

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN CARLOS GRISALES MENESES

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA**

MEDELLÍN

2020

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN CARLOS GRISALES MENESES

**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 BÁSICAS, TECNOLOGÍA E INGENIERÍA**

PROGRAMA DE INGENIERÍA ELECTRÓNICA

MEDELLÍN

2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLIN, 22 DE MAYO DE 2020

AGRADECIMIENTOS

Inicialmente le doy gracias a Dios, que me dio la fortaleza para siempre seguir adelante para alcanzar el objetivo de terminar mis estudios. A mi familia por ser mi soporte en especial a mi madre que a pesar de mis ausencias laborales o académicas nunca me juzgo por el contrario es esa voz de aliento, de apoyo, de energía ya que si se desean los sueños por difíciles que sean se pueden alcanzar con constancia y tenacidad.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE ILUSTRACIONES.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN.....	11
ESCENARIO 1.....	12
ESCENARIO 2.....	25
CONCLUSIONES.....	44
REFERENCIAS.....	45

LISTA DE TABLAS

Tabla 1 Configuración de los router 1	12
Tabla 2 Configuración de los router 2	12
Tabla 3 Configuración de los router 3	12
Tabla 4 Configuración de los router 4	12
Tabla 5 Asignar a cada PC su dirección IP, mascara de RED y puerta de enlace	34
Tabla 6 Direcciones IP en cada uno de los Switch.....	36

LISTA DE ILUSTRACIONES

Ilustración 1 Escenario 1	12
Ilustración 2 Ventana principal de un Router	13
Ilustración 3 Módulos para agregar los puertos seriales al Router.....	13
Ilustración 4 Apagar el Router	14
Ilustración 5 Módulos agregados al Router.....	14
Ilustración 6 Ventana de configuraciones del Router	15
Ilustración 7 Verificación en R1 la relación de vecino BGP.....	19
Ilustración 8 Verificación en R2 la relación de vecino BGP.....	20
Ilustración 9 Verificación en R2 la relación de vecino BGP con R3.....	21
Ilustración 10 Verificación en R3 la relación de vecino BGP.....	21
Ilustración 11 Verificación en R3 la relación de vecino BGP con R4.....	23
Ilustración 12 Verificación en R4 la relación de vecino BGP.....	24
Ilustración 13 Escenario 1 en el programa Packet Tracer.....	24
Ilustración 14 Escenario 2	25
Ilustración 15 Escenario 2 en el Programa Packet Tracer	25
Ilustración 16 Configuraciones básicas de un Switch	26
Ilustración 17 Configuración vtp del switch SW-BB.....	28
Ilustración 18 Configuración vtp del switch SW-AA.....	29
Ilustración 19 Configuración vtp del switch SW-CC	29
Ilustración 20 Verificación de enlace trunk fa0/1 en el switch SW-AA.....	31
Ilustración 21 Verificación de enlace trunk fa0/3 en el switch SW-AA.....	32
Ilustración 22 Verificación de enlace trunk fa0/3 en el switch SW-BB.....	32
Ilustración 23 Verificación de las vlan en el switch SW-BB	34
Ilustración 24 Verificación de los puertos en el switch SW-BB.....	36
Ilustración 25 Verificación de ping del PC4 al PC7	38
Ilustración 26 Verificación de ping del PC5 al PC8	38
Ilustración 27 Verificación de ping del PC6 al PC9	39
Ilustración 28 Verificación de ping del PC2 al PC6	39
Ilustración 29 Verificación de ping del PC7 al PC3	40
Ilustración 30 Verificación de ping del PC9 al PC1	40
Ilustración 31 Verificación del ping desde el switch SW-BB.....	41
Ilustración 32 Verificación del ping desde los switch.....	41
Ilustración 33 Verificación del ping desde el switch SW-AA.....	42
Ilustración 34 Verificación del ping desde los switch a los PC's	43

GLOSARIO

Ping: envía paquetes al IP o host que se le indique, y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras pocas informaciones.

Router: es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet

Packet Tracer: es una herramienta de aprendizaje y simulación de redes interactiva. Esta herramienta permite crear tipologías de red, simular una red con múltiples representaciones visuales, principalmente es una herramienta de apoyo didáctico

Dirección IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Port-Serial: En la informática, un puerto serie es una interfaz física de comunicación en serie a través de la cual la información se transfiere dentro o fuera de un bit a la vez.

Enlace trunk: Permite manejar el tráfico de distintas Vlan en un mismo puerto, o sea que cada paquete irá etiquetado y cuando se envíe a una vlan se podrá resolver correctamente.

RESUMEN

En este trabajo se encuentra el desarrollo de dos ejercicios donde se aplican los conocimientos adquiridos a lo largo del diplomado de cisco CCNP, buscando identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas y poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking en temas como la configuración EBGp, VTP, DTP, protocolos de enrutamiento Avanzado, Implementación de soluciones soportadas en enrutamiento avanzado, configuración de sistemas de red soportados en VLAN entre otros.

En este informe se explican las configuraciones y procedimientos para dar solución de forma detallada que se aplicaron según lo requerido en cada escenario.

Palabras Clave: Comunicaciones, Cisco, Networking, EBGp, VTP, DTP.

ABSTRACT

In this work we find the development of two exercises where the knowledge acquired throughout the Cisco CCNP diploma is applied, seeking to identify the degree of development of competencies and skills that were acquired and to test the levels of understanding and problem solving related to various aspects of Networking in topics such as EIGRP, VTP, DTP configuration, Advanced routing protocols, Implementation of solutions supported in advanced routing, configuration of network systems supported in VLAN, among others.

This report explains the configurations and procedures to give a detailed solution that were applied as required in each scenario.

Key Words: Communications, Cisco, Networking, EIGRP, VTP, DTP.

INTRODUCCION

Las comunicaciones siempre han sido fundamentales debido a la necesidad constante de siempre estar conectados unos con otros ya que somos seres sociales por naturaleza, a medida que las comunicaciones han ido evolucionando nos han ido conectando cada vez mejor, haciendo que la distancia no sea un obstáculo para relacionarnos y aprender continuamente de otras personas.

En el presente trabajo se desarrolló la prueba de habilidades prácticas profundizando en CCNP por medio del programa de Cisco Packet Tracer, el cuál es fácil de comprender y programar.

En este informe se encontrará el desarrollo de los ejercicios del módulo CCNP Switch y de los protocolos de enrutamiento EBGP donde se aplican los conocimientos adquiridos a lo largo del curso, además del registro de los procesos de configuración, verificación y conexión

ESCENARIO 1

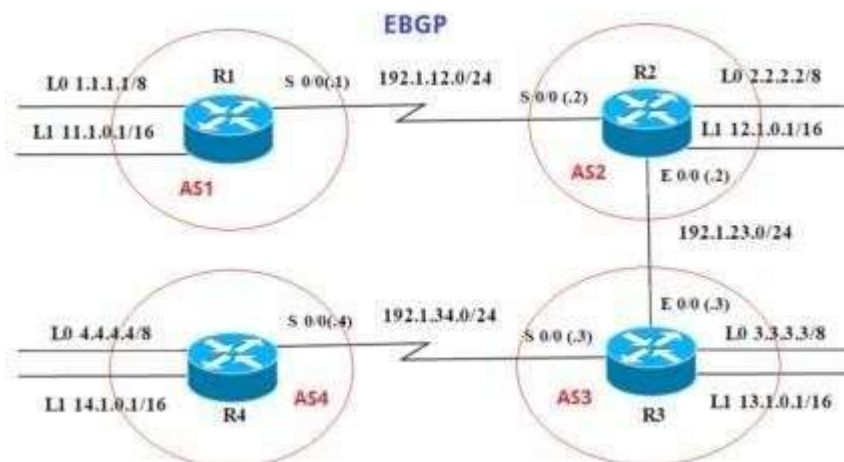


Ilustración 1 Escenario 1

Información para la configuración de los routers:

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0
R2	Interfaz	Dirección IP	Máscara
	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

Tabla 1 y 2 configuración de los routers 1 y 2

	Interfaz	Dirección IP	Máscara
R3	Interfaz	Dirección IP	Máscara
	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0
R4	Interfaz	Dirección IP	Máscara
	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Tabla 3 y 4 configuración de los routers 3 y 4

Inicialmente agregamos a la pantalla principal del programa Packet Tracer los Routers **2901** y damos clic, apareciendo una ventana como la de la ilustración 2.

