DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Edwin Alejandro Penagos Aparicio

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

BOGOTA

2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Edwin Alejandro Penagos Aparicio

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*
BOGOTA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

GLOSARIO

SWITCHES: Son dispositivos que realizan interconexión en otros equipos

DHCP: es un protocolo que se encarga de asignar direcciones a los equipos

RSTP: es un protocolo que se utiliza en la capa 2

VLAN: es la forma de crear redes lógicas dentro de una red física

IEEE 802.1Q: También se conoce como dot1Q es una forma de compartir los dispositivos físicos

RESUMEN

En esta actividad de CCNP podemos ver cómo se puede configurar una red desde los conceptos básicos y configurar capa 2, esto sobre el simulador GNS3 con las ISO de CISCO C7200, configurar ENRUTAMIENTO con trocales (trunk) con su respectiva seguridad, Configuración de first hop redundancy.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento.

ABSTRACT

In this CCNP activity we can see how a network can be configured from the basic concepts and configure layer 2 this on the GNS3 simulator with the CISCO C7200 ISO, configure ROUTING with trunks (trunk) with their respective security, Configuration of first hop redundancy

Keywords: CISCO, CCNP, Routing, Swicthing.

INTRODUCCIÓN

En este diplomado de Cisco Certified Network Professional (CCNP) podemos aprender cómo realizar un examen de certificación, el cual puede ampliar su conocimiento y ayudar a su vida laboral. Podemos conocer conceptos como protocolos de enrutamiento OSPF, BGP, ISDN, la creación de troncales y Spanning Tree. Gracias a los simuladores Packet Tracer y GNS3 se puede obtener una muy buena práctica en los momentos que se desee.

En el caso de este documento podemos observar que se realizó el laboratorio de practica con la herramienta GNS3 el cual se presta para poder realizar toda la configuración indicada en la guía, como son los enrutamientos de protocolos, configuración de seguridad, First Hop Redundancy, el cual son configuraciones de alta redundancia la cual puede tener alta disponibilidad en caso de fallas en los switches.

Trabajar con la Herramienta GNS3 fue una gran experiencia personal ya que da una interfaz muy real a los dispositivos conectados, igual que la creación de máquinas virtuales para crear laboratorios reales.

DESARROLLO

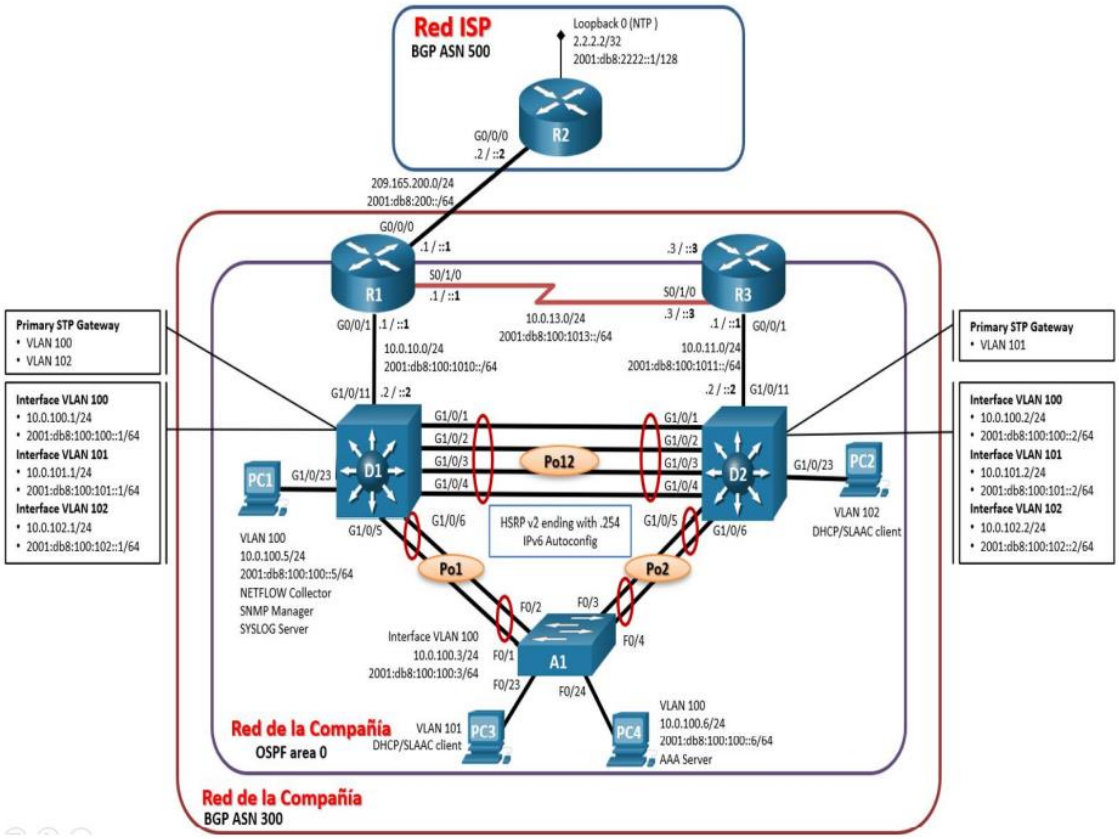

Figura 1 Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Tabla 1 Direccionamiento

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.

