DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES

CARLOS ANDRÉS ARIAS FONSECA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ANDRÉS ARIAS FONSECA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Madrid, 29 de noviembre de 2021

AGRADECIMIENTOS

El agradecimiento de este trabajo va dirigido a mi esposa y a mi hija, por su apoyo incondicional durante este tiempo de crecimiento profesional, No fue sencillo llegar a este peldaño más de mi vida profesional, pero con esfuerzo y dedicación se logran grandes sueños. Doy gracias a Dios por darme la oportunidad de cumplir mi meta de ser profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN (Virtual LAN ó red de área local virtual): es un método con el cual se crean redes lógicas de manera independiente para la propia red física.

DHCP (Dynamic Host Configuration Protocolo ó protocolo de configuración dinámica de host): es un protocolo de red con el cual un servidor DHCP establece una IP dinámica para redes de tipo cliente/servidor, con la posibilidad de configurarse para que se comuniquen con otras redes IP.

OSPF (Open Shortest Path First): es un protocolo desarrollado para redes IP, el cual se basa en el algoritmo de primera vía más corta SPF. OSPF sirve para direccionamientos de tipo enlace-estado de pasarela interior.

BGP (Border Gateway Protocol o protocolo de puerta de enlace de frontera): es un protocolo que permite el intercambio de información de enrutamiento entre varios sistemas o dispositivos, el cual puede elegir rutas que no tengan bucles de red usando las políticas de red

RADIUS (Remote Authentication Dial-In User Service): este protocolo tiene como uso la autorización y autorización para aplicaciones con acceso a redes.

SNMP (Simple Network Management Protocol o protocolo simple de administración de red): este protocolo facilita la administración de los dispositivos en una red con el fin de monitorear el estado del dispositivo y el estado de los syslog.

RESUMEN

En este documento se evidencia el desarrollo de un escenario planteado para la medir los conceptos adquiridos durante el diplomado para la certificación CISCO CCNP. En él se muestra la configuración de la topología de red suministrada y para su desarrollo se compilan temáticas de redes, enrutamiento y conmutación, vistas durante todo el proceso de aprendizaje.

Este escenario se realiza mediante un simulador virtual llamado GNS3, dado que no se contaba con la electrónica de red física, por lo cual se emula el sistema operativo que manejan los switches y enrutadores que se usan a lo largo del desarrollo del documento.

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

ABSTRACT

This document shows the development of a scenario proposed to measure the concepts acquired during the diploma for the CISCO CCNP certification. It shows the configuration of the supplied network topology and for its development, networking, routing and switching topics are compiled, seen throughout the learning process.

This scenario is carried out using a virtual simulator called GNS3, since there was no physical network electronics, which is why the operating system used by the switches and routers used throughout the development of the document is emulated.

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics.

INTRODUCCIÓN

Este documento contiene el desarrollo de un escenario propuesto de evaluación de habilidades para la certificación CISCO CCNP del diplomado de profundización CISCO, en el cual se realiza el montaje de la configuración de la topología de red suministrada, la cual consta de seis partes.

En la primera parte se configuran los parámetros básicos con los cuales se realiza la simulación, tales como la selección de los dispositivos, las conexiones cableadas y el direccionamiento. En la segunda parte, se inicia con la configuración de la capa 2 asignando servicios de DHCP y realizar la conectividad entre los enlaces troncales, port channel de cada router y habilitando Rapid Spanning Tree. En la tercera parte se inicia la configuración de los protocolos de enrutamiento donde se inicia las configuraciones de OSPF, tanto para IPv4 como IPv6, la creación de las rutas estáticas y las creaciones de los BGP. Para la cuarta parte se inicia la configuración de redundancia en el primer salto (HSRP) habilitando IP SLA, ya que es una herramienta que permite monitorear los servicios y aplicaciones IP con el tráfico activo en la red. En la quinta parte se trabaja temas de seguridad como encriptación de contraseñas, configuración de servidor radius y autenticación en los dispositivos mediante radius. Finalmente, en la sexta parte se configura las funciones para la administración de red, tales como la sincronización de la hora con NTP, configuración de envío del syslog y la configuración de SNMP.

Este escenario fue implementado en GNS3 con GNS3VM, ya que los switches disponibles tanto en Packet Tracer como en el propio GNS3 no tenían las capabilidades que se requieran para este escenario, por lo tanto, se utiliza una vios con CISCO IOSVL2 15.2.1 para hacer uso de las capabilidades requeridas para D1 y D2.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología de la red

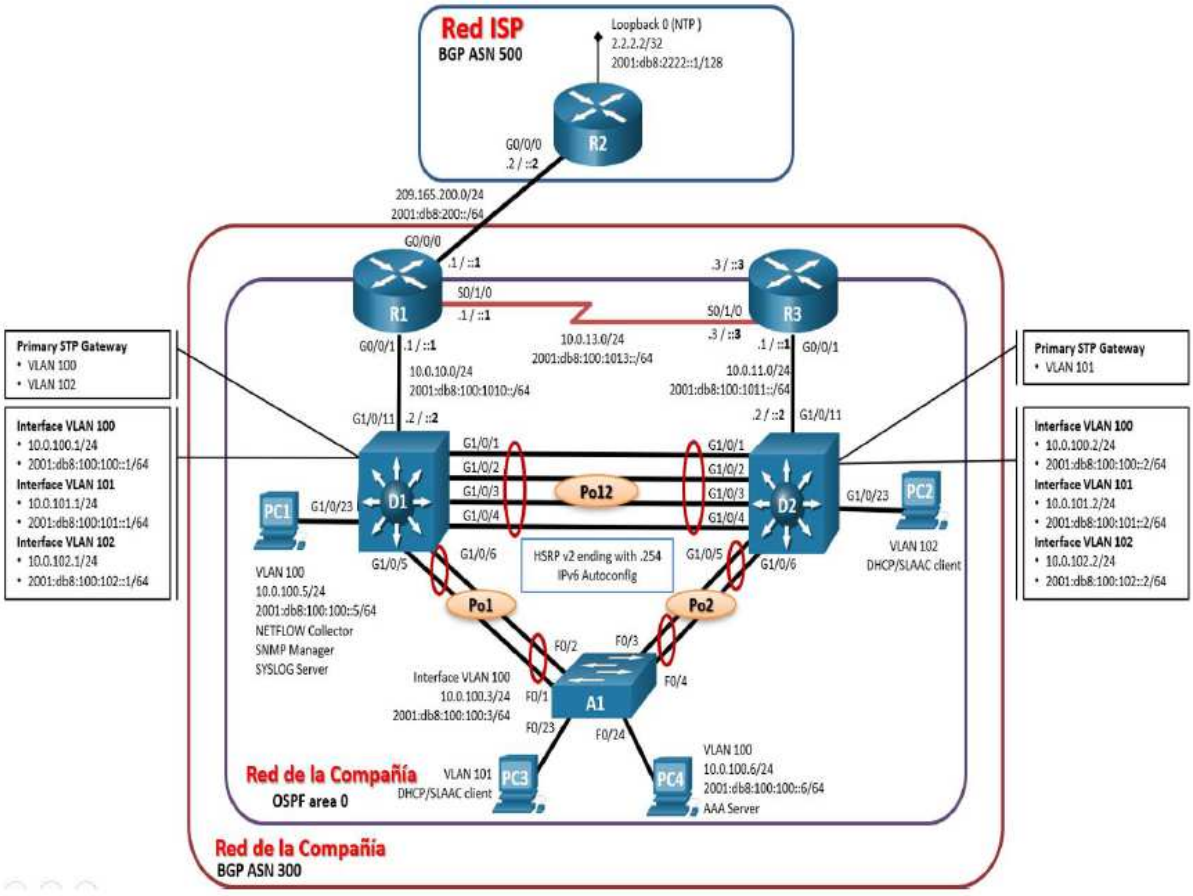


Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G2/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	Fa0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S3/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G2/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	Fa0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S3/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	GI0/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	GI0/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64

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

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.

Se hace el montaje de la topología en Packet Tracer como se describe en la guía.

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:

Después de cablear la topología propuesta iniciamos configurando los parámetros básicos y direccionamientos que nos entrega la guía para la topología propuesta.