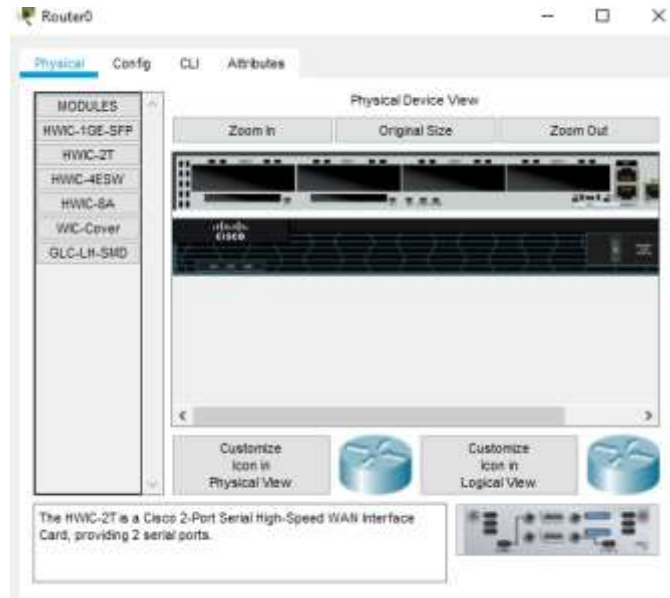


Ilustración 2 Ventana principal de un Router

Debido a que un Router en su parte física cuenta solo con las 2 interfaces Gigabit, requerimos colocar otras interfaces y para esto se le agrega un módulo HWIC-2T (2 Port-Serial) que son dos interfaces seriales y un módulo HWIC-4ESW (4 Switchports) que son cuatro puertos serial Fast Ethernet.

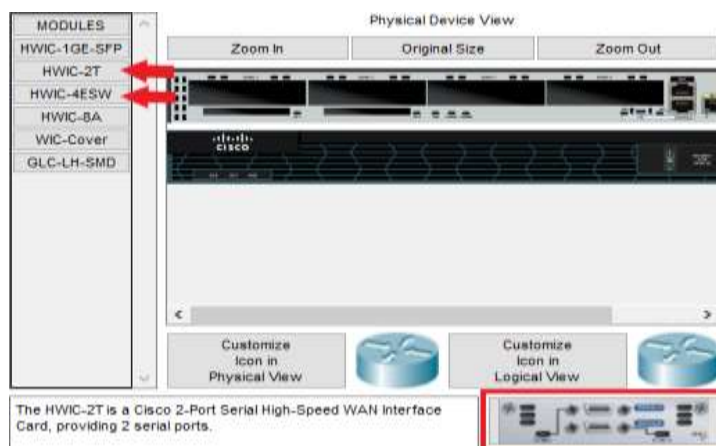


Ilustración 3 Módulos para agregar los puertos seriales al Router

En la ilustración 2 podemos observar en la parte izquierda los módulos y los que están señalados por las flechas de color rojo son los que vamos utilizar, al dar clic sobre el nombre del módulo, nos aparece en la parte inferior de la ventana.

Para agregar un módulo primero debemos apagar el Router, en la ilustración 4 vemos la opción de apagarlo en la zona donde hay un cuadrado rojo y luego arrastramos el módulo y soltamos en los puertos vacíos.

Después se debe encender el Router de nuevo quedando como en la ilustración 5.

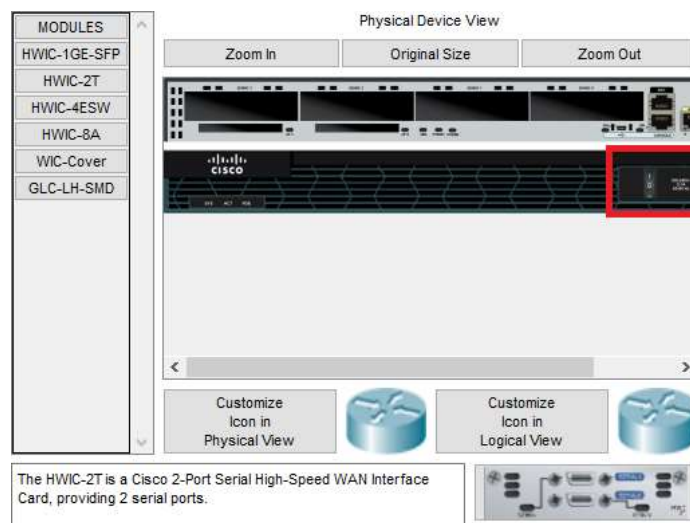


Ilustración 4 Apagar el Router

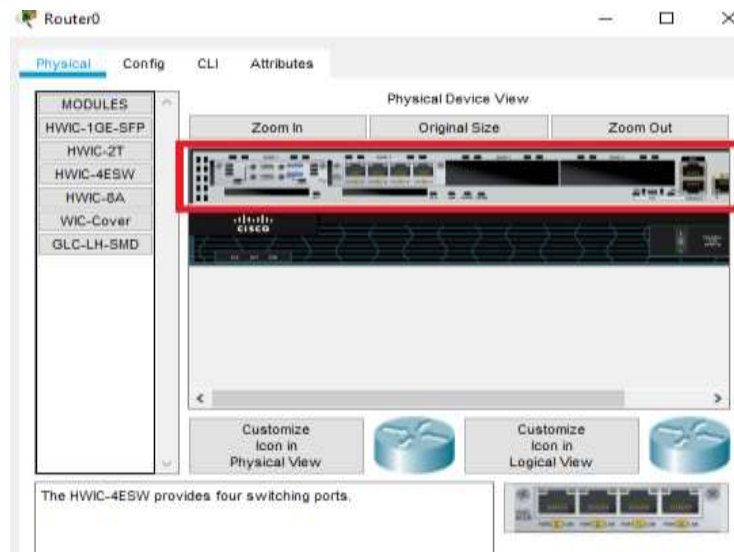
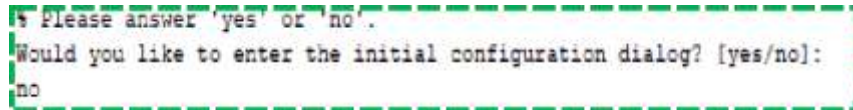


Ilustración 5 Módulos agregados al Router

Ahora vamos a la pestaña **CLI** que es la línea de comando, donde vamos a realizar las configuraciones básicas. Cuando inicia el sistema operativo del Router, nos pregunta si queremos usar el asistente de configuración, en este caso escribiremos **no**, ya que las configuraciones se harán manualmente. Ilustración 6.

A screenshot of a terminal window with a green dashed border. The text inside reads: "Please answer 'yes' or 'no'." followed by "Would you like to enter the initial configuration dialog? [yes/no]:" and the user input "no".

```
Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]:
no
```

Ilustración 6 Ventana de configuraciones del Router

Tenemos la misma ventana de un switch por lo que empezamos con las configuraciones básicas.

Primero vamos a la pestaña **CLI**, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando **Router>** que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando **enable** para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado **Router#**.

La primera configuración básica es cambiar el nombre de usuario, en este caso su nombre es switch y lo cambiaremos por medio del comando **hostname** seguido del nombre que le colocaremos al Router, en este caso **R1**.

Ahora le colocamos una contraseña secreta que no se podrá visualizar por medio del comando **enable secret cisco**. Otras configuraciones que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos **line console 0** y **line vty 0 4** enter **password cisco** después tenemos que escribir el comando **login** para que acepte y aplique las contraseñas, para salir de este modo de configuración escribimos el comando **exit**.

