# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRES LEON DOMINGUEZ

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

# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CAMILO ANDRES LEON DOMINGUEZ

Diplomado de opción de grado presentado para optar el
título de INGENIER**O ELECTRONICO**

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

**BOGOTÁ,** 07 de diciembre de 2021

AGRADECIMIENTOS

Me permito agradecer la dirección de mis amigos Julián Jiménez y Carlos Peñaranda quienes estuvieron pendientes y al tanto de los trabajos para realizar observaciones oportunas.

También me permito agradecer a mi familia, mi tía Gladys Domínguez quien me apoya económica y moralmente y a mi mama Luz Marina Domínguez quien me ha impulsado a terminar mis metas a corto plazo para mejorar mi futuro.

CONTENIDO

LISTA DE TABLAS

# LISTA DE FIGURAS

# GLOSARIO

SWITCH CISCO: son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus

ROUTER CISCO: Un router recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switches de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales.

ENLACE TRONCAL: Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. Más adelante en esta sección, aprenderá acerca de 802.1Q.

DISPOSITIVOS DE NETWORKING: Un dispositivo de interconexión de redes es un término ampliamente utilizado para cualquier hardware que conecte diferentes recursos de red. Los dispositivos clave que comprenden una red son conmutadores, enrutadores, brigde (puentes), repetidores y puertas de enlace.

GNS3: Es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

HSRP: El Hot Standby Router Protocol (o HSRP por sus siglas en inglés) es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos (single point of failure) en la red mediante técnicas de redundancia y comprobación del estado de los routers. Evitar puntos únicos de fallo en la red es muy importante para dotar de alta disponibilidad al servicio de red. Es un protocolo muy similar a VRRP, que no es propietario. Es por ello que CISCO reclama que VRRP viola una serie de patentes que le pertenecen.

## RESUMEN

Teniendo en cuenta la topología presentada para esta prueba de habilidades prácticas CCNP se realiza la configuración de una red en CISCO que incluye IPv4 e IPv6 comenzando con la configuración básica de los dispositivos con el fin de tener una conmutación completa desde un extremo a otro configurando los defaults Gateway. Se tiene en cuenta también la configuración de las VLAN el protocolo de enrutamiento OSPF, conexión DHCP y SLAAC. Seguidamente se procede a configurar el protocolo de enrutamiento y HSRP terminando con la configuración de seguridad para todos los dispositivos.



PALABRAS CLAVE: CCNP, CISCO, OSPF, DHCP, SLAAC, VLAN, topología, defaults Gateway, conmutación.



## ABSTRACT

Taking into account the topology presented for this CCNP practical skills test, the configuration of a network is carried out in CISCO that includes IPv4 and IPv6, starting with the basic configuration of the devices in order to have a complete switch from one end to the other by configuring the devices. Gateway defaults. The configuration of the VLANs, the OSPF routing protocol, DHCP connection and SLAAC are also taken into account. Next, we proceed to configure the routing protocol and HSRP, ending with the security configuration for all devices.



KEYWORDS: CCNP, CISCO, OSPF, DHCP, SLAAC, VLAN, topology, Gateway defaults, switching.

# INTRODUCCIÓN

Teniendo en cuenta la topología suministrada para este proyecto perteneciente al diplomado de profundización CCNP, se realiza la configuración de un escenario mediante la herramienta Packet Tracert. Con el fin de recopilar y plasmar la información adquirida a lo largo de este diplomado como es la configuración de protocolos de enrutamiento OSPF, EGRIP y BGP.

Dentro de esta topología también se encontrará configuración y enrutamiento de VLAN teniendo en cuenta el aseguramiento de la plataforma de comunicación. Estas configuraciones de enrutamientos se realizaron por medio de la herramienta Packet Tracert ya que permite la configuración básica de los dispositivos y poder ejecutar la simulación de los protocolos de enrutamiento.

La configuración de la red suministrada en la topología se incluye la conectividad de IPv4 e IPv6 y en la ultima parte se enfoca en la seguridad de los dispositivos, routing entre VLAN y protocolo de DHCP, listas de control de acceso (ACL) y configuración del protocolo de tiempo de red.

DESARROLLO

Figura 1. Topología de Red

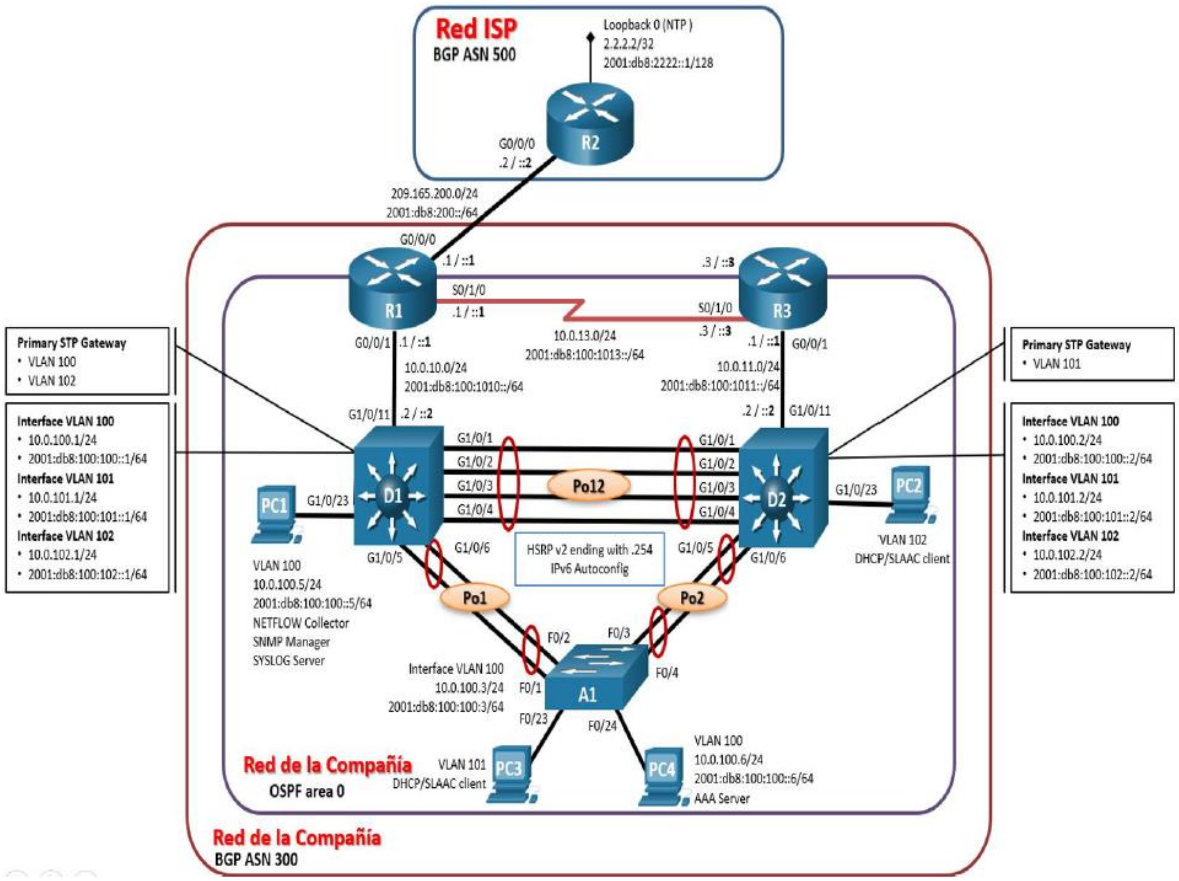


Tabla 1. Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IPv4 | Dirección IPv6 | IPv6 Link-Local |
|---|---|---|---|---|
| R1 | G0/0/0 | 209.165.200.225/27 | 2001:db8:200::1/64 | fe80::1:1 |
| | G0/0/1 | 10.0.10.1/24 | 2001:db8:100:1010::1/64 | fe80::1:2 |
| | S0/1/0 | 10.0.13.1/24 | 2001:db8:100:1013::1/64 | fe80::1:3 |
| R2 | G0/0/0 | 209.165.200.226/27 | 2001:db8:200::2/64 | fe80::2:1 |
| | Loopback0 | 2.2.2.2/32 | 2001:db8:2222::1/128 | fe80::2:3 |
| R3 | G0/0/1 | 10.0.11.1/24 | 2001:db8:100:1011::1/64 | fe80::3:2 |
| | S0/1/0 | 10.0.13.3/24 | 2001:db8:100:1013::3/64 | fe80::3:3 |
| D1 | G1/0/11 | 10.0.10.2/24 | 2001:db8:100:1010::2/64 | fe80::d1:1 |
| | VLAN 100 | 10.0.100.1/24 | 2001:db8:100:100::1/64 | fe80::d1:2 |
| | VLAN 101 | 10.0.101.1/24 | 2001:db8:100:101::1/64 | fe80::d1:3 |
| | VLAN 102 | 10.0.102.1/24 | 2001:db8:100:102::1/64 | fe80::d1:4 |
| D2 | G1/0/11 | 10.0.11.2/24 | 2001:db8:100:1011::2/64 | fe80::d2:1 |
| | VLAN 100 | 10.0.100.2/24 | 2001:db8:100:100::2/64 | fe80::d2:2 |
| | VLAN 101 | 10.0.101.2/24 | 2001:db8:100:101::2/64 | fe80::d2:3 |
| | VLAN 102 | 10.0.102.2/24 | 2001:db8:100:102::2/64 | fe80::d2:4 |
| A1 | VLAN 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 |

Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
Part 2: Configurar la capa 2 de la red y el soporte de Host
Part 3: Configurar los protocolos de enrutamiento

Part 4: Configurar la redundancia del primer salto
Part 5: Configurar la seguridad
Part 6: Configurar las características de administración de red

ESCENARIO 1

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 Compañia" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.
Nota: Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con 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.
Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.
Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global sdm prefer dual-ipv4-and-ipv6 default. Cambiar la plantilla requerirá el reinicio del switch.

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

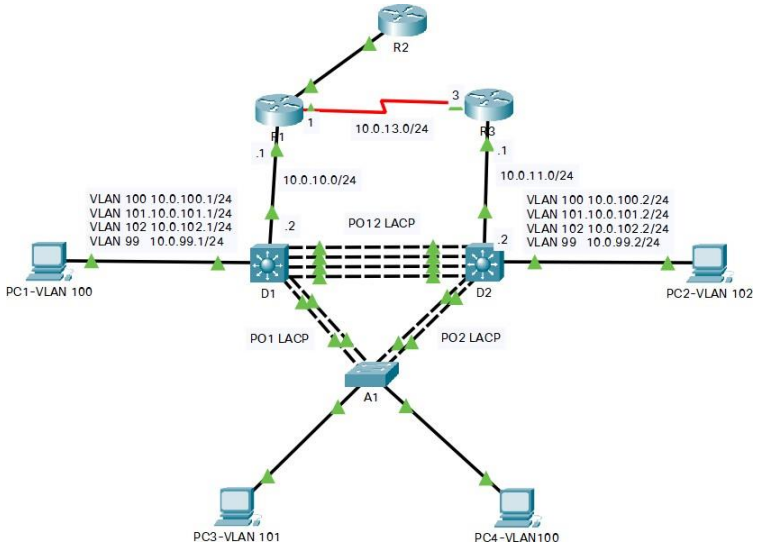
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES

Paso 1: Cablear la red como se muestra en la topología.
Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Figura 2. Topología realizada por Camilo León en Pacete Tracert




Paso 1. Se realiza la conexión de los dispositivos como se muestra en la topología teniendo en cuenta que la conexión entre Switch se realiza con un cable cruzado por esta razón se realizaron las conexiones de los interfaces G1/0/1-4 entre los Switch D1 y D2 y así mismo D1 se conecta con cable cruzado al Switch A1 y el Switch D2 se conecta por medio de dos cables cruzados al Switch A1.

La conexión de los Routers R1 y R3 se realiza por medio de un cable serial a los puertos seriales s/0/1/0 de cada Router.
Los Pcs1, PC2, PC3 y PC4 se conectan a sus respectivos Switch usando un cable Ethernet

Paso 2. Se realiza la configuración de los dispositivos de la topología del escenario 1 teniendo en cuenta la configuración suministrada en la topología a continuación se muestra la digitalización de los comandos necesarios para cada dispositivo y su explicación.

Router 1

```
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
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 g0/1
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 s0/0/1
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
```

Para configurar los parámetros básicos del Router R1 se cambian el comando: interface g0/0/0 y interface g0/0/1 por interface g0/0 e interface g0/1 respectivamente que corresponden a nuestra interfaz montada en la aplicación Packet Tracert.

Router 2

```
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
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-loca
l 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
```

Con respecto a la configuración del Router R2 también se reemplaza el comando interface g0/0/0 por interface g0/0, la cual es la interface suministrada en nuestro Router R2

Router 3

```
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 synchronousexit
interface g0/1
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 s0/0/1
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

Procedemos a configurar el Router R3 y como ya notamos anteriormente los parámetros de la interfaz generada por el router en packet tracert es interface g0/1. Por otro lado, la interface de s0/1/0 es la misma que interface s0/0/1 en nuestro diseño en packet tracert así que realizamos esa pequeña modificación en el comando.

Switch D2

hostname D1ip routing
ipv6 unicast-routing no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #line con 0
exec-timeout 0 0 logging synchronousexit
vlan 100
name Managementexit
vlan 101
name UserGroupAexit
vlan 102
name UserGroupBexit
vlan 99
name NATIVEexit
interface g1/0/11no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64no 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::1/64no 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::1/64no
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::1/64no
shutdown
exit
int vlan 99
up address 192.168.99.1 255.255.225.0
no vlan 999
 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
no shutdown
exit
interface range g1/0/12-24
shut
exit
interface range g1/1/1-4
shut
exit
```

Al realizar la configuración del Switch D1 comenzamos a realizar el enrutamiento IPv6 y desactivamos la traducción de los nombres del direccionamiento del Switch D1 y así sabremos cuando digitamos un comando no valido. Después ponemos el mensaje de Scenario 1 # para identificar nuestro primer trabajo o escenario. A continuación, ingresamos el comando logging synchronous el cual nos indicara cualquier mensaje de evento mientras ingresamos un comando y así se puede repetir para que sea mas fácil leerlo procedemos a configurar los nombres de las VLANs. Cambiamos los puertos de capa 2 a un interfaz de capa 3 con el comando “no witchport” para poderlo enrutar, lo realizamos para las vlans 100, 101 y 102. Y a continuación procedemos a reservar las Ip 10.0.101.1 10.0.101.109, 10.0.101.141

10.0.101.254, 10.0.102.1 10.0.102.109, 10.0.102.141 10.0.102.254 y establecemos las rutas por defecto.

**Switch D2** 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 synchronousexit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 99
name NATIVEexit
interface g1/0/11no 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 shutdown
exit
interface range g1/0/12-24 shutdown
exit
interface range g1/1/1-4 shutdown
exit
```

En el Switch D2 comenzamos anexando el mensaje de Scenario 1 # para identificar el primer escenario. A continuación ingresamos el comando logging synchronous el cual nos indicara cualquier mensaje de evento mientras ingresamos un comando y así se puede repetir para que se amas fácil leerlo y procedemos a configurar los nombres de las VLAN. Cambiamos los puertos de capa 2 a un interfaz de capa 3 con el comando “no witchport” para poderlo enrutar, lo realizamos para las VLAN 100, 101, 102 y 999 configuramos las interfaces de las vlans y reservamos las mismas direcciones del Switch D1.

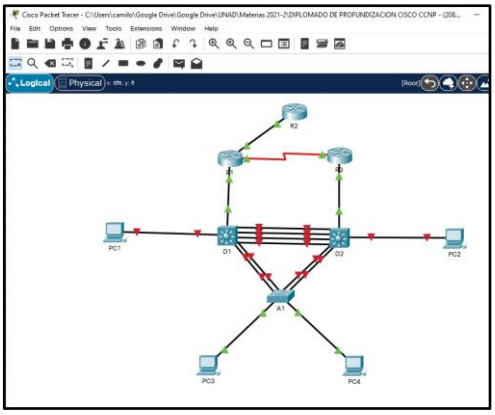
Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #line con 0
exec-timeout 0 0 logging synchronousexit
vlan 100
name Managementexit
vlan 101
name UserGroupAexit
vlan 102
name UserGroupBexit
vlan 99
name NATIVEexit
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::3/64no shutdown
exit
interface range f0/5-22shutdown
exit

En el Switch A1 no tuvimos que realizar ningún parámetro de comando ya que packet tracert los reconoce tal como están. De esta manera procedemos a dejar nombre del banner como Scenario 1 #. Modificamos el tiempo de inactividad con el comando exec-timeout 0 0, modificamos los mensajes de evento y renombramos las VLAN 100, 101, 102 y 999 apagamos las interfaces del rango f0/5-22 los resultados de las conexiones de la configuración de nuestros dispositivos iniciales terminan y a continuación se evidencia el estado de conexión en el momento de apagar las interfaces.

Figura 3. Topología de red con interfaces abajo




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

Figura 4. Running-config al archivo startup-config en R1

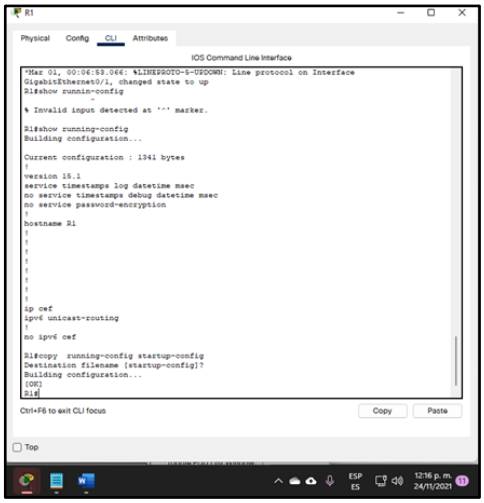


Figura 5. Running-config al archivo startup-config en R2

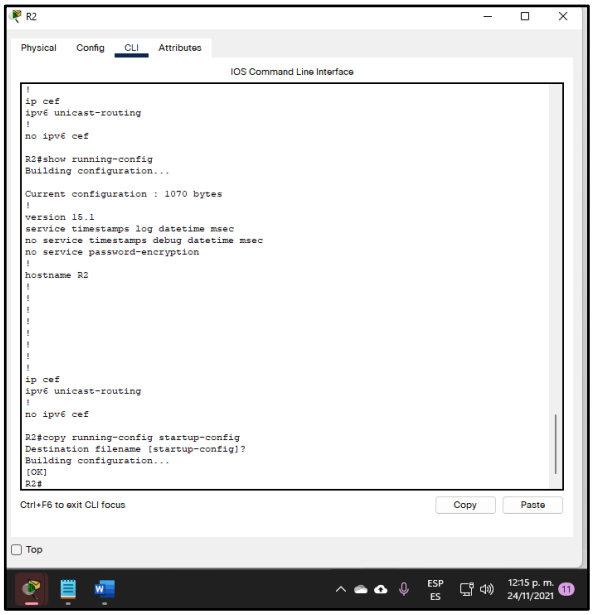



Figura 6. Running-config al archivo startup-config en R3

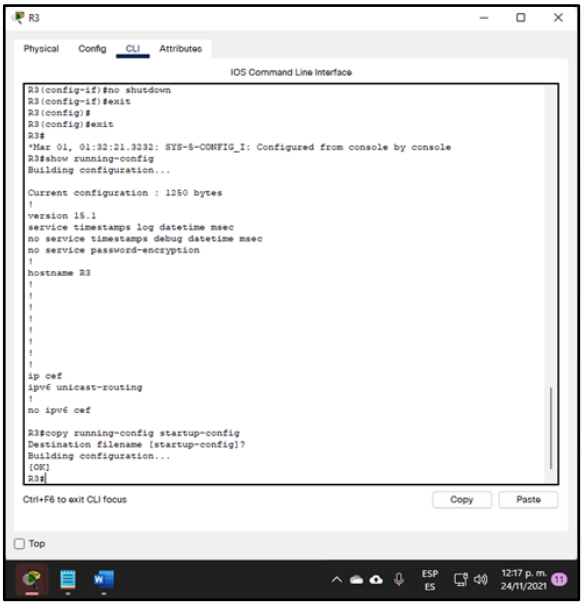


Figura 7. Running-config al archivo startup-config en D1

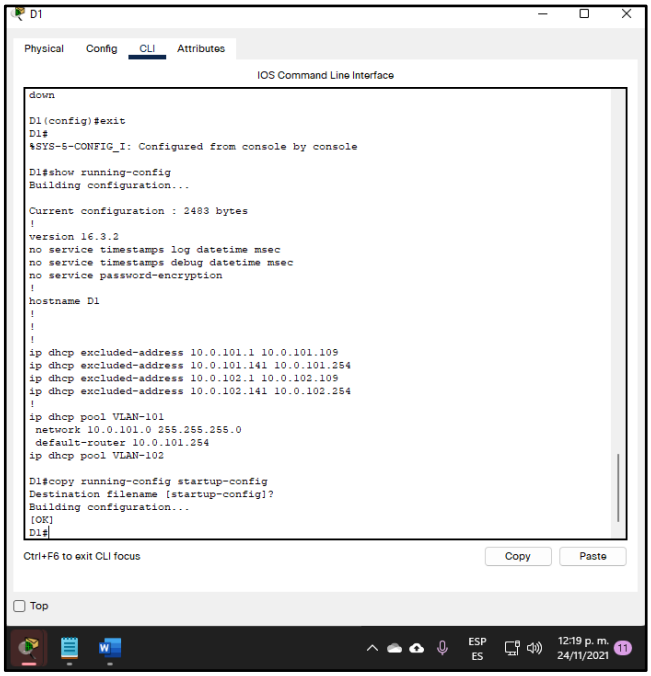



Figura 8. Running-config al archivo startup-config en D2

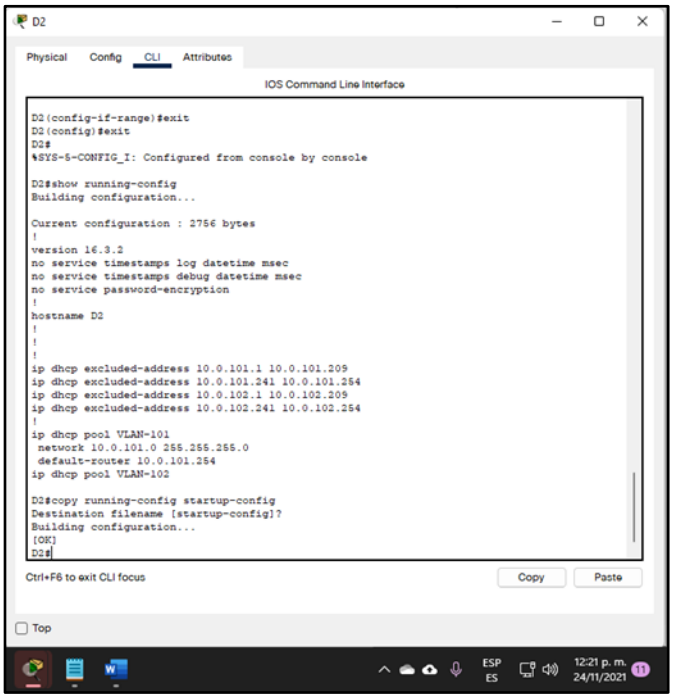
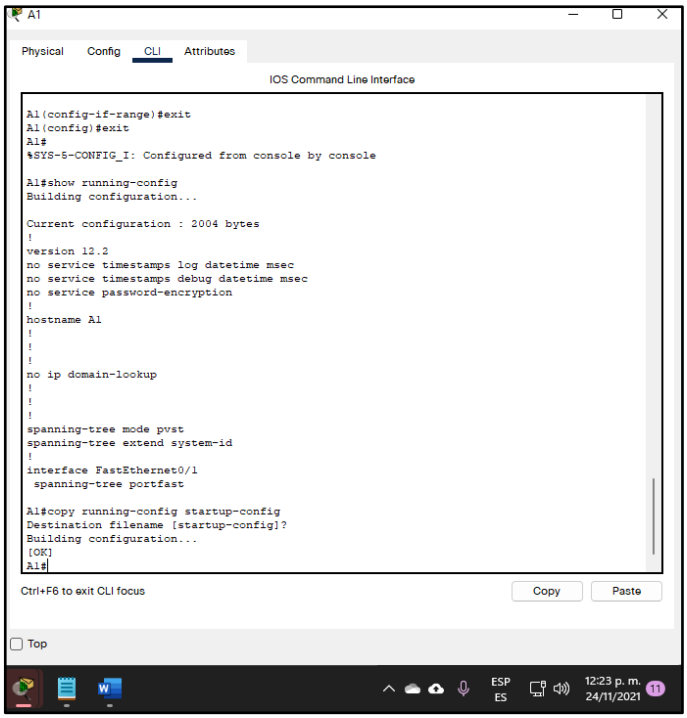
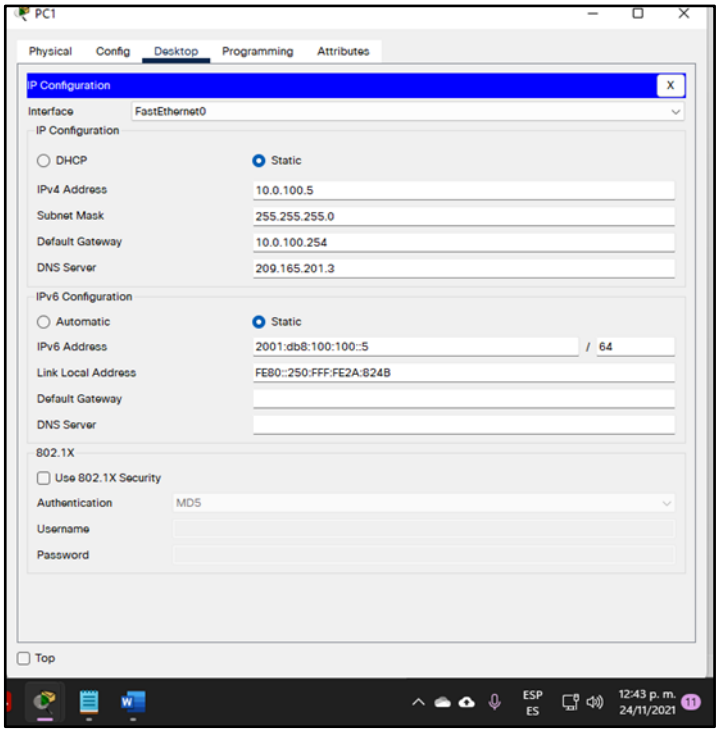


Figura 9. Running-config al archivo startup-config en A1




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.

Figura 10. Configuración IP PC1




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

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

Las tareas de configuración son las siguientes:

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

| Tarea# | Tarea | Especificación |
|---|---|---|
| 2.1 | En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches. | Habilite enlaces trunk 802.1Q entre:<br>• D1 and D2<br>• D1 and A1<br>• D2 and A1 |
| 2.2 | En todos los switches cambie la VLAN nativa en los enlaces troncales. | Use VLAN 999 como la VLAN nativa. |
| 2.3 | En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP) | Use Rapid Spanning Tree (RSPT). |
| 2.4 | En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.<br>D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge). | Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch. |
| 2.5 | En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología. | Use los siguientes números de canales:<br>• D1 a D2 – Port channel 12<br>• D1 a A1 – Port channel 1<br>• 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.<br>• Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding). |
| 2.7 | Verifique los servicios DHCP IPv4. | PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas. |
| 2.8 | Verifique la conectividad de la LAN local | PC1 debería hacer ping con éxito a:<br>• D1: 10.0.100.1<br>• D2: 10.0.100.2<br>• PC4: 10.0.100.6<br>PC2 debería hacer ping con éxito a:<br>• D1: 10.0.102.1<br>• D2: 10.0.102.2<br>PC3 debería hacer ping con éxito a:<br>• D1: 10.0.101.1<br>• D2: 10.0.101.2 |

| Tarea# | Tarea | Especificación |
|---|---|---|
| | | PC4 debería hacer ping con éxito a:<br>• D1: 10.0.100.1<br>• D2: 10.0.100.2<br>PC1: 10.0.100.5 |

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

En todos los dispositivos se procede a configurar el protocolo de enlace troncal perteneciente al estándar IEEE 802.1Q. Así podemos etiquetar los tramos de la red nombrando las VLAN. Esta configuración se realiza a nivel de capa 2 a nivel de enlace de datos, de esta manera los dispositivos identifican las VLAN de origen y de destino. Esta configuración la asignamos por medio de los comandos switchport.

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

Dentro de este parámetro realizamos la modificación dentro de las VLAN con el fin realizar el transporte de tráfico sin necesidad de etiquetas como lo es la configuración de enlaces troncales IEEE 802.1Q. se tuvo en cuenta que las VLAN nativas sean iguales en todos los dispositivos. Los comandos utilizados son native y encapsulation. A continuación se demuestra la configuración de los dispositivos y la asignación de la VLAN 99 como nativa.

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

Dentro de los dispositivos activamos el protocolo de RSTP para reducir el inconveniente de los loops y mejorar la eficacia de la red el comando usado es Spanning-tree link-type point-to-point

Switch D1

D1(config)

int range g1/0/5-6

channel-group 2 mode active switchport trunk encapsulation dot1q

Switchport mode trunk int po2

switchport trunk encapsulation dot1q

Switchport mode trunk

switchport trunk native vlan 99

spanning-tree link-type point-to-point

En el Switch D1 se realiza el ingreso de rango de interfaces desde la interfaz G1/0/5 hasta G1/0/6 para encapsularlas con el estándar 802.1Q dentro del channel-group 2 como lo indica la topología de red. Adicionalmente se configura la vlan 99 como vlan nativa

D1(config)

int range g1/0/1-4 Channel-group 1 mode active

Switchport trunk encapsulation dot1q Switchport mode trunkInt poq

Switchport trunk encapsulation dot1q Switchport mode truk

Spanning-tree link-type point-to-point

Exit

Switchport mode trunk

switchport trunk native vlan 99

Dentro del rango de interfaces entre G1/0/1 y G1/0/4 activamos la agrupación en el channel group 1 y lo encapsulamos. Y se asigna la vlan 99 como nativa

A1

Enable

configure terminal

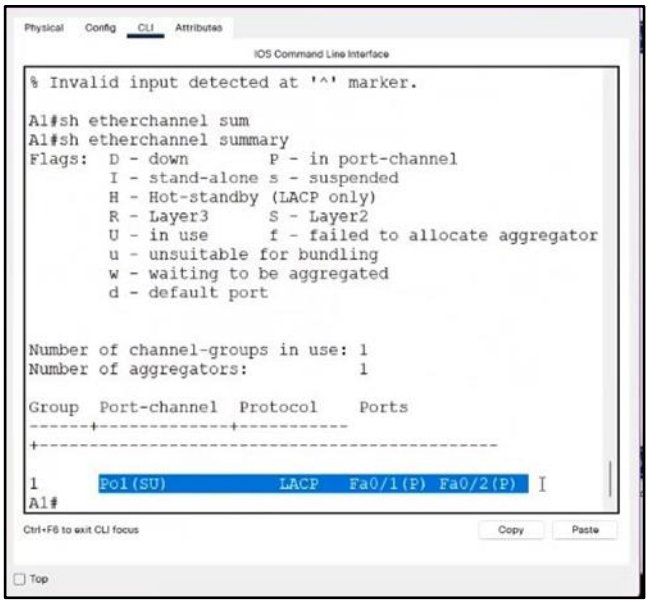
int range f0/1-2

channel-group 1 mode active switchport mode trunk

spanning-tree link-type point-to-point

Dentro del Switch A1 configuramos el rango de las fases 0 y 1 lo agrupamos en el channel group1 y configuramos punto a punto en enlace spanning-tree

Figura 11. Spanning-tree link-type point-to-point en A1




Teóricamente todas las interfaces deben ser iguales y no permite mezclar FastEthernet con Gigabit Ethernet ósea no se pueden agrupar. En nuestro caso usando packet tracert si pudimos realizar la configuración.

Figura 12. Teoría de velocidad de interfaces

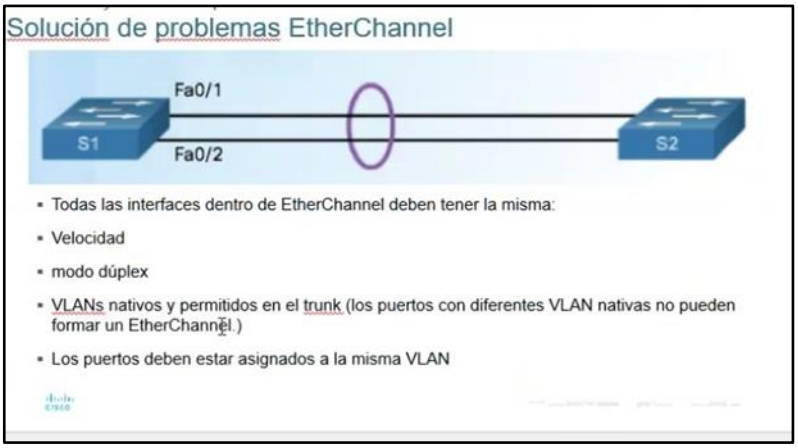
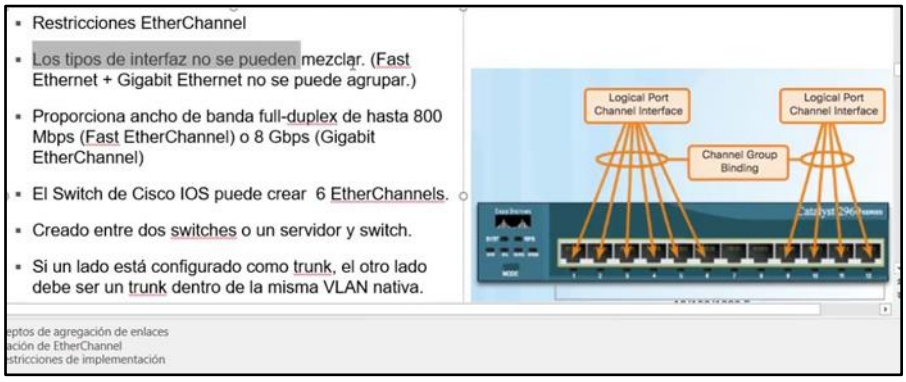



Figura 13. Teoría de velocidad de interfaces




Comenzando, configurando HSRP con la vlan 100 en Switch D1 Switch D1

#enable
#Configure terminal
# int vlan 100
# standby 100 ip 10.0.100.254
#standby 100 preempt
#standby 100 priority 105

Continuamos con la configuración de HSRP en la vlan 101

# int vlan 101
# standby 101 ip 10.0.101.254
# standby 101 preempt

No priorizamos por la vlan 101 por que la enviamos por el otro canal y Continuamoscon la vlan 102.

# int vlan 102

# standby 102 ip 10.0.102.254

# standby 102 preempt

# standby 102 priority 105

# sh stanby brief

Figura 14. Sh stanby brief en D1

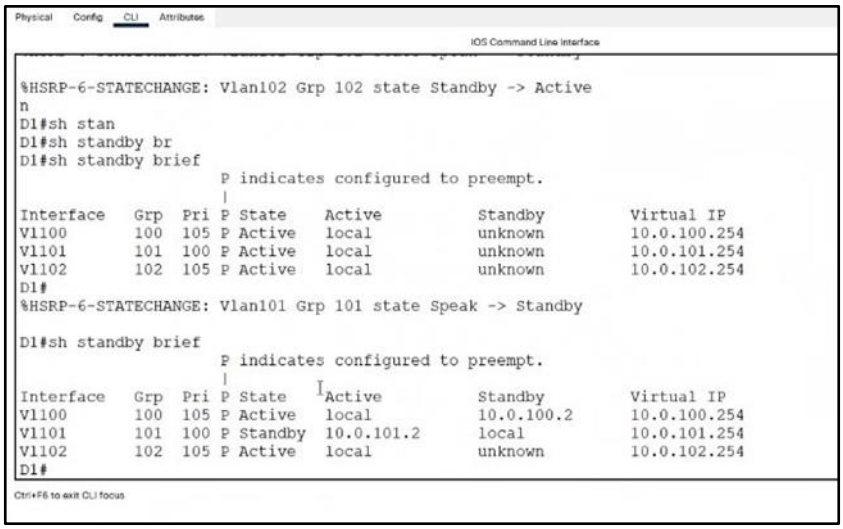
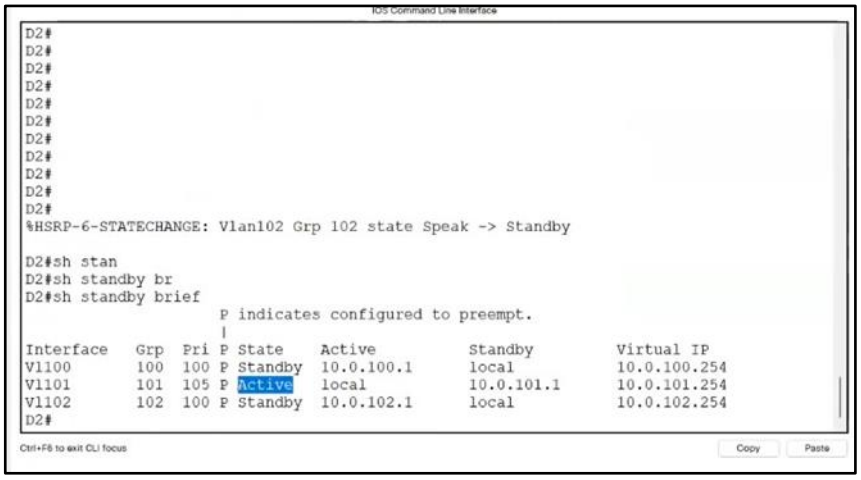


Figura 15. Sh stanby brief en D2




En el Switch D1 podemos observar que para la vlan 100 y 102 queda el estatus de activo y para la vlan 101 con la ip 10.0.101.2queda en standby y lo contrario sucede con el Switch S2 el cual tiene las vlan 100 y 102 en standby con las ips 10.0.100.1 y 10.0.102.1 correspondientemente.

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).

