DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS

LEIDER TORRES PADILLA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LEIDER TORRES PADILLA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

VALLEDUPAR, 29 de noviembre de 2021

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi tutor Héctor Julián Parra, quien con sus conocimientos y apoyo me guio a través de cada una de las etapas de este proyecto para alcanzar los resultados que buscaba.

También quiero agradecer a la universidad nacional abierta y a distancia UNAD, por brindarme todos los recursos y herramientas que fueron necesarios para llevar a cabo el proceso de investigación. No hubiese podido arribar a estos resultados de no haber sido por su incondicional ayuda.

Por último, quiero agradecer a todos mis compañeros y a mi familia, por apoyarme. En especial, quiero mencionar a mi esposa e hijos, que siempre estuvieron ahí para darme palabras de apoyo y un abrazo reconfortante para renovar energías.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Loopback: es una interfaz de red virtual. Las direcciones del rango '127.0.0.0/8' son direcciones de loopback, de las cuales se utiliza, de forma mayoritaria, la '127.0.0.1' por ser la primera de dicho rango, añadiendo '::1' para el caso de IPv6 ('127.0.0.1::1').

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

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa OSI 3 y 4).

Gateway: La pasarela (en inglés gateway) o puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.

Enrutamiento: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla.

NTP: El Network Time Protocol (NTP) es ampliamente utilizado para sincronizar un ordenador a los Servidores de tiempo de Internet o a otras fuentes, tales como una radio o receptores satelitales o servicios del módem del teléfono. La exactitud es típicamente menos de un milisegundo en las LAN y hasta algunos milisegundos en las WAN. Las configuraciones NTP típicas utilizan servidores redundantes múltiples y diversos trayectos de red para alcanzar una elevada precisión y confiabilidad.

RESUMEN

El presente documento es una prueba de habilidades, se 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 entrada predeterminada.

Para este propósito de debe de cumplir los objetivos propuestos por este trabajo y construir la red configurando los ajustes básicos para cada dispositivo, configurar la capa 2 de la red y el host, configurar los protocolos de enrutamiento, configurar la redundancia del primer salto la seguridad de la red y las características de administración de la misma.

Para el desarrollo de este trabajo se requiere de una sólida comprensión de los protocolos comunes de la industria junto con la arquitectura y configuración de los dispositivos y lo que hace valioso este diplomado, es que, mediante la obtención del título y el certificado correspondiente, se genera credibilidad en el campo laboral y académico, lo que nos abre puertas para podernos desempeñar en el cada vez más basto mundo de las redes.

ABSTRACT

This document is a skills test, network configuration must be completed for full end-to-end accessibility, so that hosts have reliable support of the default gateway.

For this purpose, you must meet the objectives proposed by this work and build the network by configuring the basic settings for each device, configure layer 2 of the network and the host, configure the routing protocols, configure the redundancy of the first jump, security. network and network management features.

For the development of this work, a solid understanding of the common protocols of the industry is required together with the architecture and configuration of the devices and what makes this diploma valuable is that, by obtaining the title and the corresponding certificate, generates credibility in the labor and academic field, which opens doors for us to be able to perform in the increasingly vast world of networks.

INTRODUCCIÓN

El presente documento comprende el desarrollo de la propuesta presentada por este diplomado de Profundización CISCO CCNP. se desarrollan las respectivas competencias describiendo el problema identificado para ser resuelto con conocimientos disciplinares de la ingeniería electrónica y/o de telecomunicaciones, el cual debe estar relacionado con los ejes y líneas de investigación de la cadena de formación en Electrónica, Telecomunicaciones y Redes CISCO CCNP.

Se plante dar solución al escenario planteado en este curso utilizando los conocimientos adquiridos en el desarrollo de este diplomado.

Como primer paso se realiza la construcción y el cableado de la red de acuerdo con la topología dada y es implementada en packet tracer; luego, se configuran los parámetros básicos de cada dispositivo teniendo presente la tabla de direccionamiento IP.

ADEMAS, se configura la capa 2 de la red y el soporte de host; para ello, en todos los DISPOSITIVOS se configura interfaces troncales, se habilita el protocolo RSTP, se crean EtherChannels y se configuran los puertos de acceso del host. Los enrutadores D1 y D2 se configuran como root para las VLAN indicadas. Finalmente se verifican los servicios DHCP IPv4 y se verifica la conectividad de la LAN local. Para la tercera parte se configuran los protocolos de enrutamiento para IPv4 e IPv6 como son OSPFv2 y OSPFv3 y se configura MP – BGP. En la cuarta parte se configura la redundancia del primer salto HSRP versión 2 para proveer la redundancia de primer salto para los hosts en la red de la compañía. La quinta parte consiste en configurar diversos mecanismos de seguridad en los dispositivos, tales como la protección del EXEC privilegiado usando el algoritmo de encriptación SCRIPT, la habilitación de AAA, la configuración de las especificaciones del servidor RADIUS y configurando la lista de métodos de autenticación AAA. Para finalizar en la sexta parte del trabajo se configuran las funciones de administración de red configurando NTP, syslog y SNMPv2.

ESCENARIO PROPUESTO

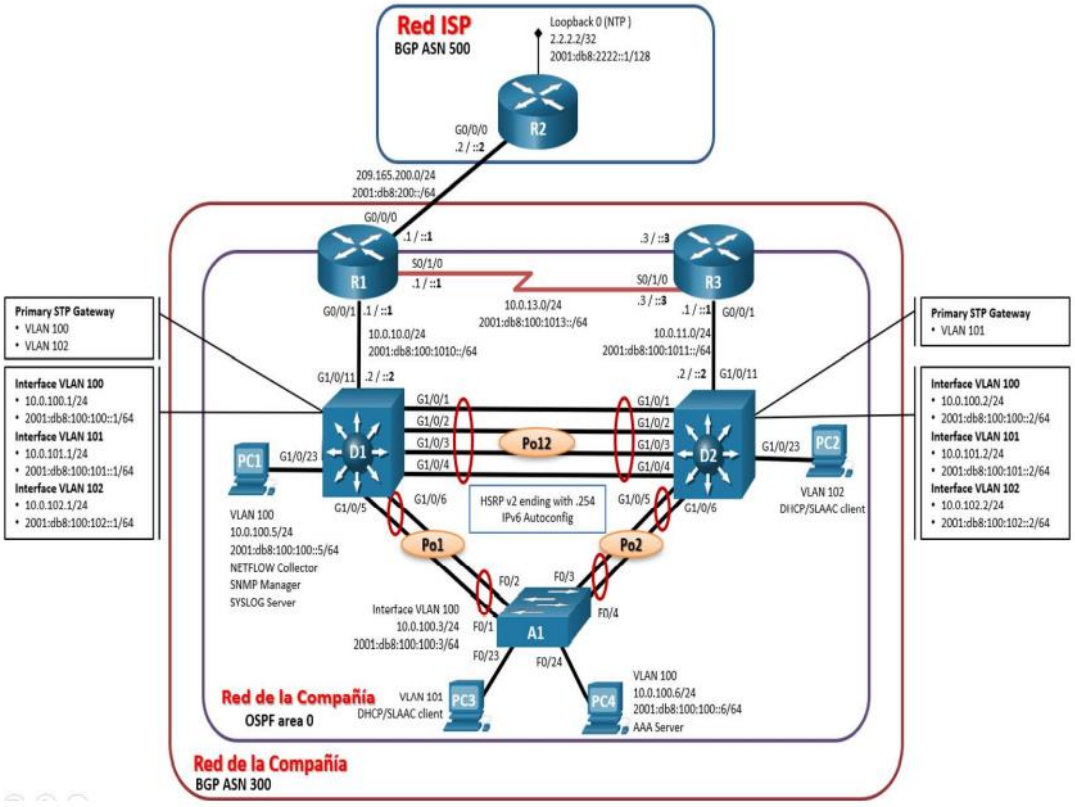

Figura 1. Topología de red escenario propuesto

DESARROLLO

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.

Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS.

Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

OBJETIVOS

- Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
- Configurar la capa 2 de la red y el soporte de Host
- Configurar los protocolos de enrutamiento
- Configurar la redundancia del primer salto
- Configurar la seguridad
- Configurar las características de administración de red

RECURSOS NECESARIOS

- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 2 switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PCs (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
- Los cables Ethernet y seriales van como se muestra en la topología

Parte 1: construir la red y configurar los parámetros básicos de los Dispositivos y el direccionamiento de las interfaces.

Para el desarrollo de esta actividad se utilizó el software packet tracer, que nos permite simular diferentes tipos de router y configurarlos de la manera en la que se haría en la vida real.

PASO 1: CABLEAR LA RED COMO SE MUESTRA EN LA TOPOLOGÍA.

