

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

RAFAEL NÚÑEZ HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
BOGOTÁ  
2019

DIPLOMADO DE PROFUNDIZACIÓN CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

RAFAEL NÚÑEZ HERNÁNDEZ

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
BOGOTÁ  
2019

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Bogotá, 12 de diciembre de 2019

## DEDICATORIA

A Luisa, tu soporte ha sido fundamental, me brindaste un apoyo ilimitado sin importar los contratiempos, tu dedicación y soporte se convirtieron en el motor para llegar a cumplir mi grado, te lo agradezco mucho amor.

A mis hijos Juanita, Samuel y Valery, quienes me dieron la fortaleza para afrontar las adversidades del camino permitiéndome avanzar sin desvanecer.

A mi papa por sus consejos, por su humildad, por su amor, por compartir conmigo los aciertos y fracasos.

A mi mamá, por sus retos y ayuda prestada en momentos complicados.

A mis hermanos por su confianza e interés en lograr culminar las metas propuestas.

A mis suegros, por otorgarme espacios de crecimiento e inmenso apoyo.

## CONTENIDO

	Pág.
DEDICATORIA .....	4
CONTENIDO .....	5
LISTA DE FIGURAS .....	6
LISTA DE TABLAS .....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT .....	9
INTRODUCCIÓN .....	10
DESARROLLO DE LOS DOS ESCENARIOS.....	11
1. ESCENARIO 1 .....	11
2. ESCENARIO 2.....	22
CONCLUSIONES .....	39
BIBLIOGRAFÍA.....	40

## LISTA DE FIGURAS

	Pág.
Figura 1. Topología de red primer escenario. ....	11
Figura 2. Configuración de interfaces. ....	16
Figura 3. Validación de Ping R1.....	20
Figura 4. Ping desde R2 a R3 y R1.....	20
Figura 5. Ping desde R1 a R2 y R3.....	21
Figura 6. Topología de red escenario 2.....	22
Figura 7. ALS2#.....	26
Figura 8. Configuración DSL1 VLAN principal.....	31
Figura 9. Interfaces VLAN.....	33
Figura 10. Host A.....	35
Figura 11. Host B.....	35
Figura 12. Host C.....	36
Figura 13. Host D:.....	36
Figura 14. Topología en red VLAN ADSL principal. ....	38

## LISTA DE TABLAS

	Pág.
Tabla 1. Listado de VLANs. ....	23
Tabla 2. Interfaces como puertos de acceso.....	23

## GLOSARIO

**CCNP:** (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

**GNS3:** Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios e imágenes IOS de Cisco Systems.

**Networking:** Es una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática conjunto de equipos informáticos y software reconectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**Protocolos de red:** Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

**VLAN:** Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

## **RESUMEN**

La prueba de habilidades practicas del diplomado de profundización CCNP aplican las habilidades adquiridas en los diferentes módulos del diplomado, dar solución a dos escenarios compuestos por necesidades propios de entornos de red corporativo donde se usaran comandos básicos como ping, traceroute, show ip route entre otros, el primer escenario recrea una compañía con tres sucursales distribuidas en diferentes ciudades, cada sucursal requerirá las condiciones necesarias como direccionamiento IP y protocolos e enrutamientos necesarios para realizar la interconexión entre sedes, en el segundo escenario una compañía con una estructura compleja de IT requiere que los equipos Core cuenten la interconexión lógica adecuada donde el direccionamiento IP, etherchannels y VLANs permitan una alta disponibilidad según el escenario propuesto.

Palabras Clave: CCNP, ping, traceroute, show ip route, direccionamiento IP, etherchannels, VLANs.

## **ABSTRACT**

The test of practical skills of the CCNP deepening diploma apply the skills acquired in the different modules of the diploma, to solve two scenarios composed of needs of corporate network environments where basic commands such as ping, traceroute, show ip route will be used among others , the first scenario recreates a company with three branches distributed in different cities, each branch will require the necessary conditions such as IP addressing and protocols and routing necessary to perform the interconnection between headquarters, in the second scenario a company with a complex IT structure requires that Core devices have the appropriate logical interconnection where IP addressing, etherchannels and VLANs allow high availability according to the proposed scenario.

Keywords: CCNP, ping, traceroute, show ip route, IP addressing, etherchannels, VLANs.

## INTRODUCCIÓN

La certificación CCNP (Cisco Certified Network Professional) permite aumentar la capacidad de planificar, implementar, verificar y solucionar problemas en redes empresariales LAN y WAN, también de integrar soluciones de: seguridad, voz, inalámbricas y video, el desarrollo de habilidades practicas permite que se implementen las temáticas en los escenarios propuestos.

El Diplomado como opción de grado está constituido por dos módulos: CCNP ROUTE y CCNP SWITCH, los cuales forman parte del currículo CCNP de la Academia CISCO.

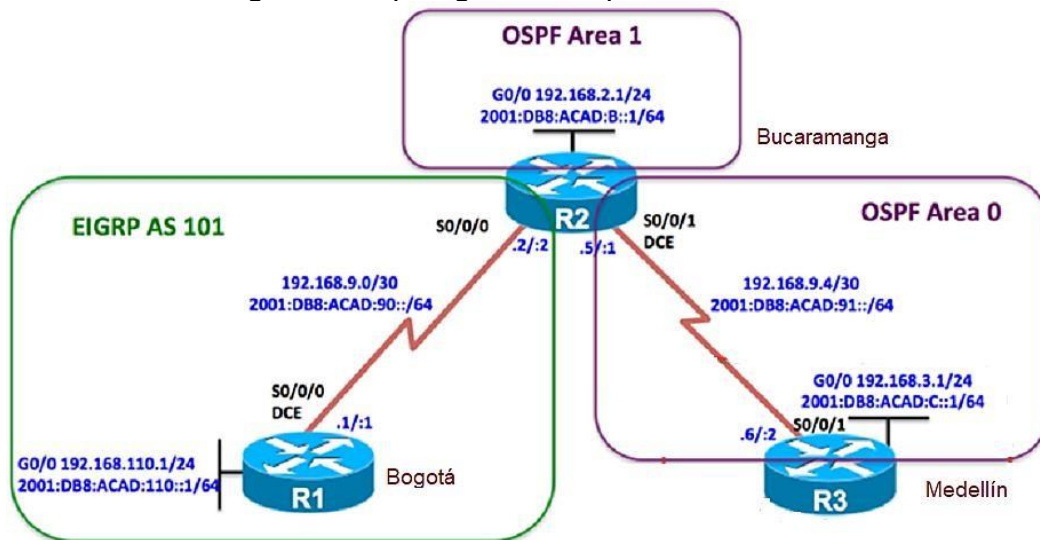
En el módulo ROUTE se abordarán conceptos principales como protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, Dynamic Multi VPN, VRF Lite y protocolos en IPv6. En el módulo SWITCH se abordarán conceptos principales como operaciones y puertos de swtiches, VLANs y troncales, Spanning Tree, manejo de ataques de spoofing y configuración de usuarios.

