

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

ALEJANDRO BERNAL SALAMANCA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP  
BOGOTÁ  
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

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

DIRECTOR:

Mag. JOHN HAROLD PEREZ CALDERON

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

2022

Nota de Aceptación

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Bogotá D.C., 17 de noviembre de 2022

## **AGRADECIMIENTOS**

A mi familia especialmente a mis dos hijos, que son un baluarte y apoyo incondicional que durante todo el proceso de aprendizaje han acompañado este camino y a los profesores y/o tutores, quienes estuvieron presentes para brindar su conocimiento apoyo y colaboración durante toda la carrera.

## CONTENIDO

	Pág.
AGRADECIMIENTOS.....	4
LISTA DE FIGURAS.....	6
LISTA DE TABLAS.....	8
GLOSARIO.....	9
RESUMEN Y ABSTRAC.....	10
INTRODUCCIÓN.....	11
DESARROLLO DEL ESCENARIO PROPUESTO .....	12
<b>a.</b> PARTE 1: Construcción de la red y configuración de ajustes básicos .....	12
<b>b.</b> PARTE 2: Configuraciones de capa 2 de la red y soporte de host .....	23
<b>c.</b> PARTE 3: Configuraciones de protocolos de enrutamiento .....	34
<b>d.</b> PARTE 4: Configuraciones de redundancia de primer salto .....	40
CONCLUSIONES .....	44
BIBLIOGRAFÍA.....	45

## LISTA DE FIGURAS

	Pág
Figura 1. Topología de red propuesta -----	12
Figura 2. Esquema de topología cableado detallado-----	14
Figura 3. Esquema de topología detallado-----	14
Figura 4. Resultados de configuración Router 1--- -----	15
Figura 5. Resultados de configuración Router 2 -----	16
Figura 6. Resultados de configuración Router 3 -----	17
Figura 7. Resultados de configuración Switch D1 -----	19
Figura 8. Resultados de configuración Switch D2 -----	21
Figura 9. Resultados de configuración Switch A1-----	22
Figura 10. Configuración PC1 -----	22
Figura 11. Configuración PC4 -----	23
Figura 12. Evidencia de puertos troncales switch D1 -----	24
Figura 13. Evidencia de puertos troncales switch D2 -----	24
Figura 14. Evidencia de puertos troncales switch A1 -----	25
Figura 15. Verificación de VLAN nativa D1 -----	25
Figura 16. Verificación de VLAN nativa D2 -----	25
Figura 17. Verificación de VLAN nativa A1 -----	26
Figura 18. Verificación RSTP Switch A1-----	26
Figura 19. Verificación RSTP Switch D1 -----	27
Figura 20. Verificación RSTP Switch D2 -----	27
Figura 21. Visualización root bridges Switch D1 -----	27
Figura 22. Visualización root bridges Switch D2 -----	28
Figura 23. Verificación de EtherChannel Switch D1 -----	28
Figura 24. Verificación de EtherChannel Switch D2-----	29
Figura 25. Verificación de EtherChannel Switch A1 -----	29
Figura 26. Verificación de puertos de acceso Switch D1-----	30
Figura 27. Verificación de puertos de acceso Switch D2-----	30

Figura 28. Verificación de puertos de acceso Switch A1-----	31
Figura 29. Verificación de protocolo DHCP en PC2-----	31
Figura 30. Verificación de protocolo DHCP en PC3-----	31
Figura 31. Verificación de conectividad de PC1 a PC4-----	32
Figura 32. Verificación de conectividad de PC2 a los SW-----	33
Figura 33. Verificación de conectividad de PC3 a los SW-----	33
Figura 34. Verificación de conectividad de PC4 a los SW y PC1-----	34
Figura 35. Verificación de configuración protocolos OSPF en Router 1-----	36
Figura 36. Verificación de loopback y protocolo BGP en Router 2-----	37
Figura 37. Verificación de protocolos OSPF en Router 3-----	38
Figura 38. Verificación de protocolos OSPF en SW D1-----	39
Figura 39. Verificación de protocolos OSPF en SW D2-----	40
Figura 40. Evidencia de configuración IP SLA en SW D1-----	41
Figura 41. Evidencia de configuración IP SLA en SW D2-----	42
Figura 42. Prueba de conexión entre PC1 y PC4-----	43
Figura 43. Prueba de conexión entre PC4 y PC1-----	43

## LISTA DE TABLAS

	Pag.
Tabla de direccionamiento IP.....	13

## GLOSARIO

**DHCP:** Dynamic Host Configuration Protocol, es un protocolo que funciona proporcionando automáticamente direcciones IP y otra información relacionada como la máscara y el Gateway desde un router o un Switch a los diferentes dispositivos que lo soporten evitando que la configuración se haga manual equipo a equipo.

**PORT-CHANNEL:** Este es un tipo de configuración en redes que utiliza una técnica para permitir balancear el tráfico entre varios puertos de un Switch, permitiendo aumentar el ancho de banda, aumentar la redundancia en caso de fallas para garantizar calidad y disponibilidad del servicio convirtiendo dos o más enlaces físicos en uno lógico.

**RSTP:** Rapid Spanning Tree Protocol, es una evolución del STP, para mejorar la gestión de los enlaces redundantes en una red LAN, reduciendo el tiempo de convergencia de la topología cuando ocurre algún cambio o falla.

**ROUTER:** Dispositivo que permite interconectar redes con distinto prefijo en su dirección IP, conocido típicamente como enrutador, ya que tiene la inteligencia y capacidad para enrutar un paquete hacia la red que realmente es destinataria.

**VLAN (red de área local virtual):** Es un protocolo para crear redes lógicas locales e independientes dentro de una misma red física, que permite separar el tráfico de las diferentes redes.

## **RESUMEN**

El presente trabajo que se expone en este documento es la compilación de diferentes actividades como diagrama y configuración de un sistema de conexión de redes utilizando diferentes protocolos de capa 2, 3 y Ethernet IP, dentro de los cuales se destaca las VLAN (redes de acceso local virtual) la cual permite, que se administre o se cuente con diferentes redes dentro una infraestructura, que facilite la administración y segmentación del tráfico de red de acuerdo a las necesidades de cada usuario.

Para este laboratorio se utilizó la aplicación GNS3, el cual es una herramienta robusta que emula de manera real, el funcionamiento de los equipos de red como router, switch y terminales host, con bastante similitud a los equipos usados en entornos reales, buscando aplicar diferentes comandos de configuración que permitan demostrar la conexión y funcionalidad, así como adjuntando las evidencias respectivas.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, ROUTER, VLAN, DHCP, Redes, Electrónica.

## **ABSTRACT**

The present work that is exposed in this document is the compilation of different activities such as diagram and configuration of a network connection system using different layer 2, 3 protocols and Ethernet IP, within which VLANs (virtual local access networks) stand out. ) which allows, to manage or have different networks within an infrastructure, which facilitates the administration and segmentation of network traffic according to the needs of each user.

For this laboratory, the GNS3 application was used, which is a robust tool that emulates in a real way, the operation of network equipment such as router, switch and host terminals, quite similar to the equipment used in real environments, seeking to apply different configuration commands that allow demonstrating the connection and functionality, as well as attaching the respective evidence.

Keywords: CISCO, CCNP, Switching, Routing, ROUTER, VLAN, DHCP, Networks, Electronics

## INTRODUCCIÓN

Este trabajo tiene como intención exponer el desarrollo de un laboratorio, mediante la configuración y simulación de una red informática bajo el estándar de Ethernet, encaminados principalmente en el uso de protocolos que permitan hacer más eficientes los recursos de infraestructura como router y switch, es así como se abordan diferentes protocolos aplicados en la capa de enrutamiento layer 2 aunado a otros servicios de conexión como VLAN que permitan diferentes redes utilizar la misma infraestructura, detallando más adelante todo este recorrido paso a paso.

Por otro lado, se destacan el uso de protocolos como STP (del inglés Spanning Tree Protocol) y el Port-Channel (EtherChannel) protocolo que permite agregar varios enlaces físicos en un único interfaz lógico, para una redundancia en caso de falla de uno de los enlaces, de igual manera desde los dispositivos host de prueba, se realizan las validaciones de conexión utilizando comando como ping y tracert.

Las actividades anteriormente descritas y que se observarán durante todo el documento se llevan a cabo en el software GNS3, realizando las implementaciones sugeridas en la guía de actividades denominada trabajo final, así mismo las conexiones cableadas según la topología de red, ejecutando a su vez protocolos de enrutamiento como OSPF en diferentes versiones, aplicando pruebas con interfaz de red virtual loopback, así como ejecución de protocolos BGP.

## DESARROLLO DEL ESCENARIO PROPUESTO

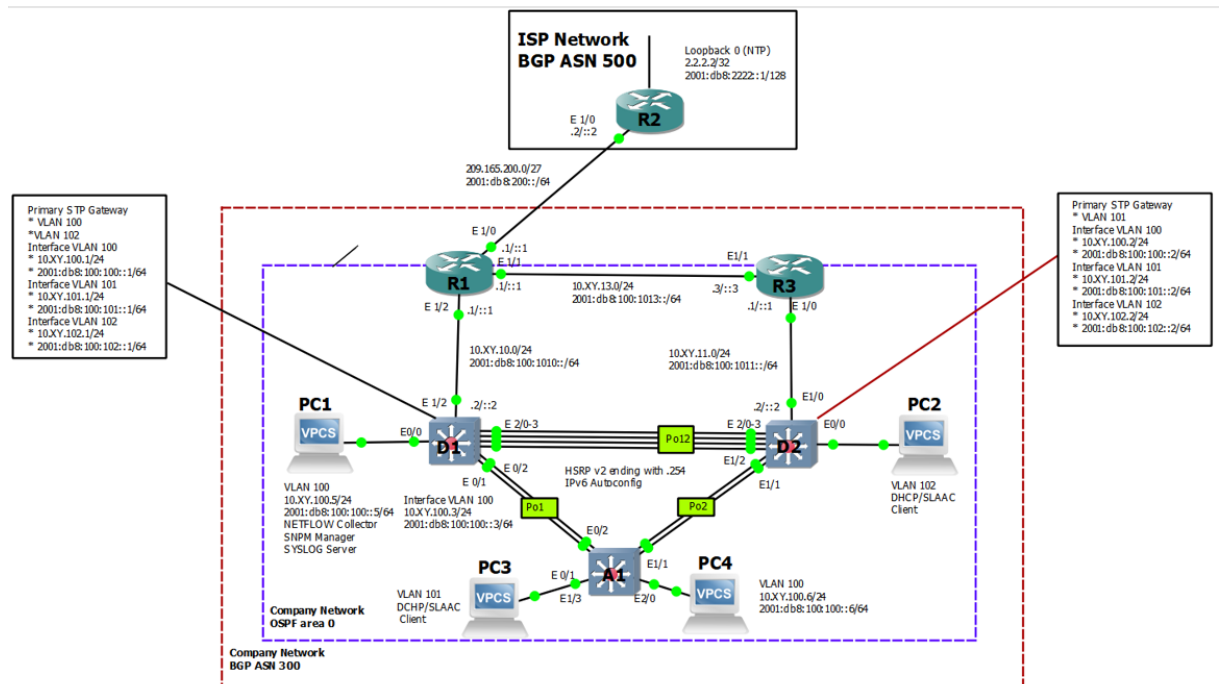
### PARTE 1: Construcción de la red y configuración de ajustes básicos del dispositivo y el direccionamiento de cada interfaz.

En este apartado se abordan los diferentes pasos de diseño y construcción de una topología de red de tipo sugerida, utilizando como aplicación de trabajo y simulación la herramienta GNS3, realizándose la elección de los diferentes equipos como ROUTER, SWICHT capa 2 y capa 3 así como equipos de usuario final.

Posterior, se lleva a cabo el cableado según los puertos e interfaces elegidas y necesarias para conexiones de tipo LAN con capacidades Ethernet y se ejecutan comandos de configuración básica para nombre de los equipos, sincronismo básico, creación de VLAN y Spanning tree.

**Paso 1: Cableado de la red como se muestra en la topología. Conexión de los dispositivos como se muestra en el diagrama de topología.**

Figura 1. Topología de red propuesta



Fuente: Diseño de red propuesto en guía de actividades trabajo final

## Paso 2: Configuración de los ajustes básicos para cada dispositivo.

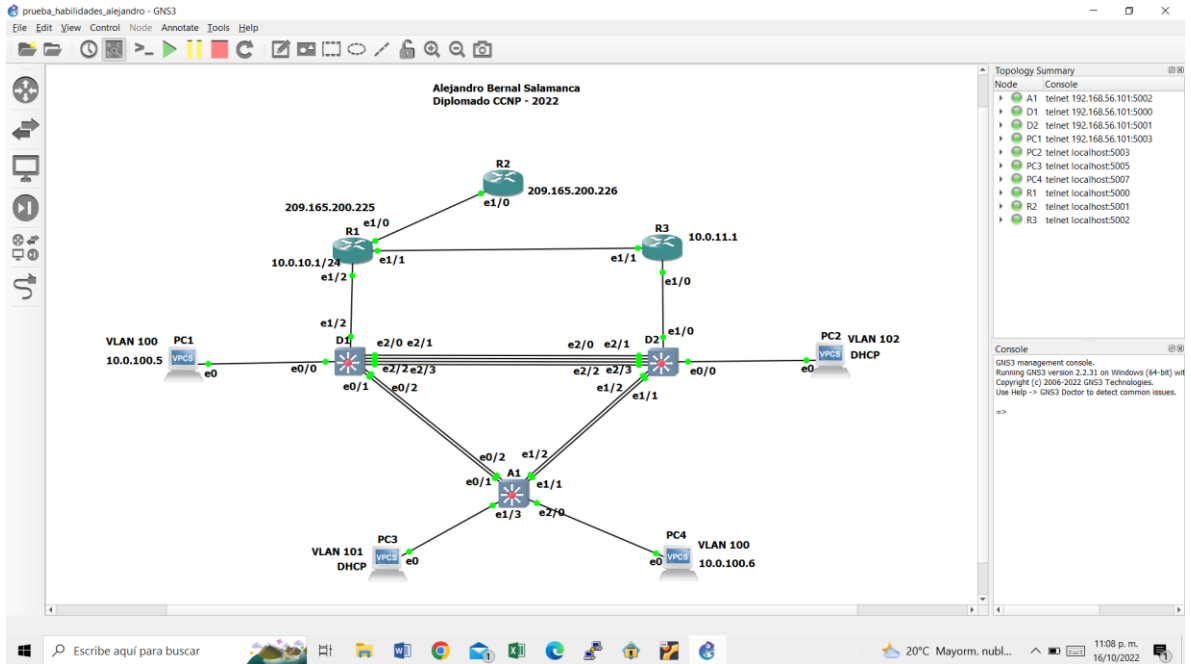
En el siguiente paso se describe las configuraciones que se realiza en cada equipo de red, siguiendo la tabla de direccionamiento que se encuentra descrita posteriormente, donde se establece el direccionamiento IPv4 e IPv6, es así como se accede a los equipos por consola, a través de la herramienta Solaris-Putty.

Figura 2. Tabla de direccionamiento IP

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.0.13.1/24	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
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	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	E1/0	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