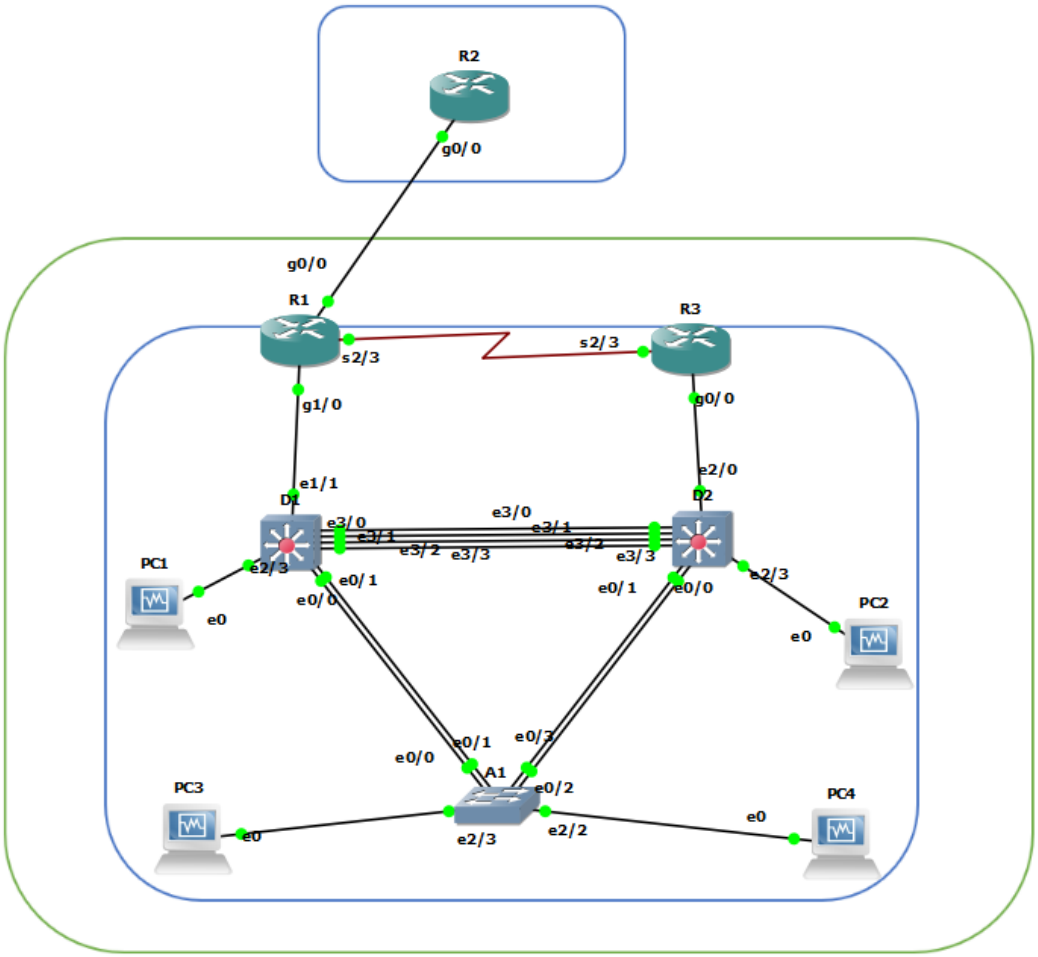

Figura 2 Implementacion

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

```
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
banner motd # R1 A R2 #
interface g0/0
ip address 209.165.200.225 255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
banner motd # R1 A D1 #
interface g1/0
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
banner motd # R1 A R3 #
interface s2/3
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
banner motd # R2 A R1 #
interface g0/0
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
banner motd # Loopback #
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
banner motd # R3 A D2 #
interface g0/0
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
banner motd # R3 A R1 #
interface s2/3
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
banner motd # D1 A R1 #
interface e1/1
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
```

```
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range e0/2-3, e1/0, e1/2-3, e2/0-2
shutdown
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
banner motd # D2 A R3 #
interface e2/0
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
interface range e0/2-3, e1/0-3, e1/1-2, e2/1-2
shutdown
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
interface range e1/0-3, e2/0-1, e3/0-3
shutdown
exit
```