## DESARROLLO DE LOS DOS ESCENARIOS

### 1. ESCENARIO 1

Una empresa de confecciones posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, 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, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Figura 1. Topología de red primer escenario.



Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Parte 1: Configuración del escenario propuesto

1. Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red.
2. Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.

3. En R2 y R3 configurar las familias de direcciones OSPFv3 para IPv4 e IPv6. Utilice el identificador de enrutamiento 2.2.2.2 en R2 y 3.3.3.3 en R3 para ambas familias de direcciones.
4. En R2, configurar la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3 en OSPF área 0.
5. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0.
6. Configurar el área 1 como un área totalmente Stubby.
7. Propagar rutas por defecto de IPv4 y IPv6 en R3 al interior del dominio OSPFv3. Nota: Es importante tener en cuenta que una ruta por defecto es diferente a la definición de rutas estáticas.
8. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Configurar la interfaz F0/0 de R1 y la conexión entre R1 y R2 para EIGRP con el sistema autónomo 101. Asegúrese de que el resumen automático está desactivado.
9. Configurar las interfaces pasivas para EIGRP según sea apropiado.
10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.
11. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL.

Parte 2: Verificar conectividad de red y control de la trayectoria.

- a. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.
- b. Verificar comunicación entre routers mediante el comando ping y traceroute
- c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Nota: Puede ser que Una o más direcciones no serán accesibles desde todos los routers después de la configuración final debido a la utilización de listas de distribución para filtrar rutas y el uso de IPv4 e IPv6 en la misma red.

Implementación

1. Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red.

R1

```
Router>ena
Router#confi term
```

```
Router# confi term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.110.1 255.255.255.0
R1(config-if)#ipv6 address 2001:DB8:ACAD:110::1/64
R1(config-if)#NO SHUTdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

```
R1(config-if)#EXIT
R1(config)#INterface Serial 0/0/0
R1(config-if)#IP ADdress 192.168.9.1 255.255.255.252
R1(config-if)#IPV6 ADdress 2001:DB8:ACAD:90::1/64
R1(config-if)#NO SHUtdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

```
R1(config-if)#EXIT
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
```

```
R1(config)#EXIT
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#W
Building configuration...
```

[OK]

R1#

Configuracion R2

R2>ENA

R2#CONF T

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#HOSTname R2

R2(config)#interface gigabitEthernet 0/0

R2(config-if)#ip address 192.168.2.1 255.255.255.0

R2(config-if)#ipv6 address 2001:DB8:ACAD:B::1/64

%GigabitEthernet0/0: Error: 2001:DB8:ACAD:B::/64 is overlapping with 2001:DB8:ACAD:B::/64 on Serial0/0/0

R2(config-if)#NO SHUTdown

R2(config-if)#EXIT

R2(config)#INTerface Serial 0/0/0

R2(config-if)#IP ADdress 192.168.9.2 255.255.255.252

R2(config-if)#IPV6 ADdress 2001:DB8:ACAD:90.2/64

% Incomplete command.

R2(config-if)#IPV6 ADdress 2001:DB8:ACAD:90::2/64

R2(config-if)#NO SHUTdown

R2(config-if)#EXIT

R2(config)#EXIT

R2#

%SYS-5-CONFIG\_I: Configured from console by console

R2#W

Building configuration...

[OK]

R2#

R2#

R2(config)#INTerface S

R2(config)#INTerface Serial 0/0/1

R2(config-if)#IP ADdress 192.168.9.5 255.255.255.252

R2(config-if)#IPV6 ADdress 2001:DB8:ACAD:91::1/64

R2(config-if)#NO SHUtdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

```
R2(config-if)#
R2(config-if)#EXIT
R2(config)#END
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2#
```

### Configuracion R3

```
R3>ena
R3#confi term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#HOStname R3
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip ad
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#ipv6 address 2001:DB8:ACAD:C::1/64
R3(config-if)#NO SHUtdown
```

```
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

```
R3(config-if)#EXIT
R3(config)#INTErface Serial 0/0/1
R3(config-if)#IPV 192.168.9.6 255.255.255.252
R3(config-if)#IPV A 192.168.9.6 255.255.255.252
R3(config-if)#IPV A 192.168.9.6 255.255.255.252D
R3(config-if)#IP AD 192.168.9.6 255.255.255.252
R3(config-if)#IP ADD 192.168.9.6 255.255.255.252
R3(config-if)#IP address 192.168.9.6 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:91::2/64
R3(config-if)#NO SHUtdown
```

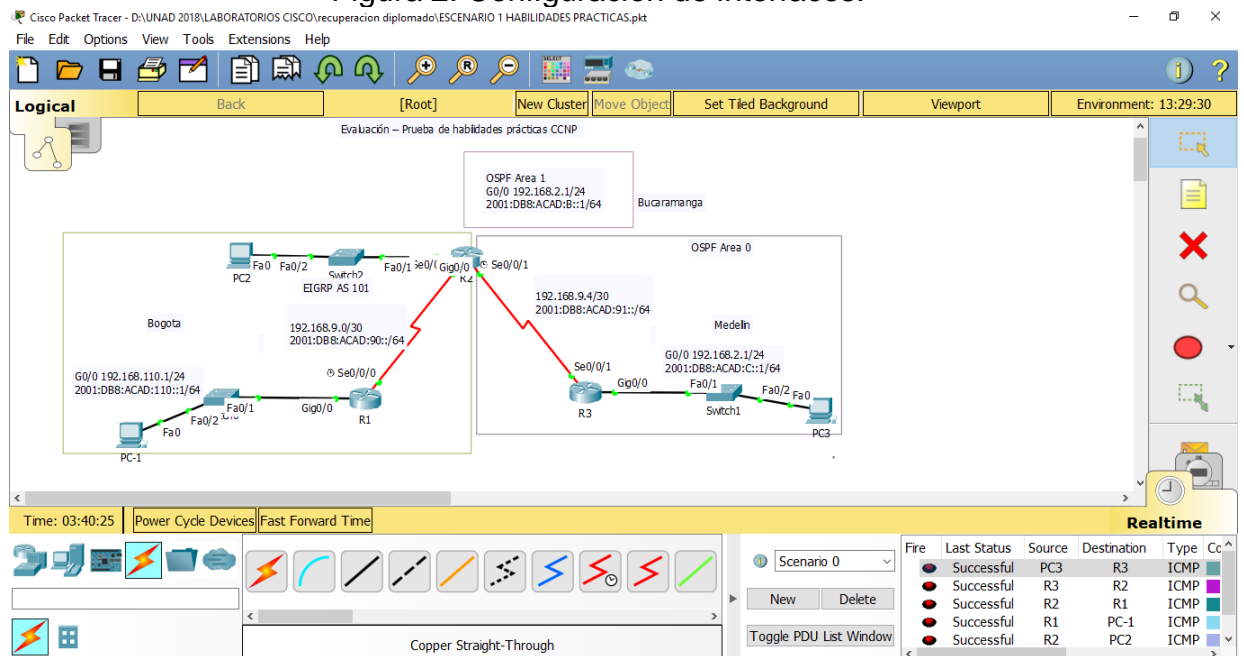
```
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

```
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
```

```
R3(config-if)#EXIT
R3(config)#EXIT
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#W
Building configuration...
[OK]
R3#
R3#
```