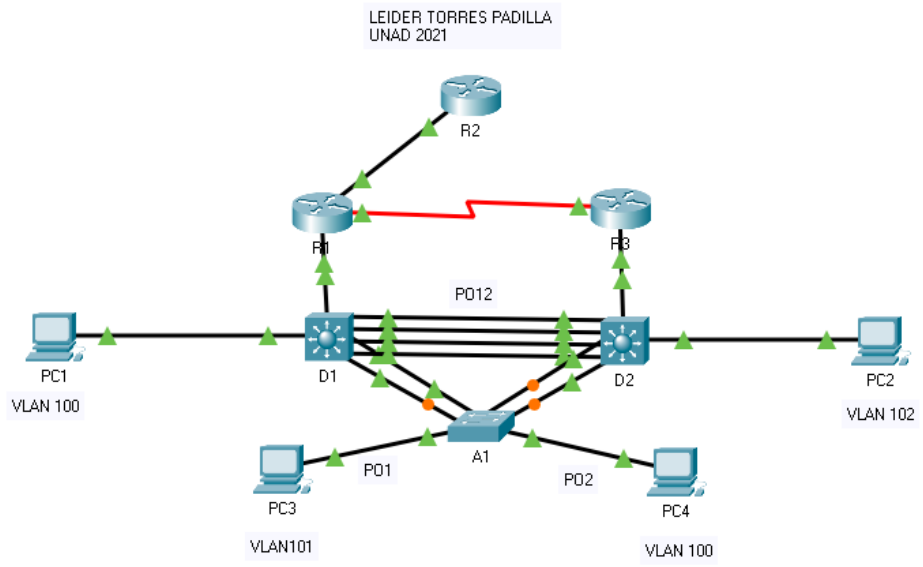

Figura 2. Escenario propuesto

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

Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Tabla 2. Tabla de direccionamiento IP

Dispositivo	Interfaz	IPv4	IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G0/0/11	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	G0/0/11	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
	VLAN102	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

ROUTER R1 CONFIGURACIÓN

⇒ hostname R1
⇒ ipv6 unicast-routing
⇒ no ip domain lookup
⇒ banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
⇒ line con 0
⇒ exec-timeout 0 0
⇒ logging synchronous
⇒ exit
⇒ interface g0/0/0
⇒ ip address 209.165.200.225 255.255.255.224
⇒ ipv6 address fe80::1:1 link-local
⇒ ipv6 address 2001:db8:200::1/64
⇒ no shutdown
⇒ exit
⇒ interface g0/0/1
⇒ ip address 10.0.10.1 255.255.255.0
⇒ ipv6 address fe80::1:2 link-local
⇒ ipv6 address 2001:db8:100:1010::1/64
⇒ no shutdown
⇒ exit
⇒ interface s0/1/0
⇒ ip address 10.0.13.1 255.255.255.0
⇒ ipv6 address fe80::1:3 link-local
⇒ ipv6 address 2001:db8:100:1013::1/64
⇒ no shutdown
⇒ exit
⇒

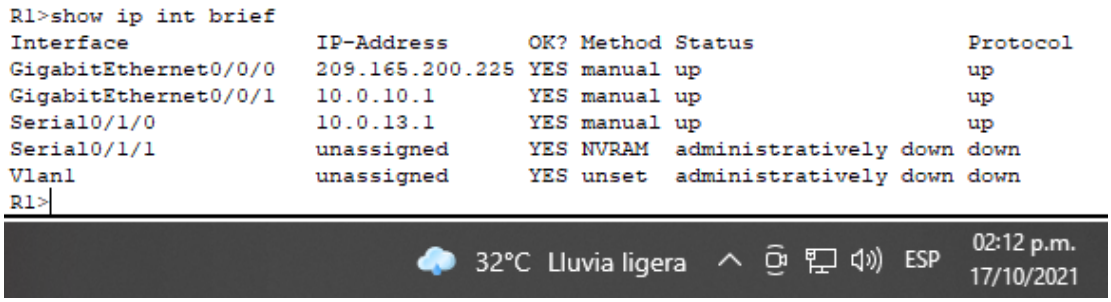

Figura 3. Configuración básica Router R1

ROUTER R2 CONFIGURACIÓN

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

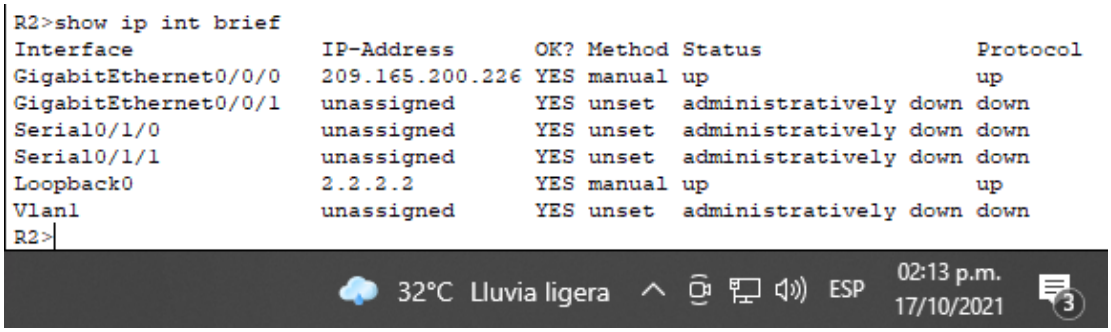

Figura 4. Configuración básica Router R2

ROUTER R3 CONFIGURACIÓN

⇒ hostname R3
⇒ ipv6 unicast-routing
⇒ no ip domain lookup
⇒ banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
⇒ line con 0
⇒ exec-timeout 0 0
⇒ logging synchronous
⇒ exit
⇒ interface g0/0/1
⇒ ip address 10.0.11.1 255.255.255.0
⇒ ipv6 address fe80::3:2 link-local
⇒ ipv6 address 2001:db8:100:1011::1/64
⇒ no shutdown
⇒ exit
⇒ interface s0/1/0
⇒ ip address 10.0.13.3 255.255.255.0
⇒ ipv6 address fe80::3:3 link-local
⇒ ipv6 address 2001:db8:100:1013::3/64
⇒ no shutdown
⇒ exit

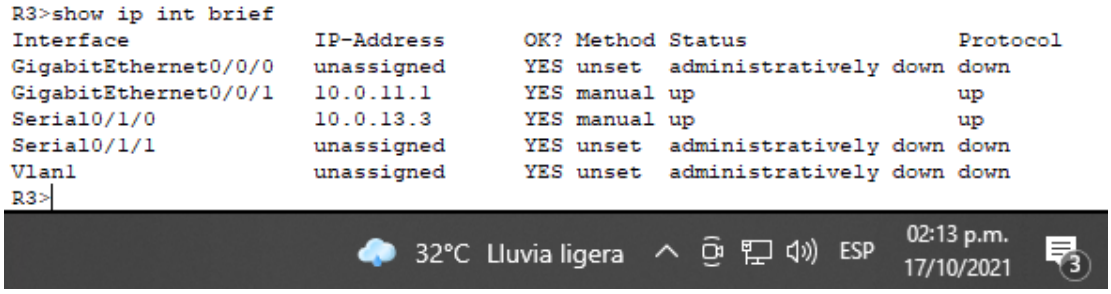

Figura 5. Configuración básica Router R1

SWITCH D1 CONFIGURACIÓN

⇒ hostname D1
⇒ ip routing
⇒ ipv6 unicast-routing
⇒ no ip domain lookup
⇒ banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
⇒ line con 0
⇒ exec-timeout 0 0
⇒ logging synchronous
⇒ exit
⇒ vlan 100
⇒ name Management
⇒ exit
⇒ vlan 101
⇒ name UserGroupA
⇒ exit
⇒ vlan 102
⇒ name UserGroupB
⇒ exit
⇒ vlan 999
⇒ name NATIVE
⇒ exit
⇒ interface g1/0/11
⇒ no switchport
⇒ ip address 10.0.10.2 255.255.255.0
⇒ ipv6 address fe80::d1:1 link-local
⇒ ipv6 address 2001:db8:100:1010::2/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 100
⇒ ip address 10.0.100.1 255.255.255.0
⇒ ipv6 address fe80::d1:2 link-local
⇒ ipv6 address 2001:db8:100:100::1/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 101
⇒ ip address 10.0.101.1 255.255.255.0
⇒ ipv6 address fe80::d1:3 link-local
⇒ ipv6 address 2001:db8:100:101::1/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 102
⇒ ip address 10.0.102.1 255.255.255.0

⇒ ipv6 address fe80::d1:4 link-local
⇒ ipv6 address 2001:db8:100:102::1/64
⇒ no shutdown
⇒ exit
⇒ ip dhcp excluded-address 10.0.101.1 10.0.101.109
⇒ ip dhcp excluded-address 10.0.101.141 10.0.101.254
⇒ ip dhcp excluded-address 10.0.102.1 10.0.102.109
⇒ ip dhcp excluded-address 10.0.102.141 10.0.102.254
⇒ ip dhcp pool VLAN-101
⇒ network 10.0.101.0 255.255.255.0
⇒ default-router 10.0.101.254
⇒ exit
⇒ ip dhcp pool VLAN-102
⇒ network 10.0.102.0 255.255.255.0
⇒ default-router 10.0.102.254
⇒ exit
⇒ interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
⇒ shutdown
⇒ exit

SWITCH D2 CONFIGURACIÓN

⇒ hostname D2
⇒ ip routing
⇒ ipv6 unicast-routing
⇒ no ip domain lookup
⇒ banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
⇒ line con 0
⇒ exec-timeout 0 0
⇒ logging synchronous
⇒ exit
⇒ vlan 100
⇒ name Management
⇒ exit
⇒ vlan 101
⇒ name UserGroupA
⇒ exit
⇒ vlan 102
⇒ name UserGroupB
⇒ exit
⇒ vlan 999
⇒ name NATIVE
⇒ exit
⇒ interface g1/0/11
⇒ no switchport
⇒ ip address 10.0.11.2 255.255.255.0
⇒ ipv6 address fe80::d1:1 link-local
⇒ ipv6 address 2001:db8:100:1011::2/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 100
⇒ ip address 10.0.100.2 255.255.255.0
⇒ ipv6 address fe80::d2:2 link-local
⇒ ipv6 address 2001:db8:100:100::2/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 101
⇒ ip address 10.0.101.2 255.255.255.0
⇒ ipv6 address fe80::d2:3 link-local
⇒ ipv6 address 2001:db8:100:101::2/64
⇒ no shutdown
⇒ exit
⇒ interface vlan 102
⇒ ip address 10.0.102.2 255.255.255.0

