DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANGELA JINETH SABOGAL ORTIZ

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANGELA JINETH SABOGAL ORTIZ

Diplomado de opción de grado presentado para optar el título de INGENIERIA 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

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 12 de diciembre de 2019

AGRADECIMIENTOS

Agradezco a la inspiración ese gran motor que conlleva a realizar cada uno de los propósitos, a la necesidad que nos abre el mundo a buscar soluciones y mitigar con barreras, y al amor que tenemos por cada uno de nuestros sueños logrando objetivos exitosos.

Al finalizar este trabajo quiero agradecer a Dios por todas sus bendiciones, a mis Padres que han sabido darme su ejemplo de trabajo y honradez por su apoyo y paciencia en este proyecto.

También quiero agradecer a la Universidad Nacional Abierta y a Distancia, directivos y profesores por la organización de cada uno de sus programas.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Los temas tratados en el curso de CCNP se trata de routing, switching y troubleshooting de forma más específica. Inicialmente se verán aplicados los temas de switching, y routing por medio de topologías donde se configuran protocolos que ayuda a optimizar la seguridad en la red, o hacerla más versátil a la hora de usar diferentes escenarios, se configurara redes simulando entorno real, donde estarán configuradas por medio de ciudades, VLAN, seguridad de puertos, asignación de IPV4 e IPV6. De esta manera se ponen en practica los recursos de redes e interconexiones usando los protocolos más eficientes y validando cada una de las configuraciones de red.

Palabras Clave: CISCO, OSPF, VLAN, redes, seguridad, escalabilidad, protocolos.

ABSTRACT

The topics covered in the CCNP course are about routing, change and problem solving more specifically. Initially you will see applications applied to the topics of switching, and routing through topologies where protocols are configured that help modify security in the network, or make it more versatile when using different movements, networks are configured simulating real environment, where directly configured through cities, VLANs, port security, IPV4 and IPV6 allocation. In this way, network and interconnection resources will be implemented using the most efficient protocols and validating each of the network configurations.

Keywords: CISCO, OSPF, VLAN, networks, security, scalability, protocols.

INTRODUCCIÓN

En el presente trabajo escrito se describen las diferentes temáticas vistas en el curso CCNP switch II-2019 y CCNP route II, poniendo en práctica conceptos y protocolos de enrutamiento por medio de dos (2) escenarios de red, donde se generaliza los protocolos de enrutamiento como OSPF, EIGRP, BGP, configuración de puertos en switches con sus datos de red y vlan. El software usado en cisco packet tracert donde también se validan las diferentes configuraciones. Se realiza ilustraciones del paso a paso donde se pueden evidenciar las diferentes configuraciones y enlaces de red, funcionalidades y demás aspectos importantes sobre enrutamiento y conectividad.

Descripción general de la prueba de habilidades

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. Escenario 1

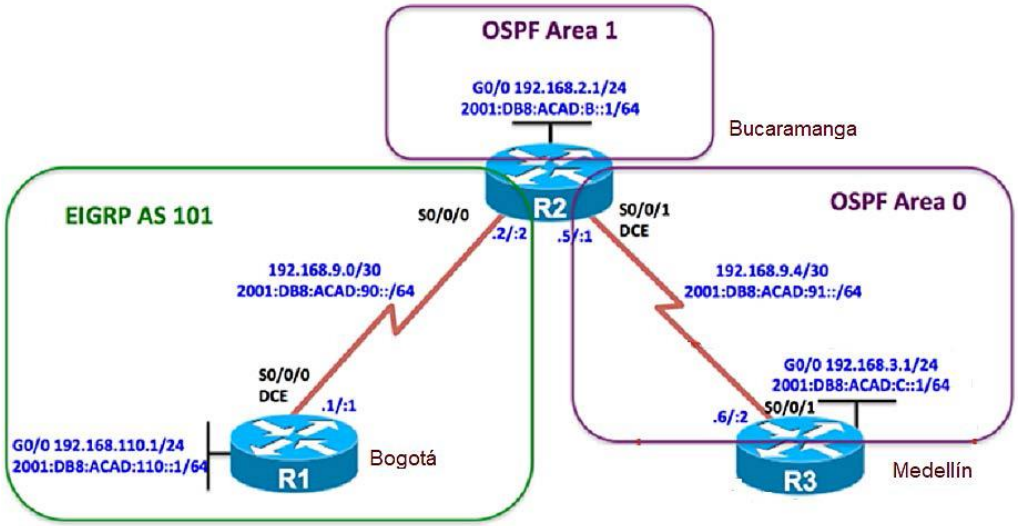
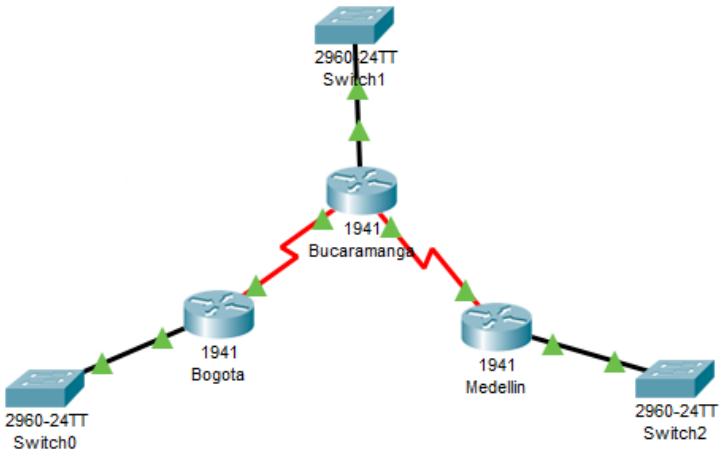


Figura 2. Simulación del escenario 1



Parte 1: Configuración del escenario propuesto

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

Código de configuración aplicado

```
enable
configure terminal
hostname Bogota
interface GigabitEthernet0/0
ip address 192.168.110.1 255.255.255.0
ipv6 address 2001:db8:acad:110::1/64
no sh
interface serial0/0/0
ip address 192.168.9.1 255.255.255.252
ipv6 address 2001:db8:acad:90::1/64
clock rate 128000
bandwidth 128

enable
configure terminal
hostname Bucaramanga
interface GigabitEthernet0/0
ip address 192.168.2.1 255.255.255.0
ipv6 address 2001:db8:acad:b::1/64
interface serial0/0/0
ip address 192.168.9.2 255.255.255.252
```

ipv6 address 2001:db8:acad:90::1/64
bandwidth 128
no sh
ip address0/0/1
ip address 192.168.9.5 255.255.255.252
ipv6 address 2001:db8:acad:91::1/64
bandwidth 128

enable
configure terminal
hostname Medellin
interface GigabitEthernet0/0
ip address 192.168.3.1 255.255.255.0
ipv6 address 2001:db8:acad:c::1/64
interface serial0/0/1
ip address 192.168.9.6 255.255.255.252
ipv6 address 2001:db8:acad:91::2/64
bandwidth 128

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.