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

En el anterior script podemos observar la configuración de los dispositivos conectas en la red como es R1, R2, R3, D1, D2 y A1 se activan las interfaces conectas entre si configurando las direcciones IPS versión 4 y versión 6, las Vlan 100, vlan 101, vlan 102 y vlan 999, en D1 se configura el servicio de DHCP

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

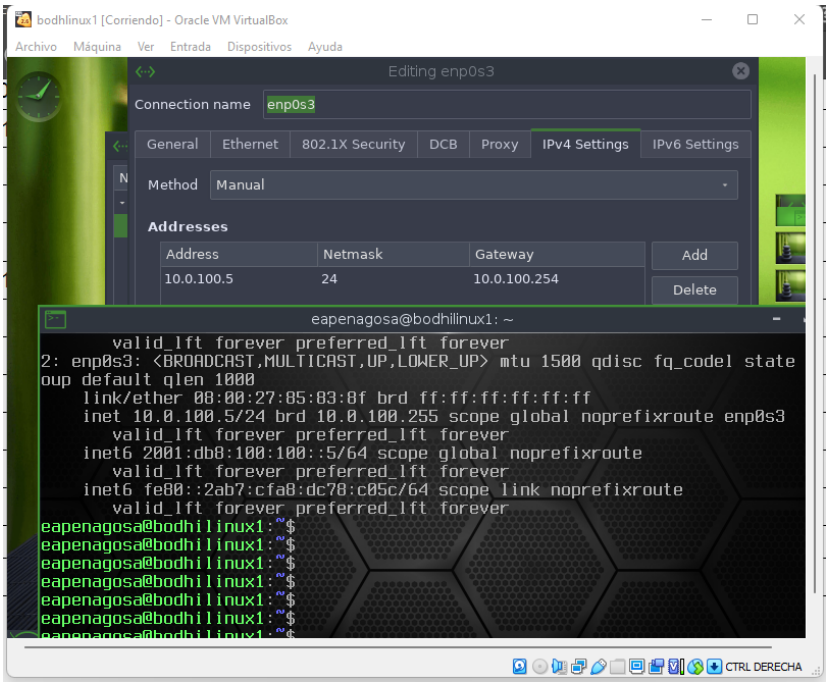

Figura 3 Configuración de IP PC 1

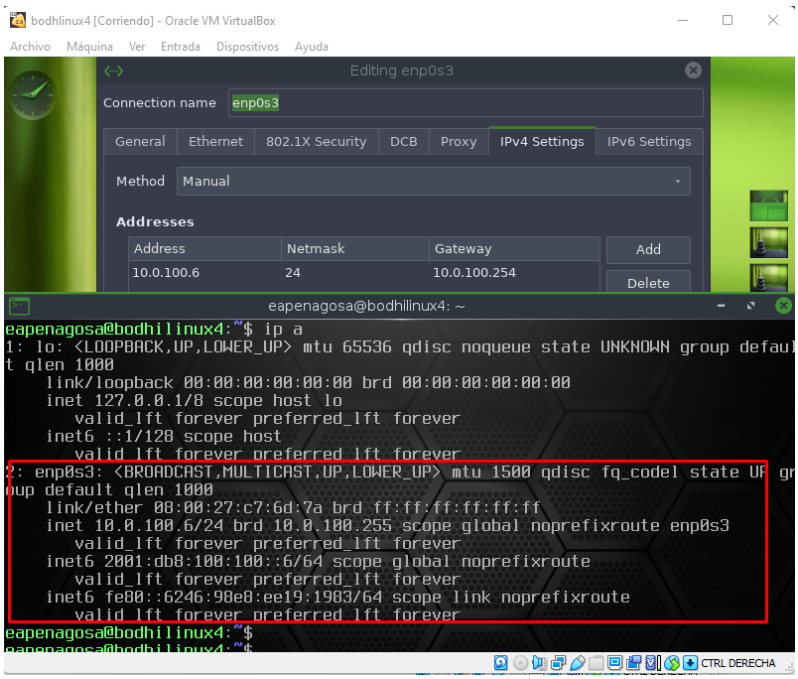

Figura 4 Configuracion de IP PC 4

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.

Habilite enlaces trunk 802.1Q entre:

D1 and D2

D1 and A1

D2 and A1

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

Use VLAN 999 como la VLAN nativa.

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

Use Rapid Spanning Tree (RSPT).

Solución

D1 a D2

interface range e3/0-3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 999

no shutdown

end

D1 a D2

interface range e3/0-3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 999

no shutdown

spanning-tree mode rapid-pvst

end

D1 a A1

interface et0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
end
interface et0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
spanning-tree mode rapid-pvst
end

A1 a D2

interface e0/2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
switchport trunk native vlan 999
end
interface e0/3
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
switchport trunk native vlan 999
spanning-tree mode rapid-pvst
end

trunk A1 a D1

interface e0/0

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

switchport trunk native vlan 999

end

interface e0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

switchport trunk native vlan 999

end

con la siguiente configuración podemos cambiar la VLAN 999 como nativa y se habilita trunk 802.1Q para D1, A1 y D2 se crea el protocolo RSPT en todos los dispositivos

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).

