DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

SERGIO ANDRES TORRES CASTILLO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

SERGIO ANDRES TORRES CASTILLO

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 ELECTRÓNICA
BOGOTÁ DC
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CONMUTACIÓN: Hace referencia a la forma de establecer una ruta entre dos puntos las cuales hace el uso de un transmisor y un receptor por medio de nodos. Esto se da en la forma que la información se envía, ya que se divide en paquetes de datos de un mismo tamaño y se envía por diferentes nodos hasta llegar a su punto de destino final.

CISCO: Este es el nombre de una empresa la cual fue fundada en 1984 en los Estados Unidos, la cual se dedica a la fabricación de equipos de telecomunicaciones en las que se desarrolla el hardware y el software propio para sus equipos. Cabe resaltar que la empresa tiene material educativo para la formación profesional en el diseño, mantenimiento y la administración de redes de comunicación o informáticas.

CCNP: Sus siglas hacen referencia a Cisco Network Professional, la cual es una certificación que acredita a una persona en la industria de las tecnologías de la información, la cual tiene la capacidad de implementar un enrutamiento, implementar redes IP conmutadas, como también la solución de problemas y mantenimiento de redes IP. Esta certificación tiene validez por 3 años.

REDES: En las comunicaciones, una red está compuesta por diferentes dispositivos como ordenadores, switch, routers entre otros. Los cuales están conectados entre sí de forma física con diferentes tipos de cables o también de forma inalámbrica, con el fin de intercambiar datos. Para que se pueda dar este intercambio de información, hay que establecer que también existe una conexión lógica entre los diferentes dispositivos que componen la red, que se da por medio de diferentes protocolos de red.

ENRUTAMIENTO: En una red sea grande o pequeña está compuesta por enrutadores la cuales tiene más de dos interfaces. Su trabajo es conectarse a distintas redes para poder llevar un paquete de datos desde un punto de inicio o un punto final. Para que el envío del paquete de datos se dé, el enrutador debe escoger la mejor ruta. La cual hace el uso de una tabla de enrutamiento que se compone de diferentes rutas donde se determina la IP de interfaz y el Gateway.

Cabe resaltar que existe el enrutamiento estático que hace referencia a la información ingresada manualmente por el administrador de red la cual limita el tipo de redes que pueda utilizar. Caso distinto para con el enrutamiento dinámico la cual obtiene de forma automática la información de otros enrutadores lo cual optimiza el tiempo de configuración de las rutas y cambios de topologías.

RESUMEN

En el presente trabajo se desarrollan las diferentes temáticas involucradas en el diplomado CCNP (Cisco Network Professional). La cual está compuesta por seis partes basados en un escenario de red corporativa.

El desarrollo se realiza por medio de herramientas de simulación basado en software en las que se menciona a continuación como los son Packet Tracert y GNS3, las cuales emulan los diferentes dispositivos electrónicos de la red de acuerdo al escenario propuesto. Inicialmente la actividad nos solicita realizar la configuración de plataformas de conmutación por medio de protocolos STP, configuración de VLAN, en donde se analiza y comprende el beneficio de la operación en subredes. Como uno de los factores importantes del trabajo es realizar la configuración avanzada de routers por medio de comandos IOS con direccionamiento IPv4 e IPv6, para ser usado en protocolos de enrutamiento OSPF y BGP para la implementación de redes escalables. Otro de los componentes importantes a desarrollar es la configuración de mecanismos de seguridad en los diferentes dispositivos de la red y la configuración de las funciones de administrador de la red para realizar el monitoreo de la misma.

ABSTRACT

In this paper, the different themes involved in the CCNP (Cisco Network Professional) diploma are developed. Which is composed of six parts based on a corporate network scenario.

The development is carried out by means of software-based simulation tools in which a continuation is mentioned, such as Packet Tracer and GNS3, which emulate the different electronic devices of the network according to the proposed scenario. Initially, the activity asks us to configure the switching platforms through STP protocols, VLAN configuration, where the benefit of the operation in subnets is analyzed and understood. As one of the important factors of the work is to carry out the advanced configuration of routers through IOS commands with IPv4 and IPv6 addressing, to be used in OSPF and BGP routing protocols for scalable network implementation. Another component to be developed is the configuration of important security mechanisms in the different network devices and the configuration of the network administrator functions to monitor it.

INTRODUCCION

Este trabajo se realiza con el objetivo primordial de fortalecer las competencias en redes de comunicación, por lo que el estudio del diplomado de profundización de Cisco CCNP marca una diferencia en el mundo profesional y laboral debido al constante avance y evolución de las TI a nivel global. Por lo tanto es importante desarrollar las capacidades para la administración de dispositivos que conforman una red, mediante el estudio de arquitectura TCP/IP y demás herramientas para mantener y garantizar la conectividad en una red.

Para el desarrollo del diplomado Cisco CCNP se realiza bajo la estrategia de aprendizaje basado en escenarios (ABE). La cual se contempla cuatro partes de gran importancia. Donde el primero es el Switching donde se usa el protocolo STP, troncales VLAN y Etherchannel. El segundo es el Routing donde se va más a fondo correspondiente a la configuración en protocolos OSPF, BGP. Como tercera parte está el Wireless el cual abarca la infraestructura inalámbrica, autenticación de usuarios y solución a problemas en la red. En la cuarta parte está el Enterprise correspondiente a una infraestructura de red corporativa, el acceso seguro y herramientas para la automatización.

El escenario mediante el cual se desarrolla el presente trabajo final, es establecido como una red corporativa, la cual es emulada por medio de software con las herramientas de Packet Tracert y GNS3. Este ejercicio está compuesto por seis partes la cual consiste en configurar plataformas de conmutación por medio de protocolos STP y configuración VLAN. Como parte importante en el desarrollo del diplomado es la configuración avanzada de routers por medio de comando IOS para ser usado en protocolos de enrutamiento OSPF y BGP. Como instancia final del desarrollo se aborda la implementación de mecanismos de seguridad en los dispositivos y las configuraciones en las funciones de administrador de red para mantener el control y garantizar la conectividad en la red.