Figura 2. Configuración de interfaces.



2. Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.

R1

```
R1(config)#INterface Serial 0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#bandwidth 128
R1(config-if)#no sh
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

R2

```
R2(config)#INterface Serial 0/0/0
R2(config-if)#BAndwidth 128
R2(config-if)#EXIT
R2(config)#EXIT
```

```
R2(config)#INterface Serial 0/0/1
R2(config-if)#CLOC R
R2(config-if)#CLOC Rate 128000
R2(config-if)#BA
R2(config-if)#BAndwidth 128
R2(config-if)#EXIT
R2(config)#
```

R3

```
R3(config)#interface serial 0/0/1
R3(config-if)#b
R3(config-if)#bandwidth 128
R3(config-if)#exit
R3(config)#
```

3. En R2 y R3 configurar las familias de direcciones OSPFv3 para IPv4 e IPv6. Utilice el identificador de enrutamiento 2.2.2.2 en R2 y 3.3.3.3 en R3 para ambas familias de direcciones.
4. En R2, configurar la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3 en OSPF área 0.

R2

```
R2(config)#router ospf 1
R2(config-router)#router
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 192.168.9.0 0.0.0.3 area 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 1
R2(config-router)#exit
```

5. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0.

R3

```
R3#confi term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router
R3(config-router)#router-id 3.3.3.3
R3(config-router)#net
R3(config-router)#network 192.168.9.4 0.0.0.3 area 1
R3(config-router)#net
R3(config-router)#network 192.168.3.0 0.0.0.255
% Incomplete command.
R3(config-router)#network 192.168.3.0 0.0.0.255 area 1
R3(config-router)#exit
```

6. Configurar el área 1 como un área totalmente Stubby.

```
R2>ena
R2# confi term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#area 1 stub
R2(config-router)#exit
R2(config)#
```

7. Propagar rutas por defecto de IPv4 y IPv6 en R3 al interior del dominio OSPFv3. Nota: Es importante tener en cuenta que una ruta por defecto es diferente a la definición de rutas estáticas.
8. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Configurar la interfaz F0/0 de R1 y la conexión entre R1 y R2 para EIGRP con el sistema autónomo 101. Asegúrese de que el resumen automático está desactivado.
9. Configurar las interfaces pasivas para EIGRP según sea apropiado.
10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.

```

R1(config)#router eig
R1(config)#router eigrp 101
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.9.0 0.0.0.3
R1(config-router)#network 192.168.110.0 0.0.0.255
R1(config-router)#network 192.168.2.0 0.0.0.255
R1(config-router)#exit
R1(config)#exit
R1#

```

11. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL.

```

R2(config)#access-list 1 perm 192.168.3.0
R2(config)#access-list 1 perm any
R2(config)#router eigrp 101
R2(config-router)#distribute-list 1 out g0/0

```

Parte 2: Verificar conectividad de red y control de la trayectoria.

- a. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.
- b. Verificar comunicación entre routers mediante el comando ping y traceroute
- c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Figura 3. Validacion de Ping R1.

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows three routers: R1, R2, and R3. R1 is connected to R2, and R2 is connected to R3. R1 is also connected to PC1. The network is configured with EIGRP AS 101. The CLI window for R1 shows the following output:

```

R1#ping 192.168.9.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#ping 192.168.9.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/19/92 ms

R1#
    
```

At the bottom right, a table shows the status of the ping tests:

Fire	Last Status	Source	Destination	Type	Color
●	Failed	R1	R3	ICMP	Green
●	Successful	R1	R2	ICMP	Blue
●	Successful	R3	R2	ICMP	Green

Figura 4. Ping desde R2 a R3 y R1.

The screenshot displays the Cisco Packet Tracer interface. On the left, the network diagram is the same as in Figure 3. The CLI window for R2 shows the following output:

```

R2#PING 192.168.9.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/18/85 ms

R2#PING 192.168.9.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/19/81 ms

R2#PING 192.168.9.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/18/83 ms

R2#
    
```

Figura 5. Ping desde R1 a R2 y R3.

Cisco Packet Tracer - D:\UNAD 2018\LABORATORIOS CISCO\recuperacion diplomado\ESCENARIO 1 HABILIDADES PRACTICAS.pkt

File Edit Options View Tools Extensions Help

Logical Back [Root] New Cluster Move Object Set Tiled Background Viewport Environment: 00:50:00

Evaluación - Prueba de habilidades prácticas CCNP

OSPF Area 1  
G0/0 192.168.2.1/24  
2001:DB8:ACAD:B::1/64 Bucaramanga

OSPF Area 0

Bogota  
192.168.9.0/30  
2001:DB8:ACAD:90::/64

Medellin  
192.168.8.4/30  
2001:DB8:ACAD:91::/64

PC2  
Switch2  
GRP AS 101  
R1  
R3  
Switch1  
PC3

Time: 07:21:38 Power Cycle Devices Fast Forward Time

Scenario 0

New Delete

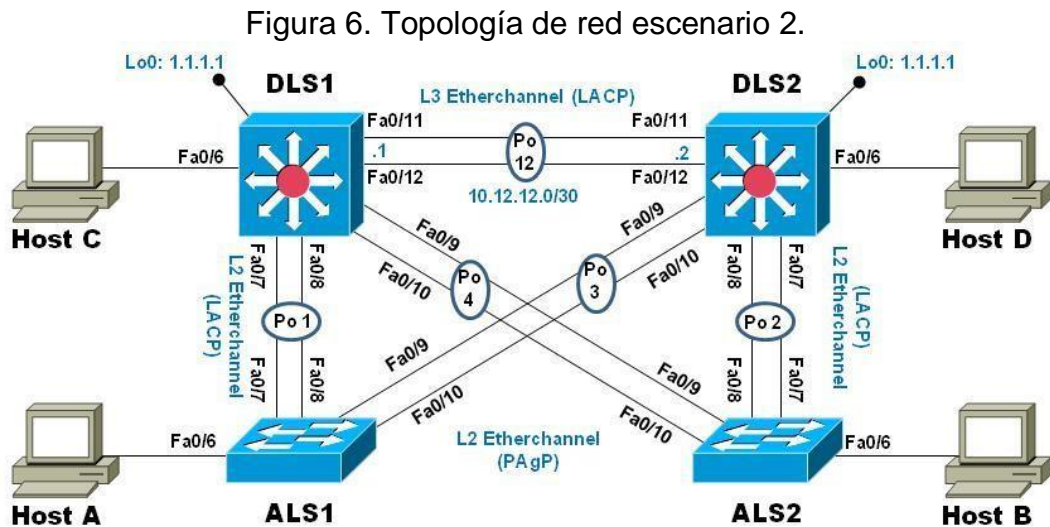
Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color
●	Successful	R3	R2	ICMP	Green
●	Successful	R1	R2	ICMP	Blue
●	Successful	R1	PC-1	ICMP	Purple
●	Successful	R2	PC2	ICMP	Light Blue

Copper Straight-Through

## 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.



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

- a. Apagar todas las interfaces en cada switch.
- b. Asignar un nombre a cada switch acorde al escenario establecido.
- 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.
  2. Los Port-channels en las interfaces Fa0/7 y Fa0/8 utilizarán LACP.
  3. Los Port-channels en las interfaces Fa0/9 y Fa0/10 utilizará PAgP.
  4. Todos los puertos troncales serán asignados a la VLAN 800 como la VLAN nativa.
- d. Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 3
  1. Utilizar el nombre de dominio UNAD con la contraseña cisco123
  2. Configurar DLS1 como servidor principal para las VLAN.

3. Configurar ALS1 y ALS2 como clientes VTP.
- e. Configurar en el servidor principal las siguientes VLAN:

Tabla 1. Listado de VLANs.

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
800	NATIVA	434	ESTACIONAMIENTO
12	EJECUTIVOS	123	MANTENIMIENTO
234	HUÉSPEDES	1010	VOZ
1111	VIDEONET	3456	ADMINISTRACIÓN

- f. En DLS1, suspender la VLAN 434.
- g. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión 2, y configurar en DLS2 las mismas VLAN que en DLS1.
- h. Suspender VLAN 434 en DLS2.
- i. En DLS2, crear VLAN 567 con el nombre de CONTABILIDAD. La VLAN de CONTABILIDAD no podrá estar disponible en cualquier otro Switch de la red.
- j. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 800, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.
- k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 800, 1010, 1111 y 3456.
- 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 éstos puertos.
- m. Configurar las siguientes interfaces como puertos de acceso, asignados a las VLAN de la siguiente manera:

Tabla 2. Interfaces como puertos de acceso.

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	N/A	567	N/A	N/A

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
- b. Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente
- c. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN.

Implementación

```
Switch(config)#interface fastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

DLS2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname DLS2
DLS2(config)#INTerface fastEthernet 0/1
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport port-security maximum 1
DLS2(config-if)#exit
DLS2(config)#exit
DLS2#
%SYS-5-CONFIG_I: Configured from console by console
```

DLS2#

ALS1

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

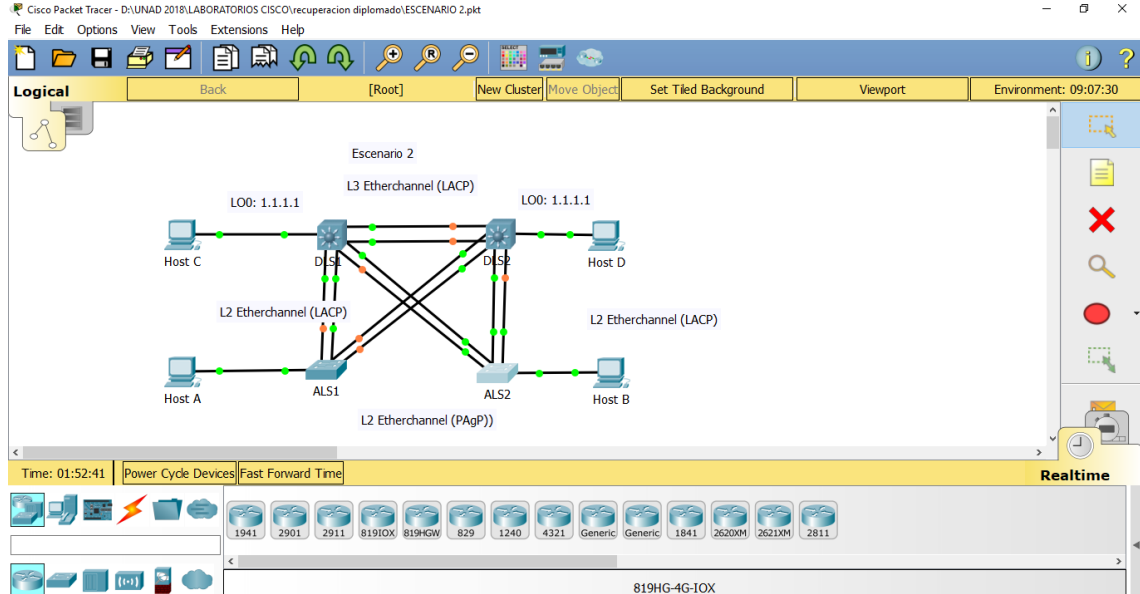
```
Switch(config)#hostname ALS1
ALS1(config)#INterface fastEthernet 0/1
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport port-security maximum 1
ALS1(config-if)#EXIT
ALS1(config)#EXIT
ALS1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
ALS1#
```

```
ALS2
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname ALS2
ALS2(config)#INterface fastEthernet 0/1
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport port-security maximum 1
ALS2(config-if)#EXIT
ALS2(config)#EXIT
ALS2#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 7. ALS2#.



