DIPLOMADO DE PROFUNDIZACION CISCO CCNP
208014A_474
EVALUACION – PRUEBA DE HABILIDADES CCNP

GRUPO 208014_8

Presentado A:
GERARDO GRANADOS ACUÑA
Tutor

ELABORADO POR:
CRISTINA ELIANA GÓMEZ LOZANO
Código: 34.639.772

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DICIEMBRE, 2018

TABLA DE CONTENIDO

INTRODUCCION

A diario nos enfrentamos con el crecimiento imparable de las redes, la comunicación y la continua preocupación de mantener la información personal y/o laboral bajo nuestro dominio. En el curso Diplomado de profundización Cisco CCNP apropiamos los conceptos presentados en los contenidos de formación y se asocian con el contexto de las telecomunicaciones respecto a su aplicación en las redes de área extendida e identificar y comprender el uso que tiene las tecnologías en el desarrollo de proyectos de conectividad de redes empresariales.

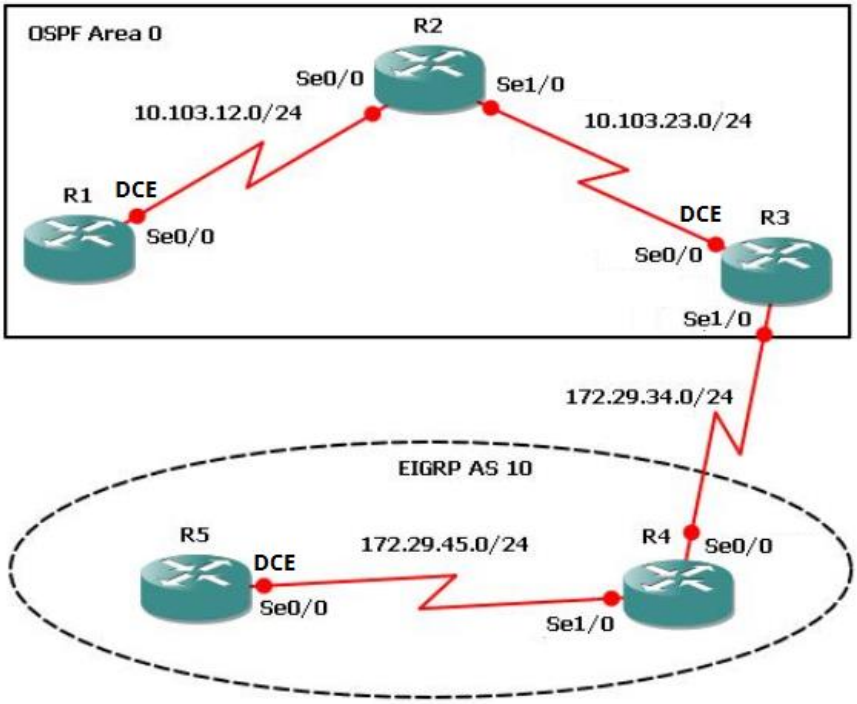
La seguridad es un motivo de preocupación cuando se utiliza Internet pública para realizar negocios. Las redes virtuales privadas (VPN) se utilizan para garantizar la seguridad de los datos a través de Internet. Una VPN se utiliza para crear un túnel privado a través de una red pública. Se puede proporcionar seguridad a los datos mediante el uso de cifrado en este túnel a través de Internet y con autenticación para proteger los datos contra el acceso no autorizado.

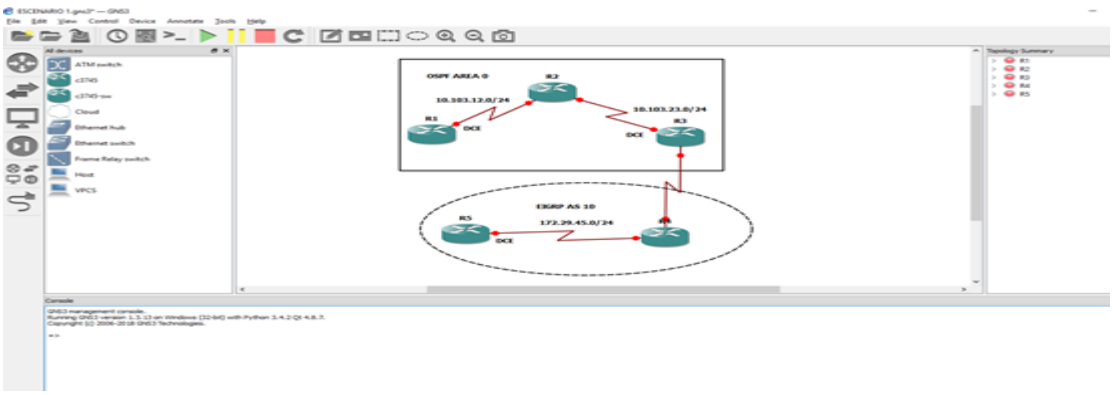
Por tanto a continuación se elaboraran tres escenarios correspondientes a la temática de implementación de soluciones soportadas en enrutamiento avanzado como etapa final del curso Diplomado de profundización Cisco CCNP.

Estos temas son el eje central del trabajo final donde se da solución a las actividades y laboratorios requeridos por la guía.
Se utilizara el software Packet Tracer o GNS3 los cuales son programas necesarios y de gran importancia para la ejecución o simulación de los laboratorios.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1





1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los

routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Configuración inicial, asignamos nombre a cada uno de los routers, direcciones de las interfaces y protocolos de comunicación correspondientes con el siguiente código.

Configuración R1

```
Router>
Router>enable                                   Ingreso a modo privilegiado
Router#configure terminal                       Ingreso a modo de configuración
Router(config)#hostname R1                      Asigno nombre al router
R1(config)#router ospf 1
R1(config-router)#router-d 1.1.1.1              Identifico el router
R1(config-router)#network 10.103.12.0 255.255.255.0 area 0
R1(config-router)#exit
R1(config)#interface s0/0                       Configuro interfaz serial 0
R1(config-if)description to R2
R1(config-if)#ip address 10.103.12.1 255.255.255.0
R1(config-if)#clock rate 128000                 Como es DCE se configura reloj
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown                       Activo la interfaz
R1(config-if)#exit
R1(config)#end
R2#wr
```

Configuración R2

Router>

Router>enable — Ingreso a modo privilegiado

Router#configure terminal — Ingreso a modo de configuración

Router(config)#hostname R2 — Asigno nombre al router

R2(config)#router ospf 1

R2(config-router)#router-id 2.2.2.2 — Identifico el router

R2(config-router)#network 10.103.12.0 255.255.255.0 area 0

R2(config-router)#network 10.103.23.0 255.255.255.0 area 0

R2(config-router)#exit

R2(config)#interface s0/0 — Configuro interfaz serial 0

R2(config-if)description to R1

R2(config-if)#ip address 10.103.12.2 255.255.255.0

R2(config-if)#no shutdown — Activo la interfaz

R2(config-if)#exit

R2(config)#interface s0/1 — Configuro interfaz serial 0

R2(config-if)description to R3

R2(config-if)#ip address 10.103.23.1 255.255.255.0

R2(config-if)#no shutdown — Activo la interfaz

R2(config-if)#exit

R2(config)#end

R2#wr

Configuración R3

Router>

Router>enable — Ingreso a modo privilegiado

Router#configure terminal — Ingreso a modo de configuración

Router(config)#hostname R3	Asigno nombre al router
R3(config)#router ospf 1	
R3(config-router)#router-id 3.3.3.3	Identifico el router
R3(config-router)#network 10.103.23.0 255.255.255.0 area 0	
R3(config-router)#exit	
R3(config)#interface s0/0	Configuro interfaz serial 0
R3(config-if)description to R2	
R3(config-if)#ip address 10.103.23.2 255.255.255.0	
R3(config-if)#clock rate 128000	Como es DCE se configura reloj
R3(config-if)#bandwidth 128	
R3(config-if)#no shutdown	Activo la interfaz
R3(config-if)#exit	
R3(config)#interface s0/1	Configuro interfaz serial 1
R3(config-if)description to R4	
R3(config-if)#ip address 172.29.34.1 255.255.255.0	
R3(config-if)#no shutdown	Activo la interfaz
R3(config-if)#exit	
R3(config)#end	
R3#wr	

Con el objetivo de permitir comunicación con ambos protocolos y teniendo en cuenta que R4 en el puerto serial 0 se configura con eigrp, se procede a configurar igualmente el puerto serial 1de R3.

R3#configure terminal	Ingreso a modo de configuración
R3(config)#router eigrp 10	Configuro eigrp
R3(config-rtr)#eigrp router-id 3.3.3.3	Asigno identidad al router
R3(config-rtr)#network 172.29.34.0 255.255.255.0	

R3(config-rtr)#exit
R3(config)#end
R3#wr

Configuración R4

Router>
Router>enable Ingreso a modo privilegiado
Router#configure terminal Ingreso a modo de configuración
Router(config)#hostname R4 Asigno nombre al router
R4(config)#router eigrp 10 Configuro eigrp
R4(config-rtr)#eigrp router-id 4.4.4.4 Asigno identidad al router
R4(config-rtr)#network 172.29.34.0 255.255.255.0
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R4(config-rtr)#exit
R4(config)#interface s0/0
R4(config-if)#ip address 172.29.34.2 255.255.255.0
R5(config-if)#no shutdown Activo la interfaz
R4(config-if)#exit
R4(config)#interface s0/1
R4(config-if)#ip address 172.29.45.1 255.255.255.0
R5(config-if)#no shutdown Activo la interfaz
R4(config-if)#exit
R4(config)#end
R4#wr

Configuración R5

Router>

Router>enable — Ingreso a modo privilegiado

Router#configure terminal — Ingreso a modo de configuración

Router(config)#hostname R5 — Asigno nombre al router

R5(config)#router eigrp 10 — Configuro eigrp

R5(config-rtr)#eigrp router-id 5.5.5.5 — Asigno identidad al router

R4(config-rtr)#network 172.29.45.0 255.255.255.0

R5(config)#interface s0/0

R5(config-if)#ip address 172.29.45.2 255.255.255.0

R5(config-if)#no shutdown — Activo la interfaz

R5(config-if)#exit

R5(config)#end

R5#wr

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Procedo a crear las interfaces Loopback, para lo cual, identifico que la máscara de red es 255.255.252.0

R1#conf t

R1(config)#interface loopback 4 — Creo la interfaz lo 4

R1(config-if)#ip address 10.1.4.1 255.255.252.0 — Establezco la dirección IP

R1(config-if)#ip ospf 1 area 0 — Con este comando configuro la int. En OSPF

R1(config-if)#exit

R1(config)# interface loopback 8 — Creo la interfaz lo 8

R1(config-if)#ip address 10.1.8.1 255.255.252.0	Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0	Con este comando configuro la int. En OSPF
R1(config-if)#exit	
R1(config)# interface loopback 12	Creo la interfaz lo 12
R1(config-if)#ip address 10.1.12.1 255.255.252.0	Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0	Con este comando configuro la int. En OSPF
R1(config-if)#exit	
R1(config)# interface loopback 16	Creo la interfaz lo 16
R1(config-if)#ip address 10.1.16.1 255.255.252.0	Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0	Con este comando configuro la int. En OSPF
R1(config-if)#exit	
R1(config)#end	
R1#wr	

Con el objetivo de verificar que las nuevas interfaces loopback hayan quedado configuradas para participar en el protocolo OSPF utilizo el comando **show ip ospf brief**, mostrando el siguiente resultado:

```
R1#sh ip ospf interface bri
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo16         1     0               10.1.16.1/22       1     LOOP  0/0
Lo12         1     0               10.1.12.1/22       1     LOOP  0/0
Lo8          1     0               10.1.8.1/22        1     LOOP  0/0
Lo4          1     0               10.1.4.1/22        1     LOOP  0/0
Se0/0        1     0               10.103.12.1/24     781   P2P   1/1
```

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

R5#configure terminal Ingreso a modo de configuración

R5(config)#int lo 4

R5(config-if)#ip address 172.5.4.1 255.255.252.0

R5(config-if)#exit

R5(config)#int lo 8

R5(config-if)#ip address 172.5.8.1 255.255.252.0

R5(config-if)#exit

R5(config)#int lo 12

R5(config-if)#ip address 172.5.12.1 255.255.252.0

R5(config-if)#exit

R5(config)#int lo 16

R5(config-if)#ip address 172.5.16.1 255.255.252.0

R5(config-if)#exit

Con el objetivo de verificar que hayan sido creadas las interfaces loopback, utilizo el comando **show ip interfaces brief | include up** arrojando el siguiente dato:

```
R5#sh ip interface bri | include up
Serial0/0                  172.29.45.2     YES NVRAM  up                    up
Vlan1                      unassigned      YES NVRAM  up                    down
Loopback4                  172.5.4.1       YES manual up                    up
Loopback8                  172.5.8.1       YES manual up                    up
Loopback12                 172.5.12.1      YES manual up                    up
Loopback16                 172.5.16.1      YES manual up                    up
```