Router R1

```
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 g2/0
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 fa0/1
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 s3/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
```

Router R2

```
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 g2/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

Router R3

```
hostname R3
```

```
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface fa0/1
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 s3/0
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
```

Switch D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface gi0/0
```

```
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

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 synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface gi0/0
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
```

```
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

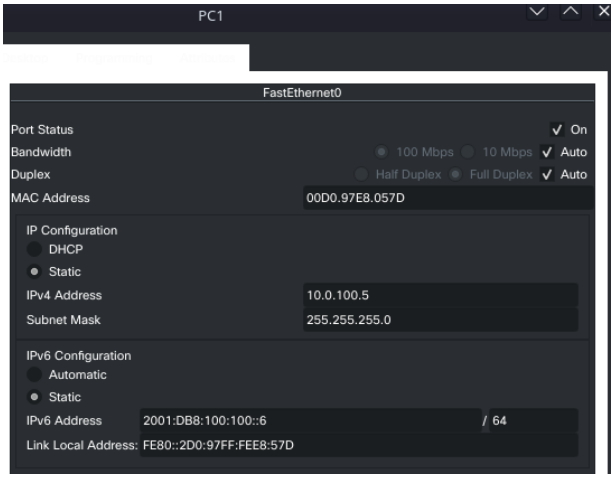
Switch A1

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

b. Copy running-config startup-config

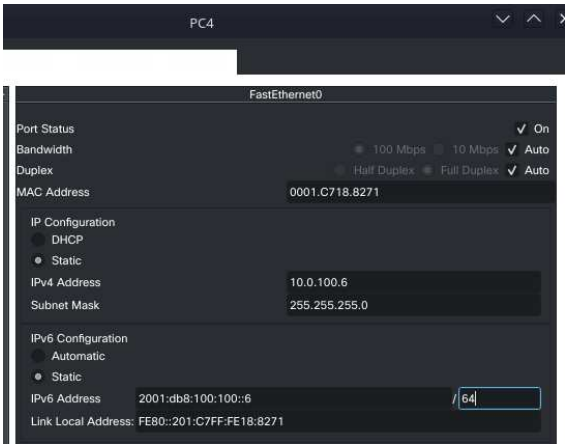
PC1

Figura 2. Direccionamiento host PC 1



PC4

Figura 3. Direccionamiento host PC 4



Parte 2

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

Tarea 2.1

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

En esta tarea vamos a proceder a configurar interfaces que van a realizar el trabajo de intercambio entre equipos de las vlan configuradas, el comando range nos ayuda a hacer una sola configuración en la cantidad de puertos seleccionada en simultaneo. y el encapsulamiento con dot1q es para poder combinar distintas vlan en las interfaces troncales sin que afecte a la vlan nativa.

Habilite enlaces trunk 802.1Q entre:

D1 and D2

```
conf t
interface range gi0/1-3
switchport trunk encapsulation dot1q
switchport mode trunk
interface gi1/0
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

D1 and A1

```
conf t
interface range gi1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

D2 and A1

```
conf t
interface range gi1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Tarea 2.2

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

Especificación Use VLAN 999 como la VLAN nativa.

En D1 y D2

```
interface range gi0/1-3
switchport trunk native vlan 999
interface gi1/0
switchport trunk native vlan 999
exit
```

En D1 y A1

```
interface range gi1/1-2
switchport trunk native vlan 999
exit
```

A1

```
interface range gi0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
exit
```

En D2 y A1

```
interface range gi1/1-2
switchport trunk native vlan 999
exit
```

A1

```
interface gi0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
interface gi1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
```

```
exit
```

Tarea 2.3

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

Este protocolo nos ayuda a gestionar los enlaces redundantes que estamos creando en la topología con el fin de crear una convergencia rápida.

```
conf t
spanning-tree mode rapid-pvst
```

Tarea 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).

Para esta configuración se determina cuales el punto de acceso principal según la configuración de la vlan y se indica el punto secundario hacia donde se puede desbordar el tráfico cuando el enlace primario falle.