Dentro de los switch D1 y D2 realizamos la configuración de root Bridge así el intercambio de paquetes viajara más rápido por el camino mas eficiente realizamos la configuración spanning-tree vlan 100,102 root primary spanning-tree vlan 101 root secondary en el caso del Switch D1 y en el caso del Switch D2 usamos #spanning-tree vlan 100,102 root secondary#spanning-tree vlan 101 root primary.

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología

Para resolver posibles problemas con el uso de ancho de banda se puede analizar la configuración con channel-group, interface port-channel asi configuramos EtherChannel.

Switch D1

D1(config)

# spanning-tree mode rapid-pvst

#wr

A1

A1(config)

# spanning-tree mode rapid-pvst

#wr

Switch D2

D2(config)

# spanning-tree mode rapid-pvst

#wr

Dentro de los Switch D1, A1 y D2 configuramos el protocolo Rapid Spanning-Tree (RSTP) por medio del comando spanning-tree mode rapid-pvst que nos permite una convergencia más rápida que la de STP para evitar bucles

Figura 16. Spanning-tree D1

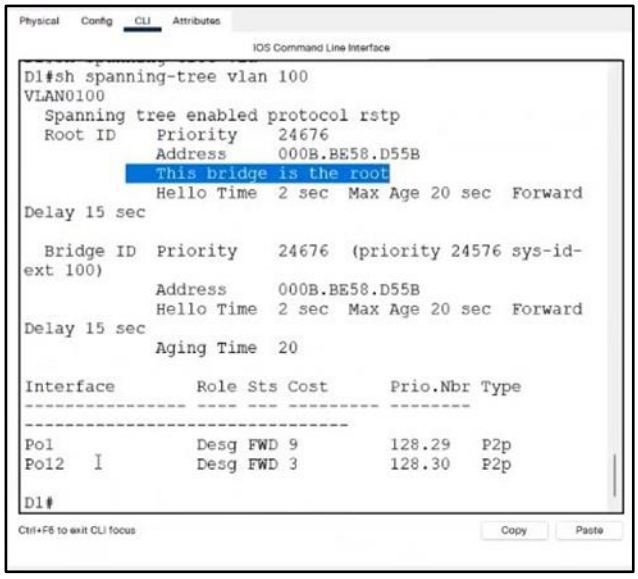
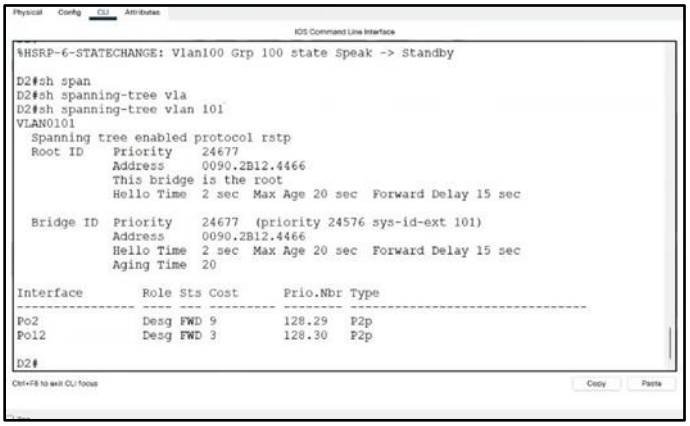



Figura 17. Spanning-tree vlan 101




D2(config)

# int range g1/0/5-6

#channel-group 2 mode active

#switchport trunk encapsulation dot1q

#Switchport mode trunk

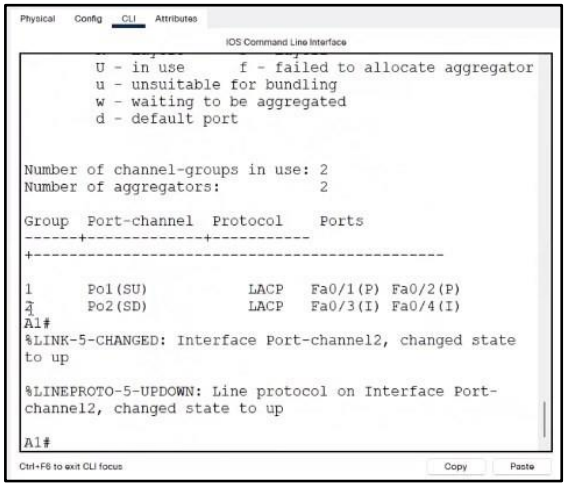
#int po2

#switchport trunk encapsulation dot1q

#Switchport mode trunk
#spanning-tree link-type point-to-point

A1
# Enable
#configure terminal
#int range f0/3-4
#channel-group 2 mode active
#switchport mode trunk
#spanning-tree link-type point-to-point

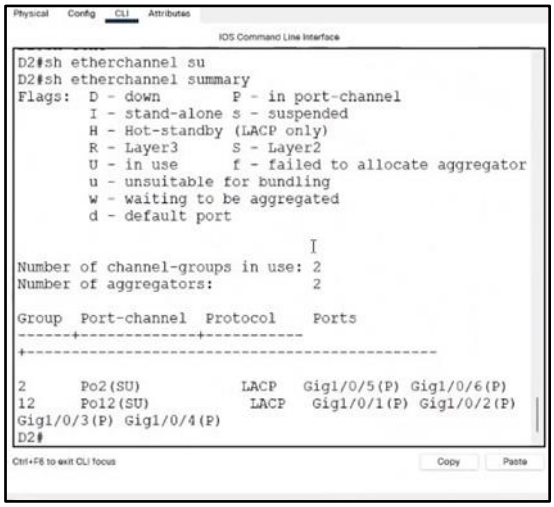
Figura 18. Spanning-tree link-type point-to-point




Switch D2

#sh etherchannel summary

Figura 19. Sh etherchannel summary




Switch D1

#enable
#configure terminal
#spanning-tree vlan 100,102 root primary
# spanning-tree vlan 101 root secondary

El paquete para la vlan 100 y 102 pasa por el Switch D1 a Switch D2

#enable
#configure terminal
#spanning-tree vlan 100,102 root secondary
#spanning-tree vlan 101 root primary

Switch D2
#enable
#configure terminal
#spanning-tree vlan 100,102 root secondary
#spanning-tree vlan 101 root primary

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).

Se realizo la configuración de los puertos de acceso como puertos troncales y dentro de cada dispositivo donde están conectados los Pcs realizamos la configuración de sus interfaces según el puerto que muestra la topología la configuración se muestra a continuación:

Switch D1

#enable
#configure terminal
#int g1/0/23
#spanning-tree portfast

Switch D1
#enable
#configure terminal
#int g1/0/23
#spanning-tree portfast

A1
#enable
#configure terminal
# int range f0/23-24
#spanning-tree

Switch D1

#enable
#configure terminal
#int g1/0/23
#switchport mode Access
#switchport Access vlan 100

#enable
#configure terminal
# int f0/23
#switchport mode Access
#switchport Access  vlan101

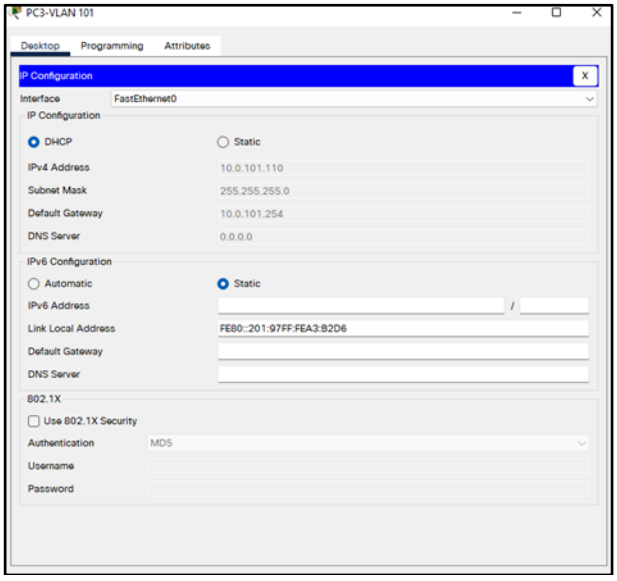
## 2.7 Verifique los servicios DHCP IPv4.

Verificamos los servicios de DHCP IPv4 del PC2 y PC3 que según la topología deberán recibir una dirección valida según corresponda su segmento de red en el caso del PC3 debe recibir una dirección ip valida de la VLAN 101 y en el caso del PC4 debe recibir una dirección IP valida de su segmento de red a continuación se evidencia en las capturas de pantallas

Switch A1

El pc3 recibe DHCP de la vlan 101

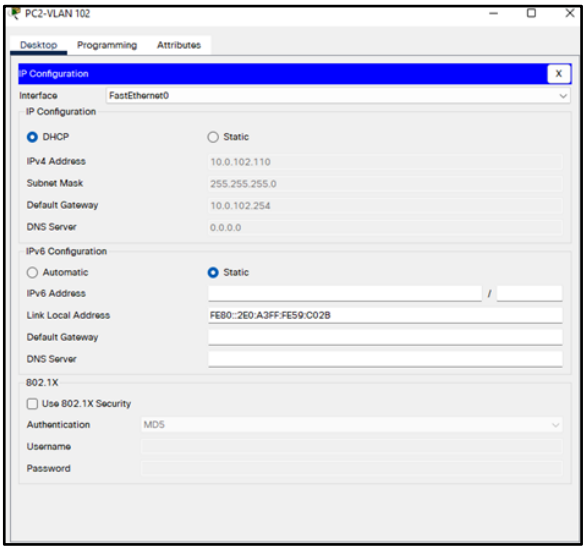
Figura 20. IP dado por DHCP de la vlan 101




Switch D2
#enable

#configure terminal
# int g1/0/23
#switchport mode Access
#switchport Access vlan 102

Figura 21. Dado por DHCP de la vlan 102

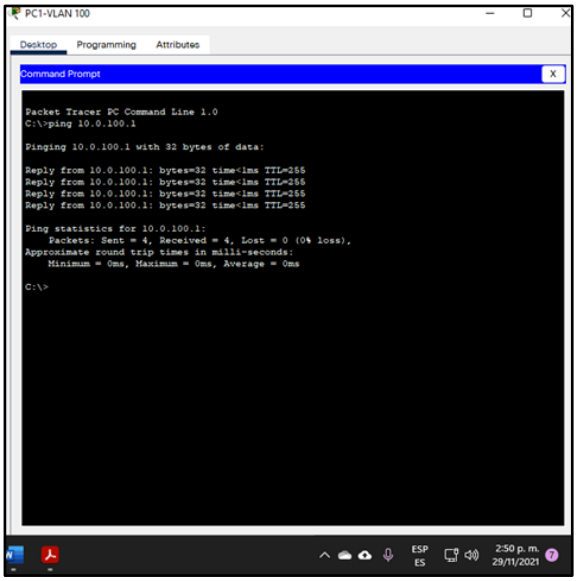



PC1 – D1: 10.0.100.1

## 2.8 Verifique la conectividad de la LAN local

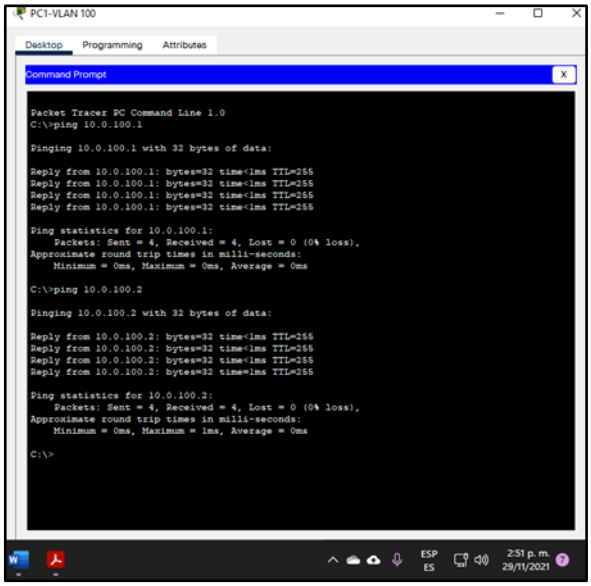
Realizamos las pruebas de conexión de los diferentes dispositivos realizando el comando ipconfig y la dirección IP perteneciente a los dispositivos Switch D1, D2, PC1 y PC4 la evidencia de la conectividad se muestra a continuación por medio de las siguientes capturas de pantalla:

Figura 22. Ping pc1 a D1: 10.0.100.1



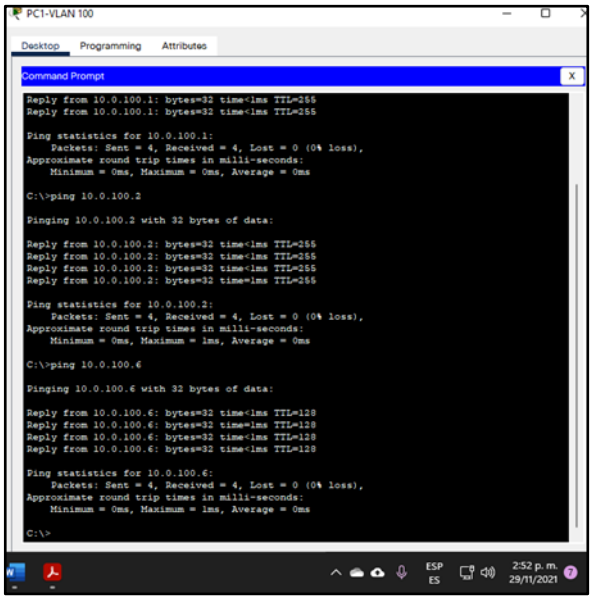

PC1 – D2: 10.0.100.2

Figura 23. Ping D1: 10.0.100.1



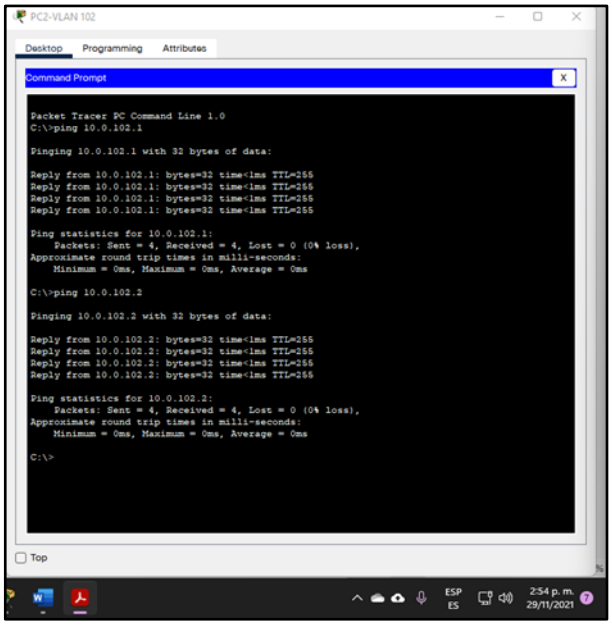
PC1 – PC4: 10.0.100.6

Figura 24. Ping PC1 – PC4: 10.0.100.6



