DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

WILSON EDUARDO BRAVO GOMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA ELECTRONICA
NEIVA
2020

PRUEBA DE HABILIDADES PRACTICAS CCNP

WILSON EDUARDO BRAVO GOMEZ

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA ELECTRONICA
NEIVA
2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Neiva, 22 de mayo de 2020

AGRADECIMIENTOS

En primer lugar deseo expresar mi agradecimiento al director de este diplomado, por el apoyo brindado, respeto y confianza ofrecidas en este trabajo, de igual manera agradezco a mis compañeros de estudio con quien he compartido trabajos, proyectos e ilusiones durante transcurso de nuestra carrera.

Doy gracias a mi familia, a mi madre, a mi compañera sentimental y a mis compañeros de trabajo que me han dado un gran apoyo moral y humano tan necesario en momentos difíciles

A todos, muchas gracias

CONTENIDO

AGRADECIMIENTOS 4
CONTENIDO 5
LISTA DE TABLAS 6
LISTA DE FIGURAS 7
GLOSARIO 8
RESUMEN 10
INTRODUCCIÓN 11
DESARROLLO LOS ESCENARIOS 12
ESCENARIO 1 12
ESCENARIO 2 20
CONCLUSIONES 33
BIBLIOGRÁFIA 34

LISTA DE TABLAS

Tabla 1. Información para configuración de los Routers 12
Tabla 2. Información para configuración de puertos y direcciones IP 27
Tabla 3. Asignación de direcciones IP al SVI..... 30

LISTA DE FIGURAS

Figura 1. Topología del escenario 1 12
Figura 2. Topología del escenario 1 en el simulador GNS3 13
Figura 3. Verificación de configuración BGP en R1 16
Figura 4. Verificación de configuración BGP en R2 16
Figura 5. Verificación de relación de vecindad entre R2 y R3 17
Figura 6. Verificación de relación de vecindad entre R3 y R4 19
Figura 7. Topología del escenario 2 20
Figura 8. Topología del escenario 2 en el simulador PACKET TRACER 20
Figura 9. Verificación de configuración de VTP 23
Figura 10. Verificación de configuración de DTP entre SW-AA y SW-BB 24
Figura 11. Verificación de enlace TRUNK estático entre SW-AA y SW-BB 25
Figura 12. Configuración de direcciones IP en PCs 27
Figura 13. Verificación de conectividad entre PCs 30
Figura 14. Verificación de conectividad entre switches 32

GLOSARIO

AS: (Autonomous System), son una red de trabajo interna de una empresa o una Infraestructura de red de un proveedor de servicios de internet.

BGP: (Border Gateway Protocol) intercambia rutas entre diferentes sistemas autónomos que forman parte de la red más grande de todas (Internet)

Broadcast: tráfico que se utiliza para enviar información a todos los dispositivos en una subred. La información se transmite de un remitente a todos los receptores conectados.

Broadcast network: red que puede conectar muchos Routers juntos con la capacidad de dirigir un solo mensaje a todos los Routers conectados. Ethernet es un ejemplo de esta red

CEF: (Cisco Express Forwarding), este método de conmutación es el modo de conmutación más rápido y requiere menos CPU que la conmutación rápida y la conmutación de proceso

Convergencia: describe el proceso de cuándo los Routers notan cambios en la red, intercambian información sobre el cambio y realizan los cálculos necesarios para reevaluar las mejores rutas

Distance vector protocols: se enfocan en determinar la dirección (vector) y la distancia (como el costo del enlace o el número de saltos) a cualquier enlace en la red.

EGP: (Exterior Gateway Protocols), estos se encargan de intercambiar rutas entre diferentes sistemas autónomos.

EIGRP: es un protocolo propietario de Cisco que combina las ventajas de los protocolos de enrutamiento de estado de enlace y vector de distancia. Sin embargo, EIGRP es un protocolo de enrutamiento de vector de distancia. EIGRP incluye características avanzadas que no se encuentran en otros protocolos de vectores de distancia, como RIP

IGP: (Interior Gateway Protocols), estos se usan dentro de la organización e intercambia rutas dentro de un sistema autónomo.

Link-state protocols: se enfocan en utilizar el algoritmo del camino más corto primero (SPF) para crear un resumen de la topología exacta de toda la red o al menos dentro de su área

Multicast: tráfico donde se envía información a múltiples destinos al mismo tiempo. Una interfaz puede pertenecer a cualquier número de grupos de multidifusión

NBMA network: (Nonbroadcast Multiaccess), red que puede admitir muchos enrutadores pero no tiene capacidad de transmisión. El remitente debe crear una

copia individual del mismo paquete para cada destinatario si desea informar a todos los vecinos conectados.

OSPF: fue desarrollado por Internet Engineering Task Force (IETF) para superar las limitaciones de los protocolos de enrutamiento por vector de distancia. Una de las principales razones por las cuales OSPF se implementa en gran medida en las redes empresariales actuales es el hecho de que es un estándar abierto; OSPF no es propietario

Path vector protocols: se enfocan en no solo intercambiar información sobre la existencia de redes de destino sino que también intercambiar la ruta sobre cómo llegar al este.

Point-to-point network: red que conecta un solo par de Router. Un paquete que se envía desde un extremo es recibido exactamente por un destinatario en el otro extremo del enlace.

RIP: es un IGP usado en las redes más pequeñas. Es un protocolo de enrutamiento de vector de distancia que utiliza el conteo de saltos como una métrica de enrutamiento. Hay tres versiones de RIP: RIPv1, RIPv2 y RIPng. Ruta RIPv1 y RIPv2 en redes IPv4

STP: (Spanning Tree Protocol), permitir los beneficios derivados de la redundancia, sin romper la red debido al Flooding

Unicast: tráfico donde se intercambia información solo entre un remitente y un receptor. Las direcciones de origen solo pueden ser una dirección de unidifusión.

VLAN: (virtual local-area network), es una extensión natural para poner lógica dentro de un Switch y permitirle elegir puertos para agrupaciones especiales.

VTP: (VLAN Trunking Protocol), es un protocolo de capa 2 que mantiene la consistencia de la configuración de VLAN al administrar las adiciones, eliminaciones y cambios de nombre de las VLAN en las redes. El Trunking es un mecanismo que se usa con mayor frecuencia para permitir que varias VLAN funcionen de manera independiente en varios conmutadores

RESUMEN

Este documento da solución a dos escenarios donde se implementan sencillas redes de enrutamiento y conmutación haciendo uso de dispositivos y protocolos propiedad de CISCO, con las cuales se pretende obtener la certificación CCNP En ellos se logra poner en práctica mediante la configuración como por ejemplo de protocolos IGP (EIGRP,OSPF) y EGP (BGP, IBGP, EBGP), creación de sistemas autónomos, relaciones de vecindad, ruteo estatico en el caso de enrutamiento y de creación de VLANS, modos de acceso, uso de protocolos de trunking (VTP y DTP), creación de SVIs en el caso de conmutación, además se utilizan comandos afines a los dos tipos de redes como los de configuración de interfaces como loopbacks, Ethernet y fastethernet, los de verificación como el comando show con muchas de sus variantes (IP route, vtp status, vlans, etc.) así como también el comando ping que nos permite la verificación de la conectividad entre dispositivos.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes.

ABSTRACT

This document provides a solution to two scenarios where simple Routing and Switching networks are implemented using devices and protocols owned by CISCO, with which the intention is to obtain the CCNP certification. In them it is possible to put into practice through the configuration such as protocols IGP (EIGRP, OSPF) and EGP (BGP, IBGP, EBGP), creation of autonomous systems, neighborhood relations, static routing in the case of Routing and VLANS creation, access modes, use of trunking protocols (VTP and DTP), creation of SVIs in the case of Switching, in addition, commands related to the two types of networks are used, such as those for configuring interfaces such as loopbacks, Ethernet and fastethernet, those for verification such as the show command with many of its variants (IP route, vtp status, vlans, etc.) as well as the ping command that allows us to verify connectivity between devices.

Keywords: CISCO, CCNP, Routing, Swicthing, Network.

INTRODUCCIÓN

Las redes de trabajo (networks) están en continuo crecimiento, volviéndose más complejas a medida que admiten más protocolos y más usuarios, por lo tanto en este trabajo se describen las mejores prácticas y técnicas para proteger los Routers y Switches dando ejemplos de configuración, verificación y técnicas de solución de problemas relacionados con el funcionamiento de la red

El trabajo consiste en el desarrollo de 2 escenarios donde se implementan redes de trabajo sencillas, en el primer escenario es una red basada en Router donde se abordan temáticas como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacencias en función del protocolo IP del Router ID e interfaces Loopback.

El segundo escenario se basa en la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configuran el enrutamiento IP respectivo, se implementan protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN.

Para esta práctica se utilizaron los simuladores GNS3 y PACKET TRACER, con los que se implementan, configuran y verifican las topologías propuestas en los escenarios, haciendo una descripción detallada del paso a paso necesario para su implementación.

DESARROLLO LOS ESCENARIOS

ESCENARIO 1

Figura 1. Topología del escenario 1

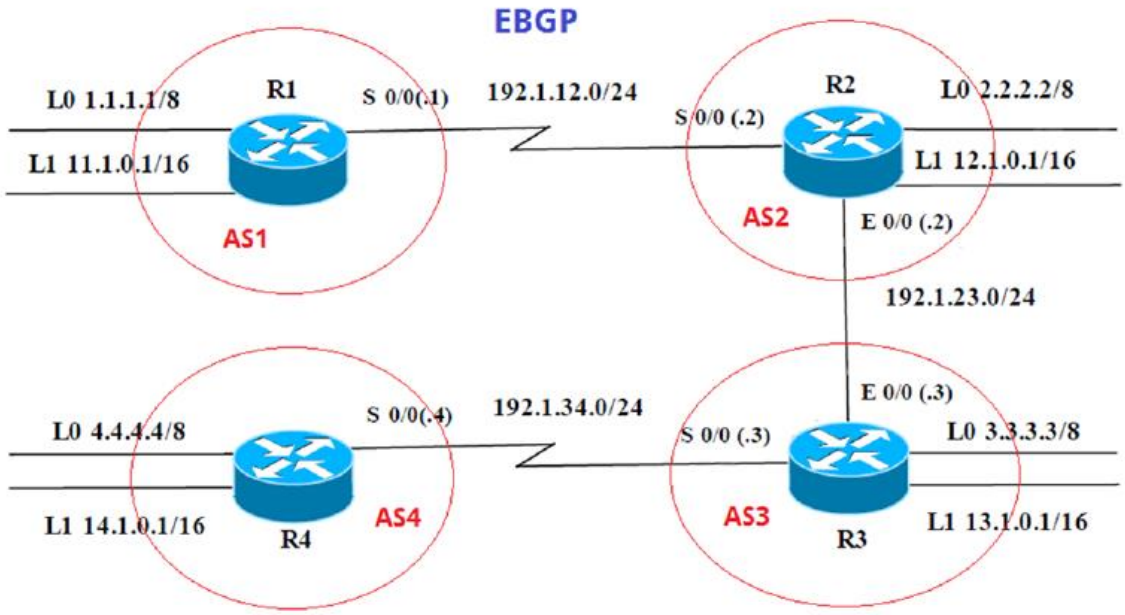


Tabla 1. Información para configuración de los Routers

R1

Interfaz	Dirección IP	Mascara
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	Mascara
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

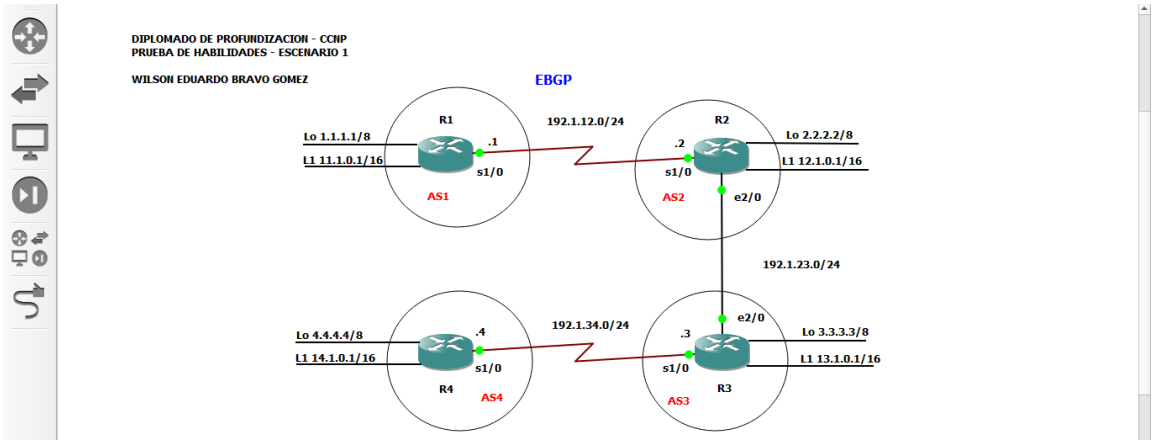
R3

Interfaz	Dirección IP	Mascara
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

	Interfaz	Dirección IP	Mascara
R4	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

Para este escenario se utilizara el simulador GNS3, con 4 routers C7200 y cables serial y Ethernet.

Figura 2. Topología del escenario 1 en el simulador GNS3



Paso 0: se aplican las configuraciones iniciales y se crean las interfaces (loopback, serial y Ethernet) correspondientes a cada router

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#interface Looopback 0
R1(config-if)#description  R1 to network link 1
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#interface Looopback 1
R1(config-if)#description  R1 to network link 2
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#interface Serial 1/0
R1(config-if)#description R1 --> R2
```

```
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exec-timeout 0 0
R2(config-line)#exit
R2(config)#interface Loopback 0
R2(config-if)#description  R2 to network link 1
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#interface Loopback 1
R2(config-if)#description  R2 to network link 2
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#interface Serial 1/0
R2(config-if)#description R2 --> R1
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Ethernet 2/0
R2(config-if)#description R2 --> R3
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#

Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#line con 0
R3(config-line)#logging synchronous
R3(config-line)#exec-timeout 0 0
R3(config-line)#exit
R3(config)#interface Loopback 0
R3(config-if)#description  R3 to network link 1
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#interface Loopback 1
R3(config-if)#description  R3 to network link 2
```

```
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#interface Serial 1/0
R3(config-if)#description R3 --> R4
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface Ethernet 2/0
R3(config-if)#description R3 --> R2
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#

Router>enable
Router#configure terminal
Router(config)#hostname R4
R4(config)#no ip domain-lookup
R4(config)#line con 0
R4(config-line)#logging synchronous
R4(config-line)#exec-timeout 0 0
R4(config-line)#exit
R4(config)#interface Loopback 0
R4(config-if)#description  R4 to network link 1
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#interface Loopback 1
R4(config-if)#description  R4 to network link 2
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#interface Serial 1/0
R4(config-if)#description R4 -> R3
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#
```

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. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

   Paso 1: Se configura BGP en los routers R1 y R2

```
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#exit
R1(config)#exit
R1#
```

```
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#exit
R2(config)#exit
R2#
```

Paso 2: Se realiza verificación de la configuración realizada

Figura 3. Verificación de configuración BGP en R1

```
R1#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

C    192.1.12.0/24 is directly connected, Serial1/0
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:01
B    192.1.23.0/24 [20/0] via 192.1.12.2, 00:00:01
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 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, 00:00:01
R1#
```

Figura 4. Verificación de configuración BGP en R2

```
R2#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

C    192.1.12.0/24 is directly connected, Serial1/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:09
C    2.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet2/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:00:09
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
R2#
```

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 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

Paso 3: Se configura BGP en el router 3

```
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit
R3(config)#exit
R3#
```

Paso 4: Se realiza verificación de la configuración realizada

Figura 5. Verificación de relación de vecindad entre R2 y R3

```
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

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:22
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:22
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:22
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:22
C    192.1.23.0/24 is directly connected, Ethernet2/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:22
C    192.1.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:22
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 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, 00:00:25
R3#
```

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 66.66.66.66. 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.***

   Paso 5: Se configura BGP en el router 4

   R4(config)#router bgp 4
   R4(config-router)#bgp router-id 66.66.66.66
   R4(config-router)#network 14.1.0.0 mask 255.255.0.0
   R4(config-router)#network 4.0.0.0 mask 255.0.0.0
   R4(config-router)#network 192.1.34.0 mask 255.255.255.0
   R4(config-router)#neighbor 192.1.34.3 remote-as 3
   R4(config-router)#exit
   R4(config)#exit
   R4#

   Paso 6: se crea ruta estática específica a R3

   R4#configure terminal
   R4(config)#ip route 3.3.3.3 255.0.0.0 serial 1/0

Paso 7: no se anuncia la loopback 0 en BGP

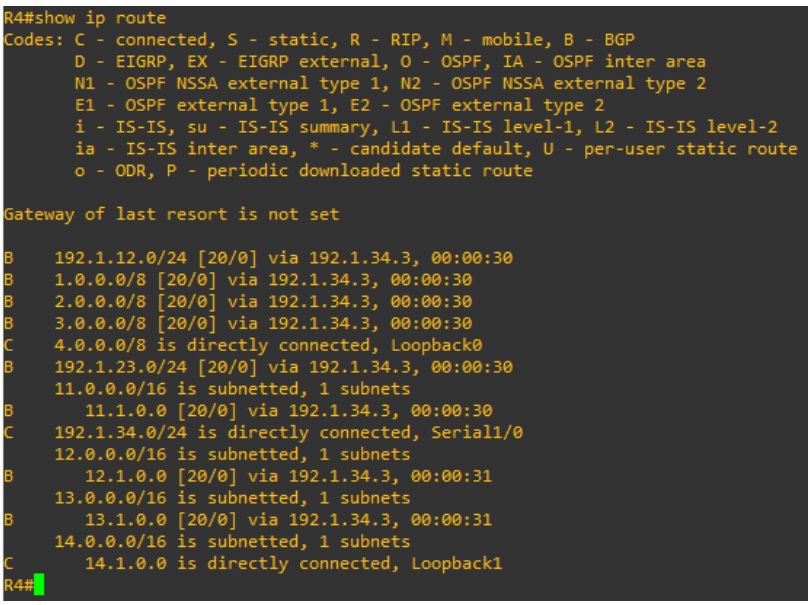
R4(config)#router bgp 4
R4(config-router)#no network 4.0.0.0 mask 255.0.0.0

Paso 8: se anuncia nuevamente la loopback 0 en BGP

R4(config)#router bgp 4
R4(config-router)#network 4.0.0.0 mask 255.0.0.0

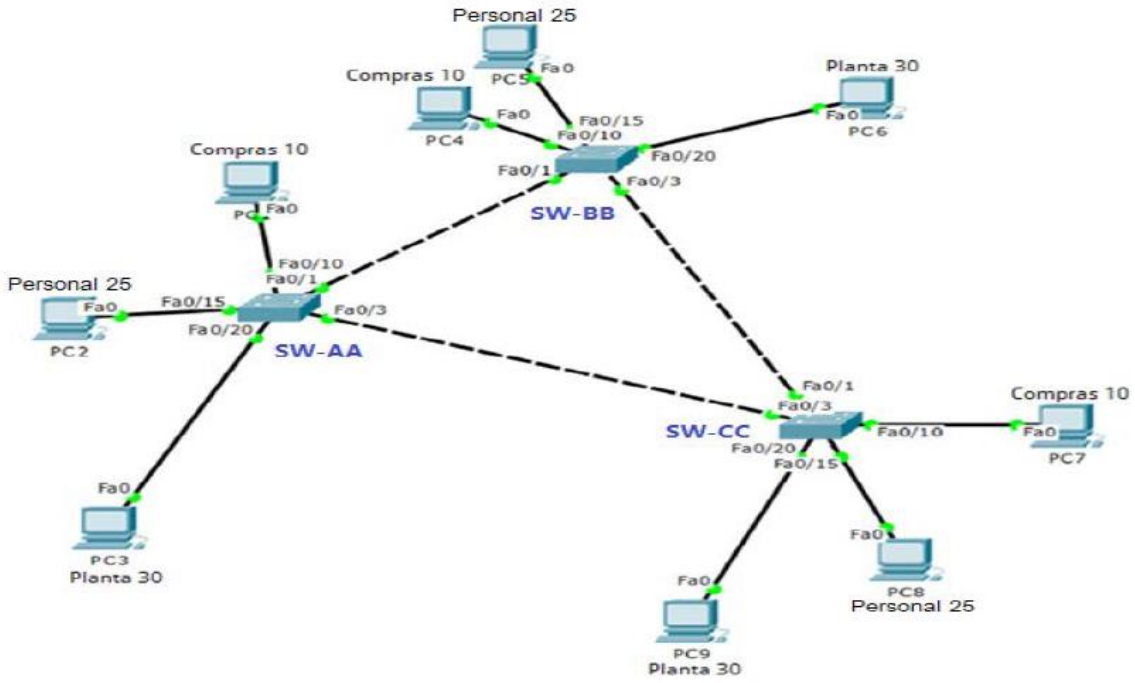
Paso 9: Se realiza verificación de las configuraciones realizadas

Figura 6. Verificación de relación de vecindad entre R3 y R4



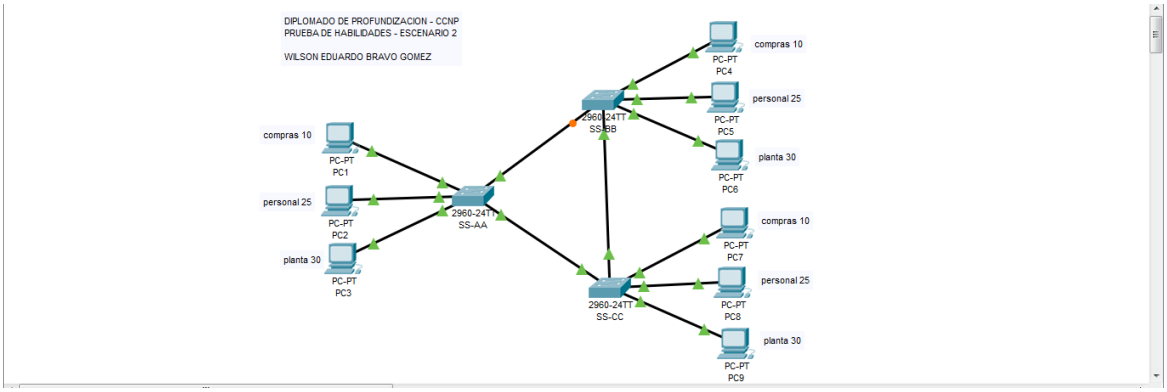
ESCENARIO 2

Figura 7. Topología del escenario 2



Para este escenario se utilizara el simulador PACKET TRACER, con 3 Switches 2960, 9 PCs y cables Fast-Ethernet.

Figura 8. Topología del escenario 2 en el simulador PACKET TRACER



Paso 0: se preparan los switches y se realiza configuración basica

```
Switch>enable
Switch#delete vlan.dat
Switch#delete multiple-fs
Switch#erase startup-config
Switch#reload
Switch#configure terminal
Switch(config)#hostname SW-AA
SW-AA(config)#line console 0
SW-AA(config-line)# exec-timeout 0 0
SW-AA(config-line)#logging synchronous
SW-AA(config-line)#end

Switch>enable
Switch#delete vlan.dat
Switch#delete multiple-fs
Switch#erase startup-config
Switch#reload
Switch#configure terminal
Switch(config)#hostname SW-BB
SW-BB(config)#line console 0
SW-BB(config-line)# exec-timeout 0 0
SW-BB(config-line)#logging synchronous
SW-BB(config-line)#end

Switch>enable
Switch#delete vlan.dat
Switch#delete multiple-fs
Switch#erase startup-config
Switch#reload
Switch#configure terminal
```

```
Switch(config)#hostname SW-CC
SW-CC(config)#line console 0
SW-CC(config-line)# exec-timeout 0 0
SW-CC(config-line)#logging synchronous
SW-CC(config-line)#end
```

A. Configurar VTP

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

Paso 1: se configura VTP en cada switch

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

```
SW-BB#configure terminal
SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco
SW-BB(config)#end
SW-BB#
```

SW-CC#configure terminal

SW-CC(config)#vtp mode client

SW-CC(config)#vtp domain CCNP

SW-CC(config)#vtp password cisco

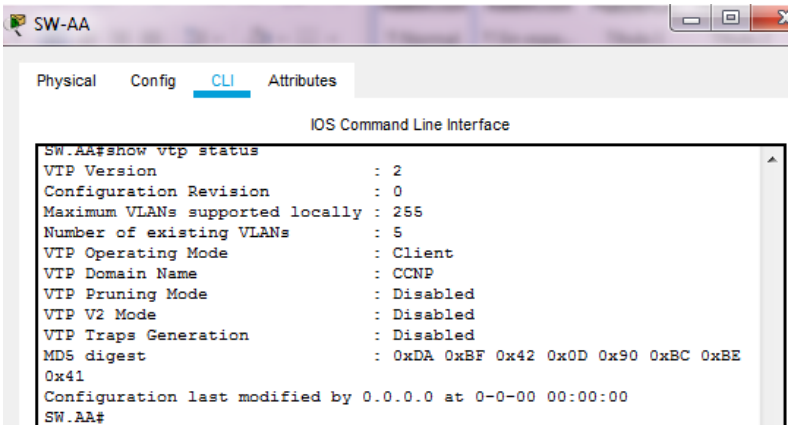
SW-CC(config)#end

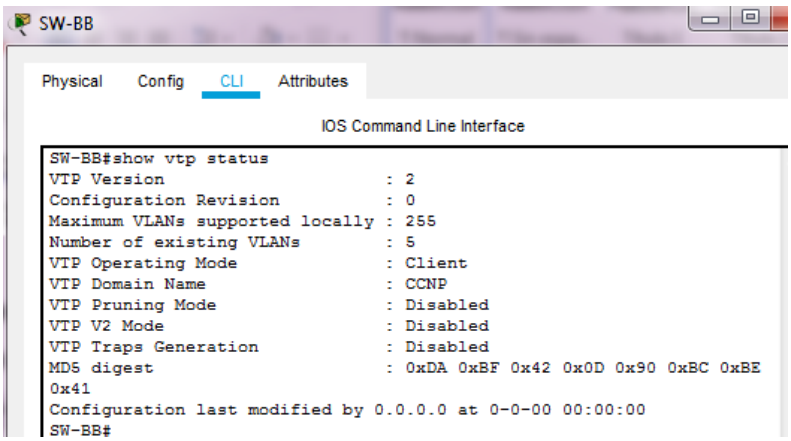
SW-CC#

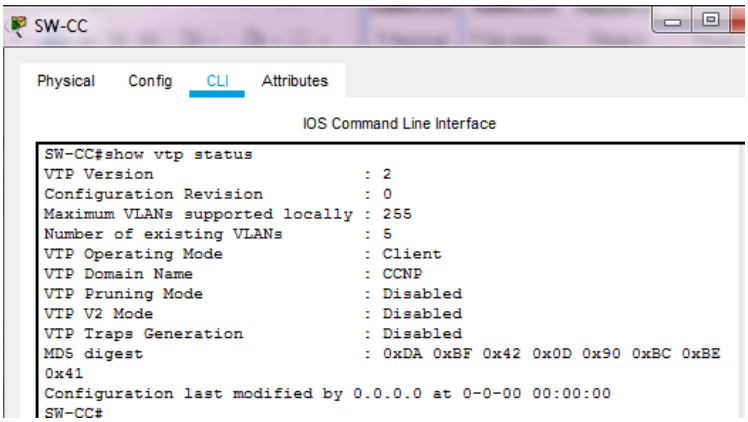
2. Verifique las configuraciones mediante el comando ***show vtp status***.

Paso 2: se verifican las configuraciones realizadas

Figura 9. Verificación de configuración de VTP







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***.

Paso 3: se configura DTP entre SW-AA y SW-BB

SW-BB#configure terminal

SW-BB(config)#interface fastEthernet 0/1

SW-BB(config-if)#switchport

SW-BB(config-if)#switchport mode dynamic desirable

SW-BB(config-if)#end

SW-BB#

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

Paso 4: se verifican las configuraciones realizadas

Figura 10. Verificación de configuración de DTP entre SW-AA y SW-BB

```
SW.AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

SW.AA#
```

```
SW-BB#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none

SW-BB#
```

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

Paso 5: se configura trunk estatico

SW-AA#configure terminal

SW-AA(config)#interface fastEthernet 0/1

SW-AA(config-if)#switchport mode trunk

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

Paso 6: se verifican las configuraciones realizadas

Figura 11. Verificación de enlace TRUNK estático entre SW-AA y SW-BB

```
SW.AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

SW.AA#
```

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

Paso 7: se configura trunk permanente

SW-BB#configure terminal

SW-BB(config)#interface fastEthernet 0/3

SW-BB(config-if)#switchport mode trunk

C. Agregar VLANs y asignar puertos.

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

Paso 8: se agregan VLANs a los switches

SS-AA#configure terminal

SS-AA(config)#vlan 10

SS-AA(config-vlan)# name Compras

SS-AA(config-vlan)#exit

SS-BB#configure terminal

SS-BB (config)#vlan 10

SS-BB (config-vlan)# name Compras

SS-BB (config)#vlan 25

SS-BB (config-vlan)# name Personal

SS-BB (config)#vlan 30

SS-BB (config-vlan)# name Planta

SS-BB (config)#vlan 99

SS-BB (config-vlan)# name Admon

SS-BB (config-vlan)#exit

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

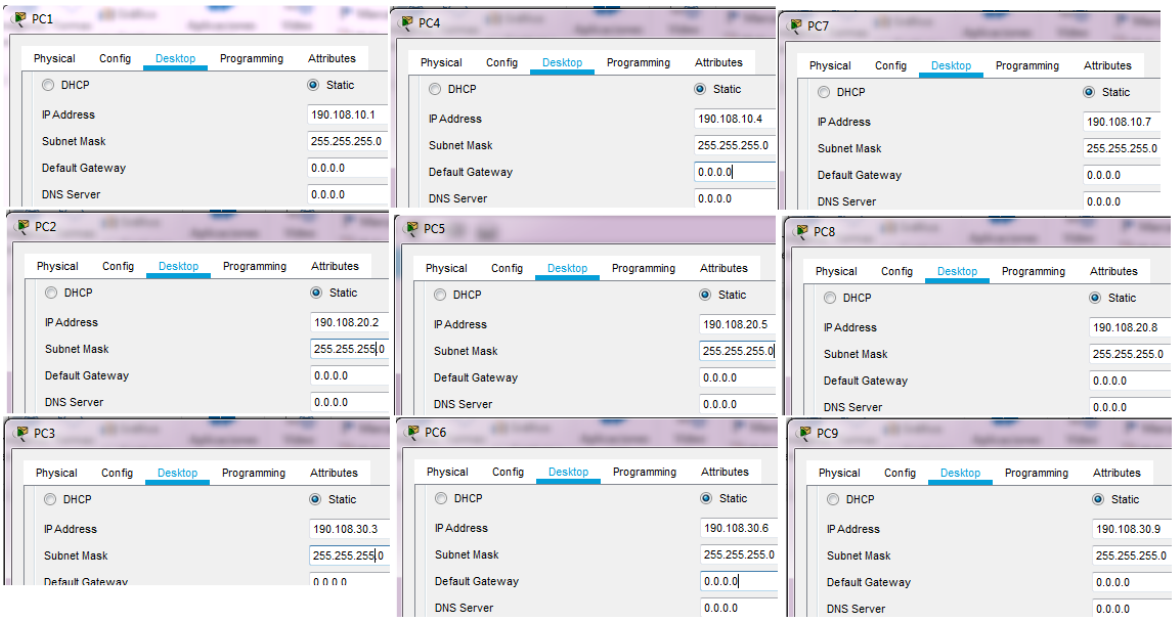
Tabla 2. Información para configuración de puertos y direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

Paso 9: se configuran IPs en los PCs

Figura 12. Configuración de direcciones IP en PCs



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

Paso 10: se configura puerto F0/10 en modo acceso en todos los switches

SW-AA(config)#interface fastethernet 0/10

SW-AA(config-if)#switchport

SW-AA(config-if)#switchport mode acess

SW-AA(config-if)#switchport acess vlan 10

SW-AA(config-if)#exit

SW-BB(config)#interface fastethernet 0/10

SW-BB(config-if)#switchport

SW-BB(config-if)#switchport mode acess

SW-BB(config-if)#switchport acess vlan 10

SW-BB(config-if)#exit

SW-CC(config)#interface fastethernet 0/10

SW-CC(config)#switchport

SW-CC(config)#switchport mode acess

SW-CC(config)#switchport acess vlan 10

SW-CC(config)#exit

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.

Paso 11: se configura puerto F0/15 y F0/20 en modo acceso en todos los switches

SW-AA(config)#interface fastethernet 0/15

SW-AA(config-if)#switchport

SW-AA(config-if)#switchport mode acess

SW-AA(config-if)#switchport acess vlan 25

SW-AA(config)#interface fastethernet 0/20
SW-AA(config-if)#switchport
SW-AA(config-if)#switchport mode acess
SW-AA(config-if)#switchport acess vlan 30
SW-AA(config-if)#exit

SW-BB(config)#interface fastethernet 0/15
SW-BB(config-if)#switchport
SW-BB(config-if)#switchport mode acess
SW-BB(config-if)#switchport acess vlan 25
SW-BB(config-if)#interface fastethernet 0/20
SW-BB(config-if)#switchport
SW-BB(config-if)#switchport mode acess
SW-BB(config-if)#switchport acess vlan 30
SW-BB(config-if)#exit

SW-CC(config)#interface fastethernet 0/15
SW-CC(config-if)#switchport
SW-CC(config-if)#switchport mode acess
SW-CC(config-if)#switchport acess vlan 25
SW-CC(config-if)#interface fastethernet 0/20
SW-CC(config-if)#switchport
SW-CC(config-if)#switchport mode acess
SW-CC(config-if)#switchport acess vlan 30
SW-CC(config-if)#exit

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.

Tabla 3. Asignación de direcciones IP al SVI

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Paso 12: se asigna dirección IP al SVI

SW-AA#configure terminal

SW-AA(config)#interface vlan 99

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

SW-BB#configure terminal

SW-BB(config)#interface vlan 99

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0

SW-CC#configure terminal

SW-CC(config-if)#interface vlan 99

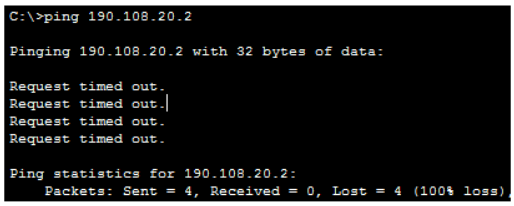
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0

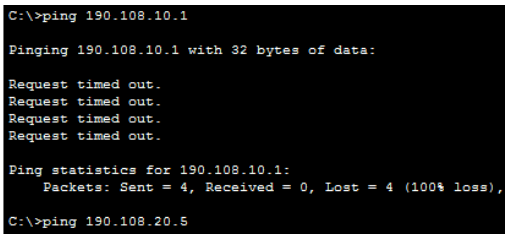
E. Verificar la conectividad Extremo a Extremo

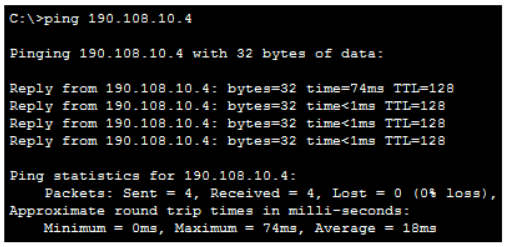
15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

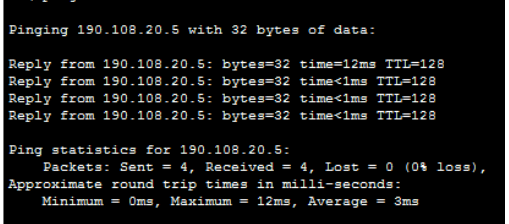
Paso 13: se verifica conectividad entre PCs

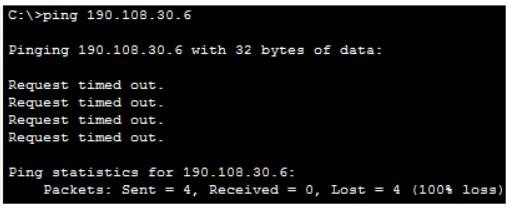
Figura 13. Verificación de conectividad entre PCs

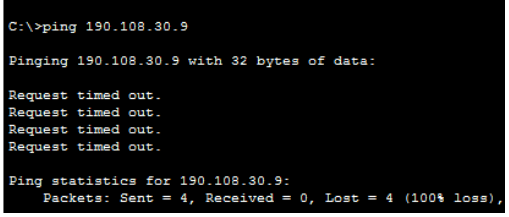


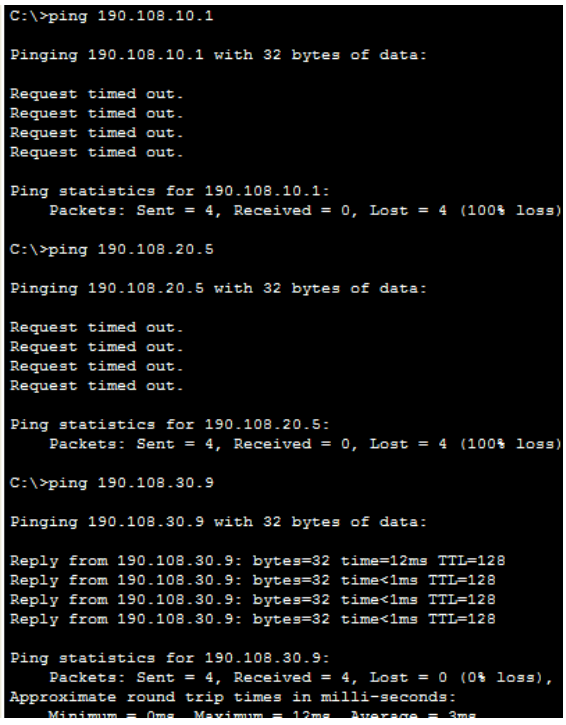












Solo tuvieron éxito los ping realizados entre PCs con la misma VLAN, ya que asi se realizo la configuracion

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

Paso 14: se verifica conectividad entre switches

Figura 14. Verificación de conectividad entre switches

```
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 0 percent (0/5)

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 0 percent (0/5)
```

```
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 0 percent (0/5)

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 0 percent (0/5)
```

```
SW-CC#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 0 percent (0/5)

SW-CC#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 0 percent (0/5)
```

CONCLUSIONES

Tras realizar las configuraciones de los escenarios se logró poner en práctica los conocimientos adquiridos a lo largo del curso referente a los temas de protocolos tanto de routing como de switching.

Al realizar las verificaciones como las de configuración y conectividad se puede solucionar problemas identificando errores, omisiones, o malos procedimientos mediante el uso e interpretación de las tablas y reportes que nos brindan dichos recursos.

Se debe tener en cuenta la importancia de la sintaxis a la hora de configurar los comandos en los simuladores para asi minimizar problemas de funcionamiento y fallos de conectividad.

BIBLIOGRÁFIA

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-NT1IlnWR0hoMxgBNv1CJ

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