

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

DAVID ESTEBAN NIÑO GUERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRÓNICA  
BOGOTÁ D.C.  
2021

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

DAVID ESTEBAN NIÑO GUERRA

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

DIRECTOR:  
ING. DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRÓNICA  
BOGOTÁ D.C.  
2021

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

\_\_\_\_\_  
Firma del Presidente del Jurado

\_\_\_\_\_  
Firma del Jurado

\_\_\_\_\_  
Firma del Jurado

Bogotá D.C, 18 de julio de 2021

## **AGRADECIMIENTOS**

Agradezco inicialmente a Dios que me permite despertar cada día lleno de vida, energía y anhelos en mi corazón, a mi madre Martha Lucia Niño Guerra, quien ayudo a forjar mi carácter, mis ganas de salir adelante y sobre todo quien me heredó su espíritu de superación.

Agradezco a la Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI), de la Universidad Nacional Abierta y a Distancia (UNAD), por permitirme ser parte de la familia Unadista y de esta manera cumplir unos de mis sueños, que es el ser profesional.

Finalmente agradezco a mis amigos más cercanos quienes me han acompañado a lo largo de mi carrera universitaria y hoy están felices con mis logros. Infinitas gracias a todos.

## TABLA DE CONTENIDO

INTRODUCCIÓN .....	10
1. ESCENARIO 1 .....	11
2. ESCENARIO 2 .....	19
ANEXOS.....	39
CONCLUSIONES .....	40
BIBLIOGRAFÍA.....	41

## LISTA DE TABLAS

Tabla 1. Interfaces de Loopback en R1 .....	13
Tabla 2. Interfaces de Loopback en R5 .....	14
Tabla 3. VLAN servidor principal.....	25
Tabla 4. Interfaces VLAN.....	31

## LISTA DE FIGURAS

Figura 1. Escenario 1 .....	11
Figura 2. Escenario 1 en Packet Tracer.....	11
Figura 3. Interfaces Loopbacks en R3. ....	15
Figura 4. Tabla de enrutamiento en R1. ....	16
Figura 5. Tabla de enrutamiento en R5. ....	17
Figura 6. Traceroute R1.....	18
Figura 7. Ping desde R1 a todos los routers.....	18
Figura 8. Escenario 2.....	19
Figura 9. Escenario 2 Packet Tracer.....	19
Figura 10. VLAN configuradas en DLS1. ....	26
Figura 11. VLAN configuradas en DLS2. ....	28
Figura 12. VLAN en switch DLS1.....	33
Figura 13. VLAN en switch DLS2.....	33
Figura 14. Show interfaces en switch DLS1. ....	34
Figura 15. Show interfaces en switch DLS2. ....	34
Figura 16. Show interfaces trunk en switch DLS1.....	35
Figura 17. Show interfaces trunk en switch DLS2.....	35
Figura 18. EtherChannel en DLS1.....	36
Figura 19. EtherChannel en ALS1. ....	36
Figura 20. Spanning tree en DLS1.....	37
Figura 21. Spanning tree en DLS2.....	37
Figura 22. Ping y traceroute DLS1.....	38
Figura 23. Ping y traceroute DLS2.....	38

## GLOSARIO

**DHCP:** el protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes.

**DNS:** el sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

**EIGRP:** es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco System, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace

**HSRP:** (Hot Stand-by Redundancy Protocol) es un protocolo propietario de Cisco que está diseñado para asegurar la redundancia (o failover) entre dos o más dispositivos Cisco.

**SPANNING TREE PROTOCOL (STP):** es un protocolo de capa 2 que se ejecuta en bridges y switches. La especificación para STP es IEEE 802.1D. El propósito principal de STP es garantizar que usted no cree loops cuando tenga trayectorias redundantes en su red.

**VLAN:** Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

**VTP:** VLAN Trunking Protocol. VTP son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco.

## RESUMEN

La CCNP (Cisco Certified Network Professional) valida la capacidad de planificar, implementar, verificar y solucionar problemas en redes empresariales LAN y WAN, así como trabajar de manera conjunta con especialistas de soluciones de: seguridad, voz, inalámbricas y video. Este curso es apropiado para aquellos que tienen al menos un año de experiencia en redes y están dispuestos a avanzar en sus habilidades y trabajar en forma soluciones de red complejas.

El diplomado está constituido por dos módulos: CCNP ROUTE y CCNP SWITCH, En el módulo CCNP ROUTE se abordarán conceptos principales como protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, entre otros, así como nuevos e interesantes temas, como Dynamic Multi VPN, VRF Lite y protocolos en IPv6. En el módulo CCNP SWITCH se abordarán conceptos principales como operaciones y puertos de switches, VLANs y troncales, Spanning Tree, entre otros, así como nuevos e interesantes temas, como manejo de ataques de spoofing y configuración de usuarios.

El objeto de este documento, consiste fundamentalmente en la aplicación de los conocimientos adquiridos en el campo profesional de las Redes demostrando amplia habilidad, capacidad de planificación, implementación y verificación de soluciones de redes complejas.

**Palabras claves:** CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## ABSTRACT

The CCNP (Cisco Certified Network Professional) validates the ability to plan, implement, verify and troubleshoot enterprise LAN and WAN networks, as well as work closely with security, voice, wireless and video solution specialists. This course is suitable for those who have at least one year of networking experience and are willing to advance their skills and work on complex network solutions.

The diploma course is made up of two modules: CCNP ROUTE and CCNP SWITCH. In the CCNP ROUTE module, main concepts such as EIGRP routing protocols, OSPF, BGP, route redistribution, among others, as well as new and interesting topics such as Dynamic Multi VPN, VRF Lite and IPv6 protocols will be addressed. The CCNP SWITCH module will cover main concepts such as switch operations and ports, VLANs and trunks, Spanning Tree, among others, as well as new and interesting topics such as handling spoofing attacks and user configuration.

The purpose of this document is basically to apply the knowledge acquired in the professional field of Networks, demonstrating a wide range of skills, planning, implementation and verification of complex network solutions.

**Keywords:** CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

Su objeto principal es demostrar los conocimientos adquiridos en el uso de comandos IOS, configuración de Routers, uso de protocolos de enrutamiento, direccionamiento, diseño e implementación de soluciones prácticas en ambientes LAN y WAN, para esto se emplean la herramienta de simulación y laboratorio GNS3 y Packet Tracer, el cual permite configurar los escenarios propuestos y analizar su comportamiento, identificar situaciones y resolver problemas.

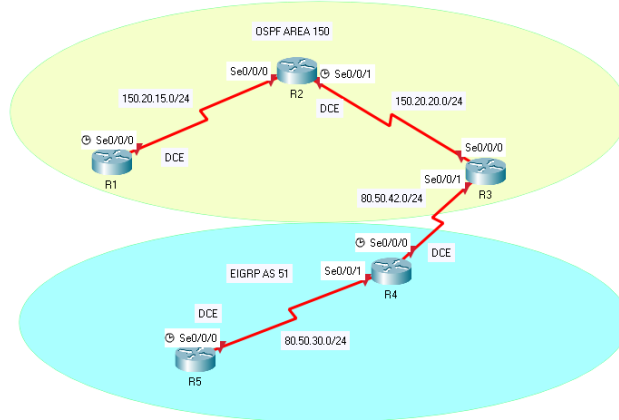
Durante esta actividad practica se desarrollaron dos escenarios (Uno con router y uno con switch) que permitían la configuración de diversos escenarios trabajados durante el diplomado, entre estos se encuentran las configuraciones básicas para ambos dispositivos (asignación de nombres, cableado, asignación de IP tanto IPv4 como IPv6, entre otros) así como la configuración de protocolos como Ethernet, OSPF, EIGRP, VTP, entre otras.

En el primer escenario, se tratan los contenidos del Módulo CCNP ROUTE CISCO, evidenciando el aprendizaje en los temas de principios básicos de Red, protocolos de enrutamiento IPv4 e IPv6, enrutamiento Gateway, EIGRP, OSPF y BGP;

En el segundo escenario, se estudian los temas del módulo CCNP SWITCH CISCO, el cual apropia temáticas relacionadas con la implementación, conmutación en una arquitectura de Red, redes VLAN's, disponibilidad y redundancia de Switches de capa 2 y capa 3 y características de redes LAN y WAN.

# 1. ESCENARIO 1

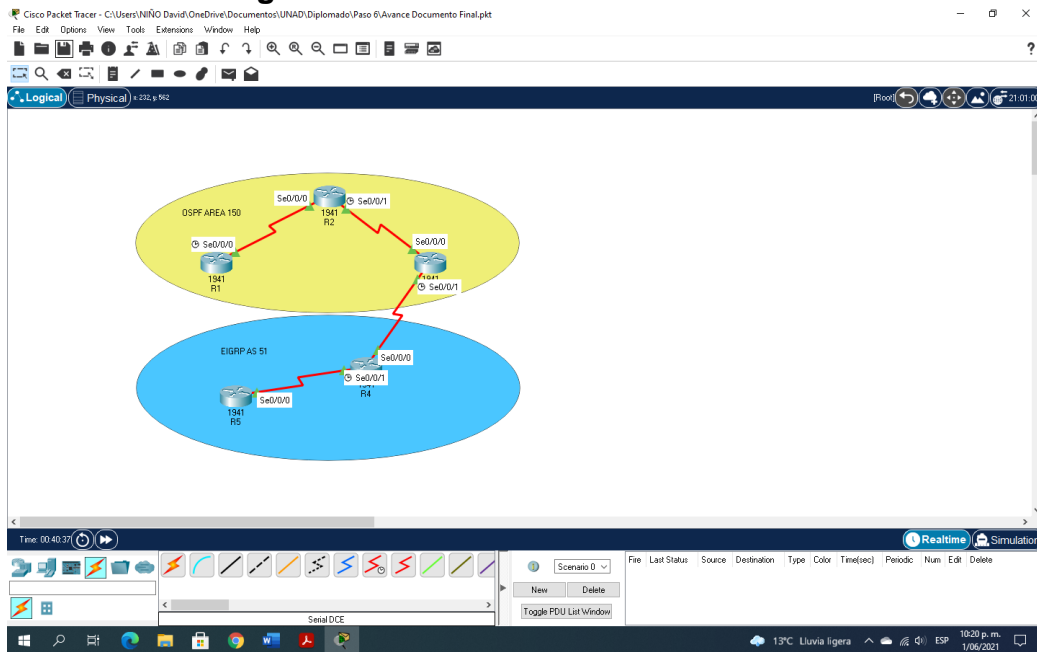
Figura 1. Escenario 1



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.