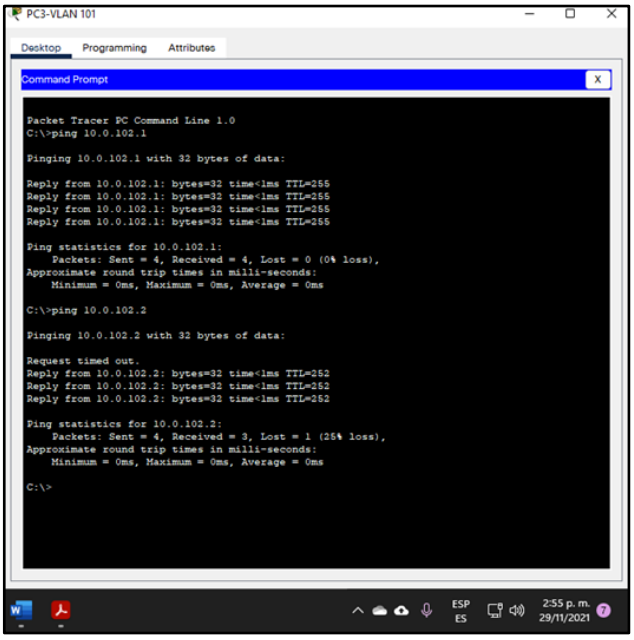

PC2 – D1: 10.0.102.1 y D2: 10.0.102.2

Figura 25. Ping a PC2 – D1: 10.0.102.1 y D2: 10.0.102.



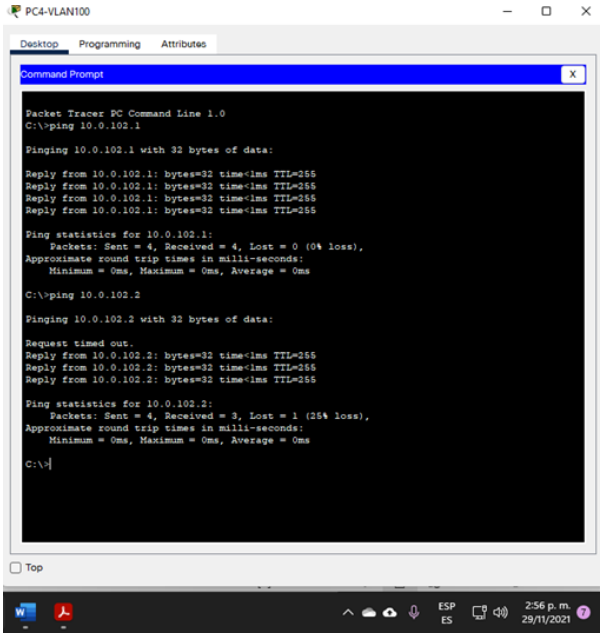

PC3 – D1: 10.0.102.1 y D2: 10.0.102.2

Figura 26. Ping PC3 – D1: 10.0.102.1 y D2: 10.0.102.2



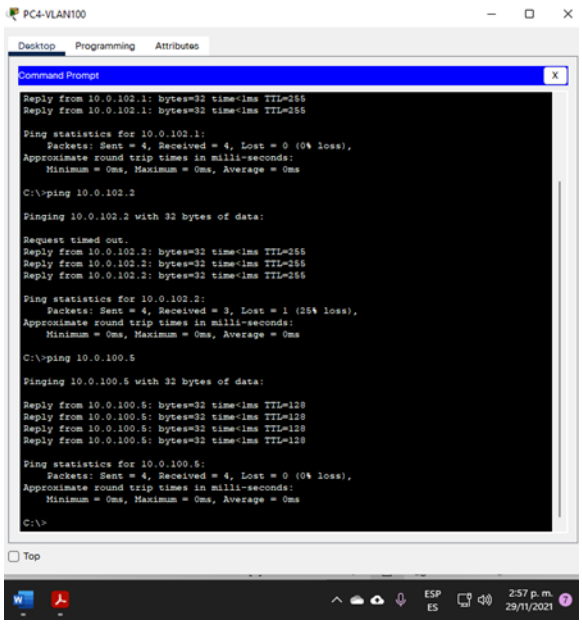

PC4 – D1: 10.0.102.1 y D2: 10.0.102.2

Figura 27. Ping PC4 – D1: 10.0.102.1 y D2: 10.0.102.2




PC4 – PC1: 10.0.100.5

Figura 28. PC4 – PC1: 10.0.100.5



## PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO

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

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

Las tareas de configuración son las siguientes:

Tabla 3 Configurar los protocolos de enrutamiento

| Tarea# | Tarea | Especificación |
|---|---|---|
| 3.1 | En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0. | Use OSPF Process ID **4** y asigne los siguientes router-IDs:<br>R1: 0.0.4.1<br>R3: 0.0.4.3<br>D1: 0.0.4.131<br>D2: 0.0.4.132<br>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.<br>En R1, no publique la red R1 – R2.<br>En R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP.<br>Deshabilite las publicaciones OSPFv2 en:<br>D1: todas las interfaces excepto G1/0/11<br>D2: todas las interfaces excepto G1/0/11 |
| 3.2 | En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0. | Use OSPF Process ID **6** y asigne los siguientes router-IDs:<br>R1: 0.0.6.1<br>R3: 0.0.6.3<br>D1: 0.0.6.131<br>D2: 0.0.6.132<br>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.<br>En R1, no publique la red R1 – R2.<br>On R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP.<br>Deshabilite las publicaciones OSPFv3 en:<br>D1: todas las interfaces excepto G1/0/11<br>D2: todas las interfaces excepto G1/0/11 |

| Tarea# | Tarea | Especificación |
|---|---|---|
| 3.3 | En R2 en la “Red ISP”, configure MP-BGP. | Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:<br>Una ruta estática predeterminada IPv4.<br>Una ruta estática predeterminada IPv6.<br><br>Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2.<br><br>Configure y habilite una relación de vecino IPv4 e IPv6con R1 en ASN 300.<br><br>En IPv4 address family, anuncie:<br>La red Loopback 0 IPv4 (/32).<br>La ruta por defecto (0.0.0.0/0).<br><br>En IPv6 address family, anuncie:<br>La red Loopback 0 IPv4 (/128).<br>La ruta por defecto (::/0). |
| 3.4 | En R1 en la “Red ISP”, configure MP-BGP. | Configure dos rutas resumen estáticas a la interfaz Null 0:<br>Una ruta resumen IPv4 para 10.0.0.0/8.<br>• Una ruta resumen IPv6 para 2001:db8:100::/48.<br>Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1.<br>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.<br>En IPv4 address family:<br>Deshabilite la relación de vecino IPv6.<br>Habilite la relación de vecino IPv4.<br>• Anuncie la red 10.0.0.0/8.En IPv6 address family:<br>Deshabilite la relación de vecino IPv4.<br>Habilite la relación de vecino IPv6.<br>Anuncie la red 2001:db8:100::/48. |

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

En los dispositivos R1, R3, D1 y D2 se realiza la configuración del protocolo OSPF el cual realiza la aplicación de algoritmos para encontrar la ruta más eficiente entre dos puntos. Después de cada código digitado dentro de el dispositivo se realiza una breve explicación de los comandos asignados.

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

La configuración se realiza dentro de los mismos dispositivos R1, R3, D1 y D2 la diferencia de OSPFv3 radica en la configuración compatible con IPV6 después de los comandos digitados a continuación se realiza una breve explicación de la configuración.

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

Dentro del router R2 se realiza la configuración del protocolo de Gateway fronterizo extendido así podemos llevar la información del enrutamiento para los diferentes protocolos que hemos configurado y nos funciona para la configuración de IPv4 e IPv6. Esta configuración tiene como fin hacer la unificación de diferentes tipos de enrutamiento

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

Dentro del R1realizamos el mismo proceso que en el R1 asignado BGP 300 y la ruta con el id 1.1.1.1 la explicación mas detallada se encuentra después de cada código.

Router R1

