

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

GUILLERMO ALFONSO LOZANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
IBAGUE
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

GUILLERMO ALFONSO LOZANO

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

DIRECTOR
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
IBAGUE
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Ibagué - Tolima, 16 de octubre de 2022

AGRADECIMIENTOS

El agradecimiento de este proyecto va dirigido primero a Dios, ya que sin su guía y bendición no alcanzaría su culminación, a mi familia por su apoyo incondicional y a las diferentes personas que a lo largo de este diplomado y demás cursos en la UNAD me brindaron su apoyo y acompañamiento para avanzar en mis conocimientos a nivel profesional y personal encaminado al objetivo principal el cual es permitir la obtención al título de ingeniero electrónico.

Deseo hacer una mención especial a mis padres y mi hijo, los cuales son un impulso primordial que me permite tener energía suficiente para cumplir con todas las metas propuestas y sueños trazados.

CONTENIDO

LISTADO DE TABLAS.....	5
LISTADO DE FIGURAS.....	6
GLOSARIO	7
RESUMEN.....	8
ABSTRACT.....	9
INTRODUCCION	10
DESARROLLO	11
Evaluación de habilidades de ENCOR	11
CONCLUSIONES	49
BIBLIOGRAFIA.....	50

LISTADO DE TABLAS

Tabla 1. Direccionamiento de la Topologia	12
---	----

LISTADO DE FIGURAS

Figura 1. Topología de la red	11
Figura 2. Escenario simulación GNS3	13
Figura 3. Configuración Router R1	14
Figura 4. Configuración Router R3	15
Figura 5. Configuración Router R3	16
Figura 6. Configuración Switch D1.....	18
Figura 7. Configuración Switch D2.....	20
Figura 8. Configuración Switch A1	21
Figura 9. Configuración Direccionamiento PC1	22
Figura 10. Configuración Direccionamiento PC4	23
Figura 11. Direccionamiento PC2	28
Figura 12. Direccionamiento PC3	28
Figura 13. Conectividad LAN PC1	29
Figura 14. Conectividad LAN PC2	29
Figura 15. Conectividad LAN PC3	30
Figura 16. Conectividad LAN PC4	30
Figura 17. Visualización protocolos de enrutamiento en R1	37
Figura 18. Visualización protocolos de enrutamiento en R1	38
Figura 19. Visualización protocolos de enrutamiento en R1	38
Figura 20. Visualización protocolos de enrutamiento en R2	39
Figura 21. Visualización protocolos de enrutamiento en R3	40
Figura 22. Visualización protocolos de enrutamiento en R3	40
Figura 23. Visualización protocolos de enrutamiento en D1	41
Figura 24. Visualización protocolos de enrutamiento en D2	41
Figura 25. Configuración HSRP versión 2 para D1.....	48
Figura 26. Configuración HSRP versión 2 para D2.....	48

GLOSARIO

ENRUTAMIENTO: Es el proceso de selección de envío de paquetes en rutas enviado por el host origen y lleguen al host destino de forma adecuada. En su viaje los han de atravesar una gran cantidad de dispositivos de red, existiendo un mecanismo capaz de direccionar la comunicación correctamente de uno a otro hasta alcanzar el destino final, este mecanismo de ruteo es responsabilidad del protocolo.

GATEWAY: Se conoce como puerta de enlace o pasarela y permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación, Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino

GNS3: (Graphic Network Simulation o Simulación Gráfica de Redes) es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Con GNS3 los usuarios tendrán la posibilidad de poder escoger cada uno de los elementos que llegarán a formar parte de una red informática, está estrechamente vinculado con el uso de IOS de equipos CISCO que simulan su funcionamiento como si se trataran de equipos reales.

HOST: Computador central o principal en un entorno de procesamiento distribuido, por lo general se refiere a un gran computador de tiempo compartido o un computador central que controla una red, se requiere de una configuración mínima de direccionamiento para permitir el intercambio de datos.

MASCARA DE RED: Combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

CONMUTACIÓN: Por medio de la conmutación se fijan los caminos físicos de un punto a otro para la comunicación de la información posicionada en redes y dominios optimizando el desempeño.

VIRTUAL MACHINE: Es un software que proporcionan la misma funcionalidad que los ordenadores físicos. Como ocurre con los ordenadores físicos, ejecutan aplicaciones y un sistema operativo. Sin embargo, son archivos informáticos que se ejecutan en un ordenador físico y se comportan como un ordenador físico. En otras palabras, se comportan como sistemas informáticos independientes.

RESUMEN

El trabajo se fundamenta principalmente en aprovechar al máximo las funciones principales de los equipos que forman la topología de la red a través de los criterios adquiridos a lo largo del curso CCNP de CISCO implementando los comandos estudiados en el desarrollo del simulador detallado.

Para la solución de las diferentes propuestas de comunicación establecidas se configuraron los dispositivos como switches, routers, ordenadores y demás equipos que se encontraban en red proporcionada, con ayuda de los parámetros de seguridad, redundancia, direccionamiento entre otros conceptos se contribuyo al aumento de la eficiencia y rendimiento de la red para cumplir con el objetivo principal, el cual tenia como meta evidenciar las habilidades adquiridas en el diplomado CCNP con el propósito de optar por el titulo ingeniero electrónico de la Universidad Nacional a Distancia (UNAD)

ABSTRACT

The work is mainly based on making the most of the main functions of the equipment that make up the topology of the network through the criteria acquired throughout the CISCO CCNP course, implementing the commands studied in the development of the detailed simulator.

For the solution of the different established communication proposals, devices such as switches, routers, computers and other equipment that were in the provided network were configured, with the help of security parameters, redundancy, addressing, among other concepts, contributing to the increase in efficiency and performance of the network to meet the main objective, which had as a goal to demonstrate the skills acquired in the CCNP diploma with the purpose of opting for the degree in electronic engineering from the National Distance University (UNAD).

INTRODUCCION

A continuación, se documenta la implementación y desarrollo de la topología de red expuesta en el escenario de prueba el cual se llevo acabo en diferentes etapas, en este trabajo se demuestra que con los comandos utilizados se solucionó la problemática paso a paso, también tiene las evidencias de su integración tomada por imágenes de los equipos intervenidos.

Se efectuó la verificación de las configuraciones implementadas y se argumentaron los conceptos obtenidos durante el transcurso del diplomado CCNP de CISCO, entro los cuales podemos encontrar habilidades de estudio como son enrutamiento en IPv4 e IPv6, segmentación de red, creación de loopback, protocolos como STP, RSTP, HSRP, HSRP V2, OSPF V2, OSPF V3, MP-BGP, seguridad de equipos y redes avanzadas para mejorar la comunicación de los dispositivos, con el propósito de evitar jaqueo de cuentas y suplantaciones, para obtener una administración de la red eficaz.