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

Use los siguientes números de canales:

D1 a D2 – Port channel 12

D1 a A1 – Port channel 1

D2 a A1 – Port channel 2

Solución

spanning-tree vlan 100 root primary

spanning-tree vlan 101 root secondary

spanning-tree vlan 102 root secondary

spanning-tree portfast Edge

D1 a D2

int range e3/0-3

channel-group 12 mode active

D2 a D1

int range e3/0-3

channel-group 12 mode active

D1 a A1

int range e0/0-1

channel-group 1 mode active

A1 a D1

int range e0/0-1

channel-group 1 mode active

D2 a A1

int range e0/0-1

channel-group 2 mode active

A1 a A2

int range e0/2-3

channel-group 2 mode active

En el script se termina la configuración RSTP en caso de falla, en los switches D1, D2 y A1 se crear Etherchannels

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.

Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

PC1 en D1

interface e2/3
switchport mode access
switchport access vlan 100

PC2 en D2

interface e2/3
switchport mode access
switchport access vlan 102

A1

interface e2/3
switchport mode access
switchport access vlan 101
exit
interface e2/2
switchport mode access
switchport access vlan 100
exit

2.7 Verifique los servicios DHCP IPv4.

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

Solución

PC2

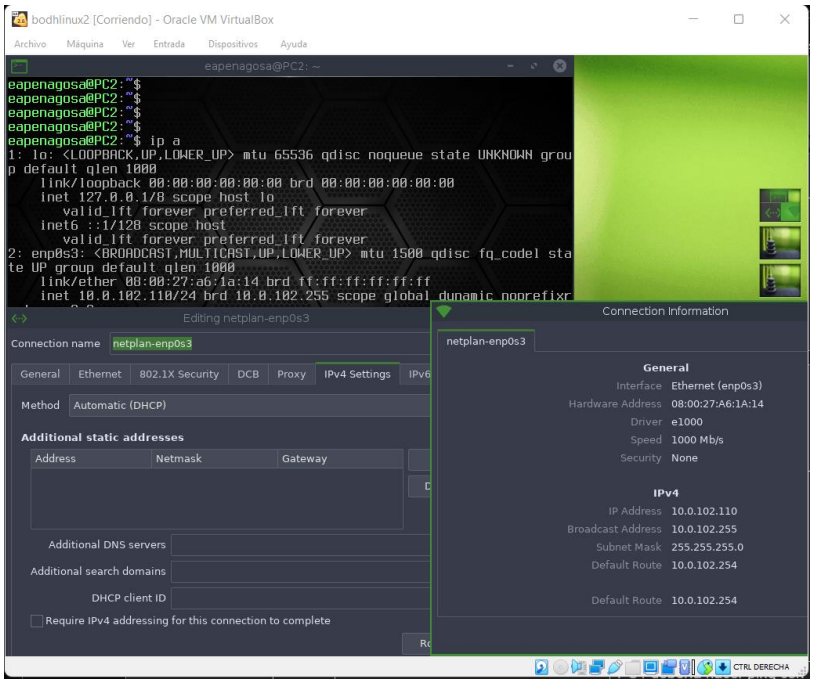

Figura 5 DHCP PC2

PC3

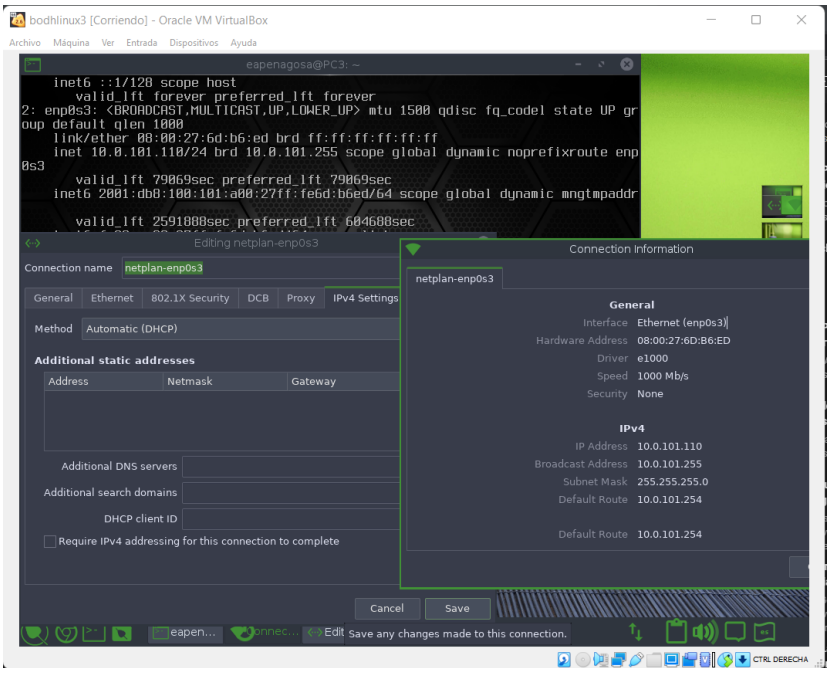

Figura 6 DHCP PC3

2.8 Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC4: 10.0.100.6

PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

D2: 10.0.102.2

PC3 debería hacer ping con éxito a:

D1: 10.0.101.1

D2: 10.0.101.2

PC4 debería hacer ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC1: 10.0.100.5

Solución

PC1

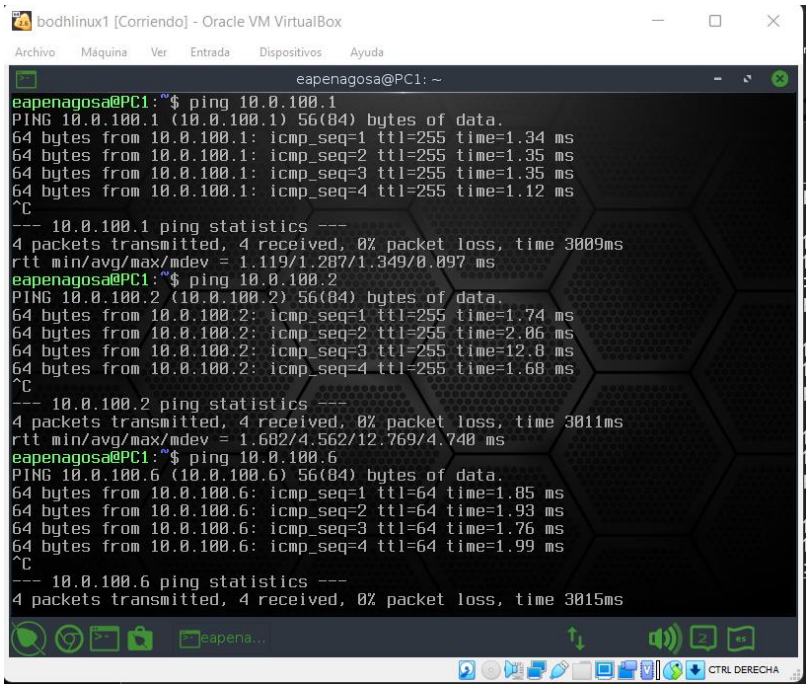

Figura 7 Ping a los dispositivos de red

PC2

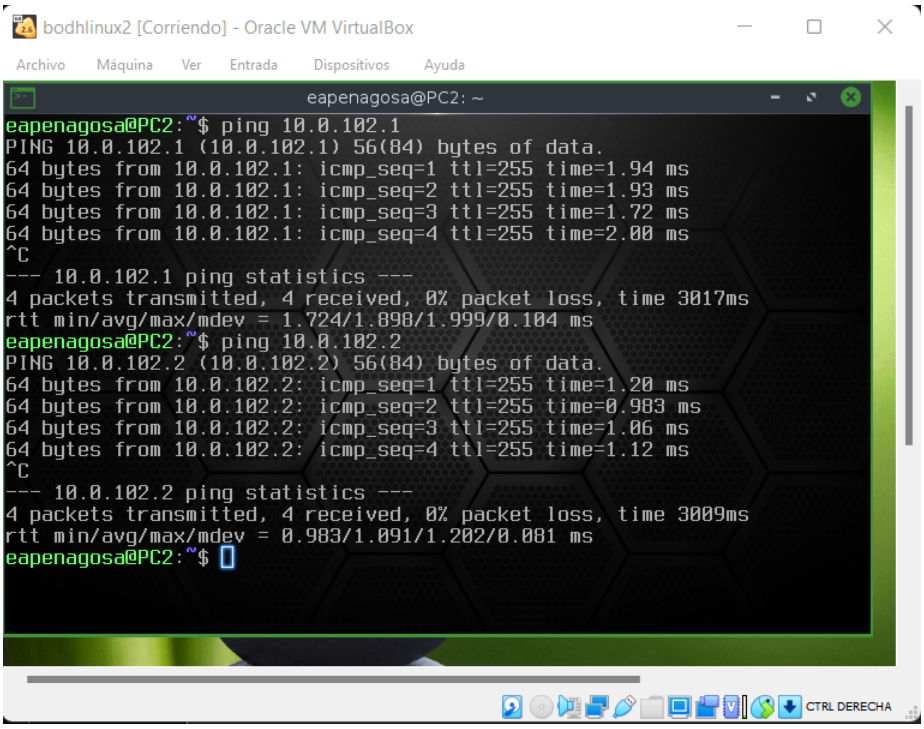

Figura 8 Ping a los dispositivos de red