ESCENARIO PROPUESTO

Figura 1. Escenario propuesto

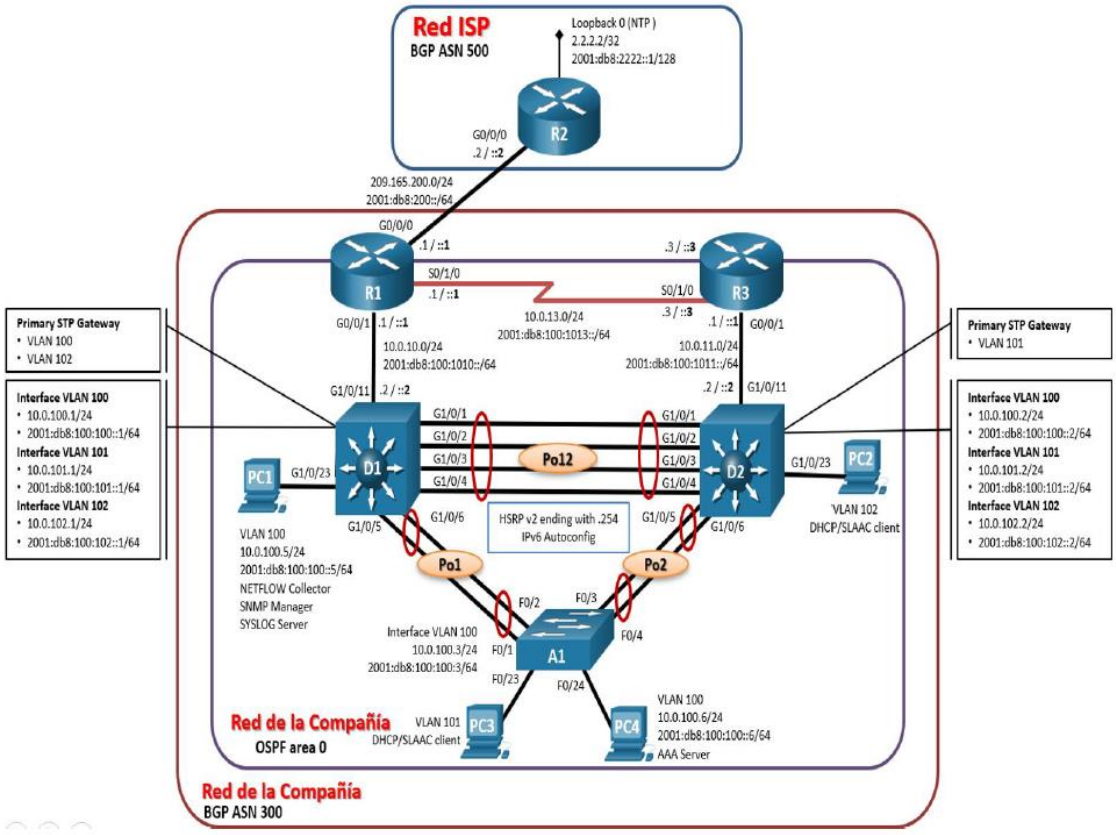


Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Direción 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

ESCENARIO

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

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.

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:

Router R1

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
```

```
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface g0/0/0
R1(config-if)#ip address 209.165.200.255 255.255.255.254
Bad mask /31 for address 209.165.200.255
R1(config-if)#ex
R1(config)#interface g0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface g0/0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config)#interface s0/1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

Router R2

```
Router>ena
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
```

```
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Router R3

```
Router>ena
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface g0/0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
```

```
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

Switch D1

```
Switch>ena
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment,Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface g1/0/11
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0
```

```
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102:1/64
% Incomplete command.
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-route 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range g1/0/1-10
D1(config-if-range)#shutdown
D1(config-if-range)#interface range g1/0/12-24
D1(config-if-range)#shutdown
D1(config-if-range)#interface range g1/1/1-4
D1(config-if-range)#shutdown
D1(config-if-range)#exit
interface vlan 999
ip address 10.0.99.10 255.255.255.0
ipv6 address fe80::d1:5 link-local ipv6 address 2001:db8:100:99::1/64
shutdown
exit
```

Switch D2

```
Switch>ena
Switch#config t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface g1/0/11
D2(config-if)#no switchport
D2(config-if)#
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
```

D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-route 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range g1/0/1-10
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range g1/0/12-24
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range g1/1/1-4
D2(config-if-range)#shutdown
D2(config)#exit
interface vlan 999
ip address 10.0.99.11 255.255.255.0
ipv6 address fe80::d1:4 link-local ipv6 address 2001:db8:100:99::2/64
no shutdown
exit

Switch A1

Switch>ena
Switch#config t

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
enter
Switch>ena
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
A1(config)#interface vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range f0/5-22
A1(config-if-range)#shutdown
A1(config-if-range)#exit
interface vlan 999
ip address 10.0.99.12 255.255.255.0
ipv6 address fe80::d1:3  link-local ipv6 address 2001:db8:100:99::3/64
```

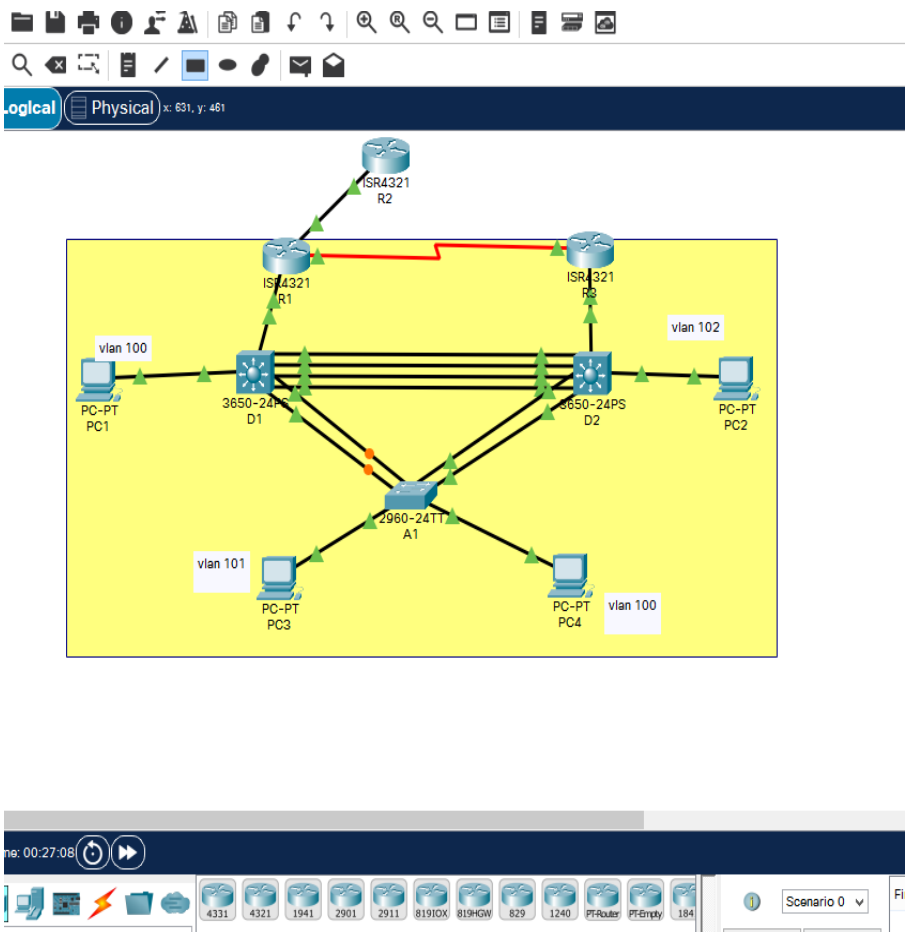
no shutdown

exit

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

c. Configure el direccionamiento de los host PC1 y PC4 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 2. Simulación de escenario propuesto Packet Tracer



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:

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

Especificación: Habilite enlaces trunk 802.1Q entre:

D1 y D2

D1 y A1

D2 y A1

Switch A1