DESARROLLO

Evaluación de habilidades de ENCOR

Figura 1. Topología de la red

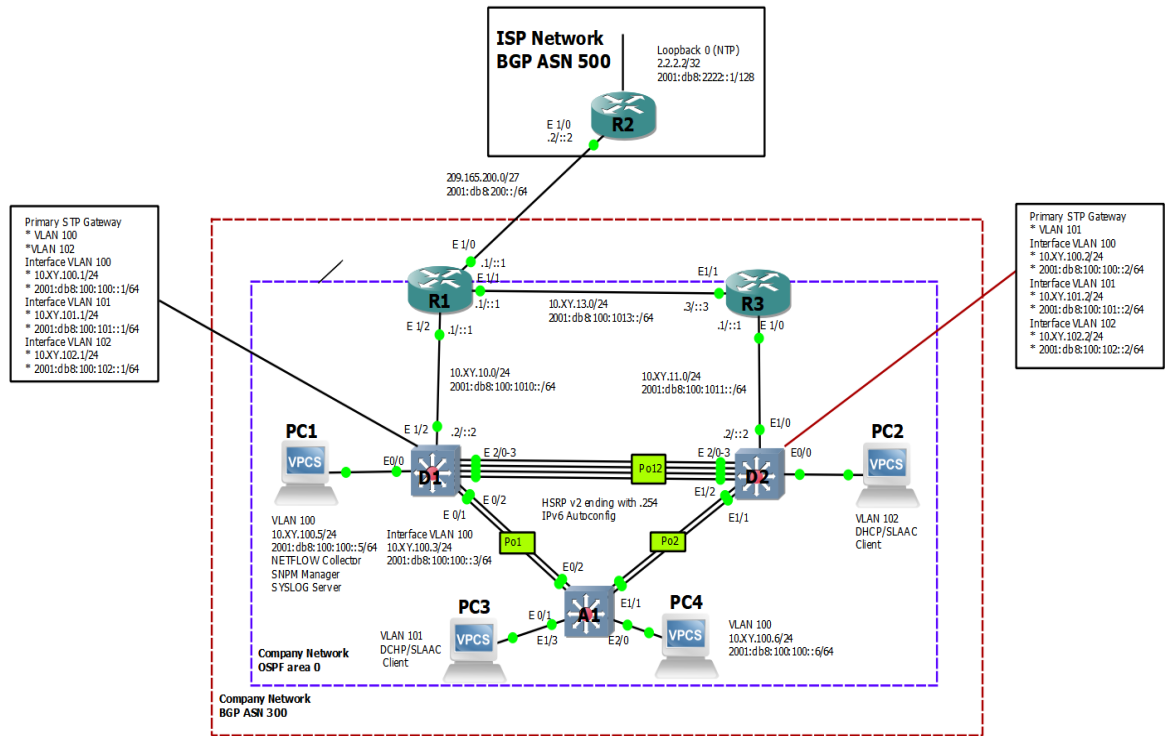
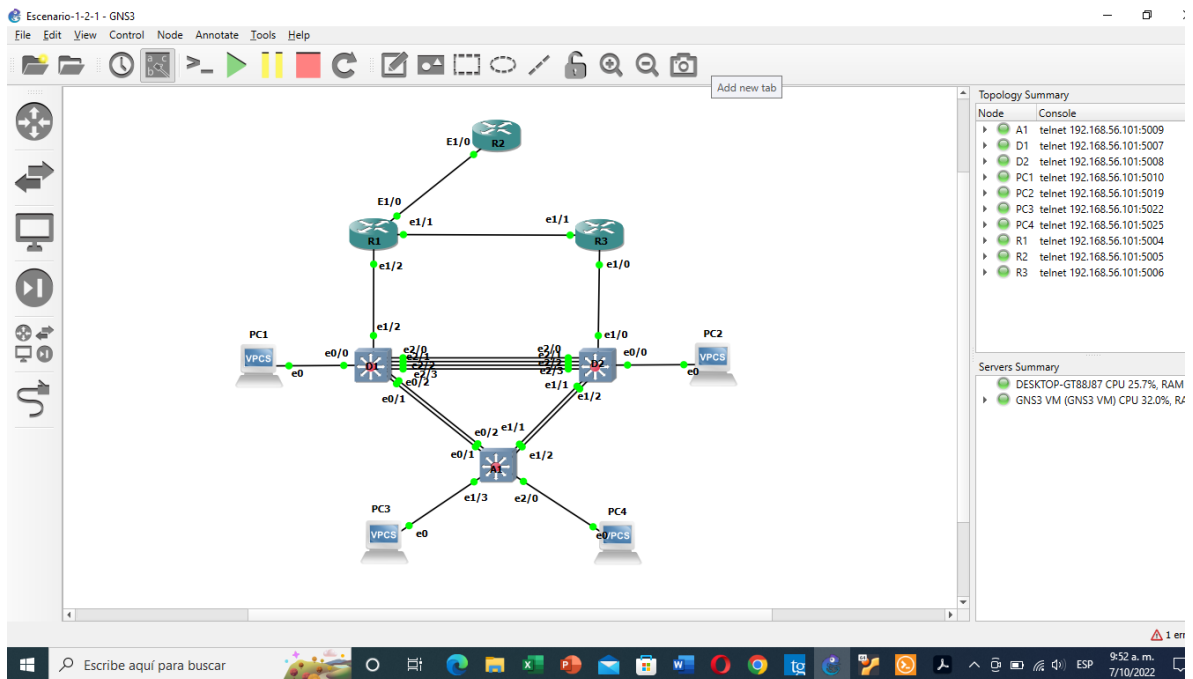


Tabla 1. Direccionamiento de la Topologia

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.61.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.61.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Bucle invertido0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.61.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.61.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.61.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	vlan 100	10.61.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	vlan 101	10.61.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	vlan 102	10.61.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.61.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	vlan 100	10.61.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	vlan 101	10.61.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	vlan 102	10.61.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	vlan 100	10.61.100.3/23	2001:db8:100:100::3/64	fe80::a1:1

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
PC1	Nada	10.61.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	Nada	DHCP	SLAAC	EUI-64
PC3	Nada	DHCP	SLAAC	EUI-64
PC4	Nada	10.61.100.6/24	2001:db8:100:100::6/64	EUI-64

Figura 2. Escenario simulación GNS3



Configuración de los ajustes básicos para cada dispositivo.

