TRABAJO FINAL DIPLOMADO CCNP HABILIDADES PRACTICAS

LEONARDO FABIO CHAVARRO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
INGENIERIA EN TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
BOGOTA
2020

TRABAJO FINAL DIPLOMADO CCNP HABILIDADES PRACTICAS

LEONARDO FABIO CHAVARRO GUTIERREZ

Diplomado de profundización pruebas de habilidades prácticas

Directora
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
INGENIERIA EN TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
BOGOTA
2020

NOTA DE ACEPTACION

_____

_____
_____
_____
_____
_____
_____
_____

Presidente del jurado

_____

Jurado

_____

Bogotá 21 de Julio de 2020

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

Desde hace algunas décadas la transmisión de datos a través de redes se ha hecho fundamental en la producción de una compañía mediana o grande. por eso contar con las habilidades necesarias como ingenieros en telecomunicaciones es vital para el ejercicio de la profesión.

En el presente documento se presentan conceptos clave en entornos amplios usando protocolos de enrutamiento dinámico OSPF, EIGRP. Igualmente, la redistribución de redes. Por otra parte, una de las habilidades más apetecidas en la interconexión de redes de datos, es la de brindar soporte y soluciones eficaces a los problemas de conmutación que se pudieran presentar en entornos de red y el aislamiento de los problemas al trazar una red resiliente.

Con ese fin también se expondrá amplios conocimientos en una red switcheada ampliación de recursos a bajo costo usando protocolos como EtherChannel, al igual que el buen uso del protocolo para evitar bucles y garantizar rendimientos en la transmisión de paquetes como lo es el spanning-tree.

RESUMEN

Usando la metodología de aprendizaje basado en proyectos aunado al método habilidades prácticas de cisco se establecen dos escenarios en los cuales se examina en profundidad la adquisición de conceptos relevantes a la interconexión de elementos de red tales como switch y routers. Con un grado de complejidad avanzado para administrar redes pequeñas y medianas mediante protocolos de enrutamiento dinámico y configuraciones de elementos de red marca CISCO, se persigue el objetivo que el lector se familiarice con la composición de una red capa 2 y capa 3.

Aunque por supuesto actualmente las redes de conmutadores o switches no son tan básicas como hace un tiempo atrás, hay conceptos que tienden a desaparecer como el protocolo de troncalización dinámico pues la simple variación de un VLAN en el elemento de red que sirve como proveedor de estos recursos a toda una red, pudiera afectar exponencialmente el rendimiento y el alcance de los recursos.

La metodología que usa este documento es el de familiarizar al lector con los conceptos y comandos básicos hasta adentrarse en protocolos y modelos avanzados de red que sin duda lo beneficiará como un profesional en redes.

Conceptos clave **OSPF, EIGRP, VTP, PORTCHANNEL, TRONCALIZACION**

GLOSARIO

EIGRP: Protocolo dinámico de enrutamiento IGP propietario de CISCO, obtiene sus actualizaciones a través de un algoritmo denominado DUAL necesita adquirir adyacencia con los elementos de red próximos y actualizar sus tablas de topología y enrutamiento hasta lograr una convergencia completa antes de intercambiar datos .

OSPF: Protocolo dinámico de enrutamiento IGP en donde todos y cada unos de los elementos de red comparten las mismas tablas de topología y de adyacencia, usando un algoritmo SPF que permite calcular la ruta más optima teniendo como base el costo de los elementos próximos, este costo es fácilmente influenciado por la configuración.

REDISTRIBUCION: Es un método mediante el cual las redes aprendidas por un determinado protocolo de red son enseñadas a otro sin tener que realizar cambios significativos en los dispositivos de interconexión como los enrutadores.

FHRP: Protocolo de redundancia de primer salto por sus siglas en inglés, se tratar de menguar las fallas de conectividad hacia las redes externas configurando elementos de capa 3 de tal manera que entre ellos se crea una puerta de enlace y mac virtuales los cuales los elementos finales encuentran los recursos de red requeridos. al fallar un de estos elementos solo depende del tiempo de conmutación típico de un protocolo de esta clase. En este taller se usan el protocolo HSRP Y VRRP.

SPANNING-TREE: Método usado por un elemento de red de capa 2 para evitar loops lógicos, en los cuales se jerarquiza los elementos para que solo uno de ellos sea el predominante al distribuir el acceso a los recursos de red.

TRONCALIZACION: Configuración aplicada en un puerto de un switch por el cual es factible que se reciban y transmitan dos o más VLAN simultáneamente , es usado particularmente en interconexiones entre switches o elementos de capa 3 que distribuyan acceso a recursos de red de diferentes áreas.

VTP (vlan trunking protocol). Es uno de los primeros métodos cuya intención ara simplificar el método de distribución de VLAN a través de una red switcheada, sin embargo, rápidamente en entornos de producción real menguo su uso pues dependía de un solo concentrador el mantener optimizados los accesos a los diferentes recursos.

PORTCHANNEL: Agregación de una o más interfaces para incrementar el ancho de banda transportado por un canal o la disponibilidad de recursos, igualmente busca

