

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FABER ORLANDOLAGUADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
CUCUTA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FABER ORLANDOLAGUADO

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

DIRECTOR:
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
CUCUTA
2020

TABLA DE CONTENIDO

GLOSARIO.....	5,6
RESUMEN.....	7
ABSTRACT.....	8
INTRODUCCION.....	9
OBJETIVOS.....	10
01. ESCENARIO 1.....	11
011. PASO 1.....	12
0111. PASO 2.....	18
02. ESCENARIO 221	
022. PASO 1.....	22
0222. PASO 2.....	29
LINK DE LAS PROPUESTAS.....	30
CONCLUSION.....	31
BIBLIOGRAFIA.....	32

LISTA DE FIGURAS

FIG. 1 PROPUESTA 1	11
FIG. 2 PROPUESTA 1	12
FIG. 3 PROPUESTA 1	18
FIG. 4 PROPUESTA 1	19
FIG. 5 PROPUESTA 1	19
FIG. 6 PROPUESTA 1	20
FIG. 7 PROPUESTA 1	20
FIG. 1 PROPUESTA 2	21
FIG. 2 PROPUESTA 2	22
FIG. 3 PROPUESTA 2	29
FIG. 4 PROPUESTA 2	30

GLOSARIO

ACL: Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos. Un ACL contiene los host se permiten que o acceso negado al dispositivo de red. El router o el Switch examinan cada paquete para determinar si remitir o caer el paquete, en base de los criterios especificados dentro de las Listas de acceso. Los criterios de lista de acceso podían ser la dirección de origen del tráfico, la dirección destino del tráfico.

IPv4: El IPv4 es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6: El IPv6 es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. El IPv6 se está desarrollando actualmente en todo el mundo. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

RSTP: El protocolo rapid Spanning-tree (RSTP) es una mejora del STP. El RSTP proporciona una convergencia del árbol de expansión más rápida después de un cambio de la topología. El STP puede tardar 30 a 50 segundos a responder a un cambio de la topología mientras que el RSTP responde en el plazo de tres veces el tiempo de saludo configurado. El RSTP es al revés compatible con el STP.

SNMP: El Simple Network Management Protocol (SNMP) es un estándar de red para salvar y compartir la información sobre los dispositivos de red. El SNMP facilita la Administración de redes, el troubleshooting, y el mantenimiento.

RESUMEN

En el curso de profundización cisco CCNP alude a un programa de certificación para ingenieros de redes de nivel básico que ayuda a aumentar su inversión en conocimiento de redes fundacional y aumenta el valor de la red de su empleador. La Certificación CCNP hace valiosa la capacidad de instalar, configurar, operar y solucionar problemas de mediano tamaño y router de redes de conmutación, incluyendo la implementación y verificación de conexiones a sitios remotos en una WAN.

En el desarrollo de las dos propuestas dadas por la guía de trabajo se investigó y adquirió conocimientos para la programación de switches, router, enrutadores entre otros dispositivo de red, se interactuar con software de común mente se utilizar para la programación de dispositivos de redes haciendo un mejor aprendizaje en los estudiantes de la UNAD.

ABSTRACT

In the Cisco CCNP Deepening Course, you allude to a certification program for entry-level network engineers that helps increase your investment in foundational network knowledge and increases the value of your employer's network. The CCNP Certification makes valuable the ability to install, configure, operate, and troubleshoot medium-sized and routed switching networks, including implementing and verifying connections to remote sites on a WAN.

In the development of the two proposals given by the work guide, knowledge was learned and acquired for the programming of switches, routers, routers, among other network devices, interacting with software commonly used for programming network devices, making better learning for UNAD students.

Palabras claves: ipv6, configuration, switches, routers, network.

INTRODUCCION

El siguiente documento se desarrolla de acuerdo a las normas de presentación de documento final para el curso diplomado de profundización CISCO CCNP dando cumplimiento a los objetivos de habilidades prácticas en redes Cisco Networking como trabajo de grado para obtener el título de ingeniero electrónico de la prestigiosa universidad Nacional Abierta a distancia UNAD.