Conecte la consola a cada dispositivo, entre en el modo de configuración global y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación

Router R1

```
hostname R1
```

```
ipv6 unicast-routing
```

```

no ip domain lookup
banner motd # R1, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
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 e1/2
ip address 10.61.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface e1/1
ip address 10.61.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit

```

Figura 3. Configuración Router R1

```

R1(config-if)# exit
R1(config)#exit
R1#
*Sep 27 15:35:17.971: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#

```

Router R2

```

hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment#

```

```

line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit

```

Figura 4. Configuración Router R3

```

R2(config-if)# exit
R2(config)#exit
R2#
*Sep 27 15:47:25.643: %SYS-5-CONFIG_I: Configured from console by console
R2#
R2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#

```

Router R3

```

hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0

```

```

ip address 10.61.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface e1/1
ip address 10.61.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

```

Figura 5. Configuración Router R3

```

R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)#exit
R3#
*Sep 27 16:12:33.147: %SYS-5-CONFIG_I: Configured from console by console
R3#
R3#wr
Building configuration...
[OK]
R3#

```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Switch D1

```

hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment#
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 e1/2
no switchport
ip address 10.61.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.61.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.61.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.61.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.16.101.1 10.61.101.109
ip dhcp excluded-address 10.61.101.141 10.61.101.254
ip dhcp excluded-address 10.61.102.1 10.61.102.109
ip dhcp excluded-address 10.61.102.141 10.61.102.254
ip dhcp pool VLAN-101
network 10.61.101.0 255.255.255.0
```

```

default-router 10.61.101.254
exit
ip dhcp pool VLAN-102
network 10.61.102.0 255.255.255.0
default-router 10.61.102.254
exit
interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
shutdown
exit

```

Figura 6. Configuración Switch D1

```

D1(config-if-range)# shutdown
D1(config-if-range)# exit
D1(config)#exit
D1#
*Sep 27 16:28:07.248: %SYS-5-CONFIG_I: Configured from console by console
D1#
D1#wr
Building configuration...
Compressed configuration from 2477 bytes to 1367 bytes[OK]
D1#

```

Switch D2

```

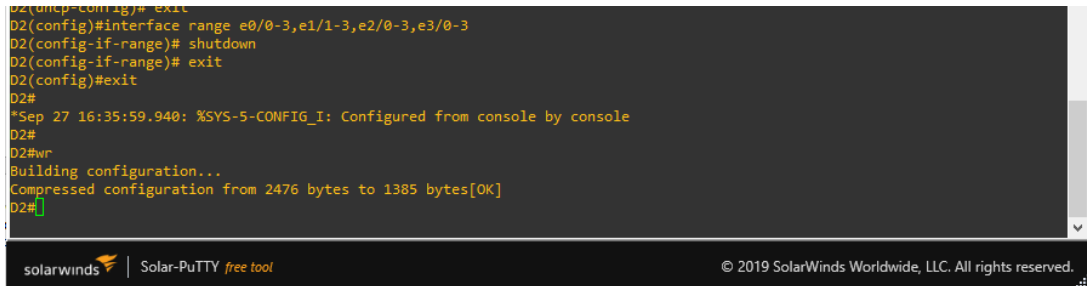
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999

```

```
name NATIVE
exit
interface e1/0
no switchport
ip address 10.61.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.61.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.61.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.61.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.61.101.1 10.61.101.209
ip dhcp excluded-address 10.61.101.241 10.61.101.254
ip dhcp excluded-address 10.61.102.1 10.61.102.209
ip dhcp excluded-address 10.61.102.241 10.61.102.254
ip dhcp pool VLAN-101
network 10.61.101.0 255.255.255.0
default-router 10.61.101.254
exit
ip dhcp pool VLAN-102
network 10.61.102.0 255.255.255.0
```

```
default-router 10.61.102.254
exit
interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
shutdown
exit
```

Figura 7. Configuración Switch D2



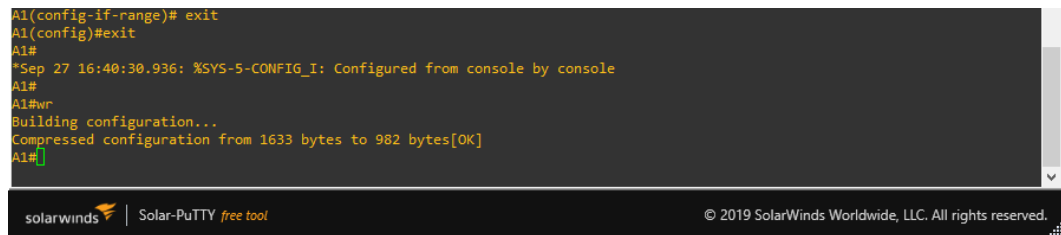
```
D2(dhcp-config)# exit
D2(config)#interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
D2(config-if-range)# shutdown
D2(config-if-range)# exit
D2(config)#exit
D2#
*Sep 27 16:35:59.940: %SYS-5-CONFIG_I: Configured from console by console
D2#
D2#wr
Building configuration...
Compressed configuration from 2476 bytes to 1385 bytes[OK]
D2#
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment#
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 10.61.100.3 255.255.255.0
```

```
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range e0/0,e0/3,e1/0,e2/1-3,e3/0-3
shutdown
exit
```

Figura 8. Configuración Switch A1



```
A1(config-if-range)# exit
A1(config)#exit
A1#
*Sep 27 16:40:30.936: %SYS-5-CONFIG_I: Configured from console by console
A1#
A1#wr
Building configuration...
Compressed configuration from 1633 bytes to 982 bytes[OK]
A1#
```

Configure el direccionamiento de host de PC 1 y PC 4 como se muestra en la tabla de direcciones. Asigne una dirección de puerta de enlace predeterminada de 10.61.100.254, que será la dirección IP virtual HSRP utilizada en la Parte 4.

Figura 9. Configuración Direccionamiento PC1



```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 10.61.100.5 255.255.255.0 gateway 10.61.100.254

PC1> ip 10.61.100.5/24 10.61.100.254
Checking for duplicate address...
PC1 : 10.61.100.5 255.255.255.0 gateway 10.61.100.254

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> sh

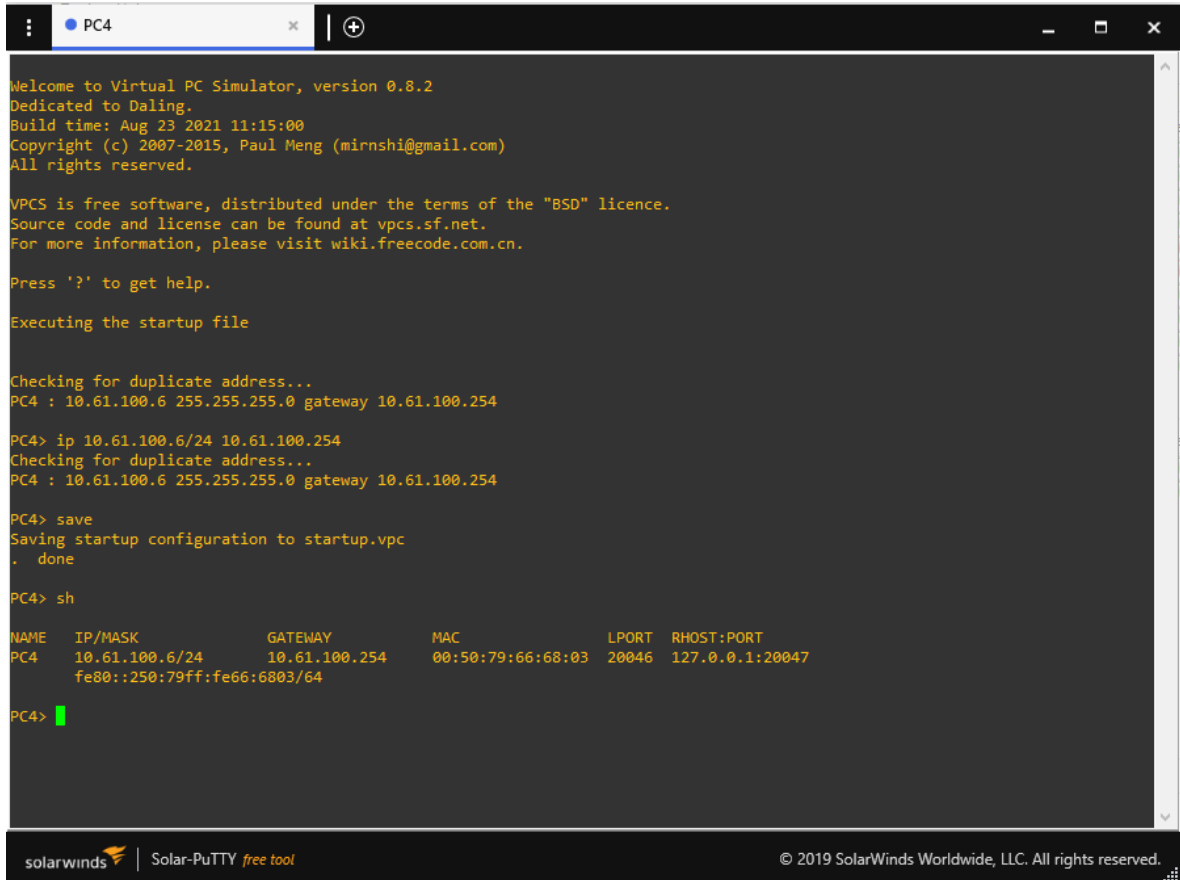
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC1      10.61.100.5/24  10.61.100.254  00:50:79:66:68:00  20044  127.0.0.1:20045
          fe80::250:79ff:fe66:6800/64

PC1> 
```

solarwinds | Solar-PuTTY free tool

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 10. Configuración Direccionamiento PC4



```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC4 : 10.61.100.6 255.255.255.0 gateway 10.61.100.254

PC4> ip 10.61.100.6/24 10.61.100.254
Checking for duplicate address...
PC4 : 10.61.100.6 255.255.255.0 gateway 10.61.100.254

PC4> save
Saving startup configuration to startup.vpc
. done

PC4> sh

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC4      10.61.100.6/24  10.61.100.254  00:50:79:66:68:03  20046  127.0.0.1:20047
         fe80::250:79ff:fe66:6803/64

PC4> █
```

2.1 En todos los conmutadores, configure las interfaces troncales IEEE 802.1Q en los enlaces de conmutación interconectados.

Habilite los enlaces troncales 802.1Q entre:

- D1 y D2
- D1 y A1
- D2 y A1

Switch D1

int range e2/0-3

switchport trunk encapsulation dot1q // comando IEEE 802.1Q

switchport mode trunk //comando modo troncal

int range e0/1-2

switchport trunk encapsulation dot1q

switchport mode trunk

Switch D2

int range e2/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
int range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk

Switch A1

int range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
int range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk

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

Utilice VLAN 999 como VLAN nativa.

Switch D1

int range e2/0-3
switchport trunk native vlan 999 // comando configuración VLAN enlace troncal
int range e0/1-2
switchport trunk native vlan 999

Switch D2

int range e2/0-3
switchport trunk native vlan 999
int range e1/1-2
switchport trunk native vlan 999

Switch A1

int range e0/1-2
switchport trunk native vlan 999
int range e1/1-2
switchport trunk native vlan 999

2.3 En todos los conmutadores, habilite el protocolo de árbol de expansión rápida. Utilice el árbol de expansión rápida.

Switch D1

spanning-tree mode rapid-pvst // comando protocolo de árbol de expansión rápida

Switch D2

spanning-tree mode rapid-pvst

Switch A1

spanning-tree mode rapid-pvst

2.4 En D1 y D2, configure los puentes raíz RSTP adecuados en función de la información del diagrama de topología. D1 y D2 deben proporcionar copia de seguridad en caso de fallo del puente raíz. Configure D1 y D2 como raíz para las VLAN adecuadas con prioridades de apoyo mutuo en caso de fallo del conmutador.

Switch D1

spanning-tree vlan 100,102 root primary // prioridad de los puentes de raíz
spanning-tree vlan 101 root secondary // puente de raíz secundario

Switch D2

spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary

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

Utilice los siguientes números de canal:

- D1 a D2 – Canal de puerto 12
- D1 a A1 – Puerto canal 1
- D2 a A1 – Puerto canal 2

Switch D1

int range e2/0-3
channel-group 12 mode active // activo modo port-chanel
no shutdown
exit
int range e0/1-2

```
channel-group 1 mode active
no shutdown
exit
```

Switch D2

```
int range e2/0-3
channel-group 12 mode active
no shutdown
exit
int range e1/1-2
channel-group 2 mode active
no shutdown
exit
```

Switch A1

```
int range e0/1-2
channel-group 1 mode active
no shutdown
exit
int range e1/1-2
channel-group 2 mode active
no shutdown
exit
```

2.6 En todos los conmutadores, configure los puertos de acceso al host que se conectan a PC1, PC2, PC3 y PC4. Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos host deben pasar inmediatamente al estado de reenvío.

Configura las interfaces como puertos de acceso y se asignan las VLAN

Switch D1

```
int e0/0
switchport mode access // configura puerto de acceso
switchport access vlan 100 // asignacion VLAN
spanning-tree portfast // habilita el modo portfast
no shutdown
exit
end
```

Switch D2

```
int e0/0
switchport mode access
switchport access vlan 102
spanning-tree portfast
```

```
no shutdown
exit
end
```

Switch A1

```
int e1/3
switchport mode access
switchpor access vlan 101
spanning-tree portfast
no shutdown
exit
int e2/0
switchport mode access
switchpor access vlan 100
spanning-tree portfast
no shutdown
exit
end
```

2.7 Compruebe los servicios DHCP IPv4. PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

Figura 11. Direccionamiento PC2

```
PC2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 0.0.0.0/0 0.0.0.0 00:50:79:66:68:01 20048 127.0.0.1:20049
fe80::250:79ff:fe66:6801/64
2001:db8:100:102:2050:79ff:fe66:6801/64 eui-64

PC2> ip dhcp
DDORA IP 10.61.102.210/24 GW 10.61.102.254

PC2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.61.102.210/24 10.61.102.254 00:50:79:66:68:01 20048 127.0.0.1:20049
fe80::250:79ff:fe66:6801/64
2001:db8:100:102:2050:79ff:fe66:6801/64 eui-64

PC2> save
Saving startup configuration to startup.vpc
. done

PC2> █
```

Figura 12. Direccionamiento PC3

```
PC3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 0.0.0.0/0 0.0.0.0 00:50:79:66:68:02 20050 127.0.0.1:20051
fe80::250:79ff:fe66:6802/64
2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64

PC3> ip dhcp
DDORA IP 10.61.101.210/24 GW 61.0.101.254

PC3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.61.101.210/24 61.0.101.254 00:50:79:66:68:02 20050 127.0.0.1:20051
fe80::250:79ff:fe66:6802/64
2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64

PC3> save
Saving startup configuration to startup.vpc
. done

PC3> █
```

2.8 Compruebe la conectividad LAN local. PC1 debería hacer ping con éxito:

- D1: 10.61.100.1
- D2: 10.61.100.2
- PC4: 10.61.100.6

Figura 13. Conectividad LAN PC1

```
PC1> ping 10.61.100.1
84 bytes from 10.61.100.1 icmp_seq=1 ttl=255 time=0.325 ms
84 bytes from 10.61.100.1 icmp_seq=2 ttl=255 time=0.329 ms
84 bytes from 10.61.100.1 icmp_seq=3 ttl=255 time=0.323 ms
84 bytes from 10.61.100.1 icmp_seq=4 ttl=255 time=0.409 ms
84 bytes from 10.61.100.1 icmp_seq=5 ttl=255 time=0.360 ms

PC1> ping 10.61.100.2
84 bytes from 10.61.100.2 icmp_seq=1 ttl=255 time=0.372 ms
84 bytes from 10.61.100.2 icmp_seq=2 ttl=255 time=0.691 ms
84 bytes from 10.61.100.2 icmp_seq=3 ttl=255 time=0.658 ms
84 bytes from 10.61.100.2 icmp_seq=4 ttl=255 time=0.593 ms
84 bytes from 10.61.100.2 icmp_seq=5 ttl=255 time=0.510 ms

PC1> ping 10.61.100.6
84 bytes from 10.61.100.6 icmp_seq=1 ttl=64 time=0.563 ms
84 bytes from 10.61.100.6 icmp_seq=2 ttl=64 time=0.588 ms
84 bytes from 10.61.100.6 icmp_seq=3 ttl=64 time=0.611 ms
84 bytes from 10.61.100.6 icmp_seq=4 ttl=64 time=0.705 ms
84 bytes from 10.61.100.6 icmp_seq=5 ttl=64 time=0.579 ms

PC1> █
```

PC2 debería hacer ping correctamente:

- D1: 10.61.102.1
- D2: 10.61.102.2

Figura 14. Conectividad LAN PC2

```
PC2> ping 10.61.102.1
84 bytes from 10.61.102.1 icmp_seq=1 ttl=255 time=0.653 ms
84 bytes from 10.61.102.1 icmp_seq=2 ttl=255 time=1.090 ms
84 bytes from 10.61.102.1 icmp_seq=3 ttl=255 time=0.960 ms
84 bytes from 10.61.102.1 icmp_seq=4 ttl=255 time=0.697 ms
84 bytes from 10.61.102.1 icmp_seq=5 ttl=255 time=0.667 ms

PC2> ping 10.61.102.2
84 bytes from 10.61.102.2 icmp_seq=1 ttl=255 time=0.202 ms
84 bytes from 10.61.102.2 icmp_seq=2 ttl=255 time=0.365 ms
84 bytes from 10.61.102.2 icmp_seq=3 ttl=255 time=0.363 ms
84 bytes from 10.61.102.2 icmp_seq=4 ttl=255 time=0.354 ms
84 bytes from 10.61.102.2 icmp_seq=5 ttl=255 time=0.363 ms

PC2> █
```

PC3 debería hacer ping correctamente:

- D1: 10.61.101.1
- D2: 10.61.101.2

Figura 15. Conectividad LAN PC3

```
PC3> ping 10.61.101.1
84 bytes from 10.61.101.1 icmp_seq=1 ttl=255 time=0.795 ms
84 bytes from 10.61.101.1 icmp_seq=2 ttl=255 time=1.100 ms
84 bytes from 10.61.101.1 icmp_seq=3 ttl=255 time=1.095 ms
84 bytes from 10.61.101.1 icmp_seq=4 ttl=255 time=0.807 ms
84 bytes from 10.61.101.1 icmp_seq=5 ttl=255 time=0.878 ms

PC3> ping 10.61.101.2
84 bytes from 10.61.101.2 icmp_seq=1 ttl=255 time=0.581 ms
84 bytes from 10.61.101.2 icmp_seq=2 ttl=255 time=0.657 ms
84 bytes from 10.61.101.2 icmp_seq=3 ttl=255 time=0.567 ms
84 bytes from 10.61.101.2 icmp_seq=4 ttl=255 time=1.213 ms
84 bytes from 10.61.101.2 icmp_seq=5 ttl=255 time=0.868 ms

PC3> █
```

PC4 debería hacer ping correctamente:

- D1: 10.61.100.1
- D2: 10.61.100.2
- PC1: 10.61.100.5

Figura 16. Conectividad LAN PC4

```
PC4> ping 10.61.100.1
84 bytes from 10.61.100.1 icmp_seq=1 ttl=255 time=0.361 ms
84 bytes from 10.61.100.1 icmp_seq=2 ttl=255 time=0.707 ms
84 bytes from 10.61.100.1 icmp_seq=3 ttl=255 time=0.619 ms
84 bytes from 10.61.100.1 icmp_seq=4 ttl=255 time=0.596 ms
84 bytes from 10.61.100.1 icmp_seq=5 ttl=255 time=0.826 ms

PC4> ping 10.61.100.2
84 bytes from 10.61.100.2 icmp_seq=1 ttl=255 time=0.614 ms
84 bytes from 10.61.100.2 icmp_seq=2 ttl=255 time=0.813 ms
84 bytes from 10.61.100.2 icmp_seq=3 ttl=255 time=0.774 ms
84 bytes from 10.61.100.2 icmp_seq=4 ttl=255 time=0.934 ms
84 bytes from 10.61.100.2 icmp_seq=5 ttl=255 time=16.189 ms

PC4> ping 10.61.100.5
84 bytes from 10.61.100.5 icmp_seq=1 ttl=64 time=0.372 ms
84 bytes from 10.61.100.5 icmp_seq=2 ttl=64 time=1.048 ms
84 bytes from 10.61.100.5 icmp_seq=3 ttl=64 time=0.914 ms
84 bytes from 10.61.100.5 icmp_seq=4 ttl=64 time=0.733 ms
84 bytes from 10.61.100.5 icmp_seq=5 ttl=64 time=0.710 ms

PC4> █
```

3.1 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv2 de área única en el área 0.

Utilice OSPF Process ID 4 y asigne los siguientes ID de router:

- 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 / VLAN conectadas directamente en el Área 0.

- En R1, no anuncie la red R1 – R2.
- En R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada.

Desactívelos anuncios de OSPF v2 en:

- D1: Todas las interfaces excepto E1/2
- D2: Todas las interfaces excepto E1/0

Se habilita el comando OSPF en el modo de configuración global

Router R1

```
router ospf 4 // habilita comando OSPFv2
router-id 0.0.4.1 // asignación de ID
network 10.61.10.0 0.0.0.255 area 0 // asignación de redes
network 10.61.13.0 0.0.0.255 area 0 // asignación de redes
default-information originate // no anuncio de red
exit
```

Router R3

```
router ospf 4
router-id 0.0.4.3
network 10.61.11.0 0.0.0.255 area 0
network 10.61.13.0 0.0.0.255 area 0
exit
```

Switch D1

```
router ospf 4
router-id 0.0.4.131
network 10.61.100.0 0.0.0.255 area 0
network 10.61.101.0 0.0.0.255 area 0
network 10.61.102.0 0.0.0.255 area 0
network 10.61.10.0 0.0.0.255 area 0
passive-interface default // no recibe actualización de enrutamiento
no passive-interface e1/2 // exceptuando esta interfaz
exit
```

Switch D2

```
router ospf 4
router-id 0.0.4.132
network 10.61.100.0 0.0.0.255 area 0
network 10.61.101.0 0.0.0.255 area 0
network 10.61.102.0 0.0.0.255 area 0
network 10.61.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/0
exit
```

3.2 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv3 clásico de área única en el área 0.

Utilice OSPF Process ID 6 y asigne los siguientes ID de router:

- 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 / VLAN conectadas directamente en el Área 0.

- En R1, no anuncie la red R1 – R2.
- En R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada.

Desactive los anuncios de OSPFv3 en:

- D1: Todas las interfaces excepto E1/2
- D2: Todas las interfaces excepto E1/0

Se configura OSPFv3 en cada interface

Router R1

```
ipv6 router ospf 6 // habilita comando OSPFv3
router-id 0.0.6.1 // asignación de ID
default-information originate
exit
interface e1/2
ipv6 ospf 6 area 0 // asignación de redes
exit
interface e1/1
```

```
ipv6 ospf 6 area 0  
exit
```

Router R3

```
ipv6 router ospf 6  
router-id 0.0.6.3  
exit  
interface e1/0  
ipv6 ospf 6 area 0  
exit  
interface e1/1  
ipv6 ospf 6 area 0  
exit  
end
```

Switch D1

```
ipv6 router ospf 6  
router-id 0.0.6.131  
passive-interface default // no recibe actualización de enrutamiento  
no passive-interface e1/2 // exceptuando esta interfaz  
exit  
interface e1/2  
ipv6 ospf 6 area 0  
exit  
interface vlan 100 // asignación de VLAN  
ipv6 ospf 6 area 0  
exit  
interface vlan 101  
ipv6 ospf 6 area 0  
exit  
interface vlan 102  
ipv6 ospf 6 area 0  
exit  
end
```

Switch D2

```
ipv6 router ospf 6  
router-id 0.0.6.132  
passive-interface default  
no passive-interface e1/0
```

```
exit
interface e1/0
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
end
```

3.3 On R2 in the “ISP Network”, configure MP-BGP.

Configure two default static routes via interface Loopback 0:

- An IPv4 default static route.
- An IPv6 default static route.

Configure R2 in BGP ASN 500 and use the router-id 2.2.2.2.

Configure and enable an IPv4 and IPv6 neighbor relationship with R1 in ASN 300.

In IPv4 address family, advertise:

- The Loopback 0 IPv4 network (/32).
- The default route (0.0.0.0/0).

In IPv6 address family, advertise:

- The Loopback 0 IPv4 network (/128).
- The default route (::/0).

Configuración de rutas estáticas predeterminada en IPv4 e IPv6, MP-BGP

Router R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0 // asignación rutas estáticas IPv4
```

```

ipv6 route ::/0 loopback 0 // asignación rutas estáticas IPv6
router bgp 500 // configuración BGP
bgp router-id 2.2.2.2 // asignación id
neighbor 209.165.200.225 remote-as 300 // asignación id vecino IPv4
neighbor 2001:db8:200::1 remote-as 300 // asignación id vecino IPv4
address-family ipv4 // asignación dirección familia IPv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6 // asignación dirección familia IPv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family
end

```

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

Configure dos rutas de resumen estáticas para la interfaz Null 0:

- Un resumen de la ruta IPv4 para 10.XY.0.0/8.
- Un resumen de la ruta IPv6 para 2001:db8:100::/48.

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

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

En la familia de direcciones IPv4:

- Deshabilite la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.
- Anuncie la red 10.XY0.0/8.

En la familia de direcciones IPv6:

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

Configuración de rutas estáticas predeterminada en IPv4 e IPv6, MP-BGP en R1

Router R1

```
ip route 10.0.0.0 255.0.0.0 null0 // configuración ruta estática IPv4
ipv6 route 2001:db8:100::/48 null0 // configuración ruta estática IPv6
router bgp 300 // configuracion BGP
bgp router-id 1.1.1.1 //asignación id
neighbor 209.165.200.226 remote-as 500 // configuración relación vecino IPv4
neighbor 2001:db8:200::2 remote-as 500 // configuración relación vecino IPv6
address-family ipv4 unicast // asignacino direccion familia IPv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast // asignacino direccion familia IPv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
end
```

A continuación, se muestran las siguientes figuras con los comandos de visualización de los protocolos de enrutamiento de los dispositivos.

Figura 17. Visualización protocolos de enrutamiento en R1

```
R1#
R1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.1
  network 10.61.10.0 0.0.0.255 area 0
  network 10.61.13.0 0.0.0.255 area 0
  default-information originate
R1#
R1#show run | section ^ipv6 route
ipv6 route 2001:DB8:100::/48 Null0
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#
R1#show ipv6 ospf interface brief
Interface    PID    Area          Intf ID    Cost    State  Nbrs  F/C
Et1/1        6      0              4           10     DR     1/1
Et1/2        6      0              5           10     DR     1/1
R1#
R1#show run | section bgp
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
R1#
```

Figura 18. Visualización protocolos de enrutamiento en R1

```
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
B*    0.0.0.0/0 [20/0] via 209.165.200.226, 00:22:37
B     2.2.2.2 [20/0] via 209.165.200.226, 00:22:37
O     10.61.11.0/24 [110/20] via 10.61.13.3, 00:21:46, Ethernet1/1
O     10.61.100.0/24 [110/21] via 10.61.13.3, 00:18:24, Ethernet1/1
O     10.61.101.0/24 [110/21] via 10.61.13.3, 00:18:24, Ethernet1/1
O     10.61.102.0/24 [110/21] via 10.61.13.3, 00:18:24, Ethernet1/1
```

Figura 19. Visualización protocolos de enrutamiento en R1

```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
B    ::/0 [20/0]
     via FE80::2:1, Ethernet1/0
S    2001:DB8:100::/48 [1/0]
     via Null0, directly connected
O    2001:DB8:100:100::/64 [110/21]
     via FE80::3:3, Ethernet1/1
O    2001:DB8:100:101::/64 [110/21]
     via FE80::3:3, Ethernet1/1
O    2001:DB8:100:102::/64 [110/21]
     via FE80::3:3, Ethernet1/1
C    2001:DB8:100:1010::/64 [0/0]
     via Ethernet1/2, directly connected
L    2001:DB8:100:1010::1/128 [0/0]
     via Ethernet1/2, receive
O    2001:DB8:100:1011::/64 [110/20]
     via FE80::3:3, Ethernet1/1
C    2001:DB8:100:1013::/64 [0/0]
     via Ethernet1/1, directly connected
L    2001:DB8:100:1013::1/128 [0/0]
     via Ethernet1/1, receive
C    2001:DB8:200::/64 [0/0]
     via Ethernet1/0, directly connected
L    2001:DB8:200::1/128 [0/0]
     via Ethernet1/0, receive
L    FF00::/8 [0/0]
     via Null0, receive
```

Figura 20. Visualización protocolos de enrutamiento en R2

```
R2#show run | section bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  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
R2#
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
```

Figura 21. Visualización protocolos de enrutamiento en R3

```

R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.61.11.0 0.0.0.255 area 0
  network 10.61.13.0 0.0.0.255 area 0
R3#
R3#show run | section ^ipv6 route
ipv6 router ospf 6
  router-id 0.0.6.3
R3#
R3#show ipv6 ospf interface brief
Interface    PID    Area          Intf ID    Cost    State  Nbrs F/C
Et1/1        6      0              4          10     BDR    1/1
Et1/0        6      0              3          10     DR     1/1
R3#
R3#show ip route ospf | begin Gateway
Gateway of last resort is 10.61.13.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.61.13.1, 00:36:08, Ethernet1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O      10.61.10.0/24 [110/20] via 10.61.13.1, 00:36:08, Ethernet1/1
O      10.61.100.0/24 [110/11] via 10.61.11.2, 00:33:01, Ethernet1/0
O      10.61.101.0/24 [110/11] via 10.61.11.2, 00:33:01, Ethernet1/0
O      10.61.102.0/24 [110/11] via 10.61.11.2, 00:33:01, Ethernet1/0

```

Figura 22. Visualización protocolos de enrutamiento en R3

```

R3#show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
OE2 ::/0 [110/1], tag 6
    via FE80::1:3, Ethernet1/1
O  2001:DB8:100:100::/64 [110/11]
    via FE80::D1:1, Ethernet1/0
O  2001:DB8:100:101::/64 [110/11]
    via FE80::D1:1, Ethernet1/0
O  2001:DB8:100:102::/64 [110/11]
    via FE80::D1:1, Ethernet1/0
O  2001:DB8:100:1013::/64 [110/10]
    via Ethernet1/1, directly connected

```

Figura 23. Visualización protocolos de enrutamiento en D1

```
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  passive-interface default
  no passive-interface Ethernet1/2
  network 10.61.10.0 0.0.0.255 area 0
  network 10.61.100.0 0.0.0.255 area 0
  network 10.61.101.0 0.0.0.255 area 0
  network 10.61.102.0 0.0.0.255 area 0
D1#
D1#show run | section ^ipv6 route
ipv6 router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/2
D1#
D1#show ipv6 ospf interface brief
Interface    PID    Area          Intf ID    Cost    State Nbrs F/C
Vl102       6      0              23         1      DOWN  0/0
Vl101       6      0              22         1      DOWN  0/0
Vl100       6      0              21         1      DOWN  0/0
Et1/2       6      0              19         10     BDR   1/1
```

Figura 24. Visualización protocolos de enrutamiento en D2

```
D2#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface Ethernet1/0
  network 10.61.11.0 0.0.0.255 area 0
  network 10.61.100.0 0.0.0.255 area 0
  network 10.61.101.0 0.0.0.255 area 0
  network 10.61.102.0 0.0.0.255 area 0
D2#
D2#show run | section ^ipv6 route
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet1/0
D2#
D2#show ipv6 ospf interface brief
Interface    PID    Area          Intf ID    Cost    State Nbrs F/C
Vl102       6      0              25         1      DR    0/0
Vl101       6      0              24         1      DR    0/0
Vl100       6      0              23         1      DR    0/0
Et1/0       6      0              21         10     BDR   1/1
```

4.1 En D1, cree SLA IP que prueben la accesibilidad de la interfaz R1 E1/2.

Cree dos SLA IP.

- Utilice el SLA número 4 para IPv4.
- Utilice el SLA número 6 para IPv6.

Los SLA IP probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.

Programa el SLA para su implementación inmediata sin hora de finalización.

Cree un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.

- Utilice el número de pista 4 para IP SLA 4.
- Utilice el número de pista 6 para IP SLA 6.

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

Se crean las IP SLAs con tiempos de implementación inmediata y sin tiempo de finalización, también se crean las IP SLAs objeto con tiempos de activación y desactivación realizando reportes aun dispositivos específico.

Switch D1