Código de configuración aplicado

Bogota_interface serial0/0/0
ip address 192.168.9.1 255.255.255.252
ipv6 address 2001:db8:acad:90::1/64
clock rate 128000
bandwidth 128

Bucaramanga_ interface serial0/0/0
bandwidth 128
interface serial0/0/1
bandwidth 128
clock rate 128000
exit

Medellin_interface serial0/0/1
ip address 192.168.9.6 255.255.255.252
ipv6 address 2001:db8:acad:91::2/64
bandwidth 128

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.

Código de configuración aplicado

```
Bucaramaga_router ospf 1
address-family ipv4 unicast
router-id 2.2.2.2
exit
ipv6 router ospf 1
router-id 2.2.2.2

Medellin_ipv6 unicast-routing
ipv6 router ospf 1
router-id 3.3.3.3
passive-interface gigabitEthernet0/0
exit
```

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.

Código de configuración aplicado

```
Bucaramanga_interface serial0/0/1
ospf 1 ipv4 area 1

Medellin_interface gigabitEthernet0/0
ospfv3 1 ipv4 area 1
```

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

Código de configuración aplicado

```
Bucaramanga_router ospf 1
area 1 stub no-summary
exit
ipv6 router ospf 1
area 1 stub no-summary
exit
ipv6 router ospf 1
area 1 stub no-summary
exit
```

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.

Código de configuración aplicado

```
Medellin_router ospf 1
default-information originate
exit
ipv6 router ospf 1
default-information originate
exit
```

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.

Código de configuración aplicado

```
Bogota_router eigrp 101
network 192.168.9.0 0.0.0.3
network 192.168.110.0 0.0.0.255
eigrp router-id 1.1.1.1
exit
ipv6 router eigrp 101
eigrp router-id 1.1.1.1
exit
```

9. Configurar las interfaces pasivas para EIGRP según sea apropiado.

Código de configuración aplicado

```
Bogota_interface gigabitEthernet0/0
passive-interface
```

10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.

Código de configuración aplicado

```
Bucaramanga_router eigrp 101
redistribute ospf 1 metric 1500 100 255 1 1500
exit
ipv6 router eigrp 101
redistribute ospf 1 metric 1500 100 255 1 1500
exit
```

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

Código de configuración aplicado

```
Bucaramanga_access-list 1 deny 192.168.3.0 0.0.0.255
access-list 1 permit deny
```

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.

Código de configuración aplicado

```
Show ip route
Show ip protocols
```

Figura 3. Validación de tablas de enrutamiento

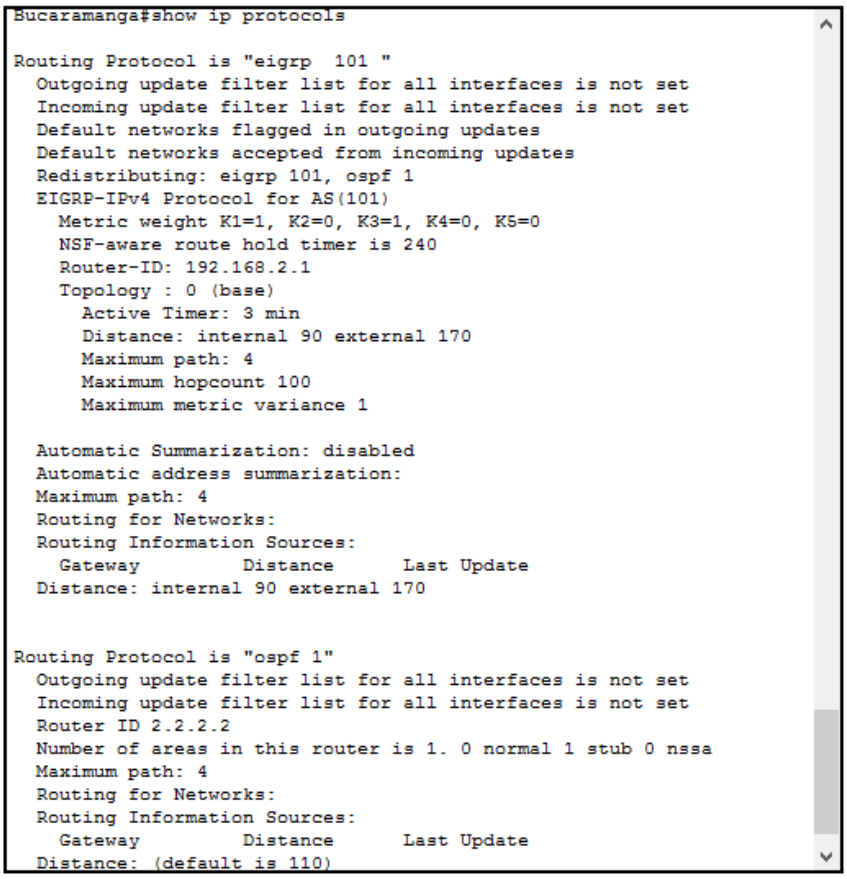
```
Bogota#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.9.0/30 is directly connected, Serial0/0/0
L       192.168.9.1/32 is directly connected, Serial0/0/0

Bogota#
```

```
Bogota#show ip protocols

Routing Protocol is "eigrp  101 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 101
  EIGRP-IPv4 Protocol for AS(101)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     192.168.9.0/30
     192.168.110.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170

Bogota#
```

