

PRUEBA DE HABILIDADES PRACTICAS CISCO CCNP

Víctor Alfonso Cardona Valencia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA ELECTRONICA
CEAD DOSQUEBRADAS
JULIO 2020

PRUEBA DE HABILIDADES PRACTICAS CISCO CCNP

Víctor Alfonso Cardona Valencia

Prueba de habilidades prácticas: trabajo de grado para optar el título de
ingeniero electrónico

Ing. Paulita Flor Salazar

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENEIRIA
INGENIERIA ELECTRONICA
CEAD DOSQUEBRADAS
JULIO 2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Cartago valle 28 julio 2020

DEDICATORIA

Dedico este trabajo a DIOS todo poderoso quien me dio el valor de cruzar este largo camino, a mi esposa e hijos quienes tuvieron que pasar las necesidades y dificultades para convertirme en un profesional.

Contenido

DEDICATORIA	4
Contenido	5
tabla de figuras	7
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN.....	11
OBJETIVOS.....	12
1. Escenario 1	13
1.1. Parte 1	14
1.2. Parte 2	24
Verificar conectividad de red y control de la trayectoria.....	24
2. Escenario 2	31
2.1. Parte 1:	32
2.2. Parte 2:	52
CONCLUSIONES	59
BIBLIOGRAFÍAS.....	60
ANEXOS.....	61

Lista de tablas

Tabla 1 direcciones vlans	42
Tabla 2 puertos de acceso.....	49

tabla de figuras

Figura 1 TOPOLOGIA GNS 3.....	14
Figura 2 show ipv6 route en R1	24
Figura 4 comando show ip route.....	25
Figura 6 comando show ipv6 ospf en R2.....	25
Figura 7 show ipv6 ospf en R2.....	26
Figura 8 show ipv6 route en R3	26
Figura 9 show ipv6 ospf en R3.....	27
Figura 10 show ipv6 ospf en R3.....	27
Figura 11 ping R1	28
Figura 12 ping R2	29
Figura 13 ping R3	29
Figura 14 show runn R1.....	30
Figura 15 show runn en R2.....	30
Figura 16 show runn en R3.....	31
Figura 17 topología escenario 2.....	32
Figura 41 comando VTP status ALS 2.....	42
Figura 42 show vlan aplicado en DSL1.....	42
Figura 43 Configuración VLAN en DSL2	44
Figura 44 habilitación VTP mode transparent.....	45
Figura 45 Configuración vlan 567 en DSL2	46
Figura 46 Configuración negación al paso vlan 567	46
Figura 47 Configuración Spanning tree	47
Figura 48 Configuración Spanning-tree	48
Figura 49 Configuración puertos troncales	49
Figura 50 Configuración interfaces	52
Figura 51 verificación vlan 1	52
Figura 52 verificación de vlan DSL1	53
Figura 53 verificación de vlan	53
Figura 54 verificación de vlan DSL2	54
Figura 55 Verificación de vlan.....	54
Figura 56 Verificación de vlan ALS1	55
Figura 57 Verificación de vlan.....	55
Figura 58 Verificación de vlan ALS2.....	56
Figura 59 Verificación de interfaces DSL 1	56

Figura 60 Verificación de interfaces DSL 2.....	57
Figura 61 Verificación de interfaces ALS 1	57
Figura 62 Spanning-tree entre DSL1 a DSL2	58
Figura 63 Spanning-tree entre DSL2 a DSL 1	58

GLOSARIO

ANCHO DE BANDA: se mide como la cantidad de datos que se puede transferir entre dos puntos de una red en un tiempo específico, el ancho de banda se mide en bits por segundos y se expresa como una tasa de bits.

DIRECCIÓN IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

GATEWAY: es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

VLAN: La utilidad de las VLAN radica en la posibilidad de separar aquellos segmentos lógicos que componen una LAN y que no tienen la necesidad de intercambiar información entre sí a través de la red de área local. Esta particularidad contribuye a una administración más eficiente de la red física

RESUMEN

El desarrollo de estas actividades como trabajo final, esta propuesto en la solución de dos escenarios, como administradores de redes y futuros ingenieros realizamos cada una de las configuraciones necesarias aplicando comandos como show ip route, show ipv6 route, show runn, configuración de interfaces y puertos troncales entre otros para dar solución a lo requerido.

El escenario 1 está planteado para una empresa de confecciones distribuidas en 3 sucursales en diferentes ciudades, la simulación de este escenario se realiza en simulador GNS3 configurando las direcciones ip, protocolos que se requieren en la guía.

Para el escenario 2 se plantea una empresa de comunicaciones que requiere configuraciones en direcciones ip, VLANs, EtherChannels para dar solución a los lineamientos de la guía.

Palabras clave: traceroute, show ip route, vlans, EtherChannels, packet tracer y GNS3.

ABSTRACT

The development of these activities as final work, is proposed in the solution of two scenarios, as network administrators and future engineers we carry out each of the necessary configurations applying commands such as show ip route, show ipv6 route, show runn, interface configuration and trunk ports among others to provide solutions to what is required.

Scenario 1 is proposed for a clothing company distributed in 3 branches in different cities, the simulation of this scenario is carried out in a GNS3 simulator configuring the IP addresses, protocols that are required in the guide.

For scenario 2, a communications company is proposed that requires configurations in IP addresses, VLANs, EtherChannels to solve the guidelines in the guide.

Keywords: traceroute, show ip route, vlans, EtherChannels, packet tracer and GNS3.

INTRODUCCIÓN

El presente trabajo busca la consolidación de los conocimientos adquiridos en los cursos de CCNA y CCNP de cisco, por medio de la solución de dos escenarios de implementación de redes de datos con la ayuda de dispositivos activos Router y switch simulados en herramientas como Packet Tracer y GNS3. De esta manera se realizara la implementación de redes capaces de generar enrutamiento simultáneo de IPV4 e IPV6, segmentación de redes y aprendizajes automáticos de enrutamiento por medio de protocolos Etherchannel, EIGRP Y OSPF.

En los escenarios que se abordan se deben configurar cada uno de los dispositivos que forman parte de esto acorde con los lineamientos establecidos por el direccionamiento IP, protocolos de enrutamientos y demás aspectos que forman parte de la Topología d red.

OBJETIVOS

Configurar y administrar dispositivos de networking mediante el uso de protocolos avanzados para el acceso de gestión remoto cisco ccnp

Adquirir habilidades para Configurar protocolos de enrutamientos IPV4 e IPV6

Describir tecnologías de conmutación mejoradas tales como, vlan, protocolo de enlace troncal de vlan (vtp) y protocolo de árbol de expansión.

Desarrollar todas las actividades propuestas por el curso diplomado de profundización cisco ccnp, para obtener el título de ingeniero electrónico.

1. 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.