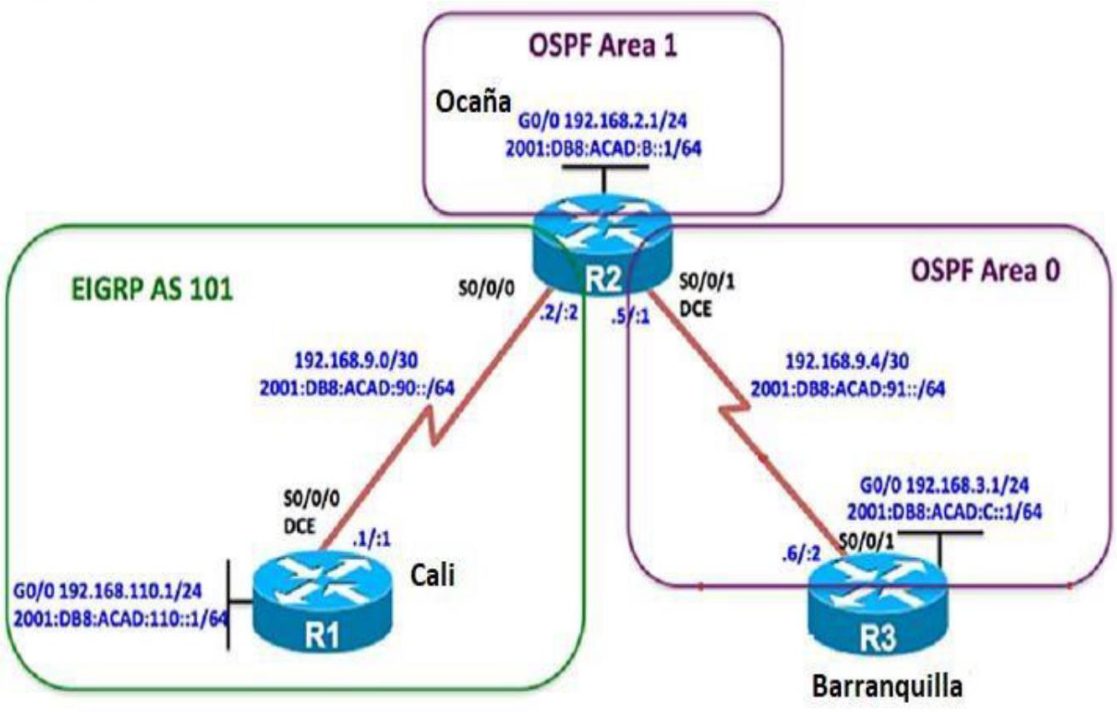
encontrar un entorno resiliente contra un fallo de una interfaz o medio de transmisión de datos definido. Usando protocolos de agregación de interfaces como LACP y PAgP busca sumarizar interfaces para este propósito.

ACCESO: Con esta expresión no solo se da referencia a la entrada de recursos de red si no a puertos en un switch que solo transporten una VLAN, el proposito es propagar solo y nada más que una VLAN a un elemento final como servidores, PCs o impresoras

1. ESCENARIO 1

1.1. CONFIGURACION DE INTERFACES DE LOS ROUTERS

FIGURA 1 ESCENARIO 1



Para establecer el escenario, el primer paso es la configuración de las interfaces y la comprobación de las redes directamente conectadas, se debe seguir el siguiente procedimiento y al finalizar revisar el proceso mediante ping:

1.1.1. Configuración de interfaces en R1,R2,R3

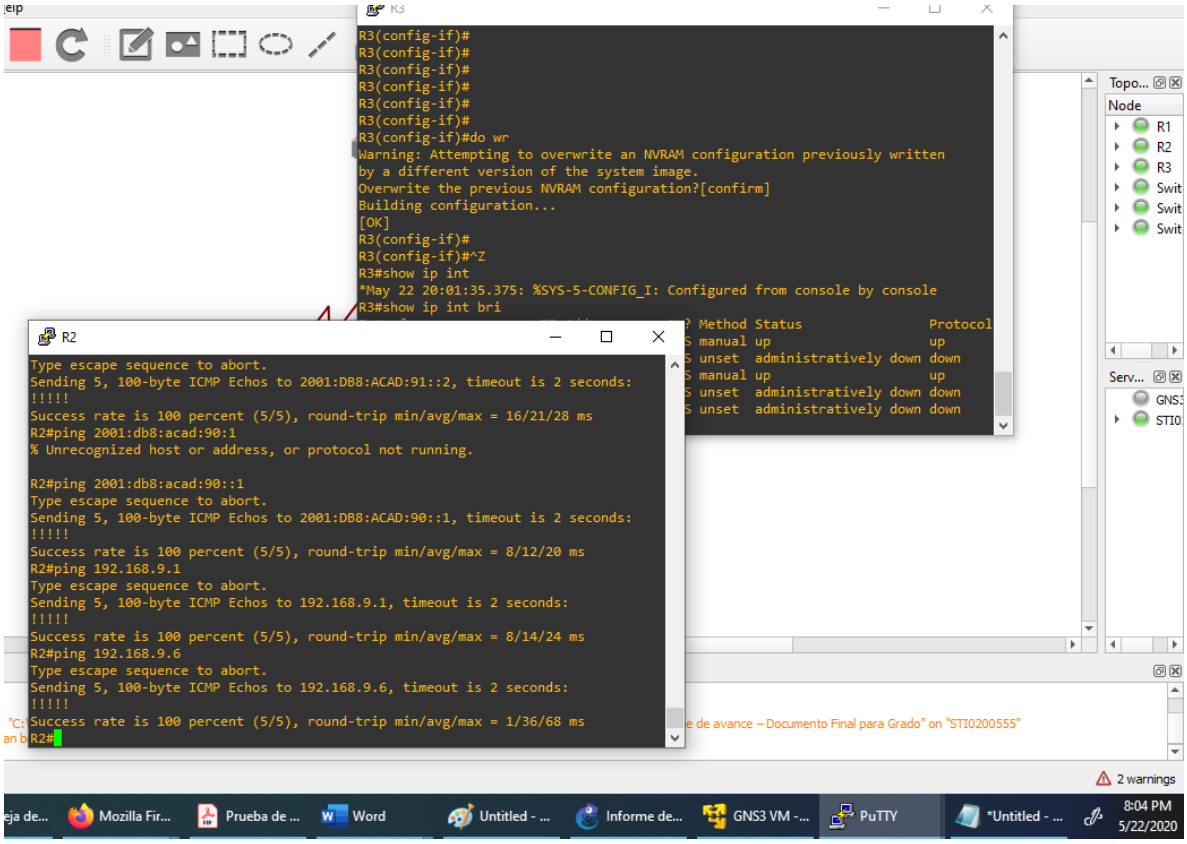
Ingresamos al modo global de router y cada uno de los modos de interfaz para la configuración se debe ejecutar el comando “ip address” para configuraciones de direccionamiento IPv4 y “ipv6 address” para configuraciones de IPv6.

```
R1(config)#int serial 1/0
R1(config-if)#clock rate 128000
R1(config-if)#ipv6 address 2001:db8:acad:90::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ip address 192.168.9.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#int f0/0
R1(config-if)#ip address 192.168.110.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:acad:110::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#do wr
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#
R1(config-if)#

R2(config)#int f0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#ipv6 address 2001:db8:acad:b::1/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#int serial 1
R2(config-if)#int serial 1/0
R2(config-if)#ipv6 address 2001:db8:acad:90::2/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ip address 192.168.9.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#int serial 1/1
R2(config-if)#clock rate 128000
R2(config-if)#ipv6 address 2001:db8:acad:91::1/64
```

```
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ip address 192.168.4.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#do wr

R3#conf terminal
R3(config)#int f0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:acad:c::1/64
R3(config-if)#ipv6 address fe80::3 link-local
R3(config-if)#int serial 1/1
R3(config-if)#ipv6 address 2001:db8:acad:91::2/64
R3(config-if)#ipv6 address fe80::3 li
R3(config-if)#ipv6 address fe80::3 link-local
R3(config-if)#ip address 192.168.9.6 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#
```

