0 "Asignar interfaces"
```

```

R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local          "Muestra dirección link"
R2(config-if)#ipv6 address 2001:db8:200::2/64          "Se configura subred"
R2(config-if)#no shutdown                              "Habilitar interfaz"
R2(config-if)#exit
R2(config)#interface Loopback 0                       "Habilita interface loopback 0"
R2(config-if)#ip address 2.2.2.2 255.255.255.255     "Habilita ip"
R2(config-if)#ipv6 address fe80::2:3 link-local        "Muestra dirección link"
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown                              "Habilita interfaz"
R2(config-if)#exit                                    "Salida"
R2(config)#

```

### **Router 3 (R3)**

```

R3#config terminal                                    "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#hostname R3                               "Asignar nombre"
R3(config)#ipv6 unicast-routing                      "Se habilita routing IPv6 en el router"
R3(config)#no ip domain lookup                      "Desactiva nombre a dirección de dispositivo"
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0                                "Ingreso configuración consola"
R3(config-line)#exec-timeout 0 0                    "Establecer tiempo de inactividad en 0"
R3(config-line)#logging synchronous                 "Evitar el desplazamiento del comando"
R3(config-line)#exit
R3(config)#interface g1/0                            "Asignan interfaces gigabit"
R3(config-if)#ip address 10.0.11.1 255.255.255.0    "Habilita ip"
R3(config-if)#ipv6 address fe80::3:2 link-local      "Muestra dirección link"
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown                            "Habilita interfaz"
R3(config-if)#exit
R3(config)#interface s3/0                            "Asigna interface serial"
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local      "Muestra dirección link"
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown                            "Habilita interfaz"
R3(config-if)#exit                                    "Salida"
R3(config)#

```

### **Switch 1 (D1)**

Switch>

%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/1 (not full duplex), with R1 GigabitEthernet1/0 (full duplex).
---

Se presenta un problema de que “**duplex mismatch**” no coincide la configuración de duplex en Gigabit1/1. Se procede a organizar el problema presentado.

Switch>enable	Ingreso a modo privilegiado
Switch#show run	Se observa que la negociación del GigabitEthernet1/1 está en automático
R1(config)#do show run	Se procede a revisar el problema presentado.  <pre>interface GigabitEthernet1/0 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</pre> <p>Se aprecia que en la interface GigabitEthernet del router 1 la negociación se encuentra en automático. Después de revisar el problema, se regresa a D1 (switch).</p>
Switch#config terminal Enter configuration commands, one per line. End with CNTL/Z.	Ingreso a modo configuración
Switch(config)#int g1/1	
Switch(config-if)#?	Habilito menú de ayuda en el sistema
Switch(config-if)#duplex ?	En el menú se puede observar que  <pre>Switch(config-if)#duplex ?  auto  Enable AUTO duplex configuration  full  Force full duplex operation  half  Force half-duplex operation</pre> <p>dúplex se encuentra en modo full</p>
Switch(config-if)#duplex full	Nos muestra que la negociación automática se encuentra activada. Por consiguiente, dúplex no puede ser establecido. Se va a proceder a quitar la configuración “ <b>interface GigabitEthernet1/1</b> ”.
Switch(config-if)#no negotiation auto	Se procede a quitar el respectivo comando
Switch(config-if)#duplex full	Se ha realizado la respectiva configuración del dúplex
Switch(config-if)#exit	Salida

Switch(config)#	Esto ya muestra que se encuentra en modo de configuración global
-----------------	--

```

Switch(config)#hostname D1                "Se asigna nombre"
D1(config)#ip routing                     "Habilitar ip routing"
D1(config)#ipv6 unicast-routing           "Se habilita routing IPv6 en el router"
D1(config)#no ip domain lookup            "Desactiva nombre a dirección de dispositivo"
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0                     "Ingreso configuración consola"
D1(config-line)#exec-timeout 0 0          "Establecer tiempo de inactividad en 0"
D1(config-line)#logging synchronous       "Evitar el desplazamiento del comando"
D1(config-line)#exit
D1(config)#vlan 100                       "Asignar vlan"
D1(config-vlan)#name Management            "Asignar nombre a la vlan"
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface g1/1                 "Asignar interfaces gigabit"
D1(config-if)#no switchport               "Configuración puertos enrutados"
D1(config-if)#ip address 10.0.10.2 255.255.255.0 "Asigna ip"
D1(config-if)#ipv6 address fe80::d1:1 link-local "Muestra dirección link"
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown                 "Habilita interfaz"
D1(config-if)#exit
D1(config)#interface vlan 100              "interface vlan"
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown                 "Habilita inetrfaz"
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0 "Asinga ip"
D1(config-if)#ipv6 address fe80::d1:3 link-local "Muestra dirección link"
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit                        "Salida"
D1(config)#interface vlan 102

```

```

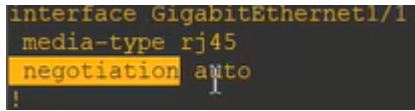
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local           "Muestra dirección link"
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109      "ip servidor"
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0      "Configuración network"
D1(dhcp-config)#default-router 10.0.101.254          "Especifica enrutadores"
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range g0/0-3, g1/0, g1/2-3, g2/0-3, g3/0-3
D1(config-if-range)#shutdown                          "Apaga rango de interfaces"
D1(config-if-range)#exit                              "Salida"
D1(config)#

```

## **Switch 2 (D2)**

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet1/1 (not full duplex), with R3 GigabitEthernet1/0 (full duplex).
```

Se presenta un problema de que **"duplex mismatch"** no coincide la configuración de duplex en Gigabit1/1. Se procede a organizar el problema presentado.

Switch>enable	Ingreso a modo privilegiado
Switch#config terminal Enter configuration commands, one per line. End with CNTL/Z.	Ingreso a modo configuración
Switch(config)#do show run	Se revisa donde está el problema   Detectado se procede a quitar
Switch(config)#int g1/1	
Switch(config-if)#no negotiation auto	Quitar el respectivo comando
Switch(config-if)#duplex full	Se realiza configuración del dúplex

