

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES CCNP

EDWAR E AVELLANEDA VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA –ECBT
INGENIERIA EN TELECOMUNICACIONES
BOGOTA 2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES CCNP

EDWAR E AVELLANEDA VARGAS

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO
DE INGENIERO EN TELECOMUNICACIONES

DIRECTOR
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA –ECBT
INGENIERIA EN TELECOMUNICACIONES
BOGOTA 2020

NOTA DE ACEPTACIÓN:

Presidente del Jurado

Jurado

Jurado

Bogotá, 13 de mayo de 2020

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES.....	5
LISTA DE TABLAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN.....	10
ESCENARIO 1.....	11
ESCENARIO 2.....	19
CONCLUSIONES.....	31
BIBLIOGRAFÍA.....	32

LISTA DE ILUSTRACIONES

Ilustración.....	Página
Ilustración 1. Escenario 1.....	11
Ilustración 2. Montaje del Escenario 1 EBGp en GNS3.....	11
Ilustración 3. comando show ip route en R01-AS01.....	14
Ilustración 4. comando show ip route en R02-AS2.....	14
Ilustración 5. comando show ip route en R02-AS2.....	15
Ilustración 6. comando show ip route en R03-AS3.....	15
Ilustración 7. comando show ip route en R03-AS3.....	16
Ilustración 8. comando show ip route en R04-AS4.....	16
Ilustración 9. comando show ip route en R03-AS3.....	17
Ilustración 10. comando show ip route en R04-AS4.....	18
Ilustración 11. escenario 2.....	19
Ilustración 12. comando show VTP status en SW-BB.....	20
Ilustración 13. comando show VTP status en SW-AA.....	20
Ilustración 14. comando show VTP status en SW-CC.....	21
Ilustración 15. comando show interface trunk en SW-BB.....	21
Ilustración 16. comando show interface trunk en SW-AA.....	22
Ilustración 17. comando show interface trunk en SW-AA.....	22
Ilustración 18. comando show interface trunk en SW-CC.....	22
Ilustración 19. comando show interface trunk en SW-BB.....	23
Ilustración 20. comando show interface trunk en SW-CC.....	23
Ilustración 21. comando show VLAN brief en SW-BB.....	24
Ilustración 22. comando show VLAN brief en SW-AA.....	24
Ilustración 23. prueba de conectividad PING del PC-1.....	27
Ilustración 24. prueba de conectividad PING del PC-9.....	28

Ilustración 25. prueba de conectividad PING del PC-5.....	28
Ilustración 26. prueba de conectividad PING del SW-AA.....	29
Ilustración 27. prueba de conectividad PING del SW-BB.....	29
Ilustración 28. prueba de conectividad PING del SW-AA.....	30
Ilustración 29. prueba de conectividad PING del SW-BB	30

LISTA DE TABLAS

Tabla 1. Direccionamiento IP de los computadores.....	25
---	----

GLOSARIO

Dirección IP: es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

Gns3: es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.

Loop-back interface: es una interfaz lógica y virtual en un enrutador Cisco y no es una interfaz física como la interfaz Fast Ethernet o la interfaz Gigabit Ethernet.

Router: es un dispositivo físico de red que facilita la conexión entre una red local e Internet a través de conmutación de paquetes, y del análisis de la cabecera de un paquete de datos que contiene la dirección IP de destino. El enrutador determina la ruta más eficiente hacia la dirección de destino.

Switch: o conmutador es un dispositivo de interconexión de redes de cómputo y tiene como función conectar dos o más segmentos de red, pasando datos de un segmento de la red a otro.

Trunk link: es un enlace troncal punto a punto que transporta el tráfico de varias VLAN a través de un único dispositivo físico. Este enlace se implementa entre los dos switches o dos dispositivos cualesquiera. El enlace troncal se usa para extender las operaciones de Capa 2 en toda una red, como las VLAN de extremo a extremo.

VLAN: es un dominio de difusión lógica que puede abarcar múltiples segmentos físicos de LAN.

VTP: VLAN Trunking Protocol, es un protocolo que se utiliza para distribuir y sincronizar información sobre bases de datos VLAN configurado a través de una red conmutada.

RESUMEN

El presente documento hace parte del diplomado de profundización Cisco CCNP y muestra el desarrollo dos escenarios que tienen como propósito identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. El primer ejercicio trata sobre Cisco IP Routing y otro sobre Cisco IP Switched Network y cada uno se ha documentado con los procesos y configuración de los dispositivos y los métodos de verificación de conectividad.

El primer escenario plantea la implementación de protocolo de enrutamiento BGP (Border Gateway Protocol) para intercambiar información de enrutamiento entre cuatro Sistemas Autónomos diferentes establecer las relaciones de vecino, anunciar las direcciones de Loop-back y establecer rutas estáticas.

El segundo escenario se trata sobre poner en funcionamiento tres switches que hacen parte de la capa de acceso de una red empresarial. Para ello se hará uso del protocolo VTP (VLAN Trunking Protocol) para configurar y administrar las VLANs en equipos Cisco, así como también la implementación de canales troncales.

