

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RAÚL SEGUNDO OLMOS CHAMORRO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RAÚL SEGUNDO OLMOS CHAMORRO

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
COROZAL
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Corozal, 27 de noviembre de 2021

AGRADECIMIENTOS

Aprovecho esta oportunidad que me ha dado la UNAD para profundizar mis conocimientos en redes. Muy agradecido a nuestro Docente de Diplomado CCNP Héctor Julián Parra por su esmero en la explicación de los protocolos de redes, agradeciendo también la guía de nuestro Director de Diplomado CCNP Gerardo Granados Acuña.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCION.....	10
DESARROLLLO.....	11
ESCENARIO.....	11
CONCLUSIONES.....	62
BIBLIOGRAFIA.....	63

LISTA DE TABLAS

Tabla 1. Enrutamiento de escenario propuesto.....	12
Tabla 2. Enrutamiento de escenario simulado en GNS3.....	14
Tabla 3. Tarea 2. Configurar la capa 2 de la red y el soporte de Host.....	22
Tabla 4. Tarea 3. Configurar los protocolos de enrutamiento.....	32
Tabla 5. Tarea 4. Configurar redundancia del primer salto.....	42
Tabla 6. Tarea 5. Seguridad.....	54
Tabla 7. Tarea 6. Configurar funciones de administración de red.....	57

LISTA DE FIGURAS

Figura 1. Escenario propuesto	11
Figura 2. Pantallazo escenario simulado en GNS3.....	13
Figura 3. Pantallazo de carga de comandos en D1.....	18
Figura 4. Pantallazo comando copy running-config startup-config en R1.....	21
Figura 5. Pantallazo de configuración de dirección IP en PC1.....	22
Figura 6. Pantallazo de comando Show interfaces trunk en D1.....	25
Figura 7. Pantallazo de comando Show interfaces trunk en D2.....	25
Figura 8. Pantallazo de comando Show interfaces trunk en A1.....	26
Figura 9. Pantallazo de comando Show Etherchannel summary en D2.....	27
Figura10. Pantallazo PC3 recibiendo dirección IPV4 válida.....	29
Figura 11. Pantallazo de ping entre PC1 y D1,D2, PC4.....	30
Figura 12. Pantallazo de ping entre PC2 y los switches D1, D2.....	30
Figura 13. Pantallazo de ping entre PC3 y los swiches D1 y D2.....	31
Figura 14. Pantallazo de ping entre PC4 y los switches D1, D2 y el PC1.....	31
Figura 15. Pantallazo comando show ip ospf interface en R1.....	35
Figura 16. Pantallazo de comando show bgp ipv4 / ipv6 unicast R1.....	41
Figura 17. Pantallazo de comando show ip sla summary en D1.....	47
Figura 18. Pantallazo de comando show standby all D1.....	51
Figura 19. Pantallazo de comando show standby all D2.....	53
Figura 19. Pantallazo de acceso a R1, solicitando username y password.....	56
Figura 20. Pantallazo de comando show ntp associations	59
Figura 21. Pantallazo de comando show logging en R1.....	60

GLOSARIO

STP: El Spanning Tree Protocol (STP) protege los dominios de broadcast de la capa 2 contra las tormentas de broadcast selectivamente fijando los links al modo de reserva para prevenir los loops. En el modo de reserva, estos links paran temporalmente el transferir de los datos del usuario. Después de que los cambios de la topología, para hacer la Transferencia de datos posible, los links se reactiven automáticamente.

STP rápido (RSTP): Detecta las topologías de red para proporcionar una convergencia más rápida de atravesar - árbol. Esto es la más eficaz cuando la topología de red árbol-se estructura naturalmente, y por lo tanto más rápidamente la convergencia pudo ser posible. El RSTP se habilita por abandono.

HSRP: El primer objetivo de HSRP es dar una trayectoria de salida completamente redundante. Comúnmente, las computadoras no tienen la capacidad de recopilar e intercambiar información de ruteo. La dirección IP del gateway predeterminado se configura estáticamente en un PC y, si el router del gateway se desactiva, el PC pierde la conectividad con cualquier dispositivo más allá de su segmento de red local. Este es el caso incluso si existe un gateway alternativo. Por esta razón el protocolo HSRP fue diseñado para hacer redundante la red.

Router: Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. El router actuará como distribuidor, seleccionado la mejor ruta de desplazamiento de la información para que la reciba rápidamente.

Conmutadores (switches): Los switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

Border Gateway Protocol (BGP): Es un protocolo de gateway exterior que permite que los Sistemas Autónomos intercambien información de ruteo entre sí. Un sistema autónomo es un conjunto de routers bajo sola administración técnica.

RESUMEN

En esta prueba de habilidades prácticas de CCNP, mediante un escenario propuesto, en la cual una compañía va a instalar una red de comunicación, profundizando con la práctica nuestros conocimientos. Esta compañía nos exige la conexión de la tipología de red de acuerdo al esquema propuesto, realizar la conectividad entre routers, switches capa 2 y 3 y los 4 computadores. La compañía nos pide que conectemos los equipos con redes IPV4 e IPV6, aplicando protocolos tales como (Rapid Spanning Tree), OSPF, BGP, HSRP, además de asegurar el acceso a la red, para proteger la compañía de accesos no permitidos. Esto acompañado de un monitoreo continuo de la red, para que en caso de falla de un dispositivo sea redundante y mantenga la comunicación.

Palabras Claves: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

ABSTRACT

In this CCNP practical skills test, through a proposed scenario, in which a company is going to install a communication network, deepening our knowledge with practice. This company requires us to connect the end of the network according to the proposed scheme, it performs the connectivity between routers, layer 2 and 3 switches and the 4 computers. The company asks us to connect the equipment with IPV4 and IPV6 networks, applying protocols such as (Rapid Spanning Tree), OSPF, BGP, HSRP, in addition to ensuring access to the network, to protect the company from unauthorized access. This is accompanied by continuous monitoring of the network, so that in the event of a device failure it is redundant and maintains communication.

Keywords: CISCO, CCNP, ROUTING, SWITCHING, NETWORKING, ELECTRONICS.

INTRODUCCIÓN

La comunicación hace de nosotros los seres humanos una característica especial, que nos ayuda a la supervivencia. Hoy en día, gracias a la tecnología estamos conectados, tenemos información de primera mano, podemos analizar datos rápidamente y tomar decisiones triviales e importantes. Es donde los medios de comunicación y sus protocolos cumplen un papel determinante en el desarrollo de la humanidad. En vista de lo anterior, es importante el conocimiento en CCNP, donde aprendemos a diseñar e instalar redes con aplicaciones diversas de protocolos de comunicación y seguridad.

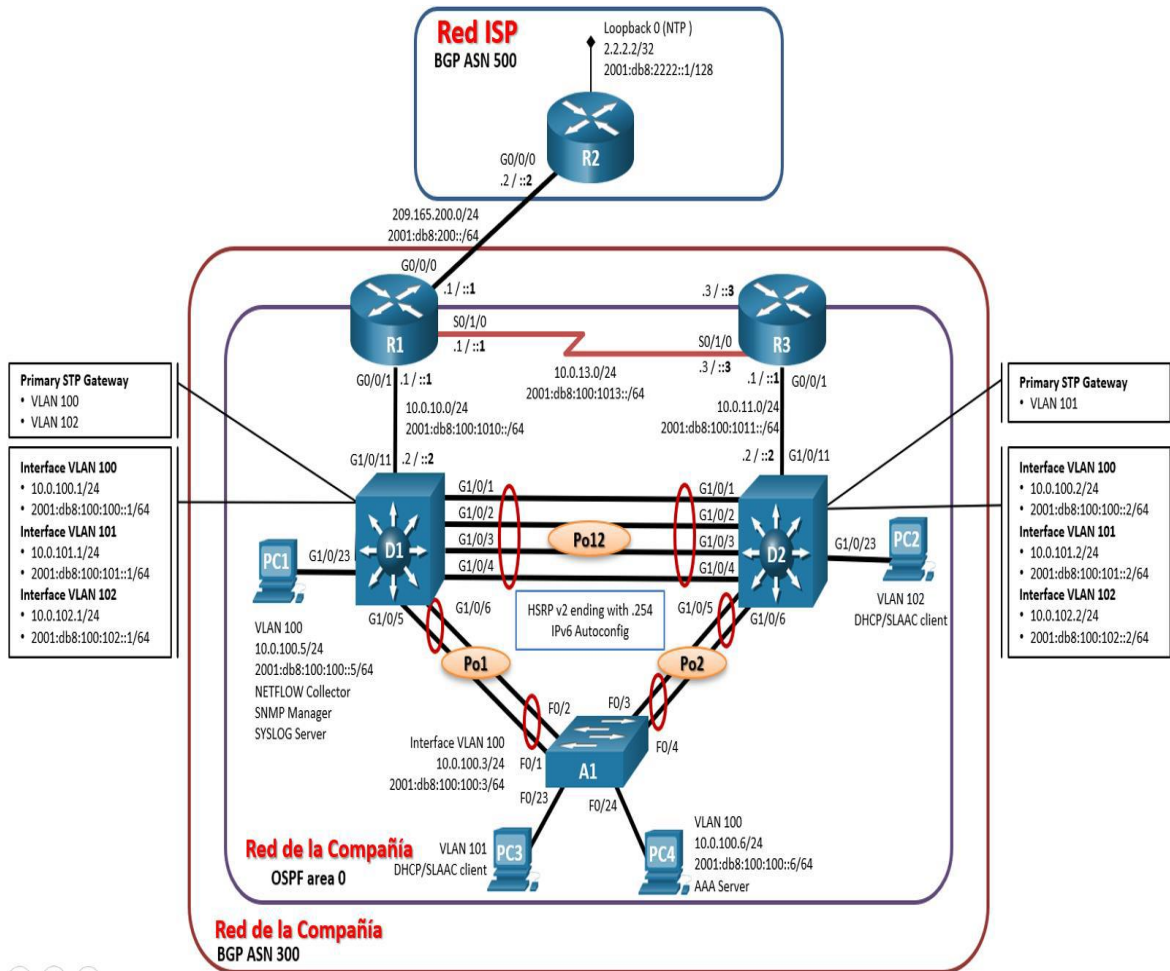
Esta prueba de habilidades se compone de 6 partes, desarrolladas todas en su totalidad en el simulador GNS3 versión 2.2.26 en máquina virtual. En la primera parte construimos la red, los parámetros básicos y direccionamiento de interfaces. En la segunda parte configuramos la capa 2 de la red, usando el protocolo RSPT, creando enlaces troncales y la configuración de puertos Etherchannel LACP. En el tercer punto configuramos el enrutamiento de las direcciones en IPV4 y también en IPV6 en protocolos OSPFv2, OSPFv3 y MP-BGP.