R5(config)#router eigrp 10

R5(config-router)#no auto-sumary

R5(config-router)#network 172.5.4.0 255.255.255.0

R5(config-router)#network 172.5.8.0 255.255.255.0

R5(config-router)#network 172.5.12.0 255.255.255.0

R5(config-router)#network 172.5.16.0 255.255.255.0

R5(config-router)#network 172.29.45.0 255.255.255.0
R5(config-router)#exit
R5(config)#end
R5#wr

Para verificar que las interfaces loopback hayan quedado integradas al protocolo EIGRP utilizo el comando **show ip eigrp interfaces.**

```
R5#sh ip eigrp int
IP-EIGRP interfaces for process 10

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0              1        0/0       18       0/15          83           0
Lo4                0        0/0        0       0/1            0           0
Lo8                0        0/0        0       0/1            0           0
Lo12               0        0/0        0       0/1            0           0
Lo16               0        0/0        0       0/1            0           0
```

Como se puede evidenciar, las 4 nuevas interfaces de loopback ya participan en EIGRP.

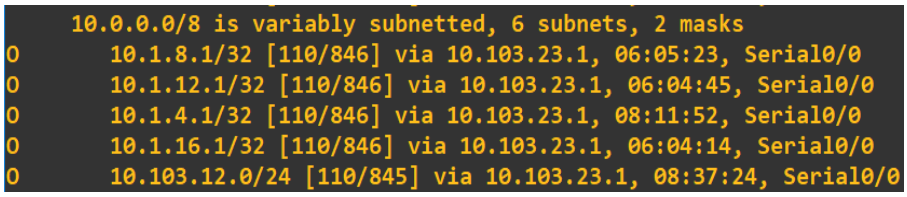
4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando **show ip route**.

Para este punto ejecuto el comando **show ip route** el cual arroja los siguientes datos:

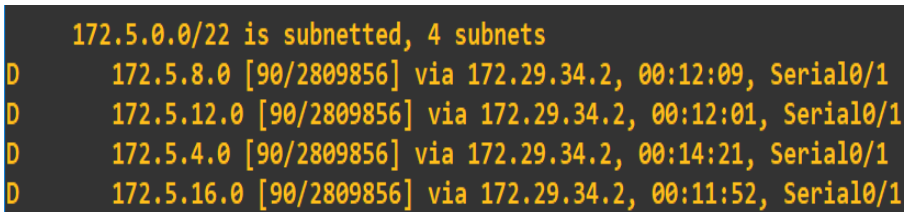
```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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

Gateway of last resort is not set

     172.5.0.0/22 is subnetted, 4 subnets
D       172.5.8.0 [90/2809856] via 172.29.34.2, 00:12:09, Serial0/1
D       172.5.12.0 [90/2809856] via 172.29.34.2, 00:12:01, Serial0/1
D       172.5.4.0 [90/2809856] via 172.29.34.2, 00:14:21, Serial0/1
D       172.5.16.0 [90/2809856] via 172.29.34.2, 00:11:52, Serial0/1
     172.29.0.0/24 is subnetted, 2 subnets
C       172.29.34.0 is directly connected, Serial0/1
D       172.29.45.0 [90/2681856] via 172.29.34.2, 08:37:06, Serial0/1
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.1.8.1/32 [110/846] via 10.103.23.1, 06:05:23, Serial0/0
O       10.1.12.1/32 [110/846] via 10.103.23.1, 06:04:45, Serial0/0
O       10.1.4.1/32 [110/846] via 10.103.23.1, 08:11:52, Serial0/0
O       10.1.16.1/32 [110/846] via 10.103.23.1, 06:04:14, Serial0/0
O       10.103.12.0/24 [110/845] via 10.103.23.1, 08:37:24, Serial0/0
```

De la información anterior, se puede evidenciar que el router R3 ha aprendido las 8 nuevas interfaces de loopback de ambos protocolos.

Protocolo OSPF en R1



Protocolo EIGRP en R5



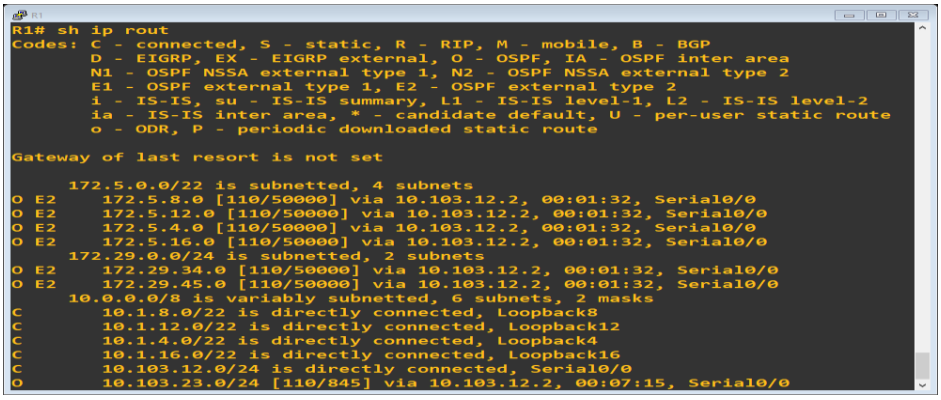
5. R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

   Para lograr redistribuir las rutas EIGRP en OSPF y viceversa utilizo los siguientes comandos:

   R3(config)#router eigrp 10
   R3(config-router)#redistribute ospf 1 metric 100000 20000 255 255 1500
   R3(config-router)#exit
   R3(config)#router ospf 1
   R3(config-router)#redistribute eigrp 10 metric 50000 subnets
   R3(config-router)#exit
   R3(config)#end
   R3#wr

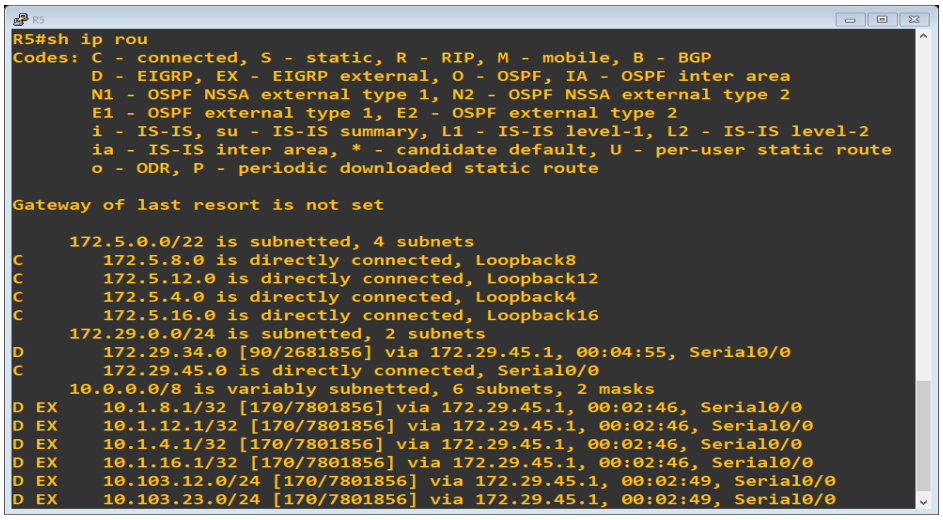
6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando **show ip route**.

Para R1



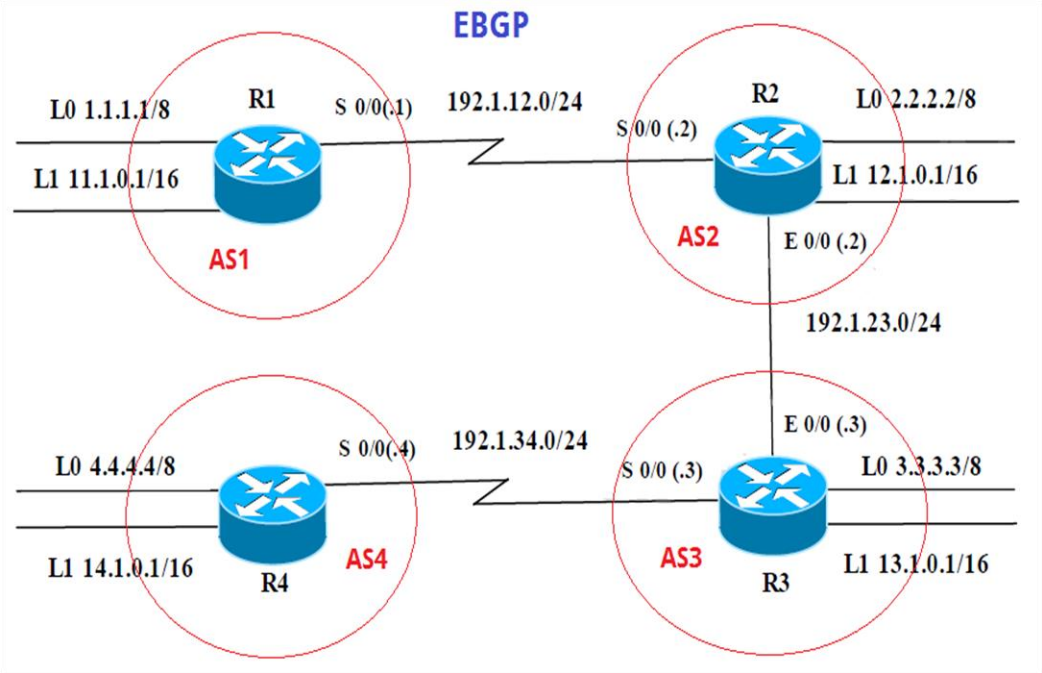
Se puede observar en R1 ya aparecen las loopbacks creadas en R5.

Para R5



Como se puede observar en R5 ya aparecen las loopbacks creadas en R1.

Escenario 2



Información para configuración de los Routers

R1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

R2

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

R3

Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

R4

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

R1

```
enable
conf terminal
int lo 0
ip address 1.1.1.1 255.0.0.0
exit
int lo 1
ip address 11.1.0.1 255.255.0.0
exit
int s0/0
ip address 192.1.12.1 255.255.255.0
clockrate 64000
no shut
exit
end
wr
```

R2

```
enable
conf terminal
int lo 0
ip address 2.2.2.2 255.0.0.0
exit
int lo 1
ip address 12.1.0.1 255.255.0.0
exit
int s0/0
```

ip address 192.1.12.2 255.255.255.0
no shut
exit
int fastEthernet 0/0
ip address 192.1.23.2 255.255.255.0
no shut

R3

enable
conf terminal
int lo 0
ip address 3.3.3.3 255.0.0.0
exit
int lo 1
ip address 13.1.0.1 255.255.0.0
exit
int fastEthernet 0/0
ip address 192.1.23.3 255.255.255.0
no shut
exit
int s0/0
ip address 192.1.34.3 255.255.255.0
no shut
exit
end

R4

enable

conf terminal
int lo 0
ip address 4.4.4.4 255.0.0.0
exit
int lo 1
ip address 14.1.0.1 255.255.0.0
exit
int s0/0
ip address 192.1.34.4 255.255.255.0
clockrate 64000
no shut
exit
end

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en **AS1** y R2 debe estar en **AS2**. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

   R1
   enable
   conf terminal
   router bgp 1
   bgp router-id 11.11.11.11
   neighbor 192.1.12.2 remote-as 2
   network 1.0.0.0 mask 255.0.0.0
   network 11.1.0.0 mask 255.255.0.0

R2

enable

conf terminal

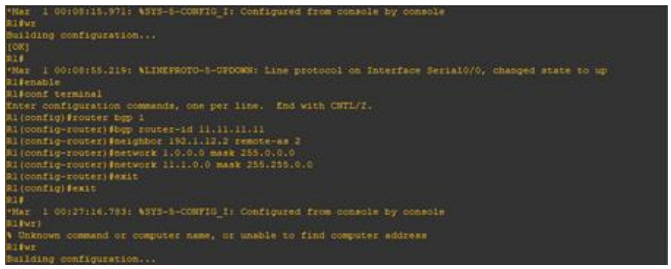
router bgp 2

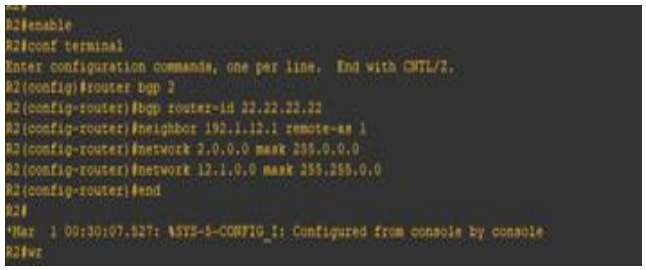
bgp router-id 22.22.22.22

neighbor 192.1.12.1 remote-as 1

network 2.0.0.0 mask 255.0.0.0

network 12.1.0.0 mask 255.255.0.0





2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

R2

enable

conf terminal

router bgp 2

neighbor 192.1.23.3 remote-as 3

R3

enable

conf terminal

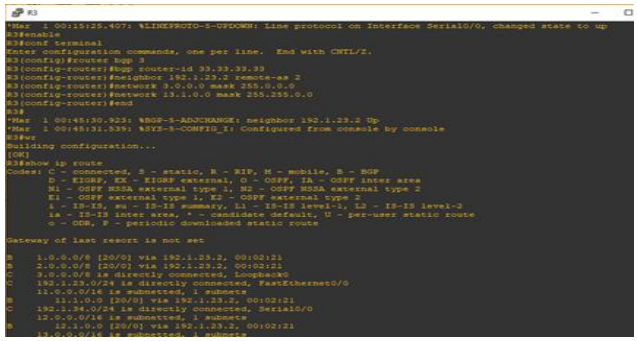
router bgp 3

bgp router-id 33.33.33.33

neighbor 192.1.23.2 remote-as 2

network 3.0.0.0 mask 255.0.0.0

network 13.1.0.0 mask 255.255.0.0



3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 44.44.44.44. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie

la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

R3

enable

conf terminal

router bgp 3

neighbor 192.1.34.4 remote-as 4

R4

enable

conf terminal

router bgp 4

bgp router-id 44.44.44.44

neighbor 192.1.34.3 remote-as 3

network 4.0.0.0 mask 255.0.0.0

exit

ip route 3.0.0.0 255.0.0.0 192.1.34.3

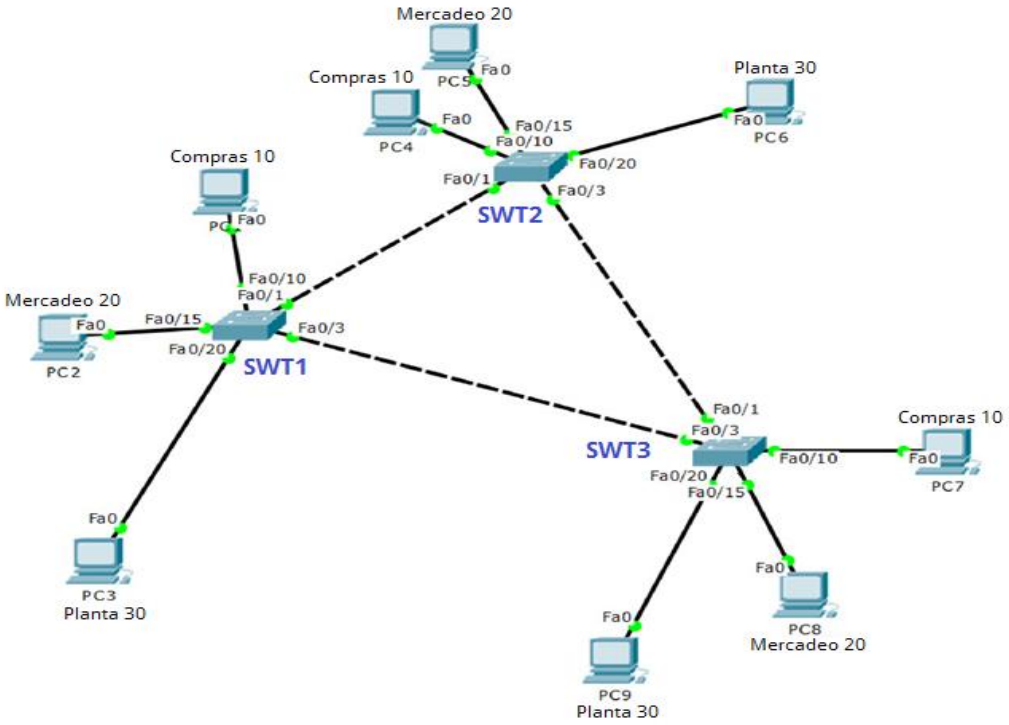
router bgp 4

no network 4.0.0.0 mask 255.0.0.0

network 4.0.0.0 mask 255.0.0.0

network 14.1.0.0 mask 255.255.0.0

Escenario 3



A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

   Para ejecutar lo anterior aplico el siguiente código en cada uno de los routers:

   Switch SWT1
   IOU1#configure terminal
   IOU1(config)#hostname SWT1
   SWT1(config)#vtp domain CCNP
   SWT1(config)#vtp mode client
   SWT1(config)#vtp password cisco
   SWT1(config)#exit
   SWT1#wr

Switch SWT2

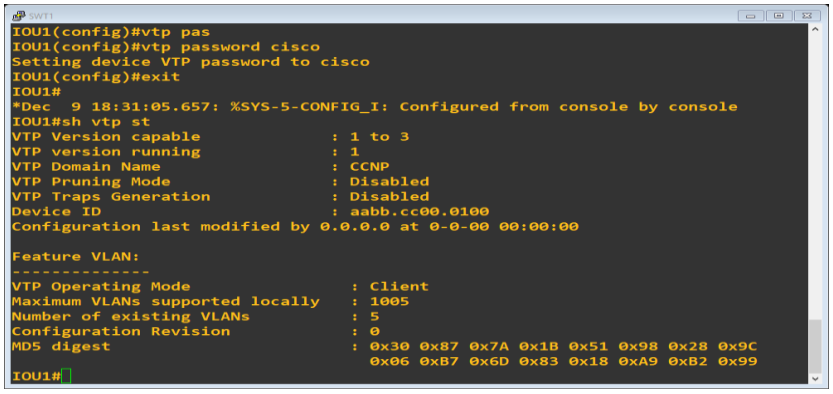
```
IOU1#configure terminal
IOU1(config)#hostname SWT2
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode server
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

Switch SWT3

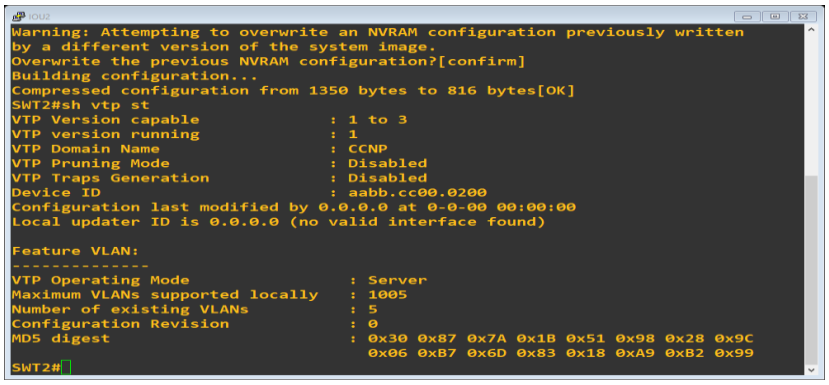
```
IOU1#configure terminal
IOU1(config)#hostname SWT3
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode client
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