```
A1(config)#interface range f0/0-4
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface vlan 999
ip address 10.0.99.4 255.255.255.0
ipv6 address fe80::d2:8 link-local
ipv6 address 2
A1(config)#interface range f0/23
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 100
A1(config-if-range)#exit
A1(config)#interface range f0/24
A1(config-if-range)#switchport mode access
A1(config-if-range)#switchport access vlan 101
```

Switch D1

```
D1(config)#interface range G1/0/1-6
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
 no shutdown
interface vlan 999
ip address 10.0.99.2 255.255.255.0
ipv6 address fe80::d2:6 link-local
ipv6 address 2001:db8:100:99::2/64
no shutdown
D1(config)#interface range G1/0/23
D1(config-if-range)#switchport mode access
D1(config-if-range)#switchport access vlan 100
```

Switch D2

```
D2(config)#interface range G1/0/1-6
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface vlan 999
ip address 10.0.99.3 255.255.255.0
ipv6 address fe80::d2:7 link-local
ipv6 address 2001:db8:100:99::3/64
no shutdown
D2(config)#interface range G1/0/23
D2(config-if-range)#switchport mode access
D2(config-if-range)#switchport access vlan 102
```

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales. Especificación: Use VLAN 999 como la VLAN nativa.

```
vlan 999
 name NATIVE
```

Switch A1

A1(config)#interface range f0/0-4
switchport trunk native vlan 999
Configuracion trunk allowed
A1(config)#interface range fastEthernet 0/1-4
A1(config-if-range)#switchport trunk allowed vlan 100
A1(config-if-range)#switchport trunk allowed vlan 101

Switch D1

D1(config)#interface range G1/0/1-6
switchport trunk native vlan 999

Switch D2

D2(config)#interface range G1/0/1-6
switchport trunk native vlan 999

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

Especificación: Use Rapid Spanning Tree (RSPT).

A1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree mode rapid-pvst

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).

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

D1(config)#spanning-tree vlan 1 root primary
D2(config)#spanning-tree vlan 1 root secondary

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

Especificación: Use los siguientes números de canales:

D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2

D1 a D2 – Port channel 12

```
D1(config)# interface range g1/0/1-4
D1(config)#shutdown
D1(config-if-range)# channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D1(config-if-range)# exit
D1(config)# interface port-channel 12
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config)# interface range g1/0/1-4
D1(config)#no shutdown
```

```
D2(config)# interface range g1/0/1-4
D2(config)#shutdown
D2(config-if-range)# channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D2(config-if-range)# exit
D2# config t
D2(config)# interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)# interface range g1/0/1-4
D2(config)#no shutdown
```

D1 a A1 – Port channel 1

D1(config)# interface range g1/0/5-6
D1(config)#shutdown
D1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
D1(config-if-range)# exit
D1(config)#interface port-channel 1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#exit
D1(config)# interface range g1/0/5-6
D2(config)#no shutdown

A1# config t
A1#(config)# interface range f0/1-2
A1#(config)#shutdown
A1# (config-if-range)# channel-group 1 mode active
A1# (config-if-range)# exit
A1# (config)#interface port-channel 1
A1# (config-if)#switchport mode trunk
A1# (config-if)#switchport trunk native vlan 999
A1# (config-if)#exit
A1#(config)# interface range f0/1-2
A1#(config)#no shutdown

D2 a A1 – Port channel 2

D2(config)# interface range g1/0/5-6
D2(config)#shutdown
D2(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)# exit
D2(config)#interface port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999

```
D2# (config-if)#exit
D2(config)# interface range g1/0/5-6
D2(config)#no shutdown
```

```
A1# config t
A1#(config)# interface range f0/3-4
A1#(config)#shutdown
A1# (config-if-range)# channel-group 2 mode active
A1# (config-if-range)# exit
A1# (config)#interface port-channel 2
A1# (config-if)#switchport mode trunk
A1# (config-if)#switchport trunk native vlan 999
A1# (config-if)#exit
A1#(config)# interface range f0/1-2
A1#(config)#no shutdown
```

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.

Especificaciones: 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).

