

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HENRY ALEXANDER MEDINA OROZCO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HENRY ALEXANDER MEDINA OROZCO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cali, 29 de noviembre de 2021

AGRADECIMIENTOS

Este trabajo de prueba de habilidades prácticas fue realizado individualmente por el estudiante de último semestre de la ingeniería en telecomunicaciones, se agradece el apoyo desinteresado a lucrarse de muchas personas que directa o indirectamente ayudaron a superar los numerosos obstáculos en el camino, por ello se tiene que dar gracias.

En primer lugar, los agradecimientos van dirigidos a Dios por proveer sabiduría, coraje y sensatez, para superar cada uno de los obstáculos que surgieron en este largo camino llegando a completar la meta.

En segundo lugar, se le agradece a la familia y compañeros por el apoyo incondicional, siempre estuvieron ahí para superar los problemas que se dieron; por el apoyo moral y motivacional que mantuvieron vivas las ganas de llegar al final del camino.

En tercer lugar, se agradece a los tutores que animaron y ayudaron a construir el conocimiento durante todo el trayecto de la educación, haciendo posible el rápido aprendizaje, el fortalecimiento de conocimientos previos y nuevos, buscando que el futuro egresado sea competitivo en el entorno profesional.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTA DE TABLAS	7
LISTA DE FIGURAS	8
GLOSARIO	9
RESUMEN	10
ABSTRACT	10
INTRODUCCIÓN	11
ESCENARIO	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	20
Paso 1: Configurar las interfaces troncales	20
Paso 2: Configurar la VLAN 99 como nativa:	20
Paso 3: Habilitar protocolo Rapid Spanning-Tree (RSTP)	21
Paso 4: Configurar los puentes raíz (root bridges)	21
Paso 5: crear los LACP	22
Paso 6: Configurar los puertos de acceso a los PC	24
Paso 7: Verificar los PC en DHCP:	25
Paso 8: Verificación de la conectividad de la LAN local	25
Parte 3: Configurar los protocolos de enrutamiento	27
Paso 1: Configuración OSPFv2	27
Paso 2: Configuración de OSPFv3	27
Paso 3: Configuración MP-BGP en la red ISP R2	29
Paso 4: Configuración MP-BGP en la red ISP R1	29
Paso 5: Verificación del MP-BGP con Ping	30
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)	31
Paso 1: En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.	31
Paso 2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.	31
Paso 3: En D1 configure HSRPv2	32
Paso 4: En D2 configure HSRPv2	33
Parte 5: Seguridad	35
Paso 1: En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT	35
Paso 2: En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT	35
Paso 3: En todos los dispositivos (excepto R2), habilite AAA	36
Parte 4: En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS	37

Paso 5: En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	38
Paso 6: Verifique el servicio AAA en todos los dispositivos (excepto R2).....	38
Parte 6: Configure las funciones de Administración de Red	40
Paso 1: En todos los dispositivos, configure el reloj local a la hora UTC actual.	40
Paso 2: Configure R2 como un NTP maestro.	40
Paso 3: Configure NTP en R1, R3, D1, D2, y A1.	40
Paso 4: Configure Syslog en todos los dispositivos excepto R2	41
Paso 5: Configure SNMPv2c en todos los dispositivos excepto R2	42
CONCLUSIONES	45
BIBLIOGRAFÍA.....	46

LISTA DE TABLAS

Tabla 1. Direccionamiento IP.....	13
-----------------------------------	----

LISTA DE FIGURAS

Figura 1.	Montaje del escenario propuesto.....	12
Figura 2.	Configuración de IP en los PC:.....	19
Figura 3.	Verificación de los enlaces troncales.....	21
Figura 4.	Verificación de spanning-tree.....	22
Figura 5.	Verificación del LACP:.....	24
Figura 6.	IP de los PC en DHCP.....	25
Figura 7.	Ping entre los dispositivos de la red local.....	25
Figura 8.	Verificación de la tabla de ruta IPv4:.....	30
Figura 9.	Ping D1 y D2 hacia Loopback 0.....	30
Figura 10.	Verificación de las SLAs.....	32
Figura 11.	Verificación del Standby.....	34
Figura 12.	Verificación de la creación de usuario y contraseñas.....	36
Figura 13.	Verificación de autenticación en los switches.....	38
Figura 14.	Verificación de autenticación routers.....	39
Figura 15.	Verificación de la configuración NTP.....	41
Figura 16.	Verificación de la configuración SNMP.....	43

GLOSARIO

ASN: Autonomous System Number, se le denomina al grupo de red que es gestionado por algún operador de red por ruteo externo.

BGP: Border Gateway Protocol, utilizado para conectar distintos sistemas autónomos principalmente con el canal de internet.

DHCP: Dynamic Host Configuration Protocol, funciona en el modelo cliente/servidor y proporciona automáticamente direcciones IP y otra información relacionada como la máscara y el Gateway.

HSRP: Host Standby Routing Protocol, asigna a un grupo de redundancia un router activo, otro standby y los demás en estado listen, donde el activo tendrá la IP virtual.

ISP: Internet Service Provider, término que identifica las compañías que proveen acceso a internet.

LACP: Link Aggregation Control Protocol, característico de la capa 2 une puertos físicos de la red en un único puerto lógico de gran ancho de banda, y crea redundancias.

MP-BGP: Multiprotocol -BGP, permite que BGP lleve información de IPv6 y otros protocolos de red múltiple.

OSPFv2: Open Shortest Path First, protocolo de enrutamiento dinámico que detecta cambios en la topología, fallas de enlace y converge en una nueva estructura rápidamente, específicamente para IPv4.

OSPFv3: Open Shortest Path First, protocolo de enrutamiento dinámico que detecta cambios en la topología, fallas de enlace y converge en una nueva estructura rápidamente, específicamente para IPv6.

Root bridge: Punto de referencia dentro de la red que puede soportar más conmutación, todos los switches deben estar conectados hacia él con el mejor coste.

RSTP: Rapid Spanning Tree Protocol, aplicable a la capa 2 reduce considerablemente la convergencia de la topología cuando ocurre algún cambio.

VLAN: Virtual LAN, método utilizado para crear varias redes lógicas dentro de una solo red física.