⇒ ipv6 address fe80::d2:4 link-local
⇒ ipv6 address 2001:db8:100:102::2/64
⇒ no shutdown
⇒ exit
⇒ ip dhcp excluded-address 10.0.101.1 10.0.101.209
⇒ ip dhcp excluded-address 10.0.101.241 10.0.101.254
⇒ ip dhcp excluded-address 10.0.102.1 10.0.102.209
⇒ ip dhcp excluded-address 10.0.102.241 10.0.102.254
⇒ ip dhcp pool VLAN-101
⇒ network 10.0.101.0 255.255.255.0
⇒ default-router 10.0.101.254
⇒ exit
⇒ ip dhcp pool VLAN-102
⇒ network 10.0.102.0 255.255.255.0
⇒ default-router 10.0.102.254
⇒ exit
⇒ interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
⇒ shutdown
⇒ exit

SWITCH A1 CONFIGURACIÓN

⇒ hostname A1
⇒ no ip domain lookup
⇒ banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
⇒ line con 0
⇒ exec-timeout 0 0
⇒ logging synchronous
⇒ exit
⇒ vlan 100
⇒ name Management
⇒ exit
⇒ vlan 101
⇒ name UserGroupA
⇒ exit
⇒ vlan 102
⇒ name UserGroupB
⇒ exit
⇒ vlan 999
⇒ name NATIVE
⇒ exit
⇒ interface vlan 100
⇒ ip address 10.0.100.3 255.255.255.0
⇒ ipv6 address fe80::a1:1 link-local
⇒ ipv6 address 2001:db8:100:100::3/64
⇒ no shutdown
⇒ exit
⇒ interface range f0/5-22
⇒ shutdown
⇒ exit

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

⇒ Copy running-config startup-config

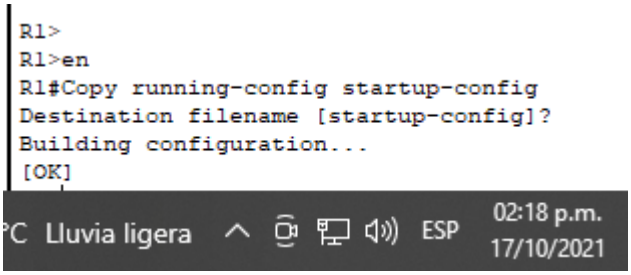

Figura 6 Copia de configuración básica del router R1

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

utilizada en la Parte 4.

⇒ Ipconfig

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2E0:F7FF:FEE6:1A55
   IPv6 Address.....: 2001:DB8:100:100::5
   IPv4 Address.....: 10.0.100.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.0.100.254

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Figura 7. Configuración PC1

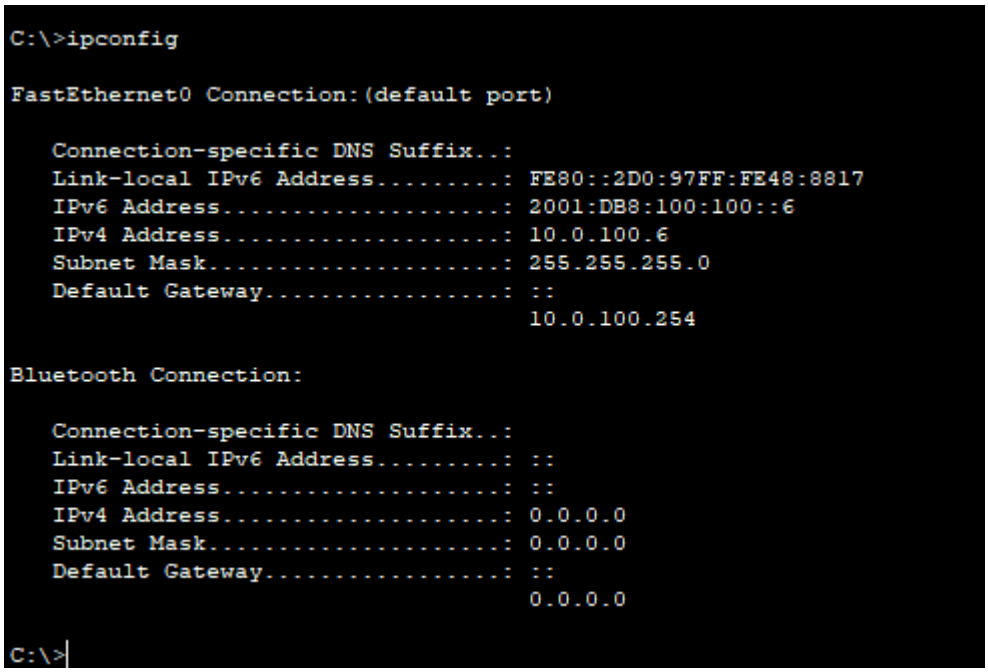

Figura 8. configuración PC4

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

Las tareas de configuración son las siguientes:

- ⇒ Config t
- ⇒ Int range g1/0/1-4
- ⇒ Switchport trunk encap dot1q
- ⇒ Switchport mode trunk
- ⇒ Switchport trunk native vlan 999
- ⇒ Exit

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Po1, Po12, Gig1/0/1, Gig1/0/2
                                                 Gig1/0/3, Gig1/0/4, Gig1/0/7, Gig1/0/8
                                                 Gig1/0/9, Gig1/0/10, Gig1/0/12, Gig1/0/13
                                                 Gig1/0/14, Gig1/0/15, Gig1/0/16,
Gig1/0/17
                                                 Gig1/0/18, Gig1/0/19, Gig1/0/20,
Gig1/0/21
                                                 Gig1/0/22, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                 Gig1/1/3, Gig1/1/4
100  Management                        active    Gig1/0/23
101  UserGroupA                        active
102  UserGroupB                        active
999  NATIVE                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
 --More--
```


Figura 9. Configuración troncal D1

```
D2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Po2, Po12, Gig1/0/1, Gig1/0/2
                                                 Gig1/0/3, Gig1/0/4, Gig1/0/7, Gig1/0/8
                                                 Gig1/0/9, Gig1/0/10, Gig1/0/12, Gig1/0/13
                                                 Gig1/0/14, Gig1/0/15, Gig1/0/16,
Gig1/0/17
                                                 Gig1/0/18, Gig1/0/19, Gig1/0/20,
Gig1/0/21
                                                 Gig1/0/22, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                 Gig1/1/3, Gig1/1/4
100  Management                        active
101  UserGroupA                        active
102  UserGroupB                        active    Gig1/0/23
999  NATIVE                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
101  enet  100101     1500  -      -      -        -    -        0      0
102  enet  100102     1500  -      -      -        -    -        0      0
```


Figura 10. Configuración troncal D2

⇒ Int range g1/0/5-6
⇒ switchport mode trunk
⇒ switchport trunk native vlan 999
⇒ channel-group 1 mode active
⇒ no shutdown
⇒ Int range g1/0/1-4
⇒ switchport mode trunk
⇒ switchport trunk native vlan 999
⇒ channel-group 12 mode active
⇒ no shutdown

Configuración D2

⇒ Int range g1/0/5-6
⇒ switchport mode trunk
⇒ switchport trunk native vlan 999
⇒ channel-group 2 mode active
⇒ no shutdown

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.

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Habilite enlaces trunk 802.1Q entre:

- D1 and D2
- D1 and A1
- D2 and A1

⇒ Show int g1/0/1 switchport

⇒ Show vlan

```
D2#show int g1/0/1 switchport
Name: Gig1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 102
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Figura 11. Interface G1/0/1 mode Trunk

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

Use VLAN 999 como la VLAN nativa.

```
D2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po2, Po12, Gig1/0/1, Gig1/0/2
                                                Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6
                                                Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/24
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
100  Management                       active
101  UserGroupA                       active
102  UserGroupB                       active    Gig1/0/23
999  NATIVE                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
101  enet  100101     1500  -      -      -        -    -        0      0
102  enet  100102     1500  -      -      -        -    -        0      0
999  enet  100999     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

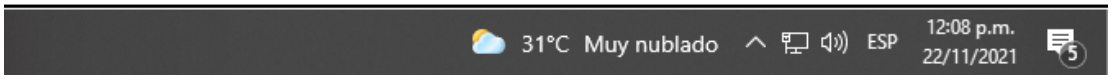

Figura 12. Vlan 999 native en D2

```
                                                Gig0/1, Gig0/2
100  Management                       active    Fa0/24
101  UserGroupA                       active    Fa0/23
102  UserGroupB                       active
999  NATIVE                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
 --More--
```

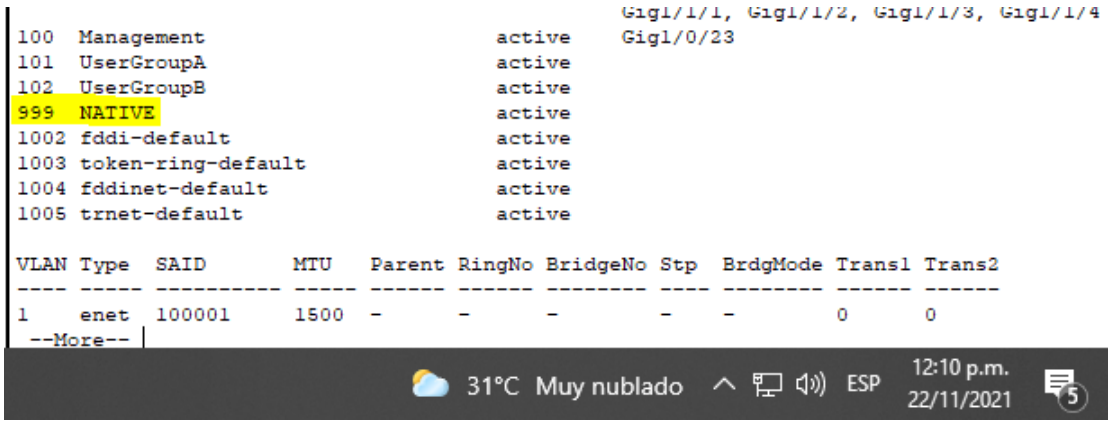

Figura 13. Vlan 999 native en D1

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

Use Rapid Spanning Tree (RSPT).

⇒ en
⇒ config t
⇒ spanning-tree mode rapid-pvst
⇒ exit

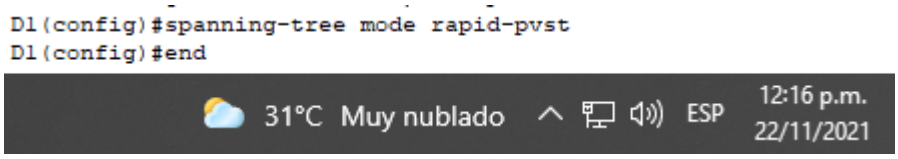

Figura 14. Protocolo Rapid Spanning-Tree (RSTP) en D1

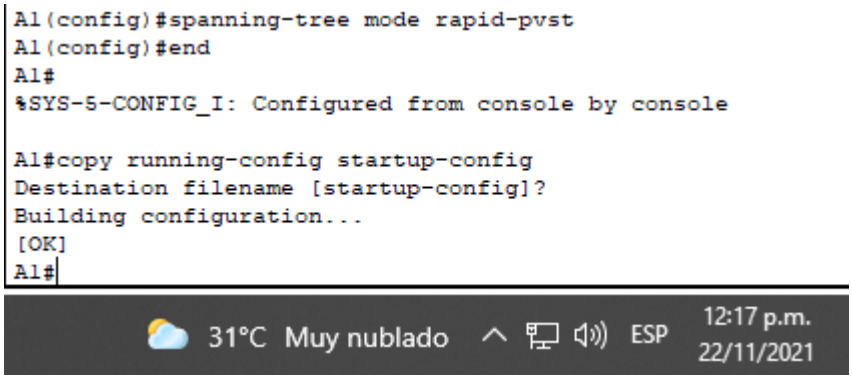

Figura 15. Protocolo Rapid Spanning-Tree (RSTP) en A1

```
D2(config)#spanning-tree mode rapid-pvst
D2(config)#end
D2#
%SYS-5-CONFIG_I: Configured from console by console

D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

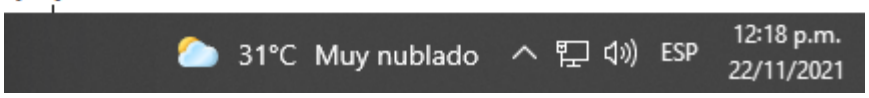

Figura 16. protocolo Rapid Spanning-Tree (RSTP) en D2

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.

⇒ en
⇒ config t
⇒ spanning-tree vlan 101 priority 4096
⇒ exit

```
D2(config)#spanning-tree vlan 101 priority 4096
D2(config)#end
D2#
%SYS-5-CONFIG_I: Configured from console by console

D2#wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
D2#
```

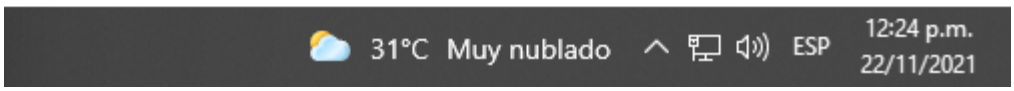

Figura 17. D1 y D2 como raíz (root)

⇒ en
⇒ config t
⇒ spanning-tree vlan 100 priority 4096

⇒ exit

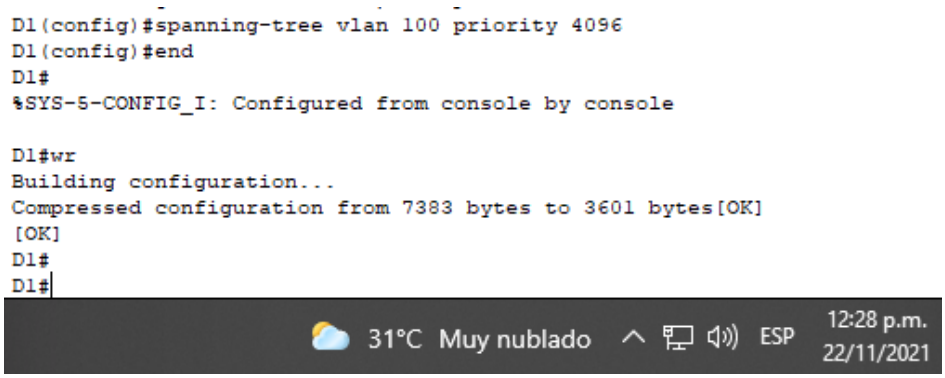

Figura 18. D1 y D2 Vlan 100 como prioridad

⇒ Show spanning-tree

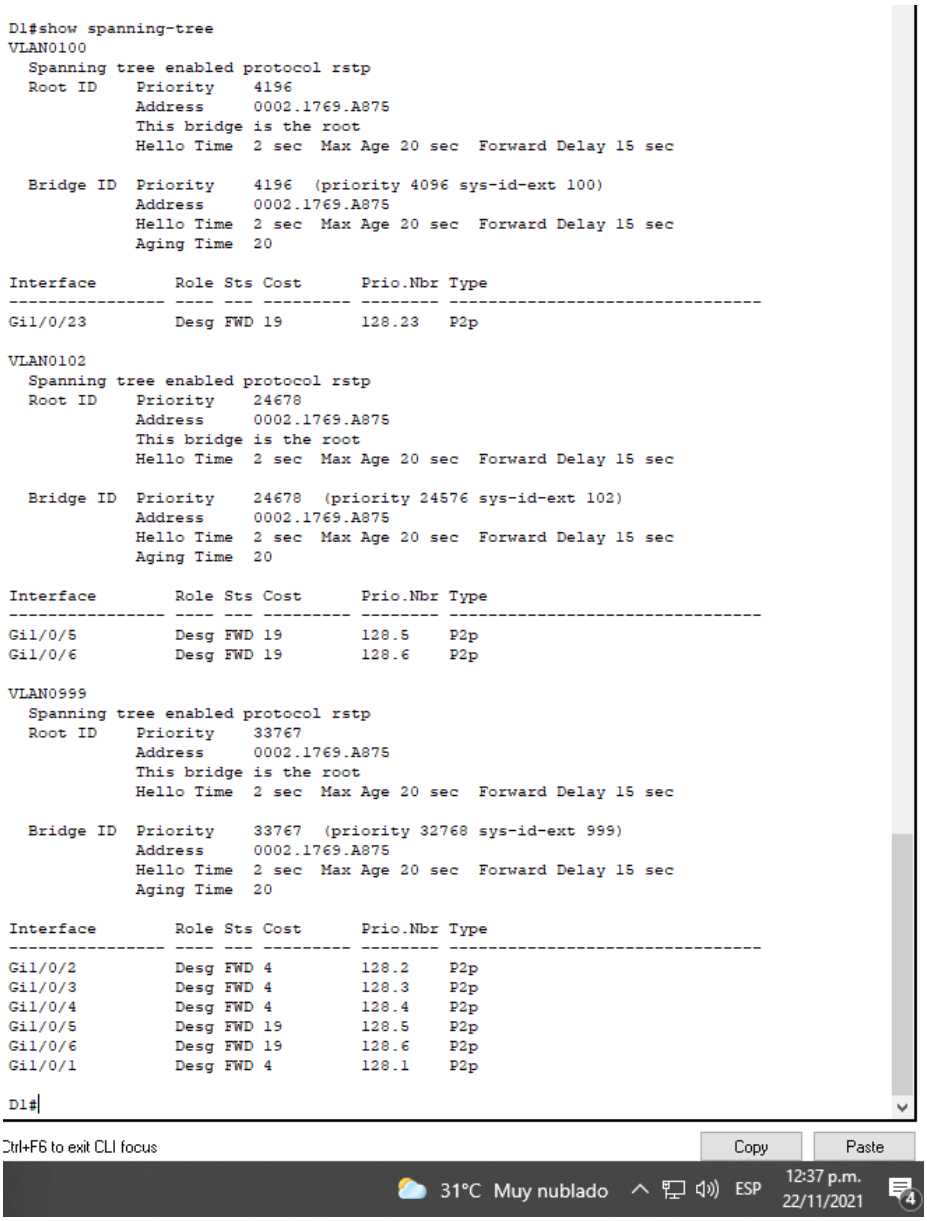

Figura 19. Show spanning-tree

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

⇒ en

⇒ config t
⇒ int range g1/0/1-4
⇒ channel-group 12 mode active
⇒ exit

- D1 a A1 – Port channel 1

⇒ en
⇒ config t
⇒ int range g1/0/5-6
⇒ channel-group 1 mode active
⇒ exit

- D2 a A1 – Port channel 2

⇒ en
⇒ config t
⇒ int range g1/0/5-6
⇒ channel-group 2 mode active
⇒ exit

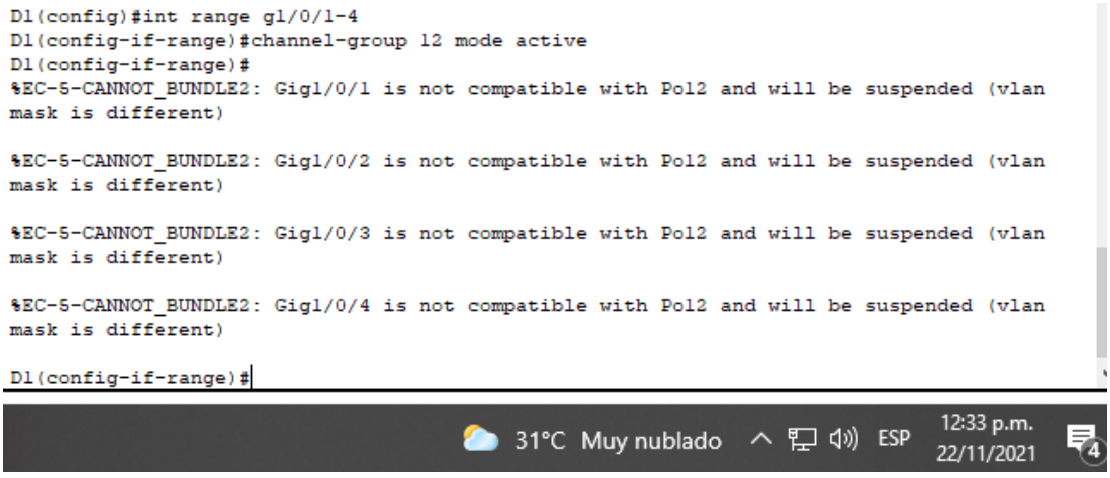

Figura 20. D1 a D2 – Port channel 12

```
D1(config)#int range g1/0/5-6
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#
%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po1 and will be suspended (vlan
mask is different)

%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po1 and will be suspended (vlan
mask is different)

D1(config-if-range)#
```

31°C Muy nublado ESP 12:34 p.m. 22/11/2021

Figura 21. D1 a A1 – Port channel 1

```
D2(config)#int range g1/0/5-6
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#
%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po2 and will be suspended (vlan mask is different)

%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po2 and will be suspended (vlan mask is different)

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

31°C Muy nublado ESP 12:35 p.m. 22/11/2021

Figura 22. 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).