2. Verifique las configuraciones mediante el comando ***show vtp status***.

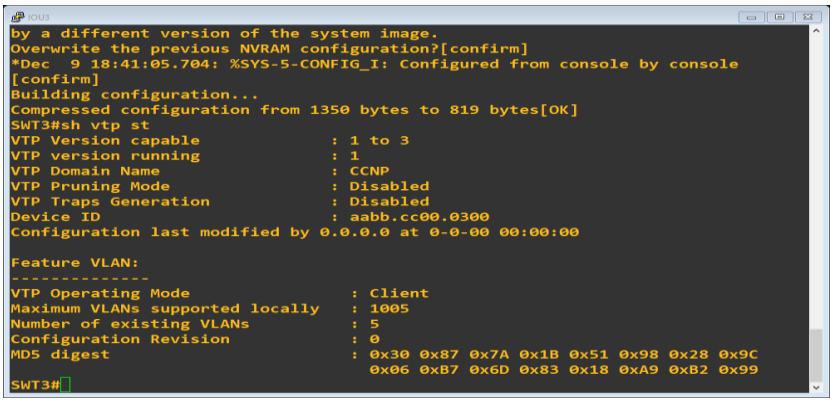
Switch SWT1



Switch SWT2



Switch SWT3



B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es **dynamic auto**, solo un lado del enlace debe configurarse como **dynamic desirable**.

   Para configurar **Dynamic desirable** se utilizó el comando **switchport mode Dynamic desirable** en ambos switches.

   Para Switch SWT1

   SWT1#configure terminal
   SWT1(config)#interface range ethernet0/0 - 1
   SWT1(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
   SWT1(config-if-range)#switchport mode trunk Habilito el modo trunk en la int.

SWT1(config-if-range)#switchport mode dynamic desirable Configuro **dynamic desirable**
SWT1(config-if-range)#no shutdown
SWT1(config-if-range)#exit
SWT1(config)#end
SWT1#wr

Para Switch SWT2

SWT2#configure terminal
SWT2(config)#interface range ethernet0/0
SWT2(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
SWT2(config-if-range)#switchport mode trunk Habilito el modo trunk en la int
SWT2(config-if-range)#switchport mode dynamic desirable Configuro **dynamic desirable**
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#interface range ethernet0/2
SWT2(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
SWT2(config-if-range)#switchport mode trunk Habilito el modo trunk en la int
SWT2(config-if-range)#switchport mode dynamic desirable Configuro **dynamic desirable**
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#end
SWT2#wr

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando **show interfaces trunk**.

Para Switch SWT1

```
IOU1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        802.1q         trunking      1
Et0/1       desirable        802.1q         trunking      1
```

Para Switch SWT2

```
SWT2#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        802.1q         trunking      1
Et0/2       desirable        802.1q         trunking      1
```

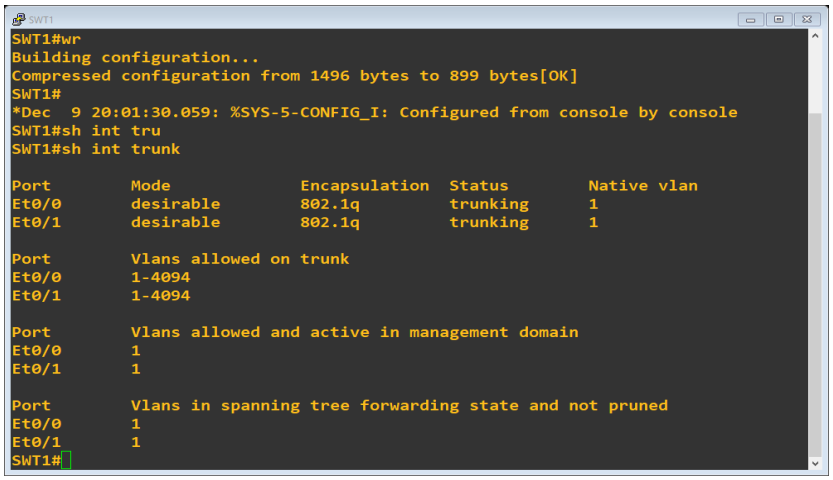
3. Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SWT1

   En el punto anterior ya configuré la interfaz del SWT1, teniendo presente que es la interfaz ethernet 0/1

   Para fvvnnfSwitch SWT3

   SWT3#configure terminal
   SWT3(config)#interface range ethernet0/1
   SWT3(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
   SWT3(config-if-range)#switchport mode trunk Habilito el modo trunk en la int.
   SWT3(config-if-range)#no shutdown
   SWT3(config-if-range)#exit
   SWT3(config)#end
   SWT3#wr

4. Verifique el enlace "trunk" el comando **show interfaces trunk** en SWT1.



5. Configure un enlace "trunk" permanente entre SWT2 y SWT3.
   En el punto anterior ya configuré la interfaz del SWT2, teniendo presente que es la interfaz ethernet 0/2

   Para Switch SWT3

   SWT3#configure terminal
   SWT3(config)#interface ethernet0/2
   SWT3(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
   SWT3(config-if-range)#switchport mode trunk Habilito el modo trunk en la int.
   SWT3(config-if-range)#no shutdown
   SWT3(config-if-range)#exit
   SWT3(config)#end
   SWT3#wr

C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99)
2. **Procedo a crear la VLAN 10 el switch SWT1 se deben crear en el switch SWT2 ya que es el que funciona en el modo servidor y es en este modo donde se pueden crear o agregar las vlan's, ya que en modo client no es posible.**

   SWT2#configure terminal
   SWT2(config)#vlan 10 Creo la vlan 10

SWT2(config-vlan)#name Compras	Asigno el nombre Compras
SWT2(config-vlan)#exit	
SWT2(config)#vlan 20	Creo la vlan 20
SWT2(config-vlan)#name Mercadeo	Asigno el nombre Mercadeo
SWT2(config-vlan)#exit	
SWT2(config)#vlan 30	Creo la vlan 30
SWT2(config-vlan)#name Planta	Asigno el nombre Planta
SWT2(config-vlan)#exit	
SWT2(config)#vlan 99	Creo la vlan 99
SWT2(config-vlan)#name Admon	Asigno el nombre Admon
SWT2(config-vlan)#exit	
SWT2(config)#exit	
SWT2#wr	

3. Verifique que las VLANs han sido agregadas correctamente.

   Para verificar las VLANS creadas utilizo el comando show vlan brief

```
SWT2#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

   Para garantizar que las VLANs aparecen en el switch SWT1 aplico el mismo comando en este.

Verifico en SWT1

```
SWT1#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

4. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 20	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

Debido que los puertos usados en los switches son diferentes a los que estoy usando, creo la tabla de acuerdo a la topología implementada.