```
ip sla 4 // creación IP SLA 4
icmp-echo 10.61.10.1 // asignación dirección
frequency 5 // frecuencia cada 5 segundos
exit
ip sla 6 // creación IP SLA 6
icmp-echo 2001:db8:100:1010::1 // asignación dirección
frequency 5
exit
ip sla schedule 4 life forever start-time now // notificación IP SLA 4
ip sla schedule 6 life forever start-time now // notificación IP SLA 6
track 4 ip sla 4
delay down 10 up 15 // retraso bajo 10, alto 15
exit
track 6 ip sla 6
delay down 10 up 15 // retraso bajo 10, alto 15
exit
```

4.2 En D2, cree SLA IP que prueben la accesibilidad de la interfaz R3 E1/0.

Cree dos SLA IP.

- Utilice el SLA número 4 para IPv4.
- Utilice el SLA número 6 para IPv6.

Los SLA IP probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.

Programa el SLA para su implementación inmediata sin hora de finalización.

Cree un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.

- Utilice el número de pista 4 para IP SLA 4.
- Utilice el número de pista 6 para IP SLA 6.

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

Se crean las IP SLAs con tiempos de implementación inmediata y sin tiempo de finalización, también se crean las IP SLAs objeto con tiempos de activación y desactivación realizando reportes aun dispositivos específico.

Switch D2

```
ip sla 4
icmp-echo 10.61.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
```

4.3 En D1, configure HSRPv2.

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

Configure HSRP versión 2.

Configure el grupo 104 de HSRP IPv4 para VLAN 100:

- Asigne la dirección IP virtual 10.XY.100.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 y disminuya en 60.

Configure el grupo 114 de HSRP IPv4 para VLAN 101:

- Asigne la dirección IP virtual 10.XY.10 1.254.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 hasta disminuir en 60.

Configure el grupo HSRP IPv4 124 para VLAN 102:

- Asigne la dirección IP virtual 10.XY.10 2.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 hasta disminuir en 60.

Configure IPv6 HSRP grupo 10 6 para VLAN 100:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

Configure el grupo HSRP IPv6 11 6 para VLAN 101:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

Configure IPv6 HSRP grupo 126 para VLAN 102:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

En D2, configure HSRPv2.

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

Configure HSRP versión 2.

Configure el grupo 104 de HSRP IPv4 para VLAN 100:

- Asigne la dirección IP virtual 10.XY.100.254.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 y disminuya en 60.

Configure el grupo 114 de HSRP IPv4 para VLAN 101:

- Asigne la dirección IP virtual 10. XY.10 1,254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 hasta disminuir en 60.

Configure el grupo HSRP IPv4 124 para VLAN 102:

- Asigne la dirección IP virtual 10. XY.10 2.254.
- Habilite la preferencia.
- Realice un seguimiento del objeto 4 hasta disminuir en 60.

Configure IPv6 HSRP grupo 10 6 para VLAN 100:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

Configure el grupo HSRP IPv6 11 6 para VLAN 101:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

Configure IPv6 HSRP grupo 126 para VLAN 102:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilite la preferencia.
- Realice un seguimiento del objeto 6 y disminuya en 60.

Configuración HSRP versión 2 para la creación de grupos de enrutamiento de tráfico mediante la figura de principal y respaldo, confirmando periódicamente las interfaces programadas.

Switch D1

```
interface vlan 100
standby version 2 // configuración HSRPv2
standby 104 ip 10.61.100.254 // asignación dirección
standby 104 priority 150 // habitación prioridad
standby 104 preempt
standby 104 track 4 decrement 60 // seguimiento objeto 4 y decremento
standby 106 ipv6 autoconfig // configuración HSRPv2 IPv6
standby 106 priority 150 // habitación prioridad
standby 106 preempt
standby 106 track 6 decrement 60 // seguimiento objeto 6 y decremento
exit
interface vlan 101
standby version 2
standby 114 ip 10.61.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.61.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

Switch D2

```
interface vlan 100
standby version 2
standby 104 ip 10.61.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
```

```
exit
interface vlan 101
standby version 2
standby 114 ip 10.61.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.61.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

A continuación, se muestran las siguientes figuras con la implementación de la configuración HSRP versión 2 para D1 y D2

Figura 25. Configuración HSRP versión 2 para D1

```
D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.61.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
D1#show standby brief
          P indicates configured to preempt.
          |
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Vl100        104 150 P Init    unknown      unknown       10.61.100.254
Vl100        106 150 P Init    unknown      unknown       FE80::5:73FF:FEA0:6A
Vl101        114 100 P Init    unknown      unknown       10.61.101.254
Vl101        116 100 P Init    unknown      unknown       FE80::5:73FF:FEA0:74
Vl102        124 150 P Init    unknown      unknown       10.61.102.254
Vl102        126 150 P Init    unknown      unknown       FE80::5:73FF:FEA0:7E
```

Figura 26. Configuración HSRP versión 2 para D2

```
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.61.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
```

CONCLUSIONES

Con la estructura de las herramientas como las VLAN, la implementación de las interfaces troncales y protocolos de enrutamiento, se puede configurar adecuadamente una red local teniendo interacción con otras redes, facilitando la administración de la red LAN y su configuración. se solucionó el inconveniente de la comunicación entre los dispositivos de la red como lo son los Routers y Switches con la implementación de la configuración (duplex-half) para corregir el error de transmisión de datos.

Las diferentes compañías que trabajan en la seguridad de las redes hoy en día, tienen un gran desafío puesto que hay personas o grupos anónimos los cuales buscan violar la red y obtener información precisa e importante para los administradores de estas, por esta razón la empresa CISCO está a la vanguardia de ofrecer soluciones de ultima generación para la seguridad de los equipos, con dispositivos los cuales ayudan a restringir vulneraciones.

Los administradores y usuarios de las redes tienen un tema fundamental de alto impacto que es la falta o fallos de conectividad, configuraciones como HSRP han ayudado a manejar automatizaciones de redundancia mediante la verificación de interfaces periódicamente, esto conlleva a que si hay un fallo en la comunicación de la red inmediatamente busca una vía que este en standby para garantizar la conexión al usuario final.

BIBLIOGRAFIA

NOBOA MIRANDA, Diego. Manual de CISCO cuarta edición, McGraw Hill Interamericana. 2007. 698p.

ARIGANELLO, Ernesto. BARRIENTOS SEVILLA, Enrique. Redes CISCO CCNP a Fondo. Primera edición. RA-MA. 2015. 915p.