En el punto cuatro configuramos en la red, la redundancia del primer salto, en la cual creamos el HSRP versión 2. En la quinta parte configuramos varios mecanismos de seguridad, usando el SCRYPT y los métodos de autenticación AAA. Y por último, en la sexta parte de esta prueba de habilidades, configuramos funciones de administración de red, tal como sincronización de los relojes mediante la aplicación NTP, mensajes de advertencia aplicando el Syslog y configurando el SNMPv2c. En vista de lo explicado anteriormente, esta prueba de habilidades afianza nuestros conocimientos en CCNP.

DESARROLLO

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

Figura 1. Escenario propuesto



ESCENARIO

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (Default Gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Este ejercicio se realiza en un simulador GNS3 versión 2.2.26, con máquina virtual, en el simulador homologamos los recursos requeridos por la guía original.

Los recursos requeridos para realizar a cabalidad el proyecto en el simulador son los siguientes:

3 routers (R1, R2 Y R3) Cisco 7200 con imagen IOS i86bi_linux-adventerprisek9-ms.154-3.S.bin

2 switches (D1 y D2) con imagen IOU i86bi_linux_l2-adventerprisek9-ms.high_iron_20160628.bin

1 switch (A1) con imagen i86bi-linux-l2-adventerprisek9-15.2d.bin

4 computadores.

Cables de consola y cables de Ethernet para la interconexión como muestra la topología.

Tabla 1. Enrutamiento de escenario propuesto

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:

	100			1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Figura 2. Pantallazo escenario simulado en GNS3

The screenshot shows a GNS3 simulation window titled 'Escenario1 - GNS3'. The main area displays a network topology with three routers (R1, R2, R3) and a central switch (A1). R1 is connected to R2 and R3. R1 is also connected to PC1 and PC2. R3 is connected to PC3 and PC4. A1 is connected to R1, R2, R3, PC3, and PC4. The interface connections are labeled as follows: R1 (e0/0, s1/0, e0/1, e1/2, e2/0, e2/1), R2 (e0/0, s1/0), R3 (e0/1, e1/2, e2/0, e2/1), A1 (e1/2, e2/0, e2/1, e2/2), PC1 (e0), PC2 (e0), PC3 (e0), and PC4 (e0).

convención de interfaces

Dispositivo	Interfaz escenario	Interfaz simulador
R1	Loopback0	E0/0
	Loopback1	E0/1
	Loopback2	S1/0
R2	Loopback0	E0/0
	Loopback1	E0/1
R3	Loopback0	E0/1
	Loopback1	S1/0
	Loopback2	G1/0/11
D1	VLAN 100	VLAN 100
	VLAN 101	VLAN 101
	VLAN 102	VLAN 102
	VLAN 103	E2/0
D2	VLAN 100	VLAN 100
	VLAN 101	VLAN 101
	VLAN 102	VLAN 102
	VLAN 103	VLAN 103
A1	VLAN 100	VLAN 100
	NIC	NIC
	NIC	NIC
	NIC	NIC

Console

=> You have unsaved preferences in IOU Devices.
Continue without saving?

1 warning

Tabla 2. Enrutamiento de escenario simulado en GNS3

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E2/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E2/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

El siguiente paso es cargar las configuraciones a cada uno de los dispositivos. Importante, separado con barra diagonal (/) explicaremos sólo algunos comandos relevantes para nuestros ejercicios, debido a que muchos de ellos se repiten en los dispositivos.

Carga de comandos iniciales en R1

```
R1# configure terminal / entramos a modo configuración global
R1(config)#hostname R1 /cambiamos el nombre del dispositivo
R1(config)#ipv6 unicast-routing / habilitamos la interconexión de IPV6
R1(config)#no ip domain lookup / desactiva la traducción de nombre
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 # /bien-
venida en consola
R1(config)#line con 0 / entramos a configuración consola
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous /sincronizar mensajes no solicitados
R1(config-line)#exit /salimos del modo consola
R1(config)#interface E0/0 /entramos a configurar la interface E0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224 /añadimos dirección IP
R1(config-if)#ipv6 address fe80::1:1 link-local /añadimos dirección Link-local IPV6
R1(config-if)#ipv6 address 2001:db8:200::1/64 /configuramos dirección IPv6
R1(config-if)#no shutdown / encendemos administrativamente la interfaz E0/0
R1(config)#interface E0/1
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)#no shutdown
R1(config-if)#exit
R1(config)#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)#exit / salimos del modo de configuración local
```

Carga de comandos iniciales en R2

```
R2#en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
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 E0/0
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)#exit
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)#no shutdown
R2(config-if)#exit
```

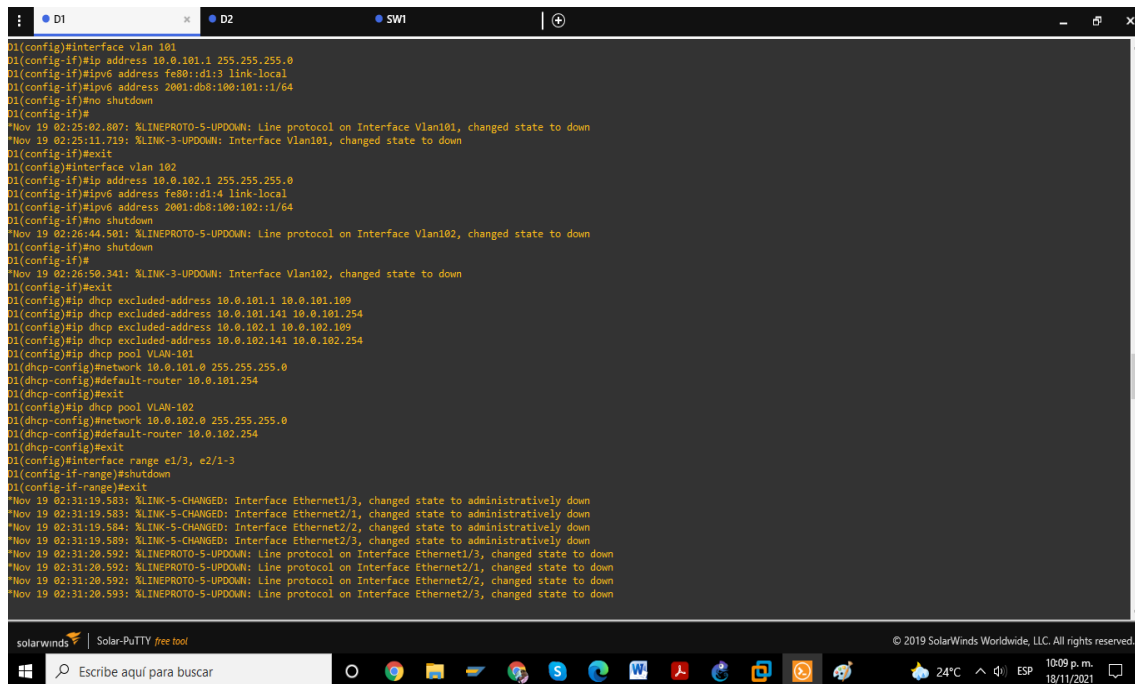
Carga de comandos iniciales en R3

```
R3#en
R3#conf t
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)#logging synchronous
R3(config-line)#exit
R3(config-if)#interface E0/1
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)#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
```