D1

```
conf t
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

D2

```
conf t
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
```

Tarea 2.5

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

En este punto se crea una interface virtual, donde se realiza una agrupación de enlace o puertos, se unen los puertos a un port channel y este envía el tráfico

distribuido por los enlaces que pertenezcan a ese port channel si uno de los enlaces falla sigue enviando el tráfico por los que estén disponibles.

Use los siguientes números de canales:

D1 a D2 – Port channel 12

```
conf t
interface range gi0/1-3
channel-group 12 mode active
interface gi1/0
channel-group 12 mode active
interface port-channel 12
switchport trunk encapsulation dot1q
switchport mode trunk
```

D1 a A1 – Port channel 1

```
conf t
interface range gi1/1-2
channel-group 1 mode active
interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

A1

```
interface range gi0/1-2
channel-group 1 mode active
interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

D2 a A1 – Port channel 2

```
conf t
interface range gi1/1-2
channel-group 2 mode active
interface port-channel 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

A1

```
interface gi0/3
channel-group 2 mode active
interface gi1/0
channel-group 2 mode active
interface port-channel 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

Tarea 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.

Aquí se configuran los equipos cliente para que puedan acceder a la vlan respectiva o puedan hacer consumo de DHCP

D1 a PC1

```
conf t
interface gi3/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
```

D2 a PC2

```
conf t
interface gi3/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
```

A1 a PC3 y PC4

```
interface gi3/2
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
```

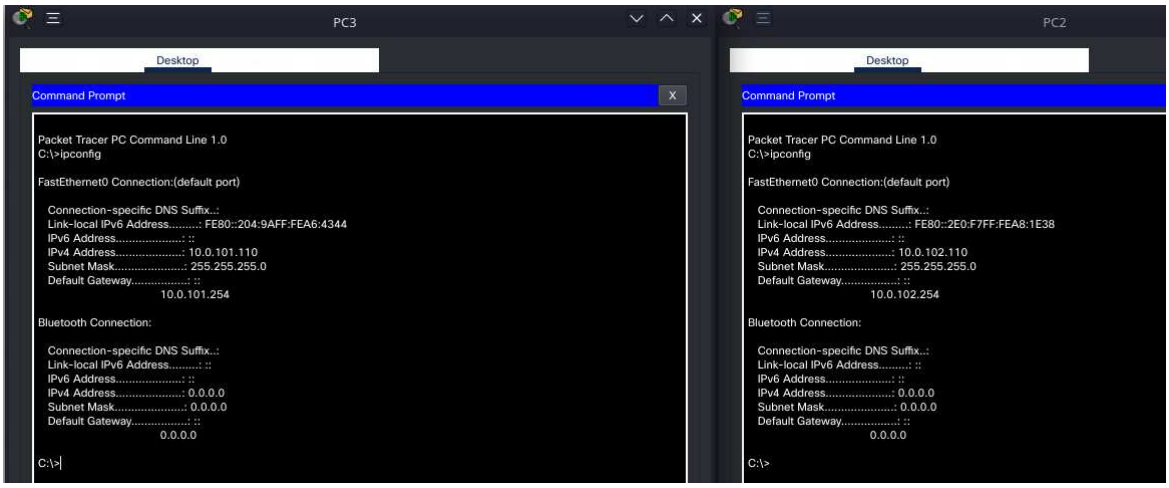
PC4