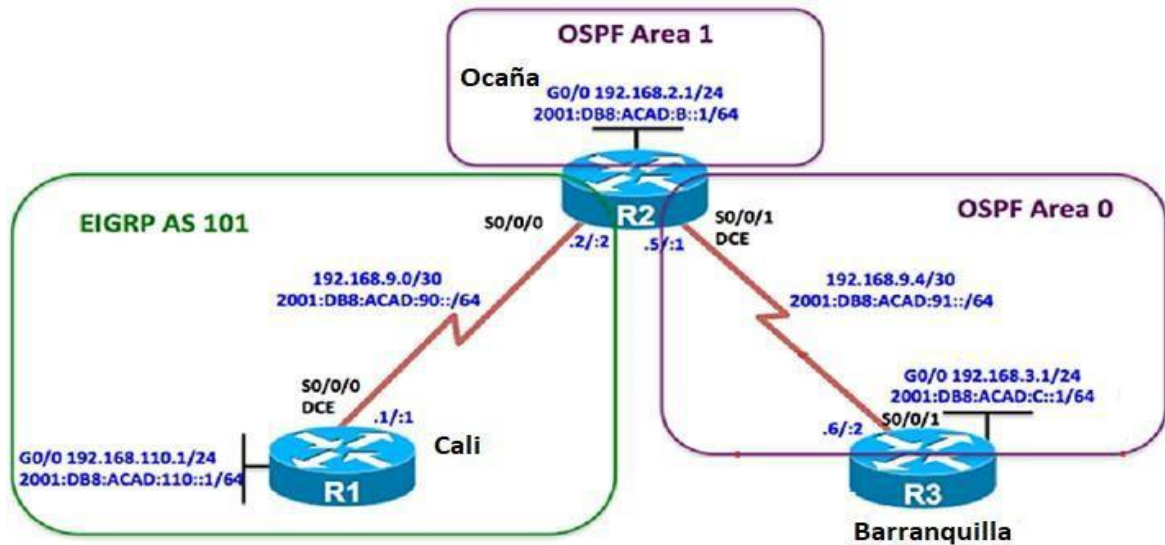


Ilustración 1. Topología de red elaboración propia

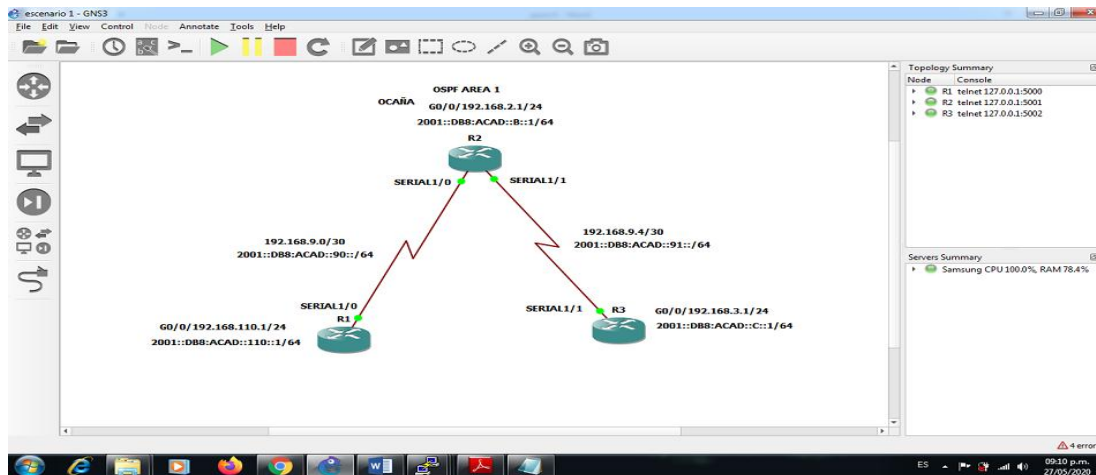


Figura 1 TOPOLOGIA GNS 3

1.1. Parte 1.

Configuración del escenario propuesto

1.1.1. Configuración de interfaces en R1, R2, R3.

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

```

R1>enable                                     modo privilegiado
R1#configure terminal                         modo configuración global
R1 (config) #hostname R1                     asignamos el nombre al Router
R1 (config) #ipv6 unicast-routing            Configuramos el enrutamiento ipv6
R1 (config) #interface FastEthernet0/0      configuramos las interfaz fastEthernet
R1 (config-if) #ip address 192.168.110.1 255.255.255.0 Configuracion direccion ip
R1 (config-if) #ipv6 address 2001:db8:acad:110::1/64 configuramos la direccion
estática global
R1 (config-if) #no shutdown                  no apagar
R1 (config-if) #interface serial1/0         Configurar la interfaz serial
1

```

R1 (config-if) #ip address 192.168.9.1 255.255.255.0 asignamos la direccion ip y mascara subred

R1 (config-if) #ipv6 address 2001:db8: acad: 90:: 1/64 configuramos la direccion ipv6 estática global

R1 (config-if) #clock rate 128000 configuramos la velocidad del reloj

R1 (config-if) #bandwidth 128 configuramos el ancho de banda

R1 (config-if) #no shutdown no apagar

R1 (config-if) # exit

1.1.2. Configuración BW sobre las interfaces seriales

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

Configuración parámetros (Ítem 1 y 2) en R2

R2 (config) #hostname R2 asignamos el nombre la Router

R2 (config) #ipv6 unicast-routing Configuramos el enrutamiento ipv6

R2 (config) #interface FastEthernet0/0 configuramos las interfaz fastEthernet

R2 (config-if) #ip address 192.168.2.1 255.255.255.0 asignamos la direccion ip y mascara subred

R2 (config-if) #ipv6 address 2001:db8: acad::1/64 configuramos la direccion estática global

R2 (config-if) #no shutdown no apagar

R2 (config-if) #interface serial1/0 configuramos la interfaz serial 1/0

R2 (config-if) #ip address 192.168.9.2 255.255.255.0 asignamos la direccion ip y mascara subred

R2 (config-if) #ipv6 address 2001:db8: acad: 90:: 2/64 configuramos la direccion ipv6 estática global

R2 (config-if) #bandwidth 128 configuramos el ancho de banda

R2 (config-if) #no shutdown no apagar

R2 (config-if) #interface serial1/1 configuramos la interfaz serial 1/1
 R2 (config-if) #ip address 192.168.9.5 255.255.255.0 asignamos la direccion ip y mascara subred
 R2 (config-if) #ipv6 address 2001:db8: acad: 91:: 1/64 configuramos la direccion ipv6 estática global
 R2 (config-if) #clock rate 128000 configuramos la velocidad del reloj
 R2 (config-if) #bandwidth 128 configuramos el ancho de banda
 R2 (config-if) #no shutdown

Configuración parámetros (Ítem 1 y 2) en R3

R3#configure terminal iniciamos modo configuración global
 R3 (config) #hostname R3 asignamos el nombre al Router
 R3 (config) #ipv6 unicast-routing Configuramos el enrutamiento ipv6
 R3 (config) #interface FastEthernet0/0 configuramos las interfaz fastEthernet
 R3 (config-if) #ip address 192.168.3.1 255.255.255.0 asignamos la direccion ip y mascara subred
 R3 (config-if) #ipv6 address 2001:db8: acad: c: 1/64 configuramos la direccion ipv6 estática global
 R3 (config-if) #no shutdown no apagar
 R3 (config-if) #interface serial1/1 configuramos la interfaz serial 1/1
 R3 (config-if) #ip address 192.168.9.6 255.255.255.0 asignamos la direccion ip y mascara subred
 R3 (config-if) #ipv6 address 2001:db8: acad: 91:: 2/64 configuramos la direccion ipv6 estática global
 R3 (config-if) #bandwidth 128 configuramos el ancho de banda
 R3 (config-if) #no shutdown no apagar

1.1.3. Configuración de protocolo ospfv3 en R2 y R3

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

Comandos utilizados:

Para R2:

R2 (config-if) #Router ospfv3 1 configuramos el protocolo de enrutamiento para ipv6

R2 (config-router) #address-family ipv4 unicast configuramos la direccion de familia ipv4

R2 (config-router-af) #router-id 2.2.2.2 identificamos el router

R2 (config-router-af) #exit-address-family salimos de la direccion de familia

R2 (config-router) #address-family ipv6 unicast direccion de familia ipv6

R2 (config-router-af) #router-id 2.2.2.2 identificamos el router

R2 (config-router-af) #exit-address-family salimos Del modo Configuracion

R3 (config-if) #Router ospfv3 1 salimos de la direccion de familia

R3 (config-router) #address-family ipv4 unicast configuramos la direccion de familia ipv4

R3 (config-router-af) #router-id 3.3.3.3 identificamos el router

R3 (config-router-af) #passive-interface FastEthernet0/0 configuramos las interfaz fastEthernet pasiva

R3 (config-router-af) #exit-address-family salimos de la direccion de familia

R3 (config-router) #address-family ipv6 unicast configuramos el direccionamiento de familias ipv6

R3 (config-router-af) #router-id 3.3.3.3 identificamos el router

R3 (config-router-af) #passive-interface FastEthernet0/0 configuramos las interfaz fastEthernet pasiva

R3 (config-router-af) #exit-address-family salimos de la direccion de familia

1.1.4. Configuración de ospf v3 en R2

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

Comandos utilizados:

Para R2:

R2 (config) #interface FastEthernet0/0 configuramos las interfaz fastEthernet

R2 (config-if) #ospfv3 1 ipv4 area 1 configuramos el protocolo enrutamiento para ipv4 area 1

R2 (config-if) #ospfv3 1 ipv6 area 1 configuramos el protocolo enrutamiento para ipv6 area 1

R2 (config-if) #interface serial1/1 configuramos la interfaz serial 1/1

R2 (config-if) #ospfv3 1 ipv4 area 0 configuramos el protocolo enrutamiento para ipv4 area 0

R2 (config-if) #ospfv3 1 ipv6 area 0 configuramos el protocolo enrutamiento para ipv6 area 0

1.1.5. Configuración de ospfv3 en R3

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

R3 (config) #interface FastEthernet0/0 configuramos las interfaz fastEthernet

R3 (config-if) #ospfv3 1 ipv4 area 0 configuramos el protocolo enrutamiento para ipv4 area 0

R3 (config-if) #ospfv3 1 ipv6 area 0 configuramos el protocolo enrutamiento para ipv4 area 0

R3 (config-if) #interface serial1/0 configuramos la interfaz serial 1/0

R3 (config-if) #ospfv3 1 ipv4 area 0 configuramos el protocolo enrutamiento para ipv4 area 0

R3 (config-if) #ospfv3 1 ipv6 area 0 configuramos el protocolo enrutamiento para ipv6 area 0

1.1.6. Configurar el área 1 como Stubby

Configurar el área 1 como un área totalmente Stubby

Configuración área 1

R2 (config) #Router ospfv3 1 configuramos el protocolo de enrutamiento

R2 (config-router) #address-family ipv4 unicast configuramos la direccion de familia ipv4

R2 (config-router-af) #area 1 stub no-Summary configuramos ruta resumida sin filtracion al area1

R2 (config-router-af) #exit-address-family salimos de la direccion de familia

R2 (config-router) #address-family ipv6 unicast configuramos la direccion de familia ipv6

R2 (config-router-af) #area 1 stub no-Summary configuramos ruta resumida sin filtracion al area1

R2 (config-router-af) #exit-address-family salimos de la direccion de familia

1.1.7. Propagar rutas por defecto de IPv4 e IPv6 en R3 al interior del dominio

Propagar rutas por defecto de IPv4 e IPv6 en R3 al interior del dominio

OSPFv3.