OBJETIVOS

Diseñar por medio del software Packet tracer los escenarios dado por la guía de trabajo como informe final del curso diplomado de profundización CNNP de la universidad UNAD

Investigar y desarrollar en el curso diplomado de profundización cisco CCNP conocimientos de profundización mediante el desarrollo de ejercicios y presentación de evaluaciones en línea que ayudan a mejorar el aprendizaje de los unadistas.

01. Escenario 1

Una empresa de confecciones posee tres sucursales distribuidas en las ciudades de Cali, Barranquilla y Ocaña, 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.

Topología de red

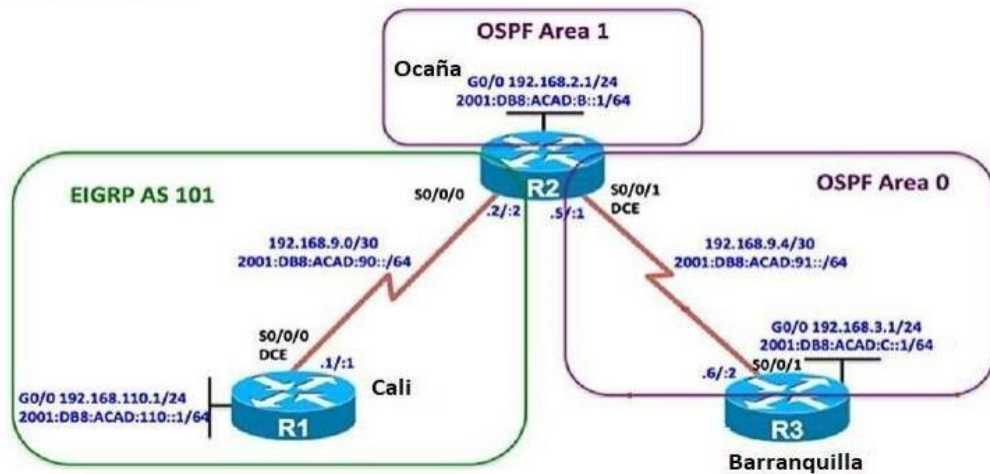


Fig. 1 propuesta 1

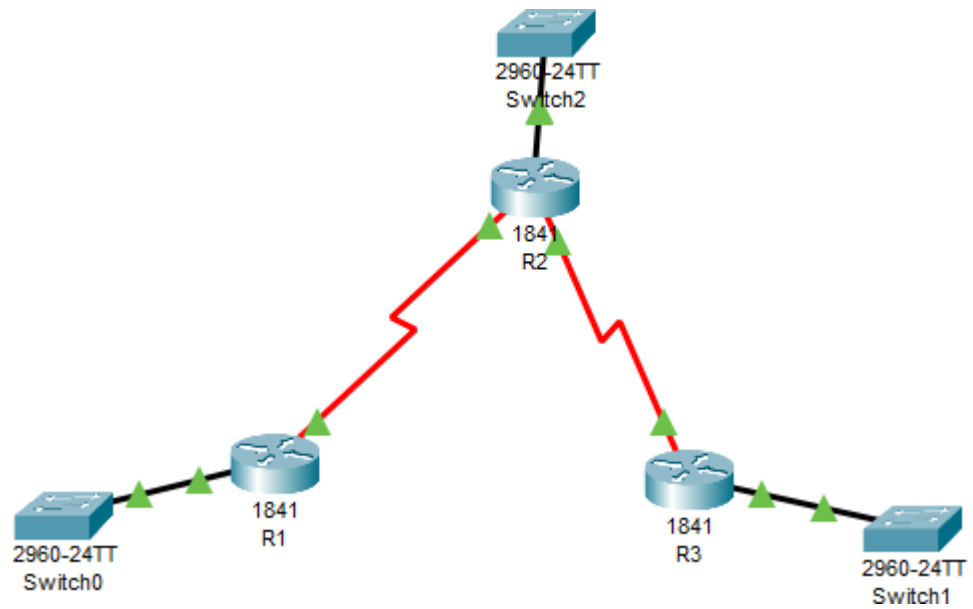


Fig. 2 propuesta 1

011. Paso 1

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

Configuración Router R1 de las interfaces ipv4 y ipv6 junto con el nombre del dispositivo:

```
Prompt R1
enable
config
```

```

hostname R1
int s0/0/0
no sn
int g0/0
ip address 192.160.110.1 255.255.255.0
no sh
ipv6 unicast-routing
int s/0/0/0
ipv6 address 2001:DB8:ACAD:90::1/64
ipv6 address FE80::1 link local
no sh
int g0/0
ipv6 address 2001:DB8:ACAD:90::1/64
ipv6 address FE80::1 link local
no sh
Exit

```

Por medio de estos comandos se programa las direcciones ip de las interfaces que vamos a utilizar del router al igual que se cambió el nombre

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.

```

Prompt R1,R2,R3
Int s/0/0/0
Bandwidth 128
Ip address 192.168.9.1 255.255.255.252
Exit
Int f0/0
Ipv6 address 2001:DB8::ACAD:0:: 1 /64
Ipv6 address feB0:: 2 link local
no sh
Int s/0/0/1
Ipv6 address 2001:DB8::ACAD:0:: 1 /64
Ipv6 address feB0:: 2 link local
no sh
int s/0/0/0
bandwidth 128
ip address 192.168.9.2 255.255.255.252
exit
int s/0/0/1
bandwidth 128 15
ip address 192.168.9.5 255.255.255.252