RESUMEN

El presente trabajo se desarrolla como opción de grado para la ingeniería en telecomunicaciones y electrónica, aplicando las habilidades prácticas CCNP bajo un escenario planteado, su montaje se realiza en el simulador GNS3 utilizando imágenes IOS de los dispositivos CISCO, esta propuesta de escenario parece simple pero los requisitos de configuración que se piden en la guía son diversos para lograr simular tal y cual es una red a nivel profesional; colocando a prueba las habilidades del estudiante en el conocimiento de las redes de datos, primero se configuran varios protocolos para la conmutación en la capa 2 del modelo OSI, paralelamente se configuran protocolos de la capa 3 para establecer el enrutamiento entre la propia LAN (red de la empresa) y otro sistema autónomo (ISP), obteniendo como resultado redes convergentes que se comunican entre sí con algunas políticas de seguridad establecidas simulando escenarios a los cuales se va a enfrentar el futuro egresado.

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

ABSTRACT

The present work is developed as a degree option for telecommunications and electronics engineering, applying CCNP practical skills under a proposed scenario, its assembly is carried out in the GNS3 simulator using IOS images of CISCO devices, this scenario proposal seems simple but the configuration requirements that are asked in the guide are diverse to achieve simulate such and which is a network at a professional level; Putting the student's skills in the knowledge of data networks to the test, first several protocols are configured for switching in layer 2 of the OSI model, in parallel, layer 3 protocols are configured to establish the routing between the LAN itself (network of the company) and another autonomous system (ISP), obtaining as a result convergent networks that communicate with each other with some established security policies simulating scenarios that the future graduate will face.

Key words: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Las redes informáticas toman más fuerza cada año a nivel de la vida cotidiana y lo empresarial porque permiten compartir información, facilitan la interacción y la comunicación entre las personas y las empresas; por eso es importante que el futuro ingeniero en Telecomunicaciones entienda estas redes y aprenda a configurar los diferentes protocolos que permiten dicha interconexión; para ello se realiza el siguiente trabajo, donde se plantea un escenario el cual consta de 3 router, 3 switches y 4 PCs simulando las redes a las que se va a ver expuesto en un futuro el ingeniero.

Inicialmente se configura el direccionamiento IP en todos los dispositivos tanto IPv4 e IPv6, luego utilizando 2 switches multicapa como si fueran los CORE de la red encargados de la conmutación cada uno enfatizado en VLAN diferente y con enlaces redundantes, adicional 1 switch de capa 2 utilizado como el acceso a los clientes, en general en la capa 2 se debe trabajar el RSTP Rapid Spanning Tree Protocol y enlaces LACP, a nivel de capa 3 se soluciona la convergencia de la red totalmente, donde se configura el OSPFv2 para IPV4 y OSPF para IPv6 de la LAN; el enrutamiento BGP para IPv4 y MP-BGP para IPv6 para conectar el sistema autónomo de las dos redes planteadas, esta primera parte asegura la interconexión de los equipos de la LAN de la empresa con los servicios del ISP.

En la segunda parte ya con una red convergente, se configura la redundancia del primer salto con el protocolo HSRP utilizando una IP virtual .254; algunas políticas de seguridad como el protocolo AAA y contraseñas de acceso, para elevar la seguridad de los dispositivos administrables; por último, se configura la sincronización de hora con NTP entre todos los dispositivos y la gestión de la red con el protocolo SNMPv2, para tener un monitoreo en tiempo real de la red.

ESCENARIO

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 1. Montaje del escenario propuesto.

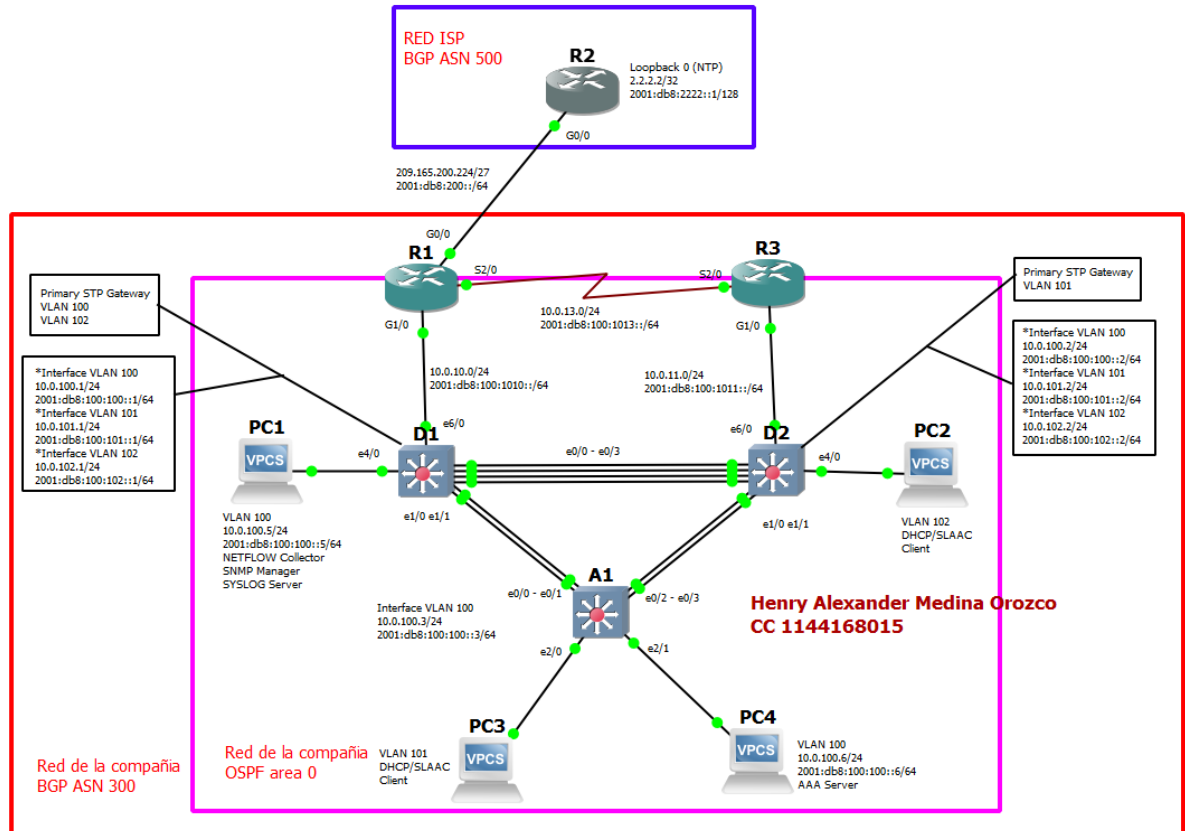


Tabla 1. Direccionamiento IP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	e6/0	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	e6/0	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

Paso 2: Configurar los parámetros básicos para cada dispositivo

Se procede a configurar los parámetros básicos de los dispositivos como los nombres, textos de banner motd para cada equipo, específicamente las IP de cada interfaz tanto en IPV4 como en IPV6 de cada uno de los router, en el caso de los switches la creación de las VLAN con sus nombres, las direcciones IP, y se crea un pool DHCP con sus respectivas exclusiones.

Router 1:

```
Router#config t //Ingreso a modo configuración global
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1 //se nombra el router
R1(config)#ipv6 unicast-routing //habilita el routing en IPV6
R1(config)#no ip domain-lookup //desactiva la traducción de nombres a dirección
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 # //Mensaje cuando
se conecta a consola
R1(config)#line con 0 //configuración de la línea de consola
R1(config-line)#exec-timeout 0 0
```

```

R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#inter g0/0 //configuración de la interfaz
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 //enciende la interfaz
R1(config-if)#exit
R1(config)#interface g1/0
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)#no shutdown
R1(config-if)#exit
R1(config)#interface s2/0
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
R1#copy run star //guarda la configuración actual
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

Router 2:

```

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(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)#exit
R2(config)#interface Loopback 0 //se configura la interfaz virtual
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

```

```
R2(config)#exit
R2#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
```

Router 3:

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain-loo
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)#interface g1/0
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 s2/0
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)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

Switch D1:

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 //se crea la VLAN
D1(config-vlan)#name Management //se nombra la VLAN
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface e6/0
D1(config-if)#no switchport //Brinda la capacidad capa 3 al puerto
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 //se configuran las IP de la VLAN
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan100, changed state to up
D1(config-if)#exit
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
%LINK-5-CHANGED: Interface Vlan101, changed state to up
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
%LINK-5-CHANGED: Interface Vlan102, changed state to up
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 //Crea el pool para la VLAN
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)#exit
D1#
%SYS-5-CONFIG_I: Configured from console by console
D1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
D1#

```

Switch D2:

```

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 e6/0
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:1 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
%LINK-5-CHANGED: Interface Vlan100, changed state to up
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
%LINK-5-CHANGED: Interface Vlan101, changed state to up
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
%LINK-5-CHANGED: Interface Vlan102, changed state to up
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)#exit

```

Switch A1:

```

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 vlan 100
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)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

```

Configuración de los PC:

Figura 2. Configuración de IP en los PC:

```

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.0.100.5/24 10.0.100.254 00:50:79:66:68:00 20024 127.0.0.1:20025
fe80::250:79ff:fe66:6800/64
2001:fb8:100:100::5/64

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> █

PC2> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 0.0.0.0/0 0.0.0.0 00:50:79:66:68:01 20026 127.0.0.1:20027
fe80::250:79ff:fe66:6801/64

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 0.0.0.0/0 0.0.0.0 00:50:79:66:68:02 20028 127.0.0.1:20029
fe80::250:79ff:fe66:6802/64

PC3> █

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.100.6/24 10.0.100.254 00:50:79:66:68:03 20030 127.0.0.1:20031
fe80::250:79ff:fe66:6803/64
2001:db8:100:100::6/64

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

PC4> █

```

PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST

Paso 1: Configurar las interfaces troncales

Switch D1:

```
D1(config)# interface range e0/0 - 3, e1/0 - 1 //configura un grupo de interfaces
D1(config-if-range)# switchport trunk encapsulation dot1q //establece la encapsulación en el
estándar IEEE 802.1Q
D1(config-if-range)#switchport mode trunk //configura la interfaz troncal
```

Switch D2:

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

Switch A1:

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

Paso 2: Configurar la VLAN 99 como nativa:

Switch D1:

```
D1(config)# interface range e0/0 - 3, e1/0 - 1
D1(config-if-range)#switchport trunk native vlan 999
```

Switch D2:

```
D2(config)# interface range e0/0 - 3, e1/0 - 1
D2(config-if-range)#switchport trunk native vlan 999
```

Switch A1:

```
A1(config)# interface range e0/0 - 3
A1(config-if-range)#switchport trunk native vlan 999
```

Figura 3. Verificación de los enlaces troncales

```
D1#show int tru
D1#show int trunk

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

Port      Vlans allowed on trunk
Po1       100-102
Po12      100-102

D2#show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po2       100-102
Po12      100-102

A1#show int trunk

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

Port      Vlans allowed on trunk
Po1       100-102
Po2       100-102
```

Paso 3: Habilitar protocolo Rapid Spanning-Tree (RSTP).

Switch D1:

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

Switch D2:

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

Switch A1:

```
A1(config)#spanning-tree mode rapid-pvst
A1(config)#
```

Paso 4: Configurar los puentes raíz (root bridges)

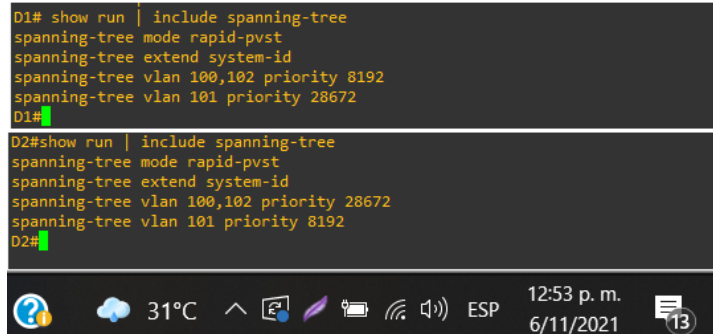
Switch D1:

```
D1(config)#spanning-tree vlan 100 root primary
D1(config)#spanning-tree vlan 102 root primary
D1(config)#spanning-tree vlan 101 root secondary
```

Switch D2:

```
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100 root secondary
D2(config)#spanning-tree vlan 102 root secondary
```

Figura 4. Verificación de spanning-tree



```
D1# show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 8192
spanning-tree vlan 101 priority 28672
D1#
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 8192
D2#
```

The screenshot shows a terminal window with a dark background. The top part displays the configuration for D1, and the bottom part displays the configuration for D2. The system tray at the bottom shows the temperature as 31°C, the time as 12:53 p.m., and the date as 6/11/2021.