R3#configure terminal entramos en Configuracion global

R3 (config) #router ospfv3 1 configuramos el protocolo de enrutamiento

R3 (config-router) #address-family ipv4 unicast configuramos la direccion de familia ipv4

R3 (config-router-af) #default-information originate always configuramos los anuncios a ningún otro enrutador

R3 (config-router-af) #exit-address-family salimos de la direccion de familia

R3 (config-router) #address-family ipv6 unicast configuramos la direccion de familia ipv6

R3 (config-router-af) #default-information originate always configuramos los anuncios a ningún otro enrutador

R3 (config-router-af) #exit-address-family salimos de la direccion de familia

1.1.8. 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.

R1#conf terminal

R1 (config) #Router eigrp DUAL-STACK configuramos el protocolo eigrp para ipv4 e ipv6

R1 (config-router) #address-family ipv4 unicast autonomous-system 4 configuramos la direccion de familia ipv4 Como Sistema autónomo

R1 (config-router-af) #af-interface FastEthernet0/0 configuramos las interfaz fastEthernet en el direccionamiento de familia

R1 (config-router-af-interface) #passive-interface configuramos el anuncio de la informacion

R1 (config-router-af-interface) #exit-af-interface salimos del modo Configuracion

R1 (config-router-af) #topology base configuramos la tabla base

R1 (config-router-af-topology) #exit-af-topology salimos de tabla base

R1 (config-router-af) #network 192.168.9.0 0.0.0.3 habilitamos el proceso en la interfaz

R1 (config-router-af) #network 192.168.110.0 0.0.0.3 habilitamos el proceso en la interfaz

R1 (config-router-af) #eigrp router-id 1.1.1.1 identificamos el router

R1 (config-router-af) #exit-address-family salimos del direccionamiento de familia

R1 (config-router) #address-family ipv4 unicast autonomous-system 6 configuramos la direccion de familia ipv4 Como Sistema autónomo

R1 (config-router-af) #af-interface FastEthernet0/0 configuramos la interfaz fastEthernet en el direccionamiento de familia

R1 (config-router-af-interface) #passive-interface configuramos el anuncio de la informacion

R1 (config-router-af-interface) #exit-af-interface salimos de la interfaz

R1 (config-router-af) #topology base configuramos la tabla base

R1 (config-router-af-topology) #exit-af-topology salimos de tabla base

R1 (config-router-af) #eigrp router-id 1.1.1.1 identificamos el router

R1 (config-router-af) #exit-address-family salimos de la direccion de familia

R2 (config) #router eigrp DUAL-STACK configuramos el protocolo eigrp para ipv4 e ipv6

R2 (config-router) #address-family ipv4 unicast autonomous-system 4 configuramos la direccion de familia ipv4 Como Sistema autónomo

R2 (config-router-af) #network 192.168.9.0 0.0.0.3 3 habilitamos el proceso en la interfaz

R2 (config-router-af) #eigrp router-id 2.2.2.2 identificamos el router

R2 (config-router-af) #exit-address-family salimos de la direccion de familia

R2 (config-router) #address-family ipv6 unicast autonomous-system 6 configuramos la direccion de familia ipv6 Como Sistema autónomo

1.1.9. Configurar las interfaces pasivas para EIGRP según sea apropiado

Configurar las interfaces pasivas para EIGRP según sea apropiado.

R2 (config-router-af) #af-interface FastEthernet0/0	configuramos las interfaz
fastEthernet en el direccionamiento de familia	
R2 (config-router-af-interface) #shutdown	apagar
R2 (config-router-af-interface) #exit-af-interface	configuramos la interfaz
R2 (config-router-af) #af-interface serial1/0	configuramos la interfaz serial
R2 (config-router-af-interface) #shutdown	apagar
R2 (config-router-af-interface) #exit-af-interface	salimos de la interfaz
R2 (config-router-af) #eigrp router-id 2.2.2.2	identificamos el router
R2 (config-router-af) #exit-address-family	salimos de la direccion de familia

R2#conf terminal

R2 (config) #router eigrp DUAL-STACK configuramos el protocolo eigrp para ipv4 e ipv6

R2 (config-router) #address-family ipv4 unicast autonomous-system 4 configuramos la direccion de familia ipv4 Como Sistema autónomo

R2 (config-router-af) #topology base configuramos la tabla base

R2 (config-router-af-topology) #distribute-list R3-to-R1 out distribuimos la lista de R3 a R1

R2 (config-router-af-topology) #redistribute ospfv3 1 metric 10000 100 255 1 1500

Distribuimos las metricas de protocolo de enrutamiento

R2 (config-router-af-topology) #exit-af-topology salimos de la tabla base

1.1.10. En R2, configurar la redistribucion mutua entre OSPF y EIGRP para IPv4 e IPv6

Asignar métricas apropiadas cuando sea necesario

R2 (config) #Router eigrp DUAL-STACK configuramos el protocolo eigrp para ipv4 e ipv6

R2 (config-router) #address-family ipv4 unicast autonomous-system 4 configuramos la direccion de familia ipv4 Como Sistema autónomo

R2 (config-router-af) #topology base configuramos la tabla base

R2 (config) #distribute-list R3-to-R1 out distribuimos la lista de R3 a R1

R2 (config-router-af-topology) #redistribute ospfv3 1 metric 10000 100 255 1 1500

Distribuimos las metricas de protocolo de enrutamiento

R2 (config-router-af-topology) #exit-af-topology salimos de la tabla base

R2 (config-router) #address-family ipv6 unicast autonomous-system 6 configuramos la direccion de familia ipv6 Como Sistema autónomo

R2 (config-router-af) #topology base configuramos la Tabla base eigrp

R2 (config-router-af-topology) #redistribute ospf 1 metric 10000 100 255 1 1500

Distribuimos las metricas de protocolo de enrutamiento

R2 (config-router-af-topology) #exit-af-topology salimos de la tabla base

1.1.11.En R2, debe hacer publicidad de ruta 192.168.3.0/24 a R1 mediante una lista de distribución ACL

R2 (config-router) #ip access-list standard R2-to-R1 configuramos el acceso de la lista standard de R2 a R1

R2 (config-std-nacl) #remark ACL to filter 192.168.3.0/24 configuramos la filtracion lista con ACL

R2 (config-std-nacl) #deny 192.168.3.0 0.0.0.255 negamos la filtracion a esta direccion ip

R2 (config-std-nacl) #permit any permitimos la filtracion al protocolo de enrutamiento

R2 (config) #router ospfv3 1 configuramos el procolo de enrutamiento

R2 (config-router) #address-family ipv4 unicast configuramos la direccion de familia ipv4

R2 (config-router-af) #redistribute eigrp 4 redistribucion al protocolo eigrp

R2 (config-router-af) #address-family ipv6 unicast configuramos la direccion de familia ipv6

R2 (config-router-af) #redistribute eigrp 6 redistribucion al protocolo eigrp

R2 (config-router-af) #exit-address-family salimos del direccionamiento de familia

1.2. Parte 2

Verificar conectividad de red y control de la trayectoria.

1.2.1. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.

```

*May 27 20:29:54.791: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, H - HSRP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - ISIS
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.9.2 to network 0.0.0.0

D*EX 0.0.0.0/0 [170/50752000] via 192.168.9.2, 00:16:12, Serial1/0
    192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.9.0/24 is directly connected, Serial1/0
L       192.168.9.1/32 is directly connected, Serial1/0
R1#

```

Figura 2 show ipv6 route en R1

Utilizamos comando show ip route para verificar las rutas en las tablas de encaminamiento en R1


```

*May 27 20:28:22.131: %SYS-5-CONFIG_I: Configured from console by console
R2#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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.9.6 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.9.6, 00:13:46, Serial1/1
     192.168.9.0/24 is variably subnetted, 3 subnets, 2 masks
C     192.168.9.0/24 is directly connected, Serial1/1
     is directly connected, Serial1/0
L     192.168.9.2/32 is directly connected, Serial1/0
L     192.168.9.5/32 is directly connected, Serial1/1
R2#

```

Figura 3 comando show ip route

Utilizamos el comando show ipv6 route para verificar si las redes ipv6 y las direcciones especificas ipv6 se instalaron en la tabla de enrutamiento ipv6 en R2

```

0 192.168.9.1          Ser1/0          10 00:26:39 111 1170 0 9
R2#show ipv6 ospf
Routing Process "ospfv3 1" with ID 2.2.2.2
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
  eigrp 6
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 1. Checksum Sum 0x00788C
Number of areas in this router is 2. 1 normal 1 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
Area BACKBONE(0)

```

Figura 4 comando show ipv6 ospf en R2

Utilizamos el comando show ipv6 route para verificar si las redes ipv6 y las direcciones especificas ipv6 se instalaron en la tabla de enrutamiento ipv6 en R2

```

R2#
R2#show ipv6 ospf database

      OSPFv3 Router with ID (2.2.2.2) (Process ID 1)

      Router Link States (Area 0)

ADV Router      Age          Seq#          Fragment ID   Link count    Bits
2.2.2.2         910          0x80000004   0              1              E
3.3.3.3         318          0x80000004   0              1              E

      Link (Type-8) Link States (Area 0)

ADV Router      Age          Seq#          Link ID        Interface
2.2.2.2         910          0x80000002   5              Se1/1
3.3.3.3         823          0x80000002   5              Se1/1

      Intra Area Prefix Link States (Area 0)

ADV Router      Age          Seq#          Link ID        Ref-lsttype   Ref-LSID
2.2.2.2         910          0x80000002   0              0x2001        0
3.3.3.3         823          0x80000002   0              0x2001        0

      Router Link States (Area 1)

```

Figura 5 show ipv6 ospf en R2

Utilizamos el comando show ipv6 ospf para verificar la información de configuración ospfv3, incluyendo la ID del proceso ospf, y la del Router con las interfaces habilitadas

```

L      192.168.9.6/32 is directly connected, Serial1/1
R3#show ipv6 route
IPv6 Routing Table - default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDP - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
C      2001:DB8:ACAD:91::/64 [0/0]
       via Serial1/1, directly connected
L      2001:DB8:ACAD:91::2/128 [0/0]
       via Serial1/1, receive
L      FF00::/8 [0/0]
       via Null0, receive
R3#

```

Figura 6 show ipv6 route en R3

Utilizamos el comando show ipv6 route para verificar si las redes ipv6 y las direcciones específicas ipv6 se instalaron en la tabla de enrutamiento ipv6 en R2

```

via null0, receive
R3#show ipv6 ospf
Routing Process "ospfv3 1" with ID 3.3.3.3
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Originate Default Route with always
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 1. Checksum Sum 0x00788C
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
Area BACKBONE(0)

```

Figura 7 show ipv6 ospf en R3

Utilizamos el comando show ipv6 ospf para verificar la información de configuración ospfv3, incluyendo la ID del proceso ospf, y la del Router con las interfaces habilitadas en R3

```

R3#show ipv6 ospf database

OSPFv3 Router with ID (3.3.3.3) (Process ID 1)

Router Link States (Area 0)

ADV Router      Age      Seq#      Fragment ID  Link count  Bits
2.2.2.2         1113    0x80000004  0            1           E
3.3.3.3         520     0x80000004  0            1           E

Link (Type-8) Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Interface
2.2.2.2         1113    0x80000002  5            Se1/1
3.3.3.3         1025    0x80000002  5            Se1/1

Intra Area Prefix Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Ref-lstype  Ref-LSID
2.2.2.2         1113    0x80000002  0            0x2001      0
3.3.3.3         1025    0x80000002  0            0x2001      0

Type-5 AS External Link States

```

Figura 8 show ipv6 ospf en R3

Utilizamos el comando show ipv6 ospf para verificar la información de configuración ospfv3, incluyendo la ID del proceso ospf, y la del Router con las interfaces habilitadas en R3

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

```
R1(tcl)#foreach address (
+>(tcl)#192.168.10.1
+>(tcl)#192.168.9.1
+>(tcl)#192.168.9.0
+>(tcl)#192.168.2.1
+>(tcl)#192.168.9.5
+>(tcl)#192.168.0.0
+>(tcl)#
+>(tcl)#192.168.3.1
+>(tcl)#) { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.0, timeout is 2 seconds:

Reply to request 0 from 192.168.9.2, 72 ms
Reply to request 1 from 192.168.9.2, 160 ms
Reply to request 2 from 192.168.9.2, 120 ms
Reply to request 3 from 192.168.9.2, 140 ms
Reply to request 4 from 192.168.9.2, 152 ms
Type escape sequence to abort.
```

Figura 9 ping R1

Con el comando ping traceroute verificamos la comunicación entre los routers

```

R2#tclsh
R2(tcl)#foreach address {
+>(tcl)#192.168.10.1
+>(tcl)#192.168.9.1
+>(tcl)#192.168.9.0
+>(tcl)#192.168.2.1
+>(tcl)#192.168.9.5
+>(tcl)#192.168.0.0
+>(tcl)#
+>(tcl)#192.168.3.1
+>(tcl)#) { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
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 = 208/288/404 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.0, timeout is 2 seconds:

Reply to request 0 from 192.168.9.1, 236 ms
Reply to request 1 from 192.168.9.1, 92 ms
Reply to request 2 from 192.168.9.1, 92 ms
Reply to request 3 from 192.168.9.1, 156 ms
Reply to request 4 from 192.168.9.1, 108 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

```

Figura 10 ping R2

Con el comando ping traceroute verificamos la comunicación entre los routers

```

R3#
R3#TCLSH
R3(tcl)#foreach address {
+>(tcl)#192.168.10.1
+>(tcl)#192.168.9.1
+>(tcl)#192.168.9.0
+>(tcl)#192.168.2.1
+>(tcl)#192.168.9.5
+>(tcl)#192.168.0.0
+>(tcl)#
+>(tcl)#192.168.3.1
+>(tcl)#) { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
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 = 192/247/324 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.0, timeout is 2 seconds:

Reply to request 0 from 192.168.9.5, 68 ms
Reply to request 1 from 192.168.9.5, 92 ms
Reply to request 2 from 192.168.9.5, 48 ms
Reply to request 3 from 192.168.9.5, 60 ms
Reply to request 4 from 192.168.9.5, 20 ms

```

Figura 11 ping R3

Con el comando ping traceroute verificamos la comunicación entre los routers

1.2.3. Verificar que las rutas filtradas no estén presentes en las tablas de enrutamiento de los routers correctas

```

interface FastEthernet0/0
 ip address 192.168.110.1 255.255.255.0
 duplex half
 ipv6 address 2001:DB8:ACAD:110::1/64
 !
interface Serial1/0
 bandwidth 128
 ip address 192.168.9.1 255.255.255.0
 ipv6 address 2001:DB8:ACAD:90::1/64
 serial restart-delay 0
 clock rate 128000
 !
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
 !
interface Serial1/2
 no ip address
 shutdown
--More--

```

Figura 12 show runn R1

Utilizamos el comando show runn para visualizar el estado del Router y las tablas de enrutamiento en R1.

```

interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex half
 ipv6 address 2001:DB8:ACAD:B::1/64
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 0
 !
interface Serial1/0
 bandwidth 128
 ip address 192.168.9.2 255.255.255.0
 ipv6 address 2001:DB8:ACAD:90::2/64
 serial restart-delay 0
 !
interface Serial1/1
 bandwidth 128
 ip address 192.168.9.5 255.255.255.0
 ipv6 address 2001:DB8:ACAD:91::1/64
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 0
 serial restart-delay 0
 clock rate 128000
 !
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
 !
interface Serial1/3

```

Figura 13 show runn en R2

Utilizamos el comando show runn para visualizar el estado del Router y las tablas de enrutamiento en R2.

```

interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
duplex half
ipv6 address 2001:DB8:ACAD:C::1/64
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
bandwidth 128
ip address 192.168.9.6 255.255.255.0
ipv6 address 2001:DB8:ACAD:91::2/64
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0

```

Figura 14 show runn en R3

Utilizamos el comando show runn para visualizar el estado del Router y las tablas de enrutamiento en R3.

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, Etherchannel, VLANs y demás aspectos que forman parte del escenario propuesto.

Topología de red

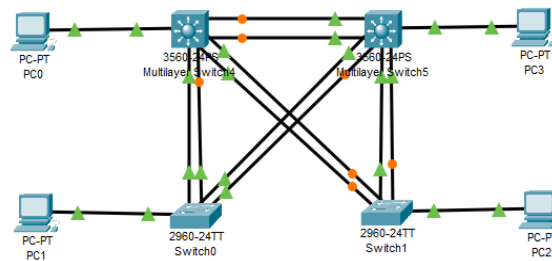
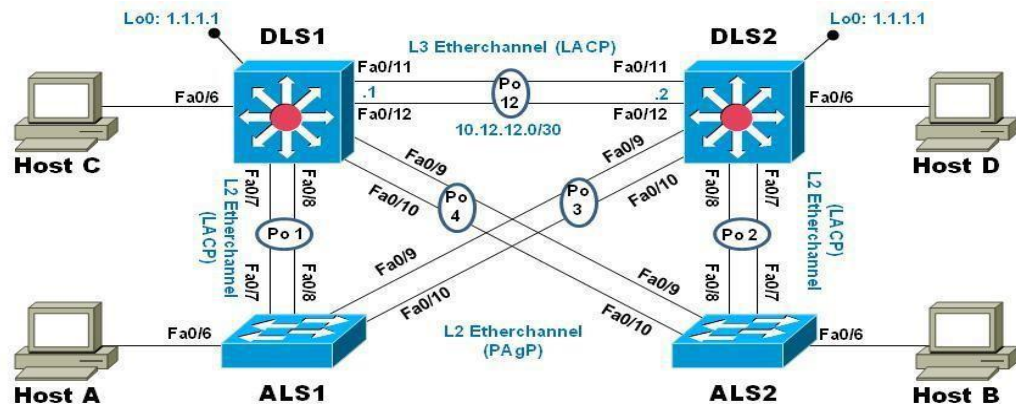


Figura 15 topología escenario 2

2.1. Parte 1:

Configurar la red de acuerdo con las especificaciones.

2.1.1. Apagar todas las interfaces en cada switch.

Ingresamos a los switch en modo de configuración global corremos el siguiente comando

Switch>enable

modo privilegiado

Switch (config) #configure terminal

Configuración global

Switch (config) # interface range f0/1-24

apagamos las interfaces

Switch (config-if-range) # shutdown apagar

2.1.2. Asignar un nombre a cada switch acorde al escenario establecido.

Con los siguientes comandos asignamos el nombre a cada switch

Switch>enable	modo privelegiado
Switch (config) #configure terminal	Configuracion global
Switch (config) #hostname DSL1	asignamos el nombre al switch
Switch>enable	modo privelegiado
Switch (config) #configure terminal	Configuracion global
Switch (config) #hostname DSL2	asignamos el nombre al switch
Switch>enable	modo privelegiado
Switch (config) #configure terminal	Configuracion global
Switch (config) #hostname ALS1	asignamos el nombre al switch
Switch>enable	modo privelegiado
Switch (config) #configure terminal	Configuracion global
Switch (config) #hostname ALS2	asignamos el nombre al switch

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

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.

Para realizar esta configuración ingresamos en modo configuración global el switch DSL1 creamos primero el Portchannel 12, al ser un Portchannel en L3 desactivamos el switchport tanto en el Portchannel como en las interfaces que participan en ese grupo

DLS1>enable	modo privelegiado
DLS1#configure terminal	Configuracion global

DLS1 (config) #interface port-channel 12	configuramos el puerto 12
DLS1 (config-if) #no switchport	desactivamos el modo enrutado
DLS1 (config-if) #ip address 10.12.12.1 255.255.255.252	configuramos la direccion ip y mascara subred
DLS1 (config-if) #exit	salimos del modo Configuracion
DLS1 (config) #interface range fa0/11-12	configuramos el rango de interfaces
DLS1 (config-if-range) #no switchport	desactivamos el mode de enrutado
DLS1 (config-if-range) #channel-group 12 mode active	activamos el grupo 12 de canalización de puertos
DLS1 (config-if-range) #exit	salimos del modo Configuracion
DLS1 (config) #exit	

DLS2>enable	modo privelegiado
DLS2#configure terminal	Configuracion global
DLS2 (config) #interface port-channel 12	configuramos el puerto 12
DLS2 (config-if) #no switchport	desactivamos el modo enrutado
DLS2 (config-if) #ip address 10.12.12.2 255.255.255.252	configuramos la direccion ip y mascara subred

DLS2 (config-if) #exit	salimos del modo Configuracion
DLS2 (config) #interface range fa0/11-12	configuramos el rango de interfaces
DLS2 (config-if-range) #no switchport	desactivamos el mode de enrutado
DLS2 (config-if-range) #channel-group 12 mode active	activamos el grupo 12 de canalización de puertos
DLS2 (config-if-range) #exit	salimos del modo Configuracion

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

Ingresamos en modo configuración global y creamos primero el port-channel 1 en DSL1 y port-channel 2 en DSL2 encenderos la interfaz, luego asociaremos las interfaces que participan en el grupo port-channel 1y 2

DLS1#enable modo privelegiado
DLS1#configure terminal modo Configuracion global
DLS1 (config) #interface range fa0/7-8 configuramos el rango de interfaces
DLS1 (config-if-range) #switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch
DLS1 (config-if-range) #switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal
DLS1 (config-if-range) #channel-group 1 mode active activamos el grupo 1 de canalización de puertos
DLS1 (config-if-range) #no shutdown no apagar

ALS1#enable modo privelegiado
ALS1#configure terminal modo Configuracion global
ALS1 (config) #interface range fa0/7-8 configuramos el rango de interfaces
ALS1 (config-if-range) #switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch
ALS1 (config-if-range) #switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal
ALS1 (config-if-range) #channel-group 1 mode active activamos el grupo 1 de canalización de puertos
ALS1 (config-if-range) #no shutdown no apagar

DLS2#enable modo privelegiado
DLS2#configure terminal modo Configuracion global

DLS2 (config) #interface range fa0/7-8 configuramos el rango de interfaces

DLS2 (config-if-range) #switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

DLS2 (config-if-range) #switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

DLS2 (config-if-range) #channel-group 2 mode active activamos el grupo 2 de canalización de puertos

DLS2 (config-if-range) #no shutdown no apagar

Configuracion de Portchannel

ALS2 (config) #interface range fa0/7-8 configuramos el rango de interfaces

ALS2 (config-if-range) #switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

ALS2 (config-if-range) #switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

ALS2 (config-if-range) #channel-group 2 mode active activamos el grupo 2 de canalización de puertos

ALS2 (config-if-range) #no shutdown no apagar

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

Ingresamos al modo configuración global y creamos el port-channel 3 L2 entre DSL1 y ALS2 luego creamos el port-channel 4 entre DSL2 y ALS21 encenderemos la interfaz y asociamos las interfaces que participan en el grupo port-channel 3 y 4

DLS1#enable modo privilegiado

DLS1#configure terminal modo Configuración global

DLS1 (config) #interface range fa0/9-10 configuramos el rango de interfaces

DLS1 (config-if-range) # switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

DLS1 (config-if-range) # switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

DLS1 (config-if-range) #channel-group 4 mode desirable establecemos el grupo 4 de canales como deseable

Creating a port-channel interface Port-channel 4

DLS1 (config-if-range) #no shutdown no apagar

ALS2#enable modo privelegiado

ALS2#configure terminal modo Configuracion global

ALS2 (config) #interface range fa0/9-10 configuramos el rango de interfaces

ALS2 (config-if-range) # switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

ALS2 (config-if-range) # switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

ALS2 (config-if-range) #channel-group 4 mode desirable establecemos el grupo 4 de canales como deseable

Creating a port-channel interface Port-channel 4

ALS2 (config-if-range) #no shutdown no apagar

DLS2#enable modo privelegiado

DLS2#configure terminal modo Configuracion global

DLS2 (config) #interface range fa0/9-10 configuramos el rango de interfaces

DLS2 (config-if-range) # switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

DLS2 (config-if-range) # switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

DLS2 (config-if-range) #channel-group 3 mode desirable establecemos el grupo 3 de canales como deseable

Creating a port-channel interface Port-channel 3

DLS2 (config-if-range) #no shutdown no apagar

ALS1#enable modo privelegiado

ALS1#configure terminal modo Configuracion global

ALS1 (config) #interface range fa0/9-10 configuramos el rango de interfaces

ALS1 (config-if-range) #switchport trunk encapsulation dot1q configuramos el canal de los puertos del switch

ALS1 (config-if-range) #switchport mode trunk configuramos el Puerto del switch a un extremo de un enlace troncal

ALS1 (config-if-range) #channel-group 3 mode desirable establecemos el grupo 3 de canales como deseable

Creating a port-channel interface Port-channel 3

ALS1 (config-if-range) #no shutdown no apagar

2.1.6. Todos los puertos troncales serán asignados a la VLAN 800 como la VLAN

Luego usamos el siguiente comando para asignar la vlan 800 como vlan nativa para todos los puertos troncales en todos los switches, en nuestro caso son las interfaces que pertenecen a los Portchannel 1, 2,3 y 4

DLS1#show interfaces trunk

DLS1#configure terminal modo Configuracion global

DLS1 (config) #interface Po1	configuramos el Puerto troncal 1
DLS1 (config-if) #switchport trunk native vlan 800	configuramos la ID de la vlan nativa 800 como puerto troncal
DLS1 (config-if) #exit	salimos del modo Configuracion
DLS1 (config) #interface Po4	configuramos el Puerto troncal 1
DLS1 (config-if) #switchport trunk native vlan 800	configuramos la ID de la vlan nativa 800 como puerto troncal
DLS1 (config-if) #exit	salimos del modo Configuracion
DLS2#enable	modo privelegiado
DLS2#configure terminal	modo Configuracion global
DLS2 (config) #interface Po2	configuramos el Puerto troncal 2
DLS2 (config-if) #switchport trunk native vlan 800	configuramos la ID de la vlan nativa 800 como puerto troncal
DLS2 (config-if) #exit	salimos del modo Configuracion
DLS2 (config-if) #interface Po3	configuramos el Puerto troncal 2
DLS2 (config-if) #switchport trunk native vlan 800	configuramos la ID de la vlan nativa 800 como puerto troncal
DLS2 (config-if) #exit	salimos del modo Configuracion
ALS1#enable	modo privelegiado
ALS1#configure terminal	modo Configuracion global
ALS1 (config-if) #interface Po1	configuramos el Puerto troncal 1
ALS1 (config-if) #switchport trunk native vlan 800	configuramos la ID de la vlan nativa 800 como puerto troncal
ALS1 (config-if) #exit	salimos del modo Configuracion
ALS1 (config) #interface Po3	configuramos el Puerto troncal 3

ALS1 (config-if) #switchport trunk native vlan 800 configuramos la ID de la vlan nativa 800 como puerto troncal

ALS2#enable modo privilegiado

ALS2#configure terminal modo Configuracion global

ALS2 (config) #interface Po2 configuramos el Puerto troncal 2

ALS2 (config-if) #switchport trunk native vlan 800 configuramos la ID de la vlan nativa 800 como puerto troncal

ALS2 (config-if) #interface Po4 configuramos el Puerto troncal 4

ALS2 (config-if) #switchport trunk native vlan 800 configuramos la ID de la vlan nativa 800 como puerto troncal

2.1.7. Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 2

Utilizar el nombre de dominio UNAD con la contraseña cisco123

DLS1 (config) #vtp domain UNAD configuramos el dominio unad en vtp
protocolo de mensajes 2

Domain name already set to UNAD.

DLS1 (config) #vtp pass cisco123 configuramos la contraseña

Setting device VLAN database password to cisco123

DLS1 (config) #vtp versión 2 configuramos vtp versión 2

ALS1 (config) #vtp domain UNAD configuramos el dominio unad
en vtp protocolo de mensajes 2

Domain name already set to UNAD.

ALS1 (config) #vtp pass cisco123 configuramos la contraseña

Setting device VLAN database password to cisco123

ALS1 (config) #vtp versión 2 configuramos vtp versión 2

ALS2 (config) #vtp domain UNAD configuramos el dominio unad en vtp
protocolo de mensajes 2

Changing VTP domain name from NULL to UNAD

ALS2 (config) #vtp pass cisco123 configuramos la contraseña

Setting device VLAN database password to cisco123

ALS2 (config) #vtp versión 2 configuramos vtp versión 2

2.1.8. Configurar DLS1 como servidor principal para las VLAN.

DLS1 (config) #vtp mode server configuramos DLS1 como servidor principal
para protocolo de mensajes 2 vlans

Device mode already VTP SERVER.

2.1.9. Configurar ALS1 y ALS2 como clientes VTP.

ALS1 (config) #vtp mode client configuramos ALS1 modo clientes para protocolo
de mensajes 2 vlans

Setting device to VTP CLIENT mode.

ALS2 (config) #vtp mode client configuramos ALS1 modo clientes para protocolo
de mensajes 2 vlans

Setting device to VTP CLIENT mode.

2.1.10. Configurar en el servidor principal las siguientes VLAN:

Tabla 1 direcciones vlans

Numero de vlan	Nombre de vlan	Numero de vlan	Nombre de vlan
800	nativa	434	estacionamiento
12	ejecutivos	123	mantenimiento
234	huéspedes	101	voz
111	videonet	345	administración

```

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
1 enet 100001 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

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

Remote SPAN VLANs
-----

Primary Secondary Type Ports
-----

```

Figura 16 comando VTP status ALS 2

2.1.11. En DLS1, suspender la VLAN 434.

DLS1 (config) #vlan 434

configuramos la vlan 434

DLS1 (config-vlan) # state suspend

suspendemos la vlan 434

```

DSL1#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
DSL1(config)#vlan 800
DSL1(config-vlan)#name NATIVA
DSL1(config-vlan)#vlan 12
DSL1(config-vlan)#name EJECUTIVOS
DSL1(config-vlan)#vlan 234
DSL1(config-vlan)#name HUESPEDES
DSL1(config-vlan)#vlan 1111
VLAN_CREATE_FAIL: Failed to create VLANs 1111 : extended VLAN(s) not allowed in current VTP mode
DSL1(config)#vlan 434
DSL1(config-vlan)#name ESTACIONAMIENTO
DSL1(config-vlan)#vlan 123
DSL1(config-vlan)#name MANTENIMIENTO
DSL1(config-vlan)#vlan 111
DSL1(config-vlan)#name VIDEONET
DSL1(config-vlan)#exit
DSL1(config)#vlan 434
DSL1(config-vlan)#state suspend
^

```

Figura 17 show vlan aplicado en DSL1

Para la versión de Switch que nos proporciona Packet Tracer 7.1.1 no se puede ejecutar este comando, por lo cual no podemos suspender la vlan.

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

En modo de configuración global publicamos el comando vtp mode transparent y seleccionamos la versión 2

DSL2#configure terminal	modo Configuración global
Enter configuration commands, one per line. End with CNTL/Z.	
DSL2 (config) #vlan 800	configuramos la vlan 800
DSL2 (config-vlan) #name NATIVA	asignamos el nombre
DSL2 (config-vlan) #vlan 12	configuramos la vlan 12
DSL2 (config-vlan) #name EJECUTIVOS	asignamos el nombre
DSL2 (config-vlan) #vlan 234	configuramos la vlan 234
DSL2 (config-vlan) #name HUESPEDES	asignamos el nombre
DSL2 (config-vlan) #vlan 111	configuramos la vlan 111
DSL2 (config-vlan) #name VIDEONET	asignamos el nombre
DSL2 (config-vlan) #vlan 434	configuramos la vlan 434
DSL2 (config-vlan) #name ESTACIONAMIENTO	asignamos el nombre
DSL2 (config-vlan) #vlan 123	configuramos la vlan 123
DSL2 (config-vlan) #name MANTENIMIENTO	asignamos el nombre
DSL2 (config-vlan) #vlan 101	configuramos la vlan 101
DSL2 (config-vlan) #name VOZ	asignamos el nombre
DSL2 (config-vlan) #vlan 345	configuramos la vlan 345
DSL2 (config-vlan) #name ADMINISTRACION	asignamos el nombre
DSL2 (config-vlan) #EXIT	salimos del modo Configuración
DSL2 (config) #	

```

DSL2#configure ter
Enter configuration commands, one per line.  End with CNTL/Z.
DSL2 (config)#vlan 800
DSL2 (config-vlan)#name NATIVA
DSL2 (config-vlan)#vlan 12
DSL2 (config-vlan)#name EJECUTIVOS
DSL2 (config-vlan)#vlan 234
DSL2 (config-vlan)#name HUESPEDES
DSL2 (config-vlan)#vlan 111
DSL2 (config-vlan)#name VIDEONET
DSL2 (config-vlan)#vlan 434
DSL2 (config-vlan)#name ESTACIONAMIENTO
DSL2 (config-vlan)#vlan 123
DSL2 (config-vlan)#name MANTENIMIENTO
DSL2 (config-vlan)#vlan 101
DSL2 (config-vlan)#name
DSL2 (config-vlan)#name VOZ
DSL2 (config-vlan)#vlan 345
DSL2 (config-vlan)#name ADMINISTRACION
DSL2 (config-vlan)#EXIT
DSL2 (config)#

```

Figura 18 Configuración VLAN en DSL2

DSL2 (config) #vtp mod Trans configuramos DLS2 en modo transparente
Setting device to VTP TRANSPARENT mode.

46

DSL2 (config) #vtp ver 2 configuramos la versión vtp 2

```

DSL2>enable
DSL2#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
DSL2(config)#vlan 800
DSL2 (config-vlan)#name NATIVA
DSL2 (config-vlan)#vlan 12
DSL2 (config-vlan)#name EJECUTIVOS
DSL2 (config-vlan)#vlan 234
DSL2 (config-vlan)#name HUESPEDES
DSL2 (config-vlan)#vlan 111
DSL2 (config-vlan)#name VIDEONET
DSL2 (config-vlan)#vlan 434
DSL2 (config-vlan)#name ESTACIONAMIENTO
DSL2 (config-vlan)#vlan 123
DSL2 (config-vlan)#name MANTENIMIENTO
DSL2 (config-vlan)#vlan 101
DSL2 (config-vlan)#name
DSL2 (config-vlan)#name VOZ
DSL2 (config-vlan)#vlan 345
DSL2 (config-vlan)#name ADMINISTRACION
DSL2 (config-vlan)#EXIT
DSL2 (config)#vtp mod trans
Setting device to VTP TRANSPARENT mode.

```

Figura 19 habilitación VTP mode transparent

2.1.13. Suspende VLAN 434 en DLS2.

Para la versión de Switch que nos proporciona Packet Tracer 7.1.1, no se puede ejecutar este comando, por lo cual no podemos suspender la vlan.

2.1.14. 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.

Creamos la vlan 567 para el departamento de contabilidad en el modo de configuración global. La vlan de contabilidad no podrá estar disponible en otro switch de la red.

DLS2#configure terminal	Configuración global
DLS2 (config) #vlan 567	configuramos la vlan 567
DLS2 (config-vlan) #name CONTABILIDAD	asignamos el nombre

```

DSL2 (config-vlan)#exit
DSL2 (config)#vlan 567
DSL2 (config-vlan)#name CONTABILIDAD
DSL2 (config-vlan)#

```

Figura 20 Configuración vlan 567 en DSL2

Luego en los 2 Portchannel troncales negamos el paso de la vlan 567.

```

DLS2#enable                                modo privilegiado
DLS2#configure terminal                    Configuración global
DLS2 (config) #interface port-channel 2   configuramos los puertos troncales 2
DLS2 (config-if) #switchport trunk allowed vlan except 567 negamos el paso de la
vlan 567 a los puertos troncales 2
DLS2 (config) #interface port-channel 3   configuramos los puertos troncales 3
DLS2 (config-if) #switchport trunk allowed vlan except 567 negamos el paso de la
vlan 567 a los puertos troncales 3

```

```

DSL2 (config-vlan)#exit
DSL2 (config)#vlan 567
DSL2 (config-vlan)#name CONTABILIDAD
DSL2 (config-vlan)#exit
DSL2 (config)#interface port-channel 2
DSL2 (config-if)#switchport trunk allowed vlan except 567
DSL2 (config-if)#interface port-channel 3
DSL2 (config-if)#switchport trunk allowed vlan except 567
DSL2 (config-if)#

```

Figura 21 Configuración negación al paso vlan 567

2.1.15. 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.

Esta configuración la realizamos en Configuración global con los siguientes comandos

DLS1#enable modo privilegiado

DLS1#configure terminal modo Configuración global

DLS1 (config) #spanning-tree vlan 1, 12,434,800,1010,1111,3456 root primary

Configuramos en DLS1 el protocolo de árbol de expansión con las vlans como raíz primaria

DLS1 (config) #spanning-tree vlan 123,234 root secondary

Configuramos en DLS1 el protocolo de árbol de expansión con las vlans como raíz secundaria

```
Spanning tree enabled protocol ieee
Root ID    Priority    25010
           Address    0050.0F1B.D833
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    25010 (priority 24576 sys-id-ext 434)
           Address    0050.0F1B.D833
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Po4          Desg FWD 9         128.28 Shr
Po1          Desg FWD 9         128.27 Shr

VLAN0800
Spanning tree enabled protocol ieee
Root ID    Priority    25376
```

Figura 22 Configuración Spanning tree

2.1.16. 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.

DLS2#enable modo privilegiado

DLS2#configure terminal modo Configuracion global

DLS2 (config) #spanning-tree vlan 123,234 root primary

Configuramos en DLS2 el protocolo de árbol de expansión con las vlans como raíz primaria

DLS2 (config) #spanning-tree vlan 1, 12, 434, 800, 1010, 1111,345 root secondary

Configuramos en DLS1 el protocolo de árbol de expansión con las vlans como raíz secundaria

```

VLAN0434
Spanning tree enabled protocol ieee
  Root ID    Priority    25010
            Address    0050.0F1B.D833
            Cost      18
            Port      28 (Port-channel3)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    29106 (priority 28672 sys-id-ext 434)
            Address    000C.CF10.0965
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Po2          Altn BLK 9         128.27 Shr
Po3          Root FWD 9         128.28 Shr

VLAN0800
Spanning tree enabled protocol ieee
  Root ID    Priority    25376
            Address    0050.0F1B.D833
            Cost      18
            Port      28 (Port-channel3)

```

Figura 23 Configuración Spanning-tree

2.1.17. 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.

Se configuran los puertos L2 mode trunk en el modo de configuración global.

DSL1# configure terminal modo Configuracion global

DLS1 (config) #int range f0/7 configuramos el rango de interfaces

DLS1 (config-if-range) #switchport mode trunk configuramos el Puerto del switch

a un extremo de un enlace troncal

DLS1 (config-if-range) #exit salimos del modo Configuracion


```

DSL1(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
%LINK-3-UPDOWN: Interface Port-channel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down
%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
%LINK-3-UPDOWN: Interface Port-channel4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4, changed state to down
%EC-5-CANNOT_BUNDLE2: Fa0/11 is not compatible with Fa0/12 and will be suspended (trunk encap of Fa0/11 is auto, Fa0/12
DSL1(config-if-range)#sw
%LINK-5-CHANGED: Interface Port-channel4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4, changed state to up
DSL1(config-if-range)#switchport trunk native vlan 8
%LINK-5-CHANGED: Interface Port-channel1, changed state to up

```

Figura 24 Configuración puertos troncales

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

Tabla 2 puertos de acceso

Interfaz	DSL1	DSL2	ALS1	ALS2
Interfaz fa0/6	3456	12, 1010	123, 1010	234
Interfaz fa0/15	1111	1111		1111
Interfaces f0/16-18		567		

Se debe ingresar al modo de configuración global de cada switch y configurar en modo acceso las interfaces indicadas en la tabla anterior con los siguientes comandos

DSL1 #configure terminal modo Configuración global
 DSL1 (config) # interface f0/6 configuramos el rango de interfaces
 DSL1 (config-if) #switchport mode Access configuramos el modo puerto de acceso
 DSL1 (config-if) #switchport mode Access vlan 3456 configuramos el modo puerto de acceso a la vlan 3456
 DSL1 (config-if) #no shutdown no apagar

```
DSL1 (config) # interface f0/15                    configuramos las interfaz
DLS1 (config-if) #switchport mode Access   configuramos el modo puerto de acceso
DLS1 (config-if) #switchport mode Access vlan 1111  configuramos el modo puerto de acceso a la vlan 1111
DLS1 (config-if) #no shutdown                no apagar

DSL2 #configure terminal                          modo Configuracion global
DSL2 (config) # interface f0/6                 configuramos las interfaz
DLS2 (config-if) #switchport mode Access   configuramos el modo puerto de acceso
DLS2 (config-if) #switchport mode Access vlan 12  configuramos el modo puerto de acceso a la vlan 12
DLS2 (config-if) #switchport mode Access   configuramos el modo puerto de acceso
DLS2 (config-if) #switchport mode Access vlan 1010  configuramos el modo puerto de acceso a la vlan 1010
DLS2 (config-if) #no shutdown                no apagar

DSL2 #configure terminal                          modo Configuracion global
DSL2 (config) # interface f0/16                configuramos las interfaz
DLS2 (config-if) #switchport mode Access   configuramos el modo puerto de acceso
DLS2 (config-if) #switchport mode Access vlan 567  configuramos el modo puerto de acceso a la vlan 567
DLS2 (config-if) #no shutdown                no apagar

DSL2 (config) # interface f0/16                configuramos las interfaz
DLS2 (config-if) #switchport mode Access   configuramos el modo puerto de acceso
DLS2 (config-if) #switchport mode Access vlan 1111  configuramos el modo puerto de acceso a la vlan 1111
DLS2 (config-if) #no shutdown                no apagar
```

ALS1 #configure terminal	modo Configuracion global
ALS1 (config) # interface range f0/6	configuramos el rango de interfaz
ALS1 (config-if) #switchport mode Access acceso	configuramos el modo puerto de acceso
ALS1 (config-if) #switchport mode Access vlan 123 de acceso a la vlan 123	configuramos el modo puerto de acceso a la vlan 123
ALS1 (config-if) #switchport mode Access acceso	configuramos el modo puerto de acceso
ALS1 (config-if) #switchport mode Access vlan 1010 de acceso a la vlan 1010	configuramos el modo puerto de acceso a la vlan 1010
ALS1 (config-if) #no shutdown	no apagar
ALS2 #configure terminal	modo Configuracion global
ALS2 (config) # interface range f0/6	configuramos el rango de interfaz
ALS2 (config-if) #switchport mode Access acceso	configuramos el modo puerto de acceso
ALS2 (config-if) #switchport mode Access vlan 234 de acceso a la vlan 234	configuramos el modo puerto de acceso a la vlan 234
ALS2 (config-if) #no shutdown	no apagar
ALS2 #configure terminal	modo Configuracion global
ALS2 (config) # interface range f0/15	configuramos el rango de interfaz
ALS2 (config-if) #switchport mode Access acceso	configuramos el modo puerto de acceso
ALS2 (config-if) #switchport mode Access vlan 1111 de acceso a la vlan 1111	configuramos el modo puerto de acceso a la vlan 1111
ALS2 (config-if) #no shutdown	no apagar

```

DSL2(config-if)#exit
DSL2(config)#spanning-tree vlan 123,234 root primary
DSL2(config)#spanning-tree vlan 123,234 root primary
DSL2(config)#spanning-tree vlan 1,12,434,800,101,111,345 root secondary
DSL2(config)#spanning-tree vlan 1,12,434,800,1010,1111,3456 root secondary
DSL2(config)#interface f0/6
DSL2(config-if)#switchport access vlan 12
DSL2(config-if)#switchport access vlan 1010
DSL2(config-if)#no shutdown

DSL2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

DSL2(config-if)#interface f0/15
DSL2(config-if)#switchport access vlan 1111
% Access VLAN does not exist. Creating vlan 1111
DSL2(config-if)#switchport access vlan 1111
DSL2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to down
DSL2(config-if)#
DSL2(config-if)#exit
DSL2(config)#interface range f0/16-18
DSL2(config-if-range)#switchport access vlan 567
DSL2(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to down
DSL2(config-if-range)#
DSL2(config-if-range)#

```

Figura 25 Configuración interfaces

2.2. Parte 2:

Conectividad de red de prueba y las opciones configuradas.

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

```

DSL1>enable
DSL1#show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
12	EJECUTIVOS	active	
111	VIDEONET	active	
123	MANTENIMIENTO	active	
234	HUESPEDES	active	
434	ESTACIONAMIENTO	active	
800	NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
12	enet	100012	1500	-	-	-	-	-	0	0
111	enet	100111	1500	-	-	-	-	-	0	0
123	enet	100123	1500	-	-	-	-	-	0	0
234	enet	100234	1500	-	-	-	-	-	0	0
434	enet	100434	1500	-	-	-	-	-	0	0
800	enet	100800	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0

Figura 26 verificación vlan 1

Utilizamos el comando show vlan para verificar el tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, 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
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

DSL1>ENABLE
DSL1#SHOW INTERFACE TRUNK
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    800
Po4       on        802.1q         trunking    800

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

Port      Vlans allowed and active in management domain
Po1       1,12,111,123,234,434,800
Po4       1,12,111,123,234,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po1       none
Po4       1,12,111,434,800

DSL1#

```

Figura 27 verificación de vlan DSL1

Utilizamos el comando show vlan para verificar el tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

IOS Command Line Interfac

VLAN	Name	Status	Ports
1	default	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
12	EJECUTIVOS	active	
101	VOZ	active	
111	VIDEONET	active	
123	MANTENIMIENTO	active	
234	HUESPEDES	active	
345	ADMINISTRACION	active	
434	ESTACIONAMIENTO	active	
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	VLAN1010	active	Fa0/6
1111	VLAN1111	active	Fa0/15

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
12	enet	100012	1500	-	-	-	-	-	0	0
101	enet	100101	1500	-	-	-	-	-	0	0
111	enet	100111	1500	-	-	-	-	-	0	0
123	enet	100123	1500	-	-	-	-	-	0	0
234	enet	100234	1500	-	-	-	-	-	0	0
345	enet	100345	1500	-	-	-	-	-	0	0
434	enet	100434	1500	-	-	-	-	-	0	0
567	enet	100567	1500	-	-	-	-	-	0	0