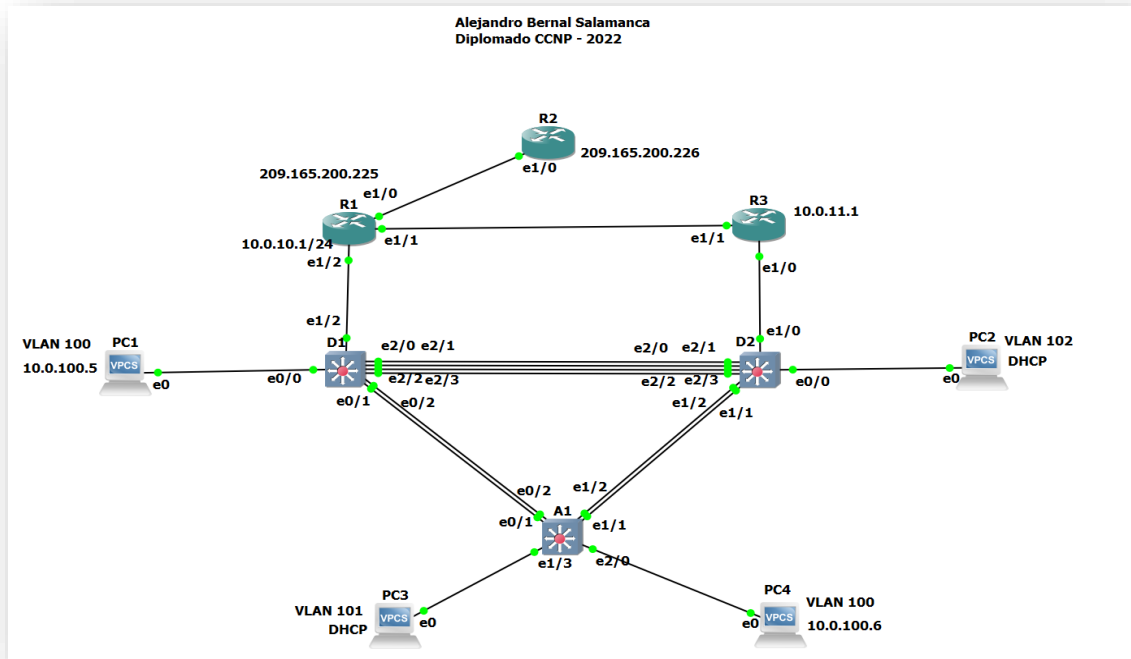
En los primeros pasos, se plantea la topología de la red y los ajustes de configuración básicos, de acuerdo a lo anteriormente descrito.

Figura 2. Esquema de topología cableado.



Fuente: propia del autor

Figura 3. Esquema de topología detallada



Fuente: propia del autor

- **Configuraciones de inicio y ajustes básicos para cada dispositivo.**

Para llevar a cabo esta actividad, es fundamental el acceso desde el modo de consola al equipo y posterior al modo de configuración global, a fin de ejecutar la configuración básica, estas se consideran configuraciones de inicio para cada dispositivo y se exponen a continuación cada uno de los comandos utilizados.

### 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 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface e1/1
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown

```

Figura 4. Resultados de configuración Router 1

```

R1#
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface Ethernet1/0
ip address 209.165.200.225 255.255.255.224
duplex half
ipv6 address FE80::1:1 link-local
ipv6 address 2001:DB8:200::1/64
!
interface Ethernet1/1
ip address 10.0.13.1 255.255.255.0
duplex half
ipv6 address FE80::1:3 link-local
ipv6 address 2001:DB8:100:1013::1/64
!
interface Ethernet1/2
ip address 10.0.10.1 255.255.255.0
duplex half
ipv6 address FE80::1:2 link-local
ipv6 address 2001:DB8:100:1010::1/64
!
interface Ethernet1/3
no ip address
shutdown
duplex half

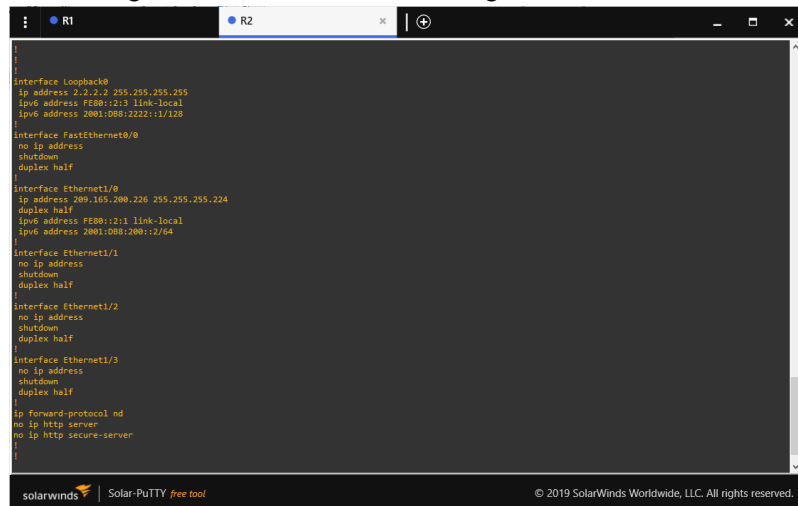
```

Fuente. Propia del autor

## 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 5. Resultados de configuración Router 2



```
!
!
interface Loopback0
ip address 2.2.2.2 255.255.255.255
ipv6 address FE80::2:3 link-local
ipv6 address 2001:DB8:2222::1/128
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface Ethernet1/0
ip address 209.165.200.226 255.255.255.224
duplex half
ipv6 address FE80::2:1 link-local
ipv6 address 2001:DB8:200::2/64
!
interface Ethernet1/1
no ip address
shutdown
duplex half
!
interface Ethernet1/2
no ip address
shutdown
duplex half
!
interface Ethernet1/3
no ip address
shutdown
duplex half
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
```

Fuente. Propia del autor

## 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 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface e1/1
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

```

Figura 6. Resultados de configuración Router 3

```

R1 R2 R3
interface FastEthernet0/0
no ip address
shutdown
duplex half
}
interface Ethernet1/0
ip address 10.0.11.1 255.255.255.0
duplex half
ipv6 address FE80::3:2 link-local
ipv6 address 2001:008:100:1011::1/64
}
interface Ethernet1/1
ip address 10.0.13.3 255.255.255.0
duplex half
ipv6 address FE80::3:3 link-local
ipv6 address 2001:008:100:1010::2/64
}
interface Ethernet1/2
no ip address
shutdown
duplex half
}
interface Ethernet1/3
no ip address
shutdown
duplex half
}
ip forward-protocol nd
no ip http server
no ip http secure-server
}
no cdp log mismatch duplex
}
control-plane
}
solarwinds Solar-PUTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

```

Fuente. Propia del autor

### 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 10.0.10.2 255.255.255.0
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 e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
shutdown
exit

```

Figura 7. Resultados de configuración Switch D1

```

D1
interface Ethernet0/1
 switchport trunk allowed vlan 100-102
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
 channel-group 1 mode active
!
interface Ethernet0/2
 switchport trunk allowed vlan 100-102
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
 channel-group 1 mode active
!
interface Ethernet0/3
 shutdown
!
interface Ethernet1/0
 shutdown
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 no switchport
 ip address 10.0.10.2 255.255.255.0
 duplex auto
 ipv6 address FE80::D11:1::1/64
 ipv6 address 2001:DB8:100:1010::1/64
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 switchport trunk allowed vlan 100-102
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
 channel-group 12 mode active
!
interface Ethernet2/1
 switchport trunk allowed vlan 100-102
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
 channel-group 12 mode active
!
interface Ethernet2/2
 switchport trunk allowed vlan 100-102
 switchport trunk encapsulation dot1q
!

```

Fuente. Autoría propia

### 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

```

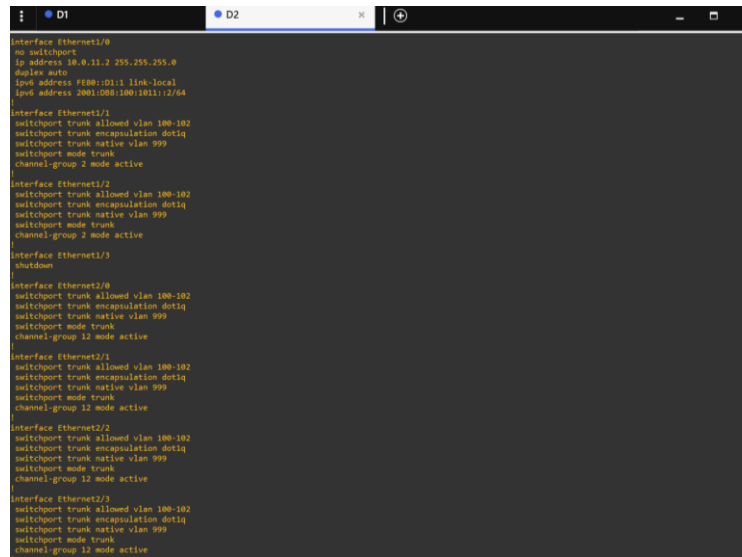
```

name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e1/0
no switchport
ip address 10.0.11.2 255.255.255.0
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 10.0.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3