Y por último escribimos el comando **service password-encryption** para encriptar las contraseñas enter y escribimos **do write** para guardar los datos.

Luego realizamos las mismas configuraciones en los otros Router colocando el nombre según corresponda.

Configuraciones EBGp

1. Asignar los nombres, las direcciones IP y las direcciones de loopback a cada Router.

- Router R1

```
R1(config)#interface
```

```
Se0/3/0
```

```
R1(config)#ip address 192.1.12.1
```

```
255.255.255.0 R1(config)#no shutdown
```

```
R1(config)#exit
```

```
R1(config)#interface loopback 0
```

```
R1(config)#ip address 1.1.1.1
```

```
255.0.0.0 R1(config)#exit
```

```
R1(config)#interface loopback 1
```

```
R1(config)#ip address 11.1.0.1
```

```
255.255.0.0 R1(config)#exit
```

- Router 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
```

- Router 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
```

- Router 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
```

2. Configurar 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 Router **BGP** como 11.11.11.11 para R1 y como 22.22.22.22 para R2.

Configurar el vecino BGP para R1 y R2:

- R1

```
R1(config)#route
r bgp 1
R1(config-router)#no
synchronization R1(config-
router)#bgp router-id 11.11.11.11
R1(config-router)#neighbor 192.1.12.2 remote-as 2
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
```

- R2

```
R2(config)#route
```

```
r bgp 2
```

```
R2(config-router)#no
```

```
synchronization R2(config-
```

```
router)#bgp router-id 22.22.22.22
```

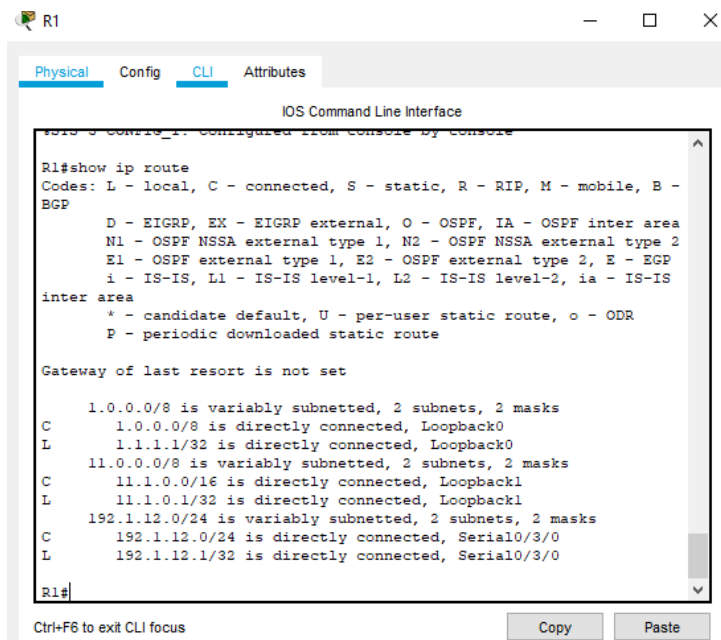
```
R2(config-router)#neighbor 192.1.12.1 remote-as 1
```

```
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
```

3. Verificar usando el comando **show ip route** en los Router R1 y R2

```
R1# show ip route
```



```
R1#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, E - EGP
       i - IS-IS, 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

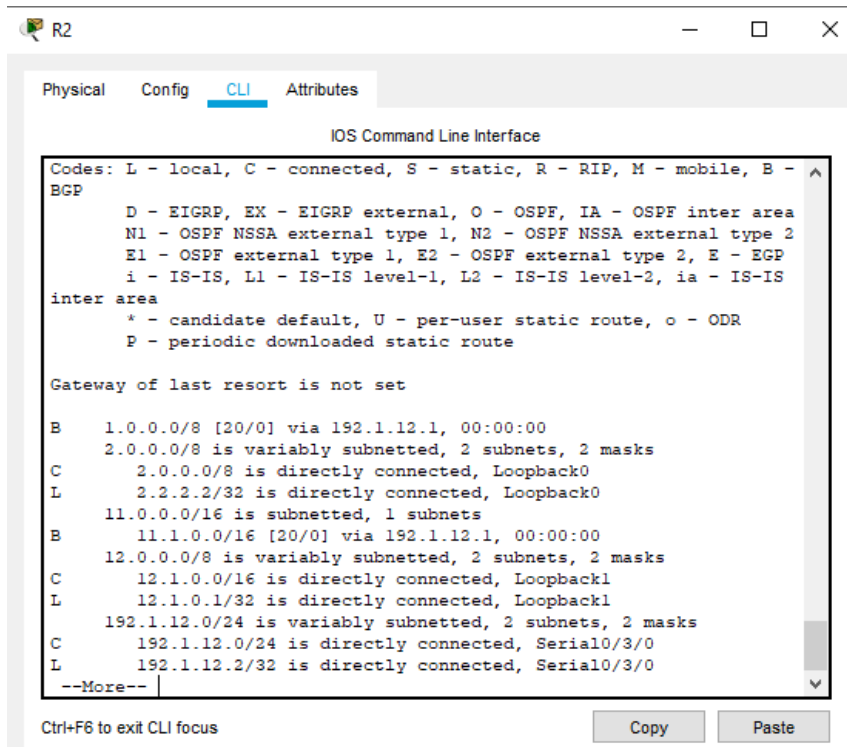
Gateway of last resort is not set

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
L       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
C       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/3/0
L       192.1.12.1/32 is directly connected, Serial0/3/0

R1#
```

Ilustración 7 Verificación en R1 la relación de vecino BGP

R2# 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, E - EGP
i - IS-IS, 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 1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
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 11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
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, Serial0/3/0
L 192.1.12.2/32 is directly connected, Serial0/3/0
--More--
```

Ilustración 8 Verificación en R2 la relación de vecino BGP

4. Configurar una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33.

Configurar el vecino BGP para R2 y R3:

- R2

```
R2(config)#route
```

```
r bgp 2
```

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

- R3

```
R3(config)#route
```

```
r bgp 3
```

```
R3(config-router)#no
```

```
synchronization R3(config-
```

```
router)#bgp router-id 33.33.33.33
```

```
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

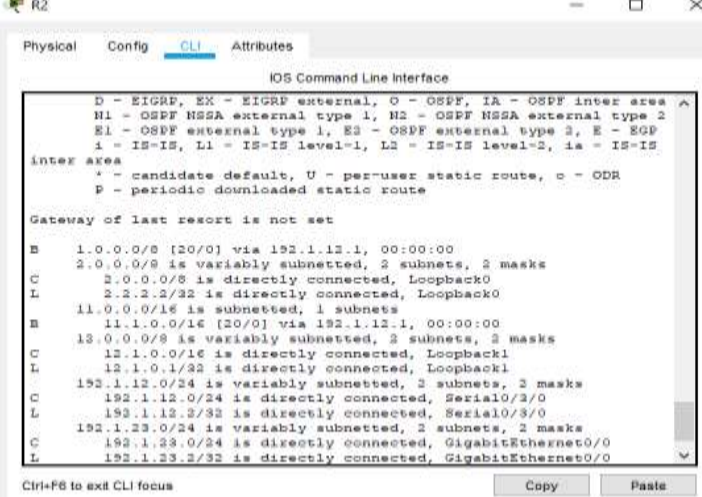
```
R3(config-router)#neighbor 192.1.34.4 remote-as 4
```

```
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
```

5. Verificar usando el comando **show ip route** en los Router R2 y R3

R2# show ip route