Puertos troncales y vlan nativa 800

ALS1

ALS1#

ALS1#CONF TERM

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#vtp mode ser

ALS1(config)#vtp mode server

Device mode already VTP SERVER.

ALS1(config)#int ran f0/7-12

ALS1(config-if-range)#switchport trunk native vlan 800

ALS1(config-if-range)#switchport trunk allowed vlan except 1999

ALS1(config-if-range)#switchport mode trunk

ALS1(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

ALS1(config-if-range)#switchport nonegotiate

ALS1(config-if-range)#no shutdown

ALS1(config-if-range)#exit

ALS1(config)#

ALS1(config)#

ALS2

ALS2(config)#vtp mode server

Device mode already VTP SERVER.

ALS2(config)#int ran f0/7-12

ALS2(config-if-range)#int ran f0/6-12

ALS2(config-if-range)#switchport trunk native vlan 800

ALS2(config-if-range)#switchport trunk allowed vlan except 1999

ALS2(config-if-range)#switchport mode trunk

ALS2(config-if-range)#

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

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

ALS2(config-if-range)#switchport nonegotiate

ALS2(config-if-range)#NO SHUTDOWN

ALS2(config-if-range)#

ALS2(config-if-range)#EXIT

ALS2(config)#EXIT

ALS2#

%SYS-5-CONFIG\_I: Configured from console by console

DLS1 SITCH 3560 CISCO

Switch(config)#vtp mode server

Device mode already VTP SERVER.

```
Switch(config)#int ran f0/6-12
Switch(config-if-range)#switchport trunk native vlan 800
Switch(config-if-range)#switchport trunk allowed vlan except 1999
Switch(config-if-range)#%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q
BPDU on non trunk FastEthernet0/9 VLAN800.
```

%SPANTREE-2-BLOCK\_PVID\_LOCAL: Blocking FastEthernet0/9 on VLAN0800.  
Inconsistent port type.

%SPANTREE-2-RECV\_PVID\_ERR: Received 802.1Q BPDU on non trunk  
FastEthernet0/10 VLAN800.

%SPANTREE-2-BLOCK\_PVID\_LOCAL: Blocking FastEthernet0/10 on VLAN0800.  
Inconsistent port type.

```
Switch(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#switchport nonegotiate
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
```

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Switch(config-if-range)#no shutdown

Switch(config-if-range)#exit

Switch(config)#exit

Switch#

%SYS-5-CONFIG\_I: Configured from console by console

Switch#

DLS2

DLS2(config)#vtp mode server

Device mode already VTP SERVER.

DLS2(config)#int ran f0/6-12

DLS2(config-if-range)#switchport trunk native vlan 800

DLS2(config-if-range)#switchport trunk allowed vlan except 1999

DLS2(config-if-range)#%SPANTREE-2-RECV\_PVID\_ERR: Received 802.1Q BPDUs on non trunk FastEthernet0/8 VLAN800.

%SPANTREE-2-BLOCK\_PVID\_LOCAL: Blocking FastEthernet0/8 on VLAN0800. Inconsistent port type.

%SPANTREE-2-RECV\_PVID\_ERR: Received 802.1Q BPDUs on non trunk FastEthernet0/7 VLAN800.

%SPANTREE-2-BLOCK\_PVID\_LOCAL: Blocking FastEthernet0/7 on VLAN0800. Inconsistent port type.

switchport mode trunk

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.

DLS2(config-if-range)#

DLS2(config-if-range)#switchport nonegotiate

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.

DLS2(config-if-range)#NO SHU

DLS2(config-if-range)#NO SHUtdown

DLS2(config-if-range)#EXIT

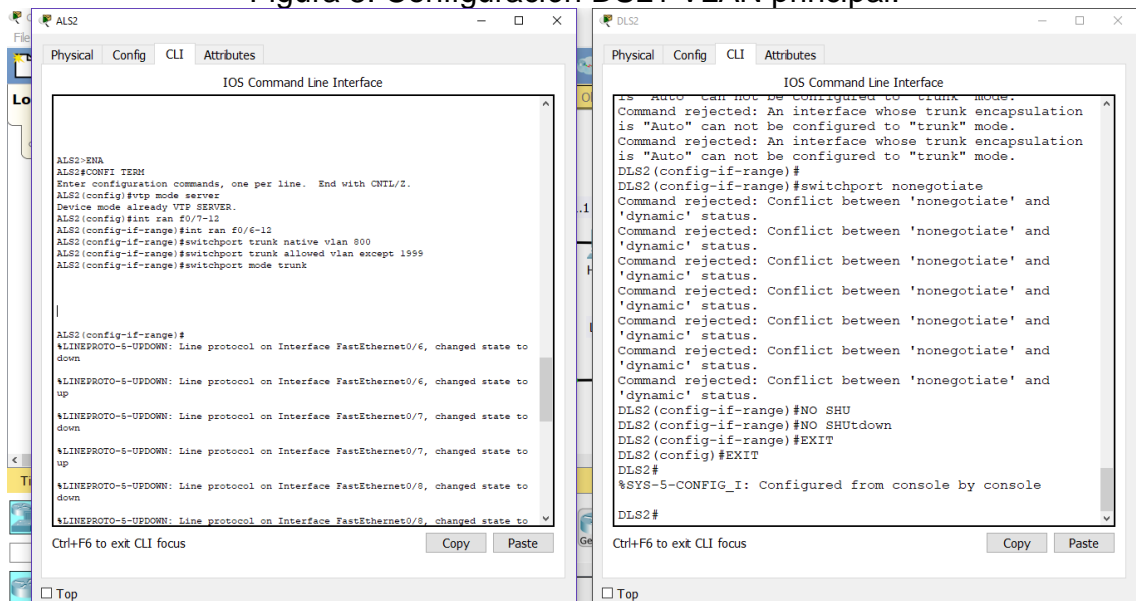
DLS2(config)#EXIT

DLS2#

%SYS-5-CONFIG\_I: Configured from console by console

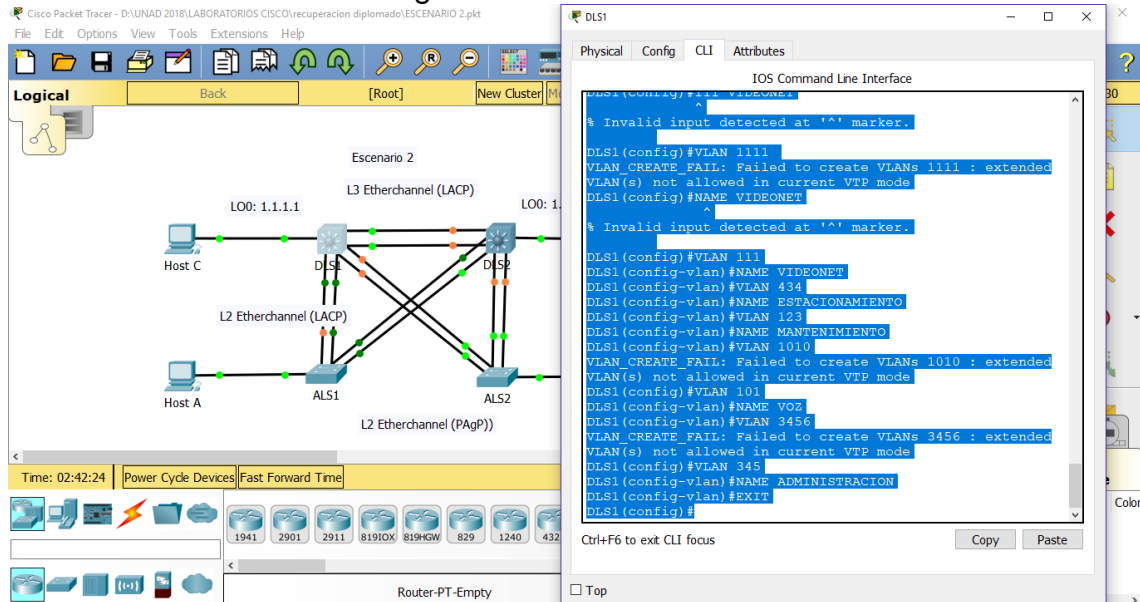
DLS2#

Figura 8. Configuración DSL1 VLAN principal.



```
Switch(config)#hostname DLS1
DLS1(config)#VLAN 800
DLS1(config-vlan)#NAME NATIVA
DLS1(config-vlan)#VLAN 12
DLS1(config-vlan)#NAME EJECUTIVOS
DLS1(config-vlan)#VLAN 234
DLS1(config-vlan)#NAME HUESPEDES
DLS1(config-vlan)#VLAN 1111
VLAN_CREATE_FAIL: Failed to create VLANs 1111 : extended VLAN(s) not
allowed in current VTP mode
DLS1(config)#111 VIDEONET
DLS1(config)#VLAN 1111
VLAN_CREATE_FAIL: Failed to create VLANs 1111 : extended VLAN(s) not
allowed in current VTP mode
DLS1(config)#NAME VIDEONET
DLS1(config)#VLAN 111
DLS1(config-vlan)#NAME VIDEONET
DLS1(config-vlan)#VLAN 434
DLS1(config-vlan)#NAME ESTACIONAMIENTO
DLS1(config-vlan)#VLAN 123
DLS1(config-vlan)#NAME MANTENIMIENTO
DLS1(config-vlan)#VLAN 1010
VLAN_CREATE_FAIL: Failed to create VLANs 1010 : extended VLAN(s) not
allowed in current VTP mode
DLS1(config)#VLAN 101
DLS1(config-vlan)#NAME VOZ
DLS1(config-vlan)#VLAN 3456
VLAN_CREATE_FAIL: Failed to create VLANs 3456 : extended VLAN(s) not
allowed in current VTP mode
DLS1(config)#VLAN 345
DLS1(config-vlan)#NAME ADMINISTRACION
DLS1(config-vlan)#EXIT
DLS1(config)#
```

Figura 9. Interfaces VLAN.



DSL1

CONFI TERM

Enter configuration commands, one per line. End with CNTL/Z.

DLS1(config)#int

DLS1(config)#interface vlan 1

DLS1(config-if)#ip ad

DLS1(config-if)#ip address 10.12.12.1 255.255.255.252

DLS1(config-if)#no shut

DLS1(config-if)#no shutdown

DLS1(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up  
exit

DLS1(config)#exit

DLS1#

DSL2

DLS2(config)#interface vl

DLS2(config)#interface vlan 1

```
DLS2(config-if)#ip ad
DLS2(config-if)#ip address 10.12.12.2 255.255.255.252
DLS2(config-if)#exit
DLS2(config)#exit
DLS2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
DLS2#
DLS2#
DLS2#confi term
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#int
DLS2(config)#interface v
DLS2(config)#interface vl
DLS2(config)#interface vlan 1
DLS2(config-if)#no su
DLS2(config-if)#no sut
DLS2(config-if)#no sh
DLS2(config-if)#no shutdown
```

```
DLS2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
DLS2(config-if)#
DLS2(config-if)#
DLS2(config-if)#exit
DLS2(config)#
DLS2(config)#
DLS2(config)#exit
DLS2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
DLS2#
DLS2#w
Building configuration...
[OK]
DLS2#
```

Figura 10. Host A.