Se realiza verificación de conectividad mediante ping entre los dos equipos R1 y R2.

FIGURA 2 PRUEBAS DE CONECTIVIDAD R1,R2,R3



En la figura 2 se realizan pruebas únicamente de las redes directamente conectadas a los enrutadores pues están siempre responderán sin un protocolo de enrutamiento configurado.

1.1.2. Configuración de enrutamiento OSPFV3 entre R2 Y R1

Para la configuración de los protocolos de enrutamiento se ingresa igualmente al modo global, pero en particular para que los protocolos de enrutamiento se puedan ejecutar en IPv6 se debe habilitar la función mediante la instrucción “ipv6 routing-unicast”

```
R2(config)#ipv6 unicast-routing
R2(config)#router ospfv3 1
```

En este punto se define el área 1 como un área totalmente aislada o NSSA mediante la instrucción mostrada

```
R2(config-router)#area 1 stub no-summary
```

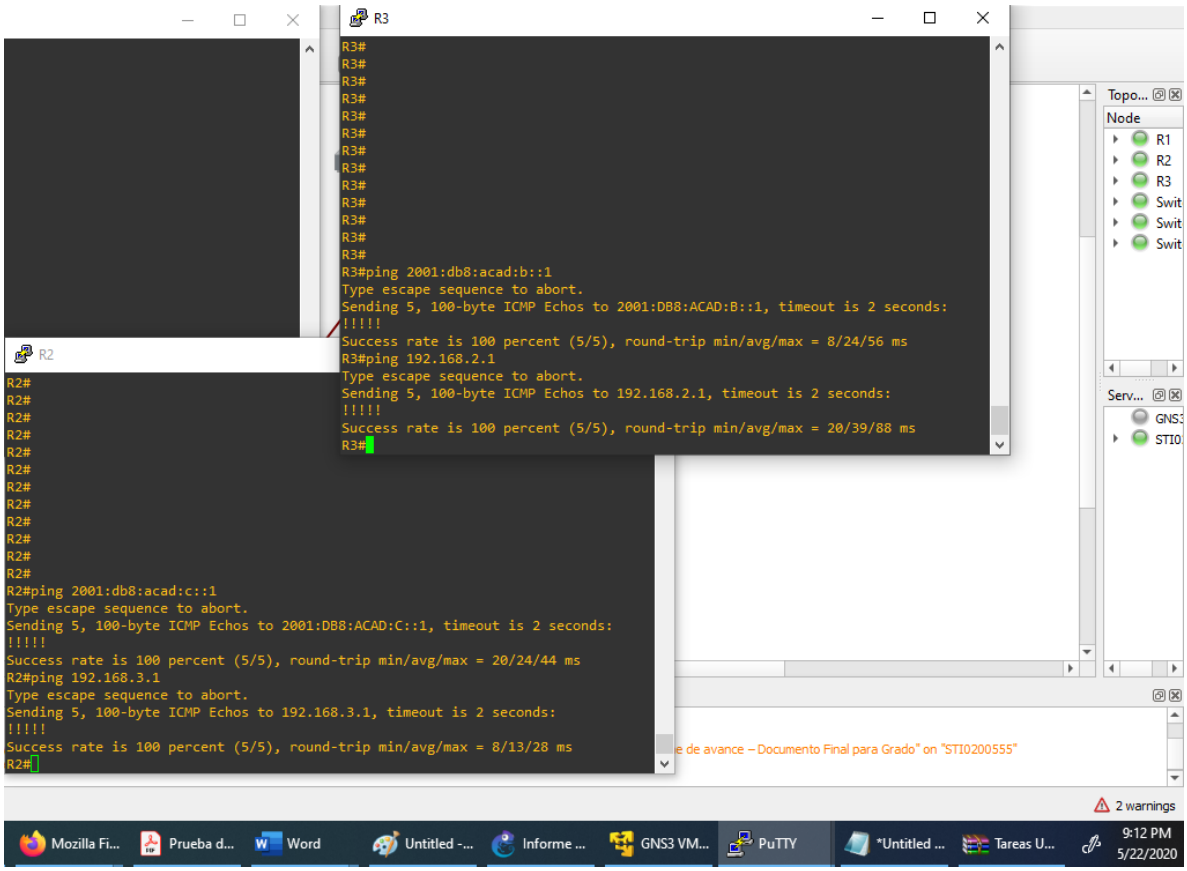
Para facilitar la configuración uniforme se crean address-familiy en ambos tipos de direccionamiento.

```
R2(config-router)#address-family ipv4 unicast
R2(config-router-af)#router-id 2.2.2.2
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#router-id 2.2.2.2
R2(config-router-af)#int f0/0
R2(config-if)#ip ospf 1 area 1
R2(config-if)#ipv6  ospf 1 area 1
R2(config-if)#int serial 1/1
R2(config-if)#ip ospf 1 area 0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#router ospfv3 1
R2(config-router)#area 1 stub no-summary
```

```
R3(config)#ipv6 unicast-routing
R3(config)#router ospfv3 1
R3(config-router)#address-family ipv4 unicast
R3(config-router-af)#rou
R3(config-router-af)#router-id 3.3.3.3
R3(config-router-af)#default-information originate
R3(config-router-af)#exit-address-family
```

```
R3(config-router)#address-family ipv6 unicast
R3(config-router-af)#router-id 3.3.3.3
R3(config-router-af)#default-information originate
R3(config-router-af)#exit
R3(config-router)#int f0/0
R3(config-if)#ip ospf 1 area 0
R3(config-if)#ipv6 ospf 1 area 0
R3(config-if)#int serial 1/1
R3(config-if)#ipv6 ospf 1 area 0
```

FIGURA 3. PRUEBAS DE CONECTIVIDAD LAN REMOTAS



Al verificar la conectividad hacia la redes remotas en el dominio OSPF se confirma conectividad correcta mediante la instrucción de ping como lo muestra la figura 3.

1.1.3. Configuración de enrutamiento entre R1 Y R2 EIGRP NAMED

Igualmente se elige la configuración de EIGRP por el método de enrutamiento nombrado para facilitar la configuración y dejar uniforme la configuración a través de address-family en ipV4 e IPv6.

```
R1(config)#ipv6 unicast-routing
R1(config)#router eigrp LABORATORIO
R1(config-router)#address-family ipv4 unicast autonomous-system 101
R1(config-router-af)#eigrp router-id 1.1.1.1
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast autonomous-system 101
R1(config-router-af)#eigrp router-id 1.1.1.1
R1(config-router)#address-family ipv4 unicast autonomous-system 101
```

Para dejar las interfaces LAN como pasivas en el protocolo de enrutamiento se realiza mediante aplicar la instrucción passive-interface dentro del modo af-interface en el protocolo en enrutamiento como se describe a continuación:

```
R1(config-router-af)#af-interface f0/0
R1(config-router-af-interface)#passive-interface
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast autonomous-system 101
R1(config-router-af)#af-interface f0/0
R1(config-router-af-interface)#passive-interface
```

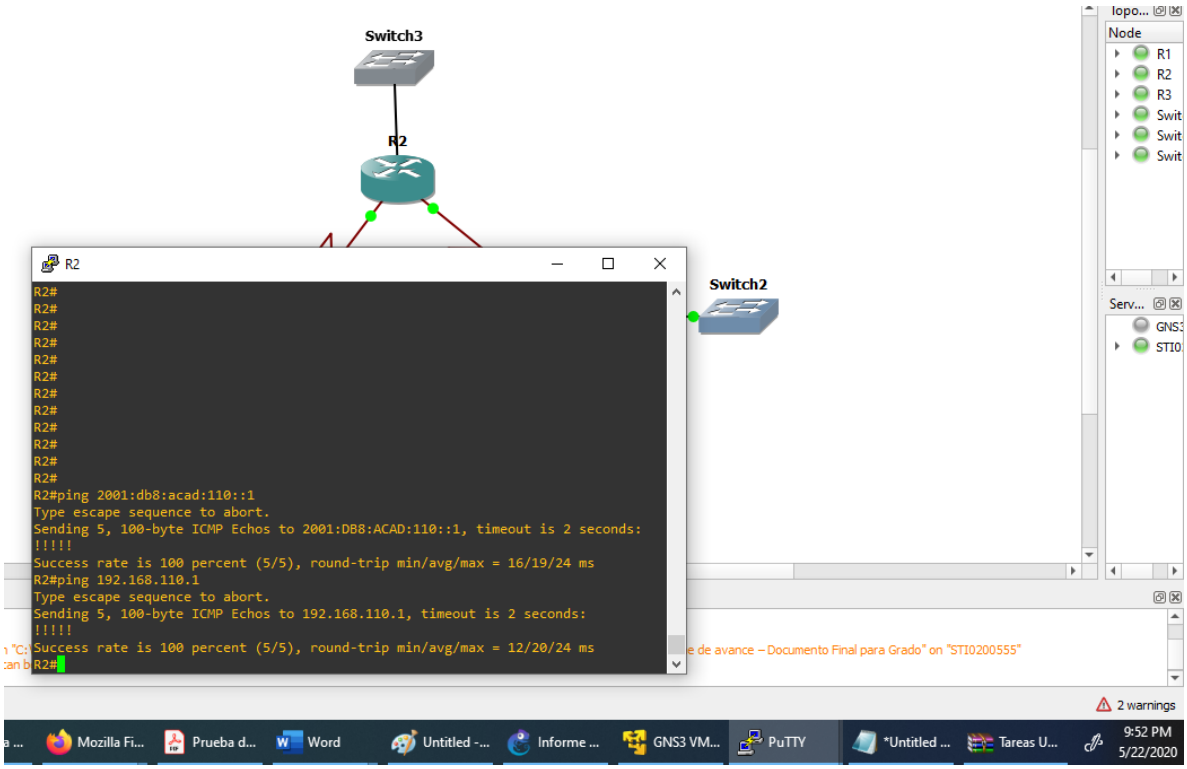
Se propagan las redes en IPv4 que se quieren exportar dentro del address-family correspondiente:

```
R1(config)#router eigrp LABORATORIO
R1(config-router)#address-family ipv4 unicast autonomous-system 101
R1(config-router-af)#network 192.168.110.0 0.0.0.255
R1(config-router-af)#network 192.168.9.0 0.0.0.3
```

Ahora se realiza la configuración correspondiente en R2 para terminar el sistema autónomo regido por EIGRP.

```
R2(config)#router eigrp LABORATORIO
R2(config-router)#address-family ipv4 unicast autonomous-system 101
R2(config-router-af)#network 192.168.9.0 0.0.0.3
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv4 unicast autonomous-system 101
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6 unicast autonomous-system 101
R2(config-router-af)#eigrp router-id 2.2.2.2
R2(config-router)#address-family ipv4 unicast autonomous-system 101
R2(config-router-af)#eigrp router-id 2.2.2.2
R2(config-router-af)#exit-address-family
```

FIGURA 4. PRUEBAS DE CONECTIVIDAD DESDE R2 TO R1



La figura 4 nos muestra la conectividad exitosa desde R2 hacia la LAN de R1 de manera correcta.

Se realiza distribución de redes en ASBR, primero se redistribuyen rutas de OSPF en EIGRP en su address-family correspondiente, usando en este caso las metricas señaladas y filtrando por método de route-map las redes de R3.

```
R2#show run | begin router
router eigrp LAB
 !
 address-family ipv4 unicast autonomous-system 101
  !
  topology base
   distribute-list 1 out ospf 1
   redistribute ospfv3 1 metric 10000 100 255 1 1500 route-map LAN-3
  exit-af-topology
  network 192.168.9.0 0.0.0.3
 exit-address-family
 !
 address-family ipv6 unicast autonomous-system 101
  !
  topology base
   redistribute ospf 1 metric 10000 100 255 1 1500
  exit-af-topology
 exit-address-family
!
```

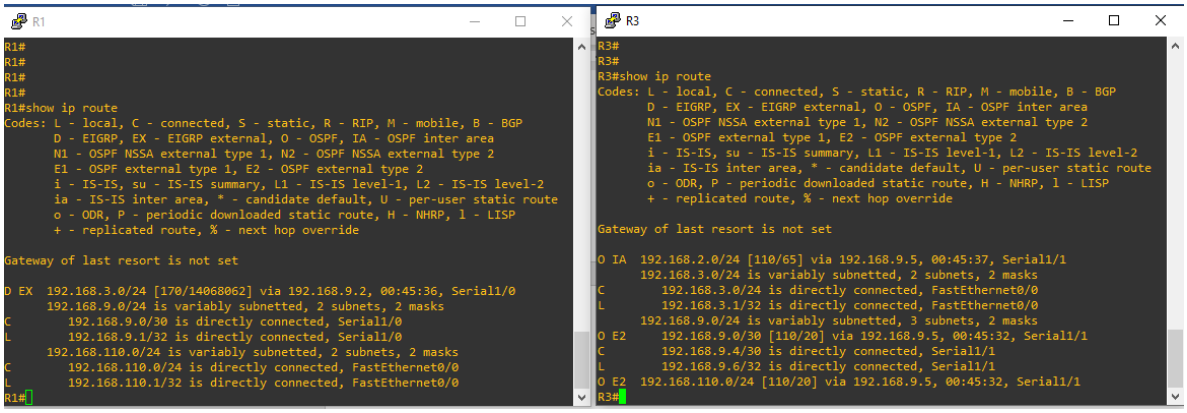
Para que la adyacencia y aprendizaje de recursos sea completo se requiere así mismo aplicar el protocolo de enrutamiento en este caso se elige redistribuir en o OSPF las redes directamente conectadas, se exhibe las líneas de comando que se corren desde el modo de enrutamiento OSPF en el ASBR es decir en R2:

```
router ospfv3 1
 router-id 2.2.2.2
 area 1 stub no-summary
 !
 address-family ipv4 unicast
  redistribute eigrp 101
  passive-interface FastEthernet0/0
```

```
exit-address-family
!
address-family ipv6 unicast
 passive-interface FastEthernet0/0
 redistribute eigrp 101 include-connected
exit-address-family
```