```
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
exit
ipv6 router ospf 6
```

```
router-id 0.0.6.1
default-information originate
exit
interface g2/0
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:10
```

realizamos la configuración de enrutamiento OSPF en el router R1 con el identificador ID 0.0.4.1 y nombrando la red 10.0.10.0.0.0.255 y 10.0.13.0.0.0.255 las cuales se encuentran dentro de la configuracion de R1

Router R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
```

```
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family
```

dentro del router R2 realizamos la configuración de el numero identificador con la ruta para conectarse al BGP y también realizamos la configuración de IPv4 e IPv6 con su respectiva mascara.

Router R3

```
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface g2/0
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
```

Realizamos el enrutamiento de OSPF con su respectivo ID 0.0.4.3 y agregamos la dirección que usara en área 0.

Switch D1

```
router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface g1/0/11
```

```
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface g1/0/11
exit
interface e2/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

Dentro del Switch D1 realizamos de mismo modo la configuración de OSPF agregando las direcciones de red suministradas en la guía menos la interfaz G1/0/11 y adicionalmente ingresamos las VLAN 100, 101 y 102 a la configuración de OSPF.

Switch D2

```
router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e2/0
exit
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g1/0/11
exit
interface e2/0
```

```
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

abrimos el enrutamiento OSPF en el Switch D2 agregando las direcciones de red. Agregamos el ID 0.0.6.132 al y realizamos el ingreso de las interfaces y VLAN al área de OSPF.

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

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

Tabla 4 Configurar la Redundancia del Primer Salto (First Hop Redundancy

| Tarea# | Tarea | Especificación |
|---|---|---|
| 4.1 | En D1, cree IP SLAs que prueben la accesibilidad dela interfaz R1 G0/0/1. | Cree dos IP SLAs.<br>Use la SLA número **4** para IPv4.<br>Use la SLA número **6** para IPv6.<br>Las IP SLAs probarán la disponibilidad de la interfaz R1G0/0/1 cada 5 segundos.<br>Programe la SLA para una implementación inmediata sintiempo de finalización.<br>Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6.<br>Use el número de rastreo **4** para la IP SLA 4.<br>Use el número de rastreo **6** para la IP SLA 6.<br>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos. |
| 4.2 | En D2, cree IP SLAs que prueben la accesibilidad dela interfaz R3 G0/0/1. | Cree IP SLAs.<br>Use la SLA número **4** para IPv4.<br>Use la SLA número **6** para IPv6.<br>Las IP SLAs probarán la disponibilidad de la interfaz R3G0/0/1 cada 5 segundos.<br>Programe la SLA para una implementación inmediata sintiempo de finalización.<br>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.<br>Use el número de rastreo **4** para la IP SLA 4.<br>Use el número de rastreo **6** para la SLA 6.<br>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos. |

| Tarea# | Tarea | Especificación |
|---|---|---|
| 4.3 | En D1 configure HSRPv2. | D1 es el router primario para las VLANs 100 y 102; por lotanto, su prioridad también se cambiará a 150..<br><br>Configure HSRP version 2.<br><br>Configure IPv4 HSRP grupo **104** para la VLAN 100:<br>Asigne la dirección IP virtual **10.0.100.254**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 y decremente en 60.<br><br>Configure IPv4 HSRP grupo **114** para la VLAN 101:<br>Asigne la dirección IP virtual **10.0.101.254**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv4 HSRP grupo **124** para la VLAN 102:<br>Asigne la dirección IP virtual **10.0.102.254**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv6 HSRP grupo **106** para la VLAN 100:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 6 y decremente en 60.<br><br>Configure IPv6 HSRP grupo **116** para la VLAN 101:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Habilite la preferencia (preemption).<br>Registre el objeto 6 y decremente en 60.<br><br>Configure IPv6 HSRP grupo **126** para la VLAN 102:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 6 y decremente en 60. |

| Tarea# | Tarea | Especificación |
|---|---|---|
| | En D2, configure HSRPv2. | D2 es el router primario para la VLAN 101; por lo tanto, suprioridad también se cambiará a 150.<br>Configure HSRP version 2.<br>Configure IPv4 HSRP grupo **104** para la VLAN 100:<br>Asigne la dirección IP virtual **10.0.100.254**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 y decremente en 60.<br>Configure IPv4 HSRP grupo **114** para la VLAN 101:<br>Asigne la dirección IP virtual **10.0.101.254**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 para disminuir en 60.<br>Configure IPv4 HSRP grupo **124** para la VLAN 102:<br>Asigne la dirección IP virtual **10.0.102.254**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 4 para disminuir en 60.<br>Configure IPv6 HSRP grupo **106** para la VLAN 100:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 6 para disminuir en 60.<br>Configure IPv6 HSRP grupo **116** para la VLAN 101:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Establezca la prioridad del grupo en **150**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 6 para disminuir en 60.<br>Configure IPv6 HSRP grupo **126** para la VLAN 102:<br>Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>Habilite la preferencia (preemption).<br>Rastree el objeto 6 para disminuir en 60. |

4.1 En D1, cree IP SLA que prueben la accesibilidad de la interfaz R1 G0/0/1.

En D1, configure HSRPv2.

Realizamos la prueba de IP SLA testeando con una frecuencia de 5 de la IPv4 y también en la IPv6, adicionalmente se realiza la configuración de la IP SLA indicando hora de inicio 6 y que dure todo el tiempo. Se agrega un retraso de 10 a 15 en las IP SLA. Adicionalmente configuramos las interfaces de VLAN HSRP teniendo en cuenta la versión 2.

4.2 En D2, cree IP SLA que prueben la accesibilidad de la interfaz R3 G0/0/1.

En D2, configure HSRPv2.

En el Switch D2 realizamos la configuración del servicio SLA para poder mejorar los servicios de datos, voz y video mejorando la infraestructura de IP midiendo los extremos y capa de IP esta configuración se realizo tanto para IPv4 como IPv6 la configuración asignada comprueba la disponibilidad de la interfaz G0/1 cada 5 segundos con un implementación de SLA inmediata y sin tiempo sin tiempo de finalización la configuración en el dispositivo Switch D2 se plasma a continuación y se realiza una breve explicación de los comandos usados.

4.3 En D1 configure HSRPv2.

En el Switch D1 realizamos la configuración del servicio SLA para poder mejorar los servicios de datos, voz y video mejorando la infraestructura de IP midiendo los extremos y capa de IP esta configuración se realizó tanto para IPv4 como IPv6 la configuración asignada. Realizamos la configuración del router primario para las VLAN 100 y 103 y la prioridad la modificamos a 150 lo realizamos mediante los comandos Standby 104 IP 10.0.100.254 la explicación detallada de los comandos s realiza a continuación:

Switch D1

```
ip sla 4
icmp-echo 10.0.10.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life-forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
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
exit
interface vlan 101
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
exit
interface vlan 102
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
exit
```

```
Switch D2
ip sla 4
icmp-echo 10.0.11.1
frequency
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
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
exit
interface vlan 101
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
exit
interface vlan 102
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
exit
```

Dentro del Switch D2 Realizamos la prueba de IP SLAs testeando con una frecuencia de 5 de la IPv4 y también en la IPv6, adicionalmente se realiza la configuración de la IP SLA indicando hora de inicio 6 y que dure todo el tiempo. Se agrega un retraso de 10 a 15 en las IP SLA. Adicionalmente configuramos las interfaces de VLAN HSRP teniendo en cuenta la versión 2.