Carga de comandos iniciales en D1

```
D1#conf t
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)#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 E2/0
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)#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)#interface vlan 101
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)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config)#interface range E1/3, E2/1-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
```

Figura 3. Pantallazo de carga de comandos en D1



```
D1(config)#interface vlan 101
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)#
*Nov 19 02:25:02.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to down
*Nov 19 02:25:11.719: %LINK-3-UPDOWN: Interface Vlan101, changed state to down
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001::db8:100:102::1/64
D1(config-if)#no shutdown
*Nov 19 02:26:44.501: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to down
D1(config-if)#no shutdown
D1(config-if)#
*Nov 19 02:26:58.241: %LINK-3-UPDOWN: Interface Vlan102, changed state to down
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 e1/3, e2/1-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
*Nov 19 02:31:19.583: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
*Nov 19 02:31:19.583: %LINK-5-CHANGED: Interface Ethernet2/1, changed state to administratively down
*Nov 19 02:31:19.584: %LINK-5-CHANGED: Interface Ethernet2/2, changed state to administratively down
*Nov 19 02:31:19.589: %LINK-5-CHANGED: Interface Ethernet2/3, changed state to administratively down
*Nov 19 02:31:20.592: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
*Nov 19 02:31:20.592: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to down
*Nov 19 02:31:20.592: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2, changed state to down
*Nov 19 02:31:20.593: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/3, changed state to down
```

Carga de comandos iniciales en D2

```
R2#conf t
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)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
```

```

D2(config-vlan)#exit
D2(config)#interface E2/0
D2(config-if)#no switchport
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 shutdown
D2(config-if)#exit
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 shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
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 shutdown
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
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 E1/3, E2/1-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit

```

Carga de comandos iniciales en A1

```
SW1#en
```

```

SW1#conf t
SW1(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-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 shutdown
A1(config-if)#exit
A1(config)#interface range E0/0-3, E1/0, e2/3,E3/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit

```

Copiamos los ajustes que están corriendo en cada dispositivo a su memoria de arranque, aplicando el siguiente comando:

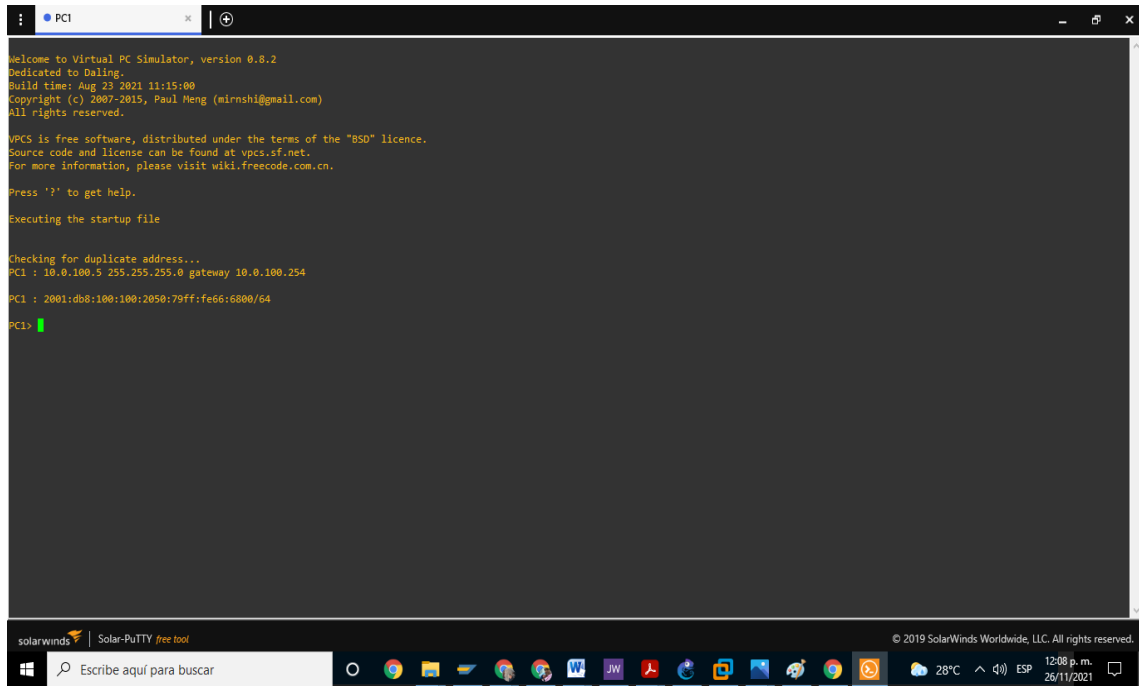
```

R1#copy running-config startup-config /copiamos en la memoria de arranque
R2#copy running-config startup-config
R3#copy running-config startup-config
D1#copy running-config startup-config
D2#copy running-config startup-config
A1#copy running-config startup-config

```

Configuramos 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. Usamos el siguiente comando:

Figura 5. Pantallazo de configuración de dirección IP en PC1



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

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

Las tareas de configuración son las siguientes:

Tabla 3. Tarea 2. Configurar la capa 2 de la red y el soporte de Host

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	Use Rapid Spanning Tree

	Rapid Spanning-Tree (RSTP)	(RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2

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

Tarea # 2.1

Procedemos a realizar el comando para encapsular y hacer posible la conexión por enlaces trunk 802.1Q de la siguiente forma:

Llamamos las interfaces que vamos a configurar en los enlaces trunk, y aplicamos el comando para encapsulación de dot1q.

En D1 ajustamos para los enlaces entre D1 y D2, también entre D1 y A1 las interfaces e0/0 has e0/3, también E1/0 y E1/1:

```
D1(config)#interface range E0/0-3, E1/0-1 /tomamos este rango de interfaces
D1(config-if-range)#switchport trunk encapsulation dot1q / permite el enlace trunk
D1(config-if-range)#switchport mode trunk /configurado extreme enlace trunk
```

Enlaces trunk entre D2 – D1, D2 – A1
interfaces E0/0 hasta E0/3, también E1/0 y E1/1

```
D2(config)#interface range E0/0-3, E1/0-1
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
```

Enlaces trunk entre A1 – D1, A1 – D2
Interfaces E1/1 hasta E1/3, y E2/0

```
A1(config)#interface range E1/1-3, E2/0
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
```

Tarea # 2.2

Configuramos la vlan nativa 999 en todos los switches

```
D1(config-if-range)##switchport trunk native vlan 999 /configuramos vlan nativa
D2(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#switchport trunk native vlan 999
```


Figura 6. Pantallazo de comando Show interfaces trunk en D1

```

D1(config-if-range)#
Nov 19 04:23:14.436: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
D1(config-if-range)#exit
D1(config)#exit
D1#
Nov 19 04:23:35.466: XSYS-5-CONFIG_I: Configured from console by console
D1#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
-----
Et0/0    on        802.1q         trunking    999
Et0/1    on        802.1q         trunking    999
Et0/2    on        802.1q         trunking    999
Et0/3    on        802.1q         trunking    999
Et1/0    on        802.1q         trunking    999
Et1/1    on        802.1q         trunking    999

Port      Vlans allowed on trunk
-----
Et0/0    100-102
Et0/1    100-102
Et0/2    100-102
Et0/3    100-102
Et1/0    100-102
Et1/1    100-102

Port      Vlans allowed and active in management domain
-----
Et0/0    100-102
Et0/1    100-102
Et0/2    100-102
Et0/3    100-102
Et1/0    100-102
Et1/1    100-102

Port      Vlans in spanning tree forwarding state and not pruned
-----
Et0/0    100-102
Et0/1    100-102
Et0/2    100-102
Et0/3    100-102
Et1/0    100-102
Et1/1    100-102
D1#
D1#
D1#

```

Figura 7. Pantallazo de comando Show interfaces trunk en D2

```

D2#show trunk interface
^
% Invalid input detected at '^' marker.
D2#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
-----
Et0/0    on        802.1q         trunking    999
Et0/1    on        802.1q         trunking    999
Et0/2    on        802.1q         trunking    999
Et0/3    on        802.1q         trunking    999
Et1/0    on        802.1q         trunking    999
Et1/1    on        802.1q         trunking    999

Port      Vlans allowed on trunk
-----
Et0/0    100-102
Et0/1    100-102
Et0/2    100-102
Et0/3    100-102
Et1/0    100-102
Et1/1    100-102

Port      Vlans allowed and active in management domain
-----
Et0/0    100-102
Et0/1    100-102
Et0/2    100-102
Et0/3    100-102
Et1/0    100-102
Et1/1    100-102

Port      Vlans in spanning tree forwarding state and not pruned
-----
Et0/0    100-102
Et0/1    none
Et0/2    none
Et0/3    none
Et1/0    100-102
Et1/1    100-102
D2#
D2#
Nov 19 04:22:43.077: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/3 (half duplex).
D2#