```
D1(config)#int g1/0/23
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#
```

31°C Muy nublado ESP 12:47 p.m. 22/11/2021

Figura 23. Int G1/0/23 en vlan 100

D1 a PC1

⇒ en
⇒ config t
⇒ int g1/0/23
⇒ switchport mode access
⇒ switchport access vlan 102
⇒ exit

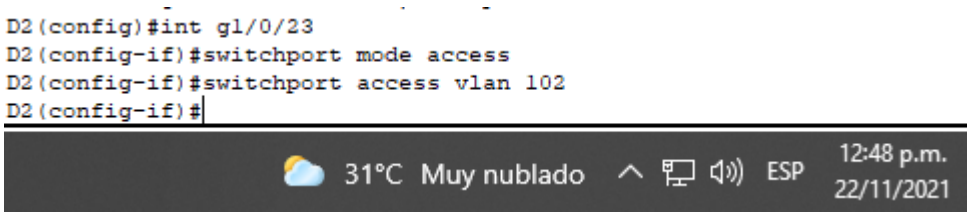

Figura 24. Int G1/0/23 en vlan 102

D2 a PC2

⇒ en
⇒ config t
⇒ int g1/0/23
⇒ switchport mode access
⇒ switchport access vlan 101
⇒ exit

Figura 25. Int Fa/23 en vlan 101

2.7 Verifique los servicios DHCP IPv4

PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

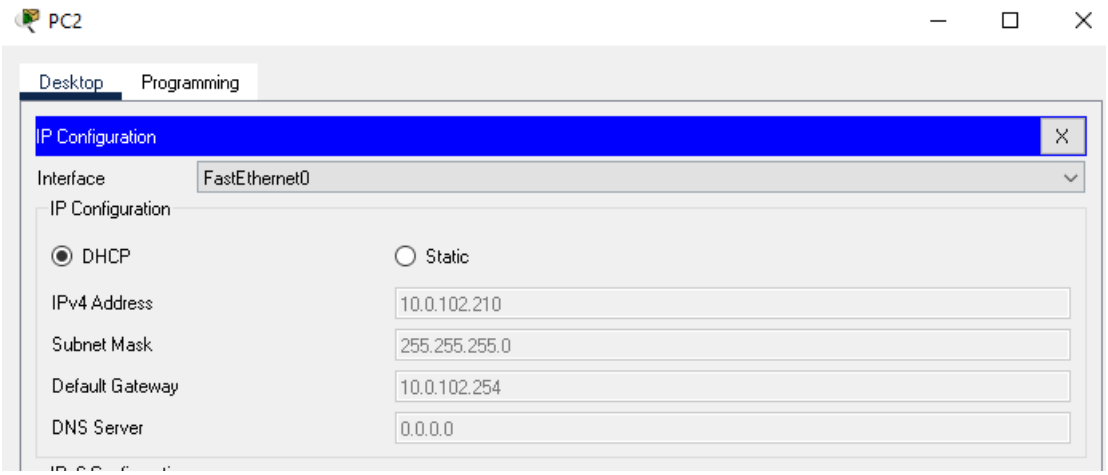

Figura 26. DHCP PC

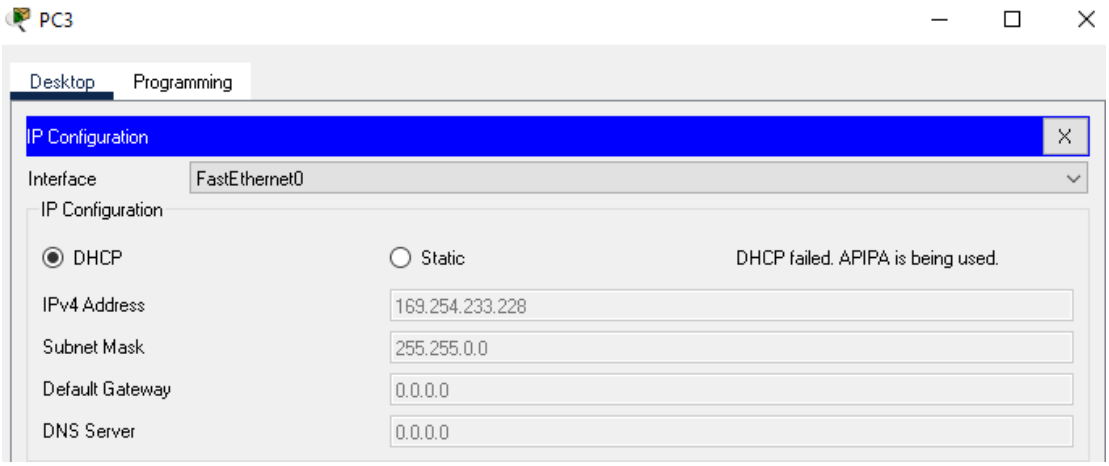

Figura 27. DHCP PC3

2.8 Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

• D1: 10.0.100.1

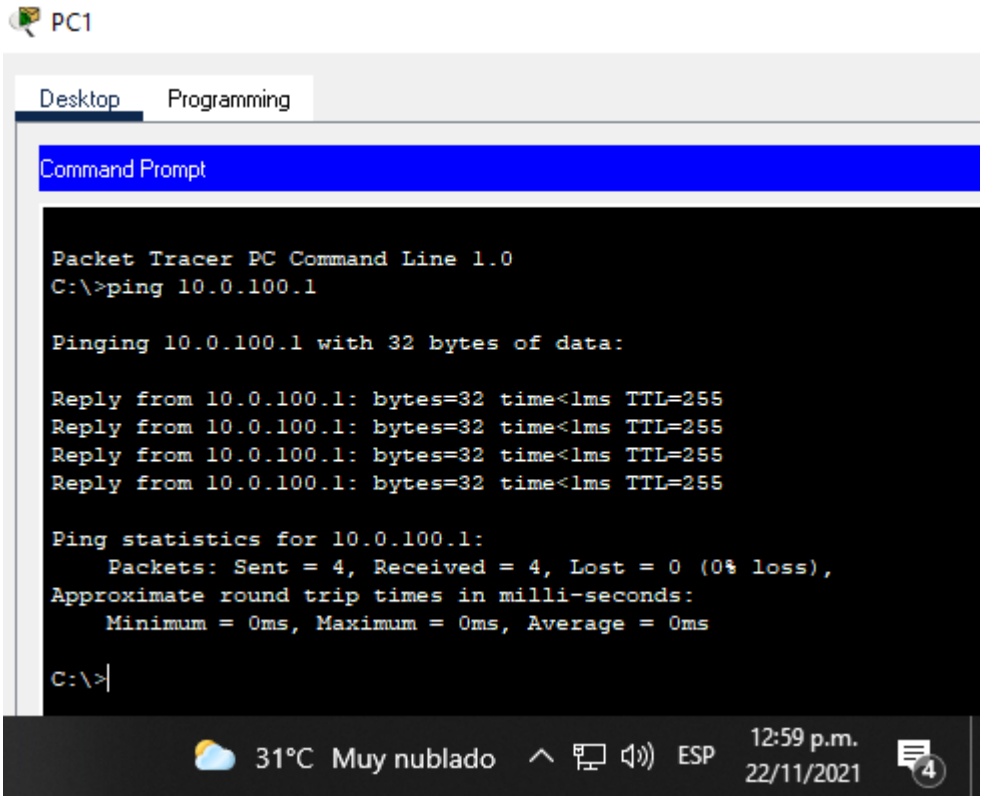

Figura 28. Ping PC1

PC2 debería hacer ping con éxito a:

• D1: 10.0.102.1

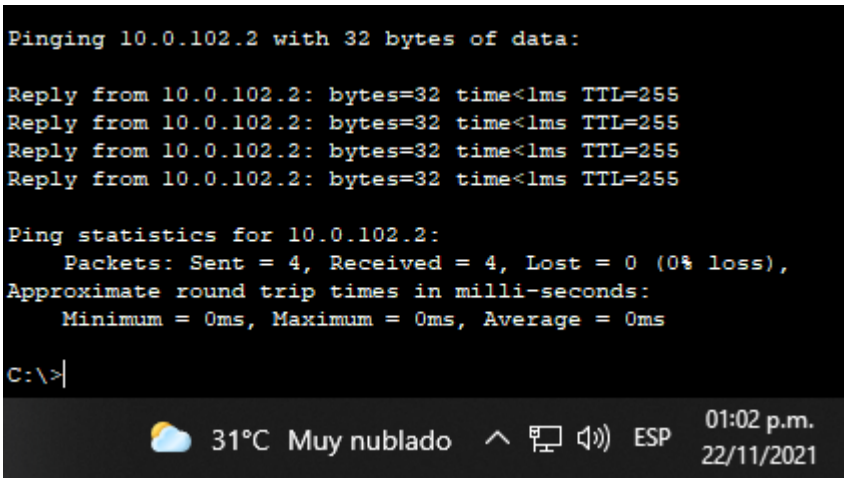

Figura 29. Ping PC2

• D2: 10.0.101.2 PC4 debería hacer ping con éxito a:

• D2: 10.0.100.2

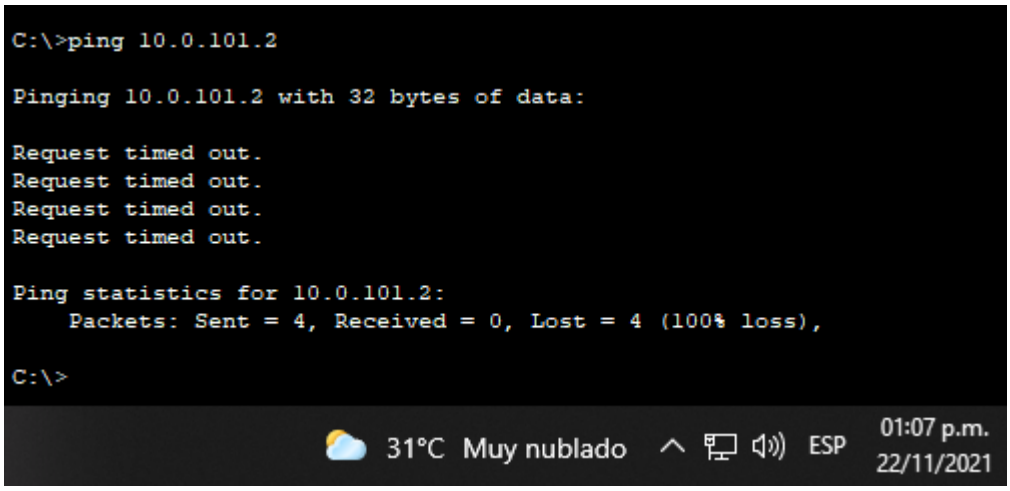

Figura 30. Ping PC3

Parte 3: Configurar los protocolos de enrutamiento

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

3.1 En la “Red de la compañía” (es decir, R1, R3, D1, y D2), configure single área OSPFv2 en área 0.

se OSPF Process ID 4 y asigne los siguientes router IDs:

• R1: 0.0.4.1

- ⇒ En
- ⇒ Config t
- ⇒ Router ospf 4
- ⇒ Network 0.0.4.1 0.0.0.255 area 0
- ⇒ exit

• R3: 0.0.4.3

- ⇒ En
- ⇒ Config t
- ⇒ Router ospf 4
- ⇒ Network 0.0.4.3 0.0.0.255 area 0
- ⇒ exit

• D1: 0.0.4.131

- ⇒ En
- ⇒ Config t
- ⇒ Router ospf 4
- ⇒ Network 0.0.4.131 0.0.0.255 area 0
- ⇒ exit

• D2: 0.0.4.132

⇒ En
⇒ Config t
⇒ Router ospf 4
⇒ Network 0.0.4.132 0.0.0.255 area 0
⇒ exit

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

- En R1, no publique la red R1 – R2.
- En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en:
- D1: todas las interfaces excepto G1/0/11
- D2: todas las interfaces excepto G1/0/11

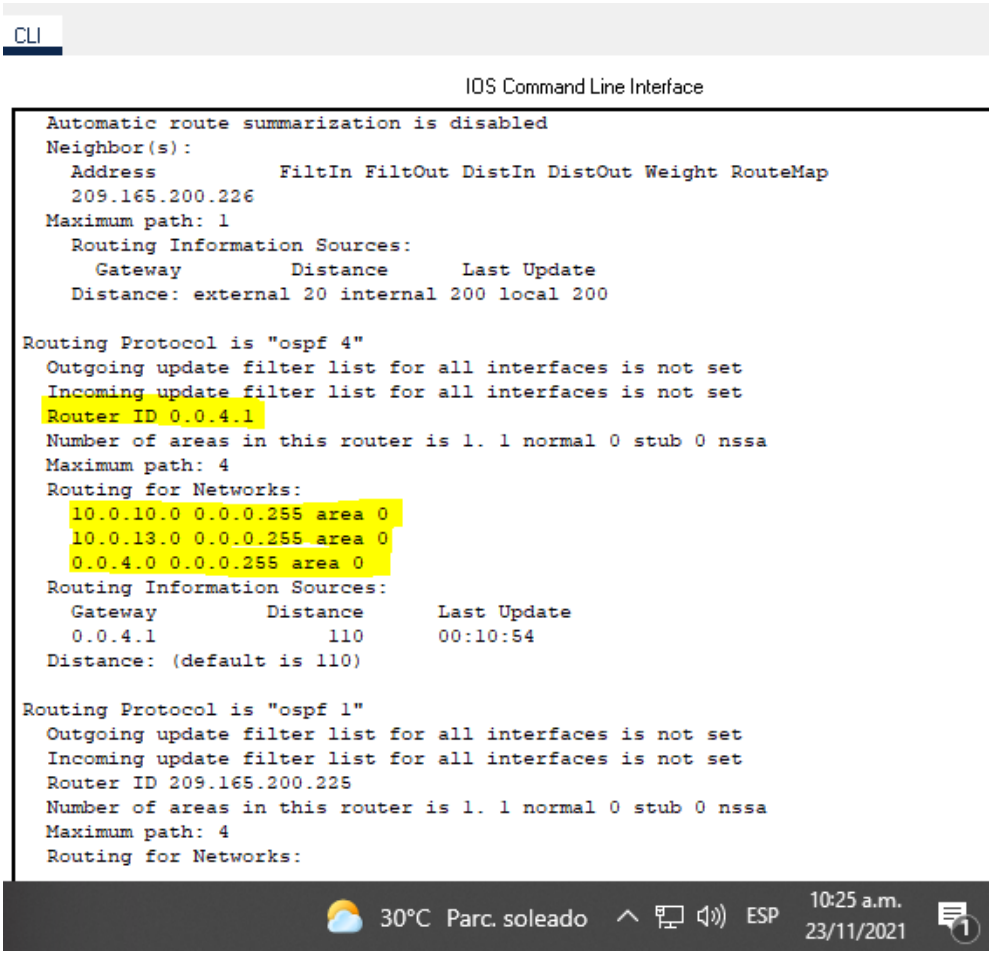

Figura 31. Show OSPF R1

3.2 En la “Red de la compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.

Use OSPF Process ID 6 y asigne los siguientes router IDs:

• R1: 0.0.6.1

⇒ En
⇒ Config t
⇒ Router ospf 6
⇒ Network 0.0.6.1 0.0.0.255 área 0
⇒ exit

• R3: 0.0.6.3

⇒ En
⇒ Config t
⇒ Router ospf 6
⇒ Network 0.0.6.3 0.0.0.255 área 0
⇒ exit

• D1: 0.0.6.131

⇒ En
⇒ Config t
⇒ Router ospf 6
⇒ Network 0.0.6.131 0.0.0.255 área 0
⇒ exit

• D2: 0.0.6.132

⇒ En
⇒ Config t
⇒ Router ospf 6
⇒ Network 0.0.6.132 0.0.0.255 área 0
⇒ exit

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

- 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. Deshabilite las publicaciones OSPFv3 en:
- D1: todas las interfaces excepto G1/0/11
- D2: todas las interfaces excepto G1/0/11

3.3 En R2 en la “Red ISP”, configure MP-BGP.

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

• Una ruta estática predeterminada IPv4.

⇒ en
⇒ config t
⇒ ip route 2.2.2.2 255.255.255.255.255 209.165.200.225
⇒ exit

• Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie:

⇒ en
⇒ config t
⇒ neighbor 2.2.2.2 remote-as 2
⇒ exit

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie:
- La red Loopback 0 IPv4 (/128).
- La ruta por defecto (::/0).

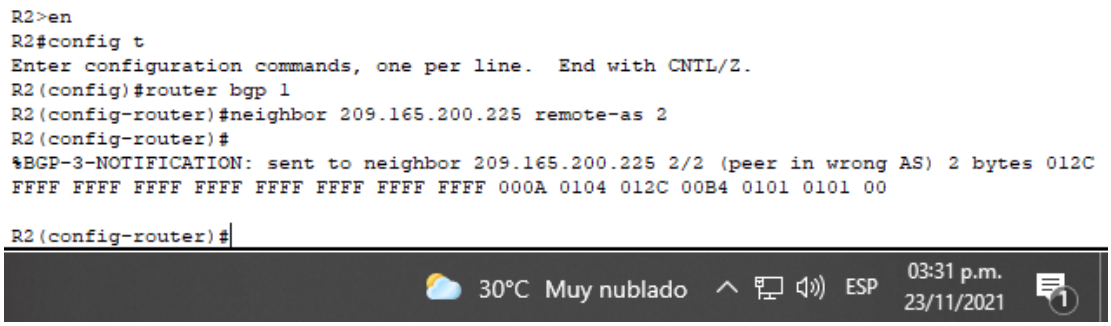

Figura 32. Configuración BGP

3.4 Configuración de MP-BGP en la red ISP de R1

⇒ R1(config)#ip route 10.0.0.0 255.0.0.0
⇒ null0
⇒ R1(config)#ipv6 route
⇒ 2001:db8:100::/48 null0
⇒ R1(config)#router bgp 300
⇒ R1(config-router)#bgp router-id 1.1.1.1
⇒ R1(config-router)#neighbor
⇒ 209.165.200.226 remote-as 500
⇒ R1(config-router)#neighbor
⇒ 2001:db8:200::2 remote-as 500
⇒ R1(config-router)#address-family ipv4
⇒ unicast
⇒ R1(config-router-af)#neighbor
⇒ 209.165.200.226 activate
⇒ R1(config-router-af)#no neighbor
⇒ 2001:db8:200::2 activate
⇒ R1(config-router-af)#network 10.0.0.0
⇒ mask 255.0.0.0
⇒ R1(config-router-af)#exit-address-family
⇒ R1(config-router)#address-family ipv6
⇒ unicast
⇒ R1(config-router-af)#no neighbor
⇒ 209.165.200.226 activate
⇒ R1(config-router-af)#neighbor
⇒ 2001:db8:200::2 activate
⇒ R1(config-router-af)#network
⇒ 2001:db8:100::/48
⇒ R1(config-router-af)#exit-address-family

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

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

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1. Para nuestro caso, la interfaz es la R1 G1/0.

- ⇒ D1(config)#ip sla 4
- ⇒ D1(config-ip-sla)#icmp-echo 10.0.10.1
