

DIPLOMADO DE PROFUNDIZACION CISCO CCNP SOLUCIÓN DE DOS  
ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO  
DE TECNOLOGÍA CISCO

OSCAR ALBERTO RUEDA GORDILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE  
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI  
INGENIERÍA EN TELECOMUNICACIONES  
BOGOTA  
2020

DIPLOMADO DE PROFUNDIZACION CISCO CCNP SOLUCIÓN DE DOS  
ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO  
DE TECNOLOGÍA CISCO

OSCAR ALBERTO RUEDA GORDILLO

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE  
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA EN TELECOMUNICACIONES  
BOGOTA  
2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

BOGOTÁ, 30 de noviembre de 2020

## AGRADECIMIENTOS

Agradezco profundamente a mi familia, amigos y todas las personas que me acompañaron, me dieron aliento para continuar con mis estudios. El resultado de esta compañía fue para mi fundamental ya que de manera continua mi crecimiento profesional y personal no se detuvo. Mis agradecimientos no estarían completos sin mencionar a la institución que me dio la oportunidad de hacer parte de ella y de la que estoy pronto a terminar mi pregrado, la UNAD y todos sus colaboradores, gracias a su modelo virtual me resulto idóneo en todo el transcurso de mi pregrado.

## CONTENIDO

	Pág.
AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN .....	11
DESARROLLO DE LOS ESCENARIOS.....	12
PRIMER ESCENARIO.....	12
SEGUNDO ESCENARIO .....	21
CONCLUSIONES .....	39
BIBLIOGRAFÍA.....	40

## LISTA DE TABLAS

	Pág.
Tabla 1. listado de VPN Segundo Escenario .....	28
Tabla 2 Interfaces específicas de VLAN segundo escenario .....	31

## LISTA DE FIGURAS

	Pág
Figura 1 Topología primer escenario .....	12
Figura 2 Primer escenario desarrollado en GNS3 .....	13
Figura 3 Verificación tabla de enrutamiento en R3 primer escenario.....	17
Figura 4 Verificación de tabla de enrutamiento en R1 primer escenario.....	19
Figura 5 Verificación de tabla de enrutamiento en R5 primer escenario.....	20
Figura 6 Topología segundo escenario.....	21
Figura 7 Segundo escenario desarrollado en GNS3.....	22
Figura 8 Verificación de VLAN en DLS1 segundo escenario .....	33
Figura 9 Verificación de VLAN en DLS2 segundo escenario .....	34
Figura 10 Verificación de VLAN en ALS1 segundo escenario .....	34
Figura 11 Verificación de VLAN en ALS2 segundo escenario .....	35
Figura 12 Verificación de EtherChannel en DLS1 segundo escenario .....	35
Figura 13 Verificación de EtherChannel en DLS2 segundo escenario .....	36
Figura 14 Verificación de Spanning tree en DLS1 segundo escenario .....	37
Figura 15 Verificación de Spanning tree en DLS2 segundo escenario .....	38

## GLOSARIO

**PROTOCOLOS DE ENRUTAMIENTO:** Consisten en un conjunto de reglas y normas que dan como resultado la forma en la cual 2 equipos activos (router) se conectan entre sí.

**PROTOCOLO OSPF:** Protocolo de enrutamiento que tiene como regla base buscar el camino más cercano para enviar los datos, este protocolo es jerárquico.

**PROTOCOLO VTP:** Protocolo para administrar y configurar en distintos niveles las VLAN, opera en 3 modos distintos Cliente, Servidor, Transparente, existente distintas versiones de este protocolo.

**ROUTER:** Equipo activo que hace parte de una red de datos, trabaja sobre la capa 3 del modelo OSI.

**SPANNING TREE PROTOCOL:** Protocolo que trabaja en la capa 2 del modelo OSI, se encarga de gestionar el tráfico de una red, evitando bucles y redundancias.

**SWITCH:** Equipo de comunicaciones, puede trabajar dependiendo el modelo, en la capa 2 o 3, su función principal es comunicar equipos cliente entre sí mismos, servidores y router.

**VLAN:** acrónimo de red de área local virtual en español, se usa para segmentar de forma virtual distintas redes conectadas al mismo o mismos equipos de comunicación (switch).

## RESUMEN

En este documento se evidenciará la aplicación práctica de los conocimientos adquiridos durante el desarrollo del diplomado CCNP, simulando dos distintos escenarios que requieren la aplicación de conocimientos teóricos y su funcionamiento de manera práctica, para esta simulación se usó el software libre GNS3, esta es una herramienta en constante crecimiento y con una comunidad de usuarios alrededor del mundo, por lo tanto, esta herramienta está en constante mejora.

El primer escenario está enfocado en aplicar los conocimientos vistos durante la fase de ROUTING, aplicando 2 distintos protocolos de enrutamiento de manera adecuada, sin dejar de lado los posibles escenarios de la vida real, en los cuales todos los factores se deben tener en cuenta, como distancia administrativa, tipo de comunicación entre equipos activos, negociación entre distintas administraciones entre otros.

El segundo escenario aborda el SWITCHING, y de igual manera que el primera aborda los temas que se involucran en la administración de una red usando Switch que están en la capa 2 y 3 del modelo OSI y como estos interactúan y se comportan dependiendo de su configuración y necesidad.

**PALABRAS CLAVE:** NETWORKING, OSP, EIGRP, GNS3, ROUTER, SWITCH, CCNP, BGP, TELECOMMUNICACIONES.

## ABSTRACT

This document will show the practical application of the knowledge acquired during the development of the CCNP diploma, simulating two different scenarios that require the application of theoretical knowledge and its operation in a practical way, for this simulation was used the free software GNS3, this is a tool in constant growth and with a community of users around the world, therefore, this tool is constantly improving.

The first scenario is focused on applying the knowledge seen during the ROUTING phase, applying 2 different routing protocols in an adequate way, without leaving aside the possible real-life scenarios, in which all factors must be taken into account, such as administrative distance, type of communication between active teams, negotiation between different administrations among others.

The second scenario deals with SWITCHING, and just like the first one deals with the issues involved in the administration of a network using switches that are in the layer 2 and 3 of the OSI model and how these interact and behave depending on their configuration and need.

**KEYWORDS:** NETWORKING, OSP, EIGRP, GNS3, ROUTER, SWITCH, CCNP, BGP, TELECOMMUNICATIONS.

## INTRODUCCIÓN

Las tecnologías de telecomunicaciones y enrutamiento son pilares fundamentales de la vida moderna, estas soportan un sinfín de sectores y servicios en todos los niveles, en la actualidad el conocimiento a detalle de los distintos protocolos que se interconectan entre sí para lograr la conectividad al año 2020 son una herramienta fundamental para cualquier persona que se involucre en las telecomunicaciones modernas.

El primer escenario es una simulación de un escenario que cualquier administrador de redes encuentra en la vida real, desde el momento mismo de la planeación de la red debe tener en cuenta todos los involucrados en las comunicaciones incluyendo equipos fuera de su administración y con protocolos distintos de enrutamiento, en este escenario se aplican posibles configuraciones que tienen en cuenta distintos factores de enrutamiento ya sea vector distancia o vector estado de enlace, también se tienen en cuenta las posibles re escalaciones de la red ya sea para ser mas grande o para reducir su tamaño.

Por otra parte, el segundo escenario aborda temas relacionados a la administración de redes en Switching, este simula la administración interna de una red corporativa, la cual cuenta con distintas VLANs y cada una con accesos específicos, esto aplicado a un escenario real es fundamental ya que a día de hoy la segmentación y restricción de los accesos en una red con muchos usuarios parte desde la misma forma en la que se encuentra la red, esto permite que usando el protocolo VTP esta administración se maneje de forma centralizada y que cualquier cambio no afecte a la red en su totalidad.

## DESARROLLO DE LOS ESCENARIOS

### PRIMER ESCENARIO

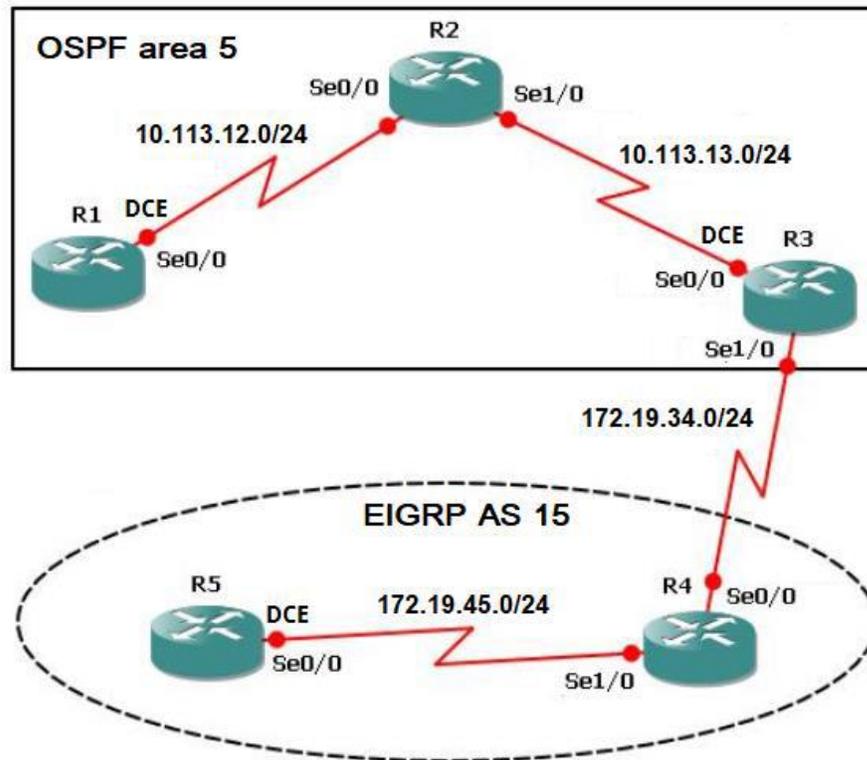


Figura 1 Topología primer escenario

## Montaje del escenario en GNS3

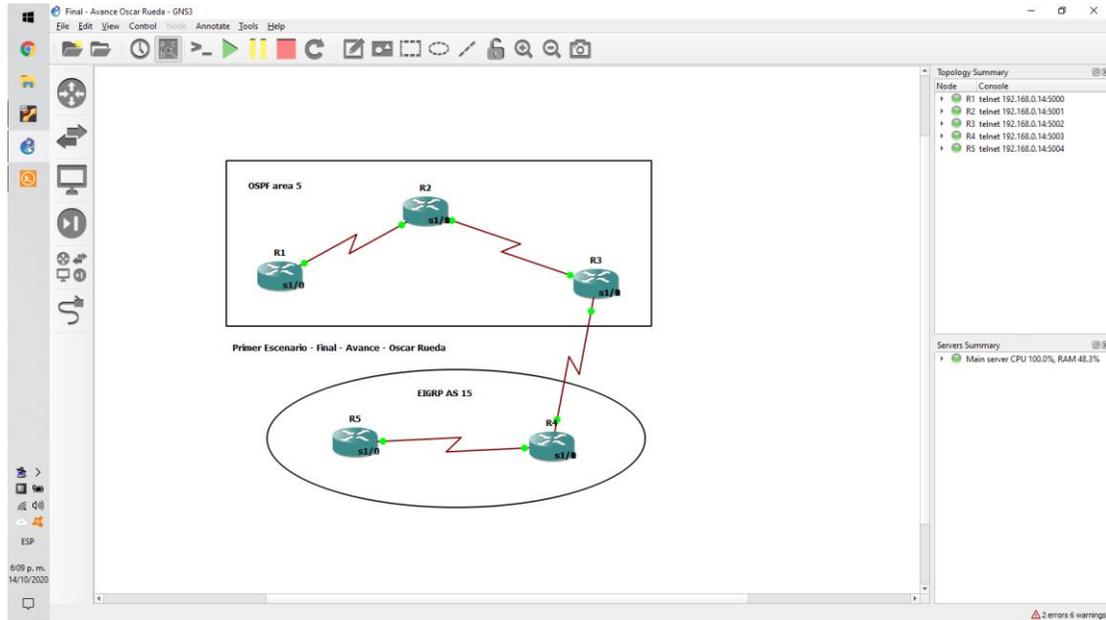


Figura 2 Primer escenario desarrollado en GNS3

1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

### Configuración en R1

```
(config)# interface Serial1/0
(config-if)# ip address 10.113.12.1 255.255.255.0
(config-if)# clock rate 64000
(config-if)# bandwidth 64
(config-if)# no shutdown
(config)# router ospf 1
(config-router)#network 10.113.12.0 0.0.0.255 area 5
```

## Configuración en R2

```
(config)# interface Serial1/0
(config-if)# ip address 10.113.12.2 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# interface Serial1/1
(config-if)# ip address 10.113.13.1 255.255.255.0
(config-if)# clock rate 64000
(config-if)# bandwidth 64
(config-if)# no shutdown
(config-if)# exit
(config)# router ospf 1
(config-router)#network 10.113.12.0 0.0.0.255 area 5
(config-router)#network 10.113.13.0 0.0.0.255 area 5
```

## Configuración en R3

```
(config)# interface Serial1/0
(config-if)# ip address 10.113.13.2 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# interface Serial1/1
(config-if)# ip address 172.19.34.1 255.255.255.0
(config-if)# clock rate 64000
(config-if)# bandwidth 64
(config-if)# no shutdown
(config-if)# exit
(config)# router ospf 1
(config-router)#network 10.113.13.0 0.0.0.255 area 5
(config-if)# exit
(config)#router eigrp 15
(config-router)#network 172.19.34.0 0.0.0.255
```

## Configuración en R4

```
(config)# interface Serial1/0
(config-if)# ip address 172.19.34.2 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# interface Serial1/1
(config-if)# ip address 172.19.45.1 255.255.255.0
(config-if)# clock rate 64000
(config-if)# bandwidth 64
(config-if)# no shutdown
(config-if)# exit
(config)#router eigrp 15
(config-router)#network 172.19.34.0 0.0.0.255
(config-router)#network 172.19.45.0 0.0.0.255
```

## Configuración en R5

```
(config)# interface Serial1/0
(config-if)# ip address 172.19.45.2 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)#router eigrp 15
(config-router)#network 172.19.45.0 0.0.0.255
```

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 5 de OSPF.

### Configuración en R1

```
(config)# interface Loopback1
(config-if)# ip address 10.1.10.1 255.255.252.0
(config-if)# exit
(config)# interface Loopback2
(config-if)# ip address 10.1.20.1 255.255.252.0
(config-if)# exit
(config)# interface Loopback3
(config-if)# ip address 10.1.30.1 255.255.252.0
(config-if)# exit
(config)# interface Loopback4
(config-if)# ip address 10.1.40.1 255.255.252.0
(config-if)# exit
(config)# router ospf 1
(config-router)# network 10.1.10.0 0.0.3.255 area 5
(config-router)# network 10.1.20.0 0.0.3.255 area 5
(config-router)# network 10.1.30.0 0.0.3.255 area 5
(config-router)# network 10.1.40.0 0.0.3.255 area 5
```

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 15.

Configuración en R5

```
(config)# interface Loopback1
(config-if)# ip address 172.5.10.1 255.255.255.0
(config-if)# exit
(config)# interface Loopback2
(config-if)# ip address 172.5.20.1 255.255.255.0
(config-if)# exit
(config)# interface Loopback3
(config-if)# ip address 172.5.30.1 255.255.255.0
(config-if)# exit
(config)# interface Loopback4
(config-if)# ip address 172.5.40.1 255.255.255.0
(config-if)# exit
(config)#router eigrp 15
(config-router)#network 172.5.0.0 0.0.255.255
```

4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando *show ip route*.

Resultado:

```
R3#show ip route
Codes: 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

Gateway of last resort is not set

D    172.5.0.0/16 [90/41152000] via 172.19.34.2, 00:12:11, Serial1/1
    172.19.0.0/24 is subnetted, 2 subnets
D    172.19.45.0 [90/41024000] via 172.19.34.2, 00:20:15, Serial1/1
C    172.19.34.0 is directly connected, Serial1/1
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O    10.1.10.1/32 [110/129] via 10.113.13.1, 00:01:51, Serial1/0
O    10.1.30.1/32 [110/129] via 10.113.13.1, 00:01:51, Serial1/0
O    10.1.20.1/32 [110/129] via 10.113.13.1, 00:01:51, Serial1/0
O    10.1.40.1/32 [110/129] via 10.113.13.1, 00:01:51, Serial1/0
C    10.113.13.0/24 is directly connected, Serial1/0
O    10.113.12.0/24 [110/128] via 10.113.13.1, 00:01:51, Serial1/0
R3#
```

Figura 3 Verificación tabla de enrutamiento en R3 primer escenario

En la tabla de enrutamiento en R3 se identifica como esta agrega las interfaces de loopback creadas en R1 y en R5

5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

### Configuración en R3

```
(config)# router ospf 1
(config-router)#redistribute eigrp 15 metric 50000 subnets
(config-router)#exit
(config)# router eigrp 15
(config-router)#redistribute ospf 1 metric 1544 20000 255 1
1500
```

6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando `show ip route`.

Resultado en R1

The screenshot shows a GNS3 interface with a network topology and a terminal window on router R1. The topology is divided into two areas: 'OSPF area 5' and 'EIGRP AS 15'. In 'OSPF area 5', routers R1, R2, and R3 are connected. R1 is connected to R2 via serial interface s1/0. R2 is connected to R3 via serial interface s1/0. In 'EIGRP AS 15', routers R4 and R5 are connected. R4 is connected to R5 via serial interface s1/0. R3 is also connected to R4 via serial interface s1/0. The terminal window on R1 shows the output of the 'show ip route' command, displaying the routing table for R1. The output includes the following information:

```
R1#show ip route
Codes: 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

Gateway of last resort is not set

O E2 172.5.0.0/16 [110/50000] via 10.113.12.2, 00:06:01, Serial1/0
O 172.19.0.0/24 is subnetted, 2 subnets
O E2 172.19.45.0 [110/50000] via 10.113.12.2, 00:06:01, Serial1/0
O E2 172.19.34.0 [110/50000] via 10.113.12.2, 00:06:01, Serial1/0
O 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.1.8.0/22 is directly connected, Loopback1
C 10.1.20.0/22 is directly connected, Loopback3
C 10.1.40.0/22 is directly connected, Loopback4
O 10.113.12.0/24 [110/3124] via 10.113.12.2, 00:24:34, Serial1/0
C 10.113.12.0/24 is directly connected, Serial1/0
R1#ping 172.5.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/80/88 ms
R1#
```

Figura 4 Verificación de tabla de enrutamiento en R1 primer escenario



## SEGUNDO ESCENARIO

Una empresa de comunicaciones presenta una estructura Core acorde a la topología de red, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, etherchannels, VLANs y demás aspectos que forman parte del escenario propuesto.

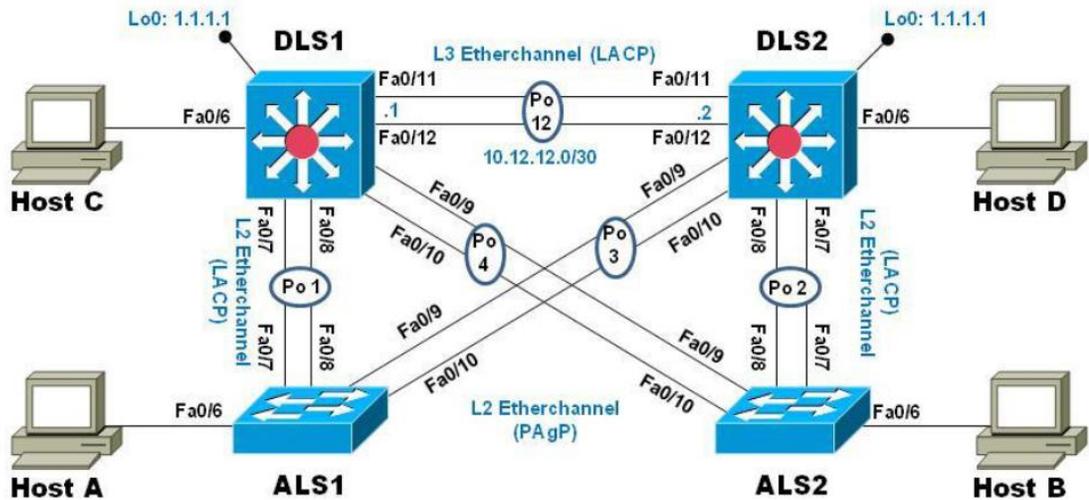


Figura 6 Topología segundo escenario

Parte 1: Configurar la red de acuerdo con las especificaciones.

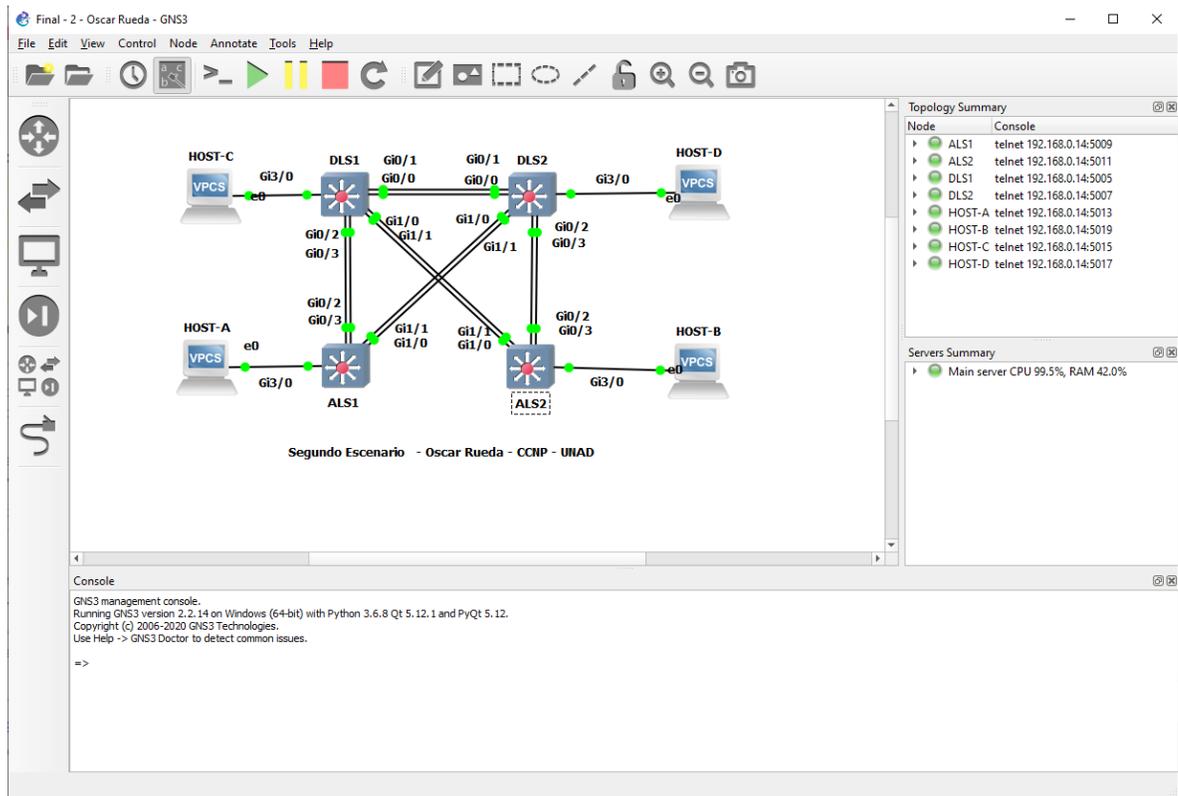


Figura 7 Segundo escenario desarrollado en GNS3

Para la simulación de la topología se usará la vios\_l2-adventerprisek9-m.03.2017, por lo tanto, los puertos cambiarán según la figura 7.

a. Apagar todas las interfaces en cada switch.

Configuración ejecutada en todos los switch

```
(config)# Interface range Gi0/0-3,Gi1/0-3,Gi2/0-3,Gi3/0-3
(config)# Shutdown
(config)# Exit
```

b. Asignar un nombre a cada switch acorde con el escenario establecido.

```
(config)# hostname (DLS1-DLS2-ALS1-ALS2)
(config)# Exit
```

c. Configurar los puertos troncales y Port-channels tal como se muestra en el diagrama.

1) La conexión entre DLS1 y DLS2 será un EtherChannel capa-3 utilizando LACP. Para DLS1 se utilizará la dirección IP 10.12.12.1/30 y para DLS2 utilizará 10.12.12.2/30.

#### Configuración en DLS1

```
(config)# interface range Gi0/0-1
(config-if)# channel-protocol lacp
(config-if)# channel-group 12 mode active
(config-if)# no shutdown
(config-if)# exit
(config)# interface port-channel 12
(config-if)# ip address 10.12.12.1 255.255.255.252
(config-if)# exit
```

#### Configuración en DLS2

```
(config)# interface range Gi0/0-1
(config-if)# channel-protocol lacp
(config-if)# channel-group 12 mode active
(config-if)# no shutdown
(config-if)# exit
(config)# interface port-channel 12
(config-if)# ip address 10.12.12.2 255.255.255.252
(config-if)# exit
```

2) Los Port-channels en las interfaces Fa0/7 y Fa0/8 utilizarán LACP.

## Configuración en DLS1

```
(config)# interface range Gi0/2-3
(config-if)# channel-protocol lacp
(config-if)# channel-group 1 mode active
(config-if)# no shutdown
(config-if)# exit
```

## Configuración en DLS2

```
(config)# interface range Gi0/2-3
(config-if)# channel-protocol lacp
(config-if)# channel-group 2 mode active
(config-if)# no shutdown
(config-if)# exit
```

## Configuración en ALS1

```
(config)# interface range Gi0/2-3
(config-if)# channel-protocol lacp
(config-if)# channel-group 1 mode active
(config-if)# no shutdown
(config-if)# exit
```

## Configuración en ALS2

```
(config)# interface range Gi0/2-3
(config-if)# channel-protocol lacp
(config-if)# channel-group 2 mode active
(config-if)# no shutdown
(config-if)# exit
```

3) Los Port-channels en las interfaces F0/9 y fa0/10 utilizará PAgP.

### Configuración en DLS1

```
(config)# interface range Gi1/0-1
(config-if)# channel-protocol pagp
(config-if)# channel-group 4 mode desirable
(config-if)# no shutdown
(config-if)# exit
```

### Configuración en ALS2

```
(config)# interface range Gi1/0-1
(config-if)# channel-protocol pagp
(config-if)# channel-group 4 mode desirable
(config-if)# no shutdown
(config-if)# exit
```

### Configuración en DLS2

```
(config)# interface range Gi1/0-1
(config-if)# channel-protocol pagp
(config-if)# channel-group 3 mode desirable
(config-if)# no shutdown
(config-if)# exit
```

### Configuración en ALS1

```
(config)# interface range Gi1/0-1
(config-if)# channel-protocol pagp
(config-if)# channel-group 3 mode desirable
(config-if)# no shutdown
(config-if)# exit
```

4) Todos los puertos troncales serán asignados a la VLAN 500 como la VLAN nativa.

### Configuración en DLS1

```
(config)#vlan 500
(config-vlan)#name NATIVA
(config-vlan)#exit
(config)#interface range port-channel 1, por 4, por 12
(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport trunk native vlan 500
(config-if)#switchport mode trunk
(config-if)#no shutdown
(config-if)#exit
```

### Configuración en DLS2

```
(config)#vlan 500
(config-vlan)#name NATIVA
(config-vlan)#exit
(config)#interface range port-channel 2, por 3, por 12
(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport trunk native vlan 500
(config-if)#switchport mode trunk
(config-if)#no shutdown
(config-if)#exit
```

### Configuración en ALS1

```
(config)#interface range Po1, Po3
(config-if)#switchport trunk native vlan 500
(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport mode trunk
(config-if)#no shutdown
(config-if)#exit
```

## Configuración en ALS2

```
(config)#interface range Po2, Po4
(config-if)#switchport trunk native vlan 500
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
(config-if)# no shutdown
(config-if)#exit
```

### d. Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 3

- 1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321
- 2) Configurar DLS1 como servidor principal para las VLAN.
- 3) Configurar ALS1 y ALS2 como clientes VTP.

Para este numeral se usará la versión 2 de VTP ya que el simulador GNS3 no lo permite

## Configuración en DLS1

```
(config)# vtp domain CISCO
(config)#vtp password ccnp321
(config)#vtp version 2
(config)#vtp mode server
```

## Configuración en ALS1

```
(config)# vtp domain CISCO
(config)#vtp password ccnp321
(config)#vtp version 2
(config)#vtp mode client
```

## Configuración en ALS2

```
(config)# vtp domain CISCO
(config)#vtp password ccnp321
(config)#vtp version 2
(config)#vtp mode client
```

e. Configurar en el servidor principal las siguientes VLAN:

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
500	NATIVA	434	PROVEEDORES
12	ADMON	123	SEGUROS
234	CLIENTES	1010	VENTAS
1111	MULTIMEDIA	3456	PERSONAL

*Tabla 1. listado de VPN Segundo Escenario*

### Configuración en DLS1

```
(config)#vlan 500
(config-vlan)#name NATIVA
(config-vlan)#exit
(config)#vlan 12
(config-vlan)#name ADMON
(config-vlan)#exit
(config)#vlan 234
(config-vlan)#name CLIENTES
(config-vlan)#exit
(config)#vlan 1111
(config-vlan)#name MULTIMEDIA
(config-vlan)#exit
(config)#vlan 434
(config-vlan)#name PROVEEDORES
(config-vlan)#exit
(config)#vlan 123
(config-vlan)#name SEGUROS
(config-vlan)#exit
(config)#vlan 1010
(config-vlan)#name VENTAS
(config-vlan)#exit
(config)#vlan 3456
(config-vlan)#name PERSONAL
(config-vlan)#exit
```

f. En DLS1, suspender la VLAN 434.

#### Configuración en DLS1

```
(config)#vlan 434
(config-vlan)# state suspend
(config-vlan)#exit
```

g. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión 2, y configurar en DLS2 las mismas VLAN que en DLS1.

#### Configuración en DLS2

```
(config)# vtp domain CISCO
(config)#vtp password ccnp321
(config)#vtp version 2
(config)#vtp mode transparent
(config)#vlan 12
(config-vlan)#name ADMON
(config-vlan)#exit
(config)#vlan 234
(config-vlan)#name CLIENTES
(config-vlan)#exit
(config)#vlan 1111
(config-vlan)#name MULTIMEDIA
(config-vlan)#exit
(config)#vlan 434
(config-vlan)#name PROVEEDORES
(config-vlan)#exit
(config)#vlan 123
(config-vlan)#name SEGUROS
(config-vlan)#exit
(config)#vlan 1010
(config-vlan)#name VENTAS
(config-vlan)#exit
(config)#vlan 3456
(config-vlan)#name PERSONAL
(config-vlan)#exit
```

h. Suspende VLAN 434 en DLS2.

#### Configuración en DLS2

```
(config)#vlan 434
(config-vlan)# state suspend
(config-vlan)#exit
```

i. En DLS2, crear VLAN 567 con el nombre de PRODUCCION. La VLAN de PRODUCCION no podrá estar disponible en cualquier otro Switch de la red.

#### Configuración en DLS2

```
(config)#vlan 567
(config-vlan)#name PRODUCCION
(config-vlan)#exit
(config)#interface range port-channel 2, por 3
(config-if)#switchport trunk allowed vlan except 567
(config-if)#exit
```

j. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 500, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.

#### Configuración en DLS1

```
(config)#spanning-tree vlan 1,12,434,500,1010,1111,3456
root primary
(config)#spanning-tree vlan 123,234 root secondary
```

k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 500, 1010, 1111 y 3456.

## Configuración en DLS2

```
(config)#spanning-tree vlan 123,234 root primary
(config)#spanning-tree vlan 12,434,500,1010,1111,3456 root
secondary
```

l. Configurar todos los puertos como troncales de tal forma que solamente las VLAN que se han creado se les permitirá circular a través de estos puertos.

## Configuración ejecutada en el paso C - 3

m. Configurar las siguientes interfaces como puertos de acceso, asignados a las VLAN de la siguiente manera:

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3456	12, 1010	123, 1010	234
Interfaz Fa0/15	1111	1111	1111	1111
Interfaces F0 /16-18		567		

*Tabla 2 Interfaces específicas de VLAN segundo escenario*

## Configuración en DLS1

```
(config)#interface Gi3/0
(config-if)#switchport mode access
(config-if)#switchport access vlan 3456
(config-if)#no shutdown
end(config-if)#exit
(config)#interface Gi3/1
(config-if)#switchport mode access
(config-if)#switchport access vlan 1111
(config-if)#no shutdown
(config-if)#exit
```

## Configuración en DLS2

```
(config)#interface Gi3/0
(config-if)#switchport mode access
(config-if)#switchport access vlan 12
(config-if)#switchport access vlan 1010
(config-if)#no shutdown
(config-if)#exit
(config)#interface Gi3/1
(config-if)#switchport mode access
(config-if)#switchport access vlan 1111
(config-if)#no shutdown
(config-if)#exit
(config)#interface range Gi2/03-3
(config-if)#switchport mode access
(config-if)#switchport access vlan 567
(config-if)#no shutdown
(config-if)#exit
```

## Configuración en ALS1

```
(config)#interface Gi3/0
(config-if)#switchport mode access
(config-if)#switchport access vlan 123
(config-if)#switchport access vlan no sh 1010
(config-if)#no shutdown
(config-if)#exit
(config)#interface Gi3/1
(config-if)#switchport mode access
(config-if)#switchport access vlan 1111
(config-if)#no shutdown
(config-if)#exit
```

## Configuración en ALS2

```
(config)#interface Gi3/0
(config-if)#switchport mode access
(config-if)#switchport access vlan 234
(config-if)#no shutdown
(config-if)#exit
(config)#interface Gi3/1
(config-if)#switchport mode access
(config-if)#switchport access vlan 1111
(config-if)#no shutdown
exit(config-if)#exit
```

Parte 2: conectividad de red de prueba y las opciones configuradas.

a. Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso

## DLS1

```
DLS1>show vlan brief
DLS1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Gi0/0, Gi0/1, Gi1/2, Gi1/3
                                           Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                           Gi3/2, Gi3/3
12   ADMON                   active
123  SEGUROS                 active
234  CLIENTES                active
345  VLAN0345                active
434  PROVEEDORES             suspended
500  NATIVA                  active
1002 fddi-default           act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default       act/unsup
1005 trbrf-default        act/unsup
1010 VENTAS                active
1111 MULTIMEDIA            active    Gi3/1
3456 PERSONAL             active    Gi3/0
DLS1#
```

Figura 8 Verificación de VLAN en DLS1 segundo escenario

## DLS2

```
DLS2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi0/1, Gi1/2, Gi1/3 Gi2/0, Gi2/1, Gi2/2, Gi3/2 Gi3/3
12	ADMON	active	
123	SEGUROS	active	
234	CLIENTES	active	
434	PROVEEDORES	suspended	
500	NATIVA	active	
567	PRODUCCION	active	Gi2/3
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	
1010	VENTAS	active	Gi3/0
1111	MULTIMEDIA	active	Gi3/1
3456	PERSONAL	active	

```
DLS2#
```

Figura 9 Verificación de VLAN en DLS2 segundo escenario

## ALS1

```
ALS1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi0/1, Gi1/2, Gi1/3 Gi2/0, Gi2/1, Gi2/2, Gi2/3 Gi3/2, Gi3/3
12	ADMON	active	
123	SEGUROS	active	
234	CLIENTES	active	
345	VLAN0345	active	
434	PROVEEDORES	suspended	
500	NATIVA	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

```
ALS1#  
ALS1#
```

Figura 10 Verificación de VLAN en ALS1 segundo escenario

## ALS2

```
ALS2#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Gi0/0, Gi0/1, Gi1/2, Gi1/3
                    Gi2/0, Gi2/1, Gi2/2, Gi2/3
                    Gi3/2, Gi3/3
12   ADMON                  active
123  SEGUROS                 active
234  CLIENTES                active    Gi3/0
345  VLAN0345                active
434  PROVEEDORES             suspended
500  NATIVA                  active
1002 fddi-default           act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default       act/unsup
1005 trbrf-default         act/unsup
ALS2#
```

Figura 11 Verificación de VLAN en ALS2 segundo escenario

b. Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente

## DLS1

```
DLS1#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: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----
1      Po1(SU)        LACP        Gi0/2(P)   Gi0/3(P)
4      Po4(SU)        PAgP        Gi1/0(P)   Gi1/1(P)
12     Po12(SD)       -
```

Figura 12 Verificación de EtherChannel en DLS1 segundo escenario

## DLS2

```
DLS2#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: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
 2     Po2(SU)       LACP       Gi0/2(P)   Gi0/3(P)
 3     Po3(SU)       PAgP       Gi1/0(P)   Gi1/1(P)
12     Po12(SD)      -
DLS2#
```

Figura 13 Verificación de EtherChannel en DLS2 segundo escenario

c. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN.

### DLS1

```
DLS1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0012, VLAN0345, VLAN0500, VLAN1010, VLAN1111
VLAN3456
Extended system ID           is enabled
Portfast Default             is disabled
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default           is disabled
PVST Simulation Default      is enabled but inactive in pvst mode
Bridge Assurance             is enabled but inactive in pvst mode
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast                   is disabled
BackboneFast                 is disabled
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	4	4
VLAN0012	0	0	0	2	2
VLAN0123	1	0	0	1	2
VLAN0234	1	0	0	1	2
VLAN0345	0	0	0	2	2
VLAN0500	0	0	0	2	2
VLAN1010	0	0	0	2	2
VLAN1111	0	0	0	3	3
VLAN3456	0	0	0	3	3
9 vlans	2	0	0	20	22

```
DLS1#
```

Figura 14 Verificación de Spanning tree en DLS1 segundo escenario

## DLS2

```
DLS2#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0123, VLAN0234, VLAN0500, VLAN0567, VLAN1010
VLAN1111, VLAN3456
Extended system ID          is enabled
Portfast Default            is disabled
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default          is disabled
PVST Simulation Default     is enabled but inactive in pvst mode
Bridge Assurance            is enabled but inactive in pvst mode
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast                  is disabled
BackboneFast                is disabled

Name                          Blocking Listening Learning Forwarding STP Active
-----
VLAN0001                       2           0           0           0           2
VLAN0012                       1           0           0           1           2
VLAN0123                       0           0           0           2           2
VLAN0234                       0           0           0           2           2
VLAN0500                       2           0           0           0           2
VLAN0567                       0           0           0           1           1
VLAN1010                       0           0           0           3           3
VLAN1111                       0           0           0           3           3
VLAN3456                       0           0           0           2           2
-----
9 vlans                        5           0           0          14          19
DLS2#
```

Figura 15 Verificación de Spanning tree en DLS2 segundo escenario

## CONCLUSIONES

Durante el desarrollo del primer escenario se evidencia el uso de 2 de los protocolos de enrutamiento más usados en la actualidad OSPF y EIGRP, evidenciando el apropiamiento teórico y práctico de los temas vistos hasta el momento en el diplomado CCNP.

EIGRP como protocolo de enrutamiento propietario de Cisco cuenta con constantes actualizaciones y distintas versiones del mismo, esto permite que, aunque se requiera comunicación con distintas marcas este protocolo puede negociar con otros sin llegar a crear problemas de compatibilidad, esto hace que el conocimiento a detalles de este protocolo, uno de los más usados sea indispensable para cualquier administrador de redes.

El segundo escenario del diplomado CCNP es a mi forma de ver un paso fundamental para cualquier profesional que trabaje en las áreas de las telecomunicaciones, para el caso específico de Switching se aprende desde la teoría aplicada a escenarios reales los cuales afianzan y apropian los conocimientos vistos durante todo el diplomado.

La aplicación del protocolo VTP su funcionamiento y sus distintos modos de uso son fundamentales para evitar la redundancia que puede resultar en errores humanos de configuración, la práctica en la implementación del VTP permite conocer y planear de forma adecuada los posibles retos que se presenten administrando una red con distintas VLANs, el desarrollo de este escenario cumple a detalle este requerimiento.

Cisco como líder mundial en equipos de telecomunicaciones tiene un valor añadido a todos sus servicios con este tipo de cursos, esto permite que existan innumerables comunidades de ingenieros y personas que conocen el funcionamiento de un sinnúmero de equipos de comunicaciones.

## BIBLIOGRAFÍA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Normas ICONTEC 2018 para crear trabajos escritos - Tutorial. (2018). Recuperado de <https://colombiaconsulta.com/normas-icontec/>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>