```

```
shutdown
exit
```

Figura 8. Resultados de configuración Switch D2



```
Interface Ethernet1/0
switchport
ip address 10.0.11.2 255.255.255.0
duplex auto
ipv6 address FE80::D11:link-local
ipv6 address 2001:008:100:1011:12/64

Interface Ethernet1/1
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 2 mode active
!

Interface Ethernet1/2
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 2 mode active
!

Interface Ethernet1/3
shutdown
!

Interface Ethernet2/0
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!

Interface Ethernet2/1
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!

Interface Ethernet2/2
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!

Interface Ethernet2/3
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 12 mode active
!
```

Fuente. Autoría propia

### 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 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
```

```

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

```

Figura 9. Resultados de configuración Switch A1

```

Interface Ethernet0/0
shutdown
Interface Ethernet0/1
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 1 mode active
Interface Ethernet0/2
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 1 mode active
Interface Ethernet0/3
shutdown
Interface Ethernet1/0
shutdown
Interface Ethernet1/1
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 2 mode active
Interface Ethernet1/2
switchport trunk allowed vlan 100-102
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
channel-group 2 mode active
Interface Ethernet1/3
switchport access vlan 101
switchport mode access
Interface Ethernet2/0
switchport access vlan 100
switchport mode access
spanning-tree portfast edge
Interface Ethernet2/1
shutdown
Interface Ethernet2/2
shutdown
Interface Ethernet2/3
shutdown

```

Fuente. Autoría propia

- **Configuración del direccionamiento de los hosts de PC1 y PC4 como se estableció en la tabla de direccionamiento y asignación de dirección de puerta de enlace predeterminada de 10.0.100.254.**

PC1

```
ip 10.0.100.5/24 10.0.100.254
```

```
ip 2001:db8:100:100::5/64
```

PC4

```
ip 10.0.100.6/24 10.0.100.254
```

```
ip 2001:db8:100:100::6/64
```

Figura 10. Configuración PC1

```

PC1>
PC1> sh
NAME      IP /MASK      GATEWAY      MAC              LPORT  RHOST:PORT
PC1      10.0.100.5/24 10.0.100.254 00:50:79:66:68:00 20023  127.0.0.1:20024
          fe80::250:79ff:fe66:6800/64
          2001:db8:100:100::5/64
PC1>

```

Fuente. Autoría propia

Figura 11. Configuración PC4

```
PC4> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.0.100.6/24 10.0.100.254 00:50:79:66:68:02 10021 127.0.0.1:10022
Fe80::250:79ff:fe66:6802/64
2001:db8:100:100::6/64
PC4>
```

Fuente. Autoría propia

## PARTE 2: CONFIGURACIONES DE CAPA 2 DE LA RED Y SOPORTE DE HOST

En esta segunda parte, se lleva a cabo la configuración de los Switches para soportar la conectividad con los dispositivos de usuario final (computadores de escritorio), siendo uno de los pasos más importantes y de mayor cuidado, debido a que involucra la parte de acceso a la red; en este punto se realiza la configuración de las VLAN 100 y 101 y 102 aunado a la VLAN NATIVA 999, que pertenecen a cada red (management, UserGroupA y UserGroupB), a cada red VLAN se le asignan los puertos que van operar con cada red, posteriormente se configura el tipo de acceso troncal o de acceso.

De igual manera se procede con la creación de dos PORT-CHANNEL para cada Switch, configuración de alta disponibilidad o redundancia, que consiste en utilizar varios enlaces físicos y volverlos una sola interfaz, permitiendo mayor capacidad de tráfico y operando aun cuando uno de los enlaces físicos presenta algún tipo de falla.

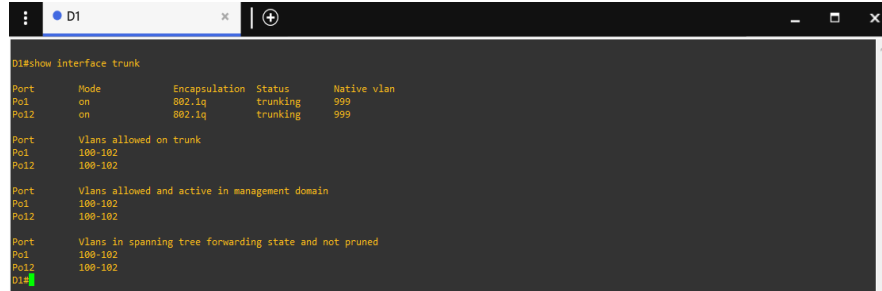
### Tarea 1: Configuración de las interfaces troncales

Es muy importante entender el comportamiento de los enlaces troncales, ya que su principal característica es la de facilitar la comunicación o permitir el paso por un mismo enlace físico de las distintas VLANs, pero también para compartir estas VLANs con otros switches gestionables que tengamos conectados a una red.

#### Switch D1

```
interface range e2/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
interface range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

Figura 12. Evidencia de puertos troncales switch D1



```
D1#show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
Po1       on        802.1q         trunking      999
Po12      on        802.1q         trunking      999

Port      Vlans allowed on trunk
Po1       100-102
Po12      100-102

Port      Vlans allowed and active in management domain
Po1       100-102
Po12      100-102

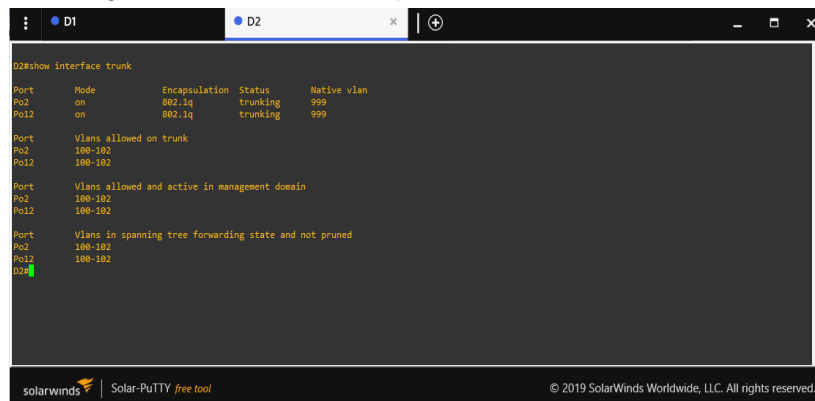
Port      Vlans in spanning tree forwarding state and not pruned
Po1       100-102
Po12      100-102
D1#
```

Fuente. Autoría propia

### Switch D2

```
interface range e2/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
interface range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

Figura 13. Evidencia de puertos troncales switch D2



```
D2#show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
Po2       on        802.1q         trunking      999
Po12      on        802.1q         trunking      999

Port      Vlans allowed on trunk
Po2       100-102
Po12      100-102

Port      Vlans allowed and active in management domain
Po2       100-102
Po12      100-102

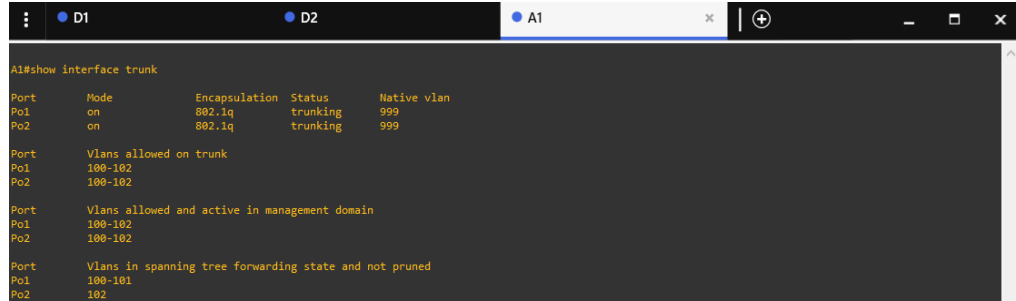
Port      Vlans in spanning tree forwarding state and not pruned
Po2       100-102
Po12      100-102
D2#
```

Fuente. Autoría propia

### Switch A1

```
interface range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
interface range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

Figura 14. Evidencia de puertos troncales switch A1



```
A1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po2       on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po1       100-102
Po2       100-102

Port      Vlans allowed and active in management domain
Po1       100-102
Po2       100-102

Port      Vlans in spanning tree forwarding state and not pruned
Po1       100-101
Po2       102
```