Switch(config-if)#exit	Salida
Switch(config)#	Modo de configuración global

Switch(config)#hostname D2	“Se asigna nombre”
D2(config)#ip routing	“Habilita ip routing”
D2(config)#ipv6 unicast-routing	“Se habilita routing IPv6 en el router”
D2(config)#no ip domain lookup	“Desactiva nombre a dirección de dispositivo”
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	
D2(config)#line con 0	“Ingreso configuración consola”
D2(config-line)#exec-timeout 0 0	“Establecer tiempo de inactividad en 0”
D2(config-line)#logging synchronous	“Evitar el desplazamiento de comando”
D2(config-line)#exit	
D2(config)#vlan 100	“Asignar vlan”
D2(config-vlan)#name Management	“Asignar nombre a la vlan”
D2(config-vlan)#exit	
D2(config)#vlan 101	
D2(config-vlan)#name UserGroupA	
D2(config-vlan)#exit	
D2(config)#vlan 102	
D2(config-vlan)#name UserGroupB	
D2(config-vlan)#exit	
D2(config)#vlan 999	
D2(config-vlan)#name NATIVE	
D2(config-vlan)#exit	
D2(config)#interface g1/1	“Asignar interfaces gigabit”
D2(config-if)#no switchport	“Configuración puertos enrutados”
D2(config-if)#ip address 10.0.11.2 255.255.255.0	“Asignar ip”
D2(config-if)#ipv6 address fe80::d1:1 link-local	“Muestra dirección link”
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64	
D2(config-if)#no shutdown	“Habilita interfaz”
D2(config-if)#exit	
D2(config)#interface vlan 100	“Interface vlan”
D2(config-if)#ip address 10.0.100.2 255.255.255.0	
D2(config-if)#ipv6 address fe80::d2:2 link-local	“Muestra dirección local”
D2(config-if)#ipv6 address 2001:db8:100:100::2/64	
D2(config-if)#no shutdown	
D2(config-if)#exit	
D2(config)#interface vlan 101	
D2(config-if)#ip address 10.0.101.2 255.255.255.0	“Asigna dirección ip”
D2(config-if)#ipv6 address fe80::d2:3 link-local	
D2(config-if)#ipv6 address 2001:db8:100:101::2/64	
D2(config-if)#no shutdown	
D2(config-if)#exit	
D2(config)#interface vlan 102	“Interface vlan”

```

D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209      "ip servidor"
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0      "Configuración network"
D2(dhcp-config)#default-router 10.0.101.254          "Especifica enrutadores"
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0      "Configuración network"
D2(dhcp-config)#default-router 10.0.102.254          "Especifica enrutadores"
D2(dhcp-config)#exit
D2(config)#interface range g0/0-3, g1/0, g1/2-3, g2/0-3, g3/0-3
D2(config-if-range)#shutdown                          "Se apaga rango de interfaces"
D2(config-if-range)#exit                              "Salida"
D2(config)#

```

### **Switch (A1)**

```

Switch>enable                                          "Ingreso a modo privilegiado"
Switch#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname A1                            "Se asigna nombre"
A1(config)#no ip domain lookup                       "Desactiva nombre a dirección de dispositivo"
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0                                 "Ingreso configuración consola"
A1(config-line)#exec-timeout 0 0                     "Establecer tiempo de inactividad en 0"
A1(config-line)#logging synchronous                  "Evitar el desplazamiento de comando"
A1(config-line)#exit
A1(config)#vlan 100                                   "Asignar vlan"
A1(config-vlan)#name Management                       "Asignar nombre a la vlan"
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE

```

```

A1(config-vlan)#exit
A1(config)#interface vlan 100                                "Interface vlan"
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local             "Muestra dirección local"
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown                                    "Habilita interfaz"
A1(config-if)#exit
A1(config)#interface range g1/1-3, g2/0-3, g3/0-3
A1(config-if-range)#shutdown                                "Apagan rango de interfaces"
A1(config-if-range)#exit                                    "Salida"
A1(config)#

```

**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 dirección de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

**Tabla 2:** Tareas a realizar de 2.1 a 2.8

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces <u>trunk</u> 802.1Q entre: <ul style="list-style-type: none"> <li>• D1 and D2</li> <li>• D1 and A1</li> <li>• D2 and A1</li> </ul>
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 <u>Spanning-Tree</u> (RSTP)	Use Rapid <u>Spanning Tree</u> (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP ( <u>root bridges</u> ) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz ( <u>root bridge</u> ).	Configure D1 y D2 como raíz ( <u>root</u> ) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

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

**Fuente:** Rúbrica de evaluación UNAD

### Switch 1 (D1)

```

D1(config)#                                     "Modo de configuración global"
D1(config)#interface range g0/1-3, g1/0         "Configuro rango interfaz"
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk      "Enlace troncal"
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

D1(config-if-range)#no shutdown                "Habilito interfaz"
D1(config-if-range)#exit
D1(config)#interface range g2/1-2              "Configuro rango interfaz"
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk      "Enlace troncal"
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active "Activa mode active"
Creating a port-channel interface Port-channel 1

D1(config-if-range)#no shutdown                "Habilito interfaz"
D1(config-if-range)#exit                       "Salida"
D1(config)#spanning-tree mode rapid-pvst

```

```

D1(config)#spanning-tree vlan 100,102 root primary          "vlan primario"
D1(config)#spanning-tree vlan 101 root secondary          "vlan secundario"
D1(config)#interface g2/3                                "Configuro interfaz"
D1(config-if)#switchport mode Access                    "Cambio al modo de acceso permante"
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
D1(config-if)#no shutdown                                "Habilita interfaz"
D1(config-if)#exit                                       "Salida"
D1(config)#end                                          "Fin"
D1#

```

## **Switch 2 (D2)**

```

D2(config)#                                                "Modo de configuración global"
D2(config)#interface range g0/1-3, g1/0                    "Configuro rango interfaz"
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk                 "Enlace troncal"
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

```

```

D2(config-if-range)#no shutdown                            "Habilito interfaz"
D2(config-if-range)#exit
D2(config)#interface range g2/1-2                          "Configuro interfaz"
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2

```

```

D2(config-if-range)#no shutdown                            "Habilito interfaz"
D2(config-if-range)#exit
D2(config)#!
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary            "vlan primario"
D2(config)#spanning-tree vlan 100,102 root secondary      "vlan secundario"
D2(config)#!
D2(config)#interface g2/3                                  "Configura interfaz gigabit"
D2(config-if)#switchport mode Access                    "Cambio al modo de acceso permante"
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown                                "Habilito interfaz"
D2(config-if)#exit                                       "Salida"
D2(config)#end                                          "Finalización"
D2#

```

## **Switch (A1)**

```
A1(config)# "Modo de configuración global"
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range g0/1-2 "Configuro interfaces"
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk "Enlace troncal"
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

A1(config-if-range)#no shutdown "Habilito interfaz"
A1(config-if-range)#exit
A1(config)#interface range g0/3, g1/0 "Rango de interfaces"
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk "Enlace troncal"
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-cahnnel 2

A1(config-if-range)#no shutdown "Habilito interfaz"
A1(config-if-range)#exit
A1(config)#interface g2/3 "Habilito interface gigabit"
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101 "Acceso vlan"
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown "Habilito interfaz"
A1(config-if)#exit
A1(config)#interface g3/0 "Habilito interface gigabit"
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown "Habilito interfaz"
A1(config-if)#exit "Salida"
A1(config)#end "Finalización"
A1#
```

## **Verificaciones**

Al no encontrarse encendido los PC en este momento, entonces puedo realizar las respectivas verificaciones en los diferentes switches.