Código de configuración aplicado

Show ip protocols

Figura 4. Validación de tablas protocolos configurados

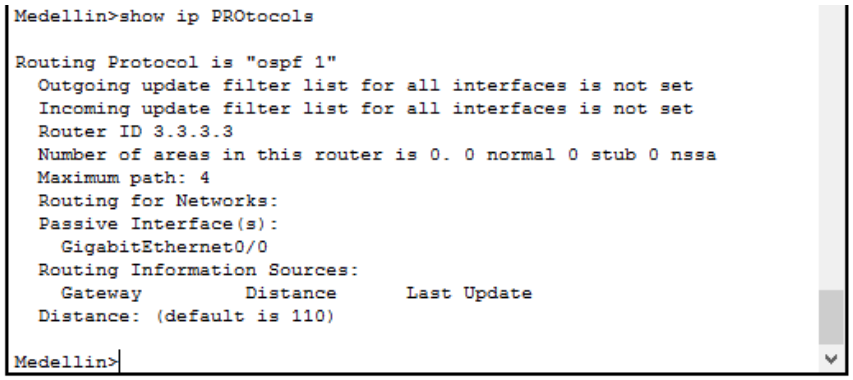


```
Bucaramanga#show ip protocols

Routing Protocol is "eigrp  101 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 101, ospf 1
  EIGRP-IPv4 Protocol for AS(101)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.2.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170


Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 0 normal 1 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

Código de configuración aplicado

Show ip protocols

Figura 5. Validación de protocolos configurados