Palabras clave: CCNP, Cisco, IP Routing, BGP, Loop-back, Trunk, VLAN, VTP

ABSTRACT

This document is part of the Cisco CCNP deepening diploma and shows the development of two scenarios that aim to identify the degree of development of competencies and skills that were acquired throughout the diploma. The first exercise is about Cisco IP Routing and another about Cisco IP Switched Network and each has been documented with the processes and configuration of the devices and the methods of verification of connectivity.

The first scenario involves the implementation of the BGP (Border Gateway Protocol) routing protocol to exchange routing information between four different Autonomous Systems, establish neighbor relations, announce Loop-back addresses and establish static routes.

The second scenario is about putting three switches into operation that stop the access layer of an enterprise network. For this, the VTP (VLAN Trunking Protocol) will be used to configure and manage VLANs on Cisco equipment, as well as the implementation of trunk channels.

Keywords: CCNP, Cisco, IP Routing, BGP, Loop-back, Trunk, VLAN, VTP

INTRODUCCIÓN

El presente documento muestra el desarrollo de la “Prueba de habilidades CCNP”, la cual hace parte de las actividades evaluativas del Diplomado de Profundización Cisco. Su objetivo es identificar el grado de desarrollo de competencias y habilidades para operar y configurar un enrutador o switch Cisco. Esta prueba de habilidades está compuesta por dos escenarios con problemas relacionados con diversos aspectos de Networking y pondrá en práctica los conocimientos adquiridos lo largo del diplomado. Cada ejercicio se ejecuta en GNS3 y está documentado con la descripción detallada del paso a paso de su solución, configuración de cada uno de los dispositivos y los procesos de verificación de conectividad.

El primer escenario evalúa las habilidades adquiridas en el tema de routing y plantea la interconexión de cuatro sistemas autónomos AS a partir de la configuración de cuatro routers con el protocolo de enrutamiento BGP (Border Gateway Protocol). Dentro de los parámetros de programación deben establecerse las adyacencias con los vecinos e intercambiar información de enrutamiento, anunciar las direcciones de Loop-back y establecer rutas estáticas para intercambiar información de las redes internas de cada AS.

El segundo escenario evalúa las competencias en el tema de Switched Network y se trata sobre poner en funcionamiento tres switches que hacen parte de la capa de acceso de una red empresarial. Como solución se hará uso del protocolo VTP (VLAN Trunking Protocol) para configurar y administrar las VLANs en los equipos Cisco, habilitar el protocolo de enlace dinámico (DTP) y así negociar la formación de los canales trcales (Trunking) entre dos switches, en cada uno de se asignara una dirección IP al SVI (Switch Virtual Interface) de acuerdo a la tabla de direccionamiento e interfaz activa.