- **Switch 1 (D1)**

**Figura 3:** Verificación D1 Port mediante “show interfaces trunk”

```
D1#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po1       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po1       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100-102,999
Po12      1,100-102,999
```

**Fuente:** Autor

Se observa en la imagen que las conexiones han salido satisfactorias

**Figura 4:** Verificación D1 mediante “show run | include spanning-tree”

```
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
```

**Fuente:** Autor

El puente raíz (o prioridad) en la vlan 100, 102 es de 24576; mientras que la prioridad secundaria vlan 101 es de 28672 teniendo esta una prioridad más alta

**Figura 5:** Verificación D1 mediante “show run int g2/3”

```
D1#show run int g2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

D1#
```

**Fuente:** Autor

Los puertos de acceso son correctos

## Switch (A1)

**Figura 6:** Verificación A1 Port mediante “show int trunk”

```
A1#show int trunk

Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    999
Po1       on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po2       1-4094
Po1       1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po1       1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po2       101
Po1       1,100,102,999
```

**Fuente:** Autor

Se observan las conexiones a los port-channel satisfactorias

**Figura 7:** Verificación A1 mediante “show run int g2/3”

```
A1#show run int g2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
```

**Fuente:** Autor

Puerto de acceso vlan 101 de forma correcta

**Figura 8:** Verificación A1 mediante “show run int g3/0”

```
A1#show run int g3/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet3/0
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```

**Fuente:** Autor

Puerto de acceso vlan 100 funcionando correctamente

### 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 4:** Tareas a realizar de 3.1 a 3.4

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"> <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>
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"> <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>

Tarea#	Tarea	Especificación
3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz <code>Loopback 0</code>:</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 <code>router-id</code> 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 <code>address family</code>, anuncie:</p> <ul style="list-style-type: none"> <li>La red <code>Loopback 0</code> IPv4 (/32).</li> <li>La ruta por defecto (0.0.0.0/0).</li> </ul> <p>En IPv6 <code>address family</code>, anuncie:</p> <ul style="list-style-type: none"> <li>La red <code>Loopback 0</code> IPv6 (/128).</li> <li>La ruta por defecto (::/0).</li> </ul>
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz <code>Null 0</code>:</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 <code>router-id</code> 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 <code>address family</code>:</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 <code>address family</code>:</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>

Fuente: Rúbrica de evaluación UNAD

### Router 1 (R1)

```

R1(config)#router ospf 4                "Configuro router ospf 4"
R1(config-router)#router-id 0.0.4.1    "Asigno id"
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate "Modo configuración router"
R1(config-router)#exit
R1(config)#ipv6 router ospf 6          "Configura router ospf 6"
R1(config-rtr)#router-id 0.0.6.1      "Asigno id"
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface g1/0              "Habilito interfaces gigabit"
R1(config-if)#ipv6 ospf 6 area 0      "Ospf 6 área 0 en ipv6"
R1(config-if)#exit
R1(config)#interface s3/0              "Habilito interface serial"
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#
R1(config)#ip route 10.0.0.0 255.0.0.0 null0 "Asigno ip route"
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#

```

```

R1(config)#router bgp 300 "Configuración BGP"
R1(config-router)#bgp router-id 1.1.1.1 "Dirección BGP router en 1"
R1(config-router)#neighbor 209.165.200.226 remote-as 500 "Vecino router"
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast "Dirección ipv4"
R1(config-router-af)#neighbor 209.165.200.226 activate "Activa vecino"
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 "Máscara subred"
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family
R1(config-router)#

```

### **Router 2 (R2)**

```

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 "Asigna ip route loopback"
%Default route without Gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500 "Configuración BGP"
R2(config-router)#bgp router-id 2.2.2.2 "Dirección BGP router en 2"
R2(config-router)#neighbor 209.165.200.225 remote-as 300 "Vecino router"
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4 "Asigna familia ipv4"
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6 "Asigna familia ipv6"
R2(config-router-af)#no neighbor 209.165.200.225 activate "Vecino activado"
R2(config-router-af)#neighbor 2001:db8:200::1 activate "Vecino activado"
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#

```

### **Router 3 (R3)**

```

R3(config)#
%CDP -4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet
1/0 (not half duplex), with Switch GigabitEthernet1/1 (half duplex).

```

- Revisando en el Switch 2 (D2)

D2#show run

```
interface GigabitEthernet1/1
no switchport
ip address 10.0.11.2 255.255.255.0
no negotiation auto
ipv6 address FE80::D1:1 link-local
ipv6 address 2001:DB8:100:1011::2/64
!
```

D2#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#int g1/1

D2(config-if)#duplex full

D2(config-if)#exit

D2(config)#

Modo de configuración global

- Regresando al router 3 (R3)

R3(config)#

Modo de configuración global

R3(config)#

R3(config)#router ospf 4

R3(config-router)#router-id 0.0.4.3

R3(config-router)#network 10.0.11.0 0.0.0.255 area 0

R3(config-router)#network 10.0.13.0 0.0.0.255 area 0

R3(config-router)#exit

R3(config)#ipv6 router ospf 6

R3(config-rtr)#router-id 0.0.6.3

R3(config-rtr)#exit

R3(config)#interface g1/0

R3(config-if)#ipv6 ospf 6 area 0

R3(config-if)#exit

R3(config)#interface s3/0

R3(config-if)#ipv6 ospf 6 area 0

R3(config-if)#exit

R3(config)#end

R3#

### **Switch 1 (D1)**

D1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

D1(config)#

Modo de configuración global

```

D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface g1/1
D1(config-router)#exit
D1(config)#ipv6 router ospf 6          Imagen no soportada de Cisco IOS
^
% Invalid input detected at '^' marker.

D1(config)#router-id 0.0.6.131
^
% Invalid input detected at '^' marker.

D1(config)#passive-interface default
^
% Invalid input detected at '^' marker.

D1(config)#no passive-interface g1/1
^
% Invalid input detected at '^' marker.

D1(config)#exit
D1#interface g1/1
^
% Invalid input detected at '^' marker.

D1#ipv6 ospf 6 area 0
^
% Invalid input detected at '^' marker.