```
A1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)# interface range fa0/23
A1(config)#switch mode access
A1(config)#switch access vlan 101
A1(config)# interface range fa0/24
A1(config)#switch mode access
A1(config)#switch access vlan 100
```

```
D1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)# interface range G1/0/23
```

D1(config)#switch mode access
D1(config)#switch access vlan 100

D2# config t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)# interface range fa0/24
D2(config)#switch mode access
D2(config)#switch access vlan 102

2.7 Verifique los servicios DHCP IPv4

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

2.8 Verifique la conectividad de la LAN local de acuerdo a la tabla 2.

Tabla 2. Tabla de direcciones IP Para realizar ping.

Realizar los siguientes ping	Direcciones IP por Dispositivos.			
	D1	D2	PC1	PC4
PC1	10.0.100.1	10.0.100.2		10.0.100.6
PC2	10.0.100.1	10.0.100.2		
PC3	10.0.100.1	10.0.100.2		
PC4	10.0.100.1	10.0.100.2	10.0.100.5	

Figura 3. Ping PC1 a D1 – D2 – PC4

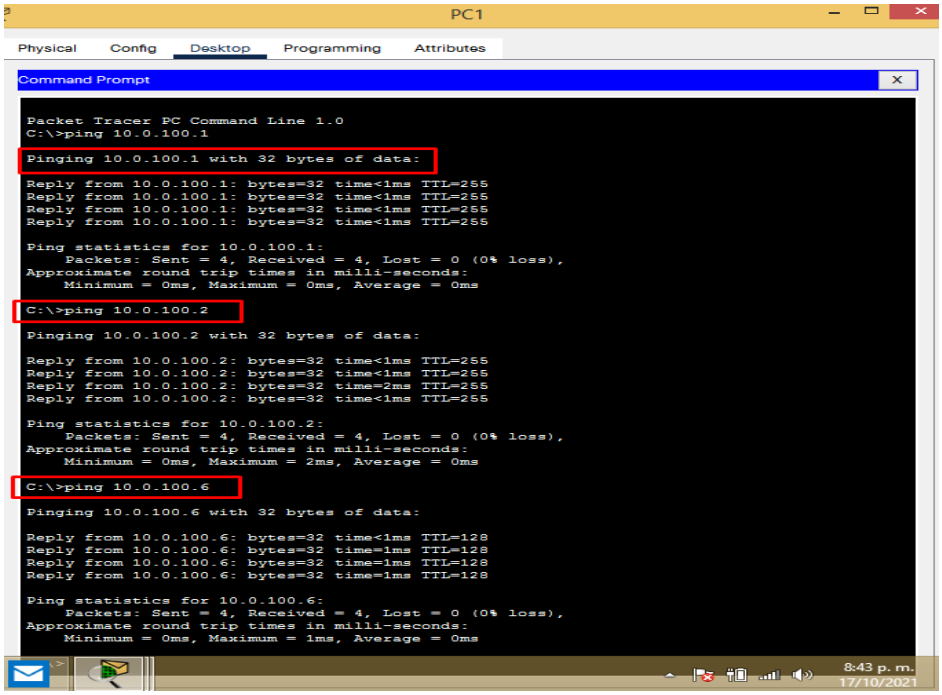


Figura 4. Ping PC2 a D1 – D2

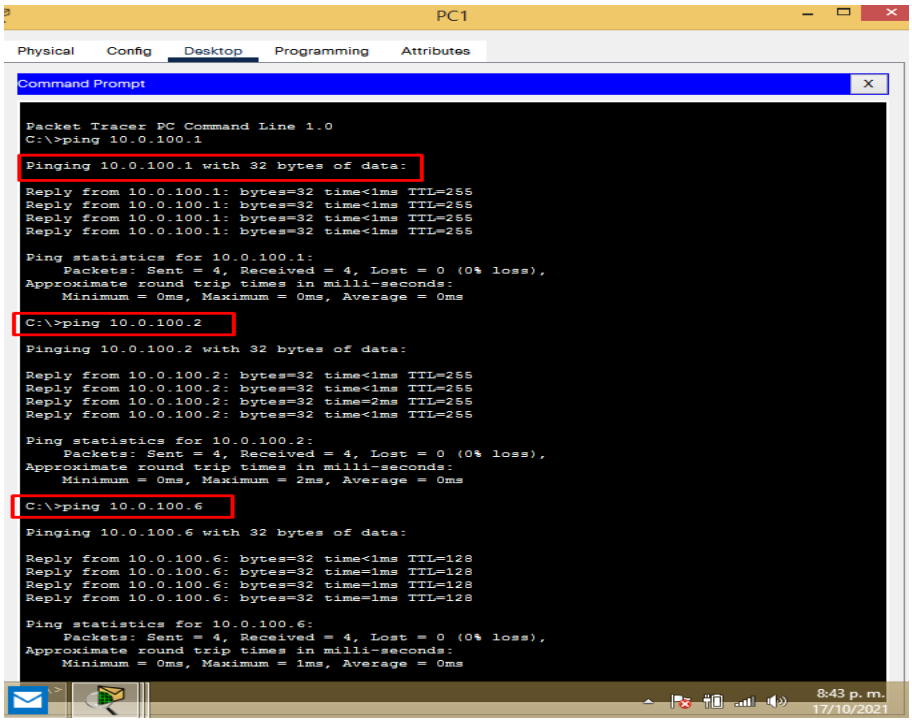


Figura 5. Ping PC3 a D1 – D2

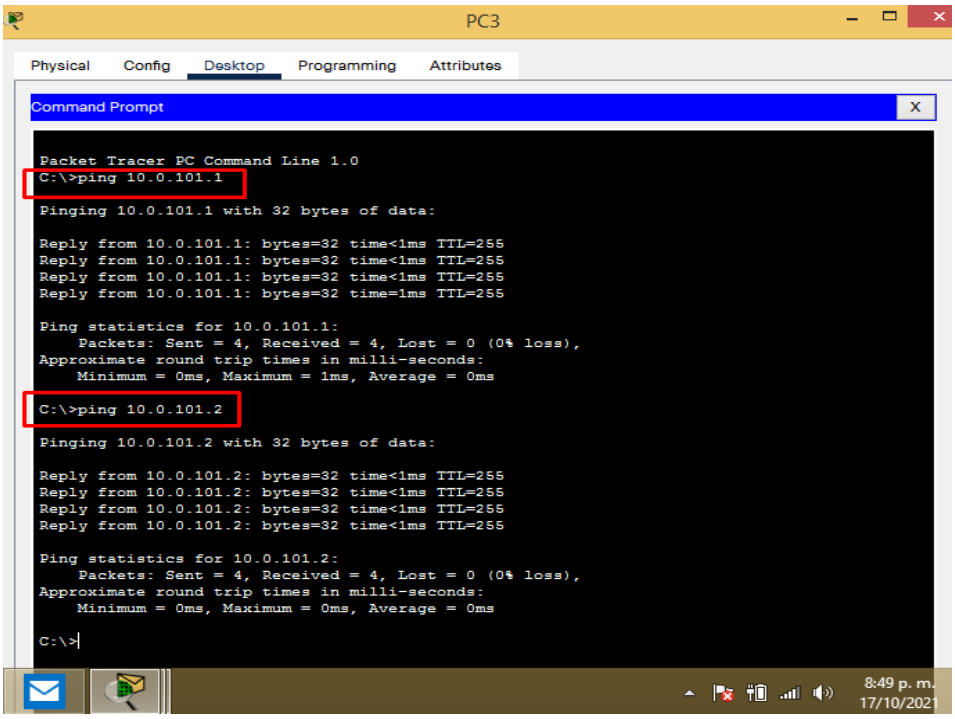
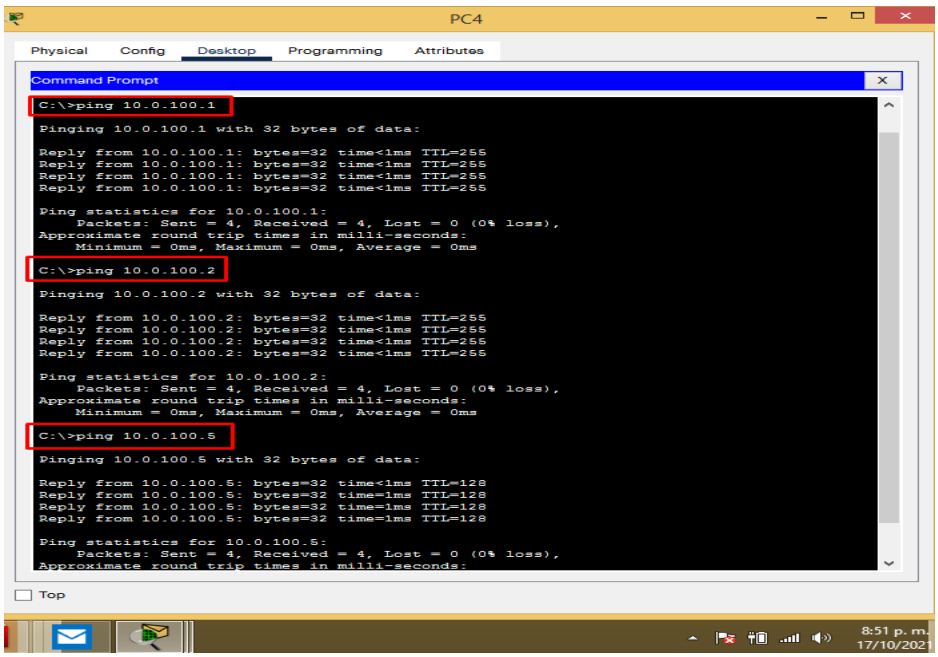


Figura 6. Ping PC4 a D1 – D2 – PC1

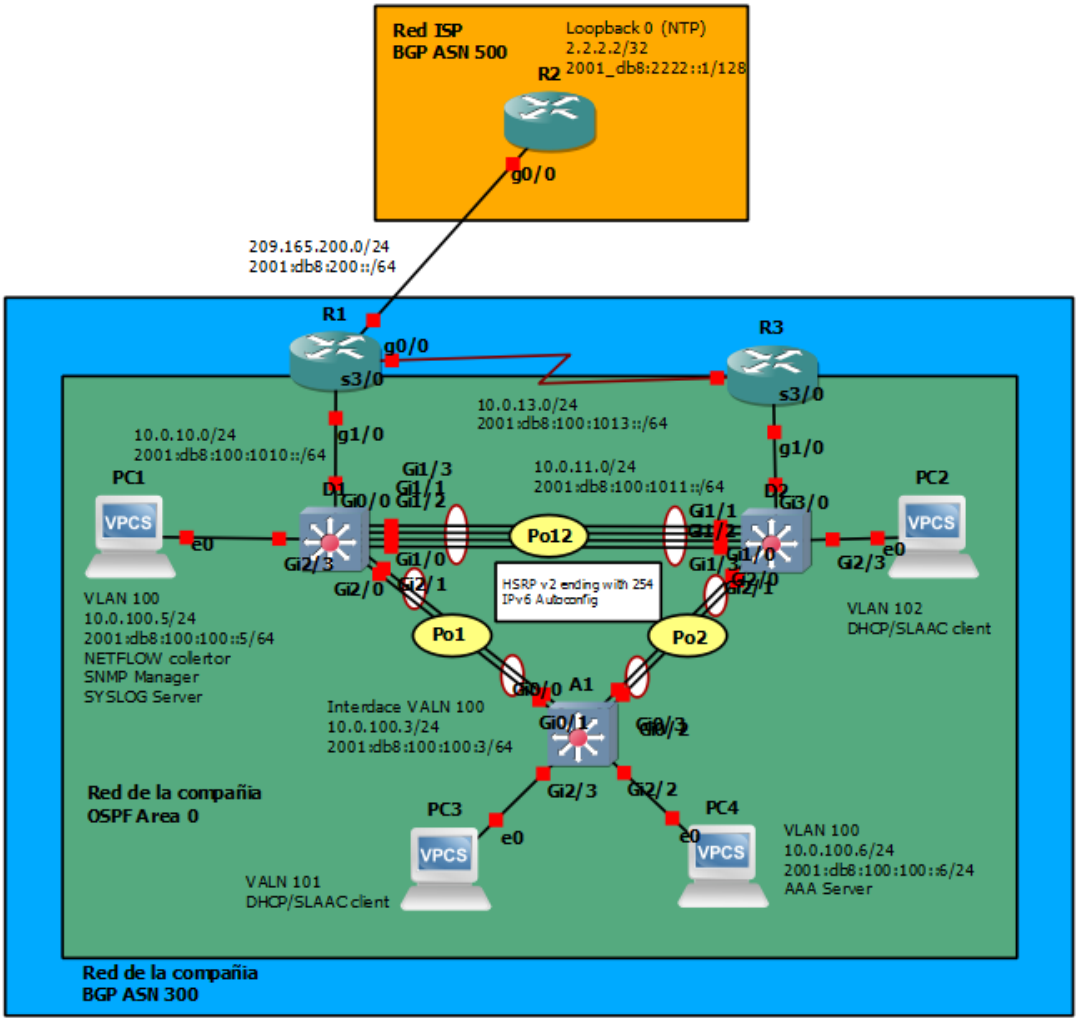


Parte 3: Configurar los protocolos de enrutamiento

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.

Figura 7. Topología de red en GNS3



Las tareas de configuración son las siguientes:

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

Especificaciones:

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

R1: 0.0.4.1

R3: 0.0.4.3

D1: 0.0.4.131

D2: 0.0.4.132

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

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

R1