ESCENARIO 1

Descripción de escenarios propuestos para la prueba de habilidades

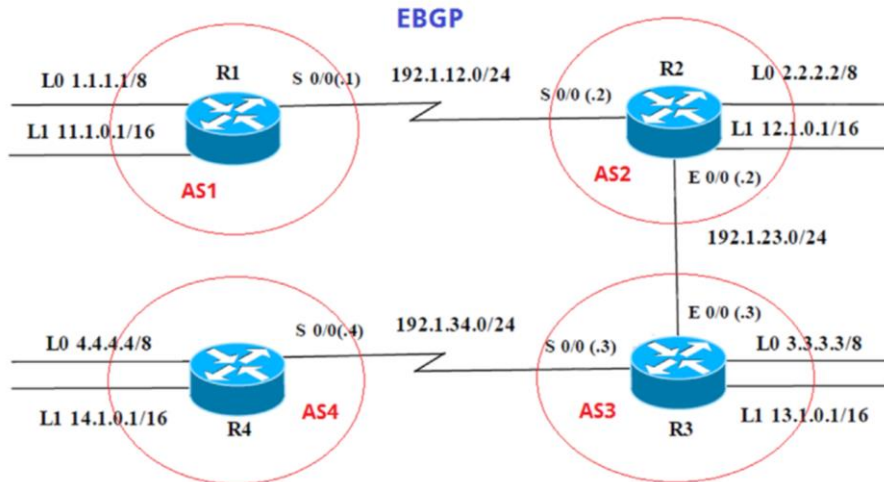


Ilustración 1 Escenario 1

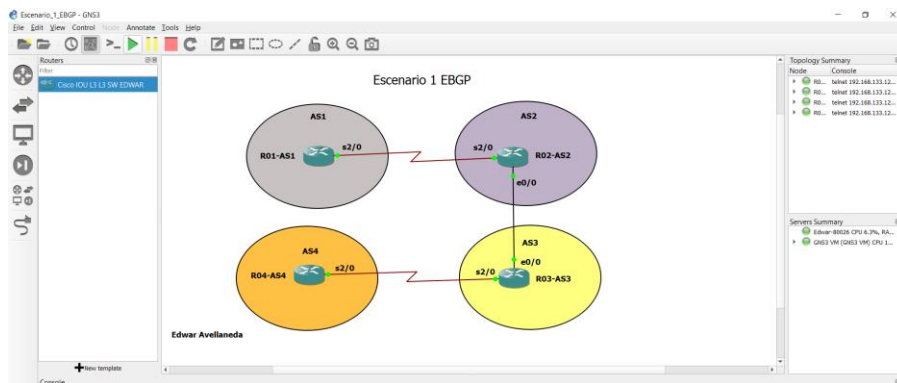


Ilustración 2 Montaje del Escenario 1 EBG en GNS3

Configuración básica de los routers de acuerdo al siguiente ejemplo:

```
R01-AS1 (config) #ip domain-name CCNP.NET
R01-AS1 (config) #no ip domain lookup
R01-AS1 (config) #interface range e0/0-3,e1/0-3
R01-AS1 (config) #shutdown
R01-AS1 (config) #exit
R01-AS1 (config) #line con 0
R01-AS1 (config) #no exec-timeout
R01-AS1 (config) #logging synchronous
R01-AS1 (config) #exit
R01-AS1 (config) #hostname R01-AS1
```

Configuración de las interfaces loop-back, serial y ethernet en R01, R02, R03 y R04:

```
R01-AS1(config)# interface Lo0
R01-AS1(config-if)# description Lo0 AS1
R01-AS1(config-if)# ip address 1.1.1.1 255.0.0.0
R01-AS1(config-if)# exit
R01-AS1(config)# interface Lo1
R01-AS1(config-if)# description Lo1 AS1
R01-AS1(config-if)# ip address 11.1.0.1 255.255.0.0
R01-AS1(config-if)# exit
R01-AS1(config)# interface Serial2/0
R01-AS1(config-if)# description Link R01 -> R02
R01-AS1(config-if)# ip address 192.1.12.1 255.255.255.0
R01-AS1(config-if)# clock rate 64000
R01-AS1(config-if)# no shutdown
R01-AS1(config-if)# end
R01-AS1#
```

```
R02-AS2(config)# interface Lo0
R02-AS2(config-if)# description Lo0 AS2
R02-AS2(config-if)# ip address 2.2.2.2 255.0.0.0
R02-AS2(config-if)# exit
R02-AS2(config)# interface Lo1
R02-AS2(config-if)# description Lo1 AS2
R02-AS2(config-if)# ip address 12.1.0.1 255.255.0.0
R02-AS2(config-if)# exit
R02-AS2(config)# interface Serial2/0
R02-AS2(config-if)# description Link R02 -> R01
R02-AS2(config-if)# ip address 192.1.12.2 255.255.255.0
R02-AS2(config-if)# clock rate 64000
R02-AS2(config-if)# no shutdown
R02-AS2(config-if)# end
R02-AS2(config)# interface Ethernet0/0
R02-AS2(config-if)# description Link R02 -> R03
R02-AS2(config-if)# ip address 192.1.23.2 255.255.255.0
R02-AS2(config-if)# no shutdown
R02-AS2(config-if)# end
R02-AS2#
```

```
R03-AS3(config)# interface Lo0
R03-AS3(config-if)# description Lo0 AS3
R03-AS3(config-if)# ip address 3.3.3.3 255.0.0.0
```

```

R03-AS3(config-if)# exit
R03-AS3(config)# interface Lo1
R03-AS3(config-if)# description Lo1 AS3
R03-AS3(config-if)# ip address 13.1.0.1 255.255.0.0
R03-AS3(config-if)# exit
R03-AS3(config)# interface Serial2/0
R03-AS3(config-if)# description Link R03 -> R04
R03-AS3(config-if)# ip address 192.1.34.3 255.255.255.0
R03-AS3(config-if)# clock rate 64000
R03-AS3(config-if)# no shutdown
R03-AS3(config-if)# end
R03-AS3(config)# interface Ethernet0/0
R03-AS3(config-if)# description Link R03 -> R02
R03-AS3(config-if)# ip address 192.1.23.3 255.255.255.0
R03-AS3(config-if)# no shutdown
R03-AS3(config-if)# end
R03-AS3#

```

```

R04-AS4(config)# interface Lo0
R04-AS4(config-if)# description Lo0 AS4
R04-AS4(config-if)# ip address 4.4.4.4 255.0.0.0
R04-AS4(config-if)# exit
R04-AS4(config)# interface Lo1
R04-AS4(config-if)# description Lo1 AS4
R04-AS4(config-if)# ip address 14.1.0.1 255.255.0.0
R04-AS4(config-if)# exit
R04-AS4(config)# interface Serial2/0
R04-AS4(config-if)# description Link R04 -> R03
R04-AS4(config-if)# ip address 192.1.34.4 255.255.255.0
R04-AS4(config-if)# clock rate 64000
R04-AS4(config-if)# no shutdown
R04-AS4(config-if)# end
R04-AS#

```

- 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 22.22.22.22 para R1 y como 33.33.33.33 para R2.**

```

R01-AS1(config)# router bgp 1
R01-AS1(config-router)#bgp router-id 22.22.22.22
R01-AS1(config-router)#neighbor 192.1.12.2 remote-as 2
R01-AS1(config-router)#network 1.0.0.0
R01-AS1(config-router)#network 11.1.0.0 mask 255.255.0.0

```

```
R01-AS1 (config-router) #end
```

```
R02-AS2 (config) # router bgp 2
```

```
R02-AS2 (config-router) #bgp router-id 33.33.33.33
```

```
R02-AS2 (config-router) #neighbor 192.1.12.1 remote-as 1
```

```
R02-AS2 (config-router) #network 2.0.0.0
```

```
R02-AS2 (config-router) #network 12.1.0.0 mask 255.255.0.0
```

```
R02-AS2 (config-router) #end
```

Presente la salida del comando show ip route.

```
1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   1.0.0.0/8 is directly connected, Loopback0
L   1.1.1.1/32 is directly connected, Loopback0
B   2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:13
    11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   11.1.0.0/16 is directly connected, Loopback1
L   11.1.0.1/32 is directly connected, Loopback1
    12.0.0.0/16 is subnetted, 1 subnets
B   12.1.0.0 [20/0] via 192.1.12.2, 00:00:13
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.12.0/24 is directly connected, Serial2/0
L   192.1.12.1/32 is directly connected, Serial2/0
R01-AS1#
```

Ilustración 3 comando show ip route en R01-AS01, se pueden observar las redes compartidas a través EBGP de R02-AS2 vía ip 192.1.12.2

```
B   1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:06
    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   2.0.0.0/8 is directly connected, Loopback0
L   2.2.2.2/32 is directly connected, Loopback0
    11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.12.1, 00:00:06
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   12.1.0.0/16 is directly connected, Loopback1
L   12.1.0.1/32 is directly connected, Loopback1
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.12.0/24 is directly connected, Serial2/0
L   192.1.12.2/32 is directly connected, Serial2/0
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.23.0/24 is directly connected, Ethernet0/0
L   192.1.23.2/32 is directly connected, Ethernet0/0
R02-AS2#
```

Ilustración 4 comando show ip route en R02-AS2, se pueden observar las redes compartidas a través EBGP de R01-AS1 vía ip 192.1.12.1

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3.

```
R02-AS2 (config) # router bgp 2
```

```
R02-AS2 (config-router) #neighbor 192.1.23.3 remote-as 3
```

```
R02-AS2 (config-router) #network 2.0.0.0
```

```
R02-AS2 (config-router) #network 12.1.0.0 mask 255.255.0.0
```

```
R02-AS2 (config-router) #end
```

Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44.

```
R03-AS3 (config) # router bgp 3
R03-AS3 (config-router) #bgp router-id 44.44.44.44
R03-AS3 (config-router) #neighbor 192.1.23.2 remote-as 2
R03-AS3 (config-router) #network 3.0.0.0
R03-AS3 (config-router) #network 13.1.0.0 mask 255.255.0.0
R03-AS3 (config-router) #end
```

Presente la salida del comando `show ip route`.

```
B 1.0.0.0/8 [20/0] via 192.1.12.1, 00:06:35
  2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   2.0.0.0/8 is directly connected, Loopback0
L   2.2.2.2/32 is directly connected, Loopback0
B 3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:34
  11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.12.1, 00:06:35
  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   12.1.0.0/16 is directly connected, Loopback1
L   12.1.0.1/32 is directly connected, Loopback1
  13.0.0.0/16 is subnetted, 1 subnets
B   13.1.0.0 [20/0] via 192.1.23.3, 00:00:34
  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.12.0/24 is directly connected, Serial12/0
L   192.1.12.2/32 is directly connected, Serial12/0
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.23.0/24 is directly connected, Ethernet0/0
L   192.1.23.2/32 is directly connected, Ethernet0/0
R02-AS2#
```

Ilustración 5 comando `show ip route` en R02-AS2, se pueden observar las redes compartidas a través EBGP de R03-AS3 vía 192.1.23.3

```
B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:20
B 2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:20
  3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   3.0.0.0/8 is directly connected, Loopback0
L   3.3.3.3/32 is directly connected, Loopback0
  11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.23.2, 00:00:20
  12.0.0.0/16 is subnetted, 1 subnets
B   12.1.0.0 [20/0] via 192.1.23.2, 00:00:20
  13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   13.1.0.0/16 is directly connected, Loopback1
L   13.1.0.1/32 is directly connected, Loopback1
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.23.0/24 is directly connected, Ethernet0/0
L   192.1.23.3/32 is directly connected, Ethernet0/0
R03-AS3#
```

Ilustración 6 comando `show ip route` en R03-AS3, se pueden observar las redes compartidas a través EBGP de R03-AS3 vía 192.1.23.2

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4.

```
R03-AS3 (config) # router bgp 3
R03-AS3 (config-router) # neighbor 192.1.34.4 remote-as 4
R03-AS3 (config-router) # end
```

Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66.

```
R04-AS4 (config) # router bgp 4
R04-AS4 (config-router) # bgp router-id 66.66.66.66
R04-AS4 (config-router) # neighbor 192.1.34.3 remote-as 3
R04-AS4 (config-router) # network 4.0.0.0
R04-AS4 (config-router) # network 14.1.0.0 mask 255.255.0.0
```

```
B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:16:07
B 2.0.0.0/8 [20/0] via 192.1.23.2, 00:16:07
 3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.0.0.0/8 is directly connected, Loopback0
L 3.3.3.3/32 is directly connected, Loopback0
B 4.0.0.0/8 [20/0] via 192.1.34.4, 00:01:39
 11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0 [20/0] via 192.1.23.2, 00:16:07
 12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0 [20/0] via 192.1.23.2, 00:16:07
 13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 13.1.0.1/32 is directly connected, Loopback1
 14.0.0.0/16 is subnetted, 1 subnets
B 14.1.0.0 [20/0] via 192.1.34.4, 00:01:39
 192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, Ethernet0/0
L 192.1.23.3/32 is directly connected, Ethernet0/0
 192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial2/0
L 192.1.34.3/32 is directly connected, Serial2/0
R03-AS3#
```

Figure 7 comando show ip route en R03-AS3, se pueden observar las redes compartidas a través EBGP de R04-AS4 vía 192.1.34.4

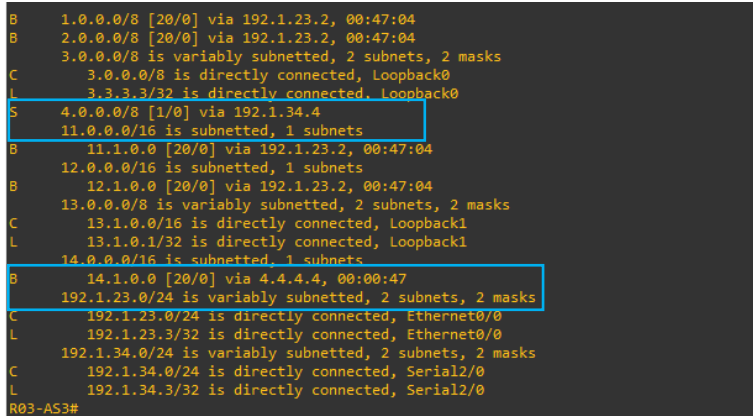
```
B 1.0.0.0/8 [20/0] via 192.1.34.3, 00:26:50
B 2.0.0.0/8 [20/0] via 192.1.34.3, 00:26:50
B 3.0.0.0/8 [20/0] via 192.1.34.3, 00:26:50
 4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 4.0.0.0/8 is directly connected, Loopback0
L 4.4.4.4/32 is directly connected, Loopback0
 11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0 [20/0] via 192.1.34.3, 00:26:50
 12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0 [20/0] via 192.1.34.3, 00:26:50
 13.0.0.0/16 is subnetted, 1 subnets
B 13.1.0.0 [20/0] via 192.1.34.3, 00:26:50
 14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 14.1.0.0/16 is directly connected, Loopback1
L 14.1.0.1/32 is directly connected, Loopback1
 192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial2/0
L 192.1.34.4/32 is directly connected, Serial2/0
R04-AS4#
```

Ilustración 8 comando show ip route en R04-AS4, se pueden observar las redes compartidas a través EBGP de R03-AS3 vía 192.1.34.3

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.

```
R03-AS3(config)# ip route 4.0.0.0 255.0.0.0 192.1.34.4
R03-AS3(config)# router bgp 3
R03-AS3(config-router)#no neighbor 192.1.34.4 remote-as 4
R03-AS3(config-router)#neighbor 4.4.4.4 remote-as 4
R03-AS3(config-router)#neighbor 4.4.4.4 update-source
loopback 0
R03-AS3(config-router)#neighbor 4.4.4.4 ebgp-multihop
R03-AS3(config-router)#end
```

```
R04-AS4(config)# ip route 3.0.0.0 255.0.0.0 192.1.34.3
R04-AS4(config)# router bgp 4
R04-AS4(config-router)# no neighbor 192.1.34.3 remote-as 3
R04-AS4(config-router)# neighbor 3.3.3.3 remote-as 3
R04-AS4(config-router)# neighbor 3.3.3.3 update-source
loopback 0
R04-AS4(config-router)# neighbor 3.3.3.3 ebgp-multihop
R04-AS4(config-router)#end
```



```
B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:47:04
B 2.0.0.0/8 [20/0] via 192.1.23.2, 00:47:04
3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.0.0.0/8 is directly connected, Loopback0
L 3.3.3.3/32 is directly connected, Loopback0
S 4.0.0.0/8 [1/0] via 192.1.34.4
11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0 [20/0] via 192.1.23.2, 00:47:04
12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0 [20/0] via 192.1.23.2, 00:47:04
13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 13.1.0.1/32 is directly connected, Loopback1
14.0.0.0/16 is subnetted, 1 subnets
B 14.1.0.0 [20/0] via 4.4.4.4, 00:00:47
192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, Ethernet0/0
L 192.1.23.3/32 is directly connected, Ethernet0/0
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial2/0
L 192.1.34.3/32 is directly connected, Serial2/0
R03-AS3#
```

Ilustración 9 comando show ip route en R03-AS3, se pueden observar las redes compartidas a través EBGP de R04-AS4 vía Look-back 4.4.4.4 y la ruta estática definida

```

R04-AS4#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
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:01:29
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:01:29
S    3.0.0.0/8 [1/0] via 192.1.34.3
     4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 3.3.3.3, 00:01:29
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:01:29
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:01:29
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial2/0
L    192.1.34.4/32 is directly connected, Serial2/0
R04-AS4#

```

Ilustración 10 comando show ip route en R04-AS4, se pueden observar las redes compartidas a través EBGP de R03-AS3 vía Look-back 3.3.3.3 y la ruta estática definida

ESCENARIO 2

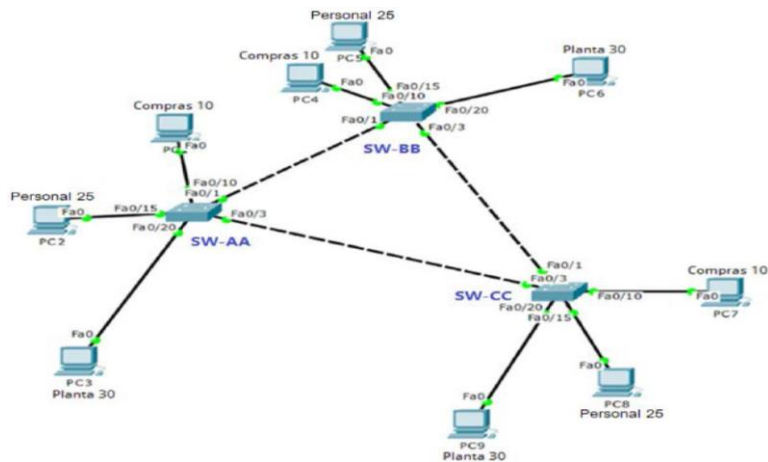


Ilustración 11, escenario 2

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN.

Configuración básica de cada switch de acuerdo al siguiente ejemplo:

```
SW-AA(config)#ip domain-name CCNP.NET
SW-AA(config)#no ip domain lookup
SW-AA(config)#interface range e0/0-3,e1/0-3,e2/0-3,e3/0-3
SW-AA(config-if)#shutdown
SW-AA(config-if)#exit
SW-AA(config)#vtp mode transparent
SW-AA(config)#line con 0
SW-AA(config-line)#no exec-timeout
SW-AA(config-line)#logging synchronous
SW-AA(config-line)#exit
SW-AA(config)#Hostname SW-AA
```

El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

```
SW-BB(config)# vtp version 2
SW-BB(config)# vtp domain CCNP
SW-BB(config)# vtp password cisco
SW-BB(config)#vtp mode server
```

```
SW-AA(config)# vtp version 2
```

```
SW-AA(config)# vtp domain CCNP
SW-AA(config)# vtp password cisco
SW-AA(config)#vtp mode client
```

```
SW-CC(config)# vtp version 2
SW-CC(config)# vtp domain CCNP
SW-CC(config)# vtp password cisco
SW-CC(config)#vtp mode client
```

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

```
SW-BB#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : CCNP
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision  : 0
MD5 digest              : 0x0A 0x1C 0xA3 0x2F 0xDE 0xE7 0x05 0xA9
                       : 0xA1 0x07 0xD6 0x5E 0x13 0xC0 0x0D 0x4E
SW-BB#
```

Ilustración 12 comando show VTP status en SW-BB

```
SW-AA#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : CCNP
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision  : 0
MD5 digest              : 0x0A 0x1C 0xA3 0x2F 0xDE 0xE7 0x05 0xA9
                       : 0xA1 0x07 0xD6 0x5E 0x13 0xC0 0x0D 0x4E
SW-AA#
```

Ilustración 13 comando show VTP status en SW-AA

```

SW-CC#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : CCNP
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision  : 0
MDS digest              : 0x0A 0x1C 0xA3 0x2F 0xDE 0xE7 0x05 0xA9
                        : 0xA1 0x07 0xD6 0x5E 0x13 0xC0 0x0D 0x4E
SW-CC#

```

Ilustración 14 comando show VTP status en SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es *dynamic auto*, solo un lado del enlace debe configurarse como *dynamic desirable*.

```

SW-BB(config)# interface e0/0
SW-BB(config-if)# switchport trunk encapsulation dot1q
SW-BB(config-if)# switchport mode dynamic auto
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit

```

```

SW-AA(config)# interface e0/0
SW-AA(config-if)# switchport trunk encapsulation dot1q
SW-AA(config-if)# switchport mode dynamic desirable
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit

```

5. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando *show interfaces trunk*.

```

SW-BB#show interface trunk

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

```

Ilustración 15 comando show interface trunk en SW-BB

```
SW-AA#show interface trunk

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

Ilustración 16 comando show interface trunk en SW-AA

6. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando *switchport mode trunk* en la interfaz F0/3 de SW-AA

```
SW-AA(config)# interface e0/3
SW-AA(config-if)# switchport trunk encapsulation dot1q
SW-AA(config-if)# switchport mode trunk
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
```

```
SW-CC(config)# interface e0/3
SW-CC(config-if)# switchport trunk encapsulation dot1q
SW-CC(config-if)# switchport mode trunk
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
```

Verifique el enlace "trunk" el comando *show interfaces trunk* en SW-AA.

```
SW-AA#show interface trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/0     desirable     802.1q         trunking      1
Et0/3     on            802.1q         trunking      1
```

Ilustración 17 comando show interface trunk en SW-AA

```
SW-CC#show interface trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/3     on            802.1q         trunking      1
```

Ilustración 18 comando show interface trunk en SW-CC

7. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

```
SW-BB(config)# interface e0/1
SW-BB(config-if)# switchport trunk encapsulation dot1q
SW-BB(config-if)# switchport mode trunk
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
```

```
SW-CC(config)# interface e0/1
SW-CC(config-if)# switchport trunk encapsulation dot1q
SW-CC(config-if)# switchport mode trunk
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
```

8. Verifique el enlace "trunk" el comando *show interfaces trunk* en SW-BB y CC.

```
SW-BB#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	auto	802.1q	trunking	1
Et0/1	on	802.1q	trunking	1

Ilustración 19 comando show interface trunk en SW-BB

```
SW-CC#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/1	on	802.1q	trunking	1
Et0/3	on	802.1q	trunking	1

Ilustración 20 comando show interface trunk en SW-CC

C. Agregar VLANs y asignar puertos.

9. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99)

```
SW-AA(config)# vlan 10
SW-AA(config-vlan)#exit
```

```
SW-BB(config)# vlan 10
SW-BB(config-vlan)# name Compras
```

```

SW-BB(config-vlan) # vlan 25
SW-BB(config-vlan) # name Personas
SW-BB(config-vlan) # vlan 30
SW-BB(config-vlan) # name Planta
SW-BB(config-vlan) # vlan 99
SW-BB(config-vlan) # name Administracion
SW-BB(config-vlan) #exit

```

10. Verifique que las VLANs han sido agregadas correctamente.

```

SW-BB#show vlan brief

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
25   Personas                active
30   Planta                  active
99   Administracion          active
1002 fddi-default           act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default       act/unsup
1005 trbrf-default         act/unsup
SW-BB#

```

Ilustración 21 comando show VLAN brief en SW-BB

```

SW-AA#show vlan brief

VLAN Name                Status    Ports
-----
1    default                 active    Et0/1, Et0/2, 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
25   Personas                active
30   Planta                  active
99   Administracion          active
1002 fddi-default           act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default       act/unsup
1005 trbrf-default         act/unsup
SW-AA#

```

Ilustración 22 comando show VLAN brief en SW-AA

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

Interfaz	VLAN	VLAN
PC - 1 E1/0	VLAN 10	190.108.10.10 / 24
PC - 2 E1/1	VLAN 25	190.108.20.20 /24
PC - 3 E1/2	VLAN 30	190.108.30.30 /24
PC - 4 E1/0	VLAN 10	190.108.10.11 / 24
PC - 5 E1/1	VLAN 25	190.108.20.21 /24
PC - 6 E1/2	VLAN 30	190.108.30.31 /24
PC - 7 E1/0	VLAN 10	190.108.10.12 / 24
PC - 8 E1/1	VLAN 25	190.108.20.22 /24
PC - 9 E1/2	VLAN 30	190.108.30.32 /24

Tabla 1 Direccionamiento IP de los computadores que hacen parte de la red

12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

```
SW-BB(config)# interface e1/0
SW-BB(config-if)# switchport mode access
SW-BB(config-if)# switchport access vlan 10
SW-BB(config-if)# spanning-tree portfast
SW-BB(config-if)# no shutdown
SW-BB(config-if)# end
```

```
SW-AA(config)# interface e1/0
SW-AA(config-if)# switchport mode access
SW-AA(config-if)# switchport access vlan 10
SW-AA(config-if)# spanning-tree portfast
SW-AA(config-if)# no shutdown
SW-AA(config-if)# end
```

```
SW-CC(config)# interface e1/0
SW-CC(config-if)# switchport mode access
SW-CC(config-if)# switchport access vlan 10
SW-CC(config-if)# spanning-tree portfast
SW-CC(config-if)# no shutdown
SW-CC(config-if)# end
```

13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW-AA(config)# interface e1/1
SW-AA(config-if)# switchport mode access
SW-AA(config-if)# switchport access vlan 25
SW-AA(config-if)# spanning-tree portfast
SW-AA(config-if)# no shutdown
SW-AA(config-if)# end
```

```
SW-AA(config)# interface e1/2
SW-AA(config-if)# switchport mode access
SW-AA(config-if)# switchport access vlan 30
SW-AA(config-if)# spanning-tree portfast
SW-AA(config-if)# no shutdown
SW-AA(config-if)# end
```

```
SW-BB(config)# interface e1/1
SW-BB(config-if)# switchport mode access
SW-BB(config-if)# switchport access vlan 25
SW-BB(config-if)# spanning-tree portfast
SW-BB(config-if)# no shutdown
SW-BB(config-if)# end
```

```
SW-BB(config)# interface e1/2
SW-BB(config-if)# switchport mode access
SW-BB(config-if)# switchport access vlan 30
SW-BB(config-if)# spanning-tree portfast
SW-BB(config-if)# no shutdown
SW-BB(config-if)# end
```

```
SW-CC(config)# interface e1/1
SW-CC(config-if)# switchport mode access
SW-CC(config-if)# switchport access vlan 25
SW-CC(config-if)# spanning-tree portfast
SW-CC(config-if)# no shutdown
```

```
SW-CC(config)# interface e1/2
SW-CC(config-if)# switchport mode access
SW-CC(config-if)# switchport access vlan 30
SW-CC(config-if)# spanning-tree portfast
SW-CC(config-if)# no shutdown
```

D. Configurar las direcciones IP en los Switches.

14. 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.

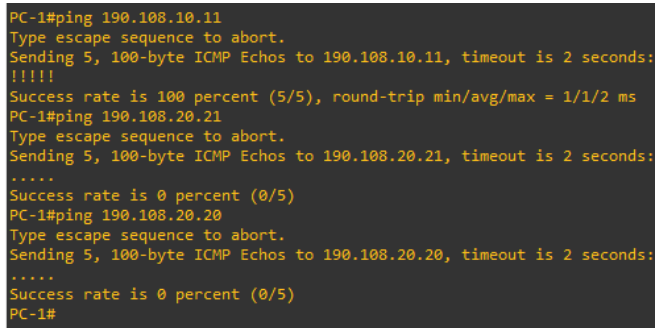
```
SW-AA(config)# interface vlan 99
SW-AA(config-vlan)# ip address 190.108.99.1 255.255.255.0
SW-AA(config-vlan)#No shutdown
SW-AA(config-vlan)# exit
```

```
SW-BB(config)# interface vlan 99
SW-BB(config-vlan)# ip address 190.108.99.2 255.255.255.0
SW-BB(config-vlan)# No shutdown
SW-BB(config-vlan)# exit
```

```
SW-CC(config)# interface vlan 99
SW-CC(config-vlan)# ip address 190.108.99.3 255.255.255.0
SW-CC(config-vlan)#No shutdown
SW-CC(config-vlan)#Exit
```

E. Verificar la conectividad Extremo a Extremo

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



```
PC-1#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC-1#ping 190.108.20.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC-1#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC-1#
```

Ilustración 23 prueba de conectividad PING del PC-1 hacia otros PCs de la red

```

PC-9#ping 190.108.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC-9#ping 190.108.20.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC-9#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Ilustración 24 prueba de conectividad PING del PC-9 hacia otros PCs de la red

```

PC-5#ping 190.108.20.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC-5#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC-5#ping 190.108.30.32
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.32, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC-5#

```

Ilustración 25 prueba de conectividad PING del PC-5 hacia otros PCs de la red

Los computadores pertenecientes a diferentes VLANs no presentaron conectividad, mientras que los computadores pertenecientes a la misma VLAN dentro de toda la red si mostraron conectividad. Esto se debe a que los computadores son de diferentes VLANs y segmentos de red y no establecen conectividad, para ello es necesario en cada uno de los Switches asignar una dirección IP al SVI (Switch Virtual Interface) y las respectivas VLANs, implementar un enrutador o Switch Multicapa.

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

```
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
SW-AA#
SW-AA#
SW-AA#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6 ms
SW-AA#
```

Ilustración 26 prueba de conectividad PING del SW-AA hacia los switches BB y CC

```
SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/5 ms
SW-BB#
SW-BB#
SW-BB#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
SW-BB#
```

Ilustración 27 prueba de conectividad PING del SW-BB hacia los switches AA y CC

Los switches presentaron conectividad ya que cuentan con la configuración del protocolo VTP, la VLAN 99 y las interfaces virtuales (SVI).

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

```
SW-AA#ping 190.108.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.22, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.30.32
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.32, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#
```

Ilustración 28 prueba de conectividad PING del SW-AA hacia varios PCs de la red ubicados en los AS 1, 2 y 3

```
SW-BB#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.31
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.31, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#
```

Ilustración 29 prueba de conectividad PING del SW-BB hacia varios PCs de la red ubicados en los AS 1, 2 y 3

No hubo conectividad ya que primero no hay configurado ninguna puerta de enlaca predeterminada ni ninguna interface virtual configurada o sistema de enrutamiento.

CONCLUSIONES

El administrador de red debe crear VLAN locales teniendo en cuenta los límites físicos en lugar de las funciones de trabajo de los usuarios en los dispositivos finales.

En un diseño jerárquico, los switches de capa de acceso se conectan a los switches de capa de distribución. Aquí es donde se implementan los canales Trunk.

En los enlaces troncales, se recomienda podar manualmente las VLAN que no se usan. A través del comando Pruning si se está usando VTP.

Los dominios VTP se pueden proteger mediante la función de contraseña VTP. Es importante asegurarse de que todos los switches en el dominio VTP tengan la misma contraseña y nombre de dominio.

Los vecinos de BGP intercambian sus mejores rutas de BGP.

El enrutador vecino que recibe esa información de red coloca la información en su tabla BGP y selecciona su mejor ruta BGP para esa red. La mejor ruta se ofrece a su tabla de enrutamiento IP.

BIBLIOGRAFÍA

- Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>
- UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>
- UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm