DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHONATAN REYNALDO AMOROCHO INFANTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHONATAN REYNALDO AMOROCHO INFANTE

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

Presentado a:

MSc. Gerardo Granados Acuña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bucaramanga 10 de septiembre del 2020

AGRADECIMIENTOS

Quiero agradecer a Dios y a mis amados padres por todo su sacrificio y esfuerzo apoyándome para poder salir adelante con mis estudios e impulsarme con mis sueños.

A mi esposa por estar siempre pendiente, por ser mi coequipera y aliada, apoyándome para sacar mis estudios adelante, e impulsándome todos los días para ser un gran profesional y ser humano.

A mis hijos por inspirarme a ser un gran padre y ejemplo de un gran profesional y referente a seguir.

Agradecerle a la Universidad Nacional Abierta y a Distancia, a sus docentes por haberme guiado y enseñado todos sus conocimientos de forma oportuna a lo largo de mi formación como profesional y en este diplomado.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

BGP: Permite crear enrutamiento entre dominios sin bucles entre sistemas autónomos (AS). Un AS es un conjunto de enrutadores bajo una única administración técnica. Los enrutadores de un AS pueden utilizar varios protocolos de puerta de enlace interior (IGP) para intercambiar información de enrutamiento dentro del AS. Los enrutadores pueden usar un protocolo de puerta de enlace exterior para enrutar paquetes fuera del AS.

DTP: (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet. Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE.

ENRUTAMIENTO: Cuando hablamos de compartir información y de realizar la comunicación entre distintos sistemas tecnológicos, el enrutamiento dinámico es uno de los primeros conceptos que nos vienen a la cabeza. Bajo este proceso una serie de máquinas que se encuentren dentro de una misma red tendrán capacidad para llevar a cabo una comunicación entre ellas de forma permanente.

VLAN: Se conoce como Virtual LAN o VLAN a una división de carácter lógico del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. Se trata, por tanto, de una agrupación de un conjunto de dispositivos que pueden mantener comunicación entre sí.

VTP: Son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

RESUMEN

En el presente informe se desarrolla el procedimiento necesario de configuración y verificación en temas como: configuración BGP para el intercambio de encaminamiento de información, VTP, creación de VLAN, asignación de puertos a las VLAN, configuración de direcciones IP, protocolo de enrutamiento DTP, entre otros vistos a lo largo del diplomado de cisco CCNP por medio del software cisco Packet Tracer.

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

ABSTRACT

This report develops the necessary configuration and verification procedure in topics such as: BGP configuration for information routing exchange, VTP, VLAN creation, port assignment to VLANs, IP address configuration, DTP routing protocol, among others seen throughout the cisco CCNP diploma course by means of the cisco Packet Tracer software.

Keywords: CISCO, CCNP, Switching, Routing, Networking, Electronics

INTRODUCCIÓN

Este informe desarrolla la evaluación final del diplomado de profundización en cisco CCNP, se desarrollan dos escenarios especificando los comandos utilizados en el procedimiento de configuración y verificación de la conexión por puertos ethernet o seriales de los distintos dispositivos como router, switch y PC’s por medio del programa de Cisco Packet Tracer.

Inicialmente, para el desarrollo de cada uno de los ejercicios, se hace la topología de la red y las configuraciones básicas de los dispositivos. En el primer escenario, se configura una relación de vecinos BGP entre los router, y por último se verifican de los enrutamientos IP realizados mediante el comando show IP Route.

En el segundo escenario, se inicia realizando la configuración VTP para las actualizaciones de VLAN. El switch SW-BB se configura como el servidor y los switch SW-AA y SW-CC se configuran como clientes con su respectivo dominio y contraseña, a su vez verificando estas configuraciones mediante el comando show vtp status. Seguidamente se configura el protocolo troncal DTP para luego agregar las VLANs, asignar puertos y las direcciones IP en los switch; y por último se verifica este procedimiento de extremo a extremo.

.

DESARROLLO

1. ESCENARIO 1

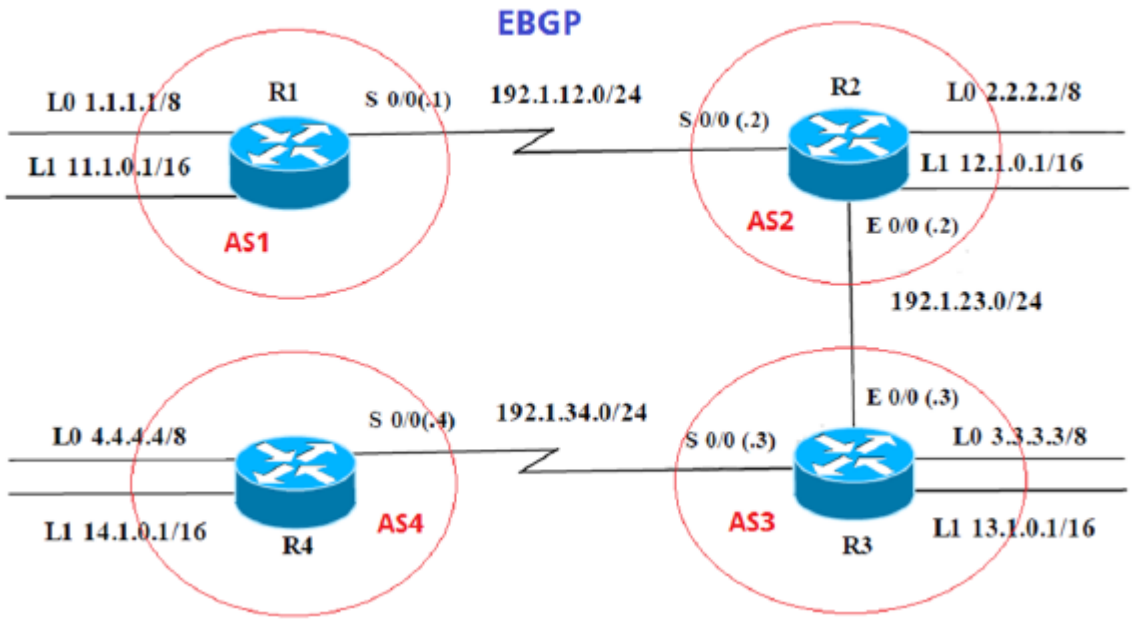

Figura 1 Escenario 1

Información para configuración de los Router.

- **R1**

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
Se0/3/0	192.1.12.1	255.255.255.0

Tabla 1 Direccionamiento del router R1

- **R2**

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
Se0/3/0	192.1.12.2	255.255.255.0
Fa0/2/0	192.1.23.2	255.255.255.0

Tabla 2 Direccionamiento del router R2

- **R3**

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
Fa0/2/0	192.1.23.3	255.255.255.0
Se0/3/0	192.1.34.3	255.255.255.0

Tabla 3 Direccionamiento del router R3

- **R4**

INTERFAZ	DIRECCION IP	MASCARA
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
Se0/3/0	192.1.34.4	255.255.255.0

Tabla 4 Direccionamiento del router R4

1.1 PARTE 1: ARMAR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS.

Paso 1: Realizar la topología de la red.

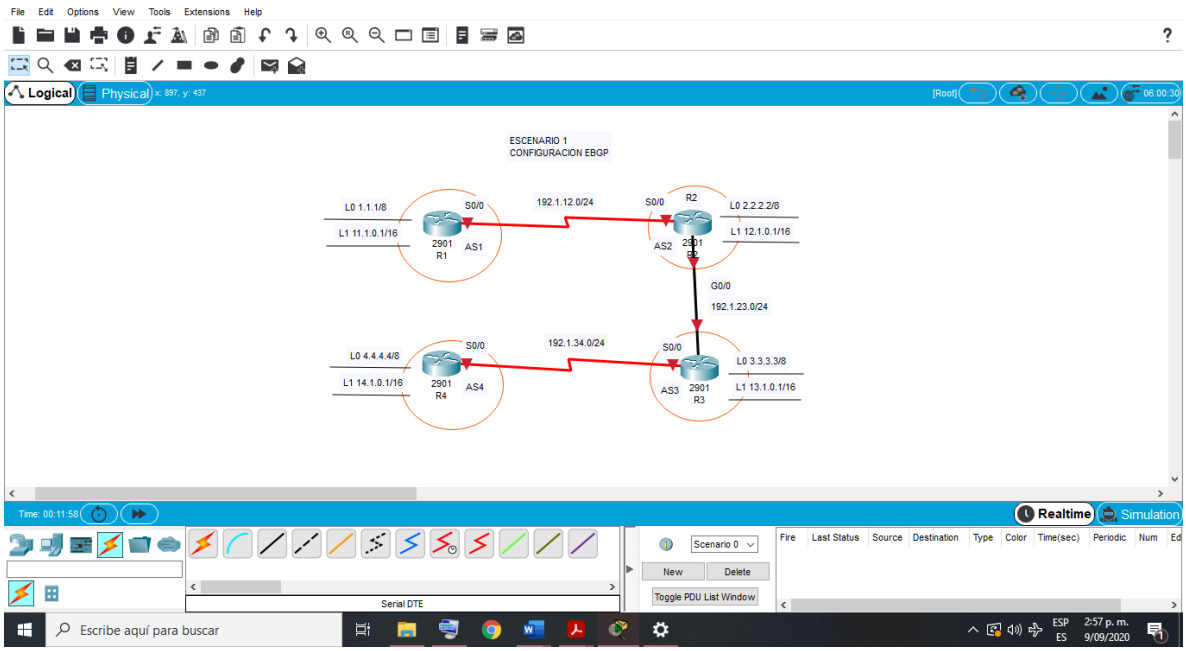

Figura 2 Simulación del escenario 1 en cisco packet tracer

Realizar la topología de la red tal como se muestra en la figura 1 en cisco packet tracer, se agregan a la ventana principal del programa 4 router de la referencia 2901 unidos por cable serial.

Por precaución hay que borrar cualquier configuración anterior que tengan los dispositivos.

Paso 2: Eliminar las configuraciones e Inicializar y volver a cargar los router.

Eliminar las configuraciones e Inicializar y volver a cargar los router, se realiza inicialmente con el comando erase startup-config, por medio de este eliminamos los archivos, seguidamente con el comando reload se volverán a cargar los dispositivos.

A continuación, se muestra cómo se escriben los comandos en la ventana CLI del router.

Route>enable	Ingreso al modo privilegiado
Router#erase startup-config	Eliminar el archivo startup-config de todos los routers
Router#reload	Volver a cargar todos los routers

1.2 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS.

Paso 1: Realizar las configuraciones basicas de los routers.

Para realizar este paso, vamos a la pestaña CLI de cada router. En esta ventana observamos primero la línea router>, esta línea significa que el router se encuentra en modo normal y en este modo no se puede realizar ninguna configuración, por lo que escribimos enable para cambiar de modo y así poder empezar con las configuraciones.

Utilizando los siguientes comandos que se muestran a continuación se realiza este paso en cada router.

Paso 2: Configurar el router 1

Router>enable	Ingreso al modo privilegiado
Router#configure terminal	Ingreso a las configuraciones
Router(config)#hostname R1	Colocar nombre al router
R1(config)#no ip domain-lookup	Desactivar la búsqueda DNS
R1(config)n#service password-encryption	Cifrar las contraseñas de texto no cifrado
R1(config)#enable secret cisco	Contraseña de exec privilegiado cifrada
R1(config)#banner motd $Se prohibe el acceso no autorizado$	Mensaje MOTD
R1(config)#line console 0	Acceso a la consola
R1(config-line)#password cisco	Contraseña de acceso a la consola
R1(config-line)#login	Aceptar la contraseña
R1(config-line)#line vty 0 4	Acceso a vty
R1(config-line)#password cisco	Contraseña de acceso vty
R1(config-line)#login	Aceptar la contraseña
R1(config)##exit.	Salir
R1(config)##do write	Guardar

Paso 3: Configurar el router 2

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#service password-encryption
R2(config)#enable secret cisco
R2(config)#banner motd $Se prohibe el acceso no autorizado$
R2(config)#line console 0
R2(config)#password cisco
R2(config)#login
R2(config)#line vty 0 4
R2(config)#password cisco
R2(config)#login
R2(config)##exit.
R2(config)##do write

Paso 4: Configurar el router 3

```
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#service password-encryption
R3(config)#enable secret cisco
R3(config)#banner motd $Se prohibe el acceso no autorizado$
R3(config)#line console 0
R3(config)#password cisco
R3(config)#login
R3(config)#line vty 0 4
R3(config)#password cisco
R3(config)#login
R3(config)##exit.
R3(config)##do write
```

Paso 5: Configurar el router 4

```
Router>enable
Router#configure terminal
Router(config)#hostname R4
R4(config)#no ip domain-lookup
R4(config)#service password-encryption
R4(config)#enable secret cisco
R4(config)#banner motd $Se prohibe el acceso no autorizado$
R4(config)#line console 0
R4(config)#password cisco
R4(config)#login
R4(config)#line vty 0 4
R4(config)#password cisco
R4(config)#login
R4(config)##exit.
R4(config)##do write
```

1.3 PARTE 3: CONFIGURACION LAS DIRECCIONES IP DE LAS INTERFACES

Para realizar las configuraciones EBGP, primero se deben asignar las direcciones IP y las direcciones de loopback a cada Router usando los siguientes comandos.

Paso 1: Asignar las direcciones a R1

R1(config)#interface Se0/3/0	Ingresar a la interfaz serial
R1(config)#ip address 192.1.12.1 255.255.255.0	Asignarle una direccion IP
R1(config)#no shutdown	Encender la interfaz
R1(config)#exit	Salir
R1(config)#interface loopback 0	Interfaz loopback 0 (servidor web simulado)
R1(config)#ip address 1.1.1.1 255.0.0.0	Asignarle una direccion IP
R1(config)#exit	Salir
R1(config)#interface loopback 1	Interfaz loopback 1 (servidor web simulado)
R1(config)#ip address 11.1.0.1 255.255.0.0	Asignarle una direccion IP
R1(config)#exit	Salir

Paso 2: Asignar las direcciones a R2

```
R2(config)#interface Se0/3/0
R2(config)#ip address 192.1.12.2 255.255.255.0
R2(config)#no shutdown
R2(config)#exit
R2(config)#interface gi0/0
R2(config)#ip address 192.1.23.2 255.255.255.0
R2(config)#no shutdown
R2(config)#exit
R2(config)#interface loopback 0
R2(config)#ip address 2.2.2.2 255.0.0.0
R2(config)#exit
R2(config)#interface loopback 1
R2(config)#ip address 12.1.0.1 255.255.0.0
R2(config)#exit
```

Paso 3: Asignar las direcciones a R3

```
R3(config)#interface Se0/3/0
R3(config)#ip address 192.1.34.3 255.255.255.0
R3(config)#no shutdown
R3(config)#exit
R3(config)#interface gi0/0
R3(config)#ip address 192.1.23.3 255.255.255.0
R3(config)#no shutdown
R3(config)#exit
R3(config)#interface loopback 0
R3(config)#ip address 3.3.3.3 255.0.0.0
R3(config)#exit
R3(config)#interface loopback 1
R3(config)#ip address 13.1.0.1 255.255.0.0
R3(config)#exit
```

Paso 4: Asignar las direcciones a R4

```
R4(config)#interface Se0/3/0
R4(config)#ip address 192.1.34.4 255.255.255.0
R4(config)#no shutdown
R4(config)#exit
R4(config)#interface loopback 0
R4(config)#ip address 4.4.4.4 255.0.0.0
R4(config)#exit
R4(config)#interface loopback 1
R4(config)#ip address 14.1.0.1 255.255.0.0
R4(config)#exit
```

1.4 PARTE 4: CONFIGURE UNA RELACIÓN DE VECINO BGP ENTRE R1 Y R2

R1 debe estar en AS1 y R2 debe estar en AS2, luego informar las direcciones de Loopback en BGP y por último recopilar los ID para los Router BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2.

Paso 1: Configurar a R1

R1(config)#router bgp 1	Ingresar a la configuración bgp en el router
R1(config-router)#no synchronization	Inhabilitar la sincronización
R1(config-router)#bgp router-id 22.22.22.22	Anunciar las direcciones de Loopback en BGP
R1(config-router)#neighbor 192.1.12.2 remote-as 2	Codificar los ID para los Router BGP
R1(config-router)#network 1.0.0.0 mask 255.0.0.0	Anunciar las redes conectadas directamente
R1(config-router)#network 11.1.0.0 mask 255.255.0.0	Anunciar las direcciones de Loopback en BGP

Paso 2: Configurar a R2

R2(config)#router bgp 2

R2(config-router)#no synchronization

R2(config-router)#bgp router-id 33.33.33.33

R2(config-router)#neighbor 192.1.12.1 remote-as 1

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

1.5 PARTE 5: VERIFICAR LOS ROUTER R1 Y R2

En esta parte vamos verificar rutas configuradas y las direcciones IP con el commando show ip route.

Paso 1: Verificar en R1

R1# show ip route	Comando que muestra las rutas IP

Paso 2: Verificar en R2

R2# show ip route	Comando que muestra las rutas IP

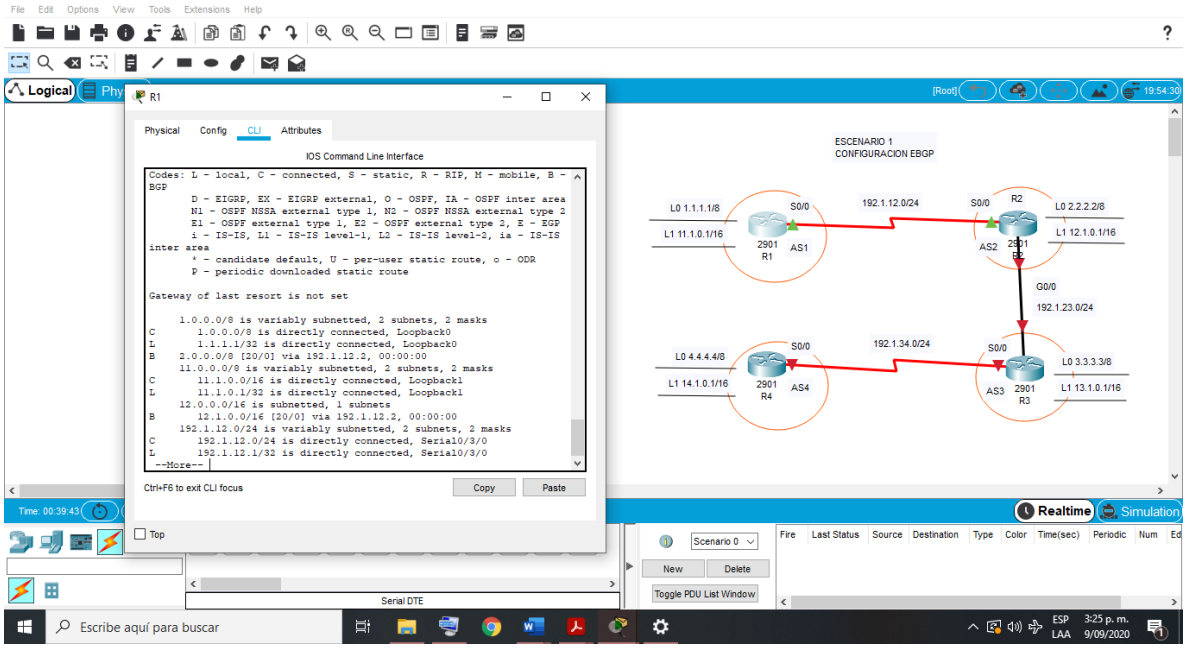

Figura 3 Verificación de la configuración BGP en R1

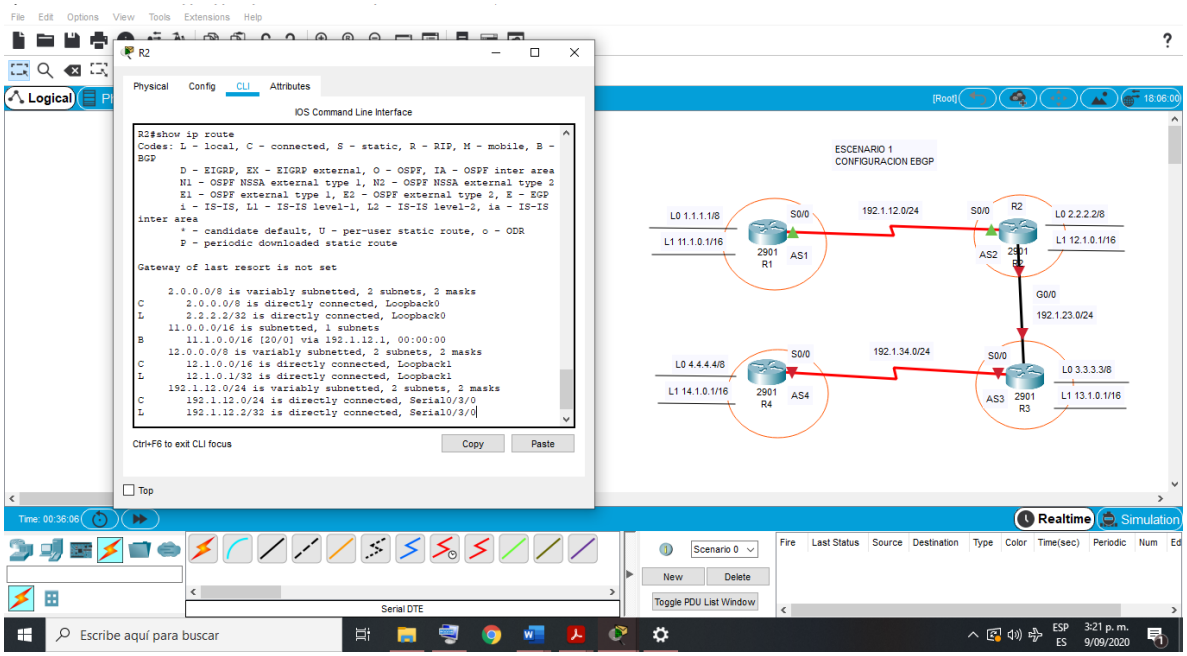

Figura 4 Verificación de la configuración BGP en R2

1.6 PARTE 6: CONFIGURE UNA RELACIÓN DE VECINO BGP ENTRE R2 Y R3

R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. luego informar las direcciones de Loopback de R3 en BGP. Por ultimo recopilar el ID del router R3 como 44.44.44.44.

Paso 1: Configurar a R2

```
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.2 remote-as 3
```

Paso 2: Configurar a R3

```
R3(config)#router bgp 3
R3(config-router)#no synchronization
R3(config-router)#bgp router-id 44.44.44.44
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)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
```

1.7 PARTE 5: VERIFICAR LOS ROUTER R2 Y R3

En esta parte vamos verificar rutas configuradas y las direcciones IP con el commando show ip route.

Paso 1: Verficar en R2

R2# show ip route

Paso 2: Verficar en R3

R3# show ip route

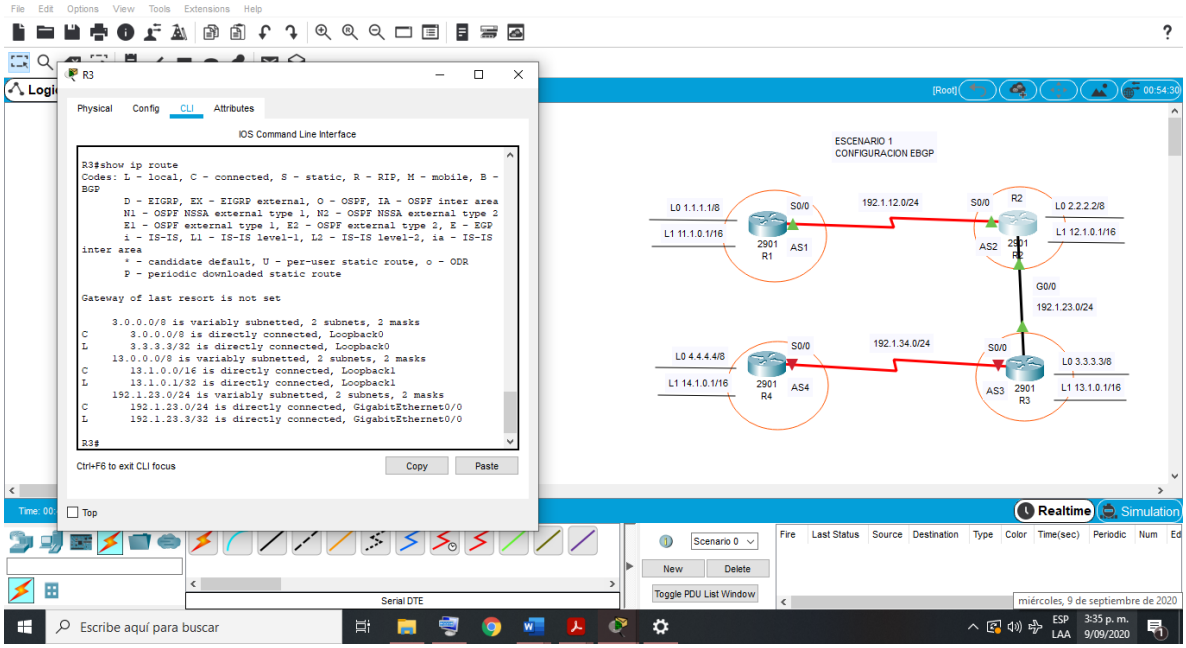

Figura 5 Verificación de la configuración BGP en R2

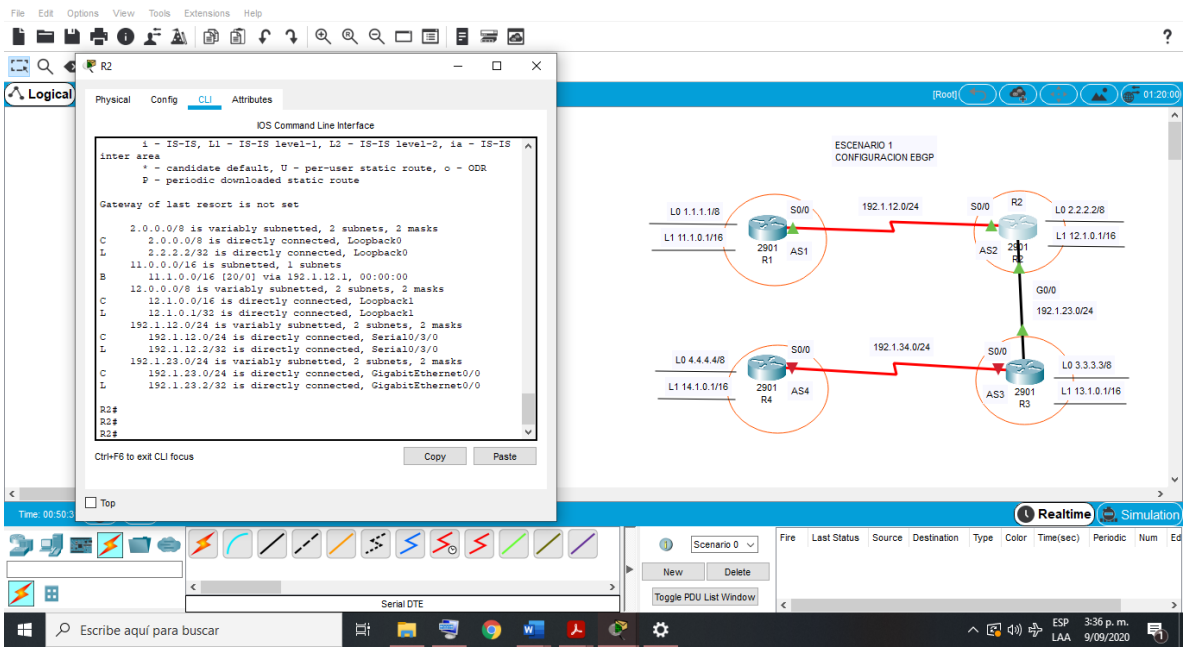

Figura 6 Verificación de la configuración BGP en R3

1.8 PARTE 7: CONFIGURE UNA RELACIÓN DE VECINO BGP ENTRE R3 Y R4

R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Luego informarlas direcciones de Loopback de R4 en BGP. el ID del router R4 como 66.66.66.66. Formar las relaciones de vecino con base en las direcciones de Loopback 0. Formar rutas estáticas para alcanzar la Loopback 0 del otro router. No informe la Loopback 0 en BGP. Informe la red Loopback de R4 en BGP.

Paso 1: Configurar a R3

```
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.2 remote-as 4
```

Paso 2: Configurar a R4

```
R4(config)#router bgp 4
R4(config-router)#no synchronization
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
```

1.9 PARTE 5: VERIFICAR LOS ROUTER R3 Y R4

En esta parte vamos verificar rutas configuradas y las direcciones IP con el commando show ip route.

Paso 1: Verficar en R3

R3# show ip route

Paso 2: Verficar en R4

R4# show ip route

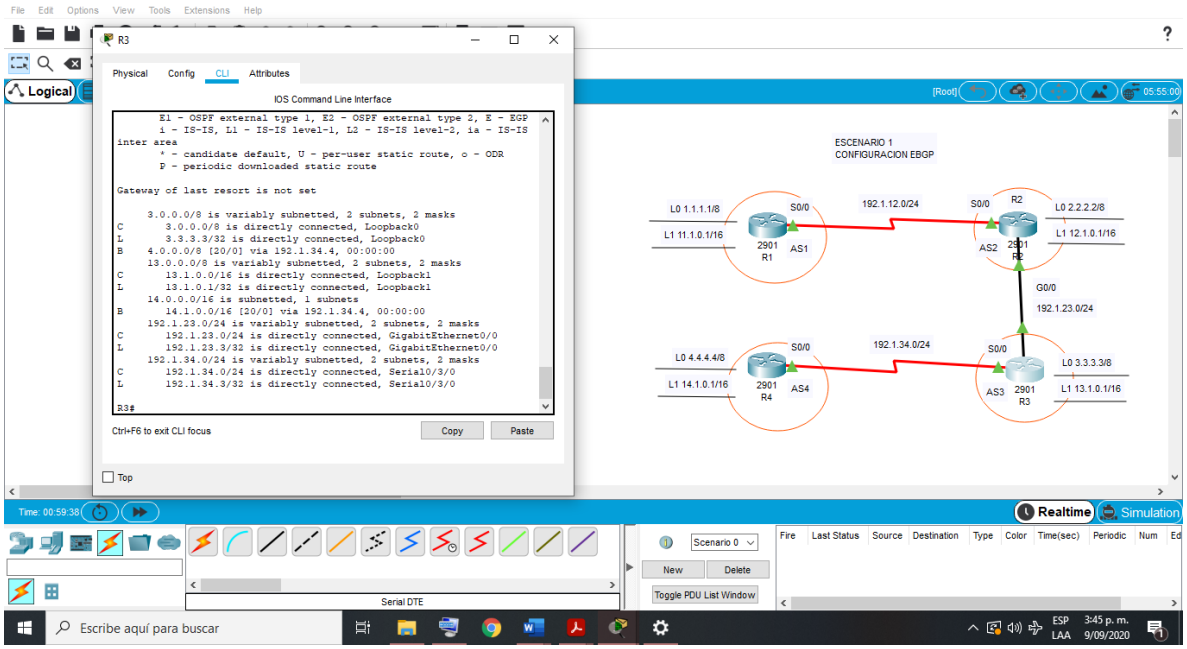

Figura 7 Verificación de la configuración BGP en R3

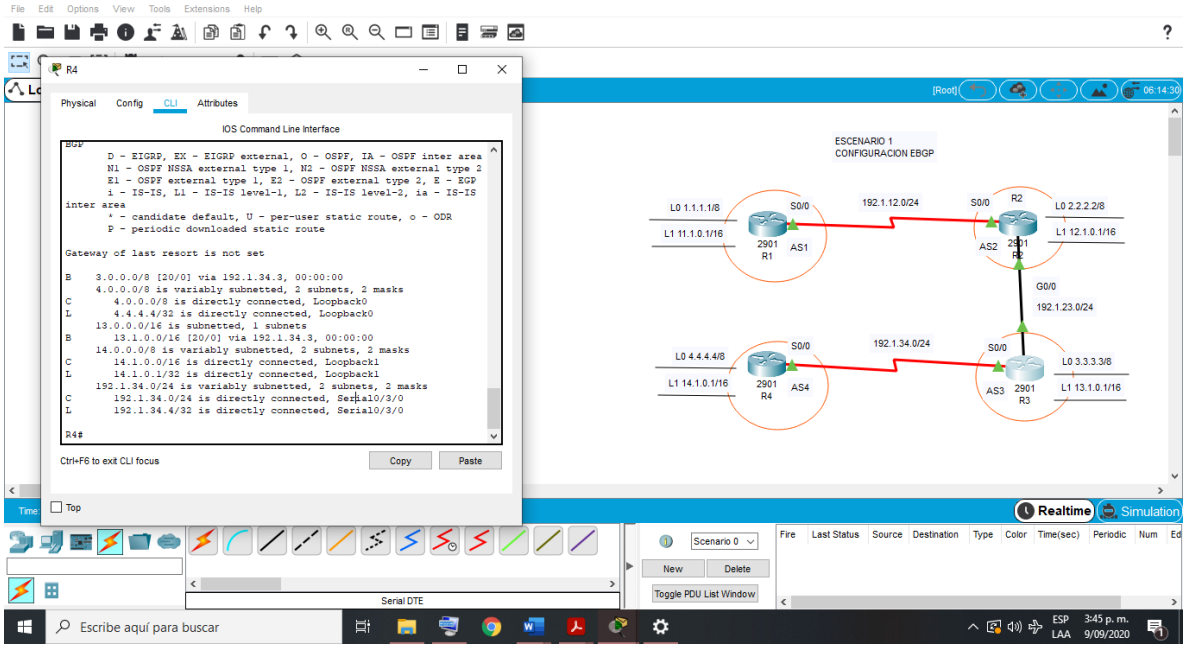

Figura 8 Verificación de la configuración BGP en R4

2. ESCENARIO 2

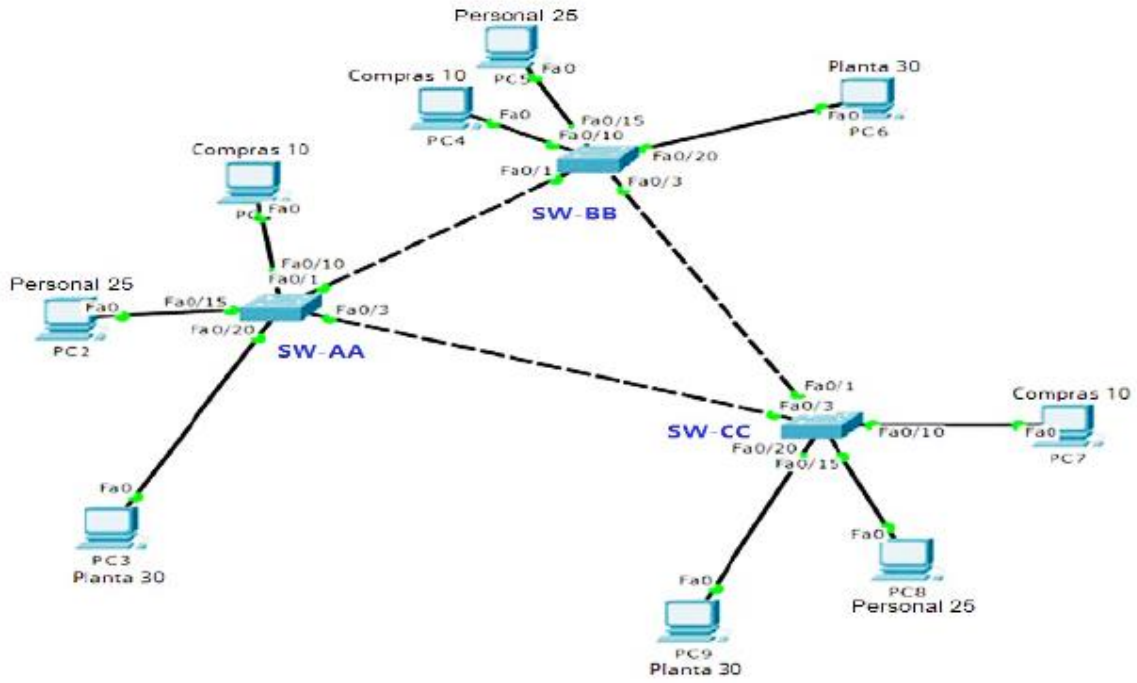

Figura 9 Escenario 2

2.1 PARTE 1: ARMAR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE LOS DISPOSITIVOS.

Paso 1: Realizar la topología de la red.

Realizar la topología de la red tal como se muestra en la figura 2 en cisco packet tracer, agregar a el panel principal del programa tres switch 1941, asignándole a cada uno su nombre correspondiente SW-AA, SW-BB y SW-CC, después colocar tres PC's por cada switch. Por precaución hay que borrar cualquier configuración anterior que tengan los dispositivos.

Paso 2: Eliminar las configuraciones e Inicializar y volver a cargar los router.

Eliminar las configuraciones e Inicializar y volver a cargar los router, se realiza inicialmente con el comando erase startup-config, por medio de este eliminamos los archivos, seguidamente con el comando reload se volverán a cargar los dispositivos.

A continuación, se muestra cómo se escriben los comandos en la ventana CLI del router.

Route>enable	Ingreso al modo privilegiado
Router#erase startup-config	Eliminar el archivo startup-config de todos los routers
Router#reload	Volver a cargar todos los routers

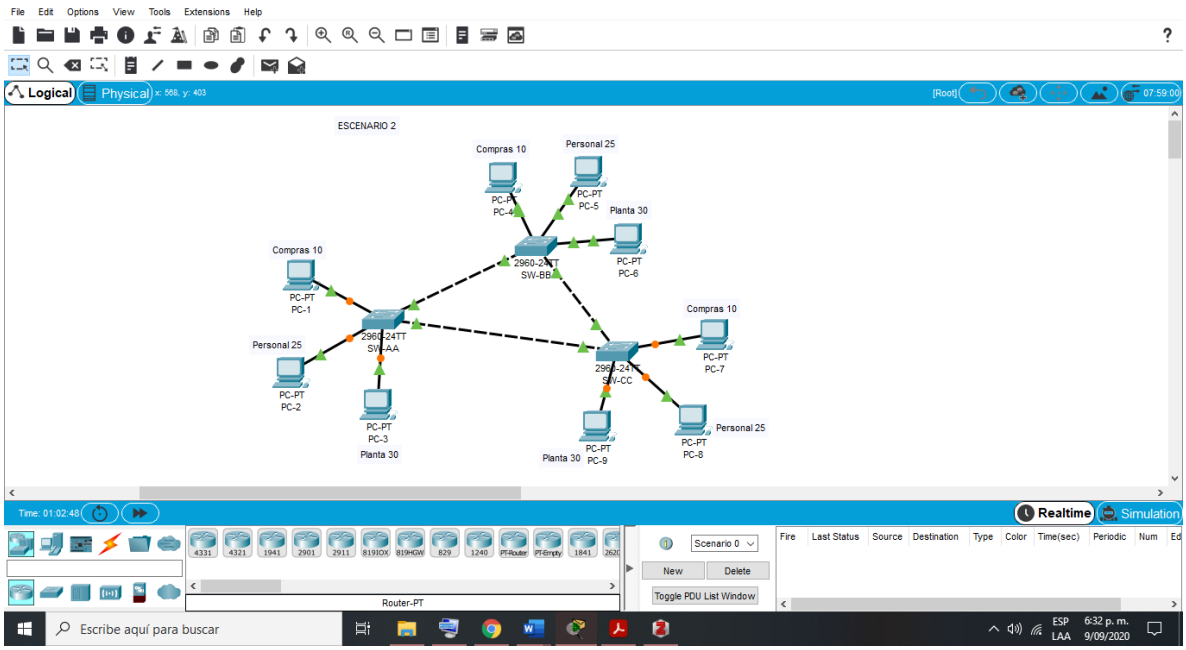

Figura 10 Simulación del escenario 2 en cisco packet tracer

2.2 PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS.

Para realizar este paso, vamos a la pestaña CLI de cada switch y utilizamos los siguientes comandos que se muestran a continuación se realiza este paso en cada router.

Paso 1: Configurar el switch 1

Switch>enable	Ingreso al modo privilegiado
Switch#configure terminal	Ingreso a las configuraciones
Switch(config)#hostname SW-AA	Colocar nombre al router
SW-AA(config)#no ip domain-lookup	Desactivar la búsqueda DNS
SW-AA(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
SW-AA(config)#enable secret cisco	Contraseña de exec privilegiado cifrada
SW-AA(config)#line console 0	Acceso a la consola
nSW-AA(config-line)#password cisco	Contraseña de acceso a la consola
SW-AA(config-line)#login	Aceptar la contraseña
SW-AA(config-line)#line vty 0 15	Acceso a vty
SW-AA(config-line)#password cisco	Contraseña de acceso vty
SW-AA(config-line)#login	Aceptar la contraseña
SW-AA(config)##exit.	Salir
SW-AA(config)##do write	Guardar

Paso 2: Configurar el switch 2

Switch > enable

Switch #configure terminal

Switch**(**config)#hostname SW-BB

SW-BB(config)#enable secret cisco.

SW-BB(config)#line console 0

SW-BB(config-line)#password cisco

SW-BB(config-line)#login

SW-BB(config-line)#line vty 0 15

SW-BB(config-line)#password cisco

SW-BB(config-line)#login

SW-BB(config)#exit.

SW-BB(config)#service password-encryption

SW-BB(config)#do write

Paso 3: Configurar el switch 3

```
Switch > enable
Switch #configure terminal
Switch(config)#hostname SW-CC
SW-CC(config)#enable secret cisco.
SW-CC(config)#line console 0
SW-CC(config-line)#password cisco
SW-CC(config-line)#login
SW-CC(config-line)#line vty 0 15
SW-CC(config-line)#password cisco
SW-CC(config-line)#login
SW-CC(config)#exit.
SW-CC(config)#service password-encryption
SW-CC(config)#do write
```

2.3 PARTE 3: CONFIGURACION VTP

Paso 1: Configurar el switch SW-BB como servidor VTP

SW-BB(config)#vtp mode server.	Configurar el switch como servidor
SW-BB(config)#vtp domain CCNA	Nombre del dominio VTP
SW-BB(config)# vtp password cisco	Contraseña de dominio VTP
SW-BB(config)# exit	Salir

Paso 2: Verificar a SW-BB

En esta parte vamos verificar rutas configuradas y las direcciones IP con el commando show vtp status.

SW-BB(config)# show vtp status

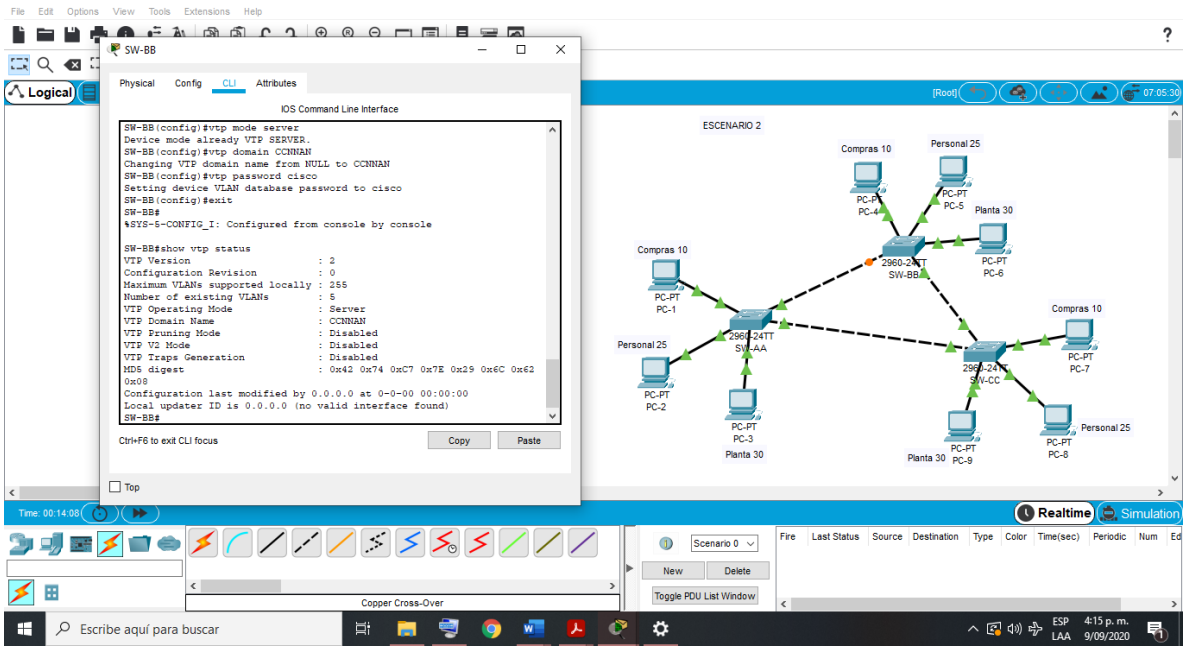

Figura 11 Verificación de la configuración VTP del SW-BB

Paso 3: Configurar los switch SW-AA y SW-CC como clientes VTP

SW-AA(config)# vtp mode client	Configurar el switch como clientes
SW-AA(config)# vtp domain CCNA	Nombre del dominio
SW-AA(config)# vtp password cisco	Contraseña de dominio VTP

SW-CC(config)# vtp mode client	Configurar el switch como clientes
SW-CC(config)# vtp domain CCNA	Nombre del dominio
SW-CC(config)# vtp password cisco	Contraseña de dominio VTP

Paso 4: Verificar a SW-AA

Verificar los cambios por medio del comando show vtp status.

SW-AA(config)# show vtp status

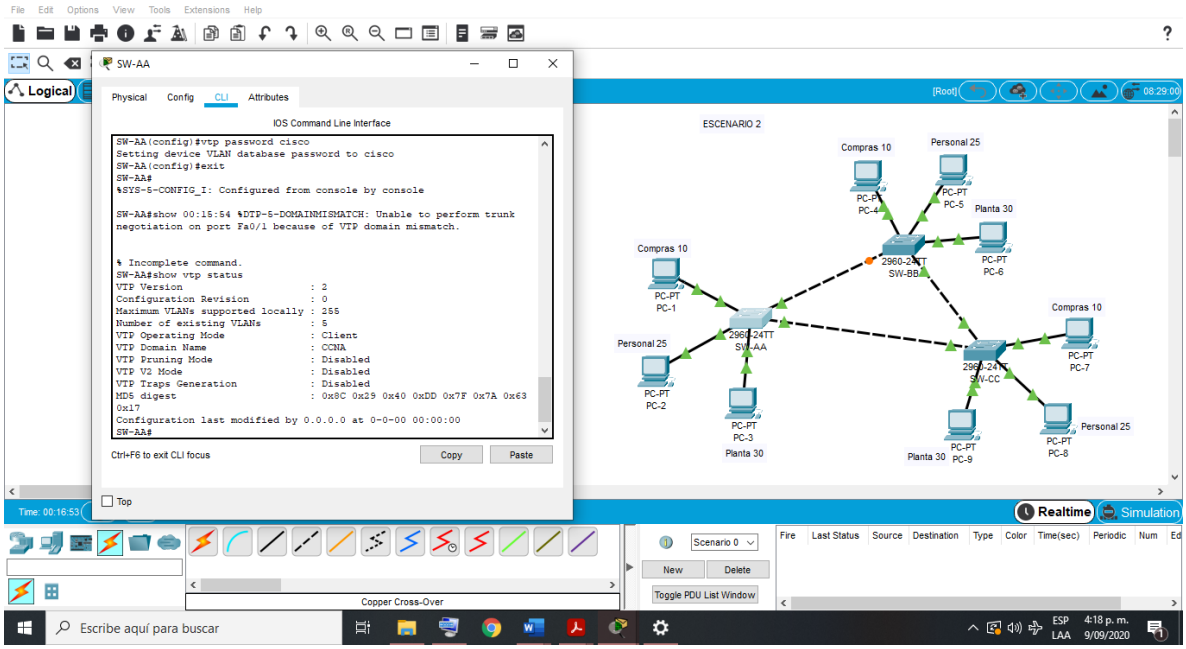

Figura 12 Verificación de la configuración VTP del SW-AA

Paso 5: Verificar a SW-CC

SW-CC(config)# show vtp status	Obtener información sobre el dominio VTP

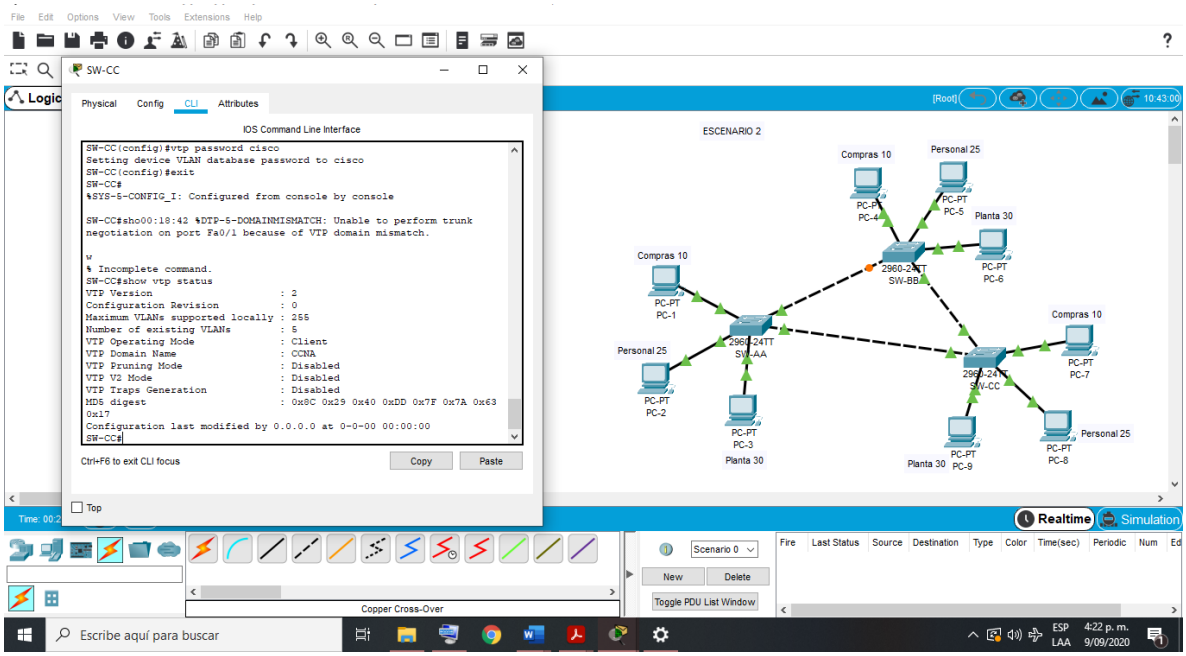

Figura 13 Verificación de la configuración VTP del SW-CC

2.4 PARTE 3: CONFIGURACION DTP (Dynamic Trunking Protocol)

Paso 1: Configurar un enlace troncal ("trunk") dinámico entre SW-AA

Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Para realizar la configuración DTP (Dynamic Trunking Protocol) usamos el comando switchport mode trunk por medio de los siguientes comandos.

Ahora seguimos configurando en el switch SW-AA el puerto FastEthernet 0/1 para enlace trunk desirable.

```
SW-AA(config)#interface fa0/1
SW-AA(config)# switchport mode dynamic desirable
SW-AA(config)# exit
```

Paso 2: Configurar un enlace troncal ("trunk") dinámico entre SW-BB.

Seguimos configurando en el switch SW-BB el puerto FastEthernet 0/1 para enlace trunk

```
SW-BB(config)#interface fa0/1
SW-BB(config)# switchport mode trunk
SW-BB(config)# exit
```

Paso 3: Verificar a SW-AA

Verifique el enlace "trunk" entre SW-AA usando el comando show interfaces trunk.

SW-AA#show interface trunk	Para ver el estado de un enlace troncal

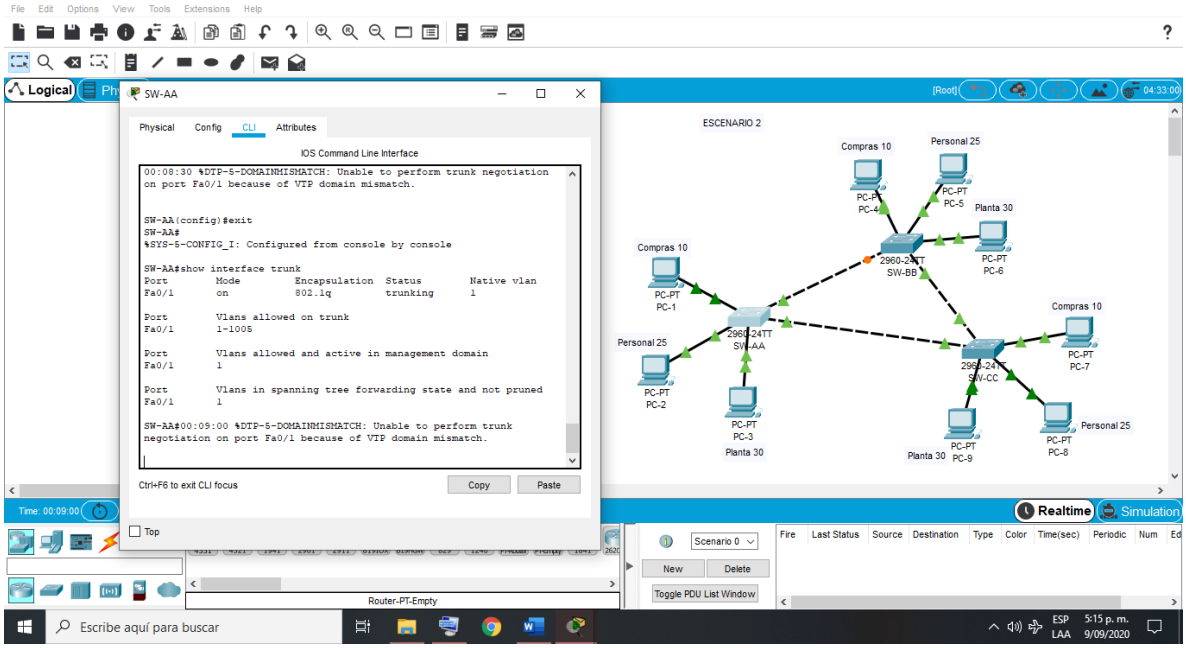

Figura 14 Verificación de la configuración DTP del SW-AA

Paso 4: Verificar a SW-BB

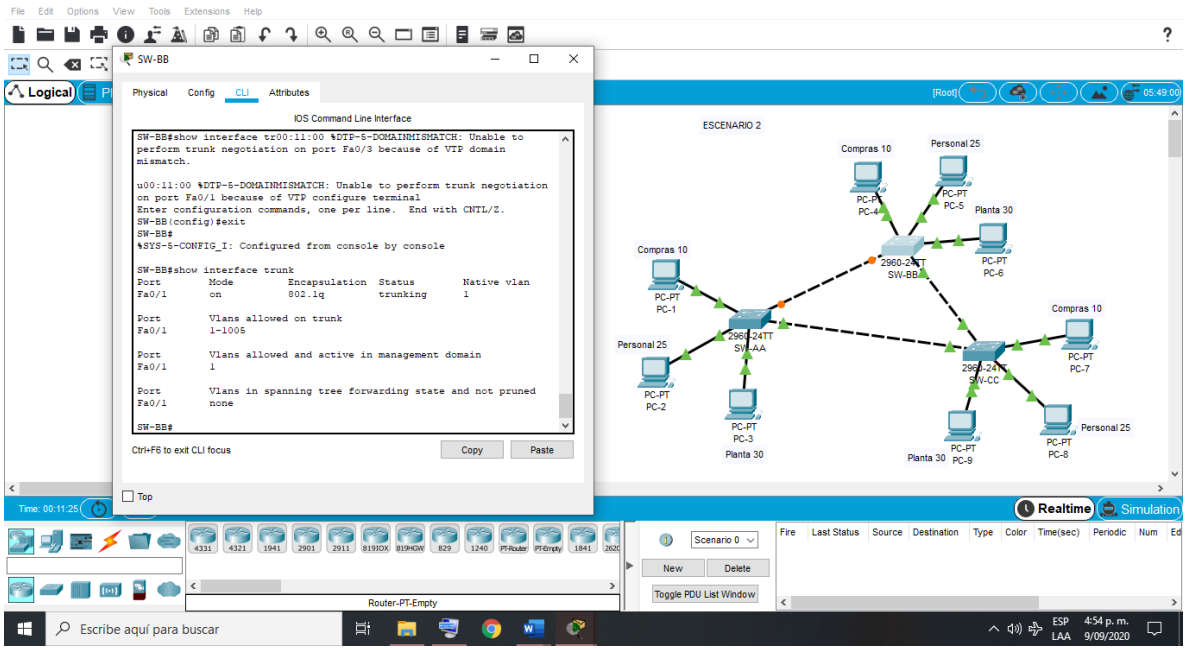

Figura 15 Verificación de la configuración DTP del SW-BB

Paso 5: Configurar en el switch SW- AA puerto FastEthernet 0/3 para enlace trunk.

SW-AA(config)#interface fa0/3

SW-AA(config)# switchport mode trunk

SW-AA(config)# exit

Paso 6: Configurar en el switch SW-BB el puerto FastEthernet 0/3 para enlace trunk.

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

SW-BB(config)#interface fa0/3

SW-BB(config)# switchport mode trunk

SW-BB(config)# exit

Paso 7: Verificar a SW-AA

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

SW-AA# show interfaces trunk.

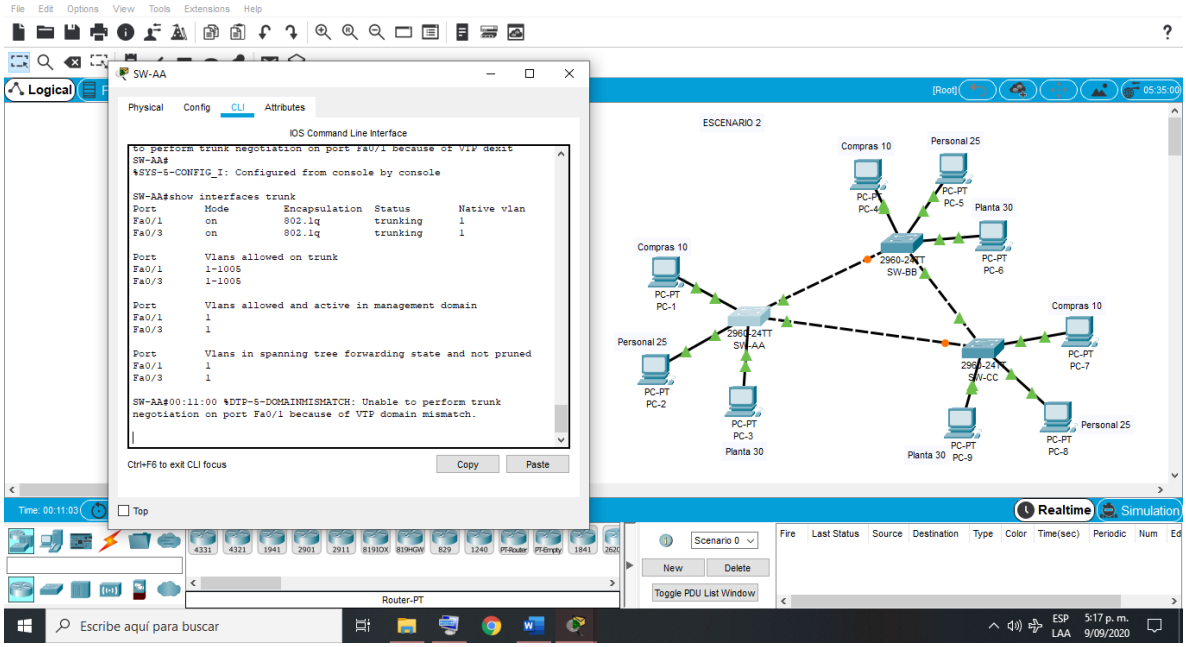

Figura 16 Verificación de la configuración trunk del SW-AA

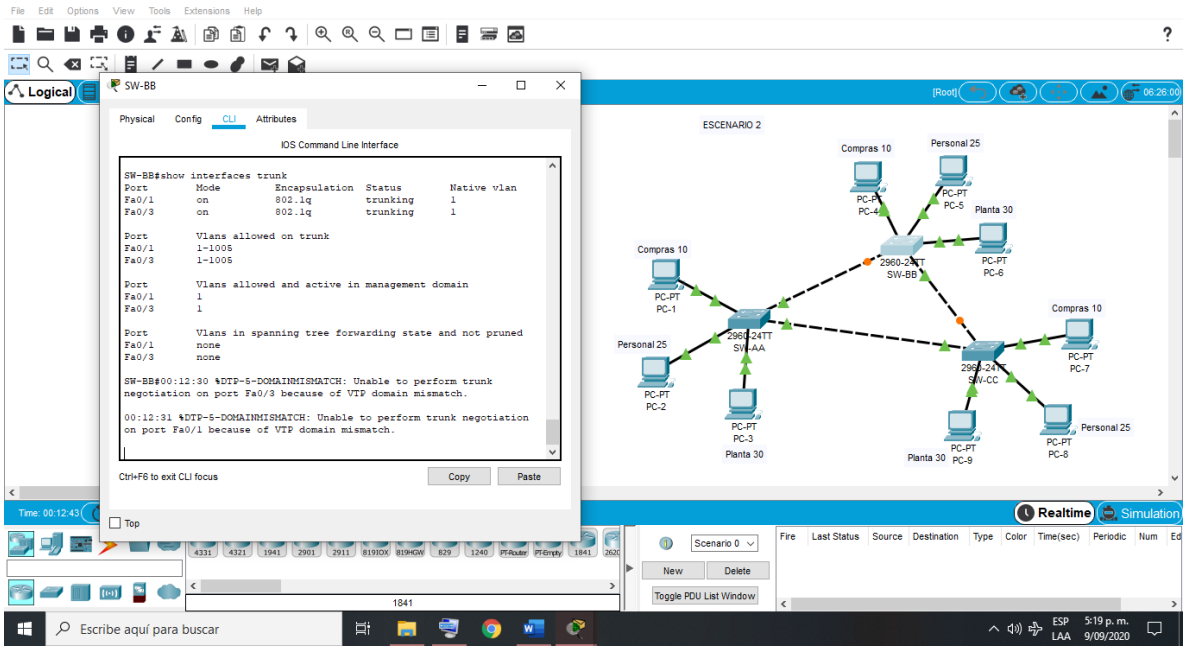

Figura 17 Verificación de la configuración trunk del SW-BB

2.5 PARTE 4: AGREGAR VLANS Y ASIGNAR PUERTOS.

Paso 1: En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

SW-BB(config)# vlan 10

SW-BB(config)# name Compras

SW-BB(config-vlan)# vlan 25

SW-BB(config-vlan)# name Personal

SW-BB(config-vlan)# vlan 30

SW-BB(config-vlan)# name Planta

SW-BB(config-vlan)# vlan 99

SW-BB(config-vlan)# name Admon

SW-BB(config-vlan)# exit

Paso 2: Verifique que las VLANs han sido agregadas correctamente.

Verificar que las VLANs han sido agregadas correctamente utilizando el comando show vlan brief.

SW-BB# show vlan brief

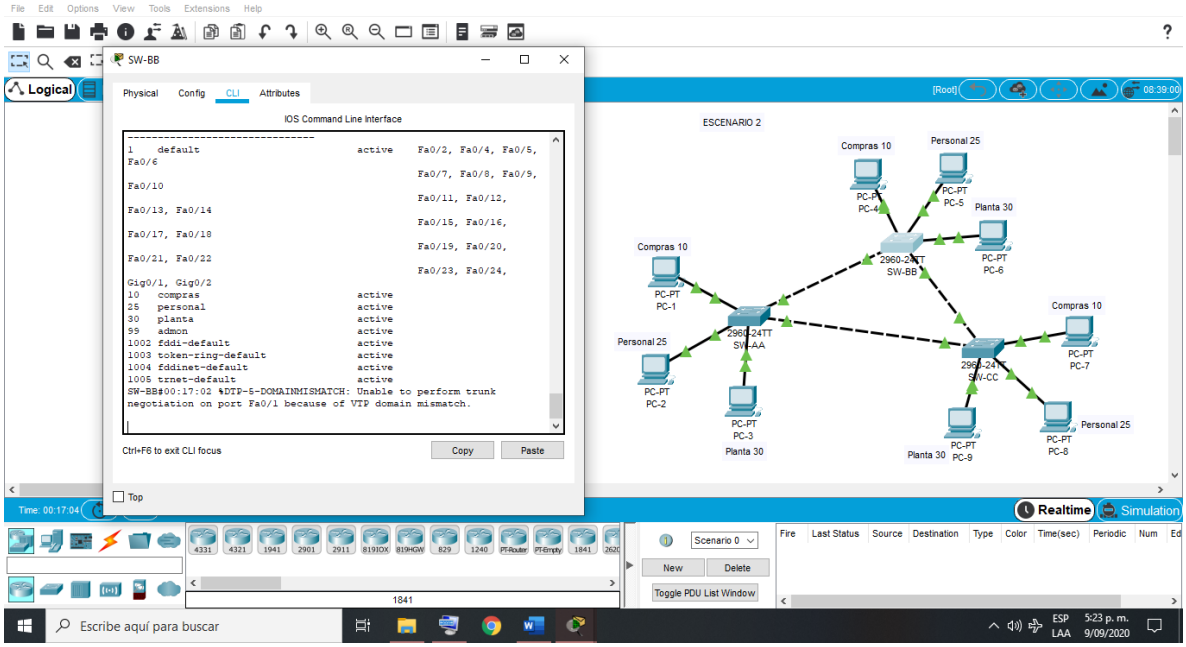

Figura 18 Verificación de la creación de las VLAN en el SW-BB

Paso 3: Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Asignar a cada PC su dirección IP, mascara de RED y puerta de enlace según corresponda de acuerdo a la siguiente tabla, donde X depende del número de cada PC.

INTERFAZ	VLAN	DIRECCION IP DE LOS PC's
FA0/10	VLAN 10	190.108.10.X
FA0/15	VLAN 25	190.108.20.X
FA0/20	VLAN 30	190.108.30.X

Tabla 5 Asignaciones de los puertos a las vlan con su dirección IP

Asignar las VLAN a los puertos en los switch por medio de los siguientes comandos.

Paso 4: Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

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 PC's de acuerdo con la tabla de arriba.

```
SW-AA#Configure terminal
SW-AA(Config)#interface fa0/10
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 10
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit
SW-AA(Config)#interface fa0/15
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 25
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit
SW-AA(Config)#interface fa0/20
SW-AA(Config-if)# switchport mode Access
SW-AA(Config-if)# switchport Access vlan 30
SW-AA(Config-if)# no shutdown
SW-AA(Config-if)# exit
```

```
SW-BB#Configure terminal
SW-BB(Config)#interface fa0/10
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport Access vlan 10
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit
SW-BB(Config)#interface fa0/15
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport Access vlan 25
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit
SW-BB(Config)#interface fa0/20
SW-BB(Config-if)# switchport mode Access
SW-BB(Config-if)# switchport Access vlan 30
SW-BB(Config-if)# no shutdown
SW-BB(Config-if)# exit
```

SW-CC#Configure terminal

SW-CC(Config)#interface fa0/10

SW-CC(Config-if)# switchport mode Access

SW-CC(Config-if)# switchport access vlan 10

SW-CC(Config-if)# no shutdown

SW-CC(Config-if)# exit

SW-CC(Config)#interface fa0/15

SW-CC(Config-if)# switchport mode Access

SW-CC(Config-if)# switchport access vlan 25

SW-CC(Config-if)# no shutdown

SW-CC(Config-if)# exit

SW-CC(Config)#interface fa0/20

SW-CC(Config-if)# switchport mode Access

SW-CC(Config-if)# switchport accessn vlan 30

SW-CC(Config-if)# no shutdown

SW-CC(Config-if)# exit

Paso 5: Configurar las direcciones IP en los Switches.

Configurar las direcciones IP en los Switch por medio de los siguientes comandos.

EQUIPO	VLAN	DIRECCION IP
SW-AA	VLAN 99	190.108.99.1/24
SW-BB	VLAN 99	190.108.99.2/24
SW-CC	VLAN 99	190.108.99.3/24

Tabla 6 Configuración de las direcciones IP a los switch

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-AA(config-if)#no shutdown

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-BB(config-if)#no shutdown

SW-CC#Configure terminal

SW-CC(config)#interface vlan 99

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

SW-CC(config-if)#no shutdown

2.6 PARTE 4: VERIFICAR EXTREMO A EXTREMO.

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

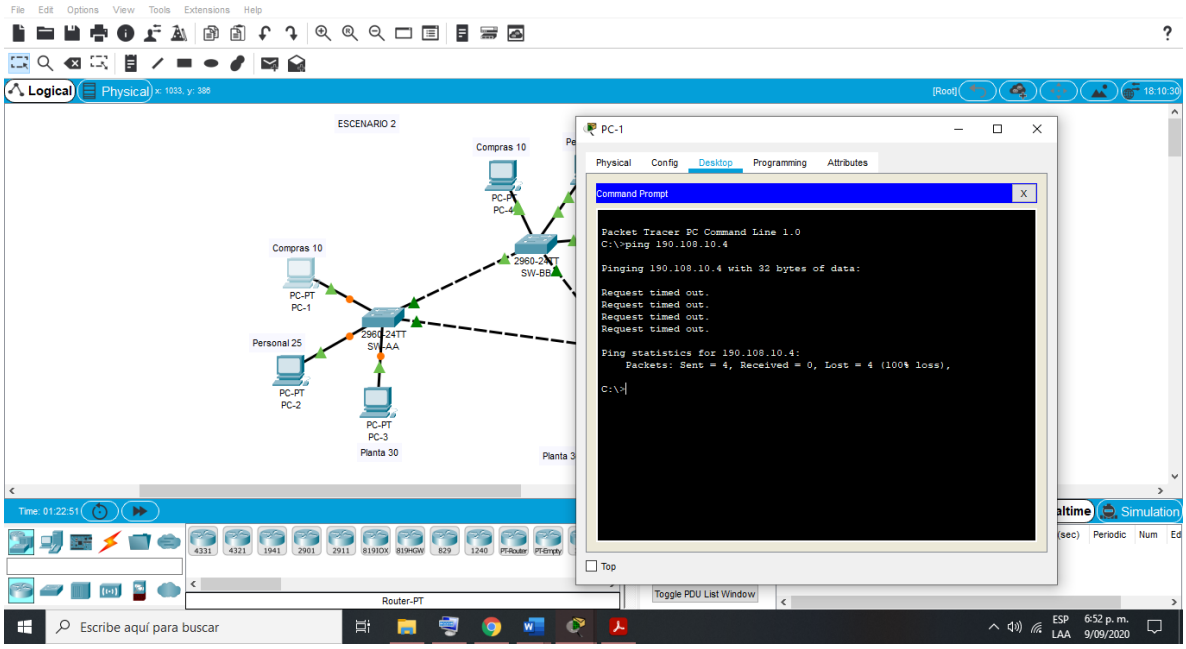

Figura 19 Verificación de un PC a otro PC de la misma vlan

La verificación de un PC a otro PC de diferente vlan no fue exitosa, debido a que en las configuraciones que se realizaron, se les asigno la diferente vlan, ocasionando el error de comunicación entre los PC's. pero al momento de realizar las verificaciones de un PC a otro con la misma vlan la comunicación es exitosa.

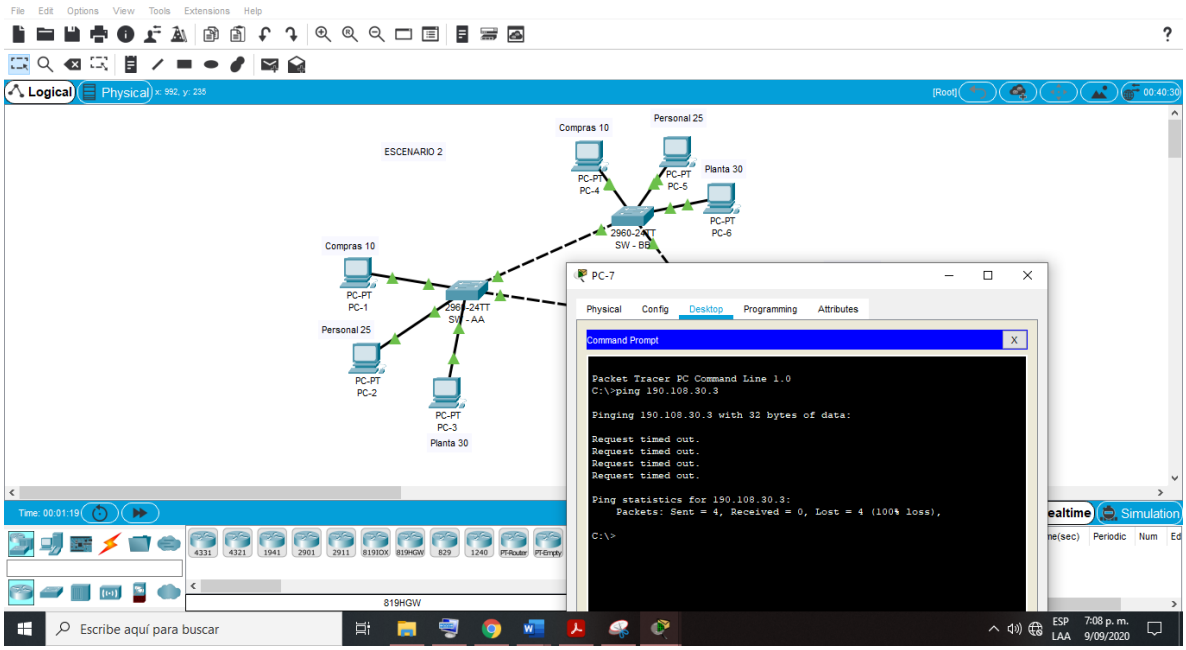

Figura 20 Verificación de un PC a otro PC de diferente vlan

Paso 2: Ejecute un Ping desde cada Switch a los demás.

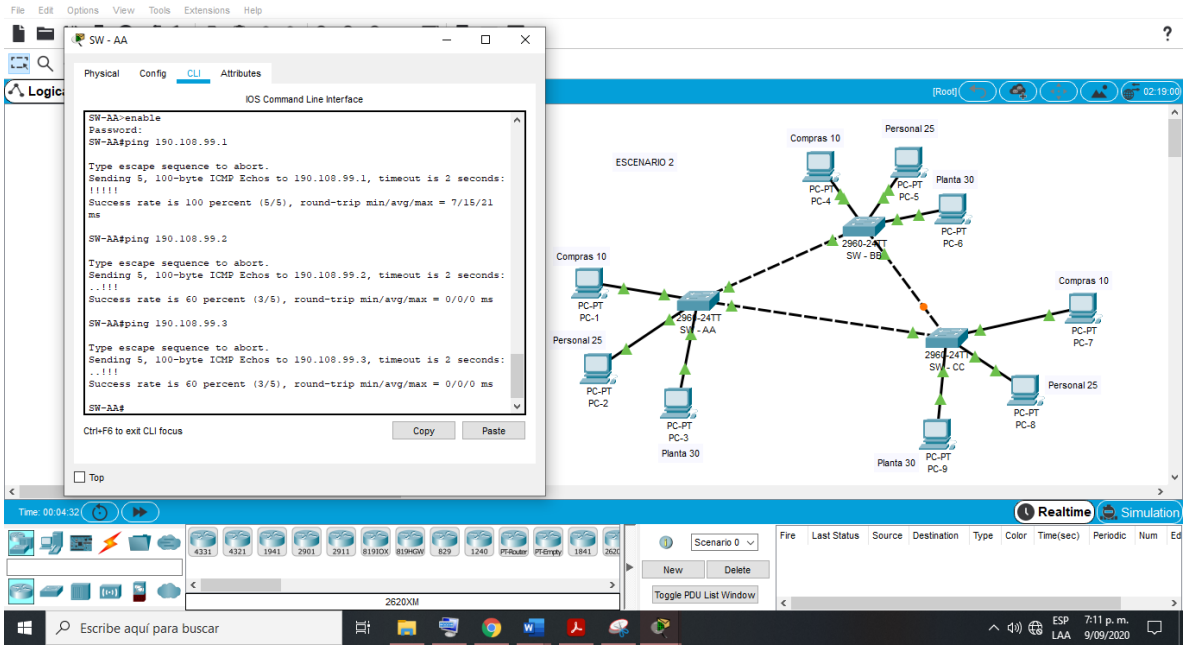

Figura 21 Verificación desde SW-AA a los demás

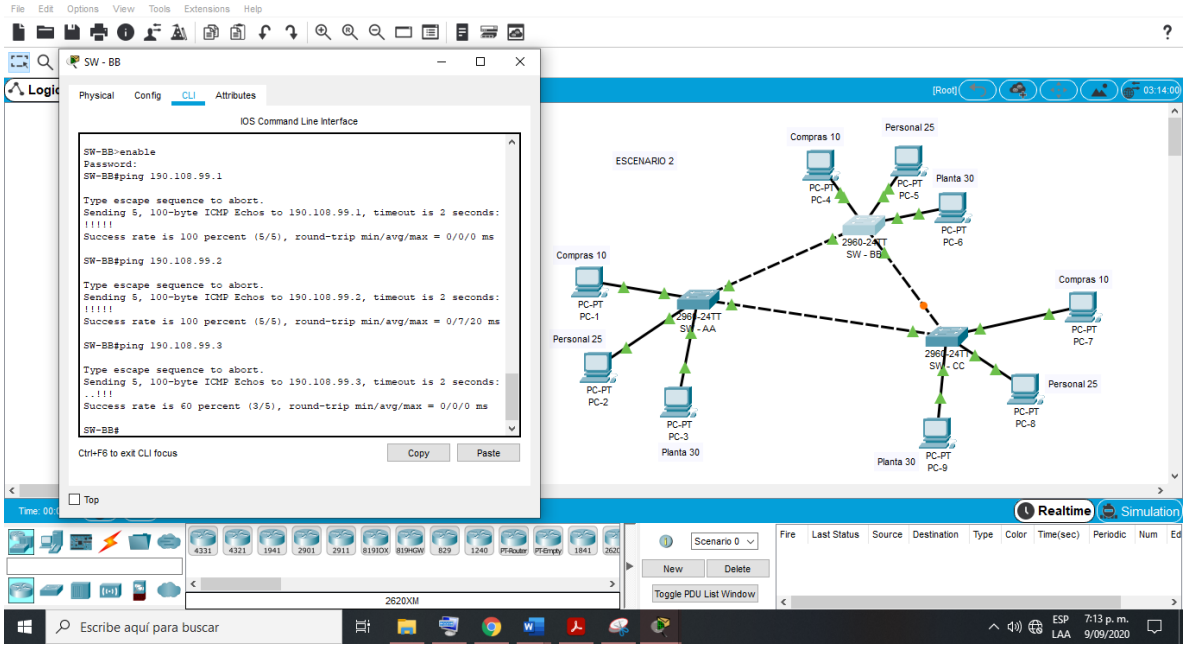

Figura 22 Verificación desde SW-BB a los demás

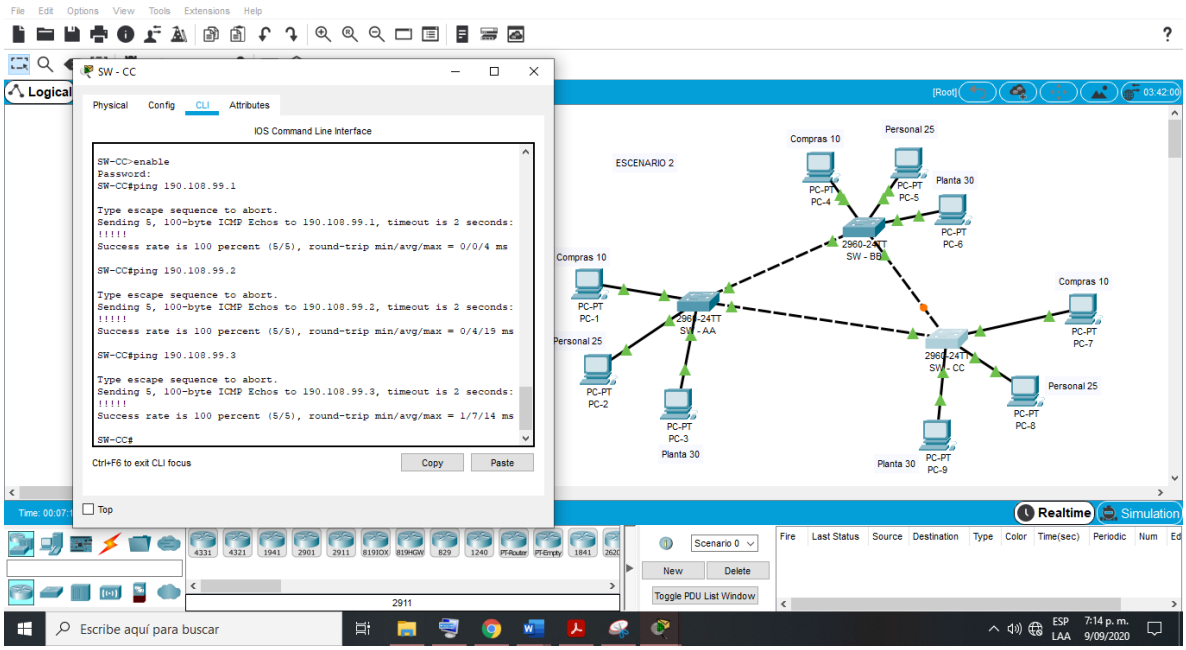

Figura 23 Verificación desde SW-CC a los demás

La verificación de un switch a otro switch fue exitosa, las configuraciones que se realizaron cuando se creó la vlan 99 permitió que fuera posible la comunicación entre ellos.