```
R1(config)#router ospf 4
R1(config-router)# router-id 0.0.4.1
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate
R1(config-router)# exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
```

R1(config)#ipv6 route 2001:db8:100::/48 null0

R3

R3(config)#router ospf 4

R3(config-router)# router-id 0.0.4.3

R3(config-router)# network 10.0.11.0 0.0.0.255 area 0

R3(config-router)# network 10.0.13.0 0.0.0.255 area 0

R3(config-router)# exit

* Nov 25 05:35:24.211: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial3/0 from LOADING to FULL, Loading Done

R3(config-router)# exit

D1

D1(config)#router ospf 4

D1(config-router)# router-id 0.0.4.131

D1(config-router)# network 10.0.100.0 0.0.0.255 area 0

D1(config-router)# network 10.0.101.0 0.0.0.255 area 0

D1(config-router)# network 10.0.102.0 0.0.0.255 area 0

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

D1(config-router)# passive-interface default

D1(config-router)# no passive-interface g1/0/11

D1(config-router)# exit

D2

D2(config)#router ospf 4

D2(config-router)# router-id 0.0.4.132

D2(config-router)# network 10.0.100.0 0.0.0.255 area 0

D2(config-router)# network 10.0.101.0 0.0.0.255 area 0

D2(config-router)# network 10.0.102.0 0.0.0.255 area 0

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

D2(config-router)# passive-interface default

D2(config-router)# no passive-interface g1/0/11

D2(config-router)# exit

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

Especificaciones:

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

R1: 0.0.6.1
R3: 0.0.6.3
D1: 0.0.6.131
D2: 0.0.6.132

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

R1