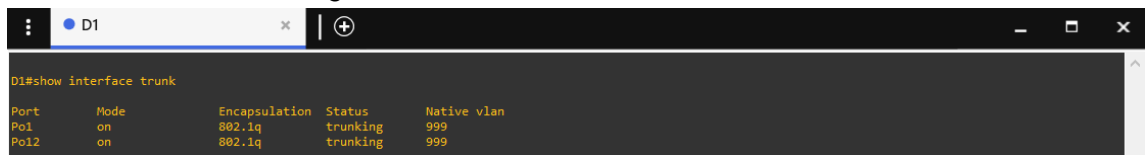
Fuente. Autoría propia

## Tarea 2: Configuración de la VLAN 999 como nativa

### Switch D1

```
interface range e2/0-3
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface range e0/1-2
switchport mode trunk
switchport trunk native vlan 999
no shutdown
```

Figura 15. Verificación de VLAN nativa D1



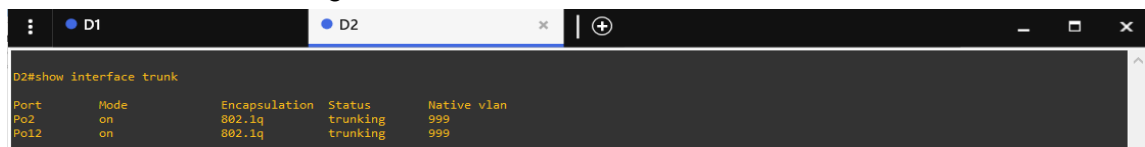
```
D1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999
```

Fuente. Autoría propia

### Switch D2

```
interface range e2/0-3
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface range e1/1-2
switchport mode trunk
switchport trunk native vlan 999
no shutdown
```

Figura 16. Verificación de VLAN nativa D2



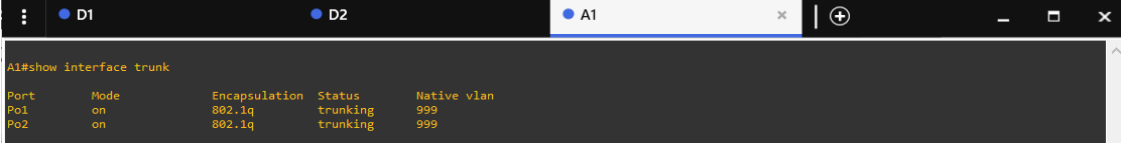
```
D2#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999
```

Fuente. Autoría propia

## Switch A1

```
interface range e0/1-2
switchport mode trunk
switchport trunk native vlan 999
no shutdown
interface range e1/1-2
switchport mode trunk
switchport trunk native vlan 999
no shutdown
```

Figura 17. Verificación de VLAN nativa A1



Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	999
Po2	on	802.1q	trunking	999

Fuente. Autoría propia

## Tarea 3: ejecución del protocolo Rapid Spanning-Tree (RSTP)


Real Time Streaming Protocol (RTSP) es un protocolo que es la evolución del STP, utilizado en la capa del nivel de aplicación utilizado para establecer y controlar sesiones de medios entre puntos finales, permite facilitar el tiempo de respuesta de redundancia en redes LAN.

Switch D1: spanning-tree mode rapid-pvst

Switch D2: spanning-tree mode rapid-pvst

Switch A1: spanning-tree mode rapid-pvst

Figura 18. Verificación RSTP Switch A1



```
A1#show run
Building configuration...

Current configuration : 2737 bytes
!
! Last configuration change at 13:07:48 UTC Sat Oct 15 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname A1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
```

Fuente. Propia del autor

Figura 19. Verificación RSTP Switch D1

```
D1#show spanning-tree
VLAN0100
Spanning tree enabled protocol rstp
Root ID    Priority    32868
           Address    aabb.cc00.0100
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32868 (priority 32768 sys-id-ext 100)
           Address    aabb.cc00.0100
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
```

Fuente. Propia del autor

Figura 20. Verificación RSTP Switch D2

```
D2#show spanning-tree
VLAN0100
Spanning tree enabled protocol rstp
Root ID    Priority    32868
           Address    aabb.cc00.0100
           Cost        41
           Port        66 (Port-channel12)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32868 (priority 32768 sys-id-ext 100)
           Address    aabb.cc00.0200
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec
```

Fuente. Propia del autor

#### Tarea 4: Configuración de los puentes raíz (root bridges)

##### Switch D1

```
spanning-tree vlan 101 root primary
spanning-tree vlan 102 root secondary
```

Figura 21. Visualización root bridges Switch D1

```

Po1          Desg FWD 56      128.65  Shr
Po12         Desg FWD 41      128.66  Shr

D1#show spanning-tree vlan 101
VLAN0101
Spanning tree enabled protocol rstp
Root ID    Priority    24677
           Address    aabb.cc00.0100
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    24677 (priority 24576 sys-id-ext 101)
           Address    aabb.cc00.0100
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface   Role Sts Cost    PrIo Nbr Type
-----
Po1         Desg FWD 56      128.65  Shr
Po12        Desg FWD 41      128.66  Shr

D1#
```

Fuente. Propia del autor

##### Switch D2

```
spanning-tree vlan 102 root primary
```

spanning-tree vlan 101 root secondary

Figura 22. Visualización root bridges Switch D2



```
D2#show sp
D2#show spanning-tree vlan 102

VLAN0102
Spanning tree enabled protocol rstp
Root ID: Priority 24678
Address aabb.cc00.0200
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID: Priority 24678 (priority 24576 sys-id-ext 102)
Address aabb.cc00.0200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
e0/0 Desg FWD 100 128.1 Shr Edge
Po2 Desg FWD 50 128.65 Shr
Po12 Desg FWD 41 128.66 Shr

D2#
```

Fuente. Propia del autor

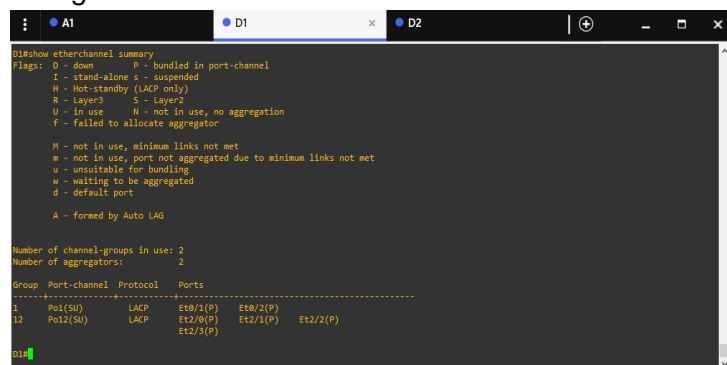
### Tarea 5: Configuración de los LACP EtherChannels.

Un EtherChannel es un protocolo de configuración que ayuda a balancear el tráfico entre varios puertos (enlaces entre SW), permitiendo aumentar el ancho de banda, aumentar la redundancia y evitar problemas de bucles, en este laboratorio se realizan 3 EtherChannels entre D1 y A1, D1 y D2 y A1 y D2, donde se utilizan dos puertos y cuatro puertos a cada uno de los lados, convirtiéndose en un solo enlace, aplicando la configuración como si fuera una interfaz física independiente.

#### Switch D1

```
interface range e2/0-3
channel-group 12 mode active
no shutdown
exit
interface range e0/1-2
channel-group 1 mode active
no shutdown
exit
```

Figura 23. Verificación de EtherChannel Switch D1



```
D1#show etherchannel summary

Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use H - not in use, no aggregation
f - failed to allocate aggregator

H - not in use, minimum links not met
W - not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

A - forced by Auto LAG

Number of channel-groups in use: 2
Number of aggregators: 2

Group Port-channel Protocol Ports
-----
1 Po1(SU) LACP Et0/1(P) Et0/2(P)
12 Po12(SU) LACP Et2/0(P) Et2/1(P) Et2/2(P)

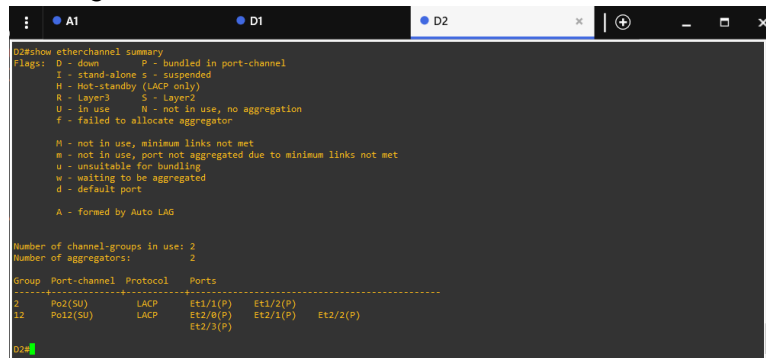
D1#
```

Fuente. Autoría propia

## Switch D2

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

Figura 24. Verificación de EtherChannel Switch D2



```
D2#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  S - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2


Group  Port-channel  Protocol    Ports
-----
  2    Po2(SU)         LACP        Et1/1(P)  Et1/2(P)
 12    Po12(SU)        LACP        Et2/0(P)  Et2/1(P)
                               Et2/3(P)
```

Fuente. Autoría propia

## Switch A1

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

Figura 25. Verificación de EtherChannel Switch A1



```
A1#show etherchannel s
A1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  S - suspended
       H - not-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----
  1    Po1(SU)         LACP        Et0/1(P)  Et0/2(P)
  2    Po2(SU)         LACP        Et1/1(P)  Et1/2(P)
```

Fuente. Autoría propia

## Tarea 6: Configuración de los puertos de acceso a los PC (host).

Para esta tarea, es típicamente configurada para los equipos de usuario final (host de escritorio) y permiten el tráfico de una sola VLAN, la diferencia a un puerto troncal es que este si permite el paso de varias VLAN.

### Switch D1

```
interface e0/0
switchport mode access
switchport access vlan 100
no shutdown
exit
```

Figura 26. Verificación de puertos de acceso Switch D1



```

@ lost carrier, 0 no carrier
@ output buffer failures, 0 output buffers swapped out
D1#show run interface ethernet 0/0
Building configuration...

Current configuration : 110 bytes
}
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
D1#show run interface ethernet 0/0
Building configuration...

Current configuration : 110 bytes
}
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
D1#
```

Fuente. Autoría propia

### Switch D2:

```
interface e0/0
switchport mode access
switchport access vlan 102
no shutdown
exit
```

Figura 27. Verificación de puertos de acceso Switch D2



```

B2#show run interface ethernet 0/0
Building configuration...

Current configuration : 136 bytes
}
interface Ethernet0/0
 description LAN-VLAN_102
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
end
B2#show run interface ethernet 0/0
Building configuration...

Current configuration : 136 bytes
}
interface Ethernet0/0
 description LAN-VLAN_102
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
end
B2#
```

Fuente. Autoría propia

## Switch A1

```
interface e1/3
switchport mode access
switchport access vlan 101
no shutdown
exit
interface e2/0
switchport mode access
switchport access vlan 100
no shutdown
exit
```

Figura 28. Verificación de puertos de acceso Switch A1



```
A1
1 Po1(SU) LACP Et0/1(P) Et0/2(P)
2 Po2(SU) LACP Et1/1(P) Et1/2(P)

A1#show run interface et
A1#show run interface ethernet 1/3
Building configuration...

Current configuration : 81 bytes
1
interface Ethernet1/3
switchport access vlan 101
switchport mode access
end

A1#show run interface ethernet 1/3
Building configuration...

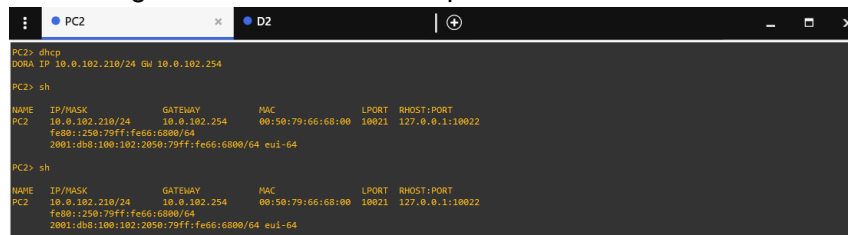
Current configuration : 81 bytes
1
interface Ethernet1/3
switchport access vlan 101
switchport mode access
end

A1#
```

Fuente. Autoría propia

## Tarea 7: Verificar los PC2 y PC3 en DHCP

Figura 29. Verificación de protocolo DHCP en PC2



```
PC2> dhcp
DORA IP 10.0.102.210/24 Gw 10.0.102.254

PC2> sh

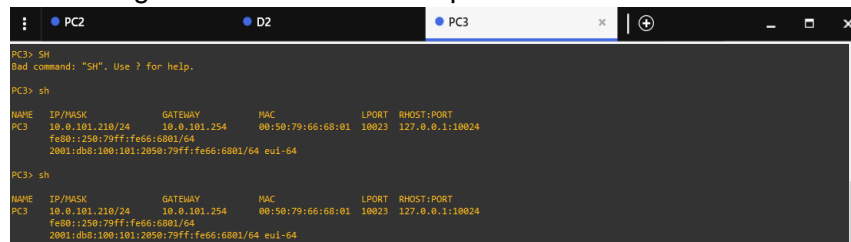
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.102.210/24 10.0.102.254 00:50:79:66:68:00 10021 127.0.0.1:10022
fe80::250:79ff:fe66:6800/64
2001:db8:100:102:2050:79ff:fe66:6800/64 eui-64

PC2> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC2 10.0.102.210/24 10.0.102.254 00:50:79:66:68:00 10021 127.0.0.1:10022
fe80::250:79ff:fe66:6800/64
2001:db8:100:102:2050:79ff:fe66:6800/64 eui-64
```

Fuente. Autoría propia

Figura 30. Verificación de protocolo DHCP en PC3



```
PC3> SH
Bad command: "SH". Use ? for help.

PC3> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.210/24 10.0.101.254 00:50:79:66:68:01 10023 127.0.0.1:10024
fe80::250:79ff:fe66:6801/64
2001:db8:100:101:2050:79ff:fe66:6801/64 eui-64

PC3> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC3 10.0.101.210/24 10.0.101.254 00:50:79:66:68:01 10023 127.0.0.1:10024
fe80::250:79ff:fe66:6801/64
2001:db8:100:101:2050:79ff:fe66:6801/64 eui-64
```

Fuente. Autoría propia

## Tarea 8: Verificación de la conectividad de la LAN local

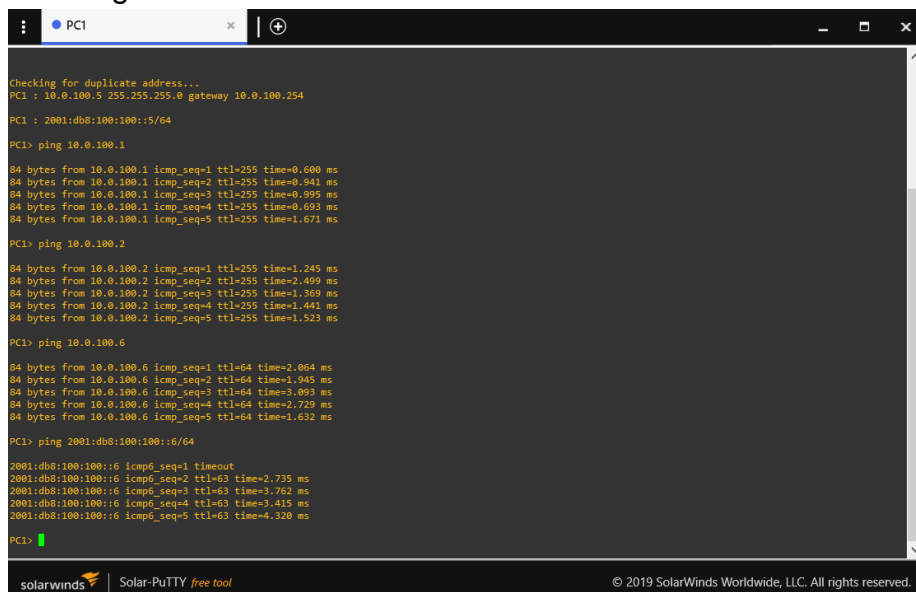
Una vez finalizadas las configuraciones de capa 2, se realizan las pruebas de conectividad desde ambos extremos de la red, desde los equipos finales (computadoras de escritorio); se va haciendo prueba a cada interfaz que pertenezca a la VLAN o red configurada hasta llegar al dispositivo final deseado.

Desde PC1, se verifica conectividad a través de comando PING en tráfico IPv4 and IPv6 hasta PC4.

PC1: pruebas de ping

- Hacia el SW-D1: 10.0.100.1
- Hacia el SW-D2: 10.0.100.2
- Hacia el PC4: 10.0.100.6

Figura 31. Verificación de conectividad de PC1 a PC4



```
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1 : 2001:db8:100:100::5/64

PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.600 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.941 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.999 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.693 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.671 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.245 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=2.499 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.369 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.441 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.523 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=2.064 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.945 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=3.093 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=2.729 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.632 ms

PC1> ping 2001:db8:100:100::6/64
2001:db8:100:100::6 icmp6_seq=1 timeout
2001:db8:100:100::6 icmp6_seq=2 ttl=63 time=2.735 ms
2001:db8:100:100::6 icmp6_seq=3 ttl=63 time=3.762 ms
2001:db8:100:100::6 icmp6_seq=4 ttl=63 time=3.415 ms
2001:db8:100:100::6 icmp6_seq=5 ttl=63 time=4.320 ms

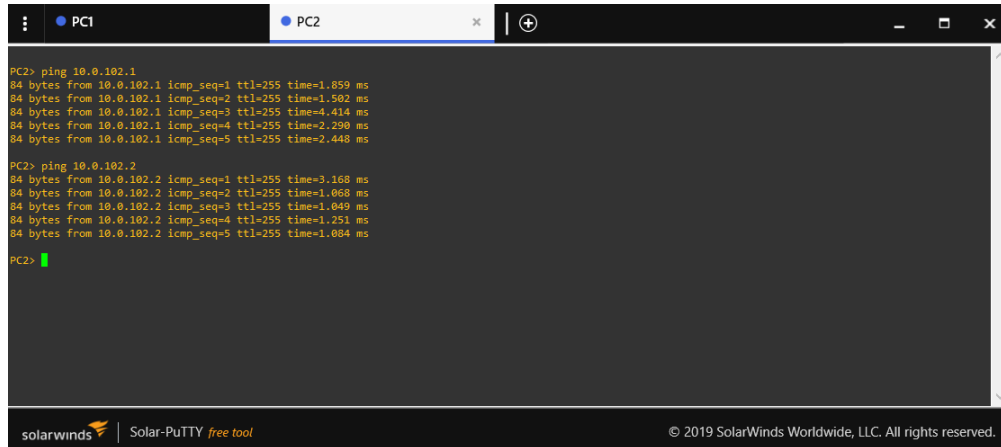
PC1>
```

Fuente. Autoría propia

PC2: pruebas de ping:

- Hacia el SW-D1: 10.0.102.1
- Hacia el SW-D2: 10.0.102.2

Figura 32. Verificación de conectividad de PC2 a los SW



```
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.859 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.502 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=4.414 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=2.290 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=2.448 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=3.168 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=1.068 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=1.049 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=1.251 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=1.084 ms

PC2> █
```

Fuente. Autoría propia

PC3: pruebas de ping:

- Hacia el SW-D1: 10.0.101.1
- Hacia el SW-D2: 10.0.101.2

Figura 33. Verificación de conectividad de PC3 a los SW



```
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=1.551 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=3.602 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.357 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=2.386 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=2.546 ms

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=2.413 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=2.199 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=2.302 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=5.071 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=6.687 ms

PC3> █
```

Fuente. Autoría propia

PC4: pruebas de ping

- Hacia el SW-D1: 10.0.100.1
- Hacia el SW-D2: 10.0.100.2
- Hacia el PC4: 10.0.100.5

Figura 34. Verificación de conectividad de PC4 a los SW y PC1



```
PC1 - 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC1 : 2001:db8:100:100:16/64

PC4> ping 10.0.100.1
64 bytes from 10.0.100.1: icmp_seq=1 ttl=255 time=1.732 ms
64 bytes from 10.0.100.1: icmp_seq=2 ttl=255 time=1.632 ms
64 bytes from 10.0.100.1: icmp_seq=3 ttl=255 time=1.771 ms
64 bytes from 10.0.100.1: icmp_seq=4 ttl=255 time=2.346 ms
64 bytes from 10.0.100.1: icmp_seq=5 ttl=255 time=1.760 ms

PC4> ping 10.0.100.2
64 bytes from 10.0.100.2: icmp_seq=1 ttl=255 time=2.184 ms
64 bytes from 10.0.100.2: icmp_seq=2 ttl=255 time=2.336 ms
64 bytes from 10.0.100.2: icmp_seq=3 ttl=255 time=2.069 ms
64 bytes from 10.0.100.2: icmp_seq=4 ttl=255 time=2.248 ms
64 bytes from 10.0.100.2: icmp_seq=5 ttl=255 time=2.249 ms

PC4> ping 10.0.100.5
64 bytes from 10.0.100.5: icmp_seq=1 ttl=64 time=1.877 ms
64 bytes from 10.0.100.5: icmp_seq=2 ttl=64 time=1.752 ms
64 bytes from 10.0.100.5: icmp_seq=3 ttl=64 time=2.720 ms
64 bytes from 10.0.100.5: icmp_seq=4 ttl=64 time=1.988 ms
64 bytes from 10.0.100.5: icmp_seq=5 ttl=64 time=2.227 ms

PC4> ping 2001:db8:100:100:15/64
2001:db8:100:100:15: icmp_seq=1 ttl=64 time=1.863 ms
2001:db8:100:100:15: icmp_seq=2 ttl=64 time=1.709 ms
2001:db8:100:100:15: icmp_seq=3 ttl=64 time=2.153 ms
2001:db8:100:100:15: icmp_seq=4 ttl=64 time=1.832 ms
2001:db8:100:100:15: icmp_seq=5 ttl=64 time=2.051 ms

PC4>
```

Fuente. Autoría propia

En los anteriores screenshot, se utilizó el comando PING para realizar las verificaciones de conexión, donde inicialmente se verifica la conectividad de red en estándar IPV4 y posterior se ejecutó en IPV6 (aplica solo para PC1 y PC4), en ambos escenarios se observa como los paquetes del comando PING fueron exitosos garantizando conexión, en ambos sentidos de la red.

### PARTE 3: CONFIGURACIONES DE PROTOCOLOS DE ENRUTAMIENTO

El tercer componente del presente laboratorio está enfocado en configurar los protocolos de enrutamiento IPv4 e IPv6, así como las configuraciones Loopback a fin de lograr una convergencia entre los diferentes dispositivos que conforman la red.

Para ello se despliegan diferentes tareas de configuración por pasos o etapas, iniciando con los protocolos OSPF (protocolo de primero la ruta más corta) y BGP (protocolo de puerta de enlace de frontera) que buscan hacer más eficiente la red y permitir el tráfico a nivel de redes o de tipo WAN.

Tarea 3.1, 3.2, 3.3 y 3.4 configuraciones de los protocolos OSPFv2, OSPFv3, BGP y MP-BGP, para garantizar convergencia a nivel de redes.

#### Router R1

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

```

exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
exit
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family

```

Figura 35. Verificación de configuración protocolos OSPF en Router 1

```

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#show ip pr
R1#show ip prot
R1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.4.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.10.0 0.0.0.255 area 0
    10.0.13.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

R1#show run | section ^router-ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
R1#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
R1#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID  Cost  State Nbrs F/C
Et1/1     6   0             5        10   DR   0/0
Et1/2     6   0             6        10   DR   0/0
R1#

```

Fuente. Autoría propia

## Router R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
  bgp router-id 2.2.2.2
  neighbor 209.165.200.225 remote-as 300
  neighbor 2001:db8:200::1 remote-as 300
  address-family ipv4
    neighbor 209.165.200.225 activate
    no neighbor 2001:db8:200::1 activate
    network 2.2.2.2 mask 255.255.255.255
    network 0.0.0.0
  exit-address-family
  address-family ipv6
    no neighbor 209.165.200.225 activate
    neighbor 2001:db8:200::1 activate
    network 2001:db8:2222::/128
    network ::/0
  exit-address-family
```

Figura 36. Verificación de loopback y protocolo BGP en Router 2



```
[OK]
R2#show bgp
R2#show bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
BPKT validation codes: V valid, I invalid, N Not found

   Network          Next Hop           Metric LocPrf  Weight Path
  *+ 0.0.0.0         0.0.0.0             0           32768 i
  *+ 2.2.2.2/32     0.0.0.0             0           32768 i

R2#show run | section bgp
router bgp 500
  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#show ip ro
R2#show ip route b
R2#show ip route bgp
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
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       Ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       * - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R2#
```

Fuente. Autoría propia

## ROUTER 3

```
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

```

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

```

Figura 37. Verificación de protocolos OSPF en Router 3

```

R3(R1)
R3(R2)
R3(R3)
R3(config)#show ip protocol
^
% Invalid input detected at '^' marker.
R3(config)#exit
R3#
*Nov 10 20:53:39.795: XSYS-5-CONFIG_I: Configured from console by console
R3#
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]
R3#
R3#
R3#
R3#show ip pro
R3#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.4.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.11.0 0.0.0.255 area 0
    10.0.13.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    0.0.4.1          110           00:01:25
  Distance: (default is 110)

R3#show run | section ^router ospf
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
R3#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
Et1/0      6   0     4        10   DR    0/0
R3#

```

Fuente. Autoría propia

### SW D1

```

router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/2
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default

```

```

no passive-interface e1/2
exit
interface e1/2
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

```

Figura 38. Verificación de protocolos OSPF en SW D1

```

D1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "application"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Maximum paths: 32
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 4)

Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.4.131
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum paths: 4
  Routing for Networks:
    10.0.100.0 0.0.0.255 area 0
    10.0.100.0 0.0.0.255 area 0
    10.0.101.0 0.0.0.255 area 0
    10.0.102.0 0.0.0.255 area 0
  Passive Interface(s):
    Vlan1
    Vlan100
    Vlan101
    Vlan102
  Routing Information Sources:
    Gateway         Distance      Last Update
    0.0.4.1          110           00:07:42
    0.0.4.3          110           00:07:42
  Distance: (default is 110)

D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
network 10.0.10.0 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
D1#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
Et1/2     6   0     21      10    BDR   1/1

D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
network 10.0.10.0 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

```

Fuente. Autoría propia

### SW D2

```

router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0

```

```

passive-interface default
no passive-interface e1/0
exit
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

```

Figura 39. Verificación de protocolos OSPF en SW D2

```

D2#
D2#
D2#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "application"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Maximum path: 32
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 4)

Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.4.132
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.11.0 0.0.0.255 area 0
    10.0.100.0 0.0.0.255 area 0
    10.0.101.0 0.0.0.255 area 0
    10.0.102.0 0.0.0.255 area 0
  Passive Interface(s):
    Vlan1
    Vlan100
    Vlan101
    Vlan102
  Routing Information Sources:
    Gateway         Distance      Last Update
    0.0.4.1          110           00:09:56
  Distance: (default is 110)

D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
network 10.0.11.0 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
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	
E1/0	6	0	21	10	BDR	1/1	

Fuente. Autoría propia

## PARTE 4: CONFIGURACIONES DE REDUNDANCIA DE PRIMER SALTO

Las configuraciones finales del presente laboratorio de habilidades prácticas, resaltan la configuración del protocolo de routing de reserva activa (HSRP) además de las IP SLA (Service Level Agreement), con el fin de mantener un monitoreo constante a los estados de la red, con unos tiempos preestablecidos.

Estas configuraciones se realizan en los equipos de capa 2, en los switth D1 y D2.

### Swicth D1

```
ip sla 4
icmp-echo 10.0.10.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
```

```

standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

```

Figura 40. Evidencia de configuración IP SLA en SW D1

```

D1
!
ipv6 ospf 6 area 0
!
interface Vlan101
ip address 10.0.101.1 255.255.255.0
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
ipv6 address FE80::D1:3 link-local
ipv6 address 2001:088:100:101::1/64
ipv6 ospf 6 area 0
!
interface Vlan102
ip address 10.0.102.1 255.255.255.0
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
ipv6 address FE80::D1:4 link-local
ipv6 address 2001:088:100:102::1/64
ipv6 ospf 6 area 0
!
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
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
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip sla 4
icmp-echo 10.0.10.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:088:100:1010::1
frequency 5
ip sla schedule 6 life forever start-time now
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet1/2

```

Fuente: autoría propia

### Switch D2

```

ip sla 4
icmp-echo 10.0.11.1
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
interface vlan 100

```

```

standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

```

Figura 41. Evidencia de configuración IP SLA en SW D2

```

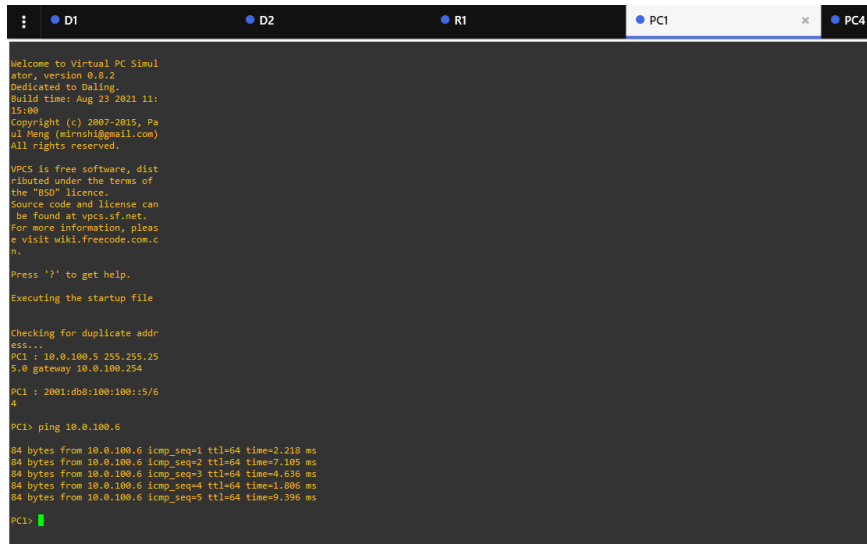
D1 D2 R1
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface Vlan101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface Vlan102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
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
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip sla 4
icmp-echo 10.0.11.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:101:1
frequency 5

```

Fuente: autoría propia

## Pruebas de conexión a través de comandos ping

Figura 42. Prueba de conexión entre PC1 y 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...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
PC1 : 2001:db8:100:100::5/64

PC1> ping 10.0.100.6


84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=2.218 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=7.105 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=4.036 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.806 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=9.396 ms

PC1>

```

Fuente: autoría propia

Figura 43. Prueba de conexión entre PC4 y PC1



```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, 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 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC1 : 2001:db8:100:100::6/64

PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=2.262 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=7.854 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=2.691 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=12.509 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=21.303 ms

PC4>

```

Fuente: autoría propia

## CONCLUSIONES

Como conclusión importante del desarrollo del presente laboratorio, se puede enfocar al uso de las redes VLAN que permiten a varias redes diferentes coexistir y utilizar la misma infraestructura de manera independiente, este protocolo también garantiza que un enrutador ejecute más de una tabla de enrutamiento simultáneamente siendo un avance muy acertado al servicio de las telecomunicaciones, aunado a esto existen otros protocolos como RSTP, que administra y hace más eficiente las redes LAN ante eventuales fallas.

Por otro lado, los servicios que ofrece el protocolo EtherChannel, ayudan a garantizar alta disponibilidad y redundancia de manera eficiente y sin generar uso ineficiente de los recursos de red, siendo necesario configurar de manera acorde los servicios troncales y de acceso dentro de la red. Existen de igual manera los protocolos de enrutamiento que permiten la conectividad entre diferentes redes, destacando OSPF en versión 2 y 3, que complementan una red convergente en sus diferentes capas 2 y 3.

Los protocolos de IP SLA, son una herramienta de monitoreo bastante útil que permite recopilar información del rendimiento de la red, tiempo de respuesta, la latencia y otros parámetros que ayudan a la administración efectiva de una red, si bien es un protocolo exclusivo, es bastante útil y aplicable como apoyo al trabajo de soporte técnico.

## BIBLIOGRAFÍA

EDGEWORTH, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>.

EDGEWORTH, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350- 401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>.

Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). <https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoWx>.

Froom, R., Frahim, E, (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementation Cisco IP Swiched Network (SWICTH) Foundation Learning Guide CCNP Swich 300-315. <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (route) Foundation Learning Guide CCNP ROUTE 300-101.(2015). <https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoWx>.