PC3

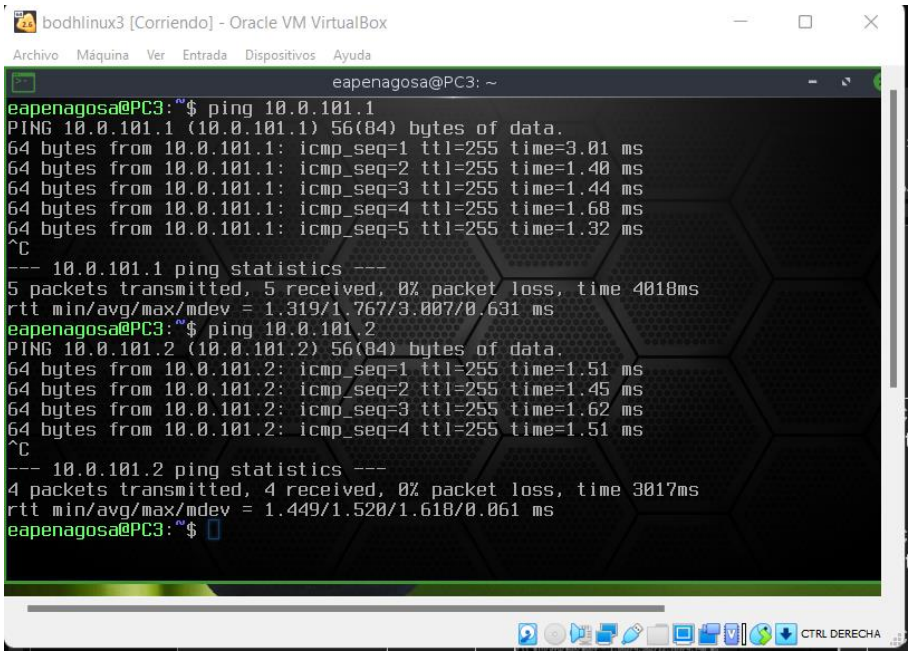

Figura 9 Ping a los dispositivos de red

PC4

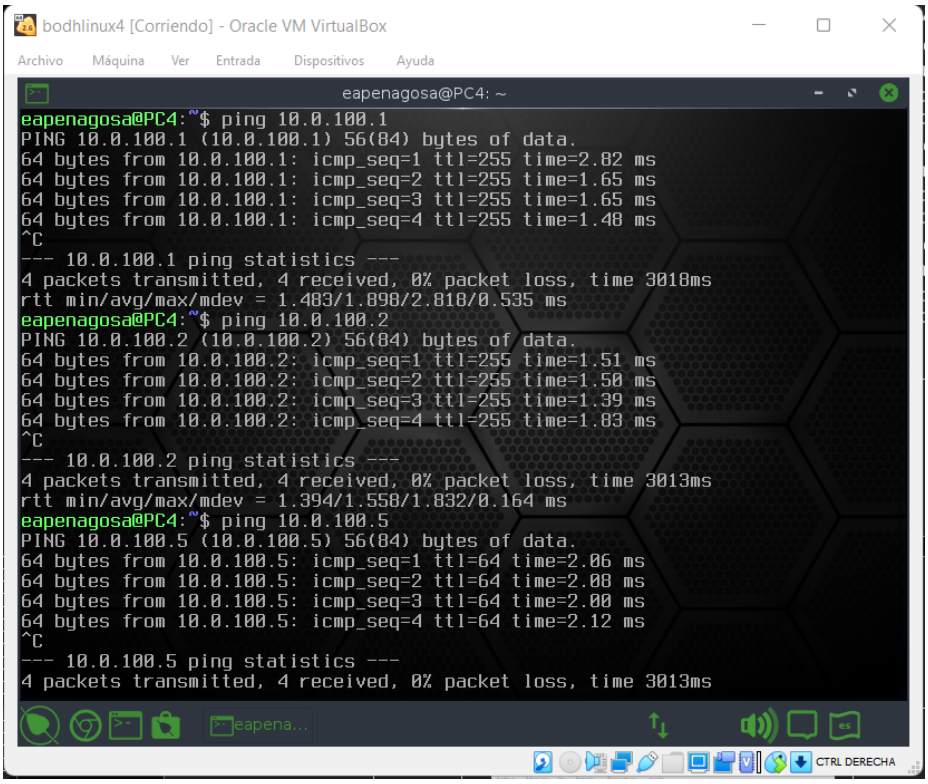

Figura 10 Ping a los dispositivos de red

Con la anterior configuración se activan los puertos para los pc dependiendo la VLAN indicada en la tabla principal