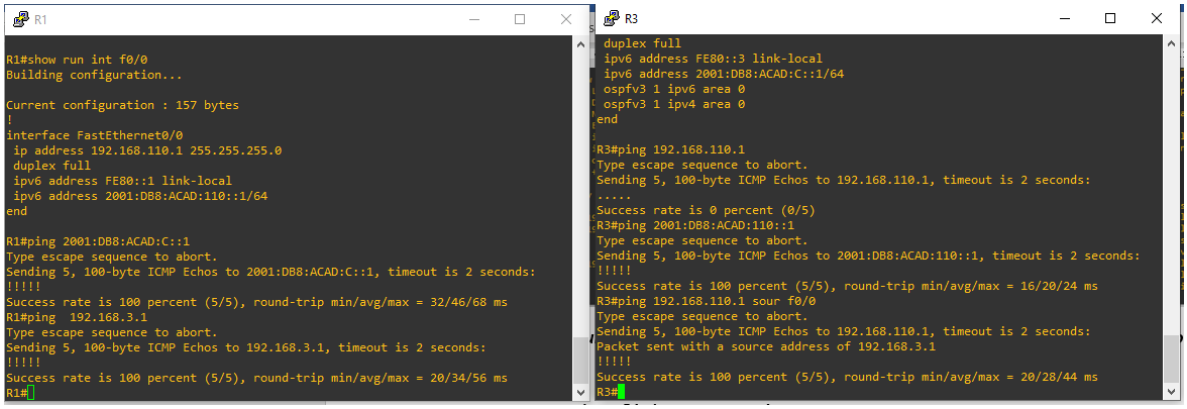
1.2. VERIFICACIÓN PROTOCOLOS DE ENRUTAMIENTO Y APRENDIZAJE DE REDES

FIGURA 5. VERIFICACIÓN DE RUTAS DESDE R1 Y R2



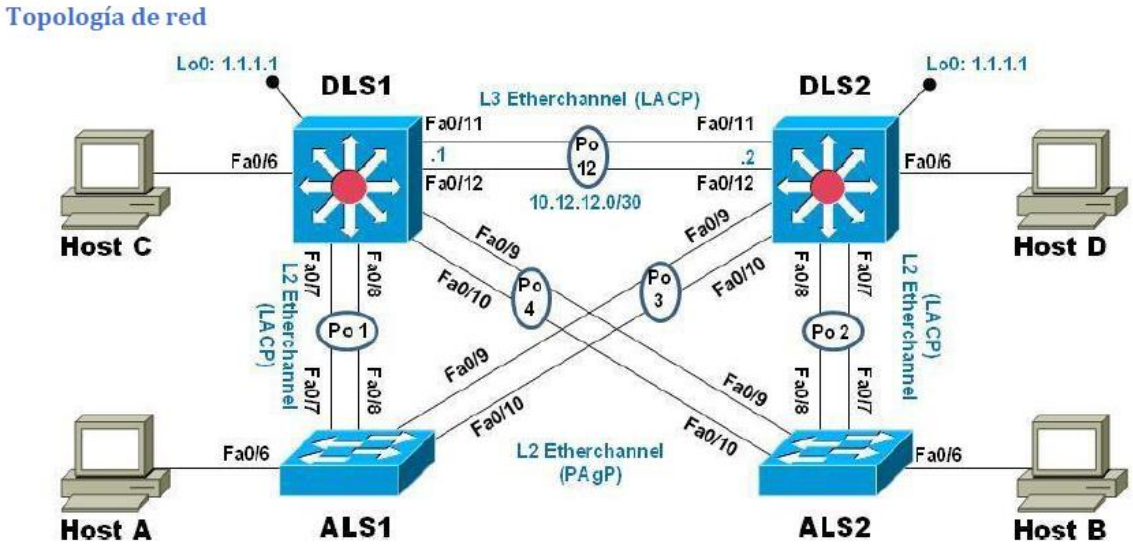
La figura 5 muestra las pruebas de conectividad entre

FIGURA 6. PRUEBAS DE CONECTIVIDAD GENERAL



2. ESCENARIO 2

FIGURA 7. ESCENARIO 2



2.1 CONFIGURAR LA RED DE ACUERDO CON LAS ESPECIFICACIONES.

2.1.1. Apagar todas las interfaces en cada switch.

Al seleccionar un rango de interfaces se optimiza la configuración pues la misma configuración se aplica a múltiples puertos en este caso apagar las interfaces

```
ALS2(config)#interface range f0/1 -24
ALS2(config-if-range)#shutdown
```

2.1.2. Configuración de los port-channel

Se configuran los port-channel que consiste en una asociación de puertos para que queden funcionando como uno solo sumándose así las características propias del servicio, existen dos tipos de agregación de interface uno es el genérico que es el LACP y el propietario de CISCO que es el PAgP , la diferencia estriba en como se asocia el port-channel si es “mode on” quedaría como LACP, si es “mode desirable” como PAgP.

En se habilita los port-channel de DLS1 como LACP

```
DLS1(config)#INTerface POrt-channel 12
DLS1(config-if)#no switchport
DLS1(config-if)#ip address 10.12.12.1 255.255.255.0
DLS1(config)#interface range f0/11-12
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#channel-group 12 mode on
DLS1(config)#interface port-channel 1
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config)#interface range f0/7-8
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#channel-group 1 mode on
DLS1(config)#interface port-channel 4
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
```

Para habilitar el modo port-channel por PAgP basta con cambiar el término “on” por “desirable”

```
DLS1(config)#interface range f0/9-10
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 4 mode desirable
```

A continuación, se describe el proceso análogo en DSL2

```
DLS2(config)#interface port-channel 12
DLS2(config-if)#ip address 10.12.12.2 255.255.255.0
DLS2(config-if)#int ran f0/11-12
DLS2(config-if-range)#no switchport
DLS2(config-if-range)#channel-group 12 mode on
DLS2(config)#int port-channel 3
DLS2(config-if)#switchport trunk encapsulation dot1q
```

DLS2(config-if)#switchport mode trunk
DLS2(config-if)#int ran f0/9-10
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 3 mode desirable
DLS2(config)#int port-channel 2
DLS2(config-if)#switchport trunk encapsulation do
DLS2(config-if)#switchport trunk encapsulation dot1q
DLS2(config-if)#switchport mode trunk
DLS2(config)#interface range f0/7- 8
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 2 mode on

Se configura los port-channel en ALS1 Y ALS2

ALS1(config)#interface port-channel 1
ALS1(config-if)#swi
ALS1(config-if)#switchport mo
ALS1(config-if)#switchport mode tru
ALS1(config-if)#switchport mod
ALS1(config-if)#switchport mode tru
ALS1(config-if)#switchport mode trunk
ALS1(config-if)#
ALS1(config-if)#
ALS1(config-if)#exi
ALS1(config-if)#exit
ALS1(config)#int
ALS1(config)#interface ran
ALS1(config)#interface range f0/7-8
ALS1(config-if-range)#swi
ALS1(config-if-range)#switchport mo
ALS1(config-if-range)#switchport mode tru
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mo
ALS1(config-if-range)#channel-group 1 mode on
ALS1(config-if-range)#exi
ALS1(config-if-range)#exit
ALS1(config)#int
ALS1(config)#interface po
ALS1(config)#interface port-channel 3
ALS1(config-if)#swi
ALS1(config-if)#switchport mo
ALS1(config-if)#switchport mode tru
ALS1(config-if)#switchport mode trunk
ALS1(config)#interface range f0/9-10

```
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 3 mode desirable

ALS2(config)#interface port-channel 4
ALS2(config-if)#switchport mode trunk
ALS2(config)#interface range f0/9-10
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config)#interface port-channel 2
ALS2(config-if)#switchport mode trunk
ALS2(config)#interface range f0/7-8
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode on
ALS2(config-if-range)#
```

2.1.3. Configuración del servicio VTP

El protocolo de troncalización por VLAN es un protocolo propietario de CISCO cuya finalidad es que desde un solo concentrador o equipo central se propaguen las VLAN a través de todo un dominio de la red conmutada en este caso se usan las tres situaciones DLS1 como VTP server es decir desde este switch de L3 se crean todas las VLAN y en el dominio VTP deben acordarse las contraseñas y el dominio hacia el cual están asociados los dispositivos.

El VTP server administra la propagación de VLAN y desde un VTP cliente se aprende todo lo que este enseñe a través de redes troncales. A continuación, se describe el proceso.