```
IOS Command Line Interface
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, E - EGP
I - IS-IS, 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 1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
  2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  3.0.0.0/8 is directly connected, Loopback0
L  2.2.2.2/32 is directly connected, Loopback0
  11.0.0.0/16 is subnetted, 1 subnets
  11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
B 13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 12.1.0.1/32 is directly connected, Loopback1
  192.1.12.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.1.12.0/24 is directly connected, Serial0/2/0
L 192.1.12.2/32 is directly connected, Serial0/3/0
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0
L 192.1.23.2/32 is directly connected, GigabitEthernet0/0
```

Ilustración 9 Verificación en R2 la relación de vecino BGP con R3

R3# show ip route



```
IOS Command Line Interface
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, E - EGP
I - IS-IS, 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

  3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C  3.0.0.0/8 is directly connected, Loopback0
L  2.2.2.2/32 is directly connected, Loopback0
  13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 12.1.0.1/32 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, GigabitEthernet0/0
L 192.1.23.3/32 is directly connected, GigabitEthernet0/0
  192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial0/3/0
L 192.1.34.2/32 is directly connected, Serial0/3/0
```

Ilustración 10 Verificación en R3 la relación de vecino BGP

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

Configurar el vecino BGP para R3 y R4:

- R3

```
R3(config)#route
```

```
r bgp 3
```

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

- R4

```
R4(config)#route
```

```
r bgp 4
```

```
R4(config-router)#no
```

```
synchronization R4(config-
```

```
router)#bgp router-id 44.44.44.44
```

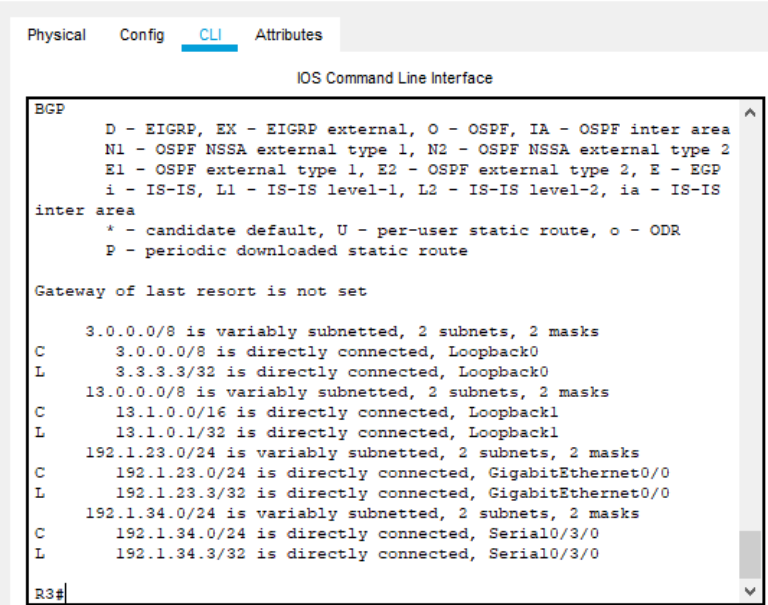
```
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

```
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
```

7. Verificar usando el comando **show ip route** en los Router R1 y R2

R3# show ip route



```
R3# show ip route
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, E - EGP
i - IS-IS, 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

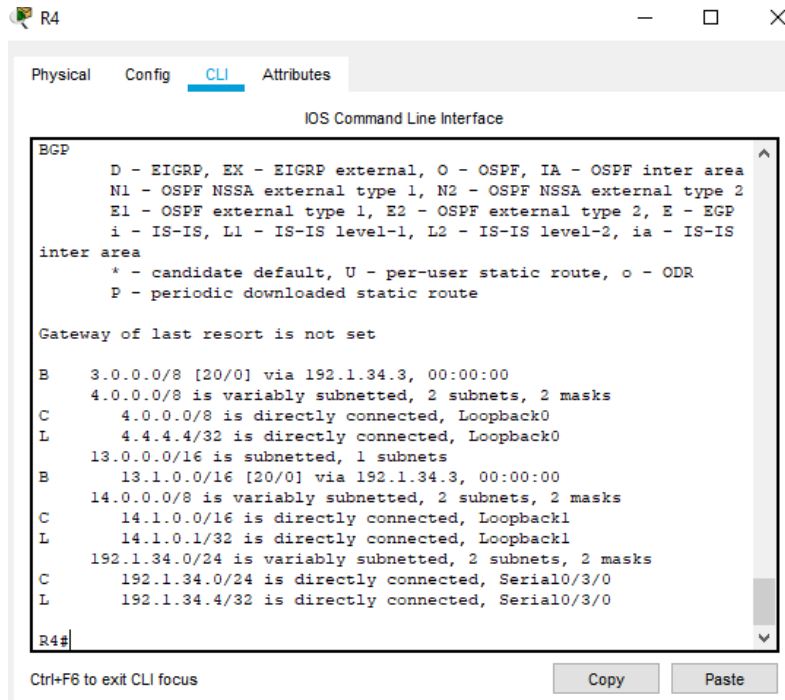
Gateway of last resort is not set

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
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, GigabitEthernet0/0
L   192.1.23.3/32 is directly connected, GigabitEthernet0/0
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.34.0/24 is directly connected, Serial0/3/0
L   192.1.34.3/32 is directly connected, Serial0/3/0

R3#
```

Ilustración 11 Verificación en R3 la relación de vecino BGP con R4

R4# show ip route



```
R4# show ip route
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, E - EGP
i - IS-IS, 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    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
    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
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
    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, Serial0/3/0
L    192.1.34.4/32 is directly connected, Serial0/3/0
R4#
```