```

Figura 8. Pantallazo de comando Show interfaces trunk en A1

```
Nov 19 04:17:51.585: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/3 (not full duplex), with D2 Ethernet1/0 (full duplex).
A1#show ip interface
Nov 19 04:17:53.742: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/0 (not full duplex), with D2 Ethernet1/1 (full duplex).
A1#show ip interface
Nov 19 04:18:11.332: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/2 (not full duplex), with D1 Ethernet1/1 (full duplex).
A1#show ip interface
Nov 19 04:18:17.303: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not full duplex), with D1 Ethernet1/0 (full duplex).
A1#show interfaces
Nov 19 04:18:45.422: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet2/0 (not full duplex), with D2 Ethernet1/1 (full duplex).
A1#show interfaces trunk
Nov 19 04:18:47.847: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/3 (not full duplex), with D2 Ethernet1/0 (full duplex).
A1#show interfaces trunk

Port      Node      Encapsulation  Status      Native vlan
-----
Et1/1     on        802.1q          trunking    999
Et1/2     on        802.1q          trunking    999
Et1/3     on        802.1q          trunking    999
Et2/0     on        802.1q          trunking    999

Port      Vlans allowed on trunk
-----
Et1/1     100-102
Et1/2     100-102
Et1/3     100-102
Et2/0     100-102

Port      Vlans allowed and active in management domain
-----
Et1/1     100-102
Et1/2     100-102
Et1/3     100-102
Et2/0     100-102

Port      Vlans in spanning tree forwarding state and not pruned
-----
Et1/1     100-102
Et1/2     none
Et1/3     none
--More--
Nov 19 04:18:59.478: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/2 (not full duplex), with D1 Ethernet1/1 (full duplex).
Et2/0     none
A1#
A1#
Nov 19 04:19:12.884: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not full duplex), with D1 Ethernet1/0 (full duplex).
A1#
```

Tarea # 2.3

Habilitamos el protocolo Rapid Spanning-Tree (RSTP)

A1(config)#spanning-tree mode rapid-pvst /activamos el Rapid Spanning-Tree

D2(config)#spanning-tree mode rapid-pvst

D1(config)#spanning-tree mode rapid-pvst

Tarea # 2.4

Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch

Ajustes en D1

D1(config)#spanning-tree vlan 100,102 root primary / en D1 configuramos la raíz

D1(config)#spanning-tree vlan 101 root secondary / configuramos el secundario

Ajustes en D2

D2(config)#spanning-tree vlan 101 root primary

D2(config)#spanning-tree vlan 100,102 root secondary

Tarea # 2.5

Creamos los Etherchannel LACP en los switches de la siguiente forma:

D1 a D2 - Portchannel 12

D1

D1(config)#interface range e0/0-3 / tomamos este rango de interfaces

D1(config-if-range)#channel-protocol lacp /configuramos un enlace alta velocidad

D1(config-if-range)#channel-group 12 mode active / activamos el grupo 12

Creating a port-channel interface Port-channel 12 /mensaje de creación del Port-channel

D2

D2(config)#interface range e0/0-3

D2(config-if-range)#channel-protocol lacp

D2(config-if-range)#channel-group 12 mode active

D1 a A1 – Port channel 1

D1

D1(config)#interface range e1/0-1

D1(config-if-range)#channel-protocol lacp

D1(config-if-range)#channel-group 1 mode active

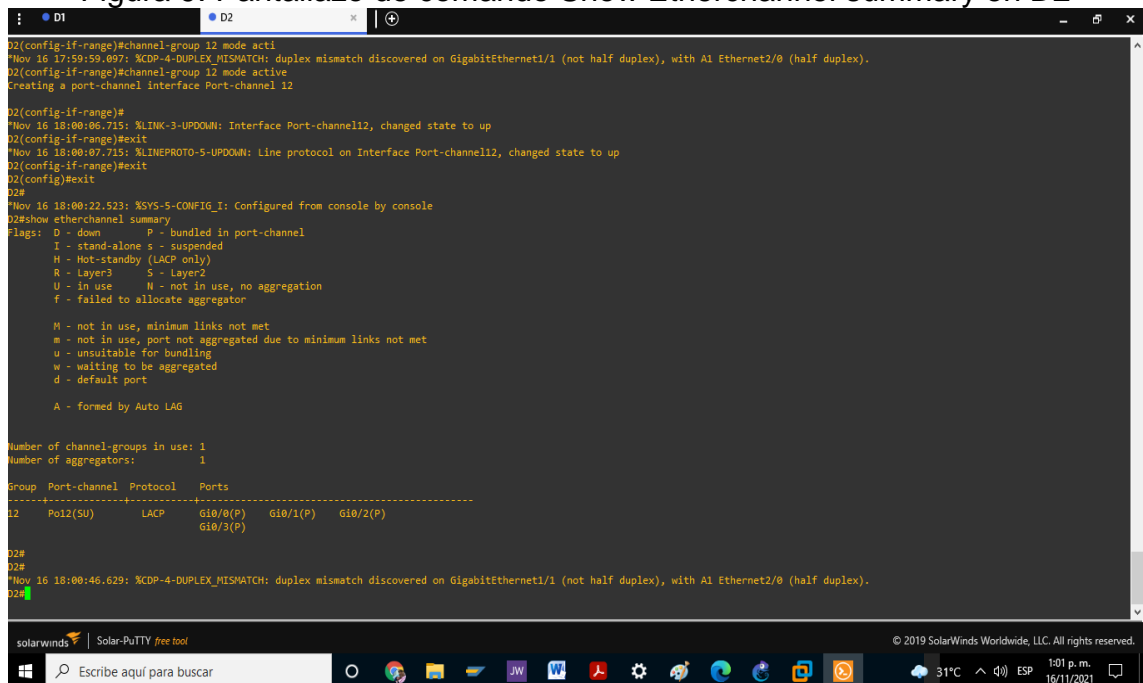
A1

A1(config)#interface range e1/1-2

A1(config-if-range)#channel-protocol lacp

A1(config-if-range)#channel-group 1 mode active

Figura 9. Pantallazo de comando Show Etherchannel summary en D2



```
D2(config-if-range)#channel-group 12 mode acti
Nov 16 17:59:59.097: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/1 (not half duplex), with A1 Ethernet2/0 (half duplex).
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel Interface Port-channel 12

D2(config-if-range)#
Nov 16 18:00:06.715: %LINK-3-UPDOWN: Interface Port-channel12, changed state to up
D2(config-if-range)#exit
Nov 16 18:00:07.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel12, changed state to up
D2(config-if-range)#exit
D2(config)#exit
D2#
Nov 16 18:00:22.523: %SYS-5-CONFIG_I: Configured from console by console
D2#show etherchannel summary
D2#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----
12     Po12(SU)         LACP       Gi0/0(P)  Gi0/1(P)  Gi0/2(P)
                               Gi0/3(P)

D2#
D2#
Nov 16 18:00:46.629: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet1/1 (not half duplex), with A1 Ethernet2/0 (half duplex).
D2#
```

```

D2 a A1 – Port channel 2
D2
D2(config)#interface range e1/0-1
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
A1
A1(config)#interface range e1/3, e2/0
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active

```

Con el código show etherchannel summary podemos ver estos Port channel

Tarea # 2.6

Configuramos los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.

```

D1
D1(config)#interface E1/2 /tomamos esta interface
D1(config-if)#switchport mode access / entramos a configuración de modo acceso
D1(config-if)#switchport access vlan 100 / seleccionamos el acceso de vlan 100
D2
D2(config)#interface E1/2
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
A1
A1(config)#interface range E2/1
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 101
A1(config)#interface range E2/2
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 100

```

Tarea # 2.7

Encendemos los PC2 y PC3, le damos comando dhcp. Recibiendo direcciones IPV4 válidas.

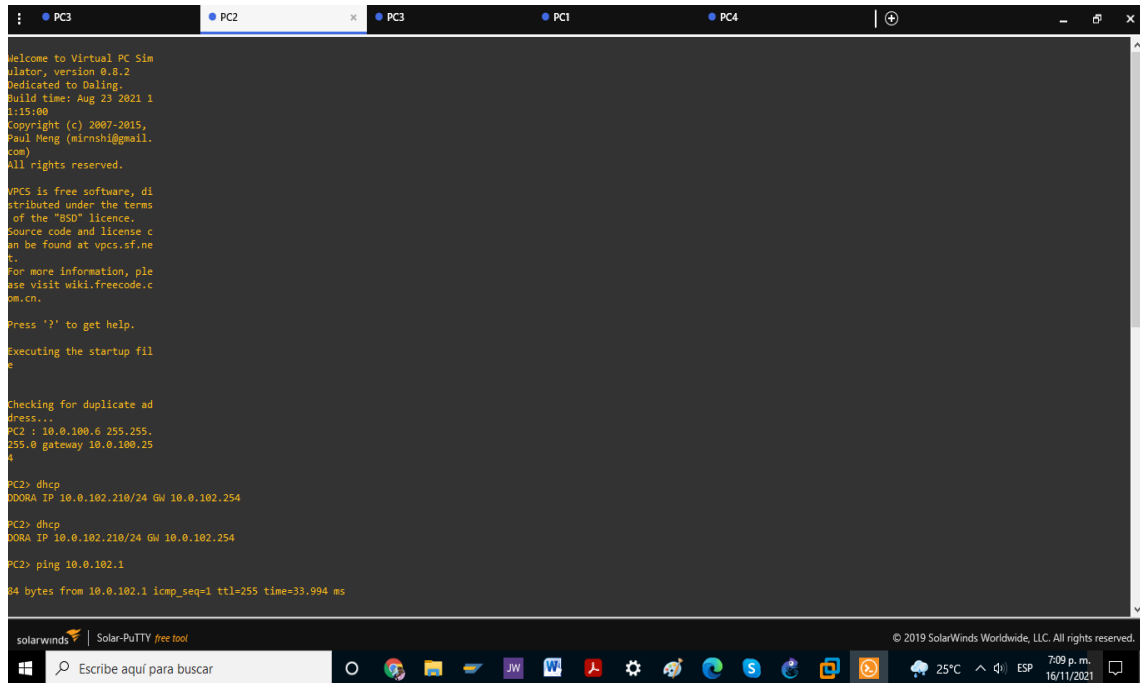
```

PC2> dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254
PC3> dhcp
DDORA IP 10.0.101.110/24 GW 10.0.101.254

```

En los computadores PC1 y PC4 se realizó la configuración de las direcciones IP accediendo directamente al PC e ingresándolas manualmente. Pero en el caso de PC2 y PC3 busca en la red y se configuran por medio de DHCP una dirección IPV4 válida. Tal como se muestra en la siguiente figura.

Figura10. Pantallazo PC3 recibiendo dirección IPV4 válida



Tarea # 2.8

Verificamos conexión de LAN local

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1 (exitoso)

D2: 10.0.100.2 (exitoso)

PC4: 10.0.100.6 (exitoso)

PC2 debería hacer ping con éxito a:

D1: 10.0.102.1 (exitoso)

D2: 10.0.102.2 (exitoso)

PC3 debería hacer ping con éxito a:

D1: 10.0.101.1 (exitoso)

D2: 10.0.101.2 (exitoso)

PC4 debería hacer ping con éxito a:

D1: 10.0.100.1 (exitoso)

D2: 10.0.100.2 (exitoso)

PC1: 10.0.100.5 (exitoso)

Parte 3. Configurar los protocolos de enrutamiento

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

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

Las tareas de configuración son las siguientes:

Tabla 4. Tarea 3. Configurar los 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.	<p>Use OSPF Process ID 4 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto E2/0 • D2: todas las interfaces excepto E2/0
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 E2/0 • D2: todas las interfaces excepto E2/0
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. En IPv4 address family, anuncie:</p>

		<ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

Tarea # 3.1

Configuramos la single-area OSPFv2 en area 0.

Use OSPF Process ID 4 y asigne los siguientes router-IDs:

R1: 0.0.4.1

R1(config)#router ospf 4 / iniciamos el proceso de redirección OSPF
R1(config-router)#router-id 0.0.4.1 / identificamos el dispositivo

Figura 15. Pantallazo comando show ip ospf interface en R1

```
LOADING to FULL, Loading Done
Nov 27 13:25:18.998: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::2 Up
Nov 27 13:25:19.095: %BGP-5-ADJCHANGE: neighbor 209.165.200.226 Up
Nov 27 13:25:19.484: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Ethernet0/1 fr
LOADING to FULL, Loading Done
Nov 27 13:25:55.486: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.131 on Ethernet0/1
from LOADING to FULL, L R1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: admin
Password:

R1#show ospf 4
% OSPFv3: Unknown Process ID 4
R1#show ip ospf interface
Serial1/0 is up, line protocol is up
Internet Address 10.0.13.1/24, Area 0, Attached via Network Statement
Process ID 4, Router ID 0.0.4.1, Network Type POINT_TO_POINT, Cost: 64
Topology-MTID      Cost      Disabled  Shutdown  Topology Name
  0                64        no        no         Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Can be protected by per-prefix Loop-Free FastReroute
Can be used for per-prefix Loop-Free FastReroute repair paths
Index 2/2, Flood queue length 0
Next 0x0(0)/0x0(0)
Last Flood scan length is 1, maximum is 2
Last Flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 0.0.4.3
Suppress hello for 0 neighbor(s)
Ethernet0/1 is up, line protocol is up
Internet Address 10.0.10.1/24, Area 0, Attached via Network Statement
Process ID 4, Router ID 0.0.4.1, Network Type BROADCAST, Cost: 10
Topology-MTID      Cost      Disabled  Shutdown  Topology Name
  0                10        no        no         Base
```

R3: 0.0.4.3

R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3

D1: 0.0.4.131

D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131

D2: 0.0.4.132

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
```

```
D2(config-router)#passive-interface default /desactivamos todas las interfaces
D2(config-router)#interface E2/0
```

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

Anunciamos las redes asociadas con R1

```
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 /anunciamos esta red
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
```

En R1, no publique la red R1 – R2.

```
R1(config-router)#passive-interface E0/0 / desactivamos publicaciones OSPF
```

En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

```
R1(config-router)#default-information originate /propagamos en R1 ruta por defecto
```

Anunciamos redes asociadas a R3

```
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
```

Anunciamos las redes asociadas a D1

```
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
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
```

Anunciamos las redes asociadas a D2

```
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
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
```

D1

Deshabilite las publicaciones OSPFv2 en la todas las interfaces excepto E2/0

```
D1(config-router)#passive-interface default / desactivamos todas las interfaces
D1(config-router)#no passive-interface E2/0/ habilitada la E2/0 para OSPF
```

D2

Deshabilite las publicaciones OSPFv2 en la todas las interfaces excepto E2/0

```
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface E2/0
```

Tarea # 3.2

En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configuramos el classic single-area OSPFv3 en area 0

Usamos el OSPF Process ID 6 y asignamos los siguientes router-IDs:

R1

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)#Router-id 0.0.6.1 /identificamos el router en la red IPV6 para OSPF
R1(config-rtr)#exit
```

R3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#
R3(config-rtr)#Router-id 0.0.6.3
R3(config-rtr)#Exit
```

D1

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
```

D2

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

En R1, R3, D1, y D2, anunciamos todas las redes directamente conectadas / VLANs en Area 0.

```
R1
R1(config)#Interface E0/1
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
```

```
R3
R3(config)#Interface E0/1
R3(config-if)#Ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#
R3(config)#Interface s1/0
R3(config-if)#Ipv6 ospf 6 area 0
R3(config-if)#exit
```

```
D1
D1(config)#Interface E2/0
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
```

```
D2
D2(config)#Interface E2/0
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

En R1, no publique la red R1 – R2.

R1(config-rtr)#Passive-interface E0/0

En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

R1(config-rtr)#Default-information originate

Deshabilitamos las publicaciones OSPFv3

D1: todas las interfaces excepto E2/0

D1(config-rtr)#passive-interface default
D1(config-rtr)#No passive-interface E0/2

D2: todas las interfaces excepto E0/2

D2(config-rtr)#passive-interface default
D2(config-rtr)#No passive-interface E0/2

Tarea # 3.3

En R2 en la “Red ISP”, configuramos el protocolo MP-BGP.

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

Una ruta estática predeterminada IPv4.

```
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 /configuramos address family en 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
```

Una ruta estática predeterminada IPv6.

Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2.

```
R2(config)#Router bgp 500
```

```
R2(config-router)#Bgp router-id 2.2.2.2 /identificamos router en BGP
```

Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

En IPv4 address family, anuncie:

La red Loopback 0 IPv4 (/32).

La ruta por defecto (0.0.0.0/0).

```
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
```

En IPv6 address family, anuncie:

La red Loopback 0 IPv4 (/128).

La ruta por defecto (::/0).

```
R2(config)#router bgp 500
```

```
R2(config-router)#Address-family ipv6
```

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

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

```
R2(config-router-af)#Network 2001:db8:2222::1/128
```

```
R2(config-router-af)#Network 0.0.0.0
```

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

En R1 en la “Red ISP”, configure MP-BGP

Configure dos rutas resumen estáticas a la interfaz Null 0:

Una ruta resumen IPv4 para 10.0.0.0/8.

```
R1(config)#Ip route 10.0.0.0 255.0.0.0 null0 /configuramos ruta resumen en IPV4
```

Una ruta resumen IPv6 para 2001:db8:100::/48.

```
R1(config)#Ipv6 route 2001:db8:100::/48 null0 /configuramos ruta resumen en IPV6
```

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1

```
R1(config)#Router bgp 300
```

```
R1(config-router)#Bgp router-id 1.1.1.1
```

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

```
R1(config-router)#Neighbor 209.165.200.226 remote-as 500
```

```
R1(config-router)#Neighbor 2001:db8:200::2 remote-as 500
```


En IPv4 address family:

Deshabilite la relación de vecino IPv6.

R1(config-router-af)#No Neighbor 2001:db8:200::2 activate

Habilite la relación de vecino IPv4.

R1(config-router-af)#Neighbor 209.165.200.226 activate

Anuncie la red 10.0.0.0/8.

R1(config-router)#Network 10.0.0.0 mask 255.0.0.0

En IPv6 address family:

Deshabilite la relación de vecino IPv4.

R1(config-router-af)#No neighbor 209.165.200.226 activate

Habilite la relación de vecino IPv6.

R1(config-router-af)#Neighbor 2001:db8:200::2 activate

Anuncie la red 2001:db8:100::/48.

R1(config-router-af)#Network 2001:db8:100::/48

Figura 16. Pantallazo de comando show bgp ipv4 / ipv6 unicast R1

```
R1#
R1#
R1#show bgp ?
*
  all           All address families
  ipv4          Address family
  ipv6          Address family
  l2vpn         Address family
  ospf          Address family
  rtfiler       Address family
  vpv4          Address family
  vpv6          Address family
  vrf           VRF scope

R1#show bgp ipv4 unicast
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
MPKI validation codes: V valid, I invalid, N Not found

  Network          Next Hop          Metric LocPrf Weight Path
*> 0.0.0.0         209.165.200.226    0         500 i
*> 2.2.2.2/32      209.165.200.226    0         500 i
*> 10.0.0.0        0.0.0.0            0         32768 i
R1#show bgp ipv6 unicast
BGP table version is 10, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
MPKI validation codes: V valid, I invalid, N Not found

  Network          Next Hop          Metric LocPrf Weight Path
*> ::0             2001:DB8:200::2    0         500 i
*> 2001:DB8:100::/48
:::                :
32768 i
*> 2001:DB8:2222::1/128
:::                :
0         500 i
R1#
```

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

En esta parte, configuraremos 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 5. Tarea 4. Configurar redundancia del primer salto

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 E0/1	<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 E0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 E0/1.	<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>Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. • Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. • Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual

		<p>10.0.102.254.</p> <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). • Rastree el objeto 6 y decremente en 60.
4.4	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</p>

		<p>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. • Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. • Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. • Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. • Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y
--	--	--

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

Tarea # 4.1

En el switch D1 creamos IP SLAs que prueben la accesibilidad de la interfaz R1 E0/1

Creamos dos IP SLA de la siguiente manera:

Use la SLAs número **4** para IPv4.

Las IP SLAs probarán la disponibilidad de la interfaz R1 E0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización.

```
D1(config)#ip sla 4 /creamos IP SLA para grupo 4 en IPV4
D1(config-ip-sla)#icmp-echo 2.2.2.2 source-ip 10.0.10.1
D1(config-ip-sla-echo)#Frequency 5 /frecuencia de prueba de interface 5 seg.
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 start-time now life forever
```

Use la SLA número **6** para IPv6.

```
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:2222::1 source-ip 2001:db8:100:1010::1
D1(config-ip-sla-echo)#Frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 start-time now life forever
```

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Use el número de rastreo 4 para la IP SLA 4.

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

```
D1(config-track)#Delay up 10
```

```
D1(config-track)#Delay down 15
```

Use el número de rastreo 6 para la IP SLA 6.

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

```
D1(config-track)#Delay up 10
```

```
D1(config-track)#Delay down 15
```

Figura 17. Pantallazo de comando show ip sla summary en D1

```
Nov 27 16:12:53.800: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 16:12:53.800: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#
Nov 27 16:13:42.259: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 16:13:42.259: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#
Nov 27 16:13:45.736: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
Nov 27 16:13:45.737: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/1 (1).
D1#
Nov 27 16:14:30.128: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 16:14:30.128: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#
Nov 27 16:14:39.751: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
Nov 27 16:14:39.751: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/1 (1).
D1#
Nov 27 16:15:29.976: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
Nov 27 16:15:29.976: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/1 (1).
D1#
Nov 27 16:15:32.700: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 16:15:32.700: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#show ip sla
% Incomplete command.
D1#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
-----
ID      Type      Destination      Stats      Return      Last
-----
*4      icmp-echo  2.2.2.2          -          Timeout     10 seconds ag
o
*6      icmp-echo  2001:DB8:2222::1 -          Timeout     10 seconds ag
o
D1#
```

Tarea # 4.2

En el switch D2 creamos IP SLAs que prueben la accesibilidad de la interfaz R3 E0/1.

Las IP SLAs probarán la disponibilidad de la interfaz R3 E0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización.

Cree IP SLAs.

- Use la SLA número 4 para IPv4.
- Use la SLA número 6 para IPv6.

Cree una IP SLA objeto para la IP SLA 4 y una para IP SLA 6.

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 2.2.2.2 source-ip 10.0.11.1
D2(config-ip-sla-echo)#Frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#Ip sla schedule 4 start-time now life forever
```

Use la SLA número 6 para IPv6.

```
D2(config)#Ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:2222::1 source-ip 2001:db8:100:1011::1
D2(config-ip-sla-echo)#Frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#Ip sla schedule 4 start-time now life forever
```

Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Use el número de rastreo 4 para la IP SLA 4.

```
D1(config)#Track 4 ip sla 4 reachability /creamos IP SLA objeto
D1(config-track)#Delay up 10 / notifica en 10 segundos
D1(config-track)#Delay down 15 / apaga en 15 segundos
```

Use el número de rastreo 6 para la IP SLA 6.

```
D1(config)#Track 6 ip sla 6 reachability
D1(config-track)#Delay up 10
D1(config-track)#Delay down 15
```

Tarea # 4.3

Configuramos en D2 HSRPv2

D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150. Configuramos las prioridades de la siguiente forma.

Configure IPv4 HSRP grupo 104 para la VLAN 100:
Asigne la dirección IP virtual 10.0.100.254.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 4 y decremente en 60.

Código aplicado para IPV4 HSRP a la Vlan 100

```
D1(config)#Interface E2/0.100 /configuramos en la subinterface
D1(config-subif)#Standby version 2 / habilitamos el HSRP
D1(config-subif)#Standby 104 ip 10.0.100.254 / ingresamos la dirección virtual
% 10.0.100.254 overlaps with Vlan100 / mensaje del sistema
D1(config-subif)#Standby 104 priority 150 / configuramos de alta prioridad
D1(config-subif)#Standby 104 preempt / Habilitamos la preferencia en grupo 104
D1(config-subif)#Standby 104 track 4 decrement 60 /seguimiento a dirección 4
```

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Aplicamos el siguiente código a Vlan 101

```
D1(config)#Interface E2/0.101
D1(config-subif)#Standby version 2
D1(config-subif)#Standby 114 ip 10.0.101.254
% 10.0.101.254 overlaps with Vlan101
D1(config-subif)#Standby 114 preempt
D1(config-subif)#Standby 114 track 4 decrement 60
```

Configure IPv4 HSRP grupo 124 para la VLAN 102:
Asigne la dirección IP virtual 10.0.102.254.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Aplicamos el siguiente código para la Vlan 102

```
D1(config)#Interface E2/0.102
D1(config-subif)#Standby version 2
D1(config-subif)#Standby 124 ip 10.0.102.254
```

```
% 10.0.102.254 overlaps with Vlan102
D1(config-subif)#Standby 124 priority 150
D1(config-subif)#Standby 124 preempt
D1(config-subif)#Standby 124 track 4 decrement 60
```

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

```
Aplicamos el siguiente código
D1(config)#Interface e2/0.100
D1(config-subif)#Standby version 2
D1(config-subif)#Standby 106 ipv6 autoconfig
D1(config-subif)#Standby 106 priority 150
D1(config-subif)#Standby 106 preempt
D1(config-subif)#Standby 106 track 6 decrement 60
```

Configure IPv6 HSRP grupo 116 para la VLAN 101:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Habilite la preferencia (preemption).
Registre el objeto 6 y decremente en 60.

```
Aplicamos el siguiente código
D1(config)#Interface e2/0.101
D1(config-subif)#Standby version 2
D1(config-subif)#Standby 116 ipv6 autoconfig
D1(config-subif)#Standby 116 preempt
D1(config-subif)#Standby 116 track 6 decrement 60
```

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

```
Aplicamos el siguiente código
D1(config)#Interface E2/0.102
D1(config-subif)#Standby version 2
D1(config-subif)#Standby 126 ipv6 autoconfig
D1(config-subif)#Standby 126 priority 150
D1(config-subif)#Standby 126 preempt
D1(config-subif)#Standby 126 track 6 decrement 60
```

Figura 18. Pantallazo de comando show standby all D1

```
Nov 27 17:47:02.225: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
Nov 27 17:47:02.225: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/1 (1).
D1#
Nov 27 17:47:05.516: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 17:47:05.516: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#
Nov 27 17:47:52.629: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/1 (half duplex).
Nov 27 17:47:52.629: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/1 (1).
D1#show standby all
Ethernet2/0.100 - Group 104 (version 2)
  State is Disabled
  Virtual IP address is unknown
  Active virtual MAC address is unknown (MAC Not In Use)
  Local virtual MAC address is unknown (unknown)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (configured 150)
  Track object 4 state Down decrement 60
  Group name is "hsrp-Et2/0.100-104" (default)
Ethernet2/0.100 - Group 106 (version 2)
  State is Active
  2 state changes, last state change 00:02:03
  Link-Local Virtual IPv6 address is FE80::5:73FP:FEA0:6A (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.006a (MAC In Use)
  Local virtual MAC address is 0005.73a0.006a (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.216 secs
  Preemption enabled
  Active router is local
D1#
Nov 27 17:48:04.592: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet1/2 (half duplex).
Nov 27 17:48:04.592: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet1/2 (1).
D1#
```

Tarea 4.4

En el switch D2 configuramos HSRPv2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:
Asigne la dirección IP virtual 10.0.100.254.
Habilite la preferencia (preemption).
Rastree el objeto 4 y decremente en 60.

Aplicamos el código

```
D2(config)#Interface E2/0.100
D2(config-subif)#Standby version 2
D2(config-subif)#Standby 104 ip 10.0.100.254
% 10.0.100.254 overlaps with Vlan100
D2(config-subif)#Standby 104 preempt
D2(config-subif)#Standby 104 track 4 decrement 60
```

Configure IPv4 HSRP grupo 114 para la VLAN 101:
Asigne la dirección IP virtual 10.0.101.254.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Aplicamos el siguiente código

```
D2(config-subif)#Standby 114 ip 10.0.101.254
% 10.0.101.254 overlaps with Vlan101
D2(config-subif)#Standby 124 priority 150
D2(config-subif)#Standby 114 preempt
D2(config-subif)#Standby 114 track 4 decrement 60
```

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Aplicamos el siguiente código

```
D2(config)#Interface E2/0.102
D2(config-subif)#Standby version 2
D2(config-subif)#Standby 124 ip 10.0.102.254
% 10.0.102.254 overlaps with Vlan102
D2(config-subif)#Standby 124 preempt
D2(config-subif)#Standby 124 track 4 decrement 60
```

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig. / usamos el autoconfig

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Aplicamos el código

```
D2(config-subif)#exit
D2(config)#Interface E2/0.100
D2(config-subif)#Standby version 2
D2(config-subif)#Standby 106 ipv6 autoconfig
D2(config-subif)#Standby 106 preempt
D2(config-subif)#Standby 106 track 6 decrement 60
```

Configure IPv6 HSRP grupo 116 para la VLAN 101:

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.

Aplicamos el código

```
D2(config-subif)#exit
D2(config)#Interface e2/0.101
D2(config-subif)#Standby version 2
```

```
D2(config-subif)#Standby 116 priority 150
D2(config-subif)#Standby 116 ipv6 autoconfig
D2(config-subif)#Standby 116 preempt
D2(config-subif)#Standby 116 track 6 decrement 60
```

Configure IPv6 HSRP grupo 126 para la VLAN 102:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Habilite la preferencia (preemption).
Rastree el objeto 6 para disminuir en 60.

Código aplicado

```
D2(config)#Interface e2/0.102
D2(config-subif)#Standby version 2
D2(config-subif)#Standby 126 ipv6 autoconfig
D2(config-subif)#Standby 126 preempt
D2(config-subif)#Standby 126 track 6 decrement 60
```

Figura 19. Pantallazo de comando show standby all D2

```

/0 (half duplex).
Nov 27 17:46:14.796: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet2/0 (1).
Nov 27 17:46:15.635: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/3 (half duplex).
Nov 27 17:46:15.635: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/3 (1).
D2#show standby all
Nov 27 17:47:02.852: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/1 (not half duplex), with A1 Ethernet2/0 (half duplex).
Nov 27 17:47:02.853: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet2/0 (1).
D2#show standby all
Ethernet2/0.100 - Group 104 (version 2)
  State is Disabled
  Virtual IP address is unknown
  Active virtual MAC address is unknown (MAC Not In Use)
  Local virtual MAC address is unknown (unknown)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 40 (default 100)
  Track object 4 state Down decrement 60
  Group name is "hsrp-Et2/0.100-104" (default)
Ethernet2/0.100 - Group 106 (version 2)
  State is Active
  2 state changes, last state change 00:01:04
  Link-Local Virtual IPv6 address is FE80::5:73FP:FEA0:6A (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.006a (MAC In Use)
  Local virtual MAC address is 0005.73a0.006a (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.776 secs
  Preemption enabled
  Active router is local
  --More--
Nov 27 17:47:06.878: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not half duplex), with A1 Ethernet1/3 (half duplex).
Nov 27 17:47:06.878: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (999), with A1 Ethernet1/3 (1).
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 6. Tarea 5. 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	Especificaciones de autenticación AAA: <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).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123 .

Tarea # 5.1, 5.2

En todos los dispositivos de la red, configuramos la protección a EXEC mediante algoritmo SCRYPT colocando como contraseña cisco 12345cisco

En cada uno entramos a modo configuración global y ejecutamos el siguiente código. Tomamos a R1 de ejemplo con el código, pero se replicó en todos.

```
R1(config)#enable secret level 15 cisco 12345cisco
R1(config)#username sadmin privilege 15 secret cisco 12345cisco
```

Tarea # 5.3, 5.4, 5.5

En todos los dispositivos except R2 configuramos AAA y le dimos las siguientes especificaciones con el servidor RADIUS

Especificaciones del servidor RADIUS.:

Dirección IP del servidor RADIUS es 10.0.100.6.

Puertos UDP del servidor RADIUS son 1812 y 1813.

Contraseña: \$trongPass

R1

```
R1(config)#aaa new-model / habilitamos el autenticador AAA
R1(config)#radius server RADIUS / usamos el Radius server
R1(config-radius-server)#$v4 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 /radius local por defecto
```

R3

```
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
```

D1

```
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)# exit
```

```
D1(config)#aaa authentication login default group radius local
```

```
D2
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#$v4 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
```

```
A1
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$v4 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
```

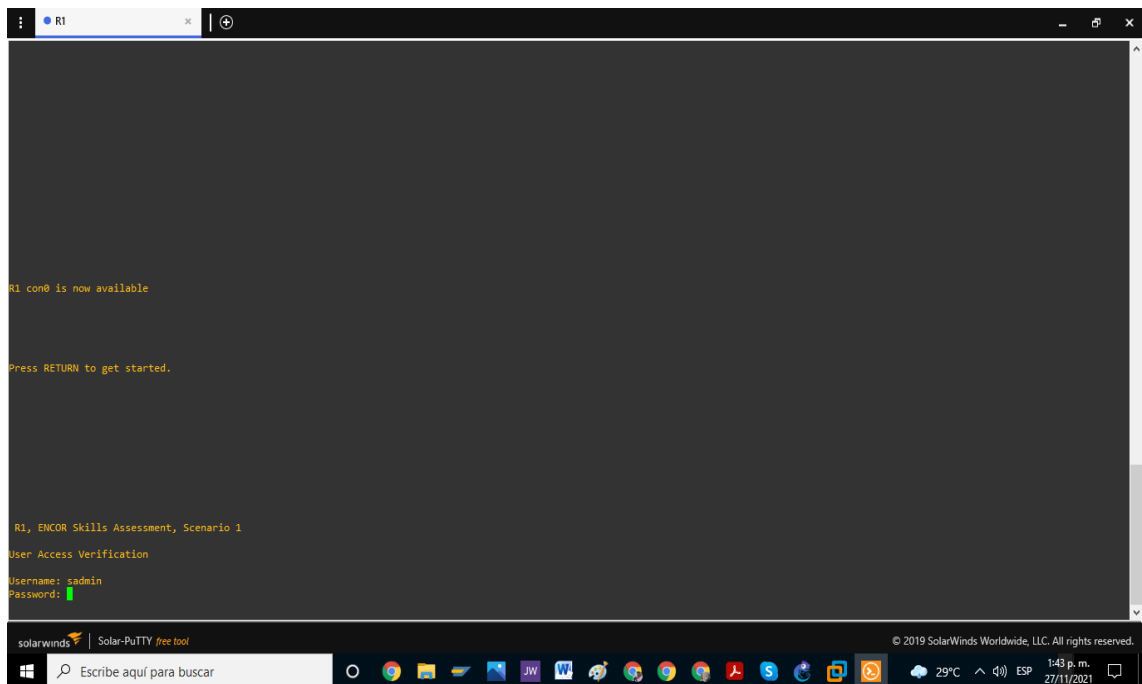
Tarea # 5.6

Reiniciamos todos los equipos, except R2 y ensayamos el usuario y la contraseña configurada

Username: sadmid

Password: cisco 12345cisco

Figura 19. Pantallazo de acceso a R1, solicitando username y password



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 7. Tarea 6. Configurar funciones de administración de red

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none">• 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 . <ul style="list-style-type: none"> • En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>. • En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>. • En A1, habilite el envío de <i>traps config</i>
--	--	--

TAREA # 6.1

Configuramos la hora en todos los dispositivos, código empleado:

```
R1#clock set 13:52:20 27 NOV 2021
R3#clock set 13:52:20 27 NOV 2021
D1#clock set 13:52:20 27 NOV 2021
D2#clock set 13:52:20 27 NOV 2021
A1#clock set 13:52:20 27 NOV 2021
```

TAREA # 6.2

Configuramos R2 como NTP maestro

```
R2(config)#ntp master 3 / configuramos R2 como NTP Maestro
```

Tarea # 6.3

Configuramos ntp en todos los dispositivos, excepto R2 de la siguiente forma.

```
R1(config)#ntp server 2.2.2.2 /sincroniza R1 con la hora de R2
R3(config)#ntp server 10.0.10.1 / sincroniza R3 con la hora de R1
D1(config)#ntp server 10.0.10.1 / sincroniza D1 con la hora de R1
D2(config)#ntp server 10.0.11.1
A1(config)#ntp server 10.0.10.1/ sincroniza A1 con la hora de R1
```

Figura 20. Pantallazo de comando show ntp associations

```

Nov 28 11:21:41.548: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/3,
changed state to down
Nov 28 11:21:49.374: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
Nov 28 11:21:53.775: %BGP-5-NBR_RESET: Neighbor 209.165.200.225 active reset (B
GP Notification sent)
Nov 28 11:21:53.775: % R2, ENCOR Skills Assessment, Scenario 1 Up
R2#show ntp
% Incomplete command.

R2#show ntp ?
  associations  NTP associations
  information   NTP Information
  packets       NTP Packet statistics
  status        NTP status

R2#show ntp status
NTPT is not enabled.
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3
R2(config)#exit
R2#show ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 600 (1/100 of seconds), resolution is 4000
reference time is E540E730.4ED91768 (11:32:00.308 UTC Sun Nov 28 2021)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 7939.05 msec, peer dispersion is 7937.98 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 6 sec ago.
R2#
Nov 28 11:32:03.895: %SYS-5-CONFIG_I: Configured from console by console
R2#show ntp associations
  address      ref clock      st  when  poll reach delay offset disp
*~127.127.1.1 .LOCL.        2   9    16  377  0.000  0.000  1.204
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

```

Tarea # 6.4, 6.5

Configuramos syslog en todos los dispositivos excepto R2 de la siguiente forma.

```

R1(config)#logging trap warning      / habilitamos los Syslog warning
R1(config)#logging host 10.0.100.5  / dirección objetivo de warning
R1(config)#logging on                / se cambia a estado encendido
R1(config)#ip access-list standard SNMP-NMS / se configure SNMP
R1(config-std-nacl)#permit host 10.0.100.5 / declaramos limite de accesos
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Cisco RaulSegundoOlmos / habilitamos contacto
R1(config)#snmp-server community ENCORSA ro SNMP-NMS /
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist / habilitamos el envio de traps
R1(config- snmp)#snmp-server enable traps bgp / habilitado traps BGP
R3(config)#snmp-server enable traps syslog / habilitado Traps de Syslog
R3(config)# snmp-server enable traps ospf / habilitado Traps de OSPF

```

```

R3
R3(config)#logging host 10.0.100.5
R3(config)#
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 RaulSegundoOlmos
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps syslog
R3(config)# snmp-server enable traps ospf

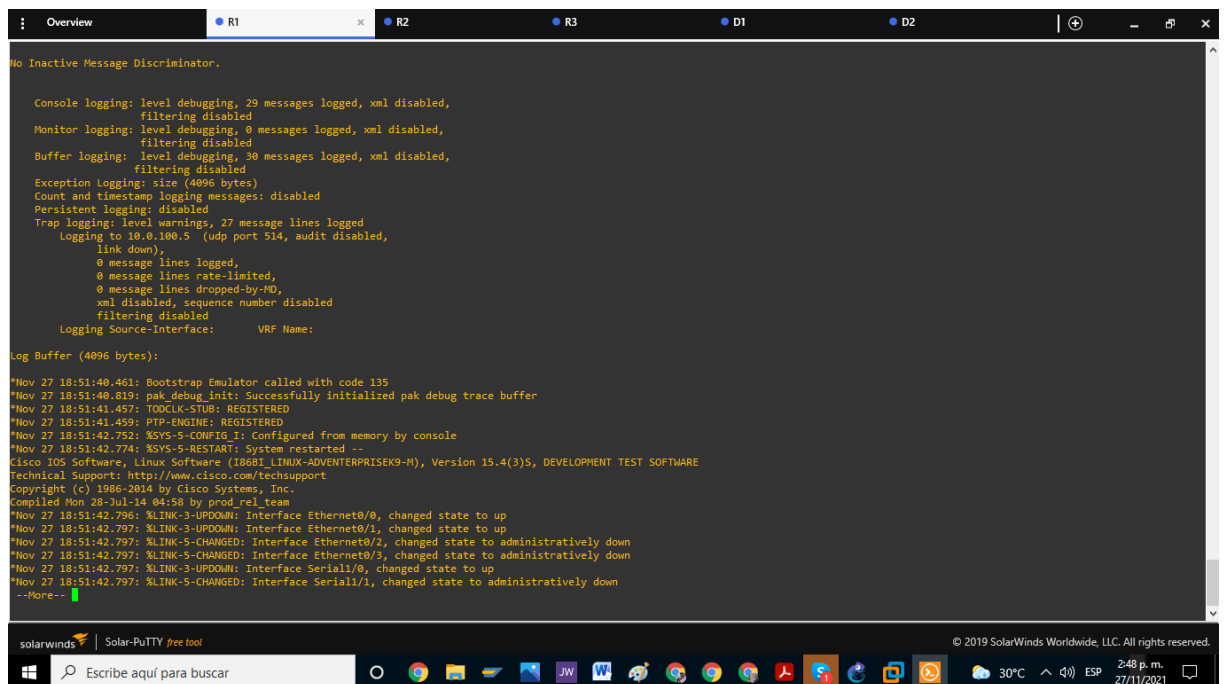
```

```

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

```

Figura 21. Pantallazo de show logging en R1



```
D2
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 Cisco RaulSegundoOlmos
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server ifindex persist
D2(config)#snmp-server enable traps syslog
D2(config)# snmp-server enable traps ospf
```

CONCLUSIONES

En el desarrollo de esta prueba de habilidades prácticas CCNP, la construcción y configuración de la red de la compañía del escenario, la realizamos en el simulador de GNS3 versión 2.2.26, descargado e instalado en su máquina virtual con todos los requerimientos necesarios para el desarrollo de la actividad.

Se realiza las conexiones de todas las terminales de la red en la topología. Por temas de limitación de simulación no utilizamos puertos Gigabit Ethernet, solicitados originalmente en el escenario, pero lo realizamos con puertos Ethernet, alcanzando los objetivos del escenario simulado con GNS3.

Se aplica la configuración a cada dispositivo, cargando las imágenes IOS necesarias con las exigencias del escenario. Después conectamos los equipos de acuerdo a la topología y se configura la capa 2 de la red, habilitando enlaces troncales y aplicando el RSTP, realizando exitosamente el comando ping desde los computadores a la red LAN local. Se aplican protocolos de enrutamiento BGP, OSPFv2 para IPV4 y OSPFv3 para IPV6.

Se configura la red de redundancia de primer salto, se desarrolla con la creación de IP SLA y del HSRP versión 2. Se da mucha importancia a la seguridad, por lo que se desarrolla el algoritmo de encriptación SCRYPT, habilitando la autenticación AAA y se configura funciones de administración de red, como la sincronización de los relojes de los dispositivos, el Syslog y el SNMPv2.

Por último, se debe destacar que estos pasos en la configuración de la red están soportados por imágenes, y en el archivo de simulación llamado Escenario 1 se puede corroborar el escenario simulado.

BIBLIOGRAFÍA

BULA, Juan Carlos “Tutorial GNS3: Instalación y Configuración Básica”. {En línea}. {1 de septiembre de 2021}. Disponible en <https://www.telectronika.com/tutoriales/gns3-tutorial-instalacion-configuracion/>

CASAS M, David “Resumen guía de comandos CISCO para administración de sistemas o ASIR”. {En línea}. {20 de octubre 2021}. Disponible en <https://informaticacoslada.com/resumen-guia-de-comandos-cisco-para-administracion-de-sistemas-asir/>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGq5JUqUBthk8>

UNAD (2017). “Configuración de Switches y Routers [OVA]”. {En línea}. {1 de noviembre 2021}. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhqL9QChD1m9EuGqC>