Interfaz	VLAN	Direcciones IP de los PCs
E1/0	VLAN 10	190.108.10.1 / 24
E1/1	VLAN 20	190.108.20.2 /24
E1/2	VLAN 30	190.108.30.3 /24
E1/0	VLAN 10	190.108.10.4 / 24
E1/1	VLAN 20	190.108.20.5 /24
E1/2	VLAN 30	190.108.30.6 /24
E1/0	VLAN 10	190.108.10.7 / 24
E1/1	VLAN 20	190.108.20.8 /24
E1/2	VLAN 30	190.108.30.9 /24

5. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.

Configuración para el switch SWT1

```
SWT1#configure terminal
SWT1(config)#interface ethernet 1/0                    Ingreso al puerto
SWT1(config-vlan)#switchport mode access               Configuro el modo
de acceso
SWT1(config-vlan)#switchport access vlan 10            Asino la VLAN10
al puerto
SWT1(config-vlan)#exit
```

Configuración para el switch SWT2

```
SWT2#configure terminal
SWT2(config)#interface ethernet 1/0                    Ingreso al puerto
SWT2(config-vlan)#switchport mode access               Configuro el modo
de acceso
SWT2(config-vlan)#switchport access vlan 10            Asino la VLAN10
al puerto
SWT2(config-vlan)#exit
```

Configuración para el switch SWT3

```
SWT3#configure terminal
SWT3(config)#interface ethernet 1/0                    Ingreso al puerto
SWT3(config-vlan)#switchport mode access               Configuro el modo
de acceso
SWT3(config-vlan)#switchport access vlan 10            Asino la VLAN10
al puerto
SWT3(config-vlan)#exit
```

6. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

Configuración para el switch SWT1 de los puertos E1/1-2

```
SWT1#configure terminal
SWT1(config)#interface ethernet 1/1                    Ingreso al puerto
```

SWT1(config-vlan)#switchport mode access	Configuro el modo de acceso
SWT1(config-vlan)#switchport access vlan 20	Asino la VLAN20 al puerto
SWT1(config-vlan)#exit	
SWT1(config)#interface ethernet 1/2	Ingreso al puerto
SWT1(config-vlan)#switchport mode access	Configuro el modo de acceso
SWT1(config-vlan)#switchport access vlan 30	Asino la VLAN30 al puerto
SWT1(config-vlan)#exit	
SWT1(config)#end	
SWT1#wr	Guardo configuración

Configuración para el switch SWT2 de los puertos E1/1-2

SWT2#configure terminal	
SWT2(config)#interface ethernet 1/1	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuro el modo de acceso
SWT2(config-vlan)#switchport access vlan 20	Asino la VLAN20 al puerto
SWT2(config-vlan)#exit	
SWT2(config)#interface ethernet 1/2	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuro el modo de acceso
SWT2(config-vlan)#switchport access vlan 30	Asino la VLAN30 al puerto
SWT2(config-vlan)#exit	
SWT2(config)#end	
SWT2#wr	Guardo configuración

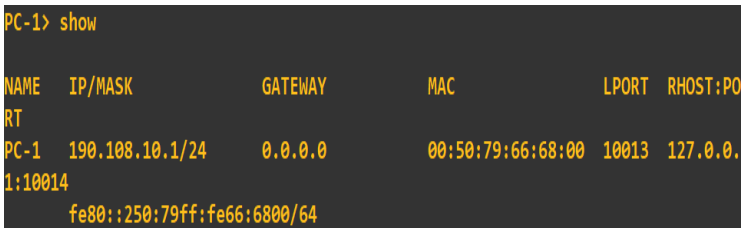
Configuración para el switch SWT3 de los puertos E1/1-2

SWT3#configure terminal	
SWT3(config)#interface ethernet 1/1	Ingreso al puerto
SWT3(config-vlan)#switchport mode access	Configuro el modo de acceso
SWT3(config-vlan)#switchport access vlan 20	Asino la VLAN20 al puerto

SWT3(config-vlan)#exit
SWT3(config)#interface ethernet 1/2 Ingreso al puerto
SWT3(config-vlan)#switchport mode access Configuro el modo de acceso
SWT3(config-vlan)#switchport access vlan 30 Asino la VLAN30 al puerto
SWT3(config-vlan)#exit
SWT3(config)#end
SWT3#wr Guardo configuración

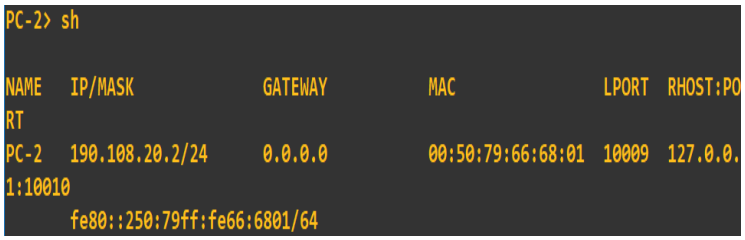
Asignación IP a VPC 01

PC-1>ip 190.108.10.1/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.



Asignación IP a VPC 02

PC-1>ip 190.108.20.2/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.



Asignación IP a VPC 03

PC-1>ip 190.108.30.3/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-3> sh

NAME   IP/MASK             GATEWAY          MAC              LPORT  RHOST:PO
RT
PC-3   190.108.30.3/24      0.0.0.0          00:50:79:66:68:02  10011  127.0.0.
1:10012
       fe80::250:79ff:fe66:6802/64
```

Asignación IP a VPC 04

PC-1>ip 190.108.10.4/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP**.**

```
PC-4> sh

NAME   IP/MASK             GATEWAY          MAC              LPORT  RHOST:PO
RT
PC-4   190.108.10.4/24      0.0.0.0          00:50:79:66:68:03  10015  127.0.0.
1:10016
       fe80::250:79ff:fe66:6803/64
```

Asignación IP a VPC 05
PC-1>ip 190.108.20.5/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-5> sh

NAME   IP/MASK             GATEWAY          MAC              LPORT  RHOST:PO
RT
PC-5   190.108.20.5/24      0.0.0.0          00:50:79:66:68:04  10017  127.0.0.
1:10018
       fe80::250:79ff:fe66:6804/64
```

Asignación IP a VPC 06

PC-1>ip 190.108.30.6/24
Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-6> sh

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PO
RT
PC-6   190.108.30.6/24      0.0.0.0          00:50:79:66:68:05  10019  127.0.0.
1:10020
       fe80::250:79ff:fe66:6805/64
```

Asignación IP a VPC 07

PC-1>ip 190.108.10.7/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-7> sh

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PO
RT
PC-7   190.108.10.7/24      0.0.0.0          00:50:79:66:68:06  10021  127.0.0.
1:10022
       fe80::250:79ff:fe66:6806/64
```

Asignación IP a VPC 08

PC-1>ip 190.108.20.8/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-8> sh

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PO
RT
PC-8   190.108.20.8/24      0.0.0.0          00:50:79:66:68:07  10023  127.0.0.
1:10024
       fe80::250:79ff:fe66:6807/64
```

Asignación IP a VPC 09

PC-1>ip 190.108.30.9/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP.