Paso 3: Ejecute un Ping desde cada Switch a cada PC

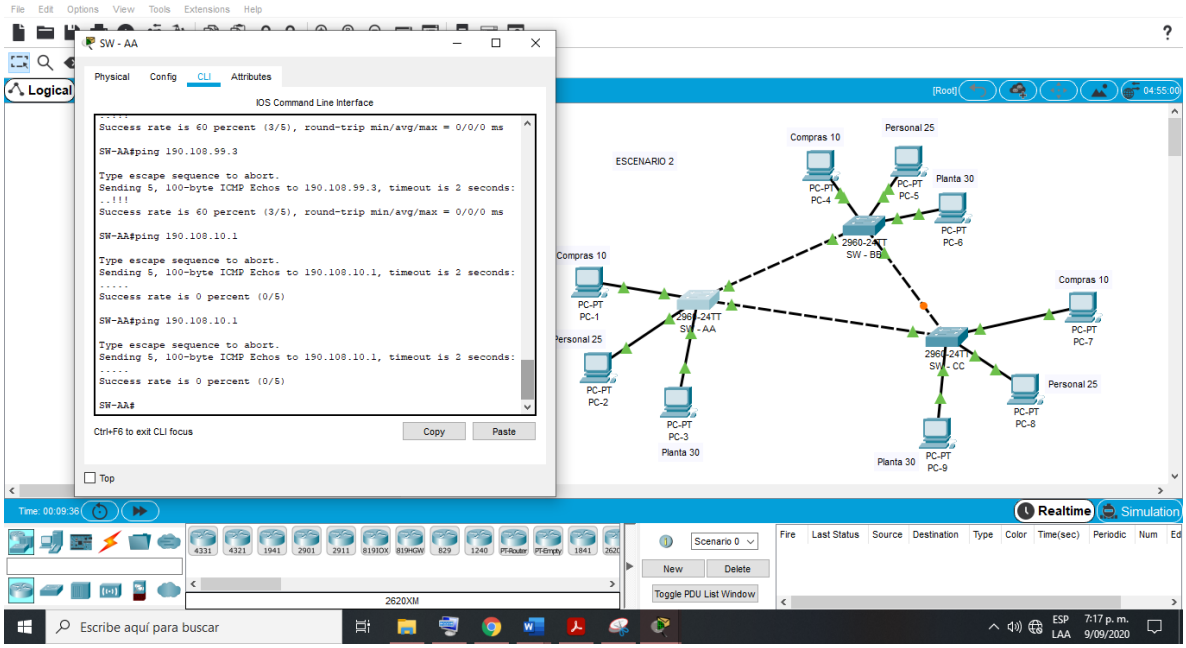

Figura 24 Verificación desde SW-AA al PC-1

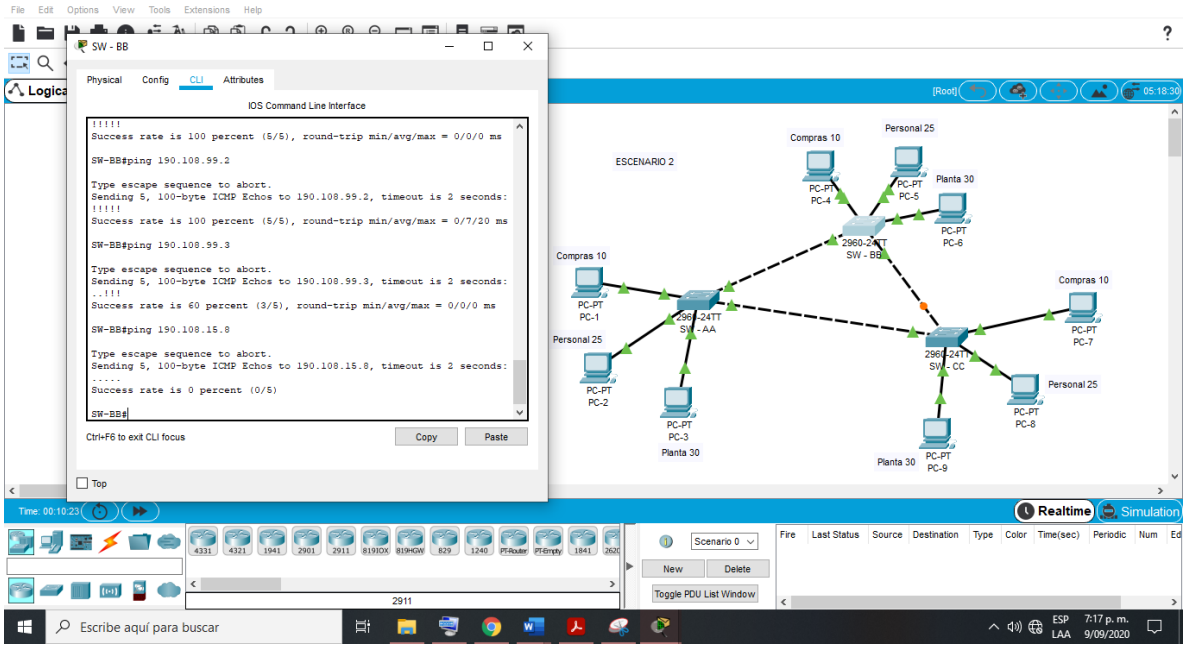

Figura 25 Verificación desde SW-BB al PC-8

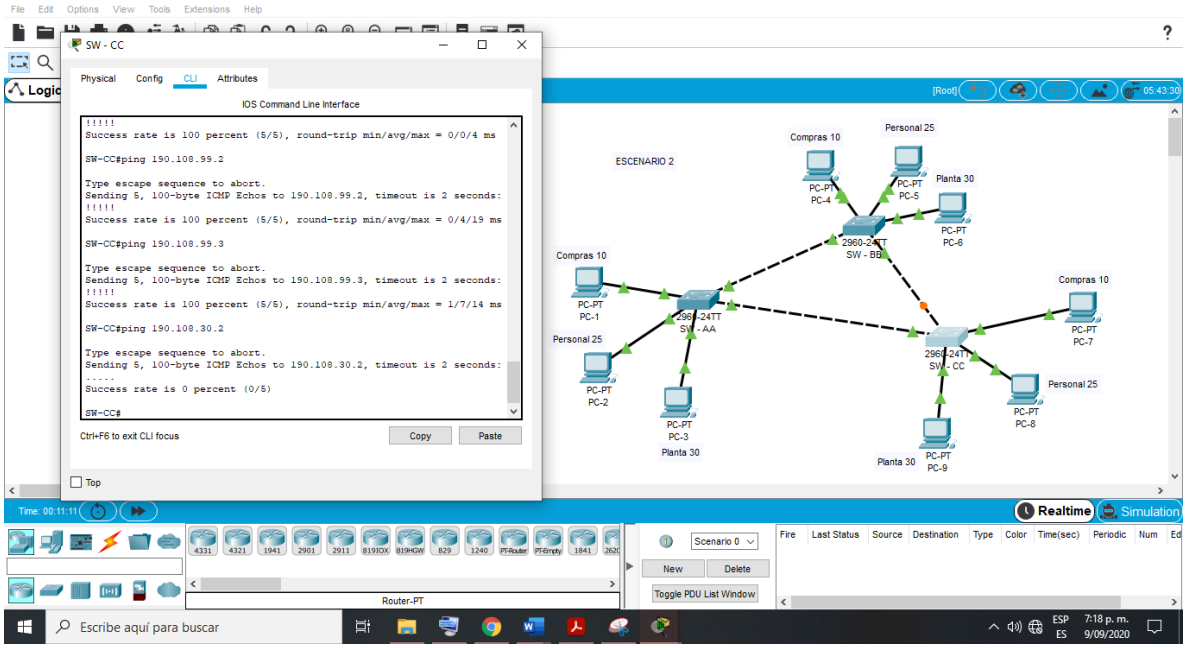

Figura 26 Verificación desde SW-CC al PC-2

La verificación de cada switch a cada PC no fue exitosa, debido a que el switch y el PC no tienen una dirección IP que permita enlazar la comunicación entre ellos.

CONCLUSIONES

Es indispensable tener claro la función de cada comando para hacer más optimo el desarrollo de las configuraciones en los escenarios, y por lo tanto, hacer más fácil las verificaciones, evitando errores en las configuraciones que se realicen en los dispositivos de la red.

La descripción detalla de cada una de las etapas realizadas paso a paso de manera ordenada, registrando cada una de las estructuras de comandos requeridos para su óptimo desarrollo, permite hacer un mejor manejo de los temas aprendiendo más rápido.

El protocolo BGP que se empleó como enrutamiento entre los routers, es fácil de configurar y permite que un grupo de redes envíen y reciban información, los routers se configuran con la información del router vecino formando una conexión para el transporte de datos informáticos.

Para evitar la realización de largas configuraciones en los switch de una red creando la misma VLAN en cada uno de ellos, se aplica el protocolo de troncal vlan más conocido como VTP, tal y como se realiza en el segundo escenario; gracias a este protocolo se ahorra tiempo y se administra mejor la red.

El desarrollo de los escenarios por medio de las simulaciones en el programa Packet Tracer es beneficioso para que el desempeño en las industrias de redes y comunicaciones sea óptimo en los diferentes procesos en una compañía, si es una red LAN; pero si es una red mas grande como las WAN, será más cómoda la comunicación entre compañías de la misma cadena, ya que es importante implementar estos sistemas de transmisión de la información e interconexión de los dispositivos, de una forma más fácil y segura, permitiendo un control más óptimo en las comunicaciones de estas.

REFERENCIAS

BGP Case Studies. (s. f.). Cisco. Recuperado 9 de septiembre de 2020, de https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. 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

Definición y tipos de enrutamiento dinámico | VIU. (s. f.). Recuperado 9 de septiembre de 2020, de https://www.universidadviu.com/definicion-tipos-enrutamiento-dinamico/

Engineering, N. (2018, julio 24). Ingeniería de redes, telecomunicaciones y ciberseguridad en Barcelona. Net Cloud Engineering. https://netcloudengineering.com/configuracion-vlan-cisco-switch/

Temática: Configuración y conceptos básicos de Switching CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de:

https://staticcourseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

Temática: VLANs CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

VTP Y DTP. (s. f.). VTP Y DTP. Recuperado 9 de septiembre de 2020, de http://conmutacion-y-enrutamiento.blogspot.com/2017/09/vtp-y-dtp.html