```
Medellin>show ip PROtocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

Medellin>
```

b. Verificar comunicación entre routers mediante el comando ping y traceroute

Figura 6.Se aplica verificación de conectividad con comando Ping en R1

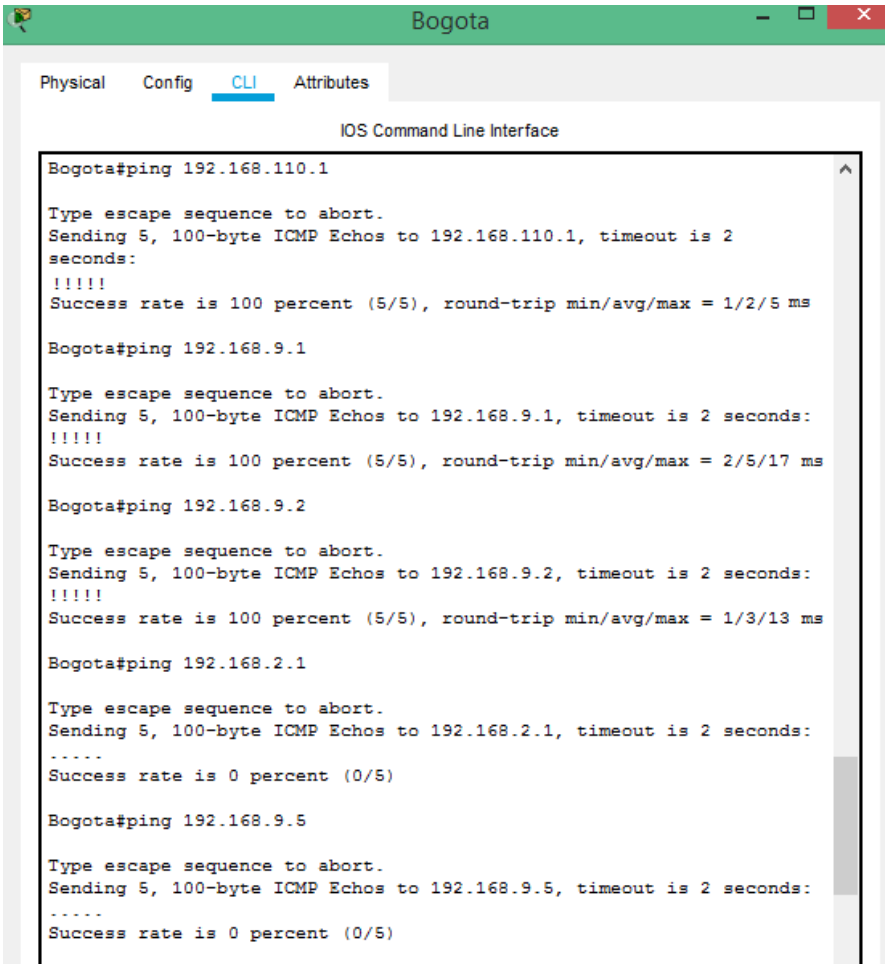


Figura 7. Se aplica verificación de conectividad con comando Ping en R1

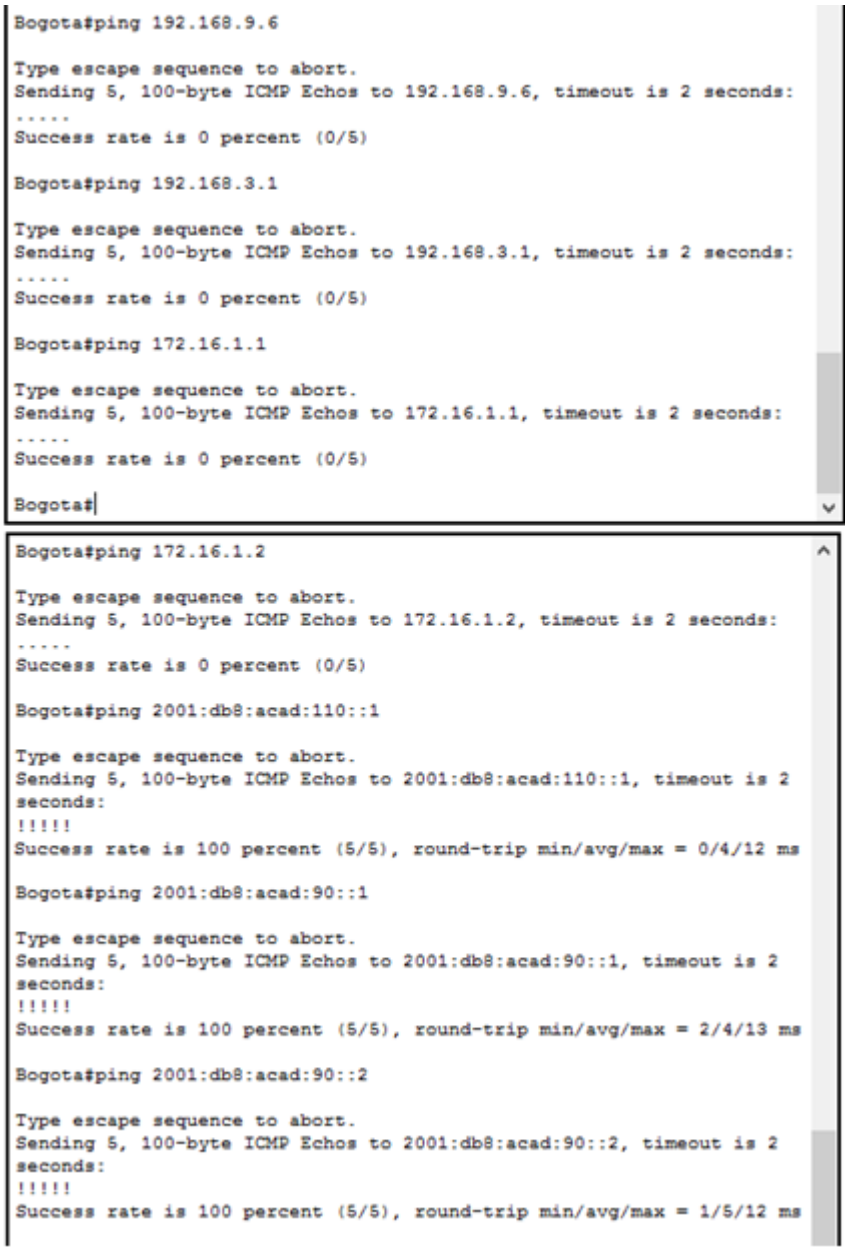
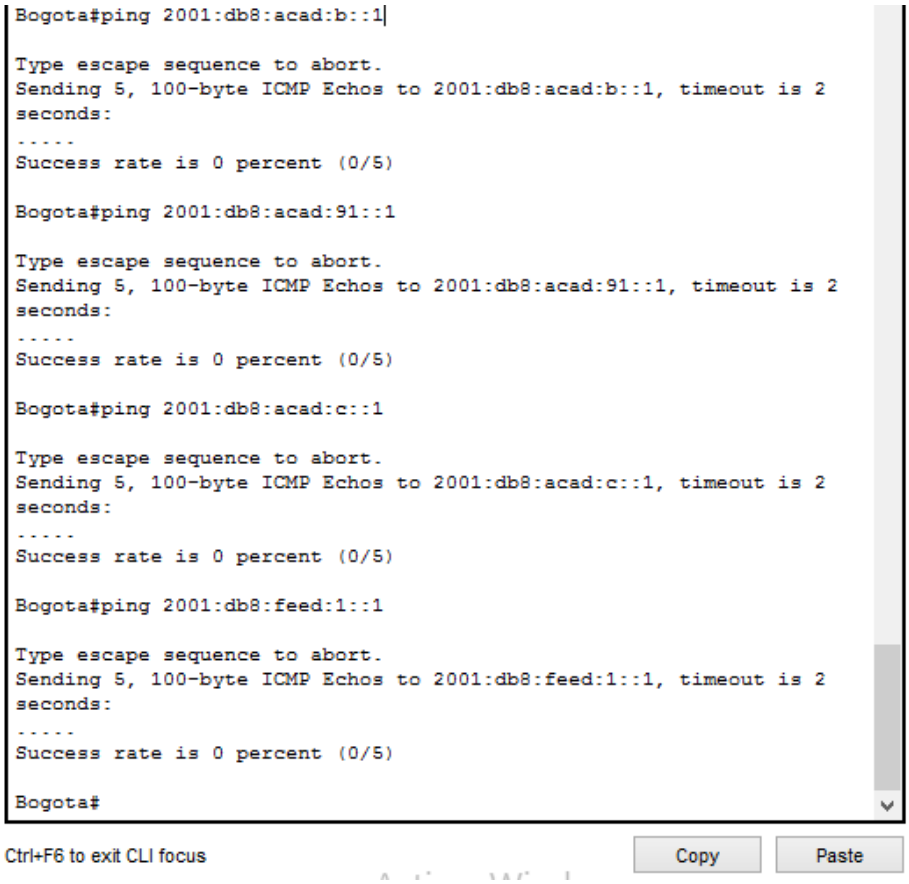


Figura 8. Se aplica verificación de conectividad con comando Ping en R1



c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Figura 9.Se aplica verificación show ip route en R1

```
Bogota#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

     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.9.0/30 is directly connected, Serial0/0/0
L       192.168.9.1/32 is directly connected, Serial0/0/0

Bogota#
```

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.

Figura 10.Escenario 2

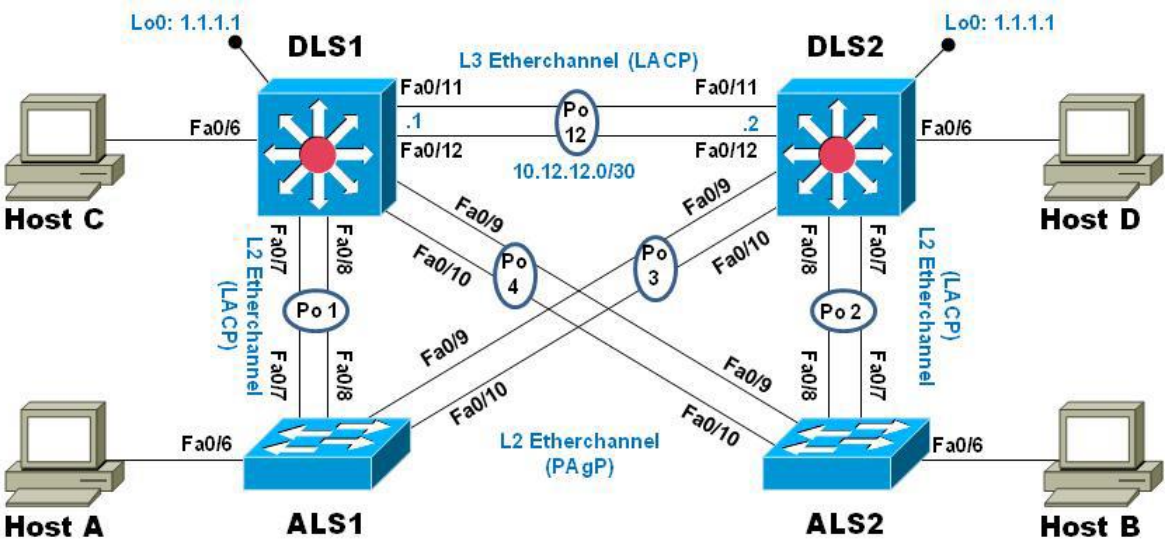
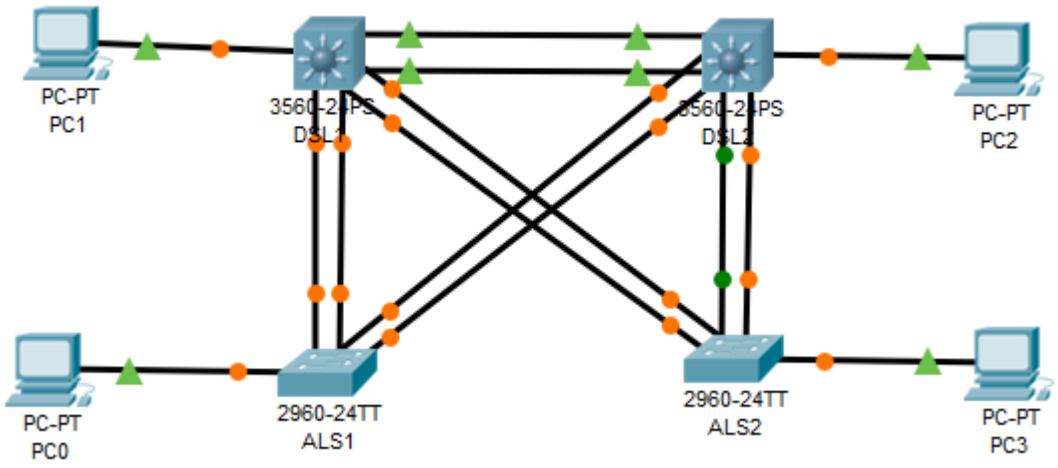


Figura 11.Simulación del escenario 2



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.

Código de configuración aplicado

```
enable
configure terminal
hostname DSL1
int ran f0/1-24, g0/1-2
shutdown
```

Código de configuración aplicado

```
DSL1_int ran f0/11-12
no switchport
channel-group 12 mode active
no shutdown
```

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 F0/9 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

Código de configuración aplicado

```
Enable
configure terminal
hostname ALS1
vtp mode client
vtp domain UNAD
vtp domain UNAD
vtp password cisco123
exit
```

```
Enable
configure terminal
hostname ALS2
vtp mode client
vtp mode client
vtp domain UNAD
vtp domain UNAD
vtp password cisco123
vtp password cisco123
exit
```

2) Configurar DLS1 como servidor principal para las VLAN.

Código de configuración aplicado

```
DSL1_vtp mode transparent
vlan 800
name NATIVE
vlan 12
name EJECUTIVOS
vlan 234
name HUESPEDES
vlan 1111
name VIDEONET
vlan 434
name ESTACIONAMIENTO
vlan 123
name MANTENIMIENTO
vlan 1010
name VOZ
vlan 3456
name ADMINISTRACION
exit
```

```
DSL2_vtp mode transparent
vtp version 2
vlan 800
name NATIVA
exit
vlan 12
name EJECUTIVOS
exit
vlan 234
name HUESPEDES
exit
vlan 1111
name VIODEONET
exit
vlan 434
name ESTACIONAMIENTO
exit
vlan 123
name MANTENIMIENTO
exit
```

vlan 1010
name VOZ
exit
vlan 3456
name ADMINISTRACION
exit

DSL1_interface ran f0/11-12
channel-group 12 mode active
exit
interface port-channel 12
ip address 10.12.12.1 255.255.255.252
exit
int ran f0/7-10
switchport trunk encapsulation dot1q
switchport trunk native vlan 800
switchport mode trunk
switchport nonegotiate
no shutdown

DSL1_exit
int ran f0/7-8
desc member of po1 to ASL1
channel-group 1 mode active
creating a port-channel interface Port-Channel 1

DSL1_exit
int ran f0/9-10
desc member of po4 to ALS2
channel-group 4 mode desirable
creating a port-channel interface Port-Channel 4

DSL2_int ran f0/11-12
no switchport
channel-group 12 mode active
no shutdown
exit
interface port-channel 12
ip address 10.12.12.2 255.255.255.252
exit

DSL2_int ran f0/7-10
switchport trunk encapsulation dot1q

switchport trunk native vlan 800
switchport mode trunk
switchport nonegiate
no shutdown

DSL2_exit
int ran f0/7-8
desc member of po1 to ASL2
channel-group 2 mode active

DSL2_exit
int ran f0/9-10
desc member of po3 to ASL1
channel-group 3 mode desirable
exit

3) Configurar ALS1 y ALS2 como clientes VTP.

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 1. VLAN Escenario 2

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
800	NATIVA	434	ESTACIONAMIENTO
12	EJECUTIVOS	123	MANTENIMIENTO
234	HUESPEDES	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.

Código de configuración aplicado

ALS1_int ran f0/7-10
switchport trunk native vlan 800
switchport mode trunk
switchport nonegotiate
no shutdown
exit
int ran f0/7-8
desc member of po1 to DSL1

ALS1_channel-group 1 mode active
Creating a port-channel interface Port-channel 1
switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
no shutdown
exit
int ran f0/9-10
desc member of po 3 to DSL2
channel-group 3 mode desirable
Creating a port-channel interface Port-channel 3

ALS1_switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
no shutdown
exit
int vlan 3456
ip address 10.34.56.101 255.255.255.0
no shutdown
exit
ip default-gateway 10.34.56.254

ALS2_int ran f0/7-10
switchport trunk native vlan 800
switchport mode trunk
switchport nonegotiate
exit
int ran f0/7-8
desc member of po2 to DSL2
channel-group 2 mode active
Creating a port-channel interface Port-channel 2

ALS2_switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
no shutdown
exit

int ran f0/9-10
desc member of po 4 to DSL1
channel-group 4 mode desirable
Creating a port-channel interface Port-channel 4

ALS2_switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
no shutdown
exit
int vlan 3456
ip add 10.34.56.102 255.255.255.0
no shutdown
exit
ip default-gateway 10.34.56.254

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.

DSL2_enable
configure terminal
vlan 567
name CONTABILIDAD
exit

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.

DSL1_enable
configure terminal
spanning-tree vlan 1,12,434,800,1010,1111,3456 root primary
spanning-tree vlan 123,234 root secondary
exit

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.

DSL2_enable
configure terminal
spanning-tree vlan 123,234 root primary
spanning-tree vlan 12,434,800,1010,3456 root secondary
exit

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.

Código de configuración aplicado