```

exit

Por medio de los comandos cambiamos el ancho de cada R y ajustamos el dce

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.

```
Prompt R2,R3
enable
config
Int s0/0/0
Bandwidth 128
Ip address 192.168.9.2 255.255.255.252
Exit
Int s0/0/1
Bandwidth 128
Ip address 192.168.9.5 255.255.255.252
Exit
Router ospf 1
Router id 2.2.2.2
Exit
Ipv6 router ospf 1
Router id 2.2.2.2 16
Exit
Int s0/0/0
Bandwidth 128
Ip address 192.168.9.1 255.255.255.252
Exit
Int f0/0
Ipv6 address 2001:DB8::ACAD:0:: 1 /64
Ipv6 address 2001:DB8:ACAD: 91:: 2 /64
Ipv6 address feB0:: 3 link local
no sh
int F/0
Ipv6 address 2001:DB8:ACAD: 91:: 2 /64
Ipv6 address feB0:: 3 link local
No sh
exit
Int s0/0/1
Bandwidth 128
ip address 192.168.9.6 255.255.255.252
router ospf 1
```

```
router id 3.3.3.3
exit
ipv6 router ospf 1 17
router id 3.3.3.3
exit
```

Se configuraron las familias ospfv3 para R2 y R3

4. En R2, configure la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3 en OSPF área 0.

```
Prompt R2
Int s/0/0/0
Bandwidth 128
ip address 192.168.9.2 255.255.255.252
exit
Int s/0/0/1
Bandwidth 128
ip address 192.168.9.6 255.255.255.252
exit
router ospf 1
router id 2.2.2.2
exit
ipv6 router ospf 1
router id 2.2.2.2
exit
network 192.168.9.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.3 area 0 18
```

se configuro la interface f0/0 en el area ospf en R2 y R3

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

```
Prompt R3
Ipv6 address 2001:DB8:ACAD: 91:: 2 /64
Ipv6 address feB0:: 3 link local
no sh
int F0/0
Ipv6 address 2001:DB8:ACAD: C:: 1 /64
Ipv6 address feB0:: 3 link local
No sh
Exit
Int s0/0/1
Bandwidth 128
Ip address 192.168.9.6 255.255.255.252
Exit
Router ospf 1
Router id 3.3.3.3
Exit
Ipv6 router ospf 1
Router id 3.3.3.3 19
Exit
Router ospf 1
Network 192.168.9.4 0.0.0.3 area 0
Exit
```