```
interface gi3/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
```

Tarea 2.7

Verifique los servicios DHCP IPv4.

Figura 4. Verificación de servicios DHCP IPv4

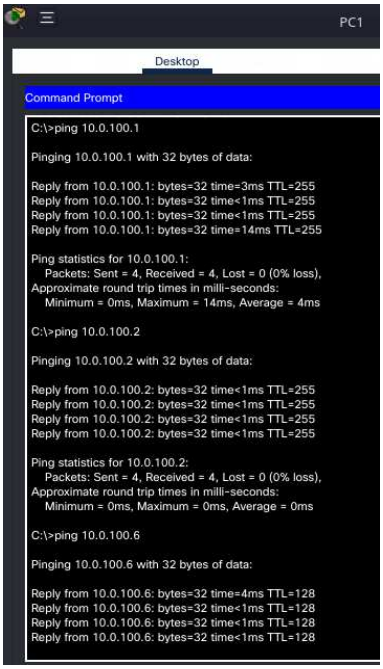


Tarea 2.8

Verifique la conectividad de la LAN local.

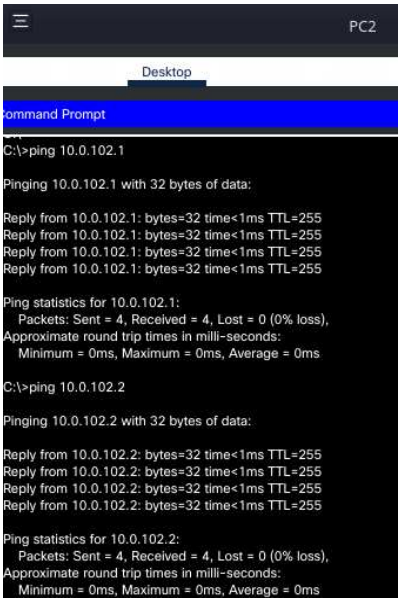
PC1

Figura 5. Ping PC1



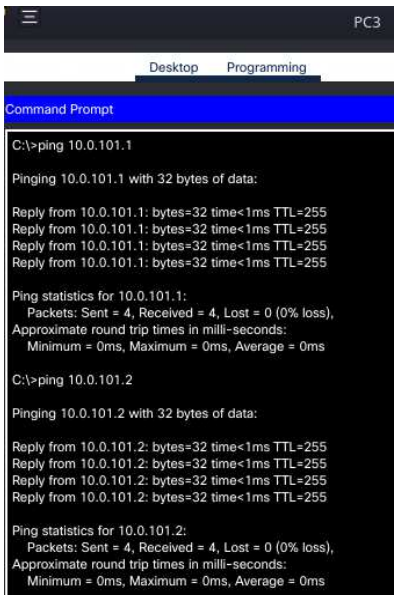
PC2

Figura 6. Ping PC2



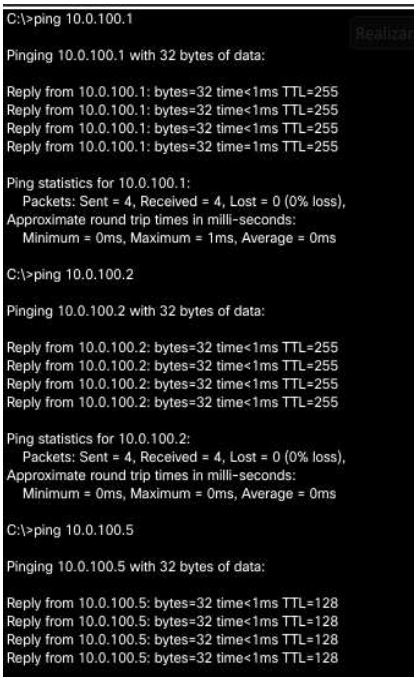
PC3

Figura 7. Ping PC3



PC4

Figura 8. 7 Ping PC4



Parte 3

Configurar los protocolos de enrutamiento

Tarea 3.1

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

En este paso vamos a crear los direccionamientos usando el protocolo de OSPF, básicamente lo que hace es buscar las vías de direccionamiento más cortas o con menos costo, y también es capaz de hacer cambios cuando una de las rutas esta caída.

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

R1: 0.0.4.1

```
conf t
router ospf 4
router-id 0.0.4.1
```

R3: 0.0.4.3

```
conf t
router ospf 4
router-id 0.0.4.3
```

D1: 0.0.4.131

```
conf t
router ospf 4
router-id 0.0.4.131
```

D2: 0.0.4.132

```
conf t
router ospf 4
router-id 0.0.4.132
```

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

R1

```
conf t
router ospf 4
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

R3

```
conf t
router ospf 4
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

D1

```
conf t
router ospf 4
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 gi0/0
exit
```

D2

```
conf t
router ospf 4
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 gi0/0
exit
```

• 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.

```
conf t
router ospf 4
default-information originate
```

Deshabilite las publicaciones OSPFv2 en:

• D1: todas las interfaces excepto G1/0/11

```
conf t
router ospf 4
passive-interface default
no passive-interface gi0/0
```

• D2: todas las interfaces excepto G1/0/11

```
conf t
router ospf 4
passive-interface default
no passive-interface gi0/0
```

Tarea 3.2

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

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

• R1: 0.0.6.1

```
conf t
ipv6 router ospf 6
 router-id 0.0.6.1
```

• R3: 0.0.6.3

```
conf t
ipv6 router ospf 6
router-id 0.0.6.3
```

• D1: 0.0.6.131

```
conf t
```

```
ipv6 router ospf 6
router-id 0.0.6.131
```
• D2: 0.0.6.132

```
conf t
ipv6 router ospf 6
router-id 0.0.6.132
```

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

R1

```
conf t
interface fa0/1
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
```

R3

```
conf t
interface fa0/1
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
```

D1

```
conf t
interface gi0/0
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
```

D2

```
conf t
interface gi0/0
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
```

• 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.