- ⇒ D1(config-ip-sla-echo)#frequency 5
- ⇒ D1(config-ip-sla-echo)#exit
- ⇒ D1(config)#ip sla 6
- ⇒ D1(config-ip-sla)#icmp-echo
- ⇒ 2001:db8:100:1010::1
- ⇒ D1(config-ip-sla-echo)#frequency 5
- ⇒ D1(config-ip-sla-echo)#exit
- ⇒ D1(config)#ip sla schedule 4 life forever
- ⇒ start-time now
- ⇒ D1(config)#ip sla schedule 6 life forever

⇒
⇒ start-time now
⇒ D1(config)#track 4 ip sla 4
⇒ D1(config-track)#delay down 10 up 15
⇒ D1(config-track)#exit
⇒ D1(config)#track 6 ip sla 6
⇒ D1(config-track)#delay down 10 up 15
⇒ D1(config-track)#exit

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1. Para nuestro caso, la interfaz es la R3 G0/0.

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

4.3 Configurando HSRPv2 en D1.

⇒ D1(config)#interface vlan 100
⇒ D1(config-if)# standby version 2
⇒ D1(config-if)# standby 104 ip
⇒ 10.0.100.254
⇒ D1(config-if)# standby 104 priority 150
⇒ D1(config-if)# standby 104 preempt
⇒ D1(config-if)#standby 104 track 4
⇒ decrement 60
⇒ D1(config-if)#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

Configurando HSRPv2 en 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)# exi

Parte 5: Seguridad

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

Contraseña: cisco12345cisco

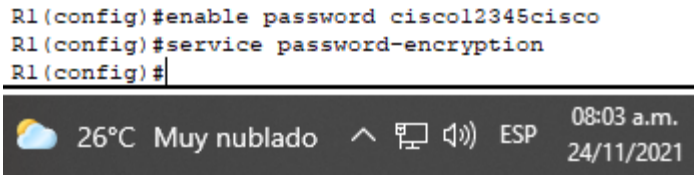

Figura 33. Enable encripción SCRYPT R1

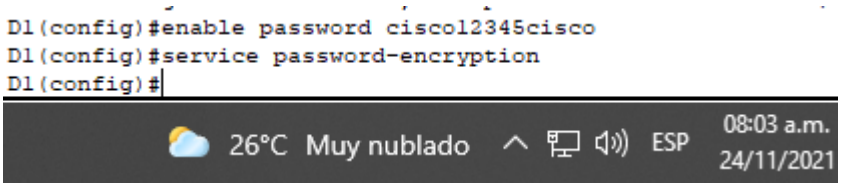

Figura 34. Enable encripción SCRYPT D1

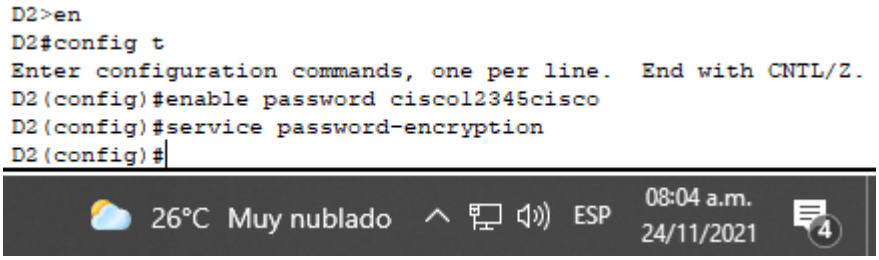

Figura 35. Enable encripción SCRYPT D2

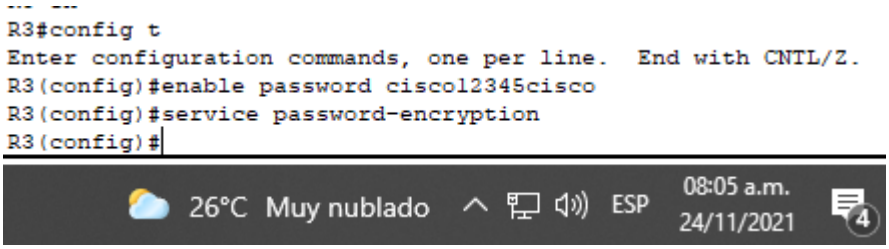

Figura 36. Enable encripción SCRYPT R3

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.
Detalles de la cuenta encriptada SCRYPT:

- Nombre de usuario Local: sadmin
- Nivel de privilegio 15
- Contraseña: cisco12345cisco

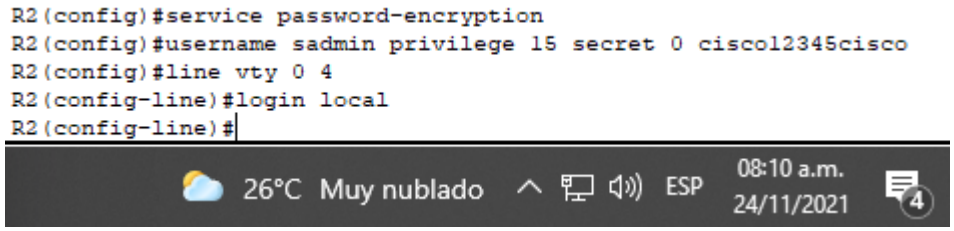

Figura 37. algoritmo de encripción SCRYPT R2

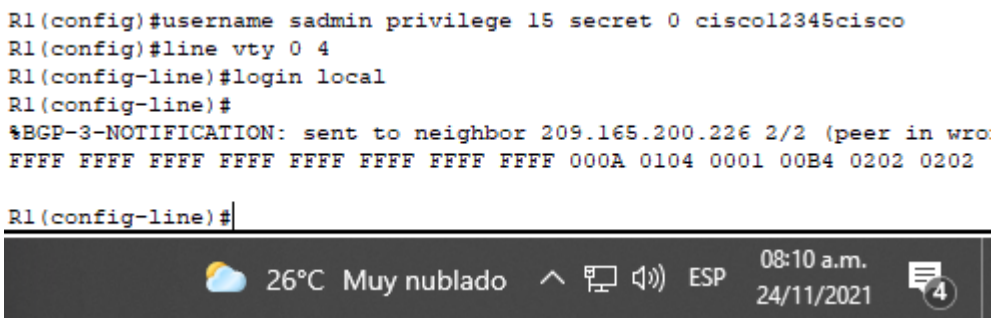

Figura 38. algoritmo de encripción SCRYPT R1

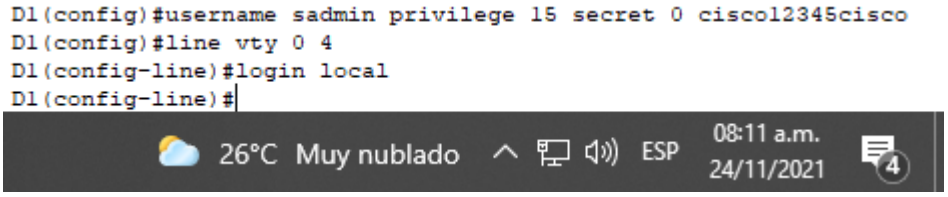

Figura 39. algoritmo de encripción SCRYPT D1

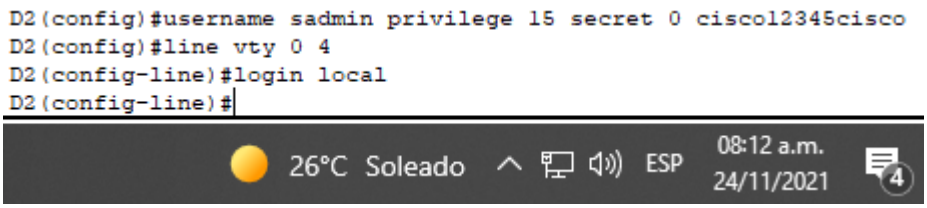

Figura 41. algoritmo de encripción SCRYPT D2

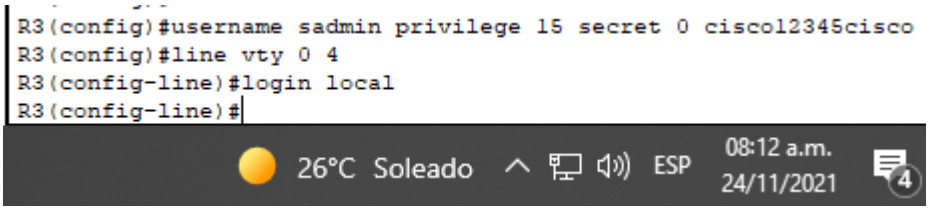

Figura 42. algoritmo de encripción SCRYPT R3

5.3 En todos los dispositivos (excepto R2), habilite AAA.

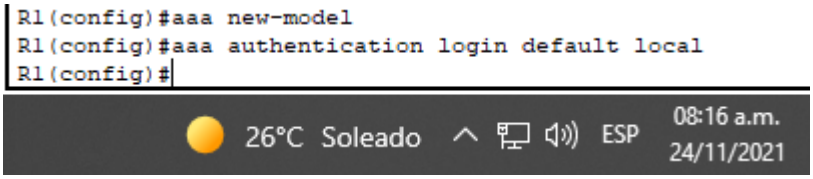

Figura 43. AAA en R1

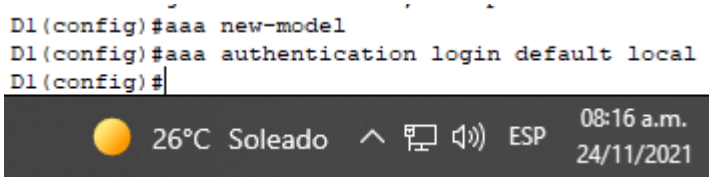

Figura 44. AAA en D1

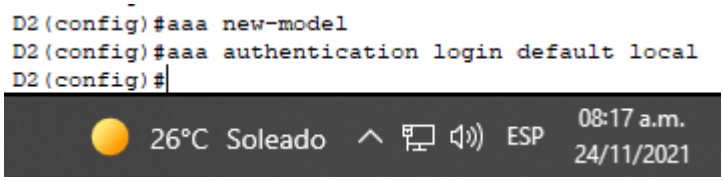

Figura 45. AAA en D2

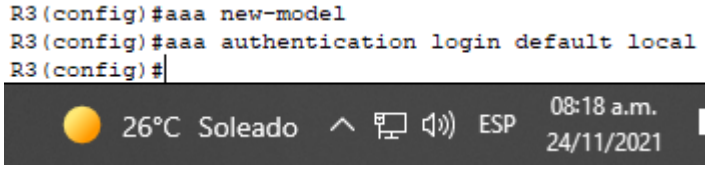

Figura 46. AAA en R3

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

⇒ 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
⇒ R1(config-radius-server)# exit

⇒ 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
⇒ R3(config-radius-server)# exit

⇒ 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
⇒ D1(config-radius-server)# exit
⇒ 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
⇒ D2(config-radius-server)# exit

⇒ 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
⇒ A1(config-radius-server)# exit

NOTA: estas configuraciones no fueron soportadas por el software packet tracer, pero se deja evidencia de cómo se debería configurar.

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

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

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

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

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

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

NOTA: estas configuraciones no fueron soportadas por el software packet tracer, pero se deja evidencia de cómo se debería configurar.

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

NOTA: estas configuraciones no fueron soportadas por el software packet tracer, pero se deja evidencia de cómo se debería configurar.

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:

6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.

Configure el reloj local a la hora UTC actual.

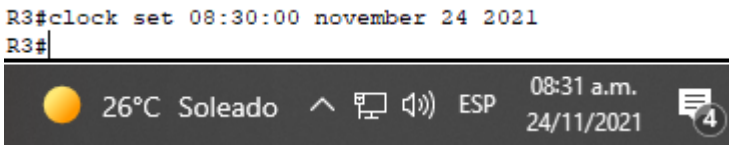

Figura 47. Clock set en R3

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.

⇒ R1(config)#ntp server 2.2.2.2
⇒ R3(config)#ntp server 10.0.10.1
⇒ D1(config)#ntp server 10.0.10.1
⇒ A1(config)#ntp server 10.0.10.1
⇒ D2(config)#ntp server 10.0.10.1
⇒ R2(config)#ntp master 3

Configure NTP de la siguiente manera:

- 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.

⇒ R1(config)# logging host 10.0.100.5
⇒ R1(config)#logging trap warning
⇒ R1(config)#logging on

⇒ R3(config)# logging on
⇒ R3(config)# logging host 10.0.100.5