```
R1(config-router)# exit
R1(config)#ipv6 router ospf 6
R1(config-rtr)# router-id 0.0.6.1
R1(config-rtr)# default-information originate
R1(config-rtr)# exit
R1(config)#interface g1/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
R1(config)#interface s3/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
```

R3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)# router-id 0.0.6.3
R3(config-rtr)# exit
R3(config)#interface g1/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#interface s3/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
```

D1

El comando OSPF en los swicth no lo soporta GNS3

```
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface g0/0
exit
interface g0/0
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
```

D2

El comando OSPF en los swicth no lo soporta GNS3

```
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g3/0
```

```
exit
interface g3/0
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
```

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

Especificaciones:

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
Una ruta estática predeterminada IPv4.
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:
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).

```
R2
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# neighbor 209.165.200.225 remote-as 300
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300
R2(config-router)# address-family ipv4
R2(config-router-af)#  neighbor 209.165.200.225 activate
R2(config-router-af)#  no neighbor 2001:db8:200::1 activate
R2(config-router-af)#  network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#  network 0.0.0.0
R2(config-router-af)#  exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)#  no neighbor 209.165.200.225 activate
R2(config-router-af)#  neighbor 2001:db8:200::1 activate
R2(config-router-af)#  network 2001:db8:2222::/128
R2(config-router-af)#  network ::/0
R2(config-router-af)#  exit-address-family
```

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

Especificaciones:

Configure dos rutas resumen estáticas a la interfaz Null 0:

Una ruta resumen IPv4 para 10.0.0.0/8.

Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1.

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

En IPv4 address family:

Deshabilite la relación de vecino IPv6.

Habilite la relación de vecino IPv4.

Anuncie la red 10.0.0.0/8. En IPv6 address family:

Deshabilite la relación de vecino IPv4.

Habilite la relación de vecino IPv6.

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

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

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 host en la “Red de la Compañia”.

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.

Especificaciones:

Cree dos IP SLAs.

Use la SLA número 4 para IPv4.

Use la SLA número 6 para IPv6.

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

Programe la SLA para una implementación inmediata sin tiempo de finalización.

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

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

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

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

D1

D1(config)#ip sla 4

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

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

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

D1(config)#ip sla 6

D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1

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

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

D1(config)#ip sla schedule 4 life forever start-time now

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

D1(config)#track 4 ip sla 4

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

D1(config-track)# exit

D1(config)#track 6 ip sla 6

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

D1(config-track)# exit

*Nov 25 05:57:13.517: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, c hanged state to down 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)#

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

D1(config)#end

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

Especificaciones:

Cree IP SLAs.
Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6.
Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.
Programe la SLA para una implementación inmediata sin tiempo de finalización.
Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la SLA 6.
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D2
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency
% Incomplete command.
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
% Incomplete command.
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
D2(config)#track 6 ip sla 6
D2(config-track)# delay down 10 up 15
D2(config-track)# exit
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
```

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

4.3 En D1 configure HSRPv2.

Especificaciones:

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

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decrementa en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 6 y decrementa en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

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

```
D1
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)#
D1(config-if)# standby 116
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)#
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
D1(config)#end
```

4.4 En D2, configure HSRPv2.

Especificaciones:

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decrementa en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

```
D2
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)# standby 114 track 4 decrement 60
D2(config-if)# standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 124 track 4 decrement 60
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
D2(config-if)# exit
D2(config)#end
```

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:

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

Especificación: Contraseña: cisco12345cisco

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

Especificaciones:

Detalles de la cuenta encriptada SCRYPT:

Nombre de usuario Local: sadmin

Nivel de privilegio 15

Contraseña: cisco12345cisco

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

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

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

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

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

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

R1(config)#aaa new-model
R1(config)#radius server RADIUS

R3(config)#aaa new-model
R3(config)#radius server RADIUS

D1(config)#aaa new-model
D1(config)#radius server RADIUS

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

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

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

Especificaciones:

Especificaciones del servidor RADIUS.:
Dirección IP del servidor RADIUS es 10.0.100.6.
Puertos UDP del servidor RADIUS son 1812 y 1813.
Contraseña: $trongPass

R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass

```
R1(config-radius-server)# exit
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass

D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)# exit

D2(config-radius-server)#$v4 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)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
```

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

Especificaciones:

Especificaciones de autenticación AAA:
Use la lista de métodos por defecto
Valide contra el grupo de servidores RADIUS
De lo contrario, utilice la base de datos local.