Paso 5: crear los LACP.

Switch D1:

```
D1(config)# interface range e0/0 – 3
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 12
D1(config-if-range)#exit
D1(config)#interfac port-channel 12
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#switchport trunk allowed vlan 100-102
D1(config-if)#exit
D1(config)# interface range e1/0 - 1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 1
D1(config-if-range)#exit
D1(config)#interfac port-channel 1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#switchport trunk allowed vlan 100-102
D1(config-if)#exit
D1(config)#
```

Switch D2:

```
D2(config)# interface range e0/0 - 3
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 12
D2(config-if-range)#exit
D2(config)#interfac port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#switchport trunk allowed vlan 100-102
D2(config-if)#exit
D2(config)# interface range e1/0 - 1
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 2
D2(config-if-range)#exit
D2(config)#interfac port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#switchport trunk allowed vlan 100-102
D2(config-if)#exit
D2(config)#
```

Switch A1:

```
A1(config)# interface range e0/0 - 1
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode passive
A1(config-if-range)#
Creating a port-channel interface Port-channel 1
A1(config-if-range)#exit
A1(config)#interfac port-channel 1
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#switchport trunk allowed vlan 100-102
A1(config-if)#switchport mode trunk
A1(config-if)#exit
A1(config)# interface range e0/2 - 3
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode passive
A1(config-if-range)#
Creating a port-channel interface Port-channel 2
A1(config-if-range)#exit
A1(config)#interfac port-channel 2
A1(config-if)#switchport mode trunk
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#switchport trunk allowed vlan 100-102
A1(config-if)#exit
```

A1(config)#

Paso 6: Configurar los puertos de acceso a los PC.

Switch D1:

```
D1(config)# interface e4/0
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
```

Switch D2:

```
D2(config)# interface e4/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
```

Switch A1:

```
A1(config)# interface e2/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#exit
A1(config)# interface e2/1
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#exit
A1(config)#
```

Figura 5. Verificación del LACP:

```
Diashow lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 1 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et1/0    SP     32768     aabb.cc00.0100  4s  0x0 0x1 0x1 0x3C
Et1/1    SP     32768     aabb.cc00.0100  8s  0x0 0x1 0x2 0x3C

Channel group 12 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et0/0    SA     32768     aabb.cc00.0300  8s  0x0 0xC 0x1 0x3D
Et0/1    SA     32768     aabb.cc00.0300  79s 0x0 0xC 0x2 0x3D
Et0/2    SA     32768     aabb.cc00.0300  19s 0x0 0xC 0x3 0x3D
Et0/3    SA     32768     aabb.cc00.0300  19s 0x0 0xC 0x4 0x3D

Diashow lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 2 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et1/0    SP     32768     aabb.cc00.0100  24s 0x0 0x2 0x3 0x3C
Et1/1    SP     32768     aabb.cc00.0100  28s 0x0 0x2 0x4 0x3C

Channel group 12 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et0/0    SA     32768     aabb.cc00.0200  6s  0x0 0xC 0x1 0x3D
Et0/1    SA     32768     aabb.cc00.0200  15s 0x0 0xC 0x2 0x3D
Et0/2    SA     32768     aabb.cc00.0200  13s 0x0 0xC 0x3 0x3D
Et0/3    SA     32768     aabb.cc00.0200  9s  0x0 0xC 0x4 0x3D

Diashow lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 1 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et0/0    SA     32768     aabb.cc00.0200  26s 0x0 0x1 0x101 0x3D
Et0/1    SA     32768     aabb.cc00.0200  19s 0x0 0x1 0x102 0x3D

Channel group 2 neighbors
Partner's information:
Port      Flags  LACP port  LACP port  Admin Oper  Port  Port
Flags  Priority Dev ID     Age  key  Key  Number State
Et0/2    SA     32768     aabb.cc00.0300  4s  0x0 0x2 0x101 0x3D
Et0/3    SA     32768     aabb.cc00.0300  21s 0x0 0x2 0x102 0x3D
```


Paso 7: Verificar los PC en DHCP:

Figura 6. IP de los PC en DHCP

```
PC2> ip dhcp
DDORA IP 10.0.102.110/24 GW 10.0.102.254

PC2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.102.110/24 10.0.102.254 00:50:79:66:68:01 20026 127.0.0.1:20027
fe80::250:79ff:fe66:6801/64
2001:db8:100:102:2050:79ff:fe66:6801/64 eui-64

PC2> █

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

PC3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.110/24 10.0.101.254 00:50:79:66:68:02 20028 127.0.0.1:20029
fe80::250:79ff:fe66:6802/64

PC3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.110/24 10.0.101.254 00:50:79:66:68:02 20028 127.0.0.1:20029
fe80::250:79ff:fe66:6802/64
2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64

PC3> █
```

Paso 8: Verificación de la conectividad de la LAN local

Figura 7. Ping entre los dispositivos de la red local

```
PC1>
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.132 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.237 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.208 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.228 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.211 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.276 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.426 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.535 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.408 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.538 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.298 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=0.425 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.480 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.426 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.569 ms

PC1> █

PC4>
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.297 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.421 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.425 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.418 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.404 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.439 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.558 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.566 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.678 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.519 ms

PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.925 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.563 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.460 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.502 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.523 ms

PC4> █
```

```
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.263 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.473 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.400 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.514 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.441 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.159 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.257 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.330 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.213 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.300 ms

PC2> █
```

```
PC3> ping 10.0.101.1

84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.486 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.676 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=0.671 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=0.767 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.588 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.299 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.422 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=0.523 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.399 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.579 ms

PC3> █
```

PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO

Paso 1: Configuración OSPFv2

Router 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)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R1(config)#router ospf 4
R1(config-router)#default-information originate
```

Router R3:

```
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
```

Switch D1:

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
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
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e6/0
```

Switch D2:

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
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
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e6/0
```

Paso 2: Configuración de OSPFv3

Router R1:

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
```

```
R1(config-rtr)#exit
R1(config)#interface s2/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#interface g1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ipv6 route ::/0 g0/0
R1(config)#ipv6 router ospf 6
R1(config-rtr)#default-information originate
```

Router R3:

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface s2/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#interface g1/0
R3(config-if)#ipv6 ospf 6 area 0
```

Switch D1:

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#interface e6/0
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)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
```

Switch D2:

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#interface e6/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
```

Paso 3: Configuración MP-BGP en la red ISP R2.

Router 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)#no bgp default ipv4-unicast
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 unicast
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0
R2(config-router-af)#exit
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::1/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit
```

Paso 4: Configuración MP-BGP en la red ISP R1

Router R1:

```
R1(config)#ip route 10.0.0.0 255.0.0.0 null 0
R1(config)#ipv6 route 2001:db8:100::/48 null 0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#no bgp default ipv4-unicast
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)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
```

Figura 8. Verificación de la tabla de ruta IPv4:

```

D1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 10.0.10.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.10.1, 01:04:40, Ethernet6/0
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C 10.0.10.0/24 is directly connected, Ethernet6/0
L 10.0.10.2/32 is directly connected, Ethernet6/0
O 10.0.11.0/24 [110/75] via 10.0.10.1, 01:04:40, Ethernet6/0
O 10.0.13.0/24 [110/74] via 10.0.10.1, 01:04:40, Ethernet6/0
C 10.0.100.0/24 is directly connected, Vlan100
L 10.0.100.1/32 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
L 10.0.101.1/32 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
L 10.0.102.1/32 is directly connected, Vlan102
D1#

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet0/0
10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
S 10.0.0.0/8 is directly connected, Null0
C 10.0.10.0/24 is directly connected, GigabitEthernet1/0
L 10.0.10.1/32 is directly connected, GigabitEthernet1/0
O 10.0.11.0/24 [110/65] via 10.0.13.3, 01:05:42, Serial2/0
C 10.0.13.0/24 is directly connected, Serial2/0
L 10.0.13.1/32 is directly connected, Serial2/0
O 10.0.100.0/24 [110/2] via 10.0.10.2, 01:05:42, GigabitEthernet1/0
O 10.0.101.0/24 [110/2] via 10.0.10.2, 00:24:58, GigabitEthernet1/0
O 10.0.102.0/24 [110/2] via 10.0.10.2, 00:24:36, GigabitEthernet1/0
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#

D2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.0.11.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.11.1, 01:07:01, Ethernet6/0
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O 10.0.10.0/24 [110/75] via 10.0.11.1, 01:07:01, Ethernet6/0
C 10.0.11.0/24 is directly connected, Ethernet6/0
L 10.0.11.2/32 is directly connected, Ethernet6/0
O 10.0.13.0/24 [110/74] via 10.0.11.1, 01:07:01, Ethernet6/0
C 10.0.100.0/24 is directly connected, Vlan100
L 10.0.100.2/32 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
L 10.0.101.2/32 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
L 10.0.102.2/32 is directly connected, Vlan102
D2#

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 01:05:35, Serial2/0
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O 10.0.10.0/24 [110/65] via 10.0.13.1, 01:04:54, Serial2/0
C 10.0.11.0/24 is directly connected, GigabitEthernet1/0
L 10.0.11.1/32 is directly connected, GigabitEthernet1/0
C 10.0.13.0/24 is directly connected, Serial2/0
L 10.0.13.3/32 is directly connected, Serial2/0
O 10.0.100.0/24 [110/2] via 10.0.11.2, 00:26:42, GigabitEthernet1/0
O 10.0.101.0/24 [110/2] via 10.0.11.2, 00:25:17, GigabitEthernet1/0
O 10.0.102.0/24 [110/2] via 10.0.11.2, 01:04:54, GigabitEthernet1/0
R3#
    
```

Paso 5: Verificación del MP-BGP con Ping

Figura 9. Ping D1 y D2 hacia Loopback 0

```

D1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 26/30/32 ms
D1#ping 2001:db8:2222::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2222::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/42/84 ms
D1#

D2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/52/53 ms
D2#ping 2001:db8:2222::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:2222::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/58/78 ms
D2#
    
```

PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO (FIRST HOP REDUNDANCY)

Paso 1: En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.

Switch D1:

```
D1(config)#
D1(config)#ip sla 4 //Crea el SLA
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-ip 10.0.10.2 //define el destino y la fuente
D1(config-ip-sla-echo)#frequency 5 //define cada cuantos segundos
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 start-time now life forever // inicia SLA ahora y siempre
D1(config)#track 4 ip sla 4 reachability //crea el objeto para saber si down o up
D1(config-track)#delay up 10 down 15 // se dan los retardos solicitados
D1(config-track)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-interface e6/0
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 6 start-time now life forever
D1(config)#track 6 ip sla 6 reachability
D1(config-track)#delay up 10 down 15
D1(config-track)#exit
```

Paso 2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.

Switch D2:

```
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-interface e6/0
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 start-time now life forever
D2(config)#track 4 ip sla 4 reachability
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-interface e6/0
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 6 start-time now life forever
D2(config)#track 6 ip sla 6 reachability
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
```

Figura 10. Verificación de las SLAs.

```
D1# show run | section ip sl
track 4 ip sla 4 reachability
  delay down 15 up 10
track 6 ip sla 6 reachability
  delay down 15 up 10
ip sla 4
  icmp-echo 10.0.10.1 source-interface Ethernet6/0
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1 source-interface Ethernet6/0
  frequency 5
ip sla schedule 6 life forever start-time now
D1#

D2#show run | section ip sla
track 4 ip sla 4 reachability
  delay down 15 up 10
track 6 ip sla 6 reachability
  delay down 15 up 10
ip sla 4
  icmp-echo 10.0.11.1 source-interface Ethernet6/0
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1 source-interface Ethernet6/0
  frequency 5
ip sla schedule 6 life forever start-time now
D2#
```

Paso 3: En D1 configure HSRPv2.