```
DSL1_interface port-channel 1
switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
exit
interface port-channel 4
switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
exit
exit
interface port-channel 2
switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
exit
interface port-channel 3
switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
exit
```

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

Tabla 2. Interfaces con puertos de acceso Escenario 2

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

Código de configuración aplicado

```
DSL1_interface f0/6
switchport access vlan 3456
no shutdown
exit
int f0/15
switchport access vlan 1111
no shutdown


DSL2_interface f0/6
switchport access vlan 12
switchport voice vlan 1010
```

no shutdown
exit
interface f0/15
switchport access vlan 1111
no shutdown
exit
int ran f0/16-18
switchport access vlan 567
no shutdown
exit

ALS1_enable
configure terminal
int f0/6
switchport access vlan 123
switchport voice vlan 1010
no shutdown
exit
int f0/15
switchport access vlan 1111
no shutdown
exit

ALS2_int f0/6
switchport access vlan 234
no shutdown
exit
int f0/15
switchport access vlan 1111
no shutdown
exit

DSL1_int ran f0/1-5, f0/13-14, f0/16-24, g0/1-2
switchport access vlan 434
shutdown

DSL2_int ran f0/1-5, f0/13-14, f0/19-24, g0/1-2
switchport access vlan 434
shutdown

ALS1_int ran f0/1-5, f0/13-14, f0/19-24, g0/1-2
switchport access vlan 434
shutdown

ALS2_int ran f0/1-5, f0/13-14, f0/19-24, g0/1-2
switchport access vlan 434
shutdown

Part 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

Figura 12.Se aplica verificación de existencia de VLAN en switch

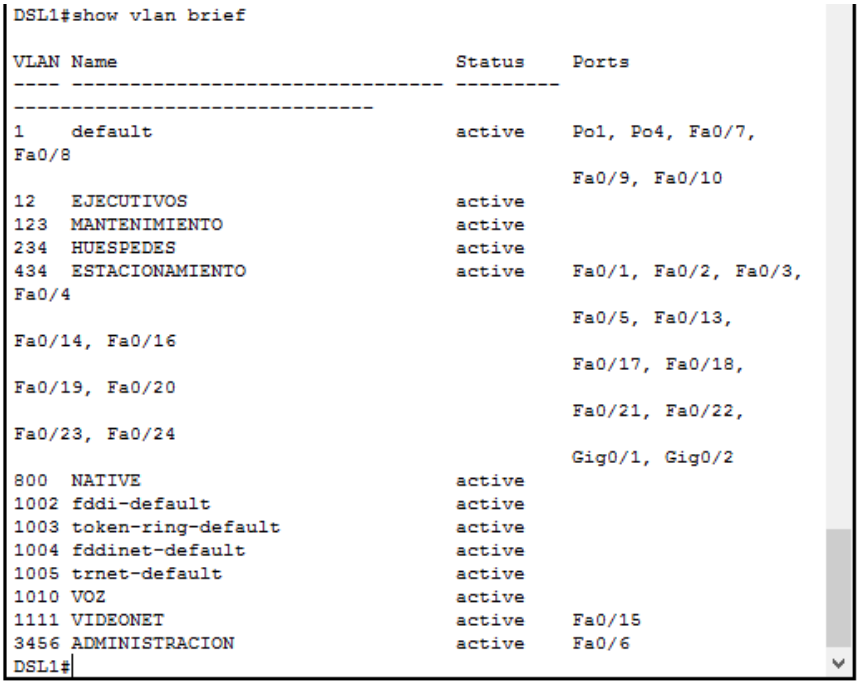
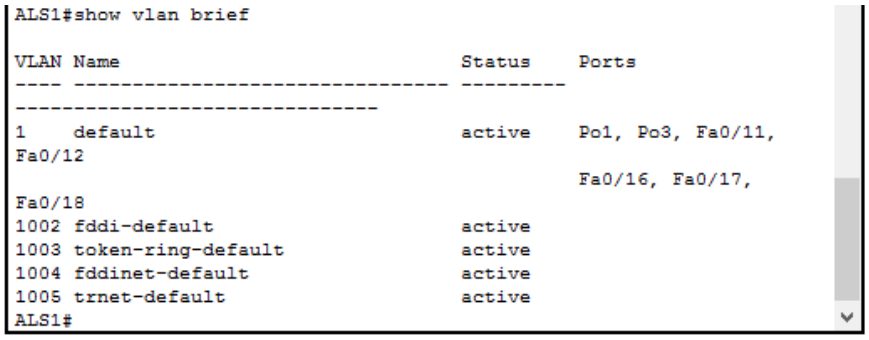
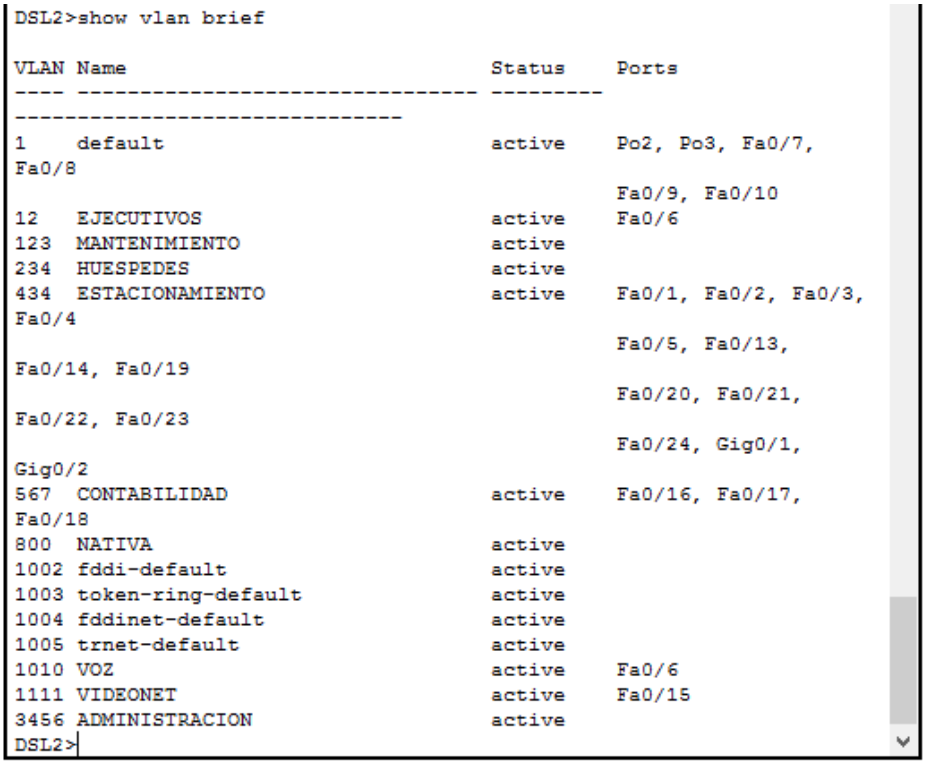


Figura 13. Se aplica verificación de existencia de VLAN en switch