D1#exit

D1>enable
D1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ipv6 unicast-routing
D1(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.

```

Se muestra que la imagen no está soportada en Cisco IOSv12

```

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

```

**Nota:** Para tener en cuenta, la respuesta en este Switch D1, sería la siguiente, ya que, al no soportar la imagen, entonces tendríamos esto:

```

ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface g1/1
exit
interface g1/1
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

```

### **Switch 2 (D2)**

```

D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/1
D2(config-router)#exit
D2(config)#ipv6 router ospf 6
^
% Invalid input detected at '^' marker.

```

```
D2(config)#router-id 0.0.6.132
^
% Invalid input detected at '^' marker.
```

```
D2(config)#passive-interface default
^
% Invalid input detected at '^' marker.
```

```
D2(config)#no passive-interface g1/1
^
% Invalid input detected at '^' marker.
```

```
D2(config)#exit
```

Se observa claramente que en el Switch 2 pasa lo mismo que en el Switch 1 ya que para Ipv4 está soportado, mientras que para Ipv6 no lo está (en cuanto a las imágenes).

**Nota:** Para tener en cuenta, la respuesta en este Switch D2, sería la siguiente, ya que, al no soportar la imagen, entonces tendríamos esto:

```
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g1/1
exit
interface g1/1
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
```

### **Verificaciones**

Se realizarán las respectivas verificaciones con el fin de demostrar que se han aplicado las debidas configuraciones:

- En R1

**Figura 9:** Verificación R1 mediante “show ip OSPF neighbor”

```
R1#show ip ospf neighbor
*Oct 29 16:29:26.805: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
0.0.4.3          0    FULL/ -         00:00:33   10.0.13.3     Serial3/0
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g1/0
R1(config-if)#negotiation auto
R1(config-if)#
```

Fuente: Autor

- En D1

**Figura 10:** Verificación D1 mediante “show ip ospf neighbor”

```
D1#show ip ospf neighbor
*Oct 29 15:52:28.053: %SYS-5-CONFIG_I: Configured from console by console
D1#show ip ospf neighbor
D1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#int g1/1
D1(config-if)#negotiation auto
Duplex is configured. Remove duplex configuration before enabling auto-negotiation

D1(config-if)#no duplex
D1(config-if)#negotiation auto
D1(config-if)#end
D1#
*Oct 29 15:53:08.479: %SYS-5-CONFIG_I: Configured from console by console
D1#
*Oct 29 15:53:09.459: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to up
*Oct 29 15:53:10.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed state to up
D1#
*Oct 29 15:53:15.011: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on GigabitEthernet1/1 from LOADING to FULL, Loading Done
D1#
```

Fuente: Autor

- En R1

**Figura 11:** Verificación R1 mediante “show ip OSPF neighbor” 2 vecinos

```
R1(config-if)#end
R1#
R1#show ip ospf neighbor
*Oct 29 16:30:46.365: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
0.0.4.3          0    FULL/ -         00:00:38   10.0.13.3     Serial3/0
0.0.4.131        1    FULL/BDR       00:00:38   10.0.10.2     GigabitEthernet1/0
R1#
```

Fuente: Autor

- En D1

**Figura 12:** Verificación vecino en D1 mediante “show ip OSPF neighbor”

```
D1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
0.0.4.1         1    FULL/DR         00:00:36   10.0.10.1   GigabitEthernet1/1
D1#
```

Fuente: Autor

- En R3

```
R3#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int g1/0
R3(config-if)#negotiation auto
Re(config-if)#exit
R3(config)#end
R3#
```

**Figura 13:** Verificación en R3 mediante “show ip OSPF neighbor”

```
R3#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
0.0.4.1         0    FULL/ -         00:00:35   10.0.13.1   Serial3/0
0.0.4.132       1    FULL/BDR        00:00:36   10.0.11.2   GigabitEthernet1/0
R3#
```

Fuente: Autor

- En D2

```
D2>enable
D2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#int g1/1
D2(config-if)#no duplex
D2(config-if)#negotiation auto
D2(config-if)#exit
D2(config)#end
D2#
```

**Figura 14:** Verificación vecino D2 mediante show ip OSPF neighbor

```
D2#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
0.0.4.3         1    FULL/DR         00:00:38   10.0.11.1   GigabitEthernet1/1
D2#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
0.0.4.3         1    FULL/DR         00:00:39   10.0.11.1   GigabitEthernet1/1
D2#
```

Fuente: Autor

**Nota:** D1, solo tiene un vecino que es R1. No está mostrando D2 como un vecino OSPF porque el enlace troncal es un enlace de capa 2 y no de capa 3.

- En R1

**Figura 15:** Verificación R1 mediante comando “show ip BGP neighbor”

```
R1#show ip bgp neighbor
BGP neighbor is 209.165.200.226, remote AS 500, external link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 07:36:39
  Last read 00:00:52, last write 00:00:31, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

      Sent      Rcvd
  Opens:          1          1
  Notifications:  0          0
  Updates:        2          2
  Keepalives:     501       505
  Route Refresh:  0          0
  Total:          504       508
  Default minimum time between advertisement runs is 30 seconds
```

Fuente: Autor

**Figura 16:** Verificación R1 conexiones mediante “show ip route”

```
R1#show ip route
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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

R*  0.0.0.0/0 [20/0] via 209.165.200.226, 08:22:36
    2.0.0.0/32 is subnetted, 1 subnets
B   2.2.2.2 [20/0] via 209.165.200.226, 08:22:36
    10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
S   10.0.0.0/8 is directly connected, Null0
C   10.0.10.0/24 is directly connected, GigabitEthernet1/0
L   10.0.10.1/32 is directly connected, GigabitEthernet1/0
O   10.0.11.0/24 [110/65] via 10.0.13.3, 08:19:10, Serial3/0
C   10.0.13.0/24 is directly connected, Serial3/0
L   10.0.13.1/32 is directly connected, Serial3/0
O   10.0.100.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
O   10.0.101.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
O   10.0.102.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
C   209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/27 is directly connected, GigabitEthernet0/0
L   209.165.200.225/32 is directly connected, GigabitEthernet0/0
R1#
```

Fuente: Autor

Se observa que se encuentran las BGP, las redes estáticas y las rutas OSPF.

**Figura 17:** Verificación de R1 bgp, ospf mediante “show ipv6 route”

```
R1#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
B   ::/0 [20/0]
    via FE80::2:1, GigabitEthernet0/0
S   2001:DB8:100::/48 [1/0]
    via Null0, directly connected
C   2001:DB8:100:1010::/64 [0/0]
    via GigabitEthernet1/0, directly connected
L   2001:DB8:100:1010::1/128 [0/0]
    via GigabitEthernet1/0, receive
O   2001:DB8:100:1011::/64 [110/65]
    via FE80::3:3, Serial3/0
C   2001:DB8:100:1013::/64 [0/0]
    via Serial3/0, directly connected
L   2001:DB8:100:1013::1/128 [0/0]
    via Serial3/0, receive
C   2001:DB8:200::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:200::1/128 [0/0]
    via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

**Fuente:** Autor

Se encuentran las redes BGP, las redes estáticas, las redes correctamente conectadas OSPF. Se observa en la figura solamente una red OSPF esto debido a que D1 no está soportando OSPF para IPv6.