```
R1(config)#aaa authentication login default group radius local
R1(config)#endR1(config)#aaa new-model

R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#end

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

D2(config)#aaa authentication login default group radius local
D2(config)#end
A1(config)#aaa authentication login default group radius local
A1 (config)#end

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

Especificación:

Cierre e inicie sesión en todos los dispositivos (Except R2) con el usuario: raduser y la contraseña: upass123.

Figura 8 . Verificación en servicio AAA en R1.

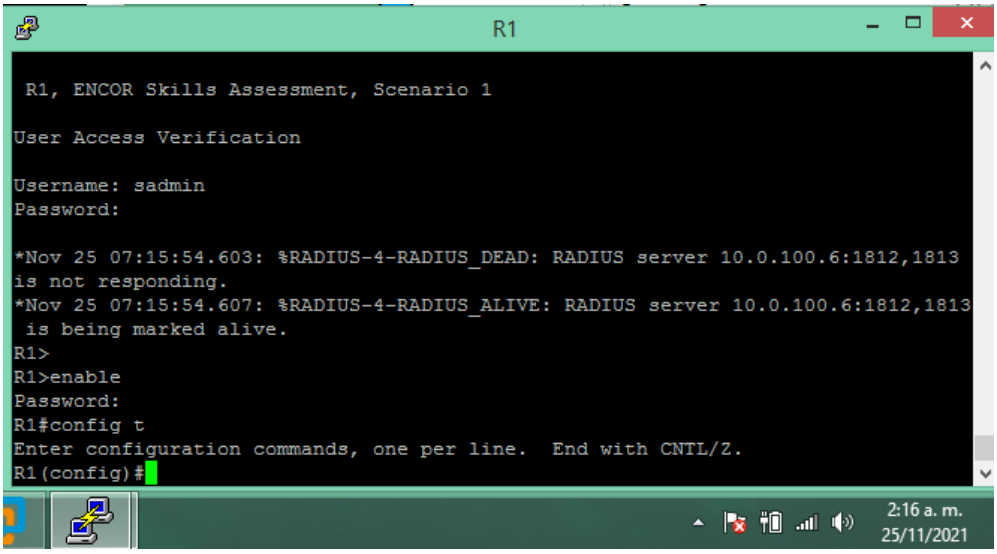


Figura 9 . Verificación en servicio AAA en R3.

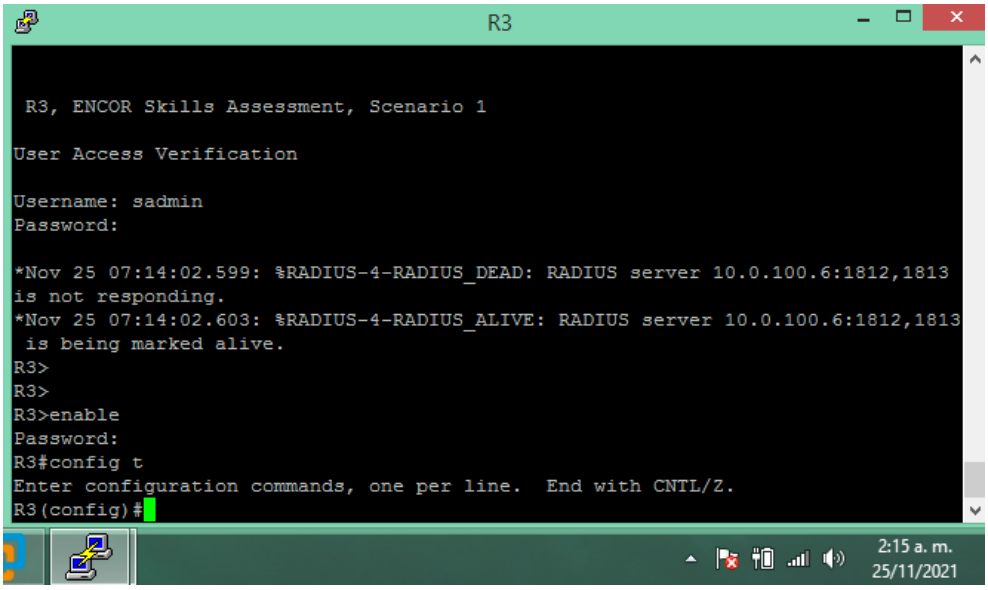


Figura 10 . Verificación en servicio AAA en D1.

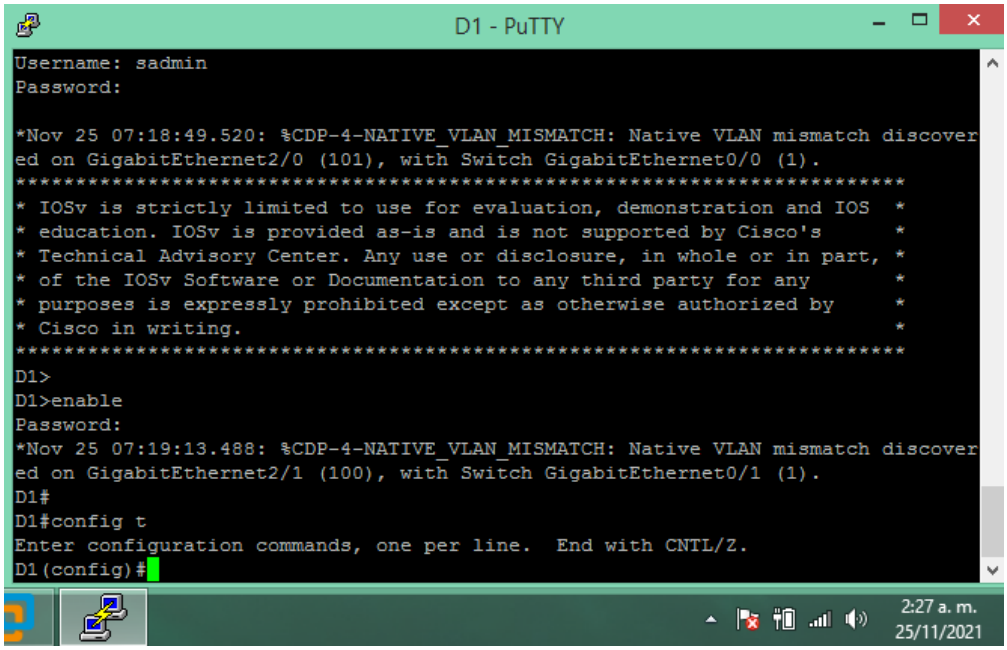


Figura 11 . Verificación en servicio AAA en D2.