```
PC-9> sh

NAME   IP/MASK             GATEWAY          MAC               LPORT  RHOST:PO
RT
PC-9   190.108.30.9/24      0.0.0.0          00:50:79:66:68:08  10025  127.0.0.
1:10026
       fe80::250:79ff:fe66:6808/64
```

D. Configurar las direcciones IP en los Switches.

1. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

Para configurar VLAN99 para el switch SWT1 procedo de la siguiente forma:

```
SWT1#configure terminal
SWT1(config)#interface vlan 99                          Ingreso a la vlan
SWT1(config-vlan)#ip address 190.108.99.1 255.255.255.0 Configuro
SWT2(config-vlan)#no shutdown
SWT1(config-vlan)#exit
SWT1(config)#end
SWT1#wr                                                 Guardo
configuración
```

Para configurar VLAN99 para el switch SWT2 procedo de la siguiente forma:

```
SWT2#configure terminal
SWT2(config)#interface vlan 99                          Ingreso a la vlan
SWT2(config-vlan)#ip address 190.108.99.2 255.255.255.0 Configuro
SWT2(config-vlan)#no shutdown
SWT2(config-vlan)#exit
SWT2(config)#end
SWT2#wr                                                 Guardo
configuración
```

SWT3#configure terminal

```
SWT3(config)#interface vlan 99                          Ingreso a la vlan
SWT3(config-vlan)#ip address 190.108.99.3 255.255.255.0 Configuro
SWT3(config-vlan)#no shutdown
SWT3(config-vlan)#exit
```

SWT3(config)#end
SWT3#wr Guardo
configuración

E. Verificar la conectividad Extremo a Extremo

1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

VERIFICACIÓN DE PING ENTRE PC's									
PC	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
1	*X*	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*
2	*NO*	*X*	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***	*NO*
3	*NO*	*NO*	*X*	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***
4	***Satisfactorio***	*NO*	*NO*	*X*	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*
5	*NO*	***Satisfactorio***	*NO*	*NO*	*X*	*NO*	*NO*	***Satisfactorio***	*NO*
6	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	*X*	*NO*	*NO*	***Satisfactorio***
7	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	*X*	*NO*	*NO*
8	*NO*	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	*X*	*NO*
9	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	***Satisfactorio***	*NO*	*NO*	*X*

Equipos en VLAN 10

Equipos en VLAN 20

Equipos en VLAN 30

PC1

Ping entre PC1 y PC4, PC1 y PC7

```
PC-1> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=64 time=3.890 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=64 time=3.885 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=64 time=3.877 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=64 time=3.898 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=64 time=3.865 ms

PC-1> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=64 time=3.909 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=64 time=3.909 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=64 time=3.896 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=64 time=0.000 ms
```

Ping entre PC1 a PC2, PC5, PC8

```
PC-1> ping 190.108.20.2
No gateway found

PC-1> ping 190.108.20.5
No gateway found

PC-1> ping 190.108.20.8
No gateway found
```

Ping entre PC1 a PC3, PC6, PC9

```
PC-1> ping 190.108.30.3
No gateway found

PC-1> ping 190.108.30.6
No gateway found

PC-1> ping 190.108.30.9
No gateway found
```

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 10

PC2

Ping entre PC2 y PC5, PC1 y PC8

Ping entre PC2 a PC1, PC4, PC7

```
PC-2> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=64 time=0.000 ms

PC-2> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=64 time=3.865 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=64 time=3.865 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=64 time=3.883 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=64 time=3.922 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=64 time=3.881 ms
```

```
PC-2> ping 190.108.10.1
No gateway found

PC-2> ping 190.108.10.4
No gateway found

PC-2> ping 190.108.10.7
No gateway found
```

Ping entre PC2 a PC3, PC6, PC9

```
PC-2> ping 190.108.30.3
No gateway found

PC-2> ping 190.108.30.6
No gateway found

PC-2> ping 190.108.30.9
No gateway found
```

Observaciones:
No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 20,

PC3
Ping entre PC3 y PC6, PC1 y PC9

Ping entre PC3 a PC1, PC4, PC7

```
PC-3> ping 190.108.30.6
84 bytes from 190.108.30.6 icmp_seq=1 ttl=64 time=3.885 ms
84 bytes from 190.108.30.6 icmp_seq=2 ttl=64 time=3.883 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=64 time=3.922 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=64 time=3.882 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=64 time=0.000 ms

PC-3> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=64 time=0.000 ms
```

```
PC-3> ping 190.108.10.1
No gateway found

PC-3> ping 190.108.10.4
No gateway found

PC-3> ping 190.108.10.7
No gateway found
```

Ping entre PC3 a PC2, PC5, PC8

```
PC-3> ping 190.108.20.2
No gateway found

PC-3> ping 190.108.20.5
No gateway found

PC-3> ping 190.108.20.8
No gateway found
```

Observaciones:
No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 30

CONCLUSIONES

- Se establece la funcionalidad de los comandos detallando paso a paso cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.
- Gracias a los programas GNS3 y Packet Tracer que son de gran apoyo para la realizacion de las tareas planteadas en la respectiva guía. Dichas tareas se pudieron realizar apoyándose en los archivos que reposan en el entorno de conocimiento y en las interacciones con la plataforma de cisco.
- Las VLANs son un medio muy poderoso a la hora de gestionar redes de área local de mediano y gran tamaño. Ampliamente utilizadas hoy en día, el conocimiento y comprensión de las mismas es fundamental para cualquier administrador de redes.
- se elaboraran tres escenarios correspondientes a la temática de implementación de soluciones soportadas en enrutamiento avanzado como etapa final del curso Diplomado de profundización Cisco CCNP.

REFERENCIAS BIBLIOGRAFICAS

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv6 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

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

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