⇒ R3(config)#logging trap warning

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

⇒ D2(config)#logging host 10.0.100.5
⇒ D2(config)#logging trap warning
⇒ D2(config)# logging on

⇒ A1(config)#logging host 10.0.100.5
⇒ A1(config)#logging trap warning
⇒ A1(config)#logging on

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

⇒ R1(config)# snmp-server community ENCORSA ro SNMP-NMS
⇒ R1(config)#ip access-list standard SNMP-NMS
⇒ R1(config-std-nacl)# permit host 10.0.100.5
⇒ R1(config-std-nacl)# exit
⇒ R1(config)#snmp-server contact leider torres
⇒ R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
⇒ R1(config)#snmp-server enable traps bgp
⇒ R1(config)# snmp-server enable traps config
⇒ R1(config)#snmp-server enable traps ospf
⇒ R1(config)#end

⇒ R3(config)# snmp-server community ENCORSA ro SNMP-NMS
⇒ R3(config)#ip access-list standard SNMP-NMS
⇒ R3(config-std-nacl)# permit host 10.0.100.5
⇒ R3(config)# exit
⇒ R3(config)# snmp-server contact leider torres

⇒ R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
⇒ R3(config)# snmp-server enable traps config
⇒ R3(config)# snmp-server enable traps ospf
⇒ R3(config)#end

⇒ D1(config)# snmp-server community ENCORSA ro SNMPNMS
⇒ 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 Leider Torres
⇒ D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
⇒ D1(config)# snmp-server enable traps config
⇒ D1(config)# snmp-server enable traps ospf
⇒ D1(config)#end

⇒ 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 Leider Torres
⇒ D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
⇒ D2(config)# snmp-server enable traps config
⇒ D2(config)# snmp-server enable traps ospf
⇒ End

⇒ A1(config)#snmp-server community ENCORSA ro SNMP-NMS
⇒ A1(config)#ip access-list standard SNMP-NMS
⇒ A1(config-std-nacl)# permit host 10.0.100.5
⇒ A1(config-std-nacl)#exit
⇒ A1(config)# snmp-server contact Leider Torres
⇒ A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
⇒ A1(config)# snmp-server enable
⇒ traps config
⇒ A1(config)#end

CONCLUSIONES

Por medio de este documento se describe cómo utilizar Cisco packet tracer para establecer la configuración básica de Routers y switches. La configuración básica del router incluye la configuración de la dirección IP para cada una de las interfaces usadas en este proyecto.

Por medio de esta actividad se pudo concluir que, Para configurar un puerto de switch en un extremo de un enlace troncal, se utiliza el comando switchport mode trunk. Con este comando, la interfaz cambia al modo de enlace troncal permanente. El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio. El comando switchport mode trunk es el único método que se implementa para la configuración de enlaces troncales.

También se implementó la configuración del protocolo OSPF, En una red OSPF, los direccionadores o sistemas de la misma área mantienen una base de datos de enlace-estado idéntica que describe la topología del área. Cada direccionador o sistema del área genera su propia base de datos de enlace-estado a partir de los anuncios de enlace-estado (LSA) que recibe de los demás direccionadores o sistemas de la misma área y de los LSA que él mismo genera. El LSA es un paquete que contiene información sobre los vecinos y los costes de cada vía. Basándose en la base de datos de enlace-estado, cada direccionador o sistema calcula un árbol de extensión de vía más corta, siendo él mismo la raíz, utilizando el algoritmo SPF.

Se implemento el protocolo de redundancia de primer salto, que no es mas que la capacidad que tiene una red para recuperarse dinámicamente de la falla de un dispositivo que funciona como gateway predeterminado.

Se estableció la seguridad de la red, Para proteger el acceso a EXEC privilegiado, utilizando el comando enable secret contraseña. El comando enable secret proporciona mayor seguridad, dado que la contraseña está encriptada.

Por ultimo se configuraron las características de administración de la red, el cual es el proceso de preparación de los dispositivos, puesto que la configuración de éstos determina el comportamiento de los datos en la red.

BIBLIOGRAFÍA

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!AAIGg5JUgUBthk8

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

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

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

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

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

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