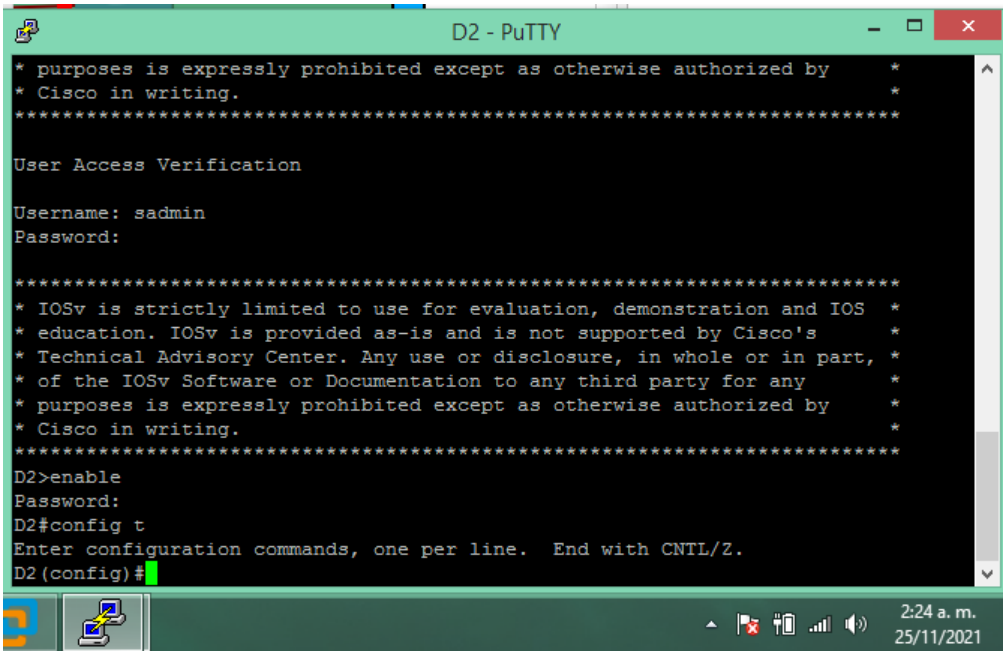


Figura 12 . Verificación en servicio AAA en D2.

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.

Especificaciones: Configure el reloj local a la hora UTC actual.

clock set 18:30:00 25 Nov 2021

6.2 Configure R2 como un NTP maestro.

Especificaciones: Configurar R2 como NTP maestro en el nivel de estrato 3.

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

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

Especificaciones:

Configure NTP de la siguiente manera:
R1 debe sincronizarse con R2.
R3, D1 y A1 para sincronizar la hora con R1.
D2 para sincronizar la hora con R3.

R1
R1(config)#ntp server 2.2.2.2
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)# permit host 10.0.100.5
R1(config-std-nacl)# exit

R3

```
R3(config)#ntp server 10.0.10.1
R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
R3(config)# logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#  permit host 10.0.100.5
R3(config-std-nacl)#  exit
```

D1

```
D1(config)#ntp server 10.0.10.1
D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
D1(config)# logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#  permit host 10.0.100.5
D1(config-std-nacl)#  exit
```

D2

```
D2(config)#ntp server 10.0.10.1
D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5
D2(config)# logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#  permit host 10.0.100.5
D2(config-std-nacl)#  exit
```

A1

```
A1(config)#ntp server 10.0.10.1
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#  permit host 10.0.100.5
A1(config-std-nacl)#  exit
```

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones:

Especificaciones de SNMPv2:
Únicamente se usará SNMP en modo lectura (Read-Only).
Limite el acceso SNMP a la dirección IP de la PC1.
Configure el valor de contacto SNMP con su nombre.
Establezca el *community string* en ENCORSA.
En R3, D1, y D2, habilite el envío de *traps config* y *ospf*.
En R1, habilite el envío de *traps bgp, config*, y *ospf*.
En A1, habilite el envío de *traps config*.

R1

```
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)# snmp-server ifindex persist
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)#end
```

R3

```
R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end
```

D1

```
D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
```

```
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps config
% Invalid input detected at '^' marker.
D1(config)# snmp-server enable traps ospf
D1(config)#end
```

D2

```
D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server enable traps config
% Invalid input detected at '^' marker.
D2(config)# snmp-server enable traps ospf
D2(config)#end
```

A1

```
A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)# snmp-server ifindex persist
A1(config)# snmp-server enable traps config
% Invalid input detected at '^' marker.
A1(config)# snmp-server enable traps ospf
A1(config)#end
```

CONCLUSIONES

Durante el desarrollo del presente trabajo se desarrolla la capacidad de identificar fallas en redes LAN y WAN, así mismo poder resolverlas de la mejor forma por medio de comandos IOS y análisis en el tráfico de las interfaces en un entorno real.

Se realiza satisfactoriamente el uso de herramientas de simulación para la emulación de redes de comunicación empresarial donde se establece la configuración de una topología de red determinada, como también analizar establecer y comprender los parámetros de configuración inicial en los dispositivos que componen la red como PCs, Switch y Routers.

Se desarrollan las capacidades para complementar la configuración de red de capa 2 para poder establecer la comunicación entre diferentes dispositivos apropiando los conceptos y en la práctica establecer la configuración de interfaces troncales, VLAN nativa, protocolo STP, como también establecer la comunicación en dispositivos por DHCP.

Por medio del escenario propuesto en el trabajo final se comprende satisfactoriamente los diferentes conceptos y aplicaciones relacionados a las partes que componen el diplomado en CISCO CCNP correspondiente al switching, routing y Wireless, el cual nos brinda el conocimiento como principal herramienta de forma avanzada para poder establecer el diseño o infraestructura de una red.

BIBLIOGRAFIA

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 186-215. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: OSPF. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 353-367. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 120-138. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 223-230. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: BGP. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 392-409. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 810-839. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley., GARZA Ramiro., GOOLEY, Jason., HUCABY, David. “CISCO Press: Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR”. {En línea}. {2020} 1072-1075. Disponible en: https://1drv.ms/b/s!AAIGg5JUgUBthk8