Ilustración 12 Verificación en R4 la relación de vecino BGP

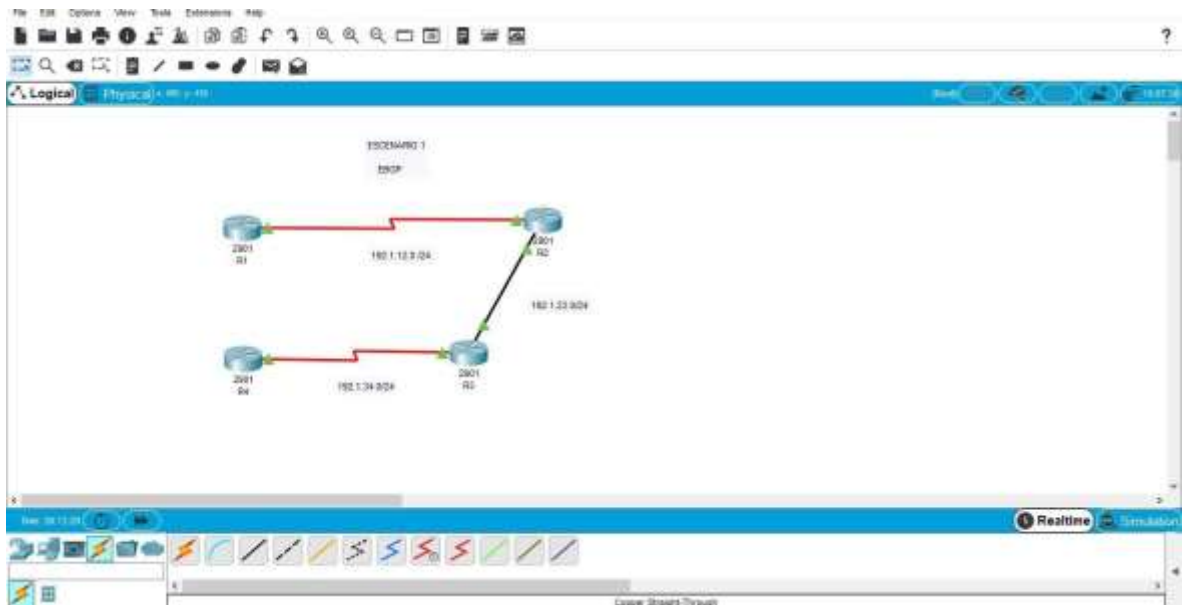


Ilustración 13 Escenario 1 en el programa Packet Tracer

ESCENARIO 2

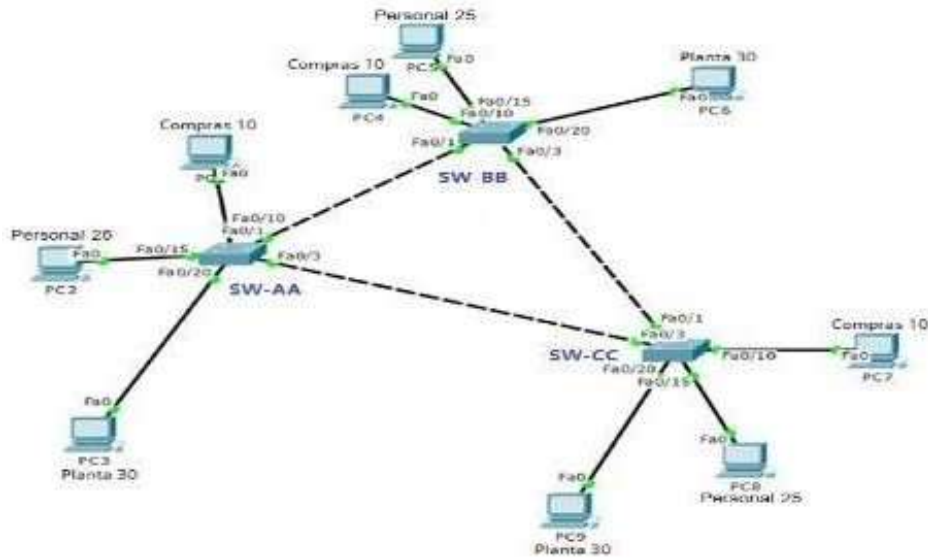


Ilustración 14 Escenario 2

Inicialmente colocamos los switch 2960 en la pantalla principal del programa Packet Tracer. Asignándole a cada uno su nombre correspondiente SW-AA, SW-BB y SW-CC además de colocar tres PC's por cada switch.

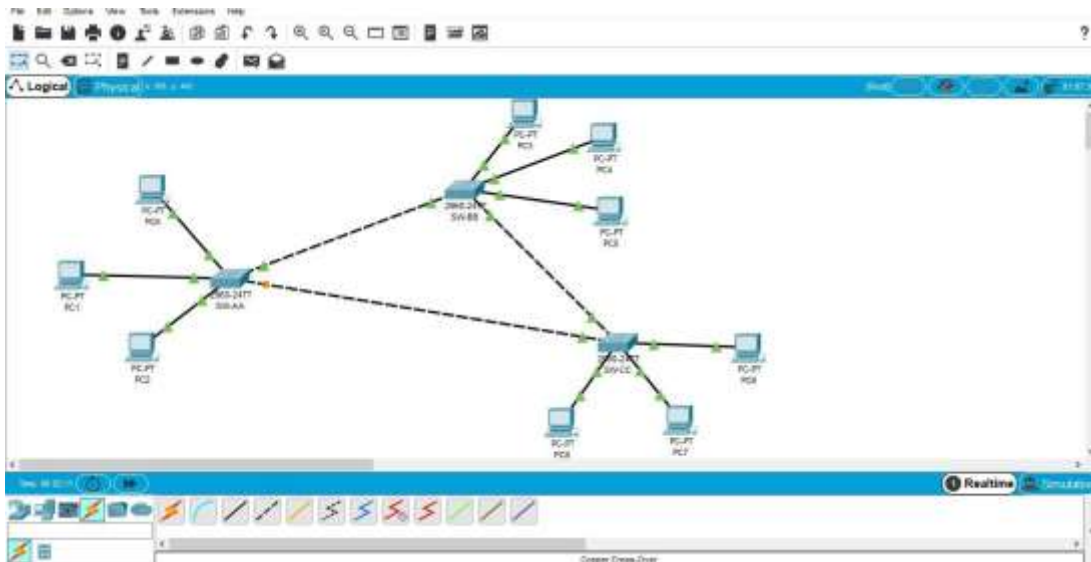


Ilustración 15 Escenario 2 en el Programa Packet Tracer

Hacemos doble clic en el switch SW-AA para realizar inicialmente las configuraciones básicas de un switch.

Primero vamos a la pestaña **CLI**, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando **switch>** que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando **enable** para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado **switch#**.

La primera configuración básica es cambiar el nombre de usuario, en este caso su nombre es switch y lo cambiaremos por medio del comando **hostname** seguido del nombre que le colocaremos al switch, en este caso **SW-AA**.

Ahora le colocamos una contraseña secreta que no se podrá visualizar por medio del comando **enable secret cisco**. Otras configuraciones que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos **line console 0** y **line vty 0 15** enter **password cisco** después tenemos que escribir el comando **login** para que acepte y aplique las contraseñas, para salir de este modo de configuración escribimos el comando **exit**.

Y por último escribimos el comando **service password-encryption** para encriptar las contraseñas enter y escribimos **do write** para guardar los datos.

Luego realizamos las mismas configuraciones en los otros switch colocando el nombre según corresponda.

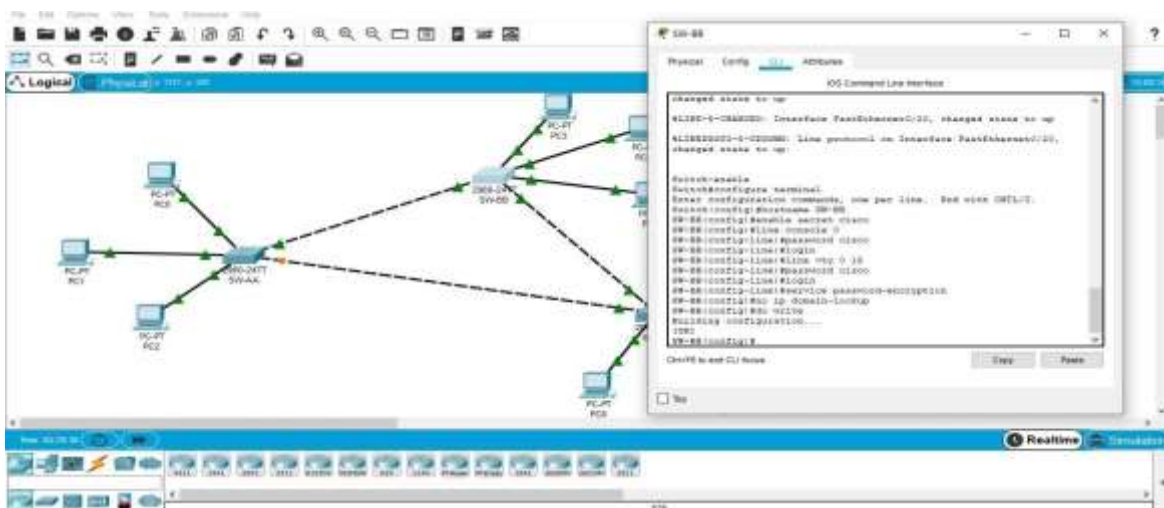


Ilustración 16 Configuraciones básicas de un Switch

A. Configuración VTP

Para realizar la configuración VTP seguimos los siguientes pasos:

1. Configurar el switch SW-BB como servidor por medio del comando **vtp mode server**. Después de escribir ese comando y dar enter podemos observar que el switch por defecto está dispuesto para el modo servidor, pero aun así es importante asegurarnos.

```
SW-BB(config)#vtp mode server
```

2. Configurar el nombre del dominio VTP con el comando **vtp domain CCNA**, donde CCNA es el nombre del dominio.

```
SW-BB(config)#vtp domain CCNA
```

3. Configurar la contraseña de dominio VTP usando el comando **vtp password cisco**, donde cisco es la contraseña.

```
SW-BB(config)# vtp password cisco
```

4. Salir del modo de configuraciones por medio del comando **exit**.

```
SW-BB(config)# exit
```

5. Verificar los cambios de la configuración en el switch SW-BB por medio del comando **show vtp status**, para asegurarnos que el modo server y el dominio se configuraron correctamente.

```
SW-BB(config)# show vtp status
```

6. Configurar el switch SW-AA y SW-CC como clientes VTP por medio del comando **vtp mode client**.

```
SW-AA(config)# vtp  
mode client SW-  
CC(config)# vtp mode  
client
```

7. Configurar el nombre del dominio en estos switch con el comando **vtp domain CCNA**.


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

2. Configurar en el switch SW-BB el puerto FastEthernet 0/1 para enlace trunk. Para ello ingresamos al switch y primero colocamos el comando **interface fa0/1** enter y escribimos el comando **switchport mode trunk**.