Switch D1:

```
D1(config)#interface vlan 100
D1(config-if)#standby version 2 //active la version 2 para ipv6
D1(config-if)#standby 104 ip 10.0.100.254 // crea el grupo con la ip virtual
D1(config-if)#standby 104 priority 150 // se cambia la prioridad defecto de 100
D1(config-if)#standby 104 preempt // sera el equipo principal
D1(config-if)#standby 104 track 4 decrement 60 //rastrea el objeto 4
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
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
```

Paso 4: En D2 configure HSRPv2.

Switch D2:

```
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)#standby 104 track 4 decrement 60
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
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)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit
```

Figura 11. Verificación del Standby

```
D1#show run | section standby
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
D1#

D2#show run | section standby
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
D2#
```

26°C ^ 3:43 p. m. 8/11/2021

PARTE 5: SEGURIDAD

Paso 1: En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

Router R1:

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

Router R2:

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

Router R3:

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

Switch D1:

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

Switch D2:

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

Switch A1:

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

Paso 2: En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

Router R1:

```
R1(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

Router R2:

```
R2(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

Router R3:

```
R3(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

Switch D1:

```
D1(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

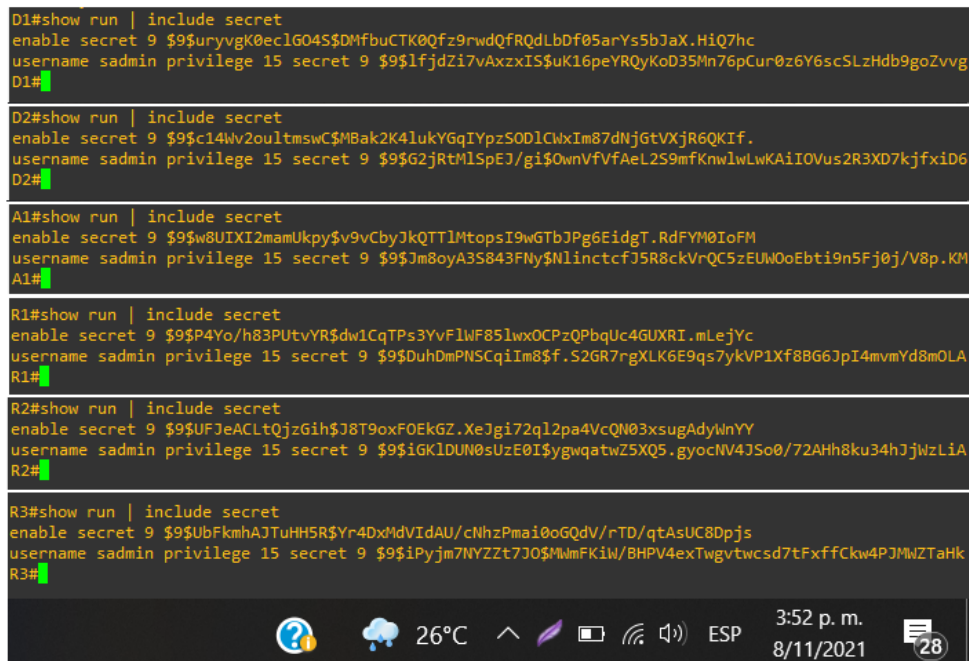
Switch D2:

```
D2(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

Switch A1:

```
A1(config)#username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco
```

Figura 12. Verificación de la creación de usuario y contraseñas.



```
D1#show run | include secret
enable secret 9 $9$uryvvgK0eclG04S$DMfbuCTK0Qfz9rwdQfRQdLbDf05arYs5bJaX.HiQ7hc
username sadmin privilege 15 secret 9 $9$1fjdzI7vAxzxIS$uK16peYRQyKoD35Mn76pCur0z6Y6scSLzHdb9goZvvg
D1#

D2#show run | include secret
enable secret 9 $9$c14wV2oultmswC$MBak2K4lukYGqIYpzSOD1CwXIm87dnJgtVXjR6QKIf.
username sadmin privilege 15 secret 9 $9$G2jRtM1SpEJ/gi$0wnVfVfAeL2S9mfKnlwLwKaiIOvus2R3XD7kfxiD6
D2#

A1#show run | include secret
enable secret 9 $9$w8UIXI2mamUkpy$V9vCbyJkQTT1MtopsI9wGTbJpg6EidgT.RdFYM0IoFM
username sadmin privilege 15 secret 9 $9$Jm8oyA3S843FNy$NlinctcfJ5R8ckVrQC5zEUW0oEbtI9n5Fj0j/V8p.KM
A1#

R1#show run | include secret
enable secret 9 $9$P4Yo/h83PUtvYR$dW1CqTPs3YvFlwF851wxOCPzQPbqUc4GUXRI.mLejYc
username sadmin privilege 15 secret 9 $9$DuhDmPNSCqiIm8$f.S2GR7rgXLK6E9qs7ykVP1Xf8BG6JpI4mvmYd8mOLA
R1#

R2#show run | include secret
enable secret 9 $9$UFJeACltQjzGih$J8T9oxFOEkGZ.XeJgi72q12pa4VcQN03xsugAdyWnYY
username sadmin privilege 15 secret 9 $9$iGKLDUN0sUzE0I$ygwqatwZ5XQ5.gyocNV4JSo0/72AHh8ku34hJjWzLiA
R2#

R3#show run | include secret
enable secret 9 $9$UbFkmhAJTuHH5R$Yr4DxMdVIdAU/cNhZPmai0oGQdV/rTD/qtAsUC8Dpjs
username sadmin privilege 15 secret 9 $9$iPyjm7NYZZt7J0$MwMFKiW/BHPV4exTwgvtwcds7tFxfCkw4PJMwZTaHk
R3#
```

Paso 3: En todos los dispositivos (excepto R2), habilite AAA.

Router R1:

```
R1(config)# aaa new-model
```

Router R3:

```
R3(config)# aaa new-model
```

Switch D1:

```
D1(config)#aaa new-model
```

Switch D2:

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

Switch A1:

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

Parte 4: En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

Router R1:

```
R1(config)#radius server RADIUS  
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
R1(config-radius-server)#key $trongPass
```

Router R3:

```
R3(config)#radius server RADIUS  
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
R3(config-radius-server)#key $trongPass
```

Switch D1:

```
D1(config)#radius server RADIUS  
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
D1(config-radius-server)#key $trongPass
```

Switch D2:

```
D2(config)#radius server RADIUS  
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
D2(config-radius-server)#key $trongPass
```

Switch A1:

```
A1(config)#radius server RADIUS  
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
A1(config-radius-server)#key $trongPass
```

Paso 5: En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

Router R1:

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

Router R3:

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

Switch D1:

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

Switch D2:

```
D2(config)#aaa authentication login default group radius local
```

Switch A1:

```
A1(config)#aaa authentication login default group radius local
```

Paso 6: Verifique el servicio AAA en todos los dispositivos (excepto R2).

Figura 13. Verificación de autenticación en los switches

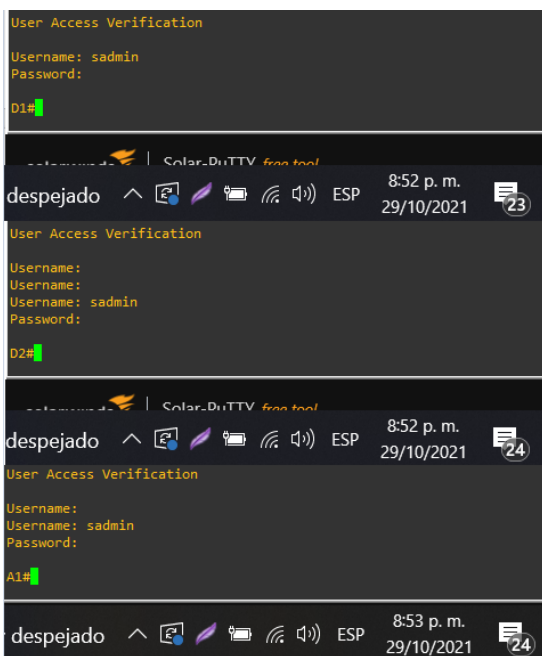
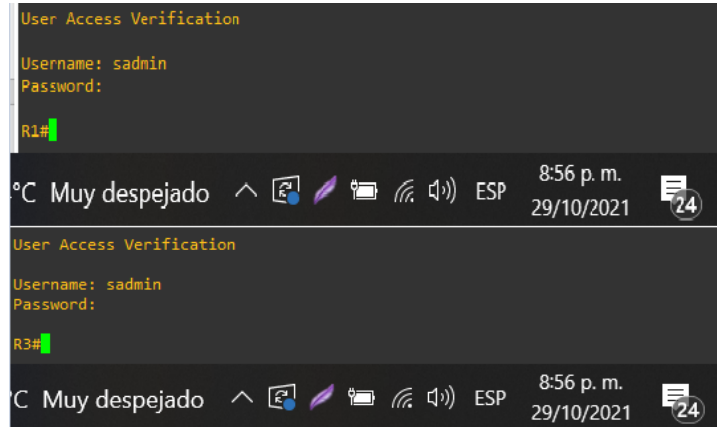


Figura 14. Verificación de autenticación routers



PARTE 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED

Paso 1: En todos los dispositivos, configure el reloj local a la hora UTC actual.

Router R1:

```
R1(config)# clock timezone UTC -5
```

Router R2:

```
R2(config)# clock timezone UTC -5
```

Router R3:

```
R3(config)# clock timezone UTC -5
```

Switch D1:

```
D1(config)# clock timezone UTC -5
```

Switch D2:

```
D2(config)# clock timezone UTC -5
```

Switch A1:

```
A1(config)#clock timezone UTC -5
```

Paso 2: Configure R2 como un NTP maestro.

Router R2:

```
R2(config)#ntp master 3
```

Paso 3: Configure NTP en R1, R3, D1, D2, y A1.

Router R1:

```
R1(config)#ntp server 209.165.200.226
```

Router R3:

```
R3(config)#ntp peer 10.0.13.1
```


Switch D1:

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

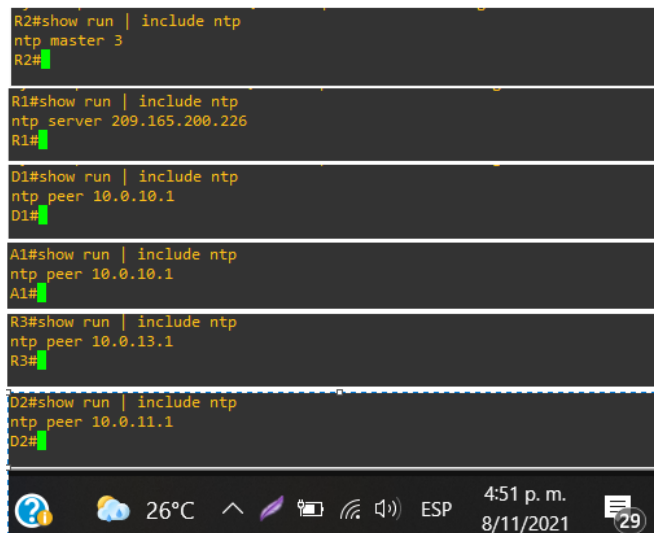
Switch D2:

```
D2(config)#ntp peer 10.0.11.1
```

Switch A1:

```
A1(config)#ntp peer 10.0.10.1
```

Figura 15. Verificación de la configuración NTP.



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

R1#show run | include ntp
ntp server 209.165.200.226
R1#

D1#show run | include ntp
ntp peer 10.0.10.1
D1#

A1#show run | include ntp
ntp peer 10.0.10.1
A1#

R3#show run | include ntp
ntp peer 10.0.13.1
R3#

D2#show run | include ntp
ntp peer 10.0.11.1
D2#
```

Paso 4: Configure Syslog en todos los dispositivos excepto R2

Router R1:

```
R1(config)# logging 10.0.100.5
R1(config)# logging trap warnings
```

Router R3:

```
R3(config)# logging 10.0.100.5
R3(config)# logging trap warnings
```

Switch D1:

```
D1(config)# logging 10.0.100.5
D1(config)# logging trap warnings
```

Switch D2:

```
D2(config)# logging 10.0.100.5
D2(config)# logging trap warnings
```

Switch A1:

```
A1(config)# logging 10.0.100.5
A1(config)# logging trap warnings
```