## PARTE 5: SEGURIDAD

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

Tabla 5 Seguridad

| Tarea# | Tarea | Especificación |
|---|---|---|
| 5.1 | En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmode encripción SCRYPT. | Contraseña: **cisco12345cisco** |
| 5.2 | En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT. | Detalles de la cuenta encriptada SCRYPT:<br>Nombre de usuario Local: **sadmin**<br>Nivel de privilegio **15**<br>Contraseña: **cisco12345cisco** |
| 5.3 | En todos los dispositivos (excepto R2),habilite AAA. | Habilite AAA. |
| 5.4 | En todos los dispositivos (excepto R2),configure las especificaciones del servidor RADIUS. | Especificaciones del servidor RADIUS.:<br>Dirección IP del servidor RADIUS es10.0.100.6.<br>Puertos UDP del servidor RADIUS son1812 y 1813.<br>Contraseña: **$trongPass** |
| 5.5 | En todos los dispositivos (excepto R2),configure la lista de métodos de autenticación AAA | Especificaciones de autenticación AAA:<br>Use la lista de métodos por defecto<br>Valide contra el grupo de servidoresRADIUS<br>De lo contrario, utilice la base de datoslocal. |
| 5.6 | Verifique el servicio AAA en todos losdispositivos (except R2). | Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y lacontraseña: **upass123**. |

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

Dentro de cada dispositivo realizamos la configuración SCRYPT haciendo uso de un algoritmo criptográfico diseñado para almacenar la contraseña el comando utilizado es enable algorithm-type SCRYPT secret cisco12345cisco

Switch D1
enable algorithm-type SCRYPT secret cisco12345cisco

Switch D2
enable algorithm-type SCRYPT secret cisco12345cisco

Router R1

enable password cisco12345cisco line console 0
password cisco12345cisco exit
line vty 0 15
password cisco12345cisco login

Router R2

enable password cisco12345cisco
line console 0
password cisco12345cisco
exit
line vty 0 15
password cisco12345cisco
login

Reuter R3
enable password cisco12345cisco
line console 0
password cisco12345cisco

```
exit
line vty 0 15
password cisco12345cisco
login
```

```
A1
enable password cisco12345cisco
line console 0
password cisco12345cisco
exit
line vty 0 15
password cisco12345cisco
login
```

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT

Realizamos la misma configuración mencionada en el punto 5.1 pero se asigna al usuario sadmin y se encripta con Scrypt

```
Switch D1
username sadmin password 15 cisco12345cisco
```

```
Switch D2
username sadmin password 15 cisco12345cisco
```

```
Router R1
username sadmin password 15 cisco12345cisco
```

```
Router R2
username sadmin password 15 cisco12345cisco
```

```
Router R3
username sadmin password 15 cisco12345cisco
```

A1
username sadmin password 15 cisco12345cisco

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

Realizamos la configuración de AAA para comprobar que los usuarios y administradores sean efectivamente quienes dicen ser, después de ello se decide los recursos a los que quiere acceder o los recursos a operar.

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

Realizamos la configuración en todos los dispositivos menos en el Router R2 para poder recibir peticiones de conexión de Usuario y devolviendo la información para que el cliente acceda al servicio que pide el usuario

5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA
y configuración lista de, métodos de autentificación AAA, RADIUS, lista de métodos de autenticación AAA y verificación de servicio AAA

realizamos la configuración en todos los dispositivos excepto en el Router R2 definiéndolo en la configuración global y nombrando el servidor de acceso y la dirección de acceso dado en la guía que se usara para comunicarse con el servidor AAA. Se configura la clave del servidor de acceso y se asigna el protocolo RADIUS

D1
aaa new-model
username backup secret $trongPass
aaa authentication login default group radius local aaa authentication login enable group radius local
radius-server host 10.0.100.6. key cisco auth-port 1812 acct-port 1813

D2
aaa new-model
username backup secret $trongPass
aaa authentication login default group radius local aaa authentication login enable group radius local
radius-server host 10.0.100.6. key cisco auth-port 1812 acct-port 1813

R1
aaa new-model
username backup secret $trongPass
aaa authentication login default group radius local aaa authentication login enable group radius local
radius-server host 10.0.100.6. key cisco auth-port 1812 acct-port 1813

R3
aaa new-model
username backup secret $trongPass
aaa authentication login default group radius local aaa authentication login enable group radius local
radius-server host 10.0.100.6. key cisco auth-port 1812 acct-port 1813

A1
aaa new-model
username backup secret $trongPass
aaa authentication login default group radius local
aaa authentication login enable group radius local
radius-server host 10.0.100.6. key cisco auth-port 1812 acct-port 1813

En todos los dispositivos se habilito la seguridad AAA para la administración de estos. De igual manera se realizó la configuración del protocolo RADIUS para autentificar y conectarse al servidor

## PARTE 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tabla 6 Funciones de Administración de Red

| Tarea# | Tarea | Especificación |
|---|---|---|
| 6.1 | En todos los dispositivos, configure el reloj local a la hora UTC actual. | Configure el reloj local a la hora UTC actual. |
| 6.2 | Configure R2 como un NTPmaestro. | Configurar R2 como NTP maestro en el nivel de estrato 3. |
| 6.3 | Configure NTP en R1, R3, D1, D2,y A1. | Configure NTP de la siguiente manera:<br>R1 debe sincronizar con R2.<br>R3, D1 y A1 para sincronizar la hora con R1.<br>D2 para sincronizar la hora con R3. |
| 6.4 | Configure Syslog en todos los dispositivos excepto R2 | Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING. |
| 6.5 | Configure SNMPv2c en todos los dispositivos excepto R2 | Especificaciones de SNMPv2:<br>Unicamente se usará SNMP en modo lectura (Read-Only).<br>Limite el acceso SNMP a la dirección IP de laPC1.<br>Configure el valor de contacto SNMP con su nombre.<br>Establezca el *community string* en **ENCORSA**.<br>En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*.<br>En R1, habilite el envío de *traps bgp, config*, y *ospf*.<br>En A1, habilite el envío de traps config. |

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

Dentro de los dispositivos configuramos la hora en clock timezone CST -5 correspondiente a Colombia.

6.2 Configure R2 como un NTP maestro.

Realizamos la configuración de el NTC para sincronizar la hora por medio de la conexión de red haciendo uso del comando ntp master

6.3 Configure NTP en R1, R3, D1, D2, y A1.

Como anteriormente asignamos el NTP master al router R2, procedemos a configurar los demás dispositivos para que vean la misma hora del Router R2 ya que todos están bajo la misma red

6.4 Configure Syslog en todos los dispositivos excepto R2

Como configuramos el NTP en todos los dispositivos procedemos a realizar la configuración de registro de mensajes a través de syslog en un bufer interno designado en el pc1 con logging trap warning y la dirección IP correspondiente 10.0.100.5.

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

En todos los dispositivos menos en el Router R2 realizamos la configuración del protocolo SNMPv2c para que permita la recopilación y la organización de la información de los dispositivos.

Router R2

ntp master 3
clock timezone CST -5
end

Router R1
clock timezone CST -5
ntp server 2.2.2.2

```
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server enable traps ospf
end
```

dentro del Router R1 activamos el inicio de sesión y habilitamos BGP y OSPF para operar en SNM.

Router R3

```
clock timezone CST -5
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
exit
```

ingresamos a ntp server 10.0.10.1 habilitando una advertencia de registro he inicio de sesión con el host 10.0.100.5 y damos permisos, seguido accedemos al protocolo de administración CISCO y habilitamos SNM para las operaciones OSPF

Switch D1
clock timezone CST -5
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf

ingresamos a ntp server 10.0.10.1 habilitando una advertencia de registro he inicio de sesión con el host 10.0.100.5 y damos permisos, seguido accedemos al protocolo de administración CISCO y habilitamos SNM para las operaciones OSPF

Switch D2
clock timezone CST -5
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA

```
snmp-server enable traps config
snmp-server enable traps ospf
```

```
Switch A1
clock timezone CST -5
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

en el Switch A1 ingresamos a ntp server 10.0.10.1 habilitando una advertencia de registro he inicio de sesión con el host 10.0.100.5 y damos permisos, seguido accedemos al protocolo de administración CISCO y habilitamos SNM para las operaciones OSPF

# CONCLUSIONES

Es importante configurar los dispositivos adecuadamente con un sistema de seguridad y backup de la configuración con el fin de evitar ataques y tener respaldo para restablecer la red en el menos tiempo posible. Gracias al análisis el contenido del diplomado de profundización CCNP aprendimos a realizar dicha configuración en IPv4 e IPv6 haciendo uso de algoritmos de encriptación en SCRYPT. Por parte del backup se realiza la copia de la configuración de los dispositivos de red usando los comandos copy running-config startup-config y con opción de extraer los archivos para almacenarlos externamente y principalmente para que queden almacenados en la NVRAM y la configuración arranque en los dispositivos si por algún motivo llegasen a apagarse.

Para resolver posibles problemas con el uso de ancho de banda se puede analizar la configuración con channel-group, interface port-channel asi configuramos EtherChannel.

Existen diferentes herramientas para virtualizar y analizar redes antes de ejecutar un proyecto como por ejemplo son las herramientas de GNS3 y Packet Tracert las cuales permiten montar una topología completa, configurarla y hallar posibles problemas y resolverlos antes de ejecutarla en la vida real. Estas herramientas nos permiten ejecutar protocolos como OSPF y EIGRP para desarrollar un adecuado enrutamiento.

Estas herramientas de virtualización también permiten analizar protocolos como spanning tree el cual optimiza los recursos de la red minimizando el envío masivo de paquetes entre dispositivos y así se realiza más eficientemente el envío de paquetes.

# BIBLIOGRAFÍA


C. (2006, 3 junio). *Problems Caused by Simultaneous Access to Router NVRAM*. Cisco. Recuperado 1 de noviembre de 2021, de https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-124-mainline/46942-nvram.html

C.I.S.C.O. (2020, 1 diciembre). *Protocolo de árbol de expansión*. Cisco. Recuperado 1 de diciembre de 2021, de https://www.cisco.com/c/es_mx/tech/lan-switching/spanning-tree-protocol/index.html

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300- 115. https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

C. (2005, 31 junio). Configuring Basic AAA on an Access Server. Cisco. Recuperado 6 de diciembre de 2021, de https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

C. (2006a, mayo 10). How to Use HSRP to Provide Redundancy in a Multihomed BGP Network. Cisco. Recuperado 6 de diciembre de 2021, de https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13768-hsrp-bgp.html

C. (2006b, junio 3). Problems Caused by Simultaneous Access to Router NVRAM. Cisco. Recuperado 1 de noviembre de 2021, de https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-124-mainline/46942-nvram.html