se configuro la interface f0/0 en el area ospf en R2 y R3

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

```
Prompt R2
Int s/0/0/0
Bandwidth 128
ip address 192.168.9.2 255.255.255.252
exit
Int s/0/0/1
Bandwidth 128
ip address 192.168.9.5 255.255.255.252
exit
router ospf 1
router id 2.2.2.2
exit
ipv6 router ospf 1
router id 2.2.2.2
```

```
exit
router ospf 1
network 192.168.9.0 0.0.0.3 area 0 20
network 192.168.4.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.3 area 0
exit
```

se configuro el area 1 por medio de direcciones de trabajo

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

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

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

```
Prompt R2
Int s/0/0/0
Bandwidth 128
ip address 192.168.9.2 255.255.255.252
exit
Int s/0/0/1
Bandwidth 128
ip address 192.168.9.5 255.255.255.252
exit
router ospf 1
router id 2.2.2.2
exit
ipv6 router ospf 1
router id 2.2.2.2 21
exit
router ospf 1
network 192.168.9.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.3 area 0
exit
ospf 1
area 1 naga
router eigrp 101
network 192.168.9.0
exit
```

Se realiza la configuración entre R2 de EIGRP, OSFP en ipv4 y ipv6

0111. Paso 2

a. Verificar conectividad de red y control de la trayectoria. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.

```
cali#show ip route
Codes: C - connected, S - static, I - IGRP, 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

      192.168.9.0/30 is subnetted, 2 subnets
C       192.168.9.0 is directly connected, Serial0/0/0
D       192.168.9.4 [90/21024000] via 192.168.9.2, 00:05:41,
Serial0/0/0
C       192.168.110.0/24 is directly connected, FastEthernet0/0

cali#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
-- -- -- -- --
```

Fig. 3 propuesta 1

```

Ocaa#show ip route
Codes: C - connected, S - static, I - IGRP, 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

        192.168.9.0/30 is subnetted, 2 subnets
C       192.168.9.0 is directly connected, Serial0/0/0
C       192.168.9.4 is directly connected, Serial0/0/1

Ocaa#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS

```

Fig. 4 propuesta 1

Por medio de las imágenes se demuestra la configuración de la red

a. Verificar comunicación entre routers mediante el comando ping y trace router

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.

```

cali#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 = 1/2/5 ms

cali#

```

Fig. 5 propuesta 1

```

Ocaa#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 = 1/3/6 ms

```

Fig. 6 propuesta 1

```
Barranquilla>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 = 1/6/25 ms
Barranquilla>
```

Fig. 7 propuesta 1

Se demuestra por medio de las imágenes la configuración de topología de la propuesta

- 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.

02. ESCENARIO 2

Configurar la red de acuerdo con las especificaciones.

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.

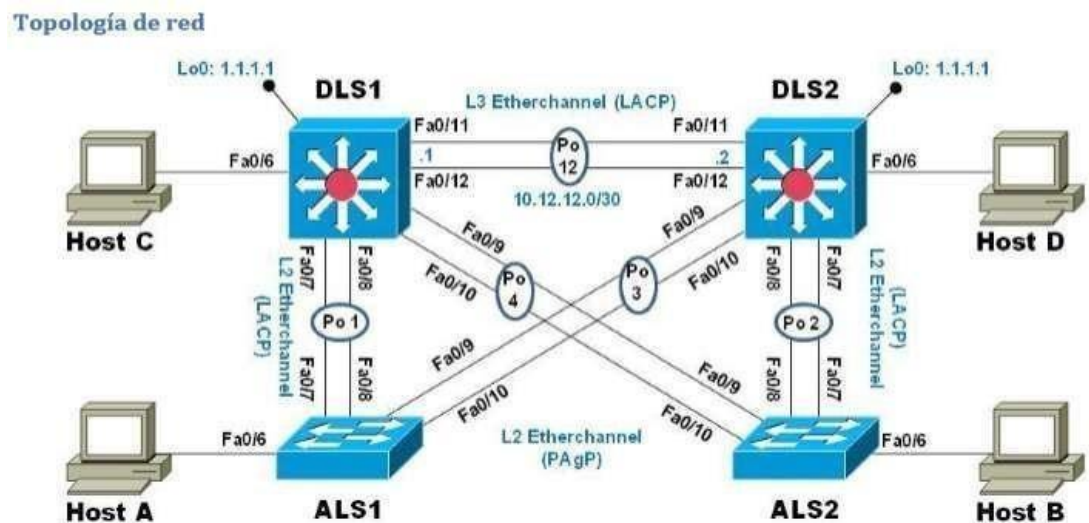


Fig 1 propuesta 2


```
exit
interface port-channel 12
exit
```

Por medio de los comandos se configura los nombres e interface de los switches y se realizar el montaje de la topología de la red

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 PAgPn.

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

e. Utilizar el nombre de dominio UNAD con la contraseña cisco123

```
Prompt DLS1
interface port-channel 12
ip address 10.12.12.1 255.255.255.252
int ran f0/7-10
switchport trunk encapsulation dot1q
switchport trunk NATIVA
vlan 800
switchport mode trunk
switchport nonegotiate
no shut
exit
int ran f0/7-8
channel-group 1 mode active
exit
int ran f0/9-10
channel-group 4 mode desirable
```

```
exit
vtp domain UNAD vtp ver 3
vtp password cisco123
```

Se configura algunas interfaces de los switches

Se crean puertos y grupo en los switches

2) Configurar DLS1 como servidor principal para las VLAN.

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

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		

```
Prompt DLS1
Int vlan 12
Ip address 10.0.12.252 255.255.255.0
No sh
Exit
int vlan 123
ip address 10.0.123.252 255.255.255.0
no sh exit
int vlan 234
ip address 10.0.234.252 255.255.255.0
no sh exit
int vlan 1010
ip add 10.10.10.252 255.255.255.0
no shut
exit
```

por medio de los comandos se configuraron las direcciones vlan se les asignaron direcciones ip

f. En DLS1, suspender la VLAN 434.

```
Prompt DLS1
ip dhcp pool EJECUTIVOS-POOL
network 10.0.12.0 255.255.255.0
default-router 10.0.12.254
dns-server 1.1.1.1
exit
ip dhcp pool MANTENIMIENTO-POOL
network 10.0.123.0 255.255.255.0
default-router 10.0.123.254
dns-server 1.1.1.1
exit
ip dhcp pool HUESPEDES-POOL
network 10.0.234.0 255.255.255.0
default-router 10.0.234.254
dns-server 1.1.1.1
exit
```

se le suspendio el vlan 434

g. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión2, y configurar en DLS2 las mismas VLAN que en DLS1.

h. Suspender VLAN 434 en DLS2.

```
Prompt DLS2
en conf t
int ran f0/1-24, g0/1-2 shutdown
exit
int ran f0/11-12
no switchport
channel-group 12 mode active
no shut
exit
interface port-channel 12
ip address 10.12.12.2 255.255.255.252
exit
int ran f0/7-10
switchport trunk encapsulation dot1q
switchport trunk NATIVA vlan 800
```

se le configure el vtp en ds2, además que se le coloca dirección ip a las interface del switch

h. 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.

i. 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.

j. 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.

k. 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:

```
Prompt DLS2,DLS1
int ran f0/7-8
channel-group 2 mode active
exit
int ran f0/9-10
channel-group 3 mode desirable
exit
vtp ver 2
vtp mode transparent
spanning-tree vlan 1,12,123,234,434,800,1010,3456 root secondary
spanning-tree vlan 123,234 root primary
vlan 800
name NATIVA-VLAN
exit
vlan 434
name ESTACIONAMIENTO-LOT
state suspend
exit
vlan 12
name EJECUTIVOS
exit
vlan 123
34
name MANTENIMIENTO
exit
vlan 234
name HUESPEDES
exit
```

se configuran las vlan para que sean las únicas que permitan circular en las troncales creadas

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		

0222. Part 2: conectividad de red de prueba y las opciones configuradas.

- Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso
- Verificar que el EtherChannel entre DLS1 ALS1 está configurado correctamente
- Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN

```

%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
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
changed state to up
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/7 (800), with DLS2 FastEthernet0/7 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/8 (800), with DLS2 FastEthernet0/8 (1).
%LINK-5-CHANGED: Interface Port-channel2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2,
changed state to up
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/10 (800), with DLS1 FastEthernet0/10 (1).
%LINK-5-CHANGED: Interface Vlan3456, changed state to up
%LINK-5-CHANGED: Interface Port-channel4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4,
changed state to up
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/9 (800), with DLS1 FastEthernet0/9 (1).
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk
Port-channel2 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel2 on VLAN0001.
Inconsistent port type.