```
conf t
ipv6 router ospf 6
default-information originate
```

Deshabilite las publicaciones OSPFv3 en:

• D1: todas las interfaces excepto G1/0/11

```
conf t
ipv6 router ospf 6
passive-interface default
no passive-interface gi0/0
```

• D2: todas las interfaces excepto G1/0/11

```
conf t
ipv6 router ospf 6
passive-interface default
no passive-interface g0/0
```

Tarea 3.3

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

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
• Una ruta estática predeterminada IPv4.
• Una ruta estática predeterminada IPv6.

```
conf t
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
```

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

```
conf t
router bgp 500
bgp 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).

```
conf t
router bgp 500
neighbor 209.165.200.225 remote-as 300
network 0.0.0.0
```

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

Tarea 3.4

En R1 en la “Red ISP”, configure MP-BGP.
Configure dos rutas resumen estáticas a la interfaz Null 0:
• Una ruta resumen IPv4 para 10.0.0.0/8.
• Una ruta resumen IPv6 para 2001:db8:100::/48.

```
conf t
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
```

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

```
conf t
router bgp 300
bgp 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.

```
conf t
router bgp 300
address-family ipv4 unicast
no neighbor 2001:db8:200::2 activate
neighbor 209.165.200.226 remote-as 500
network 10.0.0.0 mask 255.0.0.0
```

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.
- Anuncie la red 2001:db8:100::/48.

```
conf t
router bgp 300
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 209.165.200.226 remote-as 500
network 10.0.0.0 mask 255.0.0.0
```

Parte 4

Configurar la Redundancia del Primer Salto (First Hop Redundancy)

Tarea 4.1

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

Cree dos IP SLAs

- Use la SLA número 4 para IPv4.

```
conf t
```

```
ip sla 4
icmp-echo 10.0.10.1
frequency 5
exit
```

• Use la SLA número 6 para IPv6.

```
conf t
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
```

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.

```
conf t
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
exit
```

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

```
conf t
track 4 ip sla 4
delay down 10 up 15
exit
```

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

```
conf t
track 6 ip sla 6
delay down 10 up 15
exit
```

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 4.2

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

Cree IP SLAs.

• Use la SLA número 4 para IPv4.

```
conf t
ip sla 4
icmp-echo 10.0.11.1
frequency 5
exit
```

• Use la SLA número 6 para IPv6.

```
conf t
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
```

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.

```
conf t
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
exit
```

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.

```
conf t
track 4 ip sla 4
delay down 10 up 15
exit
```

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

```
conf t
track 6 ip sla 6
delay down 10 up 15
exit
```

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 4.3

En D1 configure HSRPv2.

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 decremente en 60.

```
conf t
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
exit
```

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.

```
conf t
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
exit
```

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.

```
conf t
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
exit
```

Configure IPv6 HSRP grupo 106 para la VLAN 100:
• Asigne la dirección IP virtual usando ipv6 autoconfig.

• Establezca la prioridad del grupo en 150.

• Habilite la preferencia (preemption).

• Rastree el objeto 6 y decremente en 60.

```
conf t
interface vlan 100
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
```

Configure IPv6 HSRP grupo 116 para la VLAN 101:

• Asigne la dirección IP virtual usando ipv6 autoconfig.

• Habilite la preferencia (preemption).

• Registre el objeto 6 y decremente en 60.

```
conf t
interface vlan 101
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
```

Configure IPv6 HSRP grupo 126 para la VLAN 102:

• Asigne la dirección IP virtual usando ipv6 autoconfig.

• Establezca la prioridad del grupo en 150.

• Habilite la preferencia (preemption).

• Rastree el objeto 6 y decremente en 60.

```
conf t
interface vlan 102
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Tarea 4.4

En D2, configure HSRPv2

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 decremente en 60.

```
conf t
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
exit
```

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.

```
conf t
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
exit
```

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.

```
conf t
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
exit
```

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

```
conf t
interface vlan 100
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
```

exit

.