Figura 28 verificación de vlan

Utilizamos el comando show vlan para verificar el tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

```

%LINK-5-CHANGED: Interface Port-channel3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up
%LINK-5-CHANGED: Interface Port-channel2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up

DSL2>ENABLE
DSL2#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    800
Po3       on        802.1q         trunking    800

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

Port      Vlans allowed and active in management domain
Po2       1,12,101,111,123,234,345,434,800
Po3       1,12,101,111,123,234,345,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po2       101,123,234,345
Po3       1,12,101,111,123,234,345,434,800
DSL2#

```

Figura 29 verificación de vlan DSL2

Utilizamos el comando show vlan para verificar le tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
12 EJECUTIVOS	active	
111 VIDEONET	active	
123 MANTENIMIENTO	active	
234 HUESPEDES	active	
434 ESTACIONAMIENTO	active	
800 NATIVA	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
12	enet	100012	1500	-	-	-	-	-	0	0
111	enet	100111	1500	-	-	-	-	-	0	0
123	enet	100123	1500	-	-	-	-	-	0	0
234	enet	100234	1500	-	-	-	-	-	0	0
434	enet	100434	1500	-	-	-	-	-	0	0
800	enet	100800	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Figura 30 Verificación de vlan

Utilizamos el comando show vlan para verificar le tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up
%LINK-5-CHANGED: Interface Port-channel3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

ALS1>enable
ALS1#show interface trunk
Port      Mode      Encapsulation  Status        Native vlan
Po1       on        802.1q         trunking     800
Po3       on        802.1q         trunking     800

Port      Vlans allowed on trunk
Po1       1-1005
Po3       1-1005

Port      Vlans allowed and active in management domain
Po1       1,12,111,123,234,434,800
Po3       1,12,111,123,234,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,12,111,123,234,434,800
Po3       1,12,111,123,234,434,800

ALS1#

```

Figura 31 Verificación de vlan ALS1

Utilizamos el comando show vlan para verificar le tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

```

-----
1      default                active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
12     EJECUTIVOS             active
111    VIDEONET                 active
123    MANTENIMIENTO           active
234    HUESPEDES              active
434    ESTACIONAMIENTO        active
800    NATIVA                  active
1002   fddi-default            active
1003   token-ring-default     active
1004   fddinet-default        active
1005   trnet-default          active

VLAN Type  SAID      MTU   Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1      enet   100001    1500  -      -      -        -   -         0      0
12     enet   100012    1500  -      -      -        -   -         0      0
111    enet   100111    1500  -      -      -        -   -         0      0
123    enet   100123    1500  -      -      -        -   -         0      0
234    enet   100234    1500  -      -      -        -   -         0      0
434    enet   100434    1500  -      -      -        -   -         0      0
800    enet   100800    1500  -      -      -        -   -         0      0
1002   fddi   101002    1500  -      -      -        -   -         0      0
1003   tr     101003    1500  -      -      -        -   -         0      0
1004   fdnet  101004    1500  -      -      -        ieee -         0      0
1005   trnet  101005    1500  -      -      -        ibm  -         0      0

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

```

Figura 32 Verificación de vlan

Utilizamos el comando show vlan para verificar le tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up

ALS2>enable
ALS2#show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Po2       on            802.1q         trunking      800
Po4       on            802.1q         trunking      800

Port      Vlans allowed on trunk
Po2       1-1005
Po4       1-1005

Port      Vlans allowed and active in management domain
Po2       1,12,111,123,234,434,800
Po4       1,12,111,123,234,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,12,111,123,234,434,800
Po4       1,12,111,123,234,434,800

ALS2#

```

Figura 33 Verificación de vlan ALS2

Utilizamos el comando show vlan para verificar le tipo de asignación y pertenencia de vlan para todos los puertos de los switch.

2.2.2. Verificar que el Etherchannel entre DLS1 y ALS1 está configurado correctamente.

```

DSL1#enable
DSL1#SHOW INTERFACE TRUNK
Port      Mode          Encapsulation  Status        Native vlan
Po1       on            802.1q         trunking      800
Po4       on            802.1q         trunking      800

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

Port      Vlans allowed and active in management domain
Po1       1,12,111,123,234,434,800
Po4       1,12,111,123,234,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po1       none
Po4       1,12,111,434,800

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
-----

```

Figura 34 Verificación de interfaces DSL 1

Utilizamos el comando show interface trunk para verificar port-channel entre DSL1 y DSL2 está configurado de manera correcta.


```

DSL2>enable
DSL2#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po2       on        802.1q         trunking    800
Po3       on        802.1q         trunking    800

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

Port      Vlans allowed and active in management domain
Po2       1,12,101,111,123,234,345,434,800
Po3       1,12,101,111,123,234,345,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po2       101,123,234,345
Po3       1,12,101,111,123,234,345,434,800

DSL2#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

```

Figura 35 Verificación de interfaces DSL 2

Utilizamos el comando show interface trunk para verificar port-channel entre DSL1 y DSL2 está configurado de manera correcta.

```

ALS1>enable
ALS1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    800
Po3       on        802.1q         trunking    800

Port      Vlans allowed on trunk
Po1       1-1005
Po3       1-1005

Port      Vlans allowed and active in management domain
Po1       1,12,111,123,234,434,800
Po3       1,12,111,123,234,434,800

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,12,111,123,234,434,800
Po3       1,12,111,123,234,434,800

ALS1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone   s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

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

```

Figura 36 Verificación de interfaces ALS 1

Utilizamos el comando show interface trunk para verificar port-channel entre DSL1 y DSL2 está configurado de manera correcta.

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

```

                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID      Priority 28795 (priority 28672 sys-id-ext 123)
Address       0050.0F1B.D833
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time    20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po1            Root FWD 9         128.28 Shr
Po4            Altn BLK 9         128.29 Shr

VLAN0234
Spanning tree enabled protocol ieee
Root ID       Priority 24810
Address       000C.CF10.0965
Cost          18
Port         28 (Port-channell)
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID     Priority 28906 (priority 28672 sys-id-ext 234)
Address       0050.0F1B.D833
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time    20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po1            Root FWD 9         128.28 Shr
Po4            Altn BLK 9         128.29 Shr

VLAN0434
Spanning tree enabled protocol ieee
Root ID       Priority 25010
Address       0050.0F1B.D833
--More--

```

Figura 37 Spanning-tree entre DSL1 a DSL2

Utilizamos el comando show Spanning-tree para verificar la configuración STP entre DSL1 y DSL2 incluyendo sus prioridades de puerto.

```

                Address 000C.CF10.0965
                Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
                Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po2            Desg FWD 9         128.28 Shr
Fa0/7          Desg FWD 19        128.7  P2p
Fa0/8          Desg FWD 19        128.8  P2p
Fa0/9          Desg FWD 19        128.9  P2p
Fa0/10         Desg FWD 19        128.10 P2p
Po3            Desg FWD 9         128.29 Shr

VLAN0345
Spanning tree enabled protocol ieee
Root ID       Priority 29017
Address       000C.CF10.0965
This bridge is the root
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID     Priority 29017 (priority 28672 sys-id-ext 345)
Address       000C.CF10.0965
Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time    20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po2            Desg FWD 9         128.28 Shr
Fa0/7          Desg FWD 19        128.7  P2p
Fa0/8          Desg FWD 19        128.8  P2p
Fa0/9          Desg FWD 19        128.9  P2p
Fa0/10         Desg FWD 19        128.10 P2p
Po3            Desg FWD 9         128.29 Shr
--More-- |

```

Figura 38 Spanning-tree entre DSL2 a DSL 1

Utilizamos el comando show Spanning-tree para verificar la configuración STP entre DSL1 y DSL2 incluyendo sus prioridades de puerto.

CONCLUSIONES

Por medio de la redistribucion de protocolos es posible conectar redes que tengan configurado distinto protocolo, debido a que este Proceso importa y exporta las rutas de distintas redes.

EIGRP es un protocolo de transporte de datos bastante confiable, con capacidad de establecer adyacencias, utiliza métrica compuesta y utiliza el algoritmo de actualización por difusión (DUAL).

El área a través de la cual configura el enlace virtual OSPF, se denomina área de tránsito, debe tener información completa de enrutamiento y no puede ser un área Stubby

En NAT existen tipos de funcionamiento, tales como estática, dinámica, sobrecarga y solapamiento. NAT habilita las redes de IP privado que utilizan los IP Address no registrados para conectar con el internet.

SNMP es un protocolo estándar de internet para administrar dispositivos de redes IP, dicho protocolo está compuesto por un administrador SNMP, agente SNMP y los dispositivos administrados, en su tercera versión SNMP agrega mejoras en la seguridad y la confirmación remota, como por ejemplo el protocolo de autenticación MD5 Y SHA

BIBLIOGRAFÍAS

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). *DHCP*. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Cisco Networking Academy, & Staerk, B. (29 de noviembre de 2016). Practica de laboratorio. Obtenido de Tareas Unidall.zip: <https://onedrive.live.com/?authkey=%21ANzvU5YiwKf8Qac&cid=483D35BEE8610962&id=483D35BEE8610962%212935&parId=483D35BEE8610962%212934&action=locate>

ANEXOS

<https://drive.google.com/drive/folders/1LrqBte3IV1UNXwhADKKXhtDqMKhW8jCW?usp=sharing>