Configuración de DLS1 como VTP server

```
DLS1(config)#vtp mode server
Device mode already VTP SERVER.
DLS1(config)#vtp domain UNAD
Changing VTP domain name from NULL to UNAD
DLS1(config)#VTp PASsword cisco123
DLS1(config)#vtp version 2
```

Configuración de ALS1 Y ALS2 como VTP cliente

```
ALS1(config)#vtp mode client
ALS1(config)#vtp domain UNAD
ALS1(config)#vtp password cisco123
ALS1(config)#vtp version 2

ALS2(config)#vtp mode client
ALS2(config)#vtp domain UNAD
ALS2(config)#vtp password cisco123
ALS2(config)#vtp version 2
```

Se concluye que las VLAN desde un VTP Server hacia un VTP cliente es solo posible si se cumplen condiciones como lo son puertos de conexión entre un VTP server hacia un cliente por puertos troncales , los dominios y contraseñas deben ser iguales en todos los equipos de dominio. Por otra parte se usa el método “Transparent” cuando se quiere que el sistema sea autónomo en la configuración de sus VLAN.

2.1.4. Configuración DLS1 como servidor principal para las VLAN Y ALS1, ALS2 como clientes VTP

Se debe implementar la siguiente información en la red switcheada, tal como lo describe la tabla 2.

TABLA 1 VLANS EN VTP SERVER DLS1

Número de VLAN	Nombre de VLAN	Número de VLAN	ombre de VLAN
800	NATIVA	434	TACIONAMIENTO
12	EJECUTIVOS	123	ANTENIMIENTO
234	HUESPEDES	1010	VOZ
1111	VIDEONET	3456	DMINISTRACIÓN

Para la implementación de una vlan sobre versión de IOS 15, se debe ingresar al modo de configuración global de un switch e ingresar al modo de VLAN, alternativamente se puede colocar nombres a cada una de ellas para una adecuada jerarquización de la red.

```
DLS1(config)#vlan 800
DLS1(config-vlan)#name NATIVA
DLS1(config-vlan)#vlan 12
DLS1(config-vlan)#name EJECUTIVOS
DLS1(config-vlan)#vlan 234
DLS1(config-vlan)#nameHUESPEDES
DLS1(config)#vlan 434
DLS1(config-vlan)#name ESTACIONAMIENTO
DLS1(config-vlan)#vlan 123
DLS1(config-vlan)#name MANTENIMIENTO
```

Hay una característica que por esquemas de laboratorio depende tanto de la imagen como la preferencia SDM de un switch por la limitante de laboratorio arrojaba el siguiente error en la creación de VLANs superiores al id de VLAN 1005.

```
DLS1(config-vlan)#vlan 1111
VLAN_CREATE_FAIL: Failed to create VLANs 1111 : extended VLAN(s) not allowed in
current VTP mode
```

Con la instrucción show VLAN aplicada en el modo privilegiado de un switch CISCO Se puede observar todas las VLAN creadas, igualmente los puertos del acceso a los cuales se asocian.

A continuación, se detalla la configuración de VLAN del switch DLS2 el cual funciona como VTP transparente, en este modo dependiendo de la preferencia SDM de switch permite la creación de VLAN con ID superior a la 1005.

DLS2#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
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
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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs

Otros comandos de verificación para comprobar la configuración y funcionamiento del sistema de red capa 2 en adelante L2, son:

Comprobación de adecuada configuración de los port-channel desde el modo privilegiado de un switch se da la instrucción “show etherchannel summary “

ALS2# show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

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

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

2 Po2(SU) - Fa0/7(P) Fa0/8(P)
4 Po4(SU) PAgP Fa0/9(I) Fa0/10(P)

Comprobándose en este caso que el Po4 es usa el modo PAgP y le Po2 el LACP y que ambos están correctamente configurados y en servicio.

La instrucción de modo privilegiado “show vtp status” muestra la configuración del protocolo VTP en cada uno de los dispositivos, en este caso que usa la versión 2 y que usa el dominio VTP “UNAD”.

ALS2#show vtp status
VTP Version : 2
Configuration Revision : 11
Maximum VLANs supported locally : 255
Number of existing VLANs : 10
VTP Operating Mode : Client
VTP Domain Name : UNAD
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x08 0x01 0x0E 0xAE 0x81 0x41 0x29 0x1F
Configuration last modified by 0.0.0.0 at 3-1-93 01:14:

```
DLS1#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, 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
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
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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

f. En DLS1, suspender la VLAN 434.

Para suspender una VLAN en un switch se usa la forma “no” de VLAN mas el ID de VLAN como se muestra a continuación en el comando de verificación se muestra que la VLAN configurada en un principio con ID de VLAN 434 no esta dentro de la VLAN database del equipo.

```
DLS1(config)#no vlan 434
DLS1#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, 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
123 MANTENIMIENTO active
234 HUESPEDES 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
123 enet 100123 1500 - - - - - 0 0
```

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

Siguiendo el mismo método de configuración de VLAN que en DLS1 se crean los mismos ID de VLAN en DLS2 al verificar con el comando de modo privilegiado “show vlan” se realiza la verificación de estas en la database de VLAN.

DLS2# show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, 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
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
1010 VOZ active
1111 VIDEONET active
3456 ADMINISTRACION active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
12 enet 100012 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

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1010 enet 101010 1500 - - - - - 0 0
1111 enet 101111 1500 - - - - - 0 0
3456 enet 103456 1500 - - - - - 0 0

Remote SPAN VLANs

Primary Secondary Type Ports
------- --------- ---------- ----------

h. Suspender VLAN 434 en DLS2.

Como en el ejercicio anterior para suspender una VLAN basta con aplicar la expresión “no vlan” más el ID de VLAN para que esta ya no se encuentra en la database de switch.

DLS2(config)#no vlan 434
DLS2#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, 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
123 MANTENIMIENTO active
234 HUESPEDES active
800 NATIVA active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
1010 VOZ active
1111 VIDEONET active
3456 ADMINISTRACION active

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

i. En DLS2, crear VLAN 567 con el nombre de CONTABILIDAD. La VLAN de CONTABILIDAD no podrá estar disponible en cualquier otro Switch de la red. V

Un switch en modo transparente no aprende y no enseña VLAN a través de un dominio y es autónomo en su base de datos de VLAN, por tanto para realizar el ejercicio de añadir la VLAN 567 solo basta con aplicar los comandos necesarios en modo de configuración global como lo muestra el ejemplo a continuación descrito.