- En R2

**Figura 18:** Verificación R2 rutas estáticas, bgp mediante “show ip route”

```
R2#show ip route
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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R2# 0.0.0.0/0 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
    C   2.2.2.2 is directly connected, Loopback0
B   10.0.0.0/8 [20/0] via 209.165.200.225, 08:24:07
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/27 is directly connected, GigabitEthernet0/0
L   209.165.200.226/32 is directly connected, GigabitEthernet0/0
R2#
```

**Fuente:** Autor

Figura 19: Verificación de R2 rutas estáticas, bpg mediante “show ipv6 route”

```
R2#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
S    ::/0 [1/0]
    I via Loopback0, directly connected
B    2001:DB8:100::/48 [20/0]
    I via FE80::1:1, GigabitEthernet0/0
C    2001:DB8:200::/64 [0/0]
    I via GigabitEthernet0/0, directly connected
L    2001:DB8:200::2/128 [0/0]
    I via GigabitEthernet0/0, receive
LC   2001:DB8:2222::1/128 [0/0]
    I via Loopback0, receive
L    FF00::/8 [0/0]
    I via Null0, receive
R2#
```

Fuente: Autor

- En R3

Figura 20: Verificación de R3 ospf, conexiones, mediante “show ip route”

```
R3#show ip route
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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 08:21:07, Serial3/0
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O    10.0.10.0/24 [110/65] via 10.0.13.1, 08:21:07, Serial3/0
C    10.0.11.0/24 is directly connected, GigabitEthernet1/0
L    10.0.11.1/32 is directly connected, GigabitEthernet1/0
C    10.0.13.0/24 is directly connected, Serial3/0
L    10.0.13.3/32 is directly connected, Serial3/0
O    10.0.100.0/24 [110/2] via 10.0.11.2, 00:51:39, GigabitEthernet1/0
O    10.0.101.0/24 [110/2] via 10.0.11.2, 00:51:39, GigabitEthernet1/0
O    10.0.102.0/24 [110/2] via 10.0.11.2, 00:51:39, GigabitEthernet1/0
```

Fuente: Autor

Figura 21: Verificación R3 conexiones, local, mediante “show ipv6 route”

```
R3#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
OE2 ::/0 [110/1], tag 6
    I via FE80::1:3, Serial3/0
C    2001:DB8:100:1010::/64 [0/0]
    I via Serial3/0, directly connected
L    2001:DB8:100:1010::2/128 [0/0]
    I via Serial3/0, receive
C    2001:DB8:100:1011::/64 [0/0]
    I via GigabitEthernet1/0, directly connected
L    2001:DB8:100:1011::1/128 [0/0]
    I via GigabitEthernet1/0, receive
O    2001:DB8:100:1013::/64 [110/128]
    I via FE80::1:3, Serial3/0
L    FF00::/8 [0/0]
    I via Null0, receive
R3#
```

Fuente: Autor

## 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 4:** Tareas a realizar de 4.1 a 4.3

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 <del>SLAs</del>.</p> <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> <p>Las IP <del>SLAs</del> probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</p> <p>Programa la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <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> <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>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP <del>SLAs</del>.</p> <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> <p>Las IP <del>SLAs</del> probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.</p> <p>Programa la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and <del>one for</del> IP SLA 6.</p> <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> <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>

Tarea#	Tarea	Especificación
4.3	En D1 configure HSRPv2.	<p>D1 es el <del>router</del> primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a <u>150</u>.</p> <p>Configure HSRP <del>versión 2</del>.</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>Establezca la prioridad del grupo en 150.</li> <li>Habilite la preferencia (<del>preemptio</del>).</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>Habilite la preferencia (<del>preemptio</del>).</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>Establezca la prioridad del grupo en 150.</li> <li>Habilite la preferencia (<del>preemptio</del>).</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 <del>autoconfi</del>.</li> <li>Establezca la prioridad del grupo en 150.</li> <li>Habilite la preferencia (<del>preemptio</del>).</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 <del>autoconfi</del>.</li> <li>Habilite la preferencia (<del>preemptio</del>).</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 <del>autoconfi</del>.</li> <li>Establezca la prioridad del grupo en 150.</li> <li>Habilite la preferencia (<del>preemptio</del>).</li> <li>Rastree el objeto 6 y decremente en 60.</li> </ul>

Tarea#	Tarea	Especificación
	En D2, configure HSRPv2.	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <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 80.</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 80.</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 80.</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 80.</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>Establezca la prioridad del grupo en 150.</li> <li>Habilite la preferencia (preemption).</li> <li>Rastree el objeto 6 para disminuir en 80.</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>Habilite la preferencia (preemption).</li> <li>Rastree el objeto 6 para disminuir en 80.</li> </ul>

**Fuente:** Rúbrica de evaluación UNAD

### Switch 1 (D1)

```

D1#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla 4                               "Asigna dirección ip sla"
D1(config-ip-sla)#icmp-echo 10.0.10.1
D1(config-ip-sla-echo)#frequency 5               "Asigna la frecuencia interfaz 5 seg"
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6                               "Asigna dirección ip sla"
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now    "Número rastreo 4"
D1(config)#ip sla schedule 6 life forever start-time now    "Número rastreo 6"
D1(config)#track 4 ip sla 4

```

D1(config-track)#delay down 10 up 15	“Cambios en el rastreo”
D1(config-track)#exit	
D1(config)#track 6 ip sla 6	
D1(config-track)#delay down 10 up 15	
D1(config-track)#exit	
D1(config)#interface vlan 100	“Habilito interfaz vlan”
D1(config-if)#standby version 2	
D1(config-if)#standby 104 ip 10.0.100.254	
D1(config-if)#standby 104 priority 150	“Habilita prioridad en 150”
D1(config-if)#standby 104 preempt	“Habilita preferencia”
D1(config-if)#standby 104 track 4 decrement 60	
D1(config-if)#standby 106 ipv6 autoconfig	
D1(config-if)#standby 106 priority 150	“Habilita prioridad en 150”
D1(config-if)#standby 106 preempt	
D1(config-if)#standby 106 track 6 decrement 60	
D1(config-if)#exit	
D1(config)#interface vlan 101	“Asingo interface vlan”
D1(config-if)#standby version 2	
D1(config-if)#standby 114 ip 10.0.101.254	
D1(config-if)#standby 114 preempt	“Habilita preferencia”
D1(config-if)#standby 114 track 4 decrement 60	
D1(config-if)#standby 116 ipv6 autoconfig	
D1(config-if)#standby 116 preempt	“Habilita la preferencia”
D1(config-if)#standby 116 track 6 decrement 60	
D1(config-if)#exit	
D1(config)#interface vlan 102	“Asigno interface vlan”
D1(config-if)#standby version 2	
D1(config-if)#standby 124 ip 10.0.102.254	
D1(config-if)#standby 124 priority 150	“Habilita prioridad en 150”
D1(config-if)#standby 124 preempt	
D1(config-if)#standby 124 track 4 decrement 60	
D1(config-if)#standby 126 ipv6 autoconfig	
D1(config-if)#standby 126 priority 150	
D1(config-if)#standby 126 preempt	“Habilita preferencia”
D1(config-if)#standby 126 track 6 decrement 60	
D1(config-if)#exit	“Salida”
D1(config)#end	“Finalización”
D1#	

### **Switch 2 (D2)**

D2#config terminal	“Ingreso a modo configuración”
Enter configuration commands, one per line. End with CNTL/Z.	
D2(config)#ip sla 4	“Asigna dirección ip sla”
D2(config-ip-sla)#icmp-echo 10.0.11.1	

```

D2(config-ip-sla-echo)#frequency 5      "Asigna la frecuencia interfaz en 5 seg"
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6                      "Asigna dirección ip sla"
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5      "Asigna la frecuencia interfaz en 5 seg"
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now      "Número rastreo 4"
D2(config)#ip sla schedule 6 life forever start-time now      "Número rastreo 6"
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15      "Cambios en el rastreo"
D2(config-track)#exit
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#interface vlan 100            "Habilito interfaz vlan"
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt        "Habilita preferencia"
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt        "Habilita preferencia"
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 101            "Habilito interfaz vlan"
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150    "Habilita prioridad en 150"
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150    "Habilita prioridad en 150"
D2(config-if)#standby 116 preempt        "Habilita preferencia"
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 102            "Habilita interface vlan"
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt        "Habilita preferencia"
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit                      "Salida"
D2(config)#end                          "Finalización"
D2#

```

## Verificaciones

- En D1

**Figura 22:** Verificación en D1 mediante “show standby brief”

```
D1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active           Standby           Virtual IP
Vl100     104 150 P Active local          10.0.100.2       10.0.100.254
Vl100     106 150 P Active local          FE80::D2:2       FE80::5:73FF:FEA0:6A
Vl101     114 100 P Standby 10.0.101.2       local            10.0.101.254
Vl101     116 100 P Standby FE80::D2:3       local            FE80::5:73FF:FEA0:74
Vl102     124 150 P Active local          10.0.102.2       10.0.102.254
Vl102     126 150 P Active local          FE80::D2:4       FE80::5:73FF:FEA0:7E
```

Fuente: Autor

- En D2

**Figura 23:** Verificación en D2 mediante “show standby brief”

```
D2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active           Standby           Virtual IP
Vl100     104 100 P Standby 10.0.100.1       local            10.0.100.254
Vl100     106 100 P Standby FE80::D1:2       local            FE80::5:73FF:FEA0:6A
Vl101     114 150 P Active local          10.0.101.1       10.0.101.254
Vl101     116 150 P Active local          FE80::D1:3       FE80::5:73FF:FEA0:74
Vl102     124 100 P Standby 10.0.102.1       local            10.0.102.254
Vl102     126 100 P Standby FE80::D1:4       local            FE80::5:73FF:FEA0:7E
D2#
```

Fuente: Autor

## 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 5:** Tareas a realizar de 5.1 a 5.6

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"> <li>Nombre de usuario Local: <b>sadmin</b></li> <li>Nivel de privilegio <b>15</b></li> <li>Contraseña: <b>cisco12345cisco</b></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: <b>\$strongPass</b></li> </ul>
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> <li>Use la lista de métodos por defecto</li> <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: <b>raduser</b> y la contraseña: <b>upass123</b> .

**Fuente:** Rúbrica de evaluación UNAD

- Para todos los dispositivos:

### Router 1 (R1)

R1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco  
^

% Invalid input detected at '^' marker.

R1(config)#\$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco  
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

^

% Invalid input detected at '^' marker.

**Nota:** Se observa que el “**algorithm-type Scrypt**” no está soportado en R1, por consiguiente, tampoco lo estará soportando en R2 y R3. Esto es debido al cargue de la respectiva imagen.

ALTERNATIVA para los routers 1, 2 y 3

enable secret cisco12345cisco  
username sadmin privilege 15 secret cisco12345cisco

R1(config)# enable secret cisco12345cisco  
R1(config)#username sadmin privilege 15 secret cisco12345cisco

### **Router 2 (R2)**

R2#config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)# enable secret cisco12345cisco  
R2(config)#username sadmin privilege 15 secret cisco12345cisco

### **Router 3 (R3)**

R3#config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R3(config)# enable secret cisco12345cisco  
R3(config)#username sadmin privilege 15 secret cisco12345cisco

### **Switch 1 (D1)**

D1#config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
D1(config)# enable algorithm-type SCRYPT secret cisco12345cisco  
D1(config)# \$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco  
D1(config)#

## **Switch 2 (D2)**

D2#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)# enable algorithm-type SCRYPT secret cisco12345cisco

D2(config)# \$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D2(config)#

## **Switch (A1)**

A1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

A1(config)# enable algorithm-type SCRYPT secret cisco12345cisco

A1(config)# \$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

A1(config)#

- Para todos los dispositivos, excepto R2

## **Router 1 (R1)**

R1(config)#aaa new-model

R1(config)#radius server RADIUS

R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

R1(config-radius-server)#key \$strongPass

R1(config-radius-server)#exit

R1(config)#aaa authentication login default group radius local

R1(config)#end

R1#

## **Router 3 (R3)**

R3(config)#aaa new-model

R3(config)#radius server RADIUS

R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

R3(config-radius-server)#key \$strongPass

R3(config-radius-server)#exit

R3(config)#aaa authentication login default group radius local

R3(config)#end

R3#

## **Switch 1 (D1)**

D1(config)#aaa new-model

D1(config)#radius server RADIUS

D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

```
D1(config-radius-server)#key $strongPass
D1(config-radius-server)#exit
D1(config)#aaa authentication login default group radius local
D1(config)#end
D1#
```

### **Switch 2 (D2)**

```
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $strongPass
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local
D2(config)#end
D2#
```

### **Switch (A1)**

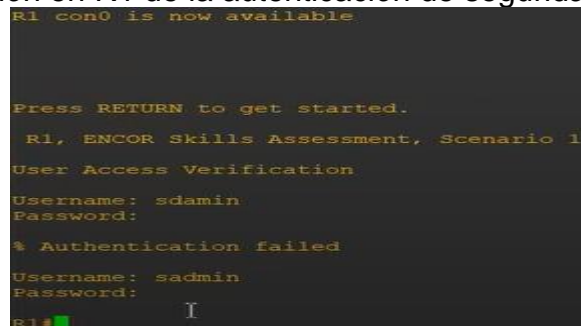
```
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)#key $strongPass
A1(config-radius-server)#exit
A1(config)#aaa authentication login default group radius local
A1(config)#end
A1#
```

### **Verificaciones**

**Nota:** En este punto no tengo acceso o habilitado las PCs.

- En R1

**Figura 24:** Verificación en R1 de la autenticación de seguridad



```
R1 con0 is now available

Press RETURN to get started.

R1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sdamin
Password:
% Authentication failed
Username: sadmin
Password:
R1#
```

**Fuente:** Autor

- En D1

**Figura 25:** Comprobación en D1 de la autenticación de la seguridad

```

D1, ENCOR Skills Assessment, Scenario 1
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: sadmin
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

D1>en
Password:
D1#

```

**Fuente:** Autor

Al realizar las configuraciones se observa que tanto R1 como D1 se encuentran en modo privilegiado

### **PARTE 6: Configure las funciones de Administración de Red**

En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

**Tabla 10:** Tareas a realizar de 6.1 a 6.2

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.

Tarea#	Tarea	Especificación
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>• Únicamente 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 <i>community string</i> en ENCORSA.</li> <li>• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.</li> <li>• En R1, habilite el envío de <i>traps bgp config</i> y <i>ospf</i>.</li> <li>• En A1, habilite el envío de <i>traps config</i>.</li> </ul>

**Fuente:** Rúbrica de evaluación UNAD

Para todos los dispositivos

- **En R1**

```
R1#clock set 13:00:00 29 October 2021
R1#
```

- **En R2**

```
R2#clock set 13:00:00 29 October 2021
R2#
```

- **En R3**

```
R3#clock set 13:00:00 29 October 2021
R3#
```

- **En D1**

```
D1#clock set 13:00:00 29 October 2021
D1#
```

- **En D2**

```
D2#clock set 13:00:00 29 October 2021
D2#
```

- **En A1**

```
A1#clock set 13:00:00 29 October 2021
A1#
```

### **Para el router 2 (R2)**

**Nota:** No es recomendable aplicar ntp master en GNS3 ya que los routers van a empezar a fallar, se volverán malucos de poder ejecutar cualquier tarea.

```
ntp master 3
end
```

### **Router 1 (R1)**

```
R1#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 2.2.2.2                     "Se configura ntp server en 2"
R1(config)#logging trap warning                   "Asignar límite de mensaje"
R1(config)#logging host 10.0.100.5
R1(config)#logging on
R1(config)#ip access-list standard SNMP-NMS      "Acceso a lista snmp-nms"
R1(config-std-nacl)#permit host 10.0.100.5      "Permiso de host"
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Cisco Student
R1(config)#snmp-server community ENCORSA ro SNMP-NMS
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)#snmp-server ifindex persist
R1(config)#snmp-server enable traps bgp          "Configuran traps BGP"
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf         "Configuran traps osps"
R1(config)#end                                    "Finalización"
R1#
```

### **Router 3 (R3)**

```
R3#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 10.0.10.1                  "Se configura ntp server"
R3(config)#logging trap warning                  "Asigna límite de mensaje"
R3(config)#logging host 10.0.100.5
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS      "Acceso a lista snmp-nms"
R3(config-std-nacl)#permit host 10.0.100.5      "Permiso de host"
R3(config-std-nacl)#exit
R3(config)#snmp-server contact Cisco Student
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf        "Configurar traps ospf"
R3(config)#end                                  "Finalización"
R3#
```

### **Switch 1 (D1)**

```
D1#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ntp server 10.0.10.1                  "Se configura ntp server"
D1(config)#logging trap warning                  "Asigna límite de mensaje"
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#ip access-list standard SNMP-NMS      "Acceso a lista snmp-nms"
D1(config-std-nacl)#permit host 10.0.100.5      "Permiso de host"
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco Student
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf        "Configurar traps ospf"
^
% Invalid input detected at '^' marker.

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

### **Switch 2 (D2)**

```

D2#config terminal                                "Ingreso a modo configuración"
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ntp server 10.0.11.1                  "Se configura ntp server"
D2(config)#logging trap warning                  "Asigna límite de mensaje"
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS      "Acceso a lista snmp-nms"
D2(config-std-nacl)#permit host 10.0.100.5     "Permiso de host"
D2(config-std-nacl)#exit
D2(config)#snmp-server contact Cisco Student
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server ifindex persist
D2(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.

D2(config)#snmp-server enable traps ospf        "Configurar traps ospf"
D2(config)#end                                  "Finalización"
D2#

```

Nota: Los routers están aceptando "config", mientras que los switches no están aceptando "config", es decir no están soportando los "traps config".

**Figura 26:** Verificación en D2 mediante "snmp-server enable traps ?"

```

D2(config)# snmp-server enable traps ?
auth-framework  Enable SNMP CISCO-AUTH-FRAMEWORK-MIB traps
bfd              Allow SNMP BFD traps
bgp             Enable BGP traps
bridge         Enable SNMP STP Bridge MIB traps
casa           Enable SNMP casa traps
cef            Enable SNMP CEF traps
dlsw          Enable SNMP dlsw traps
eigrp         Enable SNMP EIGRP traps
energywise     Enable SNMP ENERGYWISE traps
ether-oam      Enable SNMP ethernet oam traps
ethernet       Enable SNMP Ethernet traps
event-manager  Enable SNMP Embedded Event Manager traps
flowmon        Enable SNMP flowmon notifications
frame-relay    Enable SNMP frame-relay traps
hsrp           Enable SNMP HSRP traps
ike            Enable IKE traps
ipmulticast    Enable SNMP ipmulticast traps
ipsec          Enable IPsec traps
ipsla          Enable SNMP IP SLA traps
isis           Enable IS-IS traps
l2tun          Enable SNMP L2 tunnel protocol traps
mpls           Enable SNMP MPLS traps
msdp           Enable SNMP MSDP traps
mvpn           Enable Multicast Virtual Private Networks traps
ospf           Enable OSPF traps
pim            Enable SNMP PIM traps
pki            Enable SNMP PKI Traps
pw             Enable SNMP PW traps
rsvp           Enable RSVP flow change traps
slb            Enable SNMP SLB traps
snmp           Enable SNMP traps
stp           Enable SNMP STPX MIB traps
syslog         Enable SNMP syslog traps
tty            Enable TCP connection traps
vlancreate     Enable SNMP VLAN created traps
vlandelete     Enable SNMP VLAN deleted traps
vrfmib         Allow SNMP vrfmib traps

```

Fuente: Autor

## Switch A1

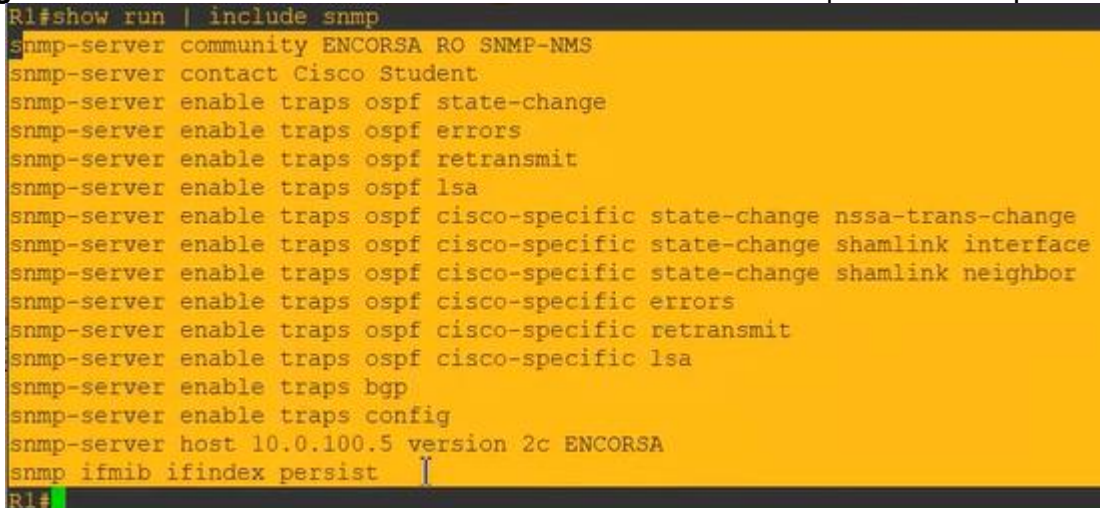
```
A1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#ntp server 10.0.10.1
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)#logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco Student
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server ifindex persist
A1(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.

A1(config)#end
A1#
```

Nota: Tampoco A1 está aceptando los “traps config”

## Verificaciones

**Figura 27:** Verificación en R1 mediante comando “show run | include snmp”



```
R1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-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 bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifindex ifindex persist
R1#
```

**Fuente:** Autor

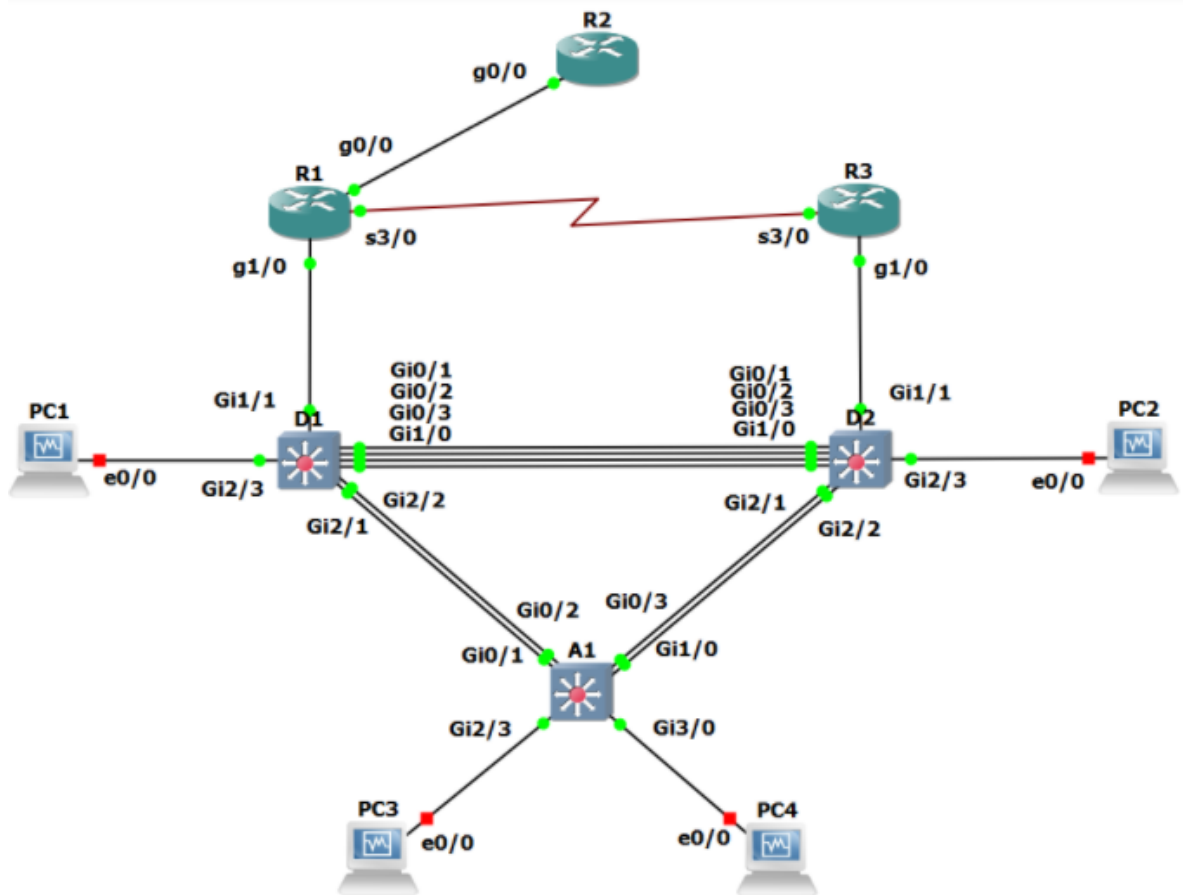
Se puede ver que todo está satisfactorio a excepción de que no aceptan los switches los “traps de config”.

**Figura 28:** Verificación en D1 mediante comando “show run | include snmp”

```
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-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 10.10.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
D1#
```

Fuente: Autor

**Figura 29:** Topología finalizada



Fuente: Autor

## CONCLUSIONES

En la realización del escenario de pruebas de habilidades se ha podido efectuar la construcción y conexión de los diferentes cables de red mediante la configuración básica de cada uno de los dispositivos. Además, se ha configurado y ejecutado la capa de red 2 que da soporte al Host, es decir, todos los switches han podido comunicarse y enlazarse entre sí, es por ello que las respectivas PC han recibido direccionamiento DHCP y SLAAC satisfactoriamente.

Mediante la configuración de protocolos de enrutamiento IPv4 e IPv6 y de la respectiva configuración HSRP versión 2 se logra proveer la redundancia de primer salto para los Host en la red de la compañía. Igualmente, se han configurado diferentes mecanismos de seguridad en los dispositivos de la topología asignándose nombres de usuario y las respectivas contraseñas. También, se ha configurado varias funciones de administración de red.

Hoy en día la importancia que tiene la administración de red radica en que se mejora la continuidad en la operación mediante mecanismos adecuados de control y monitoreo. Esto permite para las empresas el reducir costos por medio del control de gastos y de mejores mecanismos de cobro. El hacer la red más segura, permite que se vuelva imposible que personas ajenas a la compañía o empresa pueda extraer y entender la información que circula en ella.

Con la presentación de este trabajo se puede concluir que es bastante fundamental y sumamente necesario para un profesional de cualquier rama de la ingeniería (telecomunicaciones, electrónica, sistemas) el conocimiento y manejo de ciertas habilidades, capacidades y destrezas para el respectivo diagnóstico y configuración en lo relacionado con el manejo de redes de datos y así poder brindar solución a diferentes entornos que se nos pueda presentar.

En el desarrollo del diplomado y en especial para propósitos de este escenario se trabaja con el simulador GNS3 ya que el Packet Tracer no soporta algunos comandos y hace que se dificulte la realización y ejecución del ejercicio propuesto.

## BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced Spanning Tree. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Introduction to Automation Tools. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced OSPF. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). BGP. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced BGP. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multicast. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). QoS. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Services. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Signals and Modulation. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Infrastructure. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Understanding Wireless Roaming and Location Services. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCORA 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Troubleshooting Wireless Connectivity. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

Granados, G. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de <http://hdl.handle.net/10596/24167>

Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]. Recuperado de <https://repository.unad.edu.co/handle/10596/24419>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>