```

Fig 3 propuesta 2

Proceso terminado en Packet tracer

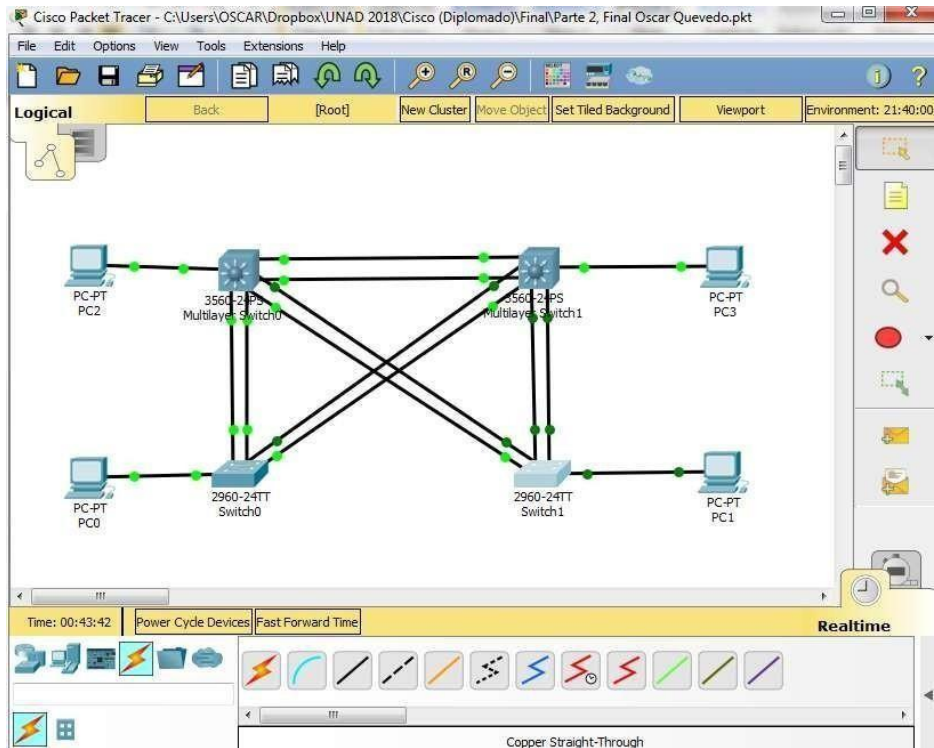


Fig. 4 propuesta 2

Link de propuestas Packet tracer

<https://drive.google.com/file/d/12F6La8PcSPke5nnQ4ggw1voDdE4mNPu4/view?usp=sharing>

<https://drive.google.com/file/d/1DwfVowLMnMrZZGVCgbXhvetxS684fbLV/view?usp=sharing>

CONCLUSIONES

Se investigaron protocolos de configuración de router, switches, pc entre otros mediante las bibliografías ofrecidas por el curso diplomado de profundización cisco CNNP

Se estudiaron las bibliografías y realizaron las propuestas necesarias para los problemas dados por las guías mediante un aprendizaje compartido con compañeros y asesorías constante de la tutora Paulita Flor

Mediante del desarrollo de las propuestas se aprendió a diferencia entre cada uno de los dispositivos de red y su importancia en la transmisión de datos entre ellos mismo mediante el aprendizaje didáctico del programa cisco Packet tracer

BIBLIOGRAFÍA

Conceptodefinicion.de, Redacción. (Última edición:9 de julio del 2014). Definición de CCNA. Recuperado de://conceptodefinicion.de/ccna/. Consultado el 10 de julio del 2020

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>

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). Switching Features and Technologies. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>