Parte 3: Configurar los protocolos de enrutamiento

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

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

Las tareas de configuración son las siguientes:

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

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

Solución

R1

router ospf 4

router-id 0.0.4.1

do show ip route connected

network 10.0.10.0 0.0.0.255 area 0

network 10.0.13.0 0.0.0.255 area 0

default-information originate

exit

R3

router ospf 4

router-id 0.0.4.3

do show ip route connected

network 10.0.11.0 0.0.0.255 area 0

network 10.0.13.0 0.0.0.255 area 0

exit

D1

router ospf 4

router-id 0.0.4.131

do show ip route connected

network 10.0.10.0 0.0.0.255 area 0

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

passive-interface default

no passive-interface e1/1

exit

D2

router ospf 4

router-id 0.0.4.132

do show ip route connected

network 10.0.11.0 0.0.0.255 area 0

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

passive-interface default

no passive-interface e2/0

exit

se configura OSPF con ID 4 en R1, R3, D1 y D2 como también se configuro los ID correspondiente a cada Router y switch según la solicitud de la Tabla

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

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

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

Solución

R1

ipv6 router ospf 6

router-id 0.0.6.1

default-information originate

interface s2/3

ipv6 ospf 6 area 0

interface g1/0

ipv6 ospf 6 area 0

R3

ipv6 router ospf 6

router-id 0.0.6.3

interface s2/3

ipv6 ospf 6 area 0

interface g0/0

ipv6 ospf 6 area 0

D1

ipv6 router ospf 6

router-id 0.0.6.131

passive-interface default

interface vlan102

ipv6 ospf 6 area 0

interface vlan101

ipv6 ospf 6 area 0

interface vlan100

ipv6 ospf 6 area 0

interface e1/1

ipv6 ospf 6 area 0

no passive-interface e1/1

end

D2

ipv6 router ospf 6

router-id 0.0.6.132

passive-interface default

interface vlan102

ipv6 ospf 6 area 0

interface vlan101

ipv6 ospf 6 area 0

interface vlan100

ipv6 ospf 6 area 0

interface e2/0

ipv6 ospf 6 area 0

no passive-interface e2/0

end

se configura OSPF con ID 6 en R1, R3, D1 y D2 como también se configuro los ID correspondiente a cada Router y switch según la solicitud de la Tabla

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.

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).

Solución

R2

```
router bgp 500
bgp router-id 2.2.2.2
neighbor 2001:DB8:200::1 remote-as 300
neighbor 209.165.200.225 remote-as 300
address-family ipv4
network 0.0.0.0
network 2.2.2.2 mask 255.255.255.255
no neighbor 2001:DB8:200::1 activate
neighbor 209.165.200.225 activate
exit-address-family
address-family ipv6
network ::/0
network 2001:DB8:2222::/128
neighbor 2001:DB8:200::1 activate
exit-address-family
address-family ipv6
network ::/0
network 2001:DB8:2222::/128
```

neighbor 2001:DB8:200::1 activate

exit-address-family

R2

router bgp 500

ip route 0.0.0.0 0.0.0.0 Loopback0

ipv6 route ::/0 Loopback0

se crean los loopback 2.2.2.2 con la configuración BGP ASN 500

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. 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.

Solución

R1

router bgp 300

bgp router-id 1.1.1.1

bgp log-neighbor-changes

neighbor 2001:DB8:200::2 remote-as 500

neighbor 209.165.200.226 remote-as 500

address-family ipv4

network 10.0.0.0

no neighbor 2001:DB8:200::2 activate

neighbor 209.165.200.226 activate

exit-address-family

address-family ipv6

network 2001:DB8:100::/48

neighbor 2001:DB8:200::2 activate

exit-address-family

se configura el MP-BGP para la red del ISP con sus respectivas rutas en IPV4 y IPV6

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

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.

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.

Solución

D1

track 4 ip sla 4

delay down 10 up 15

exit

track 6 ip sla 6

delay down 10 up 15

exit

ip sla 4

icmp-echo 10.0.10.1

frequency 5

exit

ip sla schedule 4 life forever start-time now

ip sla 6

icmp-echo 2001:DB8:100:1010::1

frequency 5

exit

ip sla schedule 6 life forever start-time now

Se crea SLAs para accesibilidad a R1 por la interface g0/0

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.

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.

Solución

D2

track 4 ip sla 4

delay down 10 up 15

exit

track 6 ip sla 6

delay down 10 up 15

exit

ip sla 4

icmp-echo 10.0.11.1

frequency 5

exit

ip sla schedule 4 life forever start-time now

ip sla 6

icmp-echo 2001:DB8:100:1011::1

frequency 5

exit

ip sla schedule 6 life forever start-time now

Se crea SLAs para accesibilidad a R3 por la interface g0/0

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.