```
DLS2(config)#vla 567
DLS2(config-vlan)#Name CONTABILIDAD
```

Se realiza la verificación de la base de datos de switch comprobando que la VLAN CONTABILIDAD se encuentre en esta.

```
DLS2#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, 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
123 MANTENIMIENTO active
234 HUESPEDES active
567 CONTABILIDAD active
800 NATIVA active
```

2.1.5. 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.

Es recomendable que el switch que se encuentra directamente conectado a las capas superiores en un sistema de redes sea el que asuma el roll de root sin embargo para este ejercicio de presentan dos switches robustos que permiten la contingencia ante cualquier eventualidad que se presente como por ejemplo la caída del switch principal o DLS1.

```
DLS1(config)#spanning-tree vlan 1,12,434,800,1010,1111,3456 root primary
DLS1(config)#spanning-tree vlan 123,234 root secondary
```

Es de resaltar que en este caso el spanning-tree siendo un protocolo para evitar loops de L2 balance la predominancia en cada uno de los switches.

2.1.6 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.

De la misma forma se aplica recíprocamente la precedencia de spanning-tree en DLS2.

DLS2(config)#spanning-tree vlan 123,234 root primary
DLS2(config)#spanning-tree vlan 12,434,800,1010,1111,3456 root secondary

2.1.6 Asociación de VLAN en interfaces de acceso

TABLA 2 ASOCIACION DE VLANS DE ACCESO

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

En la tabla 3 se describe la distribución de asociación de VLAN de acceso en los switches. Entiéndase por una VLAN de acceso aquella que únicamente se va conectar a un dispositivo terminal como una impresora, un PC , o un teléfono. A diferencia de VLAN troncales para asociar cada una de las VLAN se debe ingresar al modo de configuración de interfaz y mediante la instrucción “swithcport mode acces” y switchport Access vlan (incluyendo ID de vlan de acceso” se propaga la VLAN para que el equipo terminal pueda acceder a los recursos de red.

DLS1(config)#int f0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 3456
DLS1(config-if)#spanning-tree portfast

La expresión portfast indica un método que permite el mínimo tiempo de convergencia cuando el puerto de acceso sufre un evento en la convergencia de spanning-tree pasando directamente de un estado blocking a foward

DLS1(config)#interface f0/15
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 1111
DLS1(config-if)#spanning-tree portfast

Tambien se pueden configurar varios puertos de acceso al mismo tiempo usando el rango de interfaces como se muestra en el ejemplo a continuación descrito.

```
DLS1(config)#interface range f0/16-18
DLS1(config-if-range)#switchport mode access
DLS1(config-if-range)#switchport access vlan 567
DLS1(config-if-range)#spanning-tree portfast
```

En una puerto de acceso solo se puede asociar una y solo una VLAN para poder asociar más de una VLAN tendría que definirse una variable de función sucede asi por ejemplo con las vlan de voz que no usan el comando de interfaz “switchport acces vlan (ID de VLAN) “ si no “switchport voice vlan (ID de VLAN)

```
DLS2(config)#interface f0/6
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 12,1010
DLS2(config-if)#spanning-tree portfast

DLS2(config-if)#int f0/15
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 1111
DLS2(config)#interface range f0/16-18
DLS2(config-if-range)#switchport access vlan 567
DLS2(config-if-range)#spanning-tree portfast
```

En los switches de acceso se realiza la respectiva distribución de VLAN de acuerdo al planteamiento o necesidades específicas de red.

```
ALS1(config)#interface f0/6
ALS1(config-if)#switchport access vlan 123,1010
ALS1(config-if)#spanning-tree portfast
ALS1(config)#interface f0/15
ALS1(config-if)#switchport access vlan 1111
ALS1(config-if)#spanning-tree portfast

ALS2(config)#interface f0/6
ALS2(config-if)#switchport access vlan 234
ALS2(config-if)#spanning-tree portfast

ALS2(config)#int f0/15
ALS2(config-if)#switchport access vlan 1111
ALS2(config-if)#spanning-tree portfast
```

CONCLUSIONES

El uso de protocolos de enrutamiento dinámico simplifica la administración de una red ya que se automatiza la propagación de redes al igual que posibilita la escalabilidad sin intervención de un administrador de red.

La redistribución se aplica cuando se quiere unificar dos protocolos de red diferentes sin la afectación drástica del acceso a los servicios.

El protocolo de enrutamiento EIGRP no es recomendable en entornos múltiples proveedores de sistemas de interconexión ya que por ser un protocolo propietario de CISCO y aunque este haya liberado RFC especificando algunas características del comportamiento, por el momento no es factible la unificación de estas a otras marcas de equipos.

En una red switcheada se facilita el alcance e igualmente la estratificación de los servicios, siendo esto ultimo una ventaja en la resolución de problemas de red aislando la parte afectada. El modelo de red implementado por CISCO debería tener una amplia aceptación.

Los Switches CISCO de capa 3 , han simplificado la concepción de escalabilidad de un sistema conmutado por paquetes usando esquemas de configuración como los ether-channel que no solo agregan interfaces si no también potencian la red para ser más resistente.

BIBLIOGRAFIA

DONOHUE, D. CISCO Press (Ed). CCNP Quick Reference. (2017).

MACFARLANE, J. Network Routing Basics: Understanding IP Routing in Cisco Systems. (2014).

TEARE, D., VACHON B., GRAZIANI, R. CISCO Press (Ed). Routers and Routing Protocol Hardening. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

ANEXOS

Anexo A. Evidencias habilidades practicas

CHAVARRO. Leonardo, Escenario 1 trabajo final . (Julio, 7 de 2020). Recuperado desde https://1drv.ms/u/s!ArMGzFu2NFOMn2Ca8Z8gioks2UN7?e=lbrUbD.

CHAVARRO. Leonardo, Escenario 2 trabajo final . (Julio, 7 de 2020). Recuperado desde https://1drv.ms/u/s!ArMGzFu2NFOMoDg5Li2HpvxpjkYU?e=mQ9ocU.