Para el desarrollo del presente informe, se trabajará en el software Cisco Packet Tracer.

Figura 2. Escenario 1 en Packet Tracer.



Fuente: Autor. Escenario 1 en Packet Tracer. [Imagen]. Diplomado CCNP. Bogotá: 2021.

## R1

```
Router>enable //Cambia a modo privilegiado
Router#config terminal //Cambia a modo Configuración
Router(config)#hostname R1 //Asignación hostname
R1(config)#interface s0/0/0 //Seleccionar interface
R1(config-if)#bandwidth 128000
R1(config-if)#ip address 150.20.15.1 255.255.255.0 //Asignar IP y mascara
R1(config-if)#no shutdown //Habilitar interface
R1(config-if)#exit
R1(config)#router ospf 1 //Habilitar modo OSPF
R1(config-router)#network 150.20.15.0 0.0.0.255 area 150 //Asignar red y área
```

## R2

```
Router>enable //Cambia a modo privilegiado
Router#config terminal //Cambia a modo Configuración
Router(config)#hostname R2 //Asignación hostname
R2(config)#interface S0/0/0 //Seleccionar interface
R2(config-if)#ip address 150.20.15.2 255.255.255.0 //Asignar IP y mascara
R2(config-if)#no shutdown //Habilitar interface
R2(config-if)#exit
R2(config)#interface S0/0/1 //Seleccionar interface
R2(config-if)#ip address 150.20.20.1 255.255.255.0 //Asignar IP y mascara
R2(config-if)#no shutdown //Habilitar interface
R2(config-if)#exit
R2(config)#router ospf 1 //Habilitar modo OSPF
R2(config-router)#network 150.20.15.0 0.0.0.255 area 150 //Asignar red y área
R2(config-router)#network 150.20.20.0 0.0.0.255 area 150 //Asignar red y área
R2(config-router)#exit
```

## R3

```
Router>enable //Cambia a modo privilegiado
Router#config terminal //Cambia a modo Configuración
Router(config)#hostname R3 //Asignación hostname
R3(config)#interface S0/0/1 //Seleccionar interface
R3(config-if)#bandwidth 128000
R3(config-if)#ip address 80.50.42.1 255.255.255.0 //Asignar IP y mascara
R3(config-if)#no shutdown //Habilitar interface
R3(config-if)#exit
R3(config)#interface S0/0/0 //Seleccionar interface
R3(config-if)#ip address 150.20.20.2 255.255.255.0 //Asignar IP y mascara
R3(config-if)#no shutdown //Habilitar interface
R3(config-if)#exit
```

```

R3(config)#router ospf 1 //Habilitar modo OSPF
R3(config-router)#network 150.20.20.0 0.0.0.255 area 150 //Asignar red y área
R3(config-router)#exit
R3(config)#router eigrp 51 //Habilitar modo EIGRP
R3(config-router)#network 80.50.42.0 0.0.0.255 //Asignar red y área

```

#### R4

```

Router>enable //Cambia a modo privilegiado
Router#config terminal //Cambia a modo Configuración
Router(config)#hostname R4 //Asignación hostname
R4(config)#interface S0/0/0 //Seleccionar interface
R4(config-if)#ip address 80.50.42.2 255.255.255.0 //Asignar IP y mascara
R4(config-if)#no shutdown //Habilitar interface
R4(config-if)#interface S0/0/1 //Seleccionar interface
R4(config-if)#ip address 80.50.30.1 255.255.255.0 //Asignar IP y mascara
R4(config-if)#no shutdown //Habilitar interface
R4(config-if)#exit
R4(config)#router eigrp 51 //Habilitar modo EIGRP
R4(config-router)#network 80.50.42.0 0.0.0.255 //Asignar red y área
R4(config-router)#network 80.50.30.0 0.0.0.255 //Asignar red y área

```

#### R5

```

Router>enable //Cambia a modo privilegiado
Router#config terminal //Cambia a modo Configuración
Router(config)#hostname R5 //Asignación hostname
R5(config)#interface S0/0/0 //Seleccionar interface
R5(config-if)#bandwidth 128000
R5(config-if)#ip address 80.50.30.2 255.255.255.0 //Asignar IP y mascara
R5(config-if)#no shutdown //Habilitar interface
R5(config-if)#exit
R5(config)#router eigrp 51 //Habilitar modo EIGRP
R5(config-router)#network 80.50.30.0 0.0.0.255 //Asignar red y área

```

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 20.1.0.0/22 y configure esas interfaces para participar en el área 150 de OSPF.

Router	Loopback	IP
R1	Loopback 0	20.1.0.10
	Loopback 1	20.1.1.10
	Loopback 2	20.1.2.10
	Loopback 3	20.1.3.10

Tabla 1. Interfaces de Loopback en R1

```

R1(config)#interface Loopback 0 // Ingresa a interface Loopback
R1(config-if)#ip address 20.1.0.10 255.255.255.0 //Asigna IP y mascara
R1(config-if)#exit
R1(config)#interface Loopback 1 // Ingresa a interface Loopback
R1(config-if)#ip address 20.1.1.10 255.255.255.0 //Asigna IP y mascara
R1(config-if)#exit
R1(config)#interface Loopback 2 // Ingresa a interface Loopback
R1(config-if)#ip address 20.1.2.10 255.255.255.0 //Asigna IP y mascara
R1(config-if)#exit
R1(config)#interface Loopback 3 // Ingresa a interface Loopback
R1(config-if)#ip address 20.1.3.10 255.255.255.0 //Asigna IP y mascara
R1(config-if)#exit
R1(config)#router ospf 1 //Habilitar modo OSPF
R1(config-router)#network 20.1.0.0 0.0.0.255 area 150 //Asigna Red, mascara y
area
R1(config-router)#network 20.1.1.0 0.0.0.255 area 150 //Asigna Red, mascara y
area
R1(config-router)#network 20.1.2.0 0.0.0.255 area 150 //Asigna Red, mascara y
area
R1(config-router)#network 20.1.3.0 0.0.0.255 area 150 //Asigna Red, mascara y
area

```

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 180.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 51.

Router	Loopback	IP
R5	Loopback 0	180.5.0.10
	Loopback 1	180.5.1.10
	Loopback 2	180.5.2.10
	Loopback 3	180.5.3.10

Tabla 2. Interfaces de Loopback en R5

```

R5(config)#interface Loopback 0 // Ingresa a interface Loopback
R5(config-if)#ip address 180.5.0.10 255.255.255.0 //Asigna IP y mascara
R5(config-if)#exit
R5(config)#interface Loopback 1 // Ingresa a interface Loopback
R5(config-if)#ip address 180.5.1.10 255.255.255.0 //Asigna IP y mascara
R5(config-if)#exit
R5(config)#interface Loopback 2 // Ingresa a interface Loopback
R5(config-if)#ip address 180.5.2.10 255.255.255.0 //Asigna IP y mascara
R5(config-if)#exit
R5(config)#interface Loopback 3 // Ingresa a interface Loopback
R5(config-if)#ip address 180.5.3.10 255.255.255.0 //Asigna IP y mascara

```

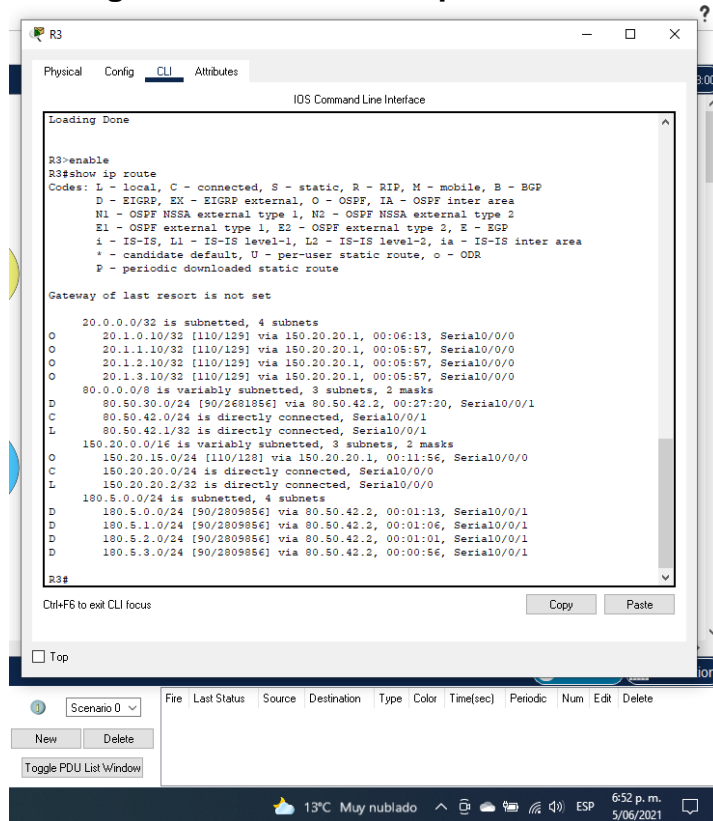
```

R5(config-if)#exit
R5(config)#router eigrp 51 //Habilitar modo EIGRP
R5(config-router)#network 180.5.0.0 0.0.0.255 //Asigna IP y mascara
R5(config-router)#network 180.5.1.0 0.0.0.255 //Asigna IP y mascara
R5(config-router)#network 180.5.2.0 0.0.0.255 //Asigna IP y mascara
R5(config-router)#network 180.5.3.0 0.0.0.255 //Asigna IP y mascara
R5(config-router)#

```

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**.

**Figura 3. Interfaces Loopbacks en R3.**



**Fuente:** Autor. Interfaces Loopbacks en R3. [Imagen]. Diplomado CCNP. Bogotá: 2021.

En la tabla de enrutamiento del R3, se evidencia que aprendió las nuevas interfaces de Loopback de R1 y R5.

5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 80000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

```

R3(config)#router ospf 1 //Habilitar modo OSPF
R3(config-router)#redistribute eigrp 51 metric 80000 subnets //Redistribución
recíproca
R3(config-router)#exit
R3(config)#router eigrp 51 //Habilitar modo EIGRP
R3(config-router)#redistribute ospf 1 metric 1544 20000 255 1 1500
//Redistribucion y selección de costos, rutas OSPF en EIGRP, ancho de banda y
retardo

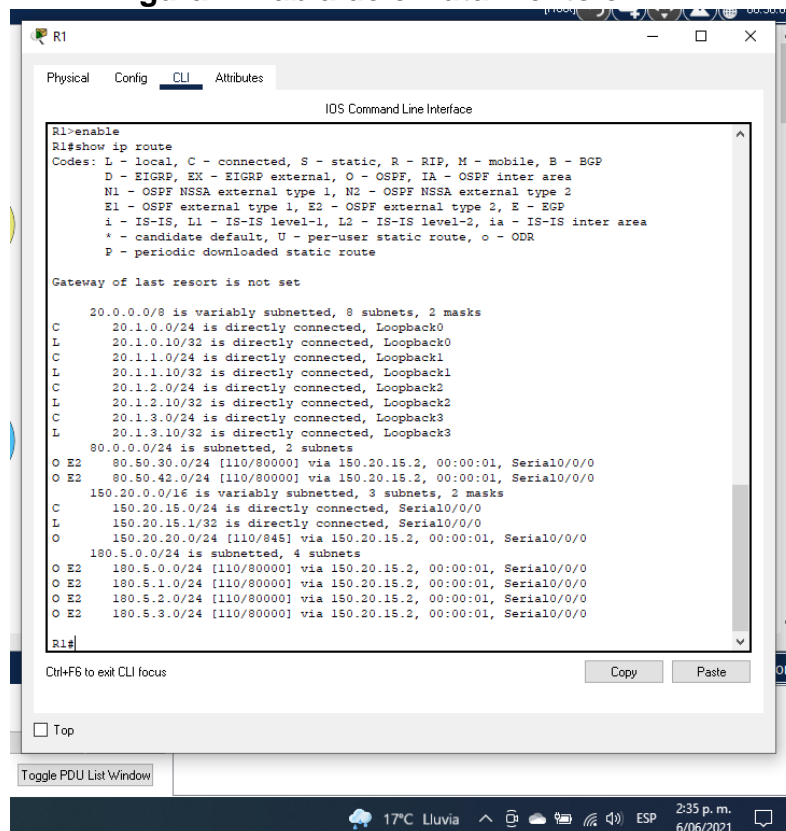
```

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**.

Con la ejecución del comando, se puede evidenciar que las rutas de R5 existen en la tabla de enrutamiento de R1 y las rutas de R1 existen en la tabla de enrutamiento de R5.

**En R1**

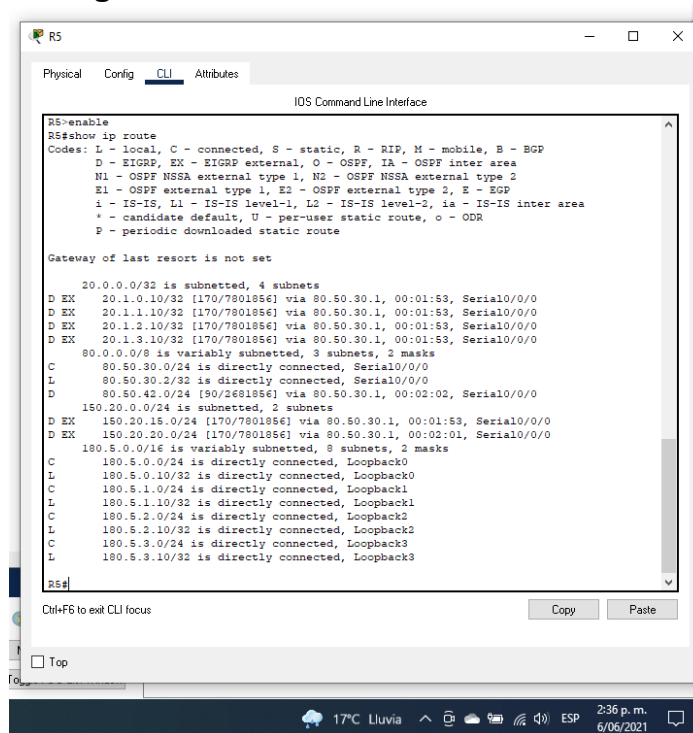
**Figura 4. Tabla de enrutamiento en R1.**



**Fuente:** Autor. Tabla de enrutamiento en R1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

En R5

Figura 5. Tabla de enrutamiento en R5.



```
R5>enable
R5#show ip route
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, E - EGP
       i - IS-IS, 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

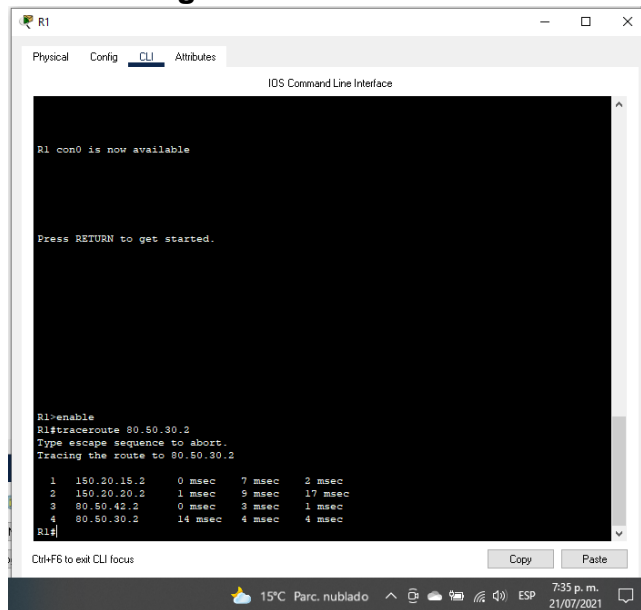
20.0.0.0/32 is subnetted, 4 subnets
D EX 20.1.0.10/32 [170/7801856] via 80.50.30.1, 00:01:53, Serial0/0/0
D EX 20.1.1.10/32 [170/7801856] via 80.50.30.1, 00:01:53, Serial0/0/0
D EX 20.1.2.10/32 [170/7801856] via 80.50.30.1, 00:01:53, Serial0/0/0
D EX 20.1.3.10/32 [170/7801856] via 80.50.30.1, 00:01:53, Serial0/0/0
80.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    80.50.30.0/24 is directly connected, Serial0/0/0
L    80.50.30.2/32 is directly connected, Serial0/0/0
D    80.50.42.0/24 [90/2681856] via 80.50.30.1, 00:02:02, Serial0/0/0
150.20.0.0/24 is subnetted, 2 subnets
D EX 150.20.15.0/24 [170/7801856] via 80.50.30.1, 00:01:53, Serial0/0/0
D EX 150.20.20.0/24 [170/7801856] via 80.50.30.1, 00:02:01, Serial0/0/0
180.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C    180.5.0.0/24 is directly connected, Loopback0
L    180.5.0.10/32 is directly connected, Loopback0
C    180.5.1.0/24 is directly connected, Loopback1
L    180.5.1.10/32 is directly connected, Loopback1
C    180.5.2.0/24 is directly connected, Loopback2
L    180.5.2.10/32 is directly connected, Loopback2
C    180.5.3.0/24 is directly connected, Loopback3
L    180.5.3.10/32 is directly connected, Loopback3

R5#
```

Fuente: Autor. Tabla de enrutamiento en R5. [Imagen]. Diplomado CCNP. Bogotá: 2021.

## VERIFICACIÓN CONECTIVIDAD ESCENARIO 1

Figura 6. Traceroute R1.



```
R1
R1 con0 is now available

Press RETURN to get started.

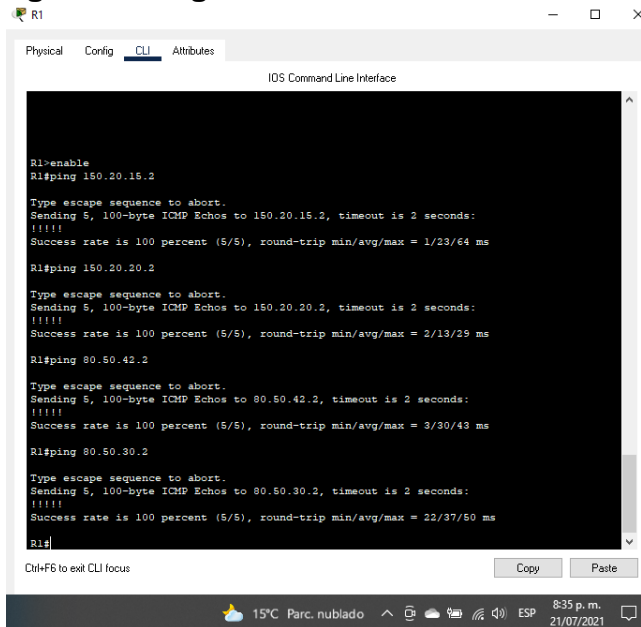
R1>enable
R1#traceroute 80.50.30.2
Type escape sequence to abort.
Tracing the route to 80.50.30.2

  1  150.20.15.2    0 msec   7 msec   2 msec
  2  150.20.20.2    1 msec   9 msec  17 msec
  3  80.50.42.2     0 msec   3 msec   1 msec
  4  80.50.30.2    14 msec  4 msec   4 msec

R1#
```

Fuente: Autor. Traceroute 1. [Imagen]. Diplomado CCNP. Bogotá: 2021

Figura 7. Ping desde R1 a todos los routers.



```
R1
R1>enable
R1#ping 150.20.15.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.20.15.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/23/64 ms

R1#ping 150.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.20.20.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/13/29 ms

R1#ping 80.50.42.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 80.50.42.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/30/43 ms

R1#ping 80.50.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 80.50.30.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/37/50 ms

R1#
```

Fuente: Autor. Ping desde R1 a todos los routers. [Imagen]. Diplomado CCNP. Bogotá: 2021

## 2. ESCENARIO 2

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.

### Topología de red

Figura 8. Escenario 2.

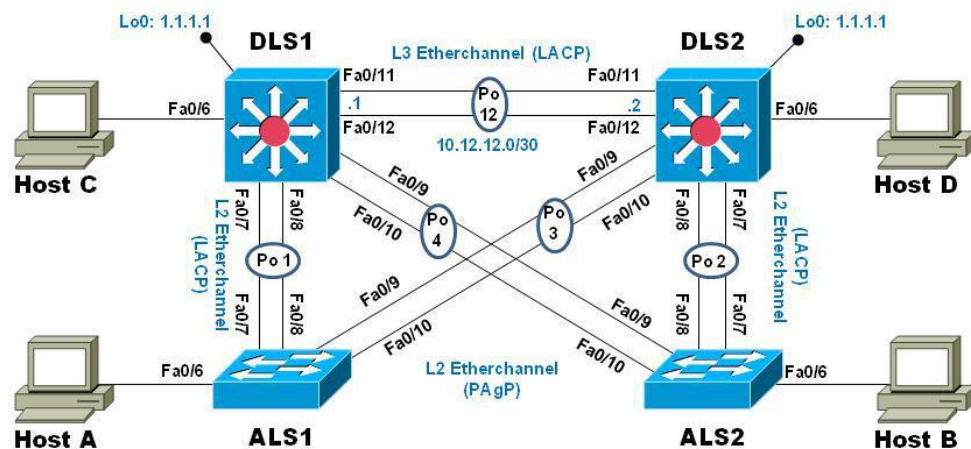
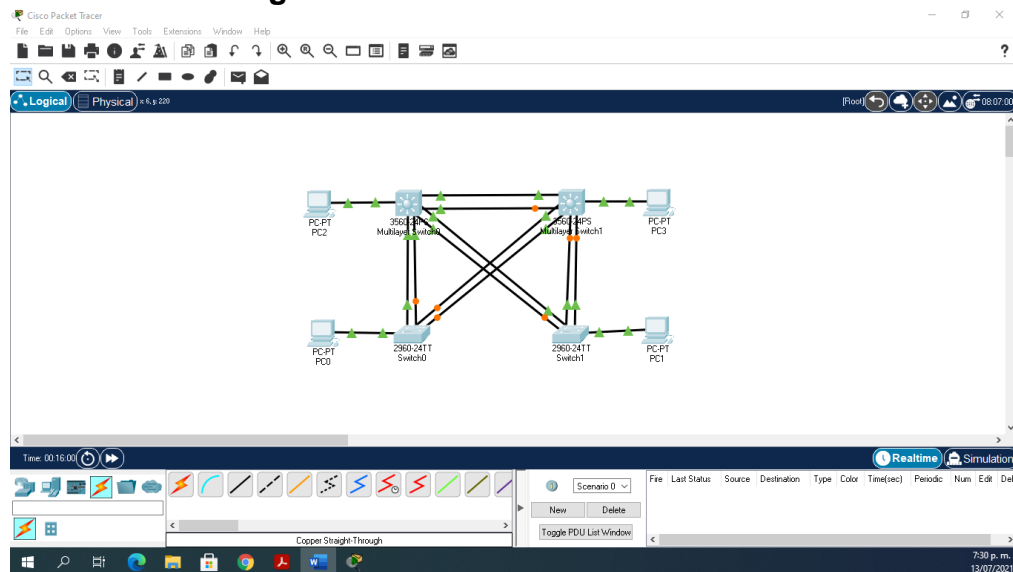


Figura 9. Escenario 2 Packet Tracer.



Fuente: Autor. Escenario 2 Packet Tracer. [Imagen]. Diplomado CCNP. Bogotá: 2021

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

a. Apagar todas las interfaces en cada switch.

Los comandos que se relacionan a continuación, será aplicados en los 4 switch.

```
Switch>enable // Cambia a modo privilegiado
Switch#conf terminal // Cambia a modo Configuración
Switch(config)#interface range fa0/1-24, gi0/1-2 // Selección rango de interfaces
Switch(config-if-range)#shutdown // Apagar interfaces
```

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

### DLS1

```
Switch>enable // Cambia a modo privilegiado
Switch#conf terminal // Cambia a modo Configuración
Switch(config)#hostname DLS1 //Asignar nombre al dispositivo
```

### DLS2

```
Switch>enable // Cambia a modo privilegiado
Switch#conf terminal // Cambia a modo Configuración
Switch(config)#hostname DLS2 //Asignar nombre al dispositivo
```

### ALS1

```
Switch>enable // Cambia a modo privilegiado
Switch#conf terminal // Cambia a modo Configuración
Switch(config)#hostname ALS1 //Asignar nombre al dispositivo
```

### ALS2

```
Switch>enable // Cambia a modo privilegiado
Switch#conf terminal // Cambia a modo Configuración
Switch(config)#hostname ALS2 //Asignar nombre al dispositivo
```

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 10.20.20.1/30 y para DLS2 utilizará 10.20.20.2/30.

## DLS1

```
DLS1#conf terminal
DLS1(config)#interface port-channel 12 //Crear interface al grupo LACP
DLS1(config-if)#no switchport //Aporta a la interfaz capacidad de
Capa 3
DLS1(config-if)#ip address 10.20.20.1 255.255.255.252
DLS1(config-if)#exit
DLS1(config)#interface range fa0/11-12 //Selección rango de interfaces
DLS1(config-if-range)#no switchport //Aporta a la interfaz capacidad de
Capa 3
DLS1(config-if-range)#channel-group 12 mode active //Asignar grupo LACP
DLS1(config-if-range)#no shutdown //Encender las interfaces
DLS1(config-if-range)#exit
DLS1(config-if)#description PO12 etherchannel (LACP) //Asignar descripción
```

## DLS2

```
DLS2#conf terminal
DLS2(config)#interface port-channel 12 //Crear interface al grupo LACP
DLS2(config-if)#no switchport //Aporta a la interfaz capacidad de
Capa 3
DLS2(config-if)#ip address 10.20.20.2 255.255.255.252
DLS2(config-if)#exit
DLS2(config)#interface range fa0/11-12 //Selección rango de interfaces
DLS2(config-if-range)#no switchport //Aporta a la interfaz capacidad de
Capa 3
DLS2(config-if-range)#channel-group 12 mode active //Asignar grupo LACP
DLS2(config-if-range)#no shutdown //Encender las interfaces
DLS2(config-if-range)#exit
DLS2(config-if)#description PO12 etherchannel (LACP) //Asignar descripción
```

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

Para la configuración troncales y EtherChannel, utilizaremos el comando switchport trunk encapsulation dot1q.

## DLS1

```
DLS1#configure terminal // Cambia a modo Configuración
DLS1(config)#interface range fa0/7-8 // Selección rango de interfaces
DLS1(config-if-range)#no shutdown //Encender las interfaces
DLS1(config-if-range)#channel-protocol lacp // Selección modo LACP
DLS1(config-if-range)#channel-group 1 mode active // Asignar grupo LACP
DLS1(config-if-range)#interface port-channel 1 // Crear interface al grupo LACP
DLS1(config-if)#description PO1 etherchannel (LACP) // Asignar descripción
```

## **ALS1**

```
ALS1#configure terminal // Cambia a modo Configuración
ALS1(config)#interface range fa0/7-8 // Selección rango de interfaces
ALS1(config-if-range)#no shutdown //Encender las interfaces
ALS1(config-if-range)#channel-protocol lacp // Selección modo LACP
ALS1(config-if-range)#channel-group 1 mode active // Asignar grupo LACP
ALS1(config-if-range)#interface port-channel 1 // Crear interface al grupo LACP
ALS1(config-if)#description PO1 etherchannel (LACP) // Asignar descripción
```

## **DLS2**

```
DLS2#configure terminal // Cambia a modo Configuración
DLS2(config)#interface range fa0/7-8 // Selección rango de interfaces
DLS2(config-if-range)#no shutdown //Encender las interfaces
DLS2(config-if-range)#channel-protocol lacp // Selección modo LACP
DLS2(config-if-range)#channel-group 2 mode active // Asignar grupo LACP
DLS2(config-if-range)#interface port-channel 2 // Crear interface al grupo LACP
DLS2(config-if)#description PO2 etherchannel (LACP) // Asignar descripción
```

## **ALS2**

```
ALS2#configure terminal // Cambia a modo Configuración
ALS2(config)#interface range fa0/7-8 // Selección rango de interfaces
ALS2(config-if-range)#no shutdown //Encender las interfaces
ALS2(config-if-range)#channel-protocol lacp // Selección modo LACP
ALS2(config-if-range)#channel-group 2 mode active // Asignar grupo LACP
ALS2(config-if-range)#interface port-channel 2 // Crear interface al grupo LACP
ALS2(config-if)#description PO2 etherchannel (LACP) // Asignar descripción
```

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

## **DLS1**

```
DLS1#configure terminal // Cambia a modo Configuración
DLS1(config)#interface range FA0/9-10 // Selección rango de interfaces
DLS1(config-if-range)#no shutdown //Encender las interfaces
DLS1(config-if-range)#channel-protocol pagp // Selección modo PAgP
DLS1(config-if-range)#channel-group 4 mode desirable // Asignar grupo PAgP
DLS1(config-if-range)#interface port-channel 4 // Crear interface al grupo PAgP
DLS1(config-if)#description PO4 etherchannel (PAgP) // Asignar descripción
```

## **ALS1**

```
ALS1#configure terminal // Cambia a modo Configuración
```

```
ALS1(config-if)#interface range fas0/9-10 // Selección rango de interfaces
ALS1(config-if-range)#no shutdown //Encender las interfaces
ALS1(config-if-range)#channel-protocol pagp // Selección modo PAgP
ALS1(config-if-range)#channel-group 3 mode desirable // Asignar grupo PAgP
ALS1(config-if-range)#interface port-channel 3 // Crear interface al grupo PAgP
ALS1(config-if)#description PO3 etherchannel (PAgP) // Asignar descripción
```

## **DLS2**

```
DLS2#configure terminal // Cambia a modo Configuración
DLS2(config)#interface range FA0/9-10 // Selección rango de interfaces
DLS2(config-if-range)#no shutdown //Encender las interfaces
DLS2(config-if-range)#channel-protocol pagp // Selección modo PAgP
DLS2(config-if-range)#channel-group 3 mode desirable // Asignar grupo PAgP
DLS2(config-if-range)#interface port-channel 3 // Crear interface al grupo PAgP
DLS2(config-if)#description PO3 etherchannel (PAgP) // Asignar descripción
```

## **ALS2**

```
ALS2#configure terminal // Cambia a modo Configuración
ALS2(config-if)#interface range fas0/9-10 // Selección rango de interfaces
ALS2(config-if-range)#no shutdown //Encender las interfaces
ALS2(config-if-range)#channel-protocol pagp // Selección modo PAgP
ALS2(config-if-range)#channel-group 4 mode desirable // Asignar grupo PAgP
ALS2(config-if-range)#interface port-channel 4 // Crear interface al grupo PAgP
ALS2(config-if)#description PO4 etherchannel (PAgP) // Asignar descripción
```

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

## **DLS1**

```
DLS1#conf terminal
DLS1(config)#interface Po1
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#exit
DLS1(config)#interface Po4
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#exit
```

## **ALS1**

```
ALS1#conf terminal
ALS1(config)#interface Po1
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#exit
ALS1(config)#interface Po3
```

```
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#exit
ALS1(config-if-range)#no shutdown
```

## **DLS2**

```
DLS2#conf terminal
DLS2(config-if-range)#exit
DLS2(config)#interface Po2
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#exit
DLS2(config)#interface Po3
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#exit
```

## **ALS2**

```
ALS2#conf terminal
ALS2(config)#interface Po2
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#exit
ALS2(config)#interface Po4
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#exit
```

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

No es posible configurar la versión VTP 3 en Cisco Packet Tracer, por esta razón se configura versión 2 y se hace de manera Transparente.

Para la realización de estos tres pasos, hemos usado los comandos vtp domain, vtp version 2, vtp mode server y vtp mode client. A continuación, se muestra la configuración realizada.

1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321

## **DLS1**

```
DLS1(config)#vtp version 2 // Selección versión de VTP
DLS1(config)#vtp domain CISCO // Nombre dominio VTP
DLS1(config)#vtp password ccnp321 // Contraseña VTP
```

## **ALS1**

```
ALS1(config)#vtp version 2 // Selección versión de VTP
ALS1(config)#vtp domain CISCO // Nombre dominio VTP
```

```
ALS1(config)#vtp password ccnp321 // Contraseña VTP
```

## ALS2

```
ALS2(config)#vtp version 2 // Selección versión de VTP  
ALS2(config)#vtp domain CISCO // Nombre dominio VTP  
ALS2(config)#vtp password ccnp321 // Contraseña VTP
```

2) Configurar DLS1 como servidor principal para las VLAN.

```
DLS1(config)#vtp mode server // Cambia al modo servidor VTP
```

3) Configurar ALS1 y ALS2 como clientes VTP.

## ALS1

```
ALS1(config)#vtp mode client // Cambia al modo cliente VTP
```

## ALS2

```
ALS2(config)#vtp mode client // Cambia al modo cliente VTP
```

e. Configurar en el servidor principal las siguientes VLAN:

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
600	<b>NATIVA</b>	420	<b>PROVEEDORES</b>
15	<b>ADMON</b>	100	<b>SEGUROS</b>
240	<b>CLIENTES</b>	1050	<b>VENTAS</b>
1112	<b>MULTIMEDIA</b>	3550	<b>PERSONAL</b>

Tabla 3. VLAN servidor principal

**Nota:** El modo VTP Server en Cisco Packet Tracer solo permite crear VLAN en el rango <1-1005>, por ende, para crear las VLAN mencionadas (1112, 1050, 3550) en el SW DLS1 es necesario configurarlo como modo VTP transparente.

```
DLS1#configure terminal // Cambia a modo Configuración  
DLS1(config)#vtp mode transparent // Selecciona modo VTP transparente  
DLS1(config)#vlan 600 // Crea nueva VLAN  
DLS1(config-vlan)#name NATIVA // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 15 // Crea nueva VLAN  
DLS1(config-vlan)#name ADMON // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 240 // Crea nueva VLAN  
DLS1(config-vlan)#name CLIENTES // Nombre de VLAN
```

```

DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vlan 1112 // Crea nueva VLAN
DLS1(config-vlan)#name MULTIMEDIA // Nombre de VLAN
DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vlan 420 // Crea nueva VLAN
DLS1(config-vlan)#name PROVEEDORES // Nombre de VLAN
DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vlan 100 // Crea nueva VLAN
DLS1(config-vlan)#name SEGUROS // Nombre de VLAN
DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vlan 1050 // Crea nueva VLAN
DLS1(config-vlan)#name VENTAS // Nombre de VLAN
DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vlan 3550 // Crea nueva VLAN
DLS1(config-vlan)#name PERSONAL // Nombre de VLAN
DLS1(config-vlan)#exit // Sale del modo de configuración
DLS1(config)#vtp mode server // Entra al modo servidor VTP

```

**Figura 10. VLAN configuradas en DLS1.**

```

DLS1
Physical Config CLI Attributes
IOS Command Line Interface

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/7 (500),
with ALS1 Port-channel1 (800).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/8 (500),
with ALS1 FastEthernet0/8 (800).

DLS1(config-if-range)#exit
DLS1(config)#vlan 600
DLS1(config-vlan)#name NATIVA
DLS1(config-vlan)#exit
DLS1(config)#vlan 15
DLS1(config-vlan)#name ADMON
DLS1(config-vlan)#exit
DLS1(config)#vlan 240
DLS1(config-vlan)#name CLIENTES
DLS1(config-vlan)#exit
DLS1(config)#vlan 1112
VLAN_CREATE_FAIL: Failed to create VLANs 1112 : extended VLAN(s) not allowed in current
VTP mode
DLS1(config)#vlan 1111
VLAN_CREATE_FAIL: Failed to create VLANs 1111 : extended VLAN(s) not allowed in current
VTP mode
DLS1(config)#vlan 420
DLS1(config-vlan)#name PROVEEDORES
DLS1(config-vlan)#exit
DLS1(config)#vlan 100
DLS1(config-vlan)#name SEGUROS
DLS1(config-vlan)#exit
DLS1(config)#vlan 1050
VLAN_CREATE_FAIL: Failed to create VLANs 1050 : extended VLAN(s) not allowed in current
VTP mode
DLS1(config)#vlan 3550
VLAN_CREATE_FAIL: Failed to create VLANs 3550 : extended VLAN(s) not allowed in current
VTP mode
DLS1(config)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

**Fuente:** Autor. VLAN configuradas en DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

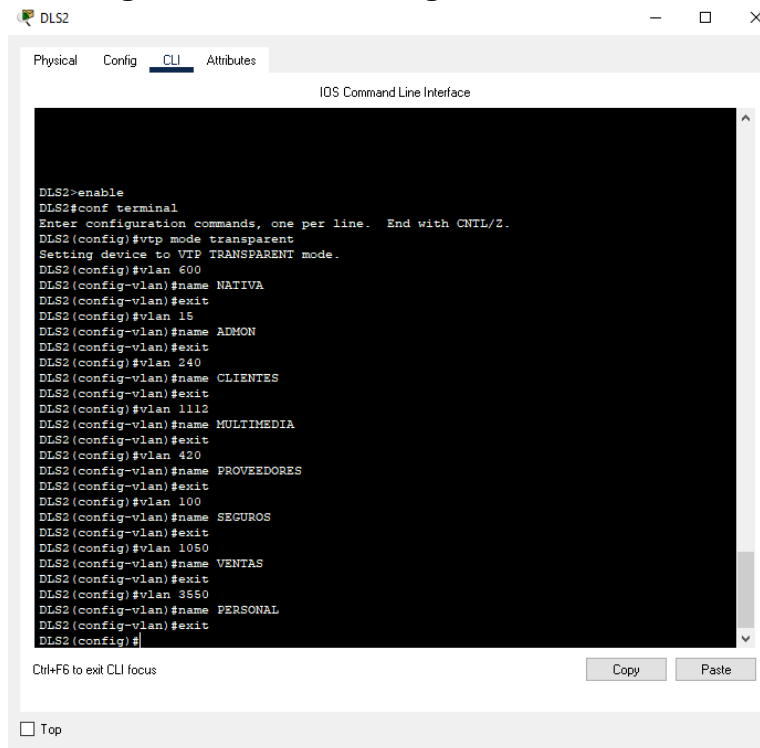
f. En DLS1, suspender la VLAN 420.

```
DLS1(config)#vlan 420 // Crea nueva VLAN  
DLS1(config-vlan)# no vlan 420 // Deshabilitar VLAN
```

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

```
DLS2#configure terminal // Cambia a modo Configuración  
DLS2(config)#vtp version 2 // Selección versión de VTP  
DLS2(config)# vtp mode transparent // Selecciona modo VTP transparente  
DLS2(config)#vlan 600 // Crea nueva VLAN  
DLS2(config-vlan)#name NATIVA // Nombre de VLAN  
DLS2(config-vlan)#exit // Sale del modo de configuración  
DLS2(config)#vlan 15 // Crea nueva VLAN  
DLS2(config-vlan)#name EJECUTIVOS // Nombre de VLAN  
DLS2(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 240 // Crea nueva VLAN  
DLS1(config-vlan)#name CLIENTES // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 1112 // Crea nueva VLAN  
DLS1(config-vlan)#name MULTIMEDIA // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 420 // Crea nueva VLAN  
DLS1(config-vlan)#name PROVEEDORES // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 100 // Crea nueva VLAN  
DLS1(config-vlan)#name SEGUROS // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 1050 // Crea nueva VLAN  
DLS1(config-vlan)#name VENTAS // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración  
DLS1(config)#vlan 3550 // Crea nueva VLAN  
DLS1(config-vlan)#name PERSONAL // Nombre de VLAN  
DLS1(config-vlan)#exit // Sale del modo de configuración
```

**Figura 11. VLAN configuradas en DLS2.**



```
DLS2>enable
DLS2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
DLS2 (config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
DLS2 (config)#vlan 600
DLS2 (config-vlan)#name NATIVA
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 15
DLS2 (config-vlan)#name ADMON
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 240
DLS2 (config-vlan)#name CLIENTES
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 1112
DLS2 (config-vlan)#name MULTIMEDIA
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 420
DLS2 (config-vlan)#name PROVEEDORES
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 100
DLS2 (config-vlan)#name SEGUROS
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 1050
DLS2 (config-vlan)#name VENTAS
DLS2 (config-vlan)#exit
DLS2 (config)#vlan 3550
DLS2 (config-vlan)#name PERSONAL
DLS2 (config-vlan)#exit
DLS2 (config)#
```

**Fuente:** Autor. VLAN configuradas en DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

h. Suspender VLAN 420 en DLS2.

```
DLS2(config)# vlan 420 // Crea nueva VLAN
DLS2(config)# no vlan 420 // Deshabilitar VLAN
```

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.

En este punto se requiere que la nueva VLAN sea restringida, por lo que usaremos el comando switchport allowed vlan except

```
DLS2(config)#vlan 567
DLS2(config-vlan)#name PRODUCCION
DLS2(config-vlan)#exit
DLS2(config)#int port-channel 2
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#int port-channel 3
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#exit
```

j. Configurar DLS1 como Spanning tree root para las VLANs 1, 12, 420, 600, 1050, 1112 y 3550 y como raíz secundaria para las VLAN 100 y 240.

El comando de Spanning tree debe ser utilizado solo en los conmutadores de red troncal. Para su habilitación se debe ingresar a la configuración general. El `spanning-tree vlan vlan-id root { primary | secondary }` se puede usar para establecer automáticamente un valor de prioridad como lo realizamos a continuación.

```
DLS1#conf terminal
```

```
DLS1(config)#spanning-tree vlan 1,12,420,600,1050,1112,3550 root primary // id-vlan con el valor de prioridad de puente más bajo
```

```
DLS1(config)#spanning-tree vlan 100,240 root secondary // adicionar id-vlan con el valor de prioridad de puente más bajo
```

k. Configurar DLS2 como Spanning tree root para las VLAN 100 y 240 y como una raíz secundaria para las VLAN 15, 420, 600, 1050, 1112 y 3550.

```
DLS2#conf terminal
```

```
DLS2(config)#spanning-tree vlan 100,240 root primary // id-vlan con el valor de prioridad de puente más bajo
```

```
DLS2(config)#spanning-tree vlan 15,420,600,1050,1112,3550 root secondary // adicionar id-vlan con el valor de prioridad de puente más bajo
```

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.

## **DLS1**

```
DLS1#conf terminal
```

```
DLS1(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
```

```
DLS1(config-if)#switchport trunk encapsulation dot1q // Enlace troncal con encapsulamiento a 4 bits
```

```
DLS1(config-if)#switchport mode trunk // Crea un enlace troncal
```

```
DLS1(config-if)#exit
```

```
DLS1(config)#int port-channel4
```

```
DLS1(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
```

```
DLS1(config-if)#switchport trunk encapsulation dot1q // Enlace troncal con encapsulamiento a 4 bits
```

```
DLS1(config-if)#switchport mode trunk // Crea un enlace troncal
```

```
DLS1(config-if)#exit
```

```
DLS1(config)#int port-channel2
```

```
DLS1(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
```

```
DLS1(config-if)#switchport trunk encapsulation dot1q // Enlace troncal con encapsulamiento a 4 bits
```

```
DLS1(config-if)#switchport mode trunk // Crea un enlace troncal
```

```
DLS1(config-if)#exit
```

```
DLS1(config)#int port-channel3
```

```
DLS1(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
```

```

DLS1(config-if)#switchport trunk encapsulation dot1q // Enlace troncal con
encapsulamiento a 4 bits
DLS1(config-if)#switchport mode trunk // Crea un enlace troncal
DLS1(config-if)#exit
DLS1(config)#interface range fa0/7-10 // Selección rango de interfaces
DLS1(config-if-range)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
DLS1(config-if-range)#switchport trunk encapsulation dot1q // Enlace troncal con
encapsulamiento a 4 bits
DLS1(config-if-range)# switchport mode trunk // Crea un enlace troncal
DLS1(config-if-range)#channel-group 1 mode active

```

## **DLS2**

```

DLS2(config)#interface range fa0/7-12 // Selección rango de interfaces
DLS2(config-if-range)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
DLS2(config-if-range)#switchport trunk encapsulation dot1q // Enlace troncal con
encapsulamiento a 4 bits
DLS2(config-if-range)#switchport mode trunk // Crea un enlace troncal
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#exit

```

## **ALS1**

```

ALS1#conf terminal
ALS1(config)#interface range fa0/7-10 // Selección rango de interfaces
ALS1(config-if-range)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
ALS1(config-if-range)#switchport mode trunk // Crea un enlace troncal

```

## **ALS2**

```

ALS2(config)#int port-channel2
ALS2(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
ALS2(config-if)#switchport mode trunk // Crea un enlace troncal
ALS2(config-if)#exit
ALS2(config)#int port-channel4
ALS2(config-if)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
ALS2(config-if)#switchport mode trunk // Crea un enlace troncal
ALS2(config-if)#exit
ALS2(config)#int range fa0/7-8 // Selección rango de interfaces
ALS2(config-if-range)#switchport trunk native vlan 500 // Identificar la VLAN Nativa
ALS2(config-if-range)#switchport mode trunk // Crea un enlace troncal
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#exit
ALS2(config)#int range fa0/9-10 // Selección rango de interfaces
ALS2(config-if-range)#switchport trunk native vlan 500 // Identificar la VLAN Nativa

```

```

ALS2(config-if-range)#switchport mode trunk // Crea un enlace troncal
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#exit

```

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

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fz0/6	3550	15, 1050	100, 1050	240
Interfaz Fz0/15	1112	1112	1112	1112
Interfaces Fz0/16 - 18		567		

Tabla 4. Interfaces VLAN

Según la tabla anterior se procede con la configuración de las interfaces como puertos de acceso, para esto utilizamos en comando switchport access vlan y encendemos la interfaz.

### DLS1

```

DLS1#configure terminal // Cambia a modo Configuración
DLS1(config)# interface fa0/6 // Selección de interface
DLS1(config-if)#switchport access vlan 3550 // Cambia VLAN a modo de acceso permanente
DLS1(config-if)#no shutdown // Habilitar interface
DLS1(config-if)# exit
DLS1(config)# interface fa0/15 // Selección de interface
DLS1(config-if)#switchport access vlan 1112 // Cambia VLAN a modo de acceso permanente
DLS1(config-if)#no shutdown // Habilitar interface
DLS1(config-if)#exit // Sale del modo de configuración

```

### DLS2

```

DLS2#configure terminal // Cambia a modo Configuración
DLS2(config)# interface fa0/6 // Selección de interface
DLS2(config-if)#switchport access vlan 15 // Cambia VLAN a modo de acceso permanente
DLS2(config-if)#switchport access vlan 1050 // Cambia VLAN a modo de acceso permanente
DLS2(config-if)#no shutdown // Habilitar interface
DLS2(config-if)# exit // Sale del modo de configuración
DLS2(config)# interface fa0/15 // Selección de interface
DLS2(config-if)#switchport access vlan 1112 // Cambia VLAN a modo de acceso permanente
DLS2(config-if)#no shutdown // Habilitar interface

```

```
DLS2(config-if)# exit // Sale del modo de configuración
DLS2(config)# interface range fa0/16-18 // Selección rango de interface
DLS2(config-if)#switchport access vlan 567 // Cambia VLAN a modo de acceso permanente
DLS2(config-if)#no shutdown // Habilitar interface
DLS2(config-if)#exit // Sale del modo de configuración
```

## **ALS1**

```
ALS1#configure terminal // Cambia a modo Configuración
ALS1(config)# interface fa0/6 // Selección de interface
ALS1(config-if)#switchport access vlan 100 // Cambia VLAN a modo de acceso permanente
ALS1(config-if)#switchport access vlan 1050 // Cambia VLAN a modo de acceso permanente
ALS1(config-if)#no shutdown // Habilitar interface
ALS1(config-if)# exit // Sale del modo de configuración
ALS1(config)# interface fa0/15 // Selección de interface
ALS1(config-if)#switchport access vlan 1112 // Cambia VLAN a modo de acceso permanente
ALS1(config-if)#no shutdown // Habilitar interface
ALS1(config-if)# end
```

## **ALS2**

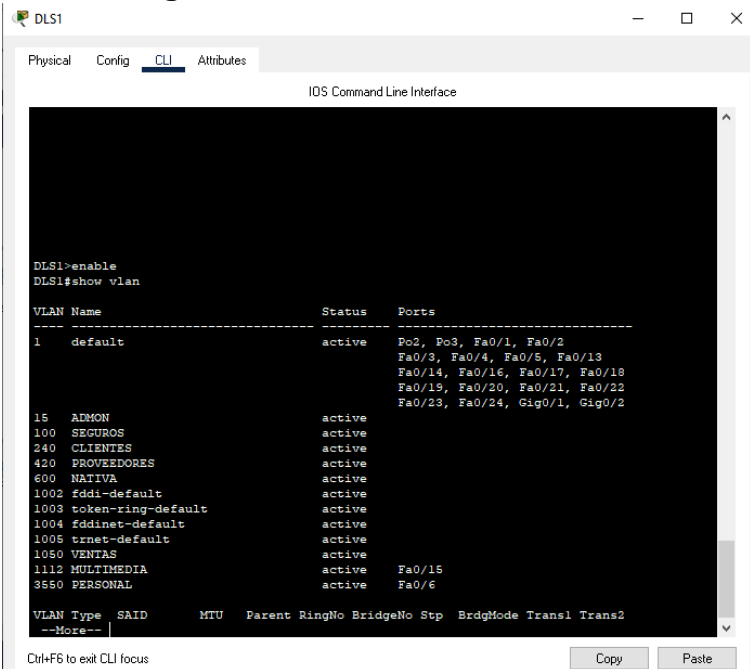
```
ALS2#configure terminal // Cambia a modo Configuración
ALS2(config)# interface fa0/6 // Selección de interface
ALS2(config-if)#switchport access vlan 240 // Cambia VLAN a modo de acceso permanente
ALS2(config-if)#no shutdown // Habilitar interface
ALS2(config-if)# exit // Sale del modo de configuración
ALS2(config)# interface fa0/15 // Selección de interface
ALS2(config-if)#switchport access vlan 1112 // Cambia VLAN a modo de acceso permanente
ALS2(config-if)#no shutdown // Habilitar interface
ALS2(config-if)# exit // Sale del modo de configuración
```

## **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.

Para verificar la existencia de VLAN, se hace a través del comando show vlan.

Figura 12. VLAN en switch DLS1.



```
DLS1>enable
DLS1#show vlan

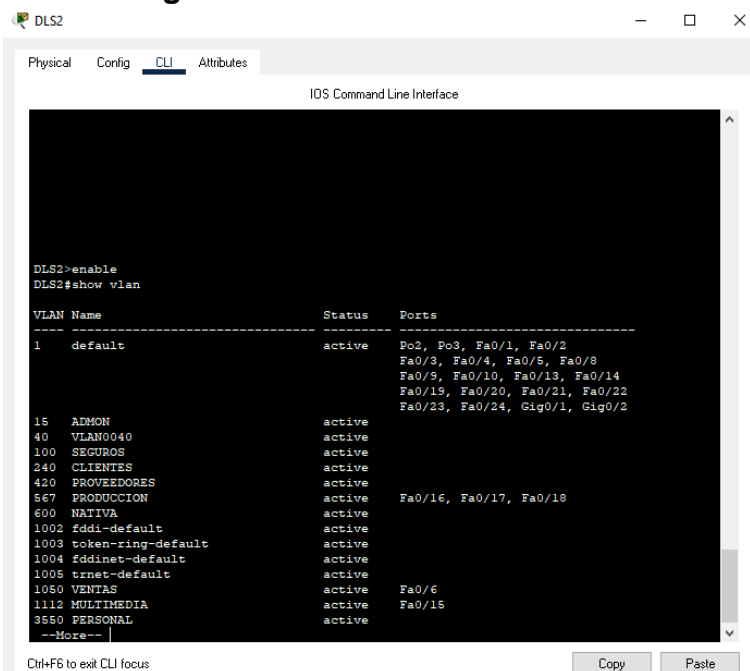
VLAN Name                Status    Ports
-----
1  default                 active    Po2, Po3, Fa0/1, Fa0/2
                               Fa0/3, Fa0/4, Fa0/5, Fa0/13
                               Fa0/14, Fa0/16, Fa0/17, Fa0/18
                               Fa0/19, Fa0/20, Fa0/21, Fa0/22
                               Fa0/23, Fa0/24, Gig0/1, Gig0/2

15  ADMON                   active
100  SEGUROS                 active
240  CLIENTES                active
420  PROVEEDORES            active
600  NATIVA                  active
1002  fddi-default            active
1003  token-ring-default      active
1004  fdnet-default           active
1005  trnet-default           active
1050  VENTAS                  active
1112  MULTIMEDIA              active    Fa0/15
3550  PERSONAL                active    Fa0/6

VLAN Type  SAID          MTU   Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
--More--
```

Fuente: Autor. VLAN en switch DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

Figura 13. VLAN en switch DLS2.



```
DLS2>enable
DLS2#show vlan

VLAN Name                Status    Ports
-----
1  default                 active    Po2, Po3, Fa0/1, Fa0/2
                               Fa0/3, Fa0/4, Fa0/5, Fa0/8
                               Fa0/9, Fa0/10, Fa0/13, Fa0/14
                               Fa0/19, Fa0/20, Fa0/21, Fa0/22
                               Fa0/23, Fa0/24, Gig0/1, Gig0/2

15  ADMON                   active
40  VLAN0040                active
100  SEGUROS                 active
240  CLIENTES                active
420  PROVEEDORES            active
567  PRODUCCION              active    Fa0/16, Fa0/17, Fa0/18
600  NATIVA                  active
1002  fddi-default            active
1003  token-ring-default      active
1004  fdnet-default           active
1005  trnet-default           active
1050  VENTAS                  active
1112  MULTIMEDIA              active    Fa0/6
3550  PERSONAL                active    Fa0/15

--More--
```

Fuente: Autor. VLAN en switch DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

Para verificar la asignación de puerto troncales, se hace a través del comando show ip interface, que proporciona un resumen de la información clave para todas las interfaces de red de un router.

**Figura 14. Show interfaces en switch DLS1.**

```

DLS1#show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
Port-channel1     unassigned     YES unset  up      up
Port-channel2     unassigned     YES unset  down    down
Port-channel4     unassigned     YES unset  up      up
Port-channel12    10.20.20.1     YES manual  up      up
FastEthernet0/1   unassigned     YES unset  administratively down down
FastEthernet0/2   unassigned     YES unset  administratively down down
FastEthernet0/3   unassigned     YES unset  administratively down down
FastEthernet0/4   unassigned     YES unset  administratively down down
FastEthernet0/5   unassigned     YES unset  administratively down down
FastEthernet0/6   unassigned     YES unset  up      up
FastEthernet0/7   unassigned     YES unset  up      up
FastEthernet0/8   unassigned     YES unset  up      up
FastEthernet0/9   unassigned     YES unset  up      up
FastEthernet0/10  unassigned     YES unset  up      up
FastEthernet0/11  unassigned     YES unset  up      up
FastEthernet0/12  unassigned     YES unset  up      up
FastEthernet0/13  unassigned     YES unset  administratively down down
FastEthernet0/14  unassigned     YES unset  administratively down down
FastEthernet0/15  unassigned     YES unset  down    down
FastEthernet0/16  unassigned     YES unset  administratively down down
FastEthernet0/17  unassigned     YES unset  administratively down down
FastEthernet0/18  unassigned     YES unset  administratively down down
FastEthernet0/19  unassigned     YES unset  administratively down down
FastEthernet0/20  unassigned     YES unset  administratively down down
FastEthernet0/21  unassigned     YES unset  administratively down down
FastEthernet0/22  unassigned     YES unset  administratively down down
FastEthernet0/23  unassigned     YES unset  administratively down down
FastEthernet0/24  unassigned     YES unset  administratively down down
GigabitEthernet0/1 unassigned     YES unset  administratively down down
GigabitEthernet0/2 unassigned     YES unset  administratively down down
Vlan1              unassigned     YES unset  administratively down down
DLS1#
  
```

**Fuente:** Autor. Show interfaces en switch DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

**Figura 15. Show interfaces en switch DLS2.**

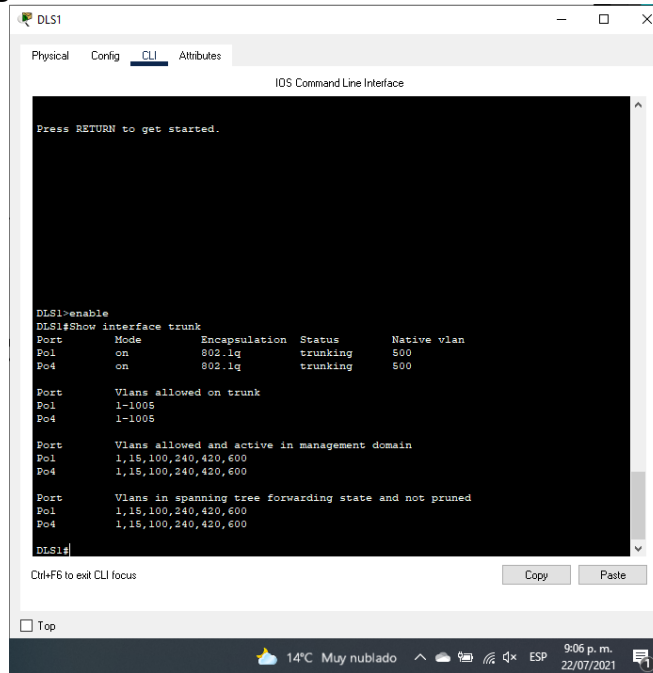
```

DLS2#enable
DLS2#show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
Port-channel2     unassigned     YES unset  up      up
Port-channel12    10.20.20.2     YES manual  up      up
FastEthernet0/1   unassigned     YES unset  administratively down down
FastEthernet0/2   unassigned     YES unset  administratively down down
FastEthernet0/3   unassigned     YES unset  administratively down down
FastEthernet0/4   unassigned     YES unset  administratively down down
FastEthernet0/5   unassigned     YES unset  administratively down down
FastEthernet0/6   unassigned     YES unset  up      up
FastEthernet0/7   unassigned     YES unset  up      up
FastEthernet0/8   unassigned     YES unset  up      up
FastEthernet0/9   unassigned     YES unset  up      up
FastEthernet0/10  unassigned     YES unset  up      up
FastEthernet0/11  unassigned     YES unset  up      up
FastEthernet0/12  unassigned     YES unset  up      up
FastEthernet0/13  unassigned     YES unset  administratively down down
FastEthernet0/14  unassigned     YES unset  administratively down down
FastEthernet0/15  unassigned     YES unset  down    down
FastEthernet0/16  unassigned     YES unset  administratively down down
FastEthernet0/17  unassigned     YES unset  administratively down down
FastEthernet0/18  unassigned     YES unset  administratively down down
FastEthernet0/19  unassigned     YES unset  administratively down down
FastEthernet0/20  unassigned     YES unset  administratively down down
FastEthernet0/21  unassigned     YES unset  administratively down down
FastEthernet0/22  unassigned     YES unset  administratively down down
FastEthernet0/23  unassigned     YES unset  administratively down down
FastEthernet0/24  unassigned     YES unset  administratively down down
GigabitEthernet0/1 unassigned     YES unset  administratively down down
GigabitEthernet0/2 unassigned     YES unset  administratively down down
Vlan1              unassigned     YES unset  administratively down down
DLS2#
  
```

**Fuente:** Autor. Show interfaces en switch DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

Para verificar los puertos troncales se hace uso del comando Show interface trunk.

**Figura 16. Show interfaces trunk en switch DLS1.**



```
DLS1#enable
DLS1#show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
-----
Po1       on        802.1q         trunking     500
Po4       on        802.1q         trunking     500

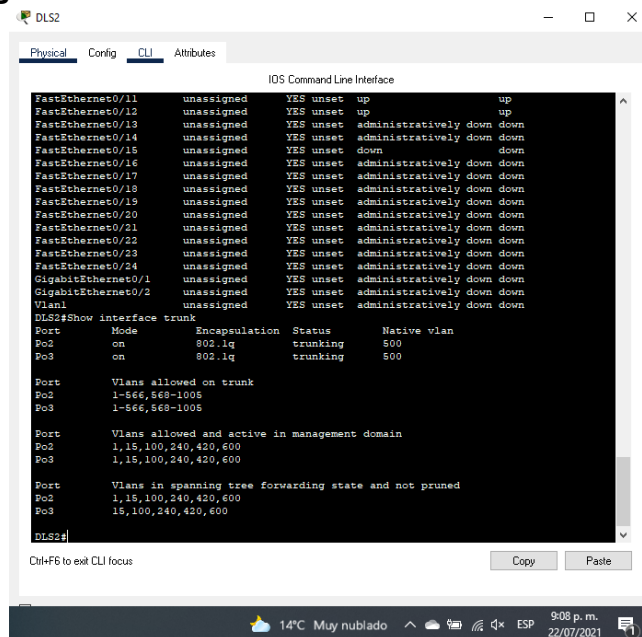
Port      Vlans allowed on trunk
-----
Po1       1-1005
Po4       1-1005

Port      Vlans allowed and active in management domain
-----
Po1       1, 15, 100, 240, 420, 600
Po4       1, 15, 100, 240, 420, 600

Port      Vlans in spanning tree forwarding state and not pruned
-----
Po1       1, 15, 100, 240, 420, 600
Po4       1, 15, 100, 240, 420, 600
DLS1#
```

**Fuente:** Autor. Show interfaces trunk en switch DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

**Figura 17. Show interfaces trunk en switch DLS2**



```
DLS2#show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
-----
Po2       on        802.1q         trunking     500
Po3       on        802.1q         trunking     500

Port      Vlans allowed on trunk
-----
Po2       1-566,568-1005
Po3       1-566,568-1005

Port      Vlans allowed and active in management domain
-----
Po2       1, 15, 100, 240, 420, 600
Po3       1, 15, 100, 240, 420, 600

Port      Vlans in spanning tree forwarding state and not pruned
-----
Po2       1, 15, 100, 240, 420, 600
Po3       15, 100, 240, 420, 600
DLS2#
```

**Fuente:** Autor. Show interfaces trunk en switch DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

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

**Figura 18. EtherChannel en DLS1.**

```

DLS1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

DLS1(config-if)#exit
DLS1(config)#interface fa0/15
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 1112
DLS1(config-if)#no shutdown
DLS1#

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to down
DLS1(config-if)#end
DLS1#

%SYS-5-CONFIG_I: Configured from console by console

DLS1#show etherchannel summary
Flags: D - down        P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
 1      Po1(SU)        LACP       Fa0/7(P) Fa0/8(P)
 2      Po2(SD)        -
 4      Po4(SU)        PAGP       Fa0/9(P) Fa0/10(P)
12      Po12(RU)       LACP       Fa0/11(P) Fa0/12(P)
DLS1#
    
```

Fuente: Autor. EtherChannel en DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

**Figura 19. EtherChannel en ALS1.**

```

ALS1
Physical Config CLI Attributes
IOS Command Line Interface

1002 fddi 101002 1500 - - - - 0 0
1003 tr 101003 1500 - - - - 0 0
1004 fdnet 101004 1500 - - - - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrgdMode Trans1 Trans2
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
Remote SPAN VLANs
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
Primary Secondary Type Ports
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
ALS1#
ALS1#show etherchannel summary
Flags: D - down        P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use      f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

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

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
 1      Po1(SU)        LACP       Fa0/7(P) Fa0/8(P)
 3      Po3(SU)        PAGP       Fa0/9(P) Fa0/10(P)
ALS1#
    
```

Fuente: Autor. EtherChannel en ALS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

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

Para verificar la configuración de Spanning tree utilizaremos el comando show spanning-tree, este comando, además, nos permitirá obtener toda la configuración de STP del switch e incluso la prioridad de puerto y costo del puerto.

**Figura 20. Spanning tree en DLS1.**

```

DLS1
-----
Physical Config CLI Attributes
IOS Command Line Interface
DLS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 000B.BE18.91C2
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 000B.BE18.91C2
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po4 Desg FWD 9 128.29 Shr
Po1 Desg FWD 9 128.38 Shr

VLAN0015
Spanning tree enabled protocol ieee
Root ID Priority 32783
Address 000B.BE18.91C2
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32783 (priority 32768 sys-id-ext 15)
Address 000B.BE18.91C2
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po4 Desg FWD 9 128.29 Shr
Po1 Desg FWD 9 128.38 Shr

VLAN0100
  
```

**Fuente:** Autor. Spanning tree en DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

**Figura 21. Spanning tree en DLS2.**

```

DLS2
-----
Physical Config CLI Attributes
IOS Command Line Interface
DLS2(config-if-range)#switchport access vlan 567
DLS2(config-if-range)#exit
DLS2(config)#end
DLS2#
$SYS-$-CONFIG_I: Configured from console by console
DLS2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 000B.BE18.91C2
Cost 18
Port 20 (Port-channel)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32769 sys-id-ext 1)
Address 00E0.A336.4655
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po2 Root FWD 9 128.29 Shr
Po3 Altn BLK 9 128.29 Shr

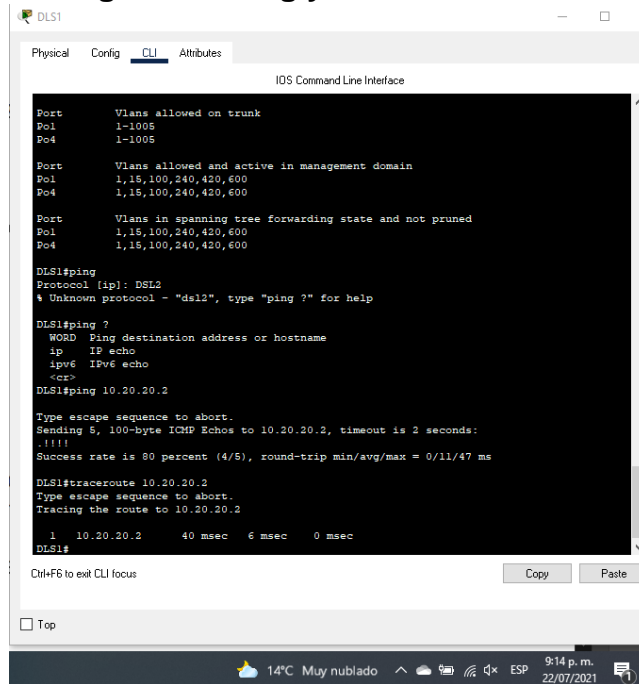
VLAN0015
Spanning tree enabled protocol ieee
Root ID Priority 28607
Address 00E0.A336.4655
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28607 (priority 28672 sys-id-ext 15)
Address 00E0.A336.4655
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
  
```

**Fuente:** Autor. Spanning tree en DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

## VERIFICACIÓN CONECTIVIDAD ESCENARIO 2

Figura 22. Ping y traceroute DLS1.



```
DLS1
Physical Config CLI Attributes
IOS Command Line Interface

Port      Vlans allowed on trunk
Po1       1-1005
Po4       1-1005

Port      Vlans allowed and active in management domain
Po1       1,15,100,240,420,600
Po4       1,15,100,240,420,600

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,15,100,240,420,600
Po4       1,15,100,240,420,600

DLS1#ping
Protocol [ip]: DSL2
% Unknown protocol - "dsl2", type "ping ?" for help

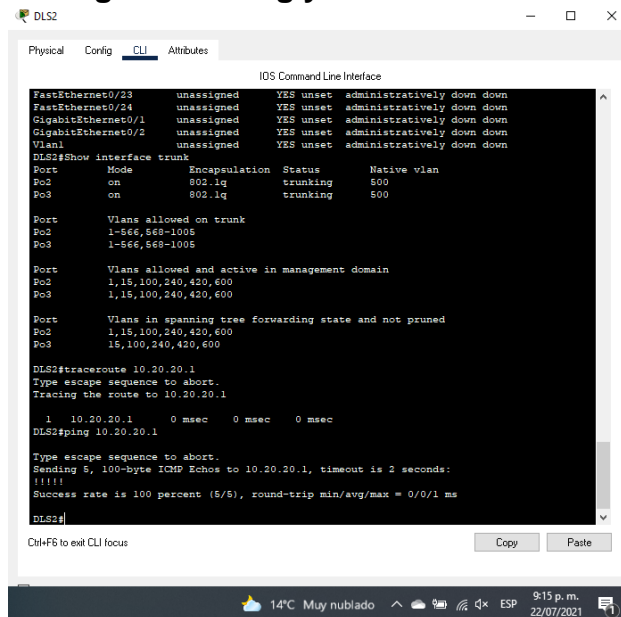
DLS1#ping ?
WORD Ping destination address or hostname
-ip IP echo
-ipv6 IPv6 echo
<cr>
DLS1#ping 10.20.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.2, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/11/47 ms

DLS1#traceroute 10.20.20.2
Type escape sequence to abort.
Tracing the route to 10.20.20.2
 0  10.20.20.2      40 msec  6 msec  0 msec
DLS1#
```

Fuente: Autor. Ping y traceroute DLS1. [Imagen]. Diplomado CCNP. Bogotá: 2021.

Figura 23. Ping y traceroute DLS2



```
DLS2
Physical Config CLI Attributes
IOS Command Line Interface

FastEthernet0/23  unassigned  YES unset  administratively down down
FastEthernet0/24  unassigned  YES unset  administratively down down
GigabitEthernet0/1 unassigned  YES unset  administratively down down
GigabitEthernet0/2 unassigned  YES unset  administratively down down
Vlan1             unassigned  YES unset  administratively down down

DLS2#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    500
Po3       on        802.1q         trunking    500

Port      Vlans allowed on trunk
Po2       1-500,500-1005
Po3       1-500,500-1005

Port      Vlans allowed and active in management domain
Po2       1,15,100,240,420,600
Po3       1,15,100,240,420,600

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,15,100,240,420,600
Po3       15,100,240,420,600

DLS2#traceroute 10.20.20.1
Type escape sequence to abort.
Tracing the route to 10.20.20.1
 0  10.20.20.1      0 msec  0 msec  0 msec
DLS2#ping 10.20.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

DLS2#
```

Fuente: Autor. Ping y traceroute DLS2. [Imagen]. Diplomado CCNP. Bogotá: 2021.

## ANEXOS

### **Link de simulación Escenario 1:**

[https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/deninog\\_unadvirtual\\_edu\\_co/ERDX5yphYixNiujeBx0oLIBTMpNrUSReqN7zvskM0mu9g?e=26te8S](https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/deninog_unadvirtual_edu_co/ERDX5yphYixNiujeBx0oLIBTMpNrUSReqN7zvskM0mu9g?e=26te8S)

### **Link de simulación Escenario 2:**

[https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/deninog\\_unadvirtual\\_edu\\_co/EcOZI\\_oGNnROrpWkS91vVQIBaAXBEJpg5Br8jXpZGV4XMg?e=mm25G8](https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/deninog_unadvirtual_edu_co/EcOZI_oGNnROrpWkS91vVQIBaAXBEJpg5Br8jXpZGV4XMg?e=mm25G8)

## CONCLUSIONES

OSPF demuestra ser un protocolo más óptimo para redes grandes, brinda mayor seguridad, además de ser un protocolo de estado de enlace. A diferencia de EIGRP, incluye el concepto de Área el cual sólo se aplica a routers y para este trabajo se refiere a un conjunto de redes inmediatas identificadas por la misma área ID.

OSPF este es un protocolo sin clase (significa que envía la máscara de subred en sus actualizaciones), y además usa las áreas como concepto de escalabilidad.

EIGRP se escala bien y proporciona tiempos de convergencia extremadamente rápidos con un tráfico de red mínimo.

EIGRP permite conocer dispositivos que son vecinos o están conectados adyacentemente y ayuda a enrutar de manera ordenada las direcciones de las redes aprendidas.

El uso de las VLAN dentro de una red es fundamental para la creación de redes no físicas independientes permitiendo la disposición de varias VLANS dentro de un mismo conmutador. Estas pueden ser estáticas con puerto asociado o dinámicas con configuración particular.

## BIBLIOGRAFÍA

- Granados, G. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de <http://hdl.handle.net/10596/24167>
- Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]. Recuperado de <https://repository.unad.edu.co/handle/10596/24419>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>
- 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-NT1IlnMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Enterprise Internet Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Routers and Routing Protocol Hardening. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>