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 decremente 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 decremente en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6

Solución

D1
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 timers 5 15
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 timers 5 15
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 timers 5 15
exit
interface vlan 100
standby version 2
standby 106 ipv6 FE80::5:73FF:FEA0:6A
standby 106 priority 150
standby 106 preempt
standby 106 timers 5 15
exit
interface vlan 101
standby version 2
standby 116 ipv6 FE80::5:73FF:FEA0:74
standby 116 preempt
standby 116 timers 5 15
exit
interface vlan 102
standby version 2
standby 126 ipv6 FE80::5:73FF:FEA0:7E
standby 126 priority 150
standby 126 preempt
standby 126 timers 5 15

se configuran HSRPv2 en D1con las VLANs 100, 101 y 102 con los standby 104,114,124,106,116 y126

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.

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

Solución

D2

interface vlan 100

standby version 2

standby 104 ip 10.0.100.254

standby 104 preempt

standby 104 timers 5 15

exit

interface vlan 101

standby version 2

standby 114 ip 10.0.101.254

standby 104 priority 150

standby 114 preempt

standby 114 timers 5 15

exit

interface vlan 102

standby version 2

standby 124 ip 10.0.102.254

standby 124 preempt

standby 124 timers 5 15

exit

interface vlan 100

standby version 2

standby 106 ipv6 FE80::5:73FF:FEA0:6A

standby 106 preempt

standby 106 timers 5 15

exit

interface vlan 101

standby version 2

standby 116 ipv6 FE80::5:73FF:FEA0:74

standby 116 priority 150

standby 116 preempt

standby 116 timers 5 15

exit

interface vlan 102

standby version 2

standby 126 ipv6 FE80::5:73FF:FEA0:7E

standby 126 preempt

standby 126 timers 5 15

se configuran HSRPv2 en D2 con las VLANs 100, 101 y 102 con los standby 104,114,124,106,116 y126

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.

Contraseña: **cisco12345cisco**

Solución

enable secret cisco12345cisco

se configura la encripcion en todos los dispositivos con la clave cisco12345cisco

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

Detalles de la cuenta encriptada SCRYPT:

Nombre de usuario Local: **sadmin**

Nivel de privilegio **15**

Contraseña: **cisco12345cisco**

Solución

username sadmin privilege 15 secret cisco12345cisco

se crea el usuario sadmin con privilegios 15 y clave cisco12345cisco

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

5.4 Habilite AAA.

Solución

aaa new-model

aaa authentication login default group radius local

se habilita el protocolo de seguridad AAA

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**

Solución

radius server RADIUS

address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

key **$trongPass**

se configura para que el equipo 4 sea el servidor RADIUS y se enruta a todos los dispositivos se loguen a este

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.

Solución

aaa session-id common

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: y la contraseña: **upass123**.

Figura 11Cierre e inicio R1

Figura 12 Cierre e inicio R3

Figura 13Cierre e inicio D1

Figura 14Cierre e inicio D2

Figura 15 Cierre e inicio A1

Parte 6: Configure las funciones de Administración de Red

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

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

Configure el reloj local a la hora UTC actual.

Solución

clock timezone utc -5

se configura el reloj utc con zona -5 que es colombia

6.2 Configure R2 como un NTP maestro.

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

Solución

ntp master 3

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

Configure NTP de la siguiente manera:

R1 debe sincronizar con R2.

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

D2 para sincronizar la hora con R3.

Solución

Clock is synchronized, stratum 4, reference is 2.2.2.2

Clock is synchronized, stratum 5, reference is 10.0.10.1

Se realiza la sincronización indicada en la guía

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.

Solución

logging trap warnings

logging host 10.0.100.5

logging synchronous

se activa el syslog para que se envían a PC1

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.

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*.

Solución

Standard IP access list SNMP-NMS
10 permit 10.0.100.5

R1
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface

snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server host 10.0.100.5 version 2c ENCORSA

R3
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

D1
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

D2

```
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
```

A1

```
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
```

se configura SNMPv2c en todos los dispositivos como lectura

CONCLUSIONES

Con el anterior trabajo puedo aprender sobre la configuración de alta disponibilidad donde se puede programar para una infraestructura empresarial la cual es muy importante para los usuarios finales y la empresa.

Sincronizar todos los dispositivos a un servidor RADIUS y un SYSLOG para que estos manejen las credenciales de los usuarios que manipulan los dispositivos de red y verificar que se realizan en cada dispositivo.

Con el simulador GNS3 puedo trabajar con toda confianza y con interfaces actualizadas, las cuales pueden ayudar una posible certificación con CISCO.

BIBLIOGRAFÍA

EDGEWORTH. (2020). Obtenido de https://1drv.ms/b/s!AAIGg5JUgUBthk8

UNAD.EDU.CO. (s.f.). Obtenido de https://estudios.unad.edu.co/diplomado-preparacion-para-la-certificacion-cisco-ccnp