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.

```
conf t
interface vlan 101
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
```

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.

```
conf t
interface vlan 102
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Parte 5

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Tarea 5.1

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

Contraseña: cisco12345cisco

```
conf t
enable algorithm-type SCRYPT secret cisco12345cisco
exit
```

Tarea 5.2

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

Detalles de la cuenta encriptada SCRYPT:

• Nombre de usuario Local: sadmin

• Nivel de privilegio 15

• Contraseña: cisco12345cisco

```
conf t
username sadmin privilege 15 algorithm-type SCRYPT secret
    cisco12345cisco
exit
```

Tarea 5.3

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

Habilite AAA

```
conf t
aaa new-model
exit
```

Tarea 5.4

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

Especificaciones del servidor RADIUS.:

• Dirección IP del servidor RADIUS es 10.0.100.6.

• Puertos UDP del servidor RADIUS son 1812 y 1813.

• Contraseña: $trongPass

```
conf t
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit
```

Tarea 5.5

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

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.

```
conf t
aaa authentication login default group radius local
exit
```

Tarea 5.6

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

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

Figura 9. Verificación autenticación radius

Parte 6

Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red.

Tarea 6.1

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

Configure el reloj local a la hora UTC actual

```
conf t
clock timezone UTC -5
exit
clock set 22:45:00 27 NOV 2021
```

Tarea 6.2

Configure R2 como un NTP maestro.

Configurar R2 como NTP maestro en el nivel de estrato 3

```
conf t
ntp master 3
exit
```

Tarea 6.3

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

Configure NTP de la siguiente manera:

• R1 debe sincronizar con R2.

```
conf t
ntp server 2.2.2.2
exit
```

• R3, D1 y A1 para sincronizar la hora con R1.

```
conf t
ntp server 10.0.10.1
exit
```

• D2 para sincronizar la hora con R3.

```
conf t
ntp server 10.0.11.1
exit
```

Tarea 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

```
conf t
logging trap warning
logging host 10.0.100.5
logging on
exit
```

Tarea 6.5

Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

• Unicamente 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.

```
conf t
ip access-list standard SNMP-PC1
snmp-server contact Carlos Andres Arias
snmp-server community ENCORSA ro SNMP-PC1
snmp-server host 10.0.100.5 version 2c ENCORSA
exit
```

• En R3, D1, y D2, habilite el envío de traps config y ospf.

```
conf t
snmp-server enable traps config
snmp-server enable traps ospf
exit
```

• En R1, habilite el envío de traps bgp, config, y ospf

```
conf t
snmp-server enable traps bgp
snmp-server enable traps ospf
snmp-server enable traps config
exit
```

.

• En A1, habilite el envío de traps config

```
conf t
snmp-server enable traps config
exit
```

CONCLUSIONES

Se logra la identificación de como conectar una red de un extremo a otro, de manera confiable a través del protocolo BGP, el cual es un protocolo de enrutamiento robusto que permite gran escalabilidad en la red de una compañía.

Se comprende la necesidad del uso de HSRP y de IP SLA para el monitoreo constante de los enlaces y generación de la conmutación en caso de falla, ya que es indispensable para la alta disponibilidad de red.

Se aprende el funcionamiento de un servidor radius y su importancia para asegurar un entorno de red de una manera centralizada.

Se identifica que de los simuladores existentes en el mercado el único que cumple con las características para el desarrollo de este tipo de escenarios propuestos es GNS3, sin embargo, presenta dificultades al configurarse y al tener que virtualizarse ciertos dispositivos genera un alto consumo de recursos en el equipo donde se ejecuta.

BIBLIOGRÁFIA

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Advanced Spanning Tree. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY,

David. (2020). CISCO Press (Ed). Advanced OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). OSPF v3. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). BGP. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Advanced BGP. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason y HUCABY, David. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

OSPF (Open Shortest Path First) {En línea} (2020). Recuperado de: https://www.ibm.com/docs/es/i/7.3?topic=routing-open-shortest-path-first

Protocolo de configuración dinámica de host {En línea} (2020). Recuperado de: https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

Protocolo simple de administración de red {En línea}. (2020). Recuperado de: https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host

Radius {En línea}. (2020). Recuperado de: https://es.wikipedia.org/wiki/RADIUS

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

VLAN {En línea}. (2020). Recuperado de: https://es.wikipedia.org/wiki/VLAN