Paso 5: Configure SNMPv2c en todos los dispositivos excepto R2

Router R1:

```
R1(config)#snmp-server community ENCORSA RO
R1(config)#snmp-server host 10.0.100.5 ENCORSA
R1(config)#snmp-server contact HENRY_MEDINA
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
```

Router R3:

```
R3(config)#snmp-server community ENCORSA RO
R3(config)#snmp-server host 10.0.100.5 ENCORSA
R3(config)#snmp-server contact HENRY_MEDINA
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
```

Switch D1:

```
D1(config)#snmp-server community ENCORSA RO
D1(config)#snmp-server host 10.0.100.5 ENCORSA
D1(config)#snmp-server contact HENRY_MEDINA
D1(config)#snmp-server enable traps ospf
D1(config)#snmp-server enable traps config
```

Switch D2:

```
D2(config)#snmp-server community ENCORSA RO
D2(config)#snmp-server host 10.0.100.5 ENCORSA
D2(config)#snmp-server contact HENRY_MEDINA
D2(config)#snmp-server enable traps ospf
D2(config)#snmp-server enable traps config
```

Switch A1:

```
A1(config)#snmp-server community ENCORSA RO
A1(config)#snmp-server host 10.0.100.5 ENCORSA
A1(config)#snmp-server contact HENRY_MEDINA
A1(config)#snmp-server enable traps config
```

Figura 16. Verificación de la configuración SNMP.

```
R1#show run | include snmp
snmp-server community ENCORSA RO
snmp-server contact HENRY_MEDINA
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 ENCORSA
R1#

R3#show run | include snmp
snmp-server community ENCORSA RO
snmp-server contact HENRY_MEDINA
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 ENCORSA
R3#
```

```
D1#show run | include snmp
snmp-server community ENCORSA RO
snmp-server contact HENRY_MEDINA
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 ENCORSA
D1#
```

```
D2#show run | include snmp
snmp-server community ENCORSA RO
snmp-server contact HENRY_MEDINA
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 ENCORSA
D2#
```

```
A1#show run | include snmp
snmp-server community ENCORSA RO
snmp-server contact HENRY_MEDINA
snmp-server host 10.0.100.5 ENCORSA
A1#
```



26°C



ESP

5:04 p. m.
8/11/2021



29

CONCLUSIONES

Es interesante notar como se utiliza la combinación de técnicas y protocolos como: Redundancia de enlaces, Spanning tree y LACP para sacar el mejor provecho a la conexión en capa 2; donde el primero permite dar tolerancia a las fallas y protección contra la inoperatividad, el segundo asegura que solo exista una ruta lógica y evita bucles en estas redundancias, finalmente el LACP combina las redundancias físicas en un solo enlace lógico de alta velocidad; una combinación poderosa pero que se debe realizar con cuidado y en orden para no crear errores premeditados en la red.

Los protocolos de enrutamiento utilizados en este escenario OSPF y BGP son los más comunes que se pueden encontrar en un entorno real, muchas organizaciones utilizan el OSPF para enrutar como protocolo interno porque permite que se conozca toda la red a través de la tabla de enrutamiento de cada router evitando loops, también actualizan automáticamente las tables con cualquier cambio en la topología; el BGP para interconectar sistemas autónomos porque es normal que no todas las organizaciones utilicen el mismo protocolo de enrutamiento interno como lo es el ISP.

De acuerdo con lo expuesto anteriormente sobre la importancia de las redundancias a nivel de capa 3 también se utilizan para evitar que los dispositivos locales queden fuera de red por algún fallo en el Gateway, utilizando SLAs para monitorear continuamente las interfaces del Gateway y el protocolo HSRP para tener un router activo con la interfaz virtual y el otro de reserva.

A causa de la gran cantidad de amenazas que existen las redes es importante utilizar protocolos para reforzar la seguridad e integridad de los dispositivos de interconexión locales, en este escenario se utiliza la familia AAA donde verifica que un usuario de ingreso es quien dice decir, le da unos privilegios preestablecidos por el administrador y además registra todos los eventos en modo de logs para poder determinar las acciones realizadas.

BIBLIOGRAFÍA

- AREAIP. (2016). *Comandos Ethernetchannel o Portchannel con LACP y PAGP*. Obtenido de http://areaip.blogspot.com/2016/09/comandos-ethernetchannel-o-portchannel_24.html
- BITACORDABYTE. (18 de Julio de 2017). *Configurar DHCP en router CISCO*. Obtenido de <https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/>
- CISCO. (26 de Octubre de 2005). *How to Configure SNMP Community Strings*. Obtenido de <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html>
- CISCO. (26 de Noviembre de 2020). *Cómo Configurar OSPF*. Obtenido de <https://ccnadesdecero.com/curso/como-configurar-ospf/>
- CISCO. (11 de Junio de 2020). *RSTP: Configuración*. Obtenido de <https://ccnadesdecero.com/curso/rstp-configuracion/>
- Eugenio, G. (24 de Agosto de 2020). *Como configurar IP SLA tracking*. Obtenido de <https://estudiaredes.com/cisco/como-configurar-ip-sla-tracking/>
- Fernández Sánchez, A. (s.f.). *¿Cómo configurar NTP en Cisco?* Obtenido de <https://network-tic.com/como-configurar-ntp-en-cisco/>
- NetworkLessons. (s.f.). *Multiprotocol BGP (MP-BGP) Configuration*. Obtenido de <https://networklessons.com/bgp/multiprotocol-bgp-mp-bgp-configuration>
- Raponi, D. (18 de Julio de 2018). *Cómo configurar el protocolo de enrutamiento de espera activa (HSRP) con un router Cisco*. Obtenido de <https://thesolving.com/es/sala-de-servidores/como-configurar-hot-standby-router-protocol-hsrp-con-un-router-cisco/>
- Rosales, D. (2015). *AAA en Routers & Switches Cisco*. Obtenido de <https://delfirosales.blogspot.com/2014/04/aaa-en-routers-switches-cisco.html>
- Zamorano, M. (30 de Abril de 2019). *CONFIGURAR ENRUTAMIENTO OSPF CON IPV6*. Obtenido de <https://www.maxizamorano.com/entrada/3/configurar-enrutamiento-ospf-con-ipv6/>