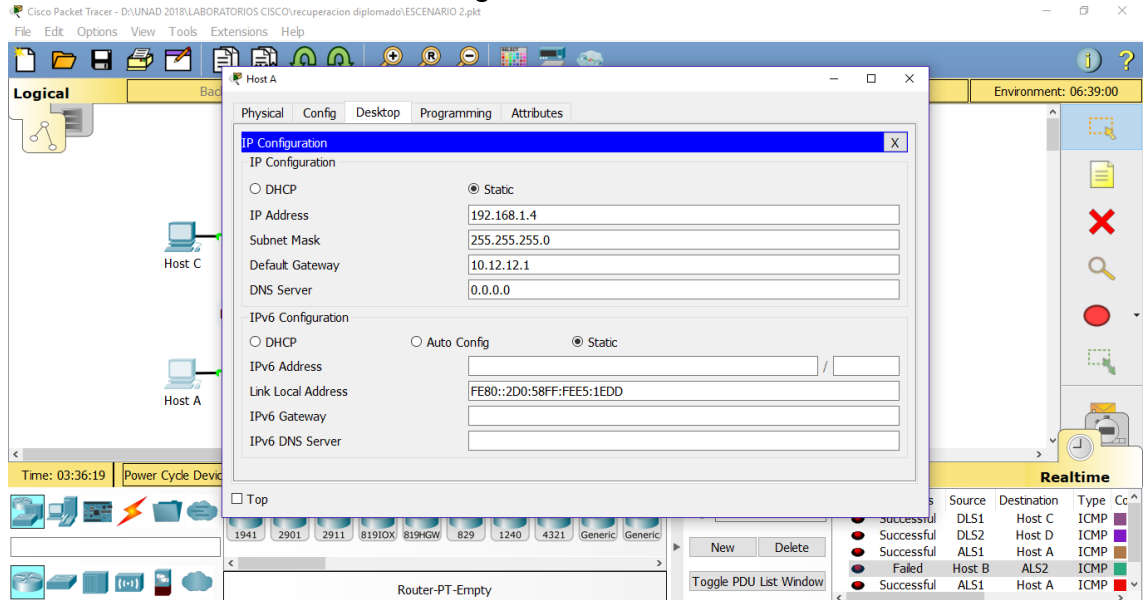


Figura 11. Host B.

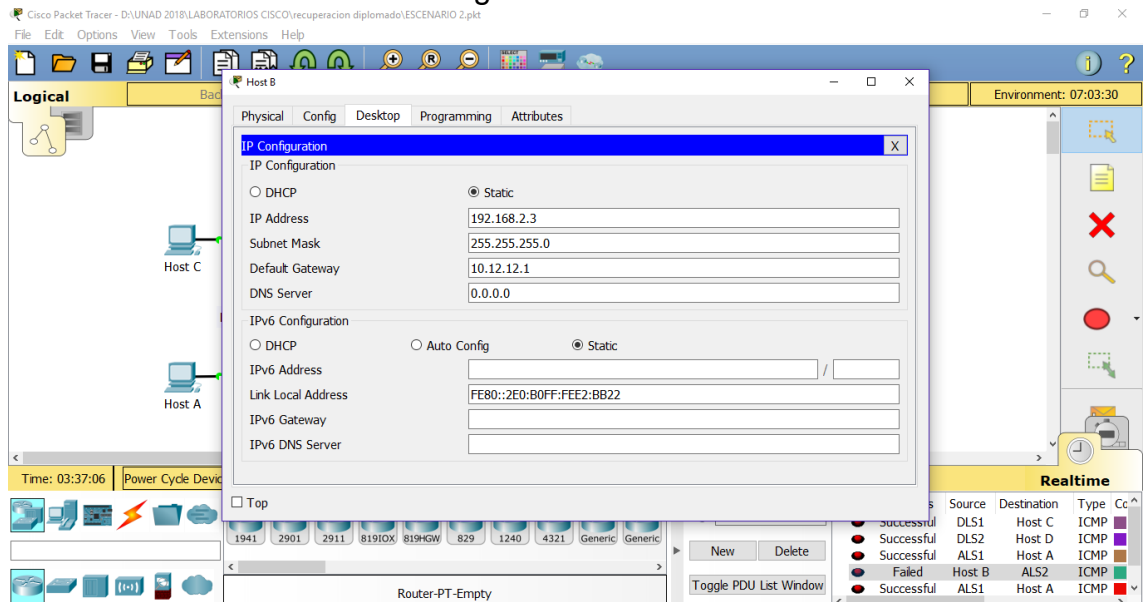


Figura 12. Host C.

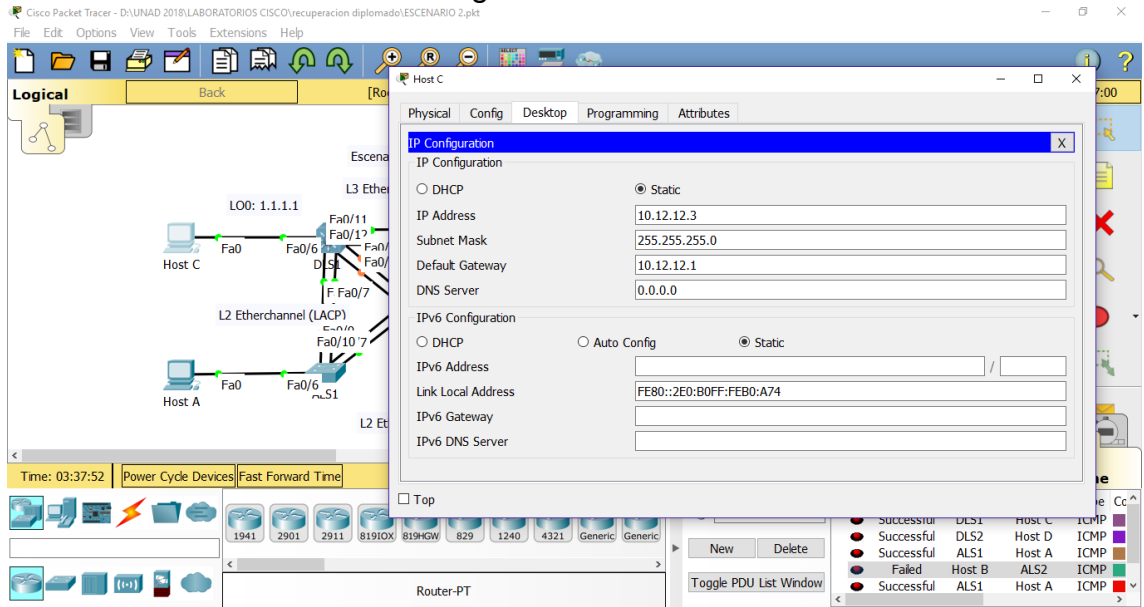
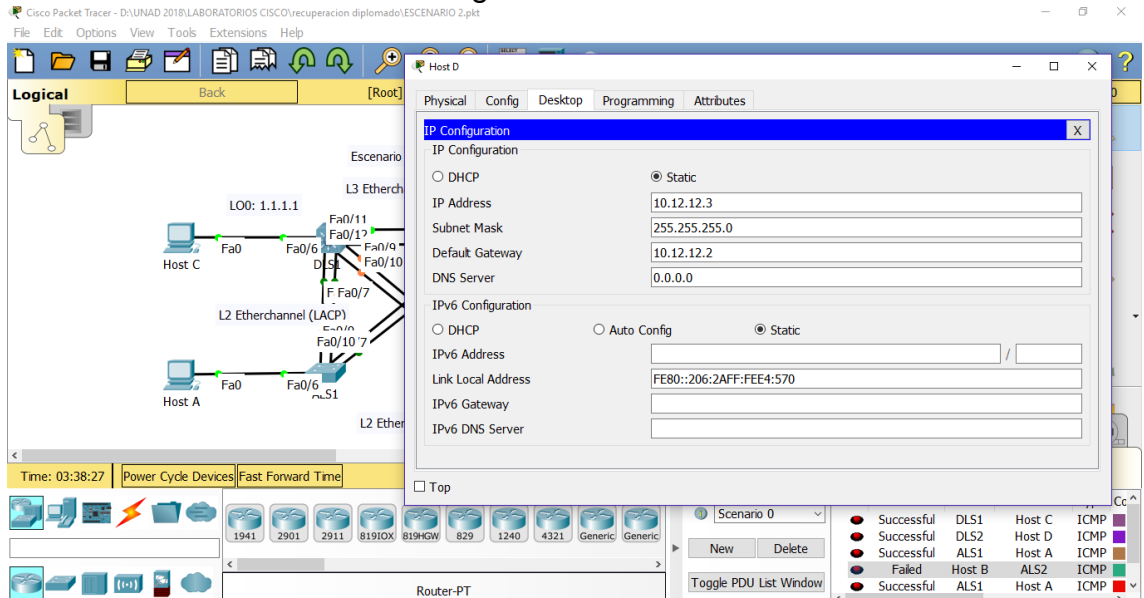


Figura 13. Host D:



## Topología en red ADSL principal

ALS1

```
ALS1(config)#interface vl
ALS1(config)#interface vlan 1
ALS1(config-if)#ip address 192.168.1.1 255.255.255.0
ALS1(config-if)#exit
ALS1(config)#exit
ALS1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
ALS1#confi term
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#interface vlan 1
ALS1(config-if)#no shutdown
```

ALS2

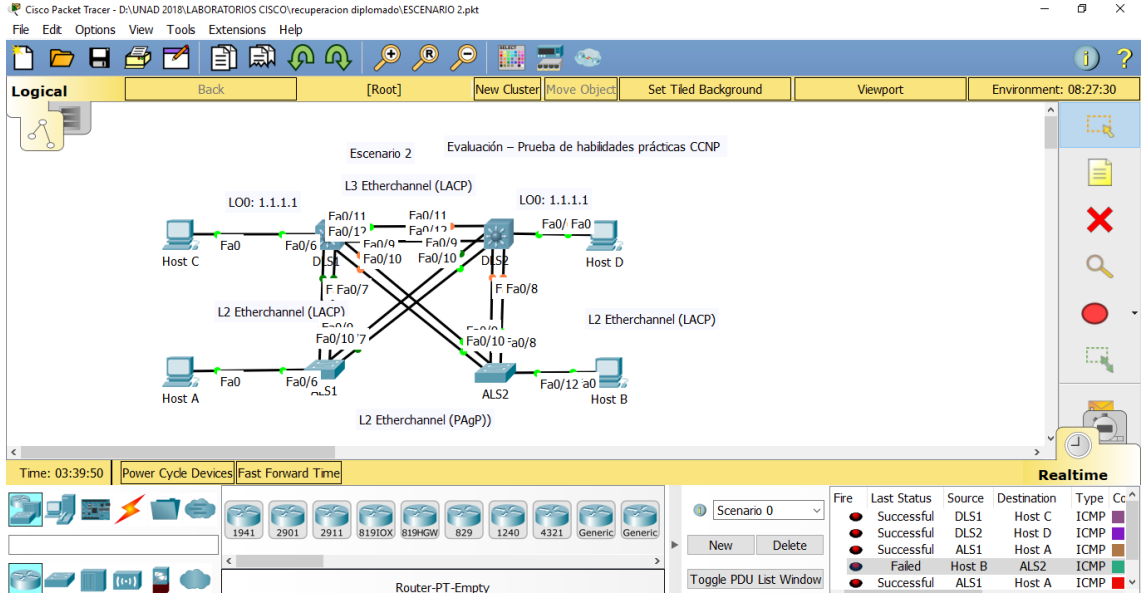
```
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface vlan 1
ALS2(config-if)#ip address 192.168.2.1 255.255.255.0
ALS2(config-if)#no shutdown
```

```
ALS2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
ALS2(config-if)#
ALS2(config-if)#exit
```

Figura 14. Topología en red VLAN ADSL principal.



## CONCLUSIONES

Se establecieron los niveles de seguridad básicos a través de la definición de criterios y políticas de seguridad aplicados en dos escenarios de red, bajo el uso de estrategias hardware y software, protegiendo la integridad de la información frente a cualquier tipo de ataque que se pueda presentar; en especial en soluciones de red que involucren el uso de aplicaciones cliente-servidor.

Los conocimientos necesarios para el diseño de redes escalables se fortalecieron mediante el uso del modelo jerárquico de tres niveles, la optimización en el rendimiento de la red e incorporación adecuada de tecnologías y protocolos de conmutación mejorados tales como: VLAN, protocolo de enlace troncal de VLAN (VTP), protocolo rápido de árbol de expansión (Rapid Spanning Tree Protocol - RSTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encapsulamiento por 802.1q.

Desarrollar la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos estableciendo alternativas a problemas de interconectividad.

## BIBLIOGRAFÍA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de <https://1drv.ms/b/s!AglGg5JUgUBthFt77ehzL5qp0OKD>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Security. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). High Availability. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

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!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>

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!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

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!AmlJYei-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!AmlJYei-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!AmlJYei-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!AmlJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-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!AmlJYei-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!AmlJYei-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!AmlJYei-NT1IlnMfy2rhPZHwEoWx>

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC>

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de [https://1drv.ms/u/s!AmlJYei-NT1IhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmlJYei-NT1IhgOyjWeh6timi_Tm)

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IlyYRohwtwPUV64dg>

UNAD (2015). Switch CISCO Security Management [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IlyVeVJCCezJ2QE5c>

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AglGg5JUgUBthFx8WOxiq6LPJppl>