```
ALS1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Po1, Po3, Fa0/11,
Fa0/12
                                                 Fa0/16, Fa0/17,
Fa0/18
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
ALS1#
```

Figura 14. Se aplica verificación de existencia de VLAN en switch



```
DSL2>show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Po2, Po3, Fa0/7,
Fa0/8
                                                 Fa0/9, Fa0/10
12   EJECUTIVOS                        active    Fa0/6
123  MANTENIMIENTO                     active
234  HUESPEDES                         active
434  ESTACIONAMIENTO                   active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/13,
Fa0/14, Fa0/19
                                                 Fa0/20, Fa0/21,
Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1,
Gig0/2
567  CONTABILIDAD                      active    Fa0/16, Fa0/17,
Fa0/18
800  NATIVA                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
1010 VOZ                               active    Fa0/6
1111 VIDEONET                          active    Fa0/15
3456 ADMINISTRACION                    active
DSL2>
```

Figura 15. Se aplica verificación de existencia de VLAN en switch

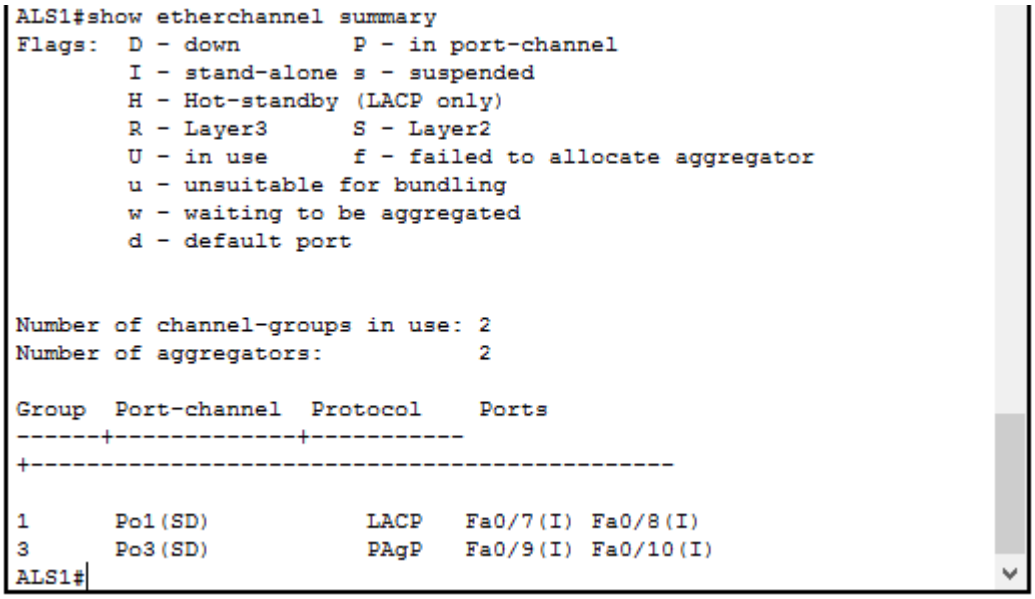
```
ALS2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Po2, Po4, Fa0/11,
Fa0/12
                                                Fa0/16, Fa0/17,
Fa0/18
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
ALS2#
```

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

Figura 16.Se aplica verificación EtherChannel entre DLS1 y ALS1

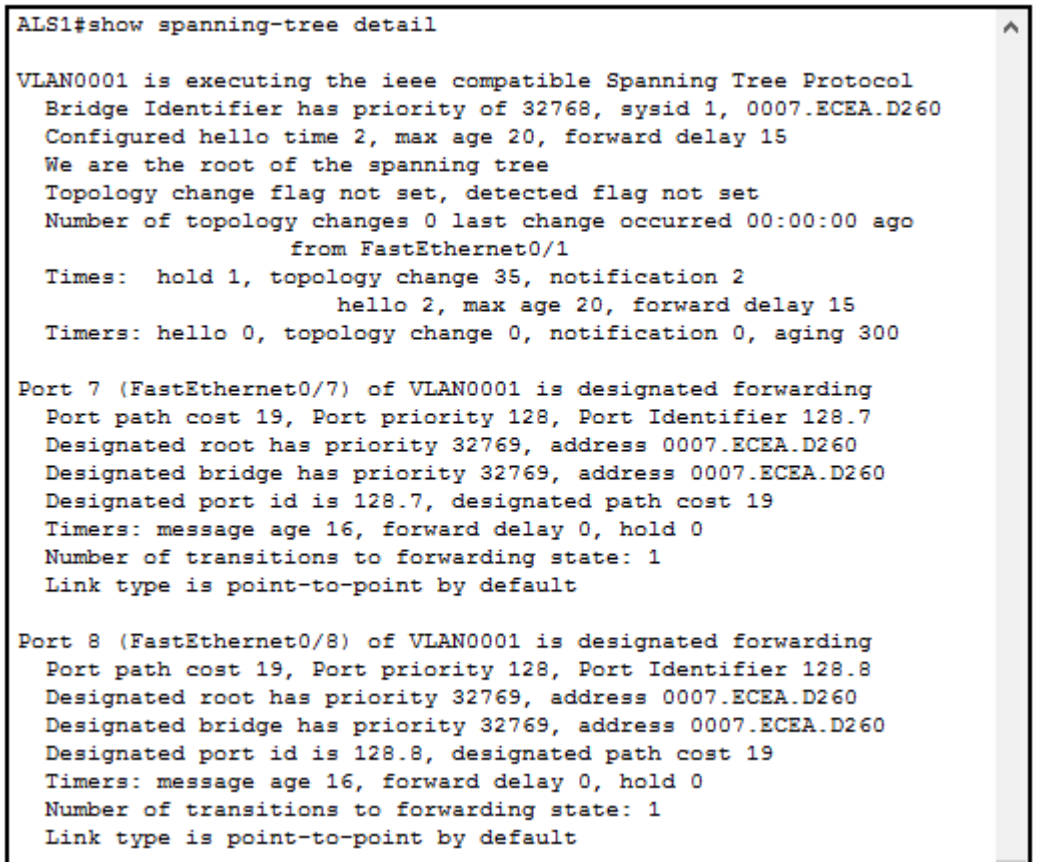
```
DSL1#show  etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

1      Po1(SD)           LACP   Fa0/7(s) Fa0/8(s)
4      Po4(SD)           PAgP   Fa0/9(s) Fa0/10(s)
12     Po12(RU)           LACP   Fa0/11(P) Fa0/12(P)
DSL1#
```

Figura 17. Se aplica verificación EtherChannel entre DLS1 y ALS1



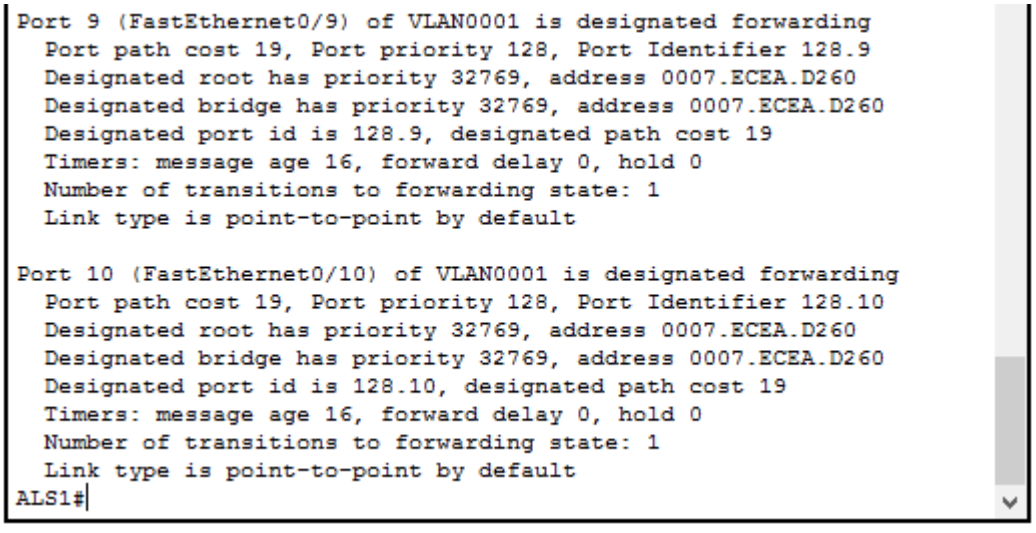
c. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN.

Figura 18. Se aplica verificación Spanning tree entre DLS1 o DLS2



```
ALS1#show spanning-tree detail

VLAN0001 is executing the ieee compatible Spanning Tree Protocol
  Bridge Identifier has priority of 32768, sysid 1, 0007.ECEA.D260
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 00:00:00 ago
                  from FastEthernet0/1
  Times:  hold 1, topology change 35, notification 2
                      hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

Port 7 (FastEthernet0/7) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.7
  Designated root has priority 32769, address 0007.ECEA.D260
  Designated bridge has priority 32769, address 0007.ECEA.D260
  Designated port id is 128.7, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default

Port 8 (FastEthernet0/8) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.8
  Designated root has priority 32769, address 0007.ECEA.D260
  Designated bridge has priority 32769, address 0007.ECEA.D260
  Designated port id is 128.8, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
```

Figura 19. Se aplica verificación Spanning tree entre DLS1 o DLS2



```
Port 9 (FastEthernet0/9) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.9
  Designated root has priority 32769, address 0007.ECEA.D260
  Designated bridge has priority 32769, address 0007.ECEA.D260
  Designated port id is 128.9, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default

Port 10 (FastEthernet0/10) of VLAN0001 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.10
  Designated root has priority 32769, address 0007.ECEA.D260
  Designated bridge has priority 32769, address 0007.ECEA.D260
  Designated port id is 128.10, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
ALS1#
```

CONCLUSIONES

Se logró poner en práctica lo aprendido durante el periodo académico, resaltando las ventajas de Routing y Switching ya que por medio de protocolos sencillos y prácticos de implementar, se permite ayudar a establecer de manera estática las direcciones ip de las diferentes interfaces de los distintos dispositivos que conforman una red, organizaciones de redes LAN y WAN por medio de VLAN, configuración de protocolos como son OSPF, EIGRP, y realizar validación de ventajas de cada una de las implementaciones por medio de las comunicaciones, establecer protocolos IPV4 e IPV6 para una mejor administración de la red e ir avanzando en el mundo de las comunicaciones.

Se adquirieron habilidades de uso de comandos en el software cisco packet tracer, donde se puede evidenciar un entorno real en el momento de ejecutar las diferentes configuraciones procediendo a validar el correcto funcia miento de enlaces y protocolos.

Se identificaron diferentes errores que pueden presentarse en entornos reales, esto nos ayuda a identificar origen del error modificando los comandos y analizar desde varias perspectivas el correcto funcionamiento de las topologías de red.

BIBLIOGRAFÍA

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!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

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!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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!AmIJYei-NT1IlnWR0hoMxgBNv1CJ