

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SANTIAGO ANDRÉS MEJÍA RAMÍREZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SANTIAGO ANDRÉS MEJÍA RAMÍREZ

Diplomado de opción de grado presentado para optar el título de INGENIERO
ELECTRÓNICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLÍN, 29 de noviembre de 2021

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESÚMEN	9
ABSTRACT	9
INTRODUCCIÓN	11
DESARROLLO	12
Escenario propuesto	12
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	12
Paso 1: Cablear la red como se muestra en la topología.	12
Paso 2: Configurar los parámetros básicos para cada dispositivo.....	13
Parte 2: Configurar la capa 2 de la red y el soporte de Host	23
Tarea 2.1 y tarea 2.2, configuración de enlaces troncales y Vlans	24
Tarea 2.3 - 2.4 - 2.5 y 2.6. Configuración de RSPVT,LACP y Hosts	26
Tarea 2.7 Verificación servicios DHCP IPV4	30
Tarea 2.8 Verificación conexiones LAN local.....	30
Parte 3: Configurar los protocolos de enrutamiento.....	33
Tarea 3.1 a 3.4. Configuraciones protocolos de enrutamiento OSPF,BGP,ISP.	35
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)	44
Tareas 4.1 - 4.3. Creación de IP SLA,HSRPv2.....	48
Parte 5: Seguridad	54
Tarea 5.1-5.2. Creación algoritmo de encriptación.	55
Tarea 5.3 -5.5. Configuración protocolo AAA y Radius.....	56
Parte 6: Configure las funciones de Administración de Red	62
Tarea 6.2 Configuración R2 como servidor NTP	63
Tarea 6.3 Configuración de NTP R1,R3 D1,D2 y A1	64
Tarea 6.4 Configuración del syslog.....	66
Enlace a archivos de simulación en GNS3	72

CONCLUSIONES73
BIBLIOGRAFÍA.....74

LISTA DE TABLAS

Tabla 1.Lista de tareas configuración de la red.	23
Tabla 2.Lista de tareas configuración protocolos de enrutamiento.	33
Tabla 3.Lista de tareas configuración redundancia primer salto.	44
Tabla 4.Lista de tareas configuración seguridad.....	54
Tabla 5.Lista de tareas configuración administración de la red	62

LISTA DE FIGURAS

Figura 1.Topología de red.....	12
Figura 2.Topología de red en GNS3.....	13
Figura 3.Verificación de configuración en D1	28
Figura 4. Verificación de configuración en D2	29
Figura 5.Verificación configuración en A1.....	29
Figura 6.Verificación asignación IP dinámicas en PC2 y PC3	30
Figura 7.Evidencia ping desde PC4.....	31
Figura 8 .Evidencia de ping desde PC1	31
Figura 9.Evidencia de ping desde PC2.....	32
Figura 10.Evidencia de ping desde PC3.....	32
Figura 11.Verificación protocolo enrutamiento en R1	37
Figura 12.Verificación BGP y tablas de enrutamiento en R1	38
Figura 13.Verificación protocolo enrutamiento en R2	39
Figura 14.Verificación protocolo enrutamiento en R3	40
Figura 15.Verificación protocolo enrutamiento en D1	42
Figura 16.Verificación protocolo enrutamiento en D2	43
Figura 17.Verificación configuración de SLA y HSRPv2 en D1	50
Figura 18.Verificación configuración de SLA y HSRPv2 en D2	53
Figura 19.Verificación algoritmo encriptación en R2.....	55
Figura 20.Verificación configuración de seguridad y login en R1.....	57
Figura 21.Verificación configuración de seguridad y login en R3	58
Figura 22.Verificación configuración de seguridad y login en D1	59
Figura 23.Verificación configuración de seguridad y login en D2	60
Figura 24.Verificación configuración de seguridad y login en A1.....	61
Figura 25.Configuración R2 como servidor NTP.....	63
Figura 26.Configuración R1 sincronizado a servidor R2.....	64
Figura 27.Configuración D1 sincronizado a servidor R1	64
Figura 28.Configuración A1 sincronizado a servidor R1	65
Figura 29.Configuración A1 sincronizado a servidor R1	65
Figura 30.Configuración D2 sincronizado a servidor R3.....	66
Figura 31.Verificación configuraciones Syslog y SNMP en R1.....	67
Figura 32.Verificación configuraciones Syslog y SNMP en R3.....	68
Figura 33.Verificación configuraciones Syslog y SNMP en D1	69
Figura 34.Verificación configuraciones Syslog y SNMP en D2.....	70
Figura 35.Verificación configuraciones Syslog y SNMP en A1	71
Figura 36.Topología de red final	72

GLOSARIO

BGP: Es el acrónimo en inglés de (Border Gateway Protocol), el cual consiste en el intercambio de información de enrutamiento entre sistemas autónomos.

DHCP: Acrónimo en inglés de (Dynamic Host Configuration Protocol) protocolo que consiste en la configuración dinámica de host en una red, por medio de un mecanismo conocido como cliente-servidor, con el fin de que dispositivo solicite y se le asigne la dirección IP de la red a la cual se encuentra conectado.

Enrutamiento: Proceso que permite determinar la mejor ruta desde cualquier segmento de red hasta el dispositivo final del destino.

NTP: Acrónimo en inglés de (Network Time Protocol, protocolo de hora de red), protocolo usado que permite definir y mantener la hora de la red, desde un dispositivo que se configura como maestro, para los demás dispositivos de la red.

Tabla de enrutamiento: Tabla donde se encuentra toda la información de enrutamiento para el envío de un paquete de datos y que permite determinar cual es la mejor ruta de acceso para llegar al destino final.

VLAN: Acrónimo de (Virtual Local Area Network), red de área local virtual, la cual es la subdivisión de una red local en redes virtuales o lógicas en un solo enlace físico.

RESÚMEN

En la actualidad el constante desarrollo de las tecnologías a nivel global, necesariamente están involucrados con el área de la electrónica y las redes de datos, donde se evidencia un crecimiento continuo en múltiples áreas, industrias y sectores económicos de la sociedad.

La siguiente prueba de habilidades Cisco CCNP plantea un escenario a pequeña escala de los elementos más comunes que están involucrados en la arquitectura de una red de datos y/o red de comunicaciones, esta prueba está compuesta por 6 pasos, que abarcan desde las configuraciones básicas hasta configuraciones de mayor nivel en los diferentes dispositivos, donde la aplicación de conceptos claros como enrutamiento y conmutación, son necesarios para comprender mejor el funcionamiento de cualquier red, adicional en la presente prueba, se configuran funciones muy útiles como VLANs, se configuran protocolos de enrutamiento, se configuran opciones de seguridad, también se configuran funciones básicas referentes al tema de la administración de una red y por último se configuran la sincronización de los routers y switches, también se emplean los diferentes comandos en los dispositivos que permiten evidenciar los estados de los diferentes puertos de los elementos, así como el estado de las diferentes configuraciones realizadas en los equipos así como pruebas de conectividad entre los equipos.

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

ABSTRACT

At present, the constant development of technologies at a global level, are necessarily involved with the area of electronics and data networks, where continuous growth is evidenced in multiple areas, industries and economic sectors of society.

The following Cisco CCNP skills test raises a small-scale scenario of the most common elements that are involved in the architecture of a data network and / or communications network, this test is composed of 6 steps, this test consists of 6 steps, ranging from basic configurations to higher-level configurations on the different devices, where the application of clear concepts such as routing and switching, are necessary to better understand the operation of any network, additional in this test, very useful functions such as VLANs are configured, routing protocols are configured, security issues are configured, also they configure basic functions related to the administration of a network and finally the synchronization of the routers and switches are configured, the different commands are also used in the devices that allow to show the states of the different ports of the elements,

as well as the status of the different configurations made in the equipment as well as connectivity tests with between the equipment.

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

INTRODUCCIÓN

El mundo actual se ha venido transformando evolucionando y se encuentra en una era digital, donde la tecnología hace una gran contribución a la transformación que se está presentando el mundo cuyo cambio mas característico se presenta en las formas y medios en como se comunican las personas, he aquí el protagonismo que tienen las redes de comunicación, siendo estas redes uno de los pilares fundamentales para el funcionamiento de muchas necesidades básicas y de servicios de toda la sociedad.

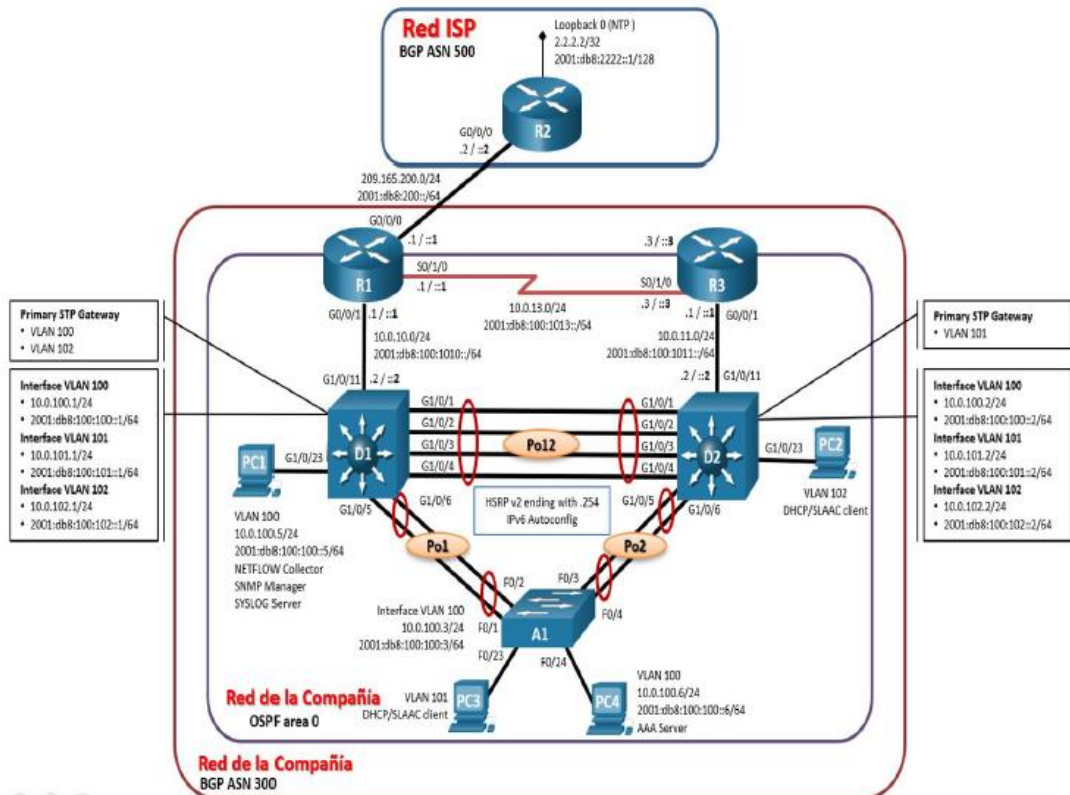
Las redes de comunicaciones han venido en constante crecimiento y desarrollo por lo que hoy en día existe la necesidad de formar muchos más profesionales en redes, que diseñen arquitecturas de red, de acuerdo a las necesidades y características de los clientes, que configuren equipos, con los diferentes protocolos para enrutamiento y envío de información, con las mejores características de seguridad para proteger la diferente información que circula por la red y con los mejores parámetros de calidad, para que desempeño de la red sea rápido y efectivo.

La prueba de habilidades CCNP Cisco está compuesta de 6 pasos, donde cada paso esta desglosado con cada actividad a realizar y con las diferentes instrucciones de configuración, así se le ofrece al estudiante y/o profesional en redes, todos los elementos para aprender, practicar e implementar los conocimientos básicos y avanzados en el diseño, configuración y administración de una red, esto con las diferentes herramientas propuestas de simulación, como Cisco Packet tracer y GNS3, las cuales ofrecen características muy avanzadas en materia de simulación y que le otorga al estudiante las herramientas necesarias para la configuración de dispositivos y monitoreo al tráfico de datos como si estuviese en un ambiente real de cualquier red.

DESARROLLO

Escenario propuesto

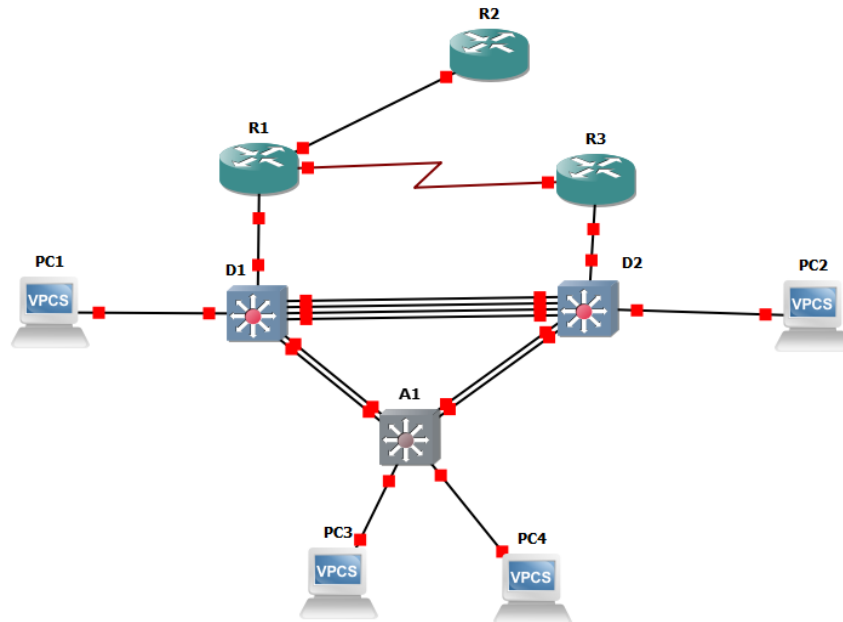
Figura 1. Topología de red



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.

Figura 2. Topología de red en GNS3



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Parámetros de configuración en dispositivos.

Configuración R1

```
R1#enab
R1#confi term
R1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#login synchronous
R1(config-line)#exit
```

```

R1(config)#interface g0/0
R1(config-if)#ip address 209.165.200.200.225 255.255.255.224
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#exit
R1(config)#interface g2/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100.1010::1/64
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#exit
R1(config)#interface s1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#

```

En la configuración anterior en el Router R1, se configuran los parámetros básicos del dispositivo, como el nombre del elemento, se crea mensaje de aviso, se configuran los puertos Giga ethernet y puerto serial, con sus respectivas direcciones IPV4 e IPV6.

Configuración R2

```

R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2,ENCOR Skills Assessment,Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exi

```

```
R2(config)#interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#exit
```

En la configuración anterior en el router R2, se configuran los parámetros básicos del dispositivo, como el nombre del elemento, se crea mensaje de aviso, se configuran los puertos Gigabitethernet , con sus respectivas direcciones IPV4 e IPV6 y máscara de la sub red.

Configuración R3

```
R3#enab
R3#confi term
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, Encor Skills Assessment , Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#login synchronous
R3(config-line)#exit
R3(config)#interface g2/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

En la configuración anterior en el Router R3, se configuran los parámetros básicos del dispositivo, como el nombre del elemento, se crea mensaje de aviso, se configuran los puertos Giga ethernet y puerto serial, con sus respectivas direcciones IPV4 e IPV6.

Configuración D1

```
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
```

```
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface e1/0
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
```



```

D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range e0/1-3
D1(config-if-range)#shutd
D1(config-if-range)#exit
D1(config-if-range)#exit
D1(config)#interface range e1/0
D1(config-if-range)#shutdo
D1(config-if-range)#
D1(config-if-range)#exit
D1(config)#interface range e1/1-3
D1(config-if-range)#shutdo
D1(config-if-range)#exit
D1(config-if-range)#exit
D1(config)#interface range e0/0
D1(config-if-range)#shutd
D1(config-if-range)#exit
D1(config)#
D1(config)#exit
D1#copy running-config startup-config
Destination filename [startup-config]?

```

En la configuración anterior en el switch D1, se configuran los parámetros básico del dispositivo, como el nombre del elemento , se crea mensaje de aviso, se configuran los puertos Giga ethernet con sus respectivas direcciones IPV4 e IPV6 y direcciones de la subred, también se habilitan y configuran las Vlan y sus nombres, se habilita la IP DHCP para la exclusión de un grupo de direcciones en un rango especificado, también se configura la puerta de enlace predeterminada para la conexión con su respectivo PC.

Configuración D2

```

D2#
D2#enab

```

```
D2#confi term
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface e1/0
D2(config-if)#no switchport
D2(config-if)#
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutd
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#
D2#
D2#ena
D2#confi term
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutd
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 101
D2(config-if)#
```

```
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutd
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 102
D2(config-if)#
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 shutd
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range e0/0-3
D2(config-if-range)#shutd
D2(config-if-range)#exit
D2(config)#
D2(config)#interface range e1/1-3
D2(config-if-range)#shutd
D2(config-if-range)#exit
D2(config-if-range)#exit
D2(config)#interface range e1/0
D2(config-if-range)#shutd
D2(config-if-range)#exit
D2(config)#
D2(config)#exit
D2#
D2#copy running-config startup-config
Destination filename [startup-config]?
```

En la configuración anterior en el switch D2, se configuran los parámetros básicos del dispositivo, como el nombre del elemento, se crea mensaje de aviso, se configuran los puertos Giga ethernet con sus respectivas direcciones IPv4 e IPv6 y direcciones de la subred, también se habilitan y configuran las Vlan y sus nombres, se habilita la IP DHCP para la exclusión de un grupo de direcciones en un rango especificado, también se configura la puerta de enlace predeterminada para la conexión con su respectivo PC. Además, se reasigna los respectivos puertos Giga por puertos Ethernet, debido a la disponibilidad de IOS de los switches empelados en la máquina virtual GNS3.

Configuración A1

```
A1#
A1#ena
A1#confi term
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#EXIT
A1(config)#interface vlan100
A1(config-if)#
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shudt
A1(config-if)#exit
A1(config-if)#exit
A1(config)#interface range e1/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
```

```
A1(config)#  
A1(config)#exit  
A1#copy running-config startup-config  
A1#
```

En la configuración anterior en el switch D2, se configuran los parámetros básicos del dispositivo, como el nombre del elemento, se crea mensaje de aviso, se configuran los puertos Giga ethernet con sus respectivas direcciones IPV4 e IPV6 y direcciones de la subred, también se habilitan y configuran las Vlan y sus nombres, se habilita la IP DHCP para la exclusión de un grupo de direcciones en un rango especificado, también se configura la puerta de enlace predeterminada para la conexión con su respectivo PC. Además, se reasigna los respectivos puertos Giga por puertos Ethernet, debido a la disponibilidad de IOS de los switches empelados en la máquina virtual GNS3.

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

En R1

```
R1#copy running-config startup-config
```

En R2

```
R2#copy running-config startup-config
```

En R3

```
R3#copy running-config startup-config
```

En D1

```
D1#copy running-config startup-config
```

En D2

```
D2 #copy running-config startup-config
```

En A1

```
A1 #copy running-config startup-config
```

Comandos para guardar la configuración de inicio en cada dispositivo.

- 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.

Parámetros para configuración de direcciones PC1 y PC4.

PC1

```
PC1> ip 10.0.100.5 10.0.100.254
```

```
Checking for duplicate address...
```

```
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
```

```
PC1> save
```

```
Saving startup configuration to startup.vpc
```

```
.done
```

PC4

```
PC4> ip 10.0.100.6 10.0.100.254
```

```
Checking for duplicate address...
```

```
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
```

```
PC4> save
```

```
Saving startup configuration to startup.vpc
```

```
. done
```

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

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

Las tareas de configuración son las siguientes:

Tabla 1. Lista de tareas configuración de la red.

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío

		(forwarding).
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"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Tarea 2.1 y tarea 2.2, configuración de enlaces troncales y Vlans

En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches, en todos los switches cambie la VLAN nativa en los enlaces troncales.

Habilite enlaces trunk 802.1Q entre:

D1 and D2

Comandos en D1 y D2

D1

D1#confi term

D1(config)#interf range e0/0-3

D1(config-if-range)#switchport trunk native vlan 999

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

D1(config-if-range)#end

D2

```
D2(config)#interf range e0/0-3
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#end
D2#
```

Los comandos anteriores se utilizan para configurar los enlaces troncales de los switches D1 y D2, en sus respectivos puertos E0, desde el rango 0 al 1, para cada switch.

D1 and A1

```
D1(config)#interface range e1/2-3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#exit
```

D2 and A1

```
D2(config)#
D2(config)#interface range e1/2-3
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)#exit
D2(config)#exit
D2#
```

Los comandos anteriores se configuran como enlaces tróncales para los puertos e1 rango 2-3 en los suiches D1 y D2, estos enlaces están conectados al switch A1.

A1

```
A1#
A1#enable
A1#confi term
A1(config)#interface range e0/0-3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
```

```
A1(config-if-range)#  
A1(config-if-range)#switchport trunk native vlan 999  
A1(config-if-range)#exit  
A1(config)#  
A1(config)#exit
```

Los comandos anteriores se configuran como enlaces tróncales para los puertos e1 rango 0-3 en el swtich A1, estos enlaces están conectados a los switches D1 y D2.

Tarea 2.3 - 2.4 - 2.5 y 2.6. Configuración de RSPVT,LACP y Hosts

Configuración en switch D1

```
D1(config)#spanning-tree mode rapid-pvst  
D1(config)#spanning-tree vlan 100,102 root primary  
D1(config)#spanning-tree vlan 101 root secondary  
D1(config)#  
D1(config)#exit  
D1#confi term  
D1(config)#interface range e0/0-3  
D1(config-if-range)#switchport mode trunk  
D1(config-if-range)#channel-group 12 mode active  
D1(config-if-range)#no shutdown  
D1(config-if-range)#  
D1(config)#interface range e1/2-3  
D1(config-if-range)#switchport mode trunk  
D1(config-if-range)#channel-group 1 mode active  
D1(config-if-range)#no shutdown  
D1(config-if-range)#  
D1(config)#  
D1(config)#interface e1/1  
D1(config-if)#switchport mode access  
D1(config-if)#switchport access vlan 100  
D1(config-if)#spanning-tree portfast  
D1(config-if)#no shutdown
```

En la configuración anterior en el switch D1, se habilitan el protocolo RSPT, se activan los puentes raíz primario y secundario, se crean y habilitan los LACP en los diferentes puertos según la topología de la red, también se crean los hosts para la conexión con los PC.

Configuración en switch D2

```
D2(config)#
```

```

D2(config)#interface range e0/0-3
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#
D2(config)#interface range e1/2-3
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#
D2(config-if-range)#exit
D2(config)#
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#
D2(config)#interface e1/1
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#

```

En la configuración anterior en el switch D2, se habilitan el protocolo RSPT, se activan los puentes raíz primario y secundario, se crean y habilitan los LACP en los diferentes puertos según la topología de la red, también se crean los hosts para la conexión con los PC.

Configuración en A1

```

A1#
A1#confi term
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/0-1
A1(config-if-range)#switchport mode trunk
A1(config-if-range)# switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range e0/2-3
A1(config-if-range)#switchport mode trunk
A1(config-if-range)# switchport trunk native vlan 999

```

```

A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#
A1(config-if-range)#no shutdown
A1(config-if-range)#
A1(config-if-range)#exit
A1(config)#interface range e1/0
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 101
A1(config-if-range)#spanning-tree portfast
A1(config-if-range)#exit
A1(config)#interface range e1/1
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 100
A1(config-if-range)#spanning-tree portfast
A1(config-if-range)#
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#
A1(config)#exit

```

En la configuración anterior en el switch A1, se habilitan el protocolo RSPT, se activan los puentes raíz primario y secundario, se crean y habilitan los LACP en los diferentes puertos según la topología de la red, también se crean los hosts para la conexión con los PC.

Figura 3.Verificación de configuración en D1

```

D1#show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Et0/0     on            802.1q         trunking     999
Et0/1     on            802.1q         trunking     999

Port      Vlans allowed on trunk
Et0/0     none
Et0/1     none

Port      Vlans allowed and active in management domain
Et0/0     none
Et0/1     none

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     none
Et0/1     none
D1#
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
D1#show run interface e1/1
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end

```

Figura 4. Verificación de configuración en D2

```
D2#show interface trunk
Port      Mode           Encapsulation  Status        Native vlan
Et0/0     on             802.1q         trunking      999
Et0/1     on             802.1q         trunking      999

Port      Vlans allowed on trunk
Et0/0     none
Et0/1     none

Port      Vlans allowed and active in management domain
Et0/0     none
Et0/1     none

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     none
Et0/1     none
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
spanning-tree portfast edge
D2#show run interface e1/1
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/1
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
end
```

Figura 5. Verificación configuración en A1

```
A1#
A1#show run interface e1/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/0
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end

A1#show run interface e1/1
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end

A1#show run interface e0/1
Building configuration...

Current configuration : 153 bytes
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
 channel-group 1 mode active
end

A1#show run interface e0/0
Building configuration...
```

Tarea 2.7 Verificación servicios DHCP IPV4

En PC2

```
PC2> ip dhcp
```

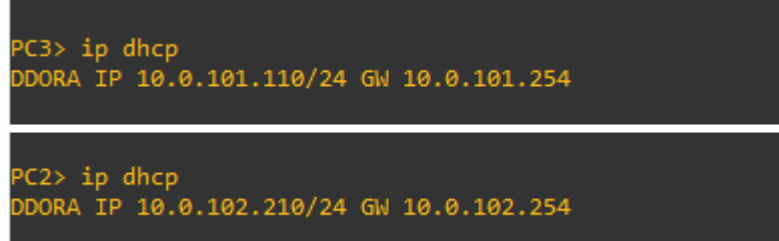
```
DDORA IP 10.0.102.210/24 GW 10.0.102.254
```

En PC3

```
PC3> ip dhcp
```

```
DDORA IP 10.0.101.110/24 GW 10.0.101.254
```

Figura 6.Verificación asignación IP dinámicas en PC2 y PC3



```
PC3> ip dhcp
DDORA IP 10.0.101.110/24 GW 10.0.101.254

PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254
```

Tarea 2.8 Verificación conexiones LAN local.

Verificación de comando ping desde cada Pc hacia los demás dispositivos.

Figura 7.Evidencia ping desde PC4

```
host (10.0.100.5) not reachable
PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> save
Saving startup configuration to startup.vpc
done
PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=1.555 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=1.103 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.921 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.778 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.246 ms

PC4> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=1.099 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.203 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.114 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.106 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.223 ms

PC4> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.657 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.162 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.299 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.491 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.534 ms

PC4>
```

Figura 8 .Evidencia de ping desde PC1

```
PC1> ping 10.0.100.6

84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.514 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=5.474 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.614 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=2.067 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.413 ms

PC1> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.715 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.794 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.752 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.673 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.622 ms

PC1> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=2.020 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.711 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.886 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.789 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.162 ms

PC1>
```

Figura 9.Evidencia de ping desde PC2

```
PC2>
PC2>
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.321 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.651 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=2.614 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.911 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.697 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.524 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.778 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.554 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=1.007 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.705 ms

PC2> █
```

Figura 10.Evidencia de ping desde PC3

```
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=2.353 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=2.479 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.796 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.880 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=4.100 ms

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=1.029 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=3.017 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=1.693 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=1.416 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=1.309 ms

PC3> █
```


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.

Las tareas de configuración son las siguientes:

Tabla 2. Lista de tareas configuración protocolos de enrutamiento

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.	Use OSPF Process ID 4 y asigne los siguientes router-IDs: <ul style="list-style-type: none">• R1: 0.0.4.1• R3: 0.0.4.3• D1: 0.0.4.131• D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. <ul style="list-style-type: none">• En R1, no publique la red R1 – R2.• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: <ul style="list-style-type: none">• D1: todas las interfaces excepto G1/0/11• D2: todas las interfaces excepto G1/0/11
3.2	En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID 6 y asigne los siguientes router-IDs: <ul style="list-style-type: none">• R1: 0.0.6.1• R3: 0.0.6.3• D1: 0.0.6.131• D2: 0.0.6.132

		<p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la “Red ISP”, configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128).

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

Tarea 3.1 a 3.4. Configuraciones protocolos de enrutamiento OSPF,BGP,ISP.

Configuración R1

R1(config)#router ospf 4

R1(config-router)#router-id 0.0.4.1

R1(config-router)#network 10.0.10.0 0.0.0.255 area 0

R1(config-router)#network 10.0.13.0 0.0.0.255 area 0

```
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface g2/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface s1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family
```

R1(config-router)#

Se configura en Router R1, OSPF para calcular las rutas más cortas en las áreas de la red, también se configura el protocolo BGP para compartir información de enrutamiento.

Figura 11.Verificación protocolo enrutamiento en R1

```
OR Skills Assesment, Scenario 1
R1#
R1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.1
  network 10.0.10.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
  default-information originate
R1#
R1#show ipv6 ospf interface brief
Interface      PID   Area          Intf ID   Cost   State  Nbrs F/C
Gi2/0          6     0              9         1     DR     0/0
Se1/0          6     0              5         64    DOWN  0/0
R1#
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#show run | section BGP
R1#
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
```

Figura 12.Verificación BGP y tablas de enrutamiento en R1

```

R1#show ip route | include 0|8
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
S       10.0.0.0/8 is directly connected, Null0
C       10.0.10.0/24 is directly connected, GigabitEthernet2/0
L       10.0.10.1/32 is directly connected, GigabitEthernet2/0
       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#
R1#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       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
S       2001:DB8:100::/48 [1/0]
       via Null0, directly connected
C       2001:DB8:100:1010::/64 [0/0]
       via GigabitEthernet2/0, directly connected
L       2001:DB8:100:1010::1/128 [0/0]
       via GigabitEthernet2/0, 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

```

Configuración en R2

```

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6

```

```
R2(config-router-af)#no neighbor 209.165.200.225 activate
```

```
R2(config-router-af)#neighbor 2001:db8:200::1 activate
```

```
R2(config-router-af)#network 2001:db8:2222::/128
```

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

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

```
R2(config-router)#exit
```

```
R2(config)#
```

```
R2(config)#exit
```

Se configura en Router R2, OSPF para calcular las rutas más cortas en las áreas de la red, también se configura el protocolo BGP para compartir información de enrutamiento.

Figura 13.Verificación protocolo enrutamiento en R2

```
*Nov 26 00:29:59.415: %LINEPROTO-5-UPDOWN: Line protocol on
R2#show run | section bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
    no neighbor 2001:DB8:200::1 activate
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network ::/0
    network 2001:DB8:2222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
R2#
```

Configuración en R3

```
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 g2/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#end

```

Se configura en Router R3, OSPF para calcular las rutas más cortas en las áreas de la red, también se configura el protocolo BGP para compartir información de enrutamiento.

Figura 14.Verificación protocolo enrutamiento en R3

```

R3#
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
R3#show ipv6 ospf interface brief
Interface      PID   Area          Intf ID    Cost   State Nbrs F/C
Gi2/0          6     0              9          1     DR    0/0
Se1/0          6     0              5          64    DOWN  0/0
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ip route ospf | begin gateway
R3#show ip route ospf | begin Gateway
Gateway of last resort is not set

R3#show ip route ospf
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 not set

R3#

```


Configuración en D1

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e1/0
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface e1/0
D1(config-rtr)#exit
D1(config)#interface e1/0
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#
```

Figura 15.Verificación protocolo enrutamiento en D1

```
D1#
D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/0
network 10.0.10.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
D1#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet1/0
D1#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Vl102      6   0         41       1    DOWN  0/0
Vl101      6   0         40       1    DOWN  0/0
Vl100      6   0         39       1    DR    0/0
Et1/0      6   0         37      10    DOWN  0/0
D1#
```

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

Configuración en 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 e1/0
D2(config-router)#exit
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface e1/0
D2(config-rtr)#exit
D2(config)#interface e1/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
```

```

D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#end

```

Figura 16.Verificación protocolo enrutamiento en D2

```

D2#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface Ethernet1/0
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.100.0 0.0.0.255 area 0
  network 10.0.101.0 0.0.0.255 area 0
  network 10.0.102.0 0.0.0.255 area 0
D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet1/0
D2#show ipv6 ospf interface brief

```

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Vl102	6	0	41	1	DR	0/0	
Vl101	6	0	40	1	DOWN	0/0	
Vl100	6	0	39	1	DOWN	0/0	
Et1/0	6	0	37	10	DOWN	0/0	

```

D2#

```

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

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

Las tareas de configuración son las siguientes:

Tabla 3. Lista de tareas configuración redundancia primer salto.

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none">• Use la SLA número 4 para IPv4.• Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</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">• Use el número de rastreo 4 para la IP SLA 4.• Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

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

		<ul style="list-style-type: none"> • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). <p>Rastree el objeto 6 y decremente en 60.</p>
--	--	---

	<p>En D2, configure HSRPv2.</p>	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p>
--	---------------------------------	--

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

Tareas 4.1 - 4.3. Creación de IP SLA,HSRPv2

Configuración D1

```
D1(config)#ip sla 4
```

```
D1(config-ip-sla)#icmp-echo 10.0.10.1
```

```
D1(config-ip-sla-echo)#frequency 5
```

```
D1(config-ip-sla-echo)#exit
```

```
D1(config)#ip sla 6
```

```
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::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
```

```
D1(config)#ip sla schedule 6 life forever start-time now
```

```
D1(config)#track 4 ip sla 4
```

```
D1(config-track)#delay down 10 up 15
```

```
D1(config-track)#track 6 ip sla 6
```



```
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
```

```

D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
D1(config-if)#exit

```

Se realiza configuración de servicios IP SLA para probar la disponibilidad de los puertos cada 5 segundos.

Para monitorear el tráfico de la red, se configura el protocolo HSRP con el comando standby para administrar redundancia en la red, siendo D1 el router primario para las Vlan 100 y 102.

Figura 17.Verificación configuración de SLA y HSRPv2 en D1

```

D1#
D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State  Active      Standby      Virtual IP
Vl100          104  90 P Active local      unknown     10.0.100.254
Vl100          106  90 P Active local      unknown     FE80::5:73FF:FEA0:6A
Vl101          114  40 P Init  unknown   unknown     10.0.101.254
Vl101          116  40 P Init  unknown   unknown     FE80::5:73FF:FEA0:74
Vl102          124  90 P Init  unknown   unknown     10.0.102.254
Vl102          126  90 P Init  unknown   unknown     FE80::5:73FF:FEA0:7E
D1#

```

Configuración D2

```
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#
```

```
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#
D2(config-if)##standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#
D2(config-if)#standby 126 preempt
```

```
D2(config-if)#
```

```
D2(config-if)#standby 126 track 6 decrement 60
```

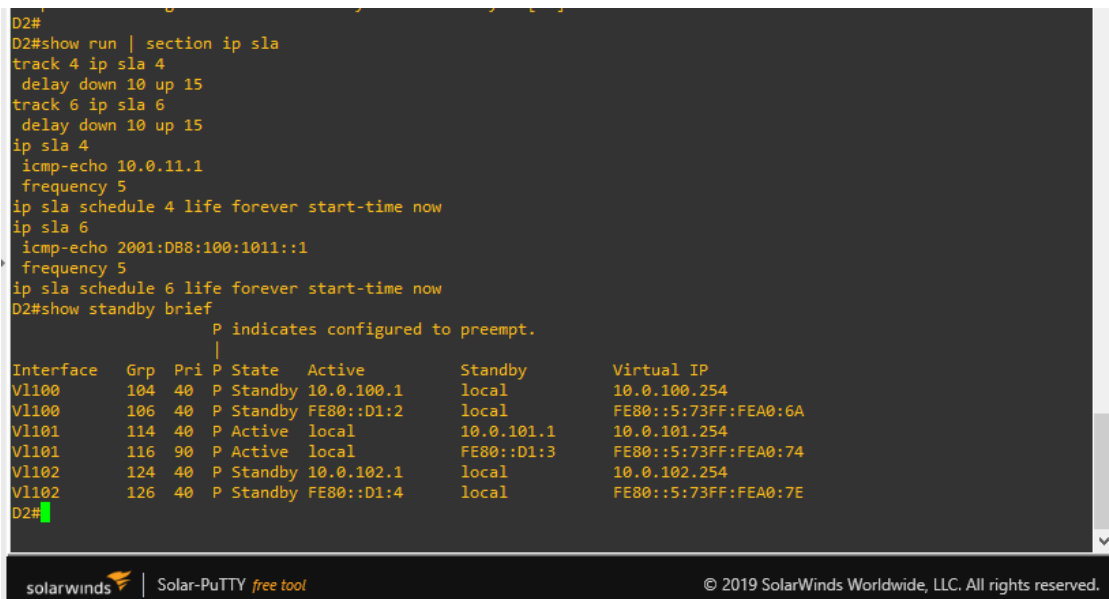
```
D2(config-if)#exit
```

Se realiza configuración de servicios IP SLA para probar la disponibilidad de los puertos cada 5 segundos.

Para monitorear el tráfico de la red, se configura el protocolo HSRP con el comando standby para administrar redundancia en la red, siendo D1 el router primario para las Vlan 100 y 102.

Figura 18.Verificación configuración de SLA y HSRPv2 en D2

```
D2#
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
D2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State  Active        Standby        Virtual IP
Vl100      104  40   P Standby 10.0.100.1    local          10.0.100.254
Vl100      106  40   P Standby FE80::D1:2    local          FE80::5:73FF:FEA0:6A
Vl101      114  40   P Active  local         10.0.101.1     10.0.101.254
Vl101      116  90   P Active  local         FE80::D1:3     FE80::5:73FF:FEA0:74
Vl102      124  40   P Standby 10.0.102.1    local          10.0.102.254
Vl102      126  40   P Standby FE80::D1:4    local          FE80::5:73FF:FEA0:7E
D2#
```



Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tabla 4. Lista de tareas configuración seguridad

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
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">• Nombre de usuario Local: sadmin• Nivel de privilegio 15• Contraseña: cisco12345cisco
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none">• Dirección IP del servidor RADIUS es 10.0.100.6.• Puertos UDP del servidor RADIUS son 1812 y 1813.• Contraseña: \$strongPass

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

Tarea 5.1-5.2. Creación algoritmo de encriptación.

Configuración Algoritmo seguridad en todos los dispositivos

Router R2

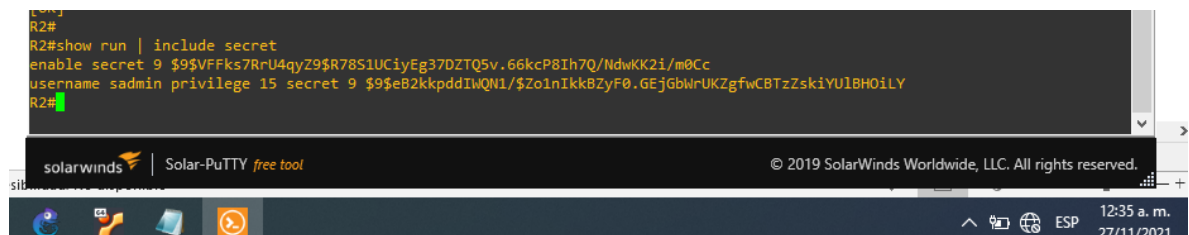
```
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
```

```
R2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
R2(config)#exit
```

Se configura algoritmo de encriptación, se crea usuario y contraseña y se protege con el enable algorithm-type scrypt secret.

Figura 19.Verificación algoritmo encriptación en R2.



Router R1

```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

```
R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
R1(config)#exit
```

Router R3

```
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
```

```
R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
R3(config)#exit
```

Switich D1

```
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

```
D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

```
D1(config)#exit
```

Switich D2

```
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
```

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

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

Switich A1

```
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

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

```
A1(config)#exit
```

Tarea 5.3 -5.5. Configuración protocolo AAA y Radius.

Router R1

```
R1#ena
```



```

R1#confi term
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)#key $trongPass
R1(config-radius-server)#exit
R1(config)#aaa authentication login default group radius local
R1(config)#end

```

Se configuran los métodos de autenticación en todos los dispositivos a excepción de R2, método AAA y Radius.

Figura 20.Verificación configuración de seguridad y login en R1.

```

*Nov 27 02:14:03.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed state to down
*Nov 27 02:14:03.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3, changed state to down R1,
ENCOR Skills Assesment, Scenario 1

User Access Verification
===
Username: sadmin
Password:

R1#show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$GB9oDSmDc2W/e4$MyKVXrDbAP3Wqy51Uaa9n/UwNBG.OgAkLxhlL1yEkFc
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $trongPass
aaa new-model
aaa session-id common

R1#show run | include secret
enable secret 9 $9$.Yx0jMhn58NYu9$j.2IwLI5xG7TXAfU73X/r1vHP0bUoRm.HS13035cngA
username sadmin privilege 15 secret 9 $9$GB9oDSmDc2W/e4$MyKVXrDbAP3Wqy51Uaa9n/UwNBG.OgAkLxhlL1yEkFc
R1#

```

Router R3

```

R3#ena
R3#confi term
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$4 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

```

Figura 6.3 Configuración R3 y Login de ingreso

Figura 21.Verificación configuración de seguridad y login en R3

```

*Nov 27 02:09:41.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial11/0, changed state to down
R3#
R3#show run | include secret
enable secret 9 $9$350/.Ysb9/kbVP$E80KkpTwbq4xJeeF62ZED31jtGktVjUPi9.JrindJ76
username sadmin privilege 15 secret 9 $9$dA3PyVZz/qos.Q$pJi98UqRREicXuwNwI0hSuWFMQ3mcz1YgoxkNRpJTCY
R3#show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$dA3PyVZz/qos.Q$pJi98UqRREicXuwNwI0hSuWFMQ3mcz1YgoxkNRpJTCY
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
R3#

```

```

Switch D1
D1#confi term
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$ 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

```

Figura 22.Verificación configuración de seguridad y login en D1

```
User Access Verification
Username: sadmin
Password:

*Nov 27 02:43:13.666: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
D1#
D1#
*Nov 27 02:43:22.990: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
D1#show run | include secret
enable secret 9 $9$lvrBDb.voKZP3y$wMl9NlrI3JycCzYccAqrBihrygOonmMPIEa5bweEJbU
username sadmin privilege 15 secret 9 $9$st1dtZRS/JXFTi$mBeHC9aFK.99zgZbpYCov6DVzM94NoBGRmDs2NTUklw
D1#show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$st1dtZRS/JXFTi$mBeHC9aFK.99zgZbpYCov6DVzM94NoBGRmDs2NTUklw
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common

D1#
```

Switch D2

```
D2#ena
```

```
D2#confi term
```

```
D2(config)#aaa new-model
```

```
D2(config)#radius server RADIUS
```

```
D2(config-radius-server)#$4 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
```

Figura 23.Verificación configuración de seguridad y login en D2

```
User Access Verification
Username: sadmin
Password:

*Nov 27 02:45:20.257: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Speak -> Standby
*Nov 27 02:45:20.578: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Standby -> Active
*Nov 27 02:45:21.331: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
*Nov 27 02:45:22.515: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby
*Nov 27 02:45:31.714: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Speak -> Standby
D2#
*Nov 27 02:45:41.006: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby
D2#show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$2DzW.30Zn49yfy$VADU1REKdauqiFNWhEw7K5njNH6jFB0voRCKEwC0.u.
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common

D2#show run | include secret
enable secret 9 $9$xZHSFitoLjhJDS$q3ApJDgTyz8g750h.jopKVtCkDFamAEA.Ab.aKTKWxk
username sadmin privilege 15 secret 9 $9$2DzW.30Zn49yfy$VADU1REKdauqiFNWhEw7K5njNH6jFB0voRCKEwC0.u.
D2#
```

Switch A1

```
A1#confi term
```

```
A1(config)#aaa new-model
```

```
A1(config)#radius server RADIUS
```

```
A1(config-radius-server)#$4 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
```

Figura 24.Verificación configuración de seguridad y login en A1

```
A1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
A1#show run | include secret
enable secret 9 $9$LKeuQ450utQZVS$t5agtrSEnqiMDaHZZsae7IQ9IvG2808iezxIoIMjL0c
username sadmin privilege 15 secret 9 $9$3MqvIY3gpd60PS$7musptHL5FDLnml6ZvE7ogR2XZ1ERkhgwLepXIQAHW.
A1#show run aaa | exclude!
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$3MqvIY3gpd60PS$7musptHL5FDLnml6ZvE7ogR2XZ1ERkhgwLepXIQAHW.
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $trongPass
aaa new-model
aaa session-id common
A1#
```

Parte 6: Configure las funciones de Administración de Red
 En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

Tabla 5. Lista de tareas configuración administración de la red

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

		<ul style="list-style-type: none">• En A1, habilite el envío de <i>traps config</i>.
--	--	--

Tarea 6.2 Configuración R2 como servidor NTP

R2#ena

R2#confi term

R2(config)#ntp master 3

R2(config)#end

R2#

Luego de ajustar la hora en R2, se configura como servidor NTP y los dispositivos que se configuren con NTP y la dirección 2.2.2.2 se sincronizarán a R2.

Figura 25. Configuración R2 como servidor NTP

```
R2(config)#exit
R2#show run | include ntp
*Nov 29 02:03:36.675: %SYS-5-CONFIG_I: Configured from console by console
R2#show run | include ntp
ntp master 3
R2#show ntp status | include stratum
Clock is unsynchronized, stratum 3, reference is 127.127.1.1
R2#
```

Tarea 6.3 Configuración de NTP R1,R3 D1,D2 y A1 Comandos para la sincronización de R1 con R2

En R1

```
R1#ena
```

```
R1#confi term
```

```
R1(config)#ntp server 2.2.2.2
```

```
R1(config)#
```

R1 se sincronizará a R2.

Figura 26.Configuración R1 sincronizado a servidor R2

```
Username: sadmin
Password:

R1#show ntp status | include stratum
Clock is synchronized, stratum 4, reference is 2.2.2.2
R1#show run | include ntp
ntp server 2.2.2.2
R1#
```

Comandos para sincronización de D1,A1 y R3 con R1

En D1

```
D1#ena
```

```
D1#confi term
```

```
D1(config)#ntp server 10.0.10.1
```

```
D1(config)#exit
```

Figura 27.Configuración D1 sincronizado a servidor R1

```
ntp server 10.0.10.1
D1#show run | include ntp
ntp server 10.0.10.1
D1#show ntp status | include stratum
Clock is unsynchronized, stratum 16, no reference clock
D1#
```

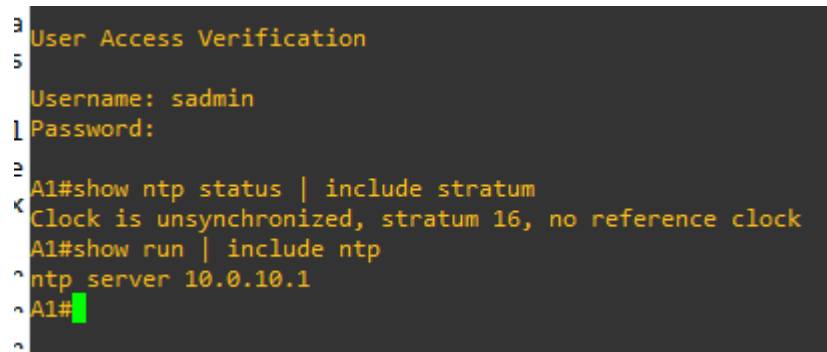
En A1

```
A1#ena
```



```
A1#confi term
A1(config)
#ntp server 10.0.10.1
A1(config)#exit
```

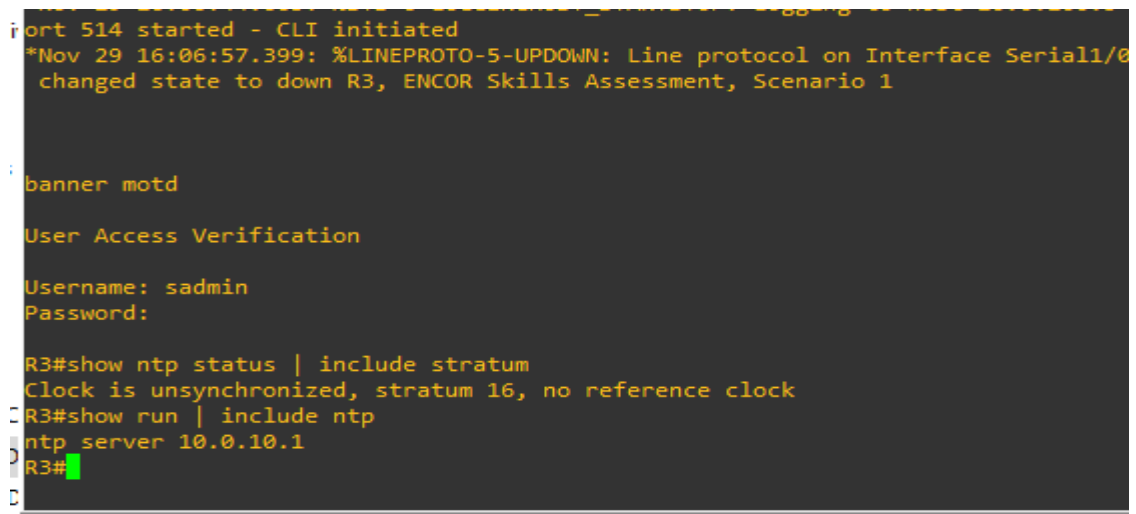
Figura 28. Configuración A1 sincronizado a servidor R1



```
3 User Access Verification
5
Username: sadmin
| Password:
3
A1#show ntp status | include stratum
Clock is unsynchronized, stratum 16, no reference clock
A1#show run | include ntp
ntp server 10.0.10.1
A1#
```

```
En R3
R3#ena
R3#confi term
R3(config)#ntp server 10.0.10.1
R3(config)#exit
```

Figura 29. Configuración A1 sincronizado a servidor R1



```
port 514 started - CLI initiated
*Nov 29 16:06:57.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0
changed state to down R3, ENCOR Skills Assessment, Scenario 1
:
: banner motd
:
: User Access Verification
:
: Username: sadmin
: Password:
:
: R3#show ntp status | include stratum
: Clock is unsynchronized, stratum 16, no reference clock
: R3#show run | include ntp
: ntp server 10.0.10.1
: R3#
```

Comandos para sincronización de D2 con R3

En D2

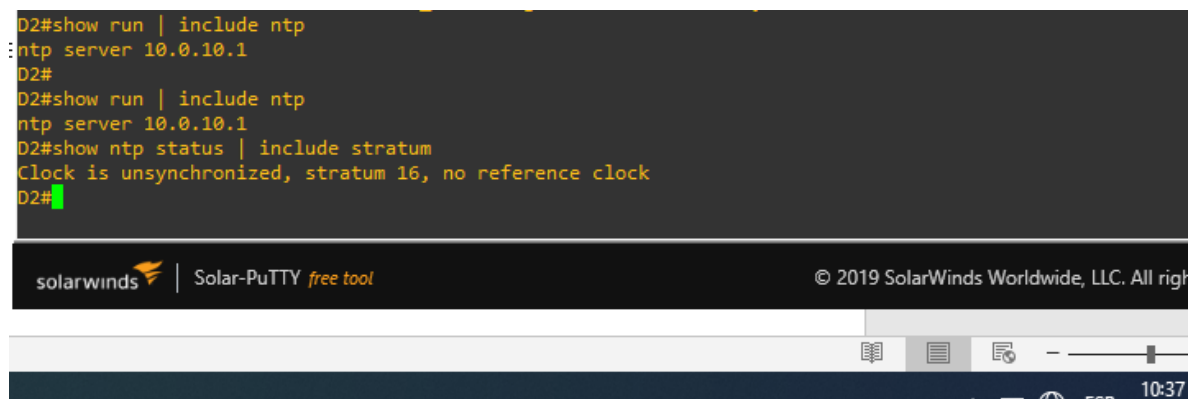
D2#ena

D2#confi term

D2(config)#ntp server 10.0.11.1

D2(config)#exit

Figura 30. Configuración D2 sincronizado a servidor R3



```
D2#show run | include ntp
ntp server 10.0.10.1
D2#
D2#show run | include ntp
ntp server 10.0.10.1
D2#show ntp status | include stratum
Clock is unsynchronized, stratum 16, no reference clock
D2#
```

The screenshot shows a terminal window with a dark background and yellow text. The text displays the configuration of the ntp server and the status of the clock. The terminal window has a title bar with the SolarWinds logo and the text "Solar-PuTTY free tool". The bottom right corner of the window shows the time "10:37".

Tarea 6.4 Configuración del syslog

En R1

R1(config)#logging trap warning

R1(config)#logging host 10.0.100.5

R1(config)#logging on

R1(config)#ip access-list standard SNMP-NMS

R1(config-std-nacl)#permit host 10.0.100.5

R1(config-std-nacl)#exit

R1(config)#snmp-server contact Cisco student

R1(config)#snmp-server community ENCORSA ro SNMP-NMS

R1(config)#snmp-server host 10.0.10.5 version 2c ENCORSA

R1(config)#snmp-server ifindex persist

```
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#exit
```

Se habilitan servicio de envío de mensajes y de advertencias, también se configura acceso a las listas snmp.

Figura 31.Verificación configuraciones Syslog y SNMP en R1

```
R1#
R1#show run | include logging
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
R1#
R1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
10 permit 10.0.100.5
R1#
R1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
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 entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.10.5 version 2c ENCORSA
R1#
```

En R3

```
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
```

```

R3(config-std-nacl)#exit
R3(config)#snmp-server contact Cisco student
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
R3(config)#snmp-server host 10.0.10.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#exit

```

Figura 32.Verificación configuraciones Syslog y SNMP en R3

```

[OK]
R3#
R3#show run | include logging
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
R3#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
R3#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
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 entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.10.5 version 2c ENCORSA
R3#

```

```

D1
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#

```

```

D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Santiago Mejia
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server host 10.0.10.5 version 2c ENCORSA
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config)#exit

```

Figura 33.Verificación configuraciones Syslog y SNMP en D1

```

D1#show run | include ntp
ntp server 10.0.10.1
D1#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
10 permit 10.0.100.5
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Santiago Mejia
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.10.5 version 2c ENCORSA
snmp ifmib ifindex persist
D1#

```

D2

D2#ena

D2#confi term

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

D2(config)#logging trap warning

D2(config)#logging host 10.0.100.5

D2(config)#logging on

D2(config)#ip access-list standard SNMP-NMS

D2(config-std-nacl)#permit host 10.0.100.5

D2(config-std-nacl)#exit

D2(config)#snmp-server contact Santiago Mejia

D2(config)#snmp-server community ENCORSA ro SNMP-NMS

D2(config)#snmp-server host 10.0.10.5 version 2c ENCORSA

D2(config)#snmp-server ifindex persist

D2(config)#snmp-server enable traps config

D2(config)#snmp-server enable traps ospf

D2(config)#exit

Figura 34. Verificación configuraciones Syslog y SNMP en D2

```
D2#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
D2#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D2#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Santiago Mejia
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.10.5 version 2c ENCORSA
snmp ifmib ifindex persist
D2#
D2#
```

```

A1
A1#ena
A1#confi term
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 10.0.10.5 version 2c ENCORSA
A1(config)#snmp-server ifindex persist
A1(config)#snmp-server enable traps config
A1(config)#snmp-server enable traps ospf

```

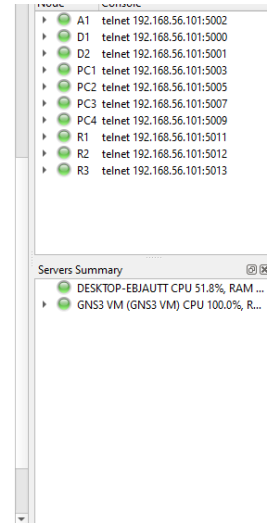
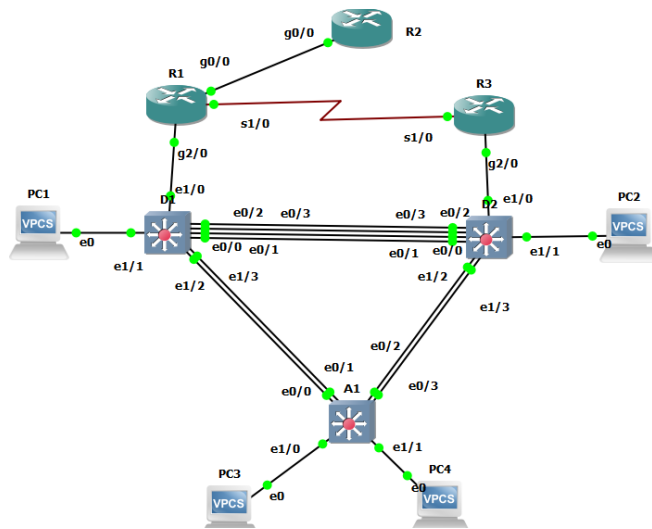
Figura 35.Verificación configuraciones Syslog y SNMP en A1

```

Building configuration...
Compressed configuration from 4028 bytes to 2141 bytes[OK]
A1#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
A1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
A1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Santiago Mejia
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.10.5 version 2c ENCORSA
snmp ifmib ifindex persist
A1#

```

Figura 36. Topología de red final



Enlace a archivos de simulación en GNS3

<https://drive.google.com/file/d/1wMrfJ5nnow4SeeohtaVxgF0nN0t8sOpU/view?usp=sharing>

CONCLUSIONES

El uso del software de simulación de redes GNS3 implementado por medio de una máquina virtual, le otorga al estudiante unas herramientas de simulación muy completas, que le permiten un mayor acercamiento al escenario real de una red, con lo cual es posible realizar análisis y monitoreo de las principales características que debe tener una red para su óptimo funcionamiento.

El desarrollo de la presente prueba de habilidades prácticas le permitió al estudiante desarrollar habilidades y conocimientos con las cuales puede, diseñar, implementar, programar y administrar una red, esto debido al escenario propuesto, que abarca desde las configuraciones básicas de los dispositivos hasta configuraciones de mucha mayor jerarquía y dificultad.

La prueba de habilidades prácticas CCNP se convierte en un escenario ideal para que los profesionales en las áreas de electrónica, telecomunicaciones y sistemas logren poner en práctica todos los conocimientos adquiridos durante su etapa académica y que luego estos conocimientos sirvan como una base sólida para enfrentarse a los retos que se presenta en el mundo real de las redes.

El alto crecimiento y presencia de las redes en muchos lugares, hace indispensable que existan profesionales certificados y capacitados para asumir el rol de administradores y/o arquitectos de red, que tengan las capacidades para administrar y crear redes seguras y con altos estándares de calidad y de rendimiento, ya que hoy en día estas características son esenciales para garantizar la velocidad, confiabilidad y confidencialidad de la red.

BIBLIOGRAFÍA

CISCO. Principios de Enrutamiento y Conmutación: Conceptos de Routing. {Sitio web}. {27 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. Principios de Enrutamiento y Conmutación: Configuración y conceptos básicos de Switching. {En línea}. {27 octubre de 2021}. Disponible en: <https://staticcourseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. Principios de Enrutamiento y Conmutación: Enrutamiento entre VLANS. {En línea}. {28 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. Principios de Enrutamiento y Conmutación: Enrutamiento Estático. {En línea}. {28 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

CISCO. Principios de Enrutamiento y Conmutación: VLANS. {En línea}. {28 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. Fundamentos de Networking: Asignación de direcciones IP. {En línea}. {30 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. Fundamentos de Networking: Soluciones de red. {En línea}. {30 octubre de 2021}. Disponible en: <https://static-courseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