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

3. Verificar en el switch SW-AA que sí, se está enlazando por medio del comando **show interface fa0/1 switchport** o **show vtp status**.

```
SW-AA#show interface trunk
```

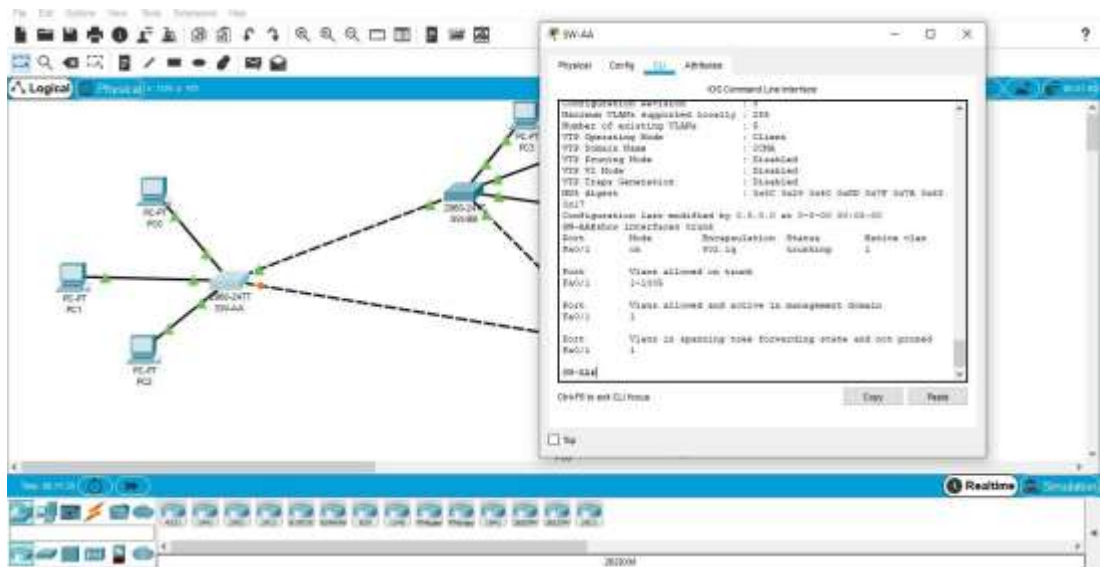


Ilustración 20 Verificación de enlace trunk fa0/1 en el switch SW-AA

- Configurar en el switch SW-AA el puerto FastEthernet 0/3 para enlace trunk. Para ello ingresamos al switch y primero colocamos el comando **interface fa0/3** enter y escribimos el comando **switchport mode trunk**.

```

SW-AA(config)#interface fa0/3
SW-AA(config)# switchport
mode trunk SW-AA(config)# exit

```

- Verificar en el switch SW-AA con el comando **show vtp status**.

```

SW-AA# show vtp status.

```

- Verificar en el switch SW-AA que sí, se está enlazando por medio del comando **show interfaces trunk**.

```

SW-AA# show interfaces trunk.

```

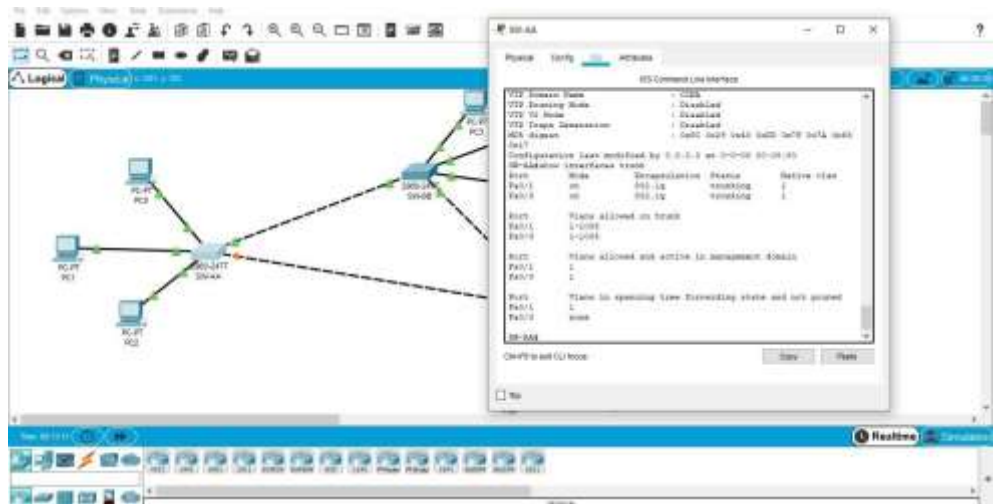


Ilustración 21 Verificación de enlace trunk fa0/3 en el switch SW-AA

7. Configurar en el switch SW-BB el puerto FastEthernet 0/3 para enlace trunk. Para ello ingresamos al switch y primero colocamos el comando **interface fa0/3** enter y escribimos el comando **switchport mode trunk**.

```

SW-BB(config)#interface fa0/3
SW-BB(config)# switchport
mode trunk SW-BB(config)# exit

```

8. Verificar en el switch SW-CC que sí, se está enlazando por medio del comando **show interfaces trunk** o **show vtp status**.

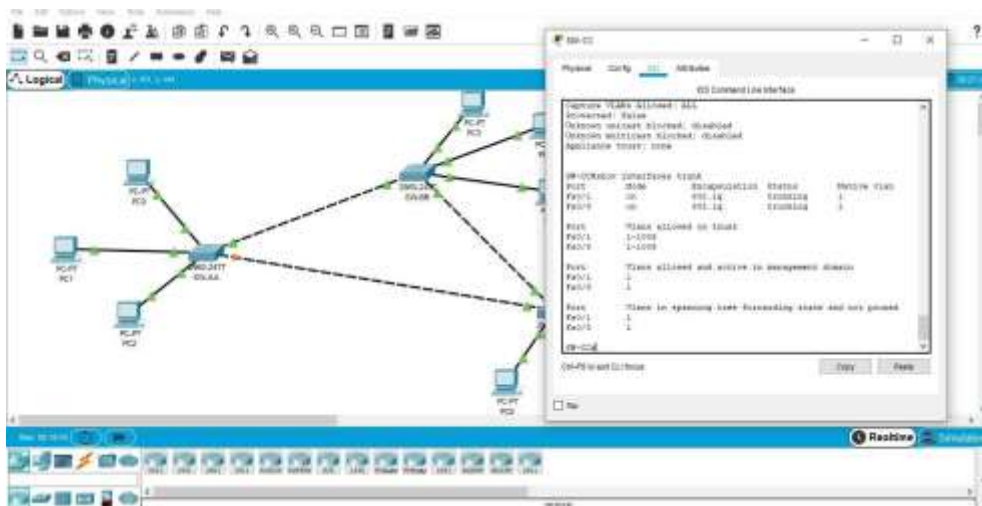


Ilustración 22 Verificación de enlace trunk fa0/3 en el switch SW-BB

C. Asignación de los puertos y Agregar VLANs.

Ahora se empiezan a configurar las vlan que son redes de área local virtuales en la configuración global del switch.

Las VLAN se pueden crear en el servidor VTP y distribuir a otros switch en el dominio VTP, en este caso creamos las 4 VLAN en el servidor VTP de SW-BB y estas VLAN se distribuyen al SW-AA y SW-BB por medio del VTP.

Las vlan se identifican con números desde el 1 al 1005, en caso debemos crear las vlan (10,25,30,99).

1. Crear las vlan en el switch SW-BB, primero entramos en el modo configuración del switch por medio del comando **configure terminal**, damos enter y creamos la primera **vlan 10** enter y con el comando **name** se le asigna un nombre, en este caso sería **name Compras**, luego damos enter para añadir la segunda **vlan 25** enter y le asignamos un nombre **name Personal**, creamos la siguiente VLAN que sería **vlan 30** enter **name Planta** y la última **vlan 99** enter **name Admon**.

```
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
```

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

```
SW-BB# show vlan brief
```

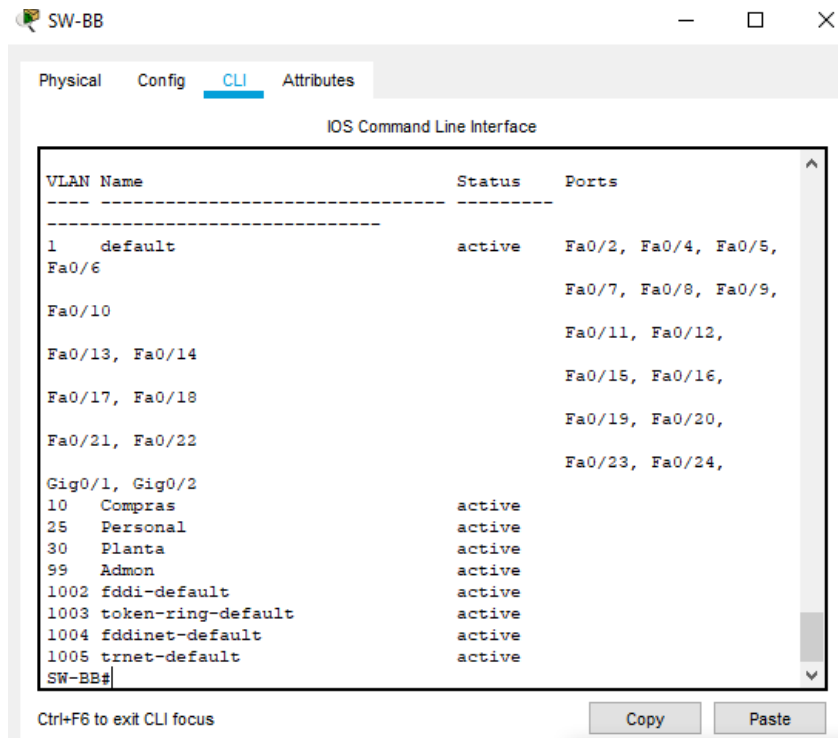


Ilustración 23 Verificación de las vlan en el switch SW-BB

3. 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 . Asignar a cada PC su dirección IP, mascara de RED y puerta de enlace.

4. Asignar las VLAN a los puertos en los switch. Primero ingresamos a la interfaz con el comando **interface fa0/10** según corresponda, seguido del comando **switchport mode access** para establecer el modo de acceso, seguido del comando **switchport Access vlan id** de la vlan a un puerto de acceso, enter y finalmente el comando **no shutdown**, luego continuamos con los mismos comandos para la **interfaz fa0/15** y la **interfaz fa0/20**. El procedimiento se repite según cada switch.

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

```

5. Verificar la configuración de las VLAN y las asignaciones de los puertos por medio del comando **show vlan brief**.

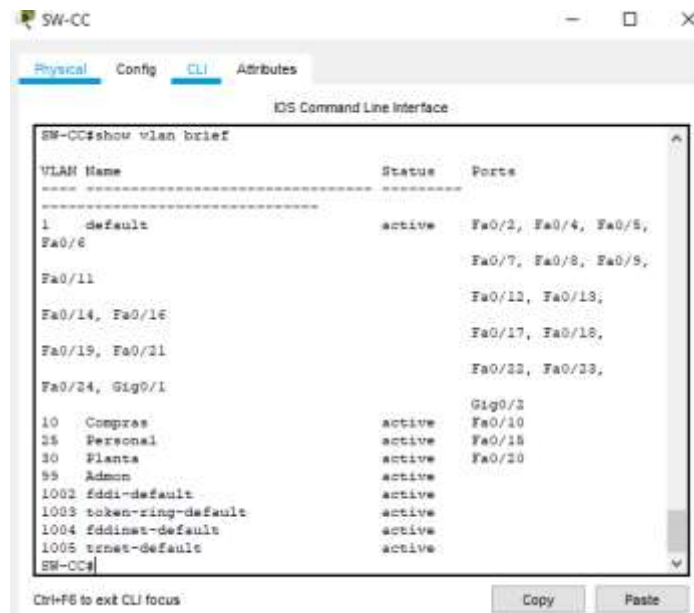


Ilustración 24 Verificación de los puertos en el switch SW-BB

D. Configurar las direcciones IP en cada Switch.

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 . Direcciones IP en cada uno de los Switch.

El procedimiento se repite según cada switch.

1. Ingresar al switch, escribir el comando **configure terminal** para entrar en el modo de configuraciones.

SW-AA#Configure terminal

2. Escribir el comando **interface vlan 99**.

SW-AA(config)#interface vlan 99

3. Por medio del comando **ip address** colocamos la dirección IP y la máscara de red, según corresponda en cada switch.

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

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

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

4. Colocar el comando **no shutdown** para activar la interfaz.

SW-AA(config-if)#no shutdown

E. Verificar la conectividad Extremo a Extremo.

Una vez asignado una IP a cada PC y de haber realizado el procedimiento anterior, procedemos a comprobar si hay comunicación entre los PC's por medio de la opción **Command prompt** que aparece en la pestaña Desktop.

Damos clic, ahora nos aparece una ventana y escribimos **ping** damos espacio y la dirección IP del PC con el que quiero hacer conexión.

1. Ejecutar un Ping desde cada PC a los demás.

Al comprobar la conectividad entre los PC's, se pudo observar que haciendo ping entre los PC's que tienen las mismas vlan. De la siguiente manera y efectivamente si hay comunicación.

- Desde el PC1 hacer ping al PC4 y el PC7.

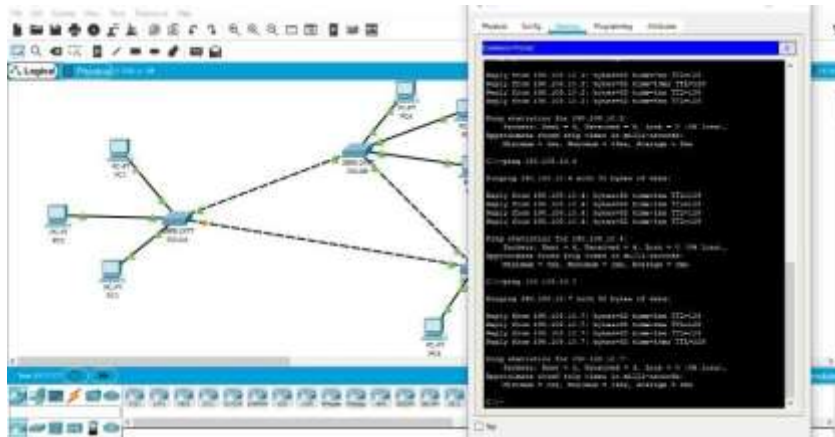


Ilustración 25 Verificación de ping del PC4 al PC7

- Desde el PC2 hacer ping al PC5 y el PC8.

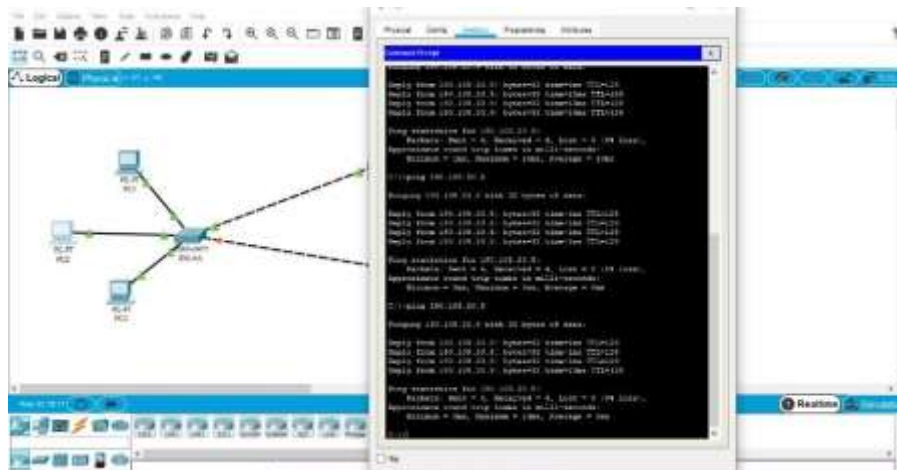


Ilustración 26 Verificación de ping del PC5 al PC8

- Desde el PC3 hacer ping al PC6 y el PC9.

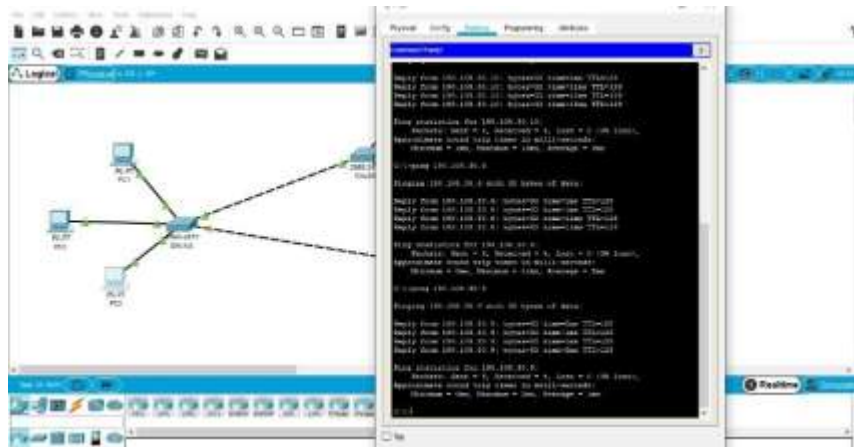


Ilustración 27 Verificación de ping del PC6 al PC9

Mientras que sí, hacemos ping entre los PC's de diferente vlan. De la siguiente manera, comprobamos que no hay comunicación.

- Desde el PC2 hacer ping al PC6.

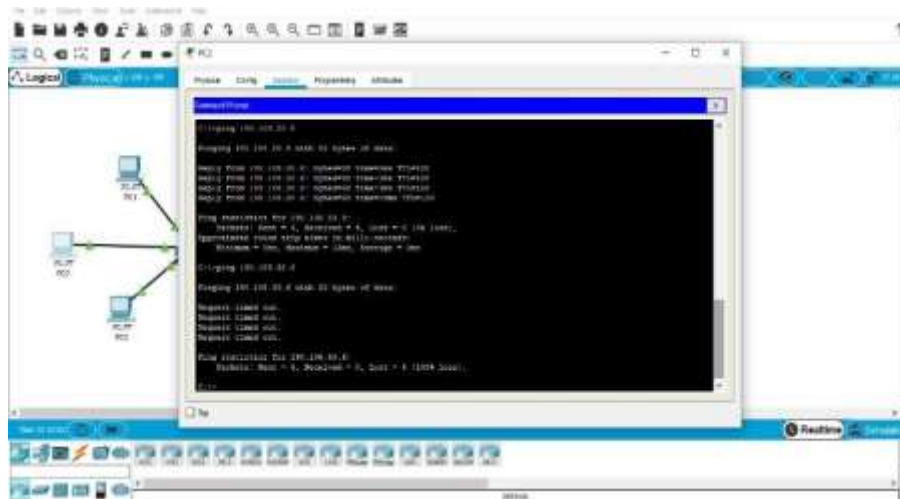


Ilustración 28 Verificación de ping del PC2 al PC6

- Desde el PC7 hacer ping al PC3.

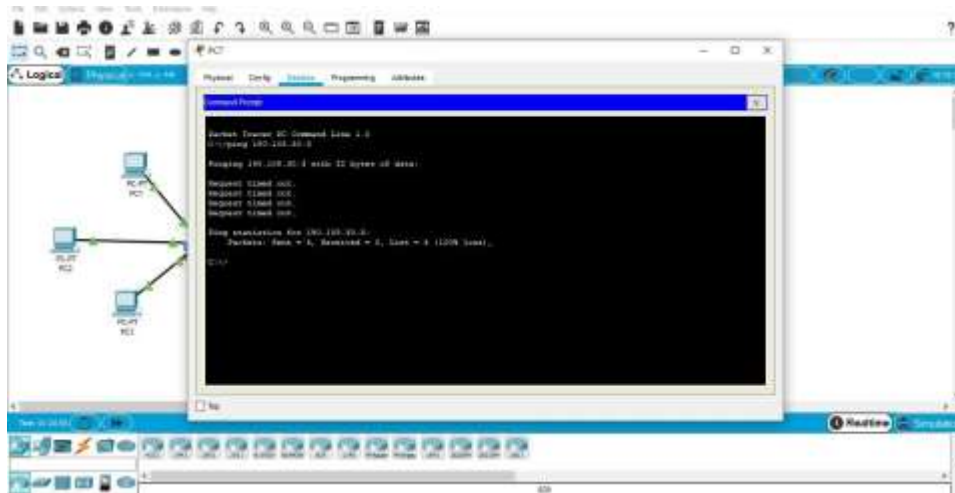


Ilustración 29 Verificación de ping del PC7 al PC3

- Desde el PC9 hacer ping al PC1.

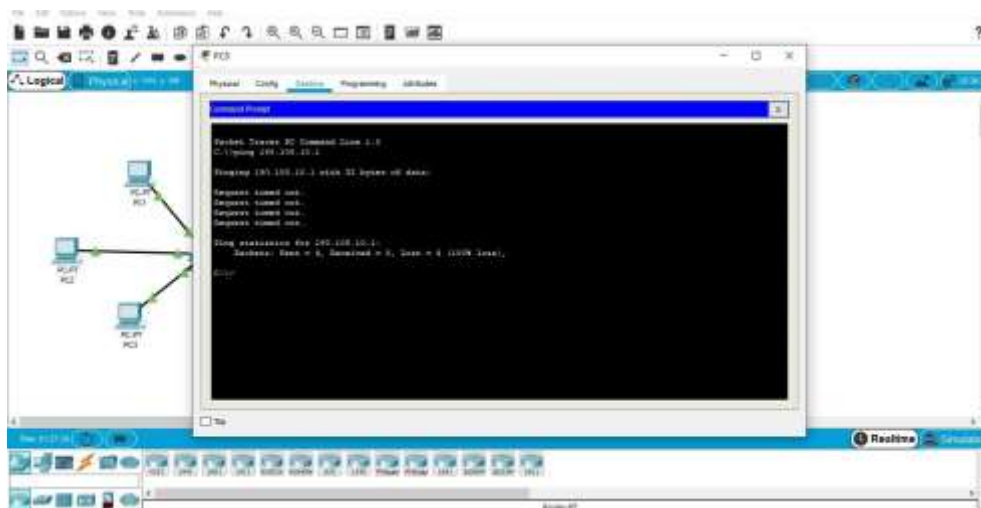


Ilustración 30 Verificación de ping del PC9 al PC1

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

Al comprobar en el switch SW-BB efectivamente tiene éxito ya que se configura una VLAN común para todos que fue la vlan 99, por lo que se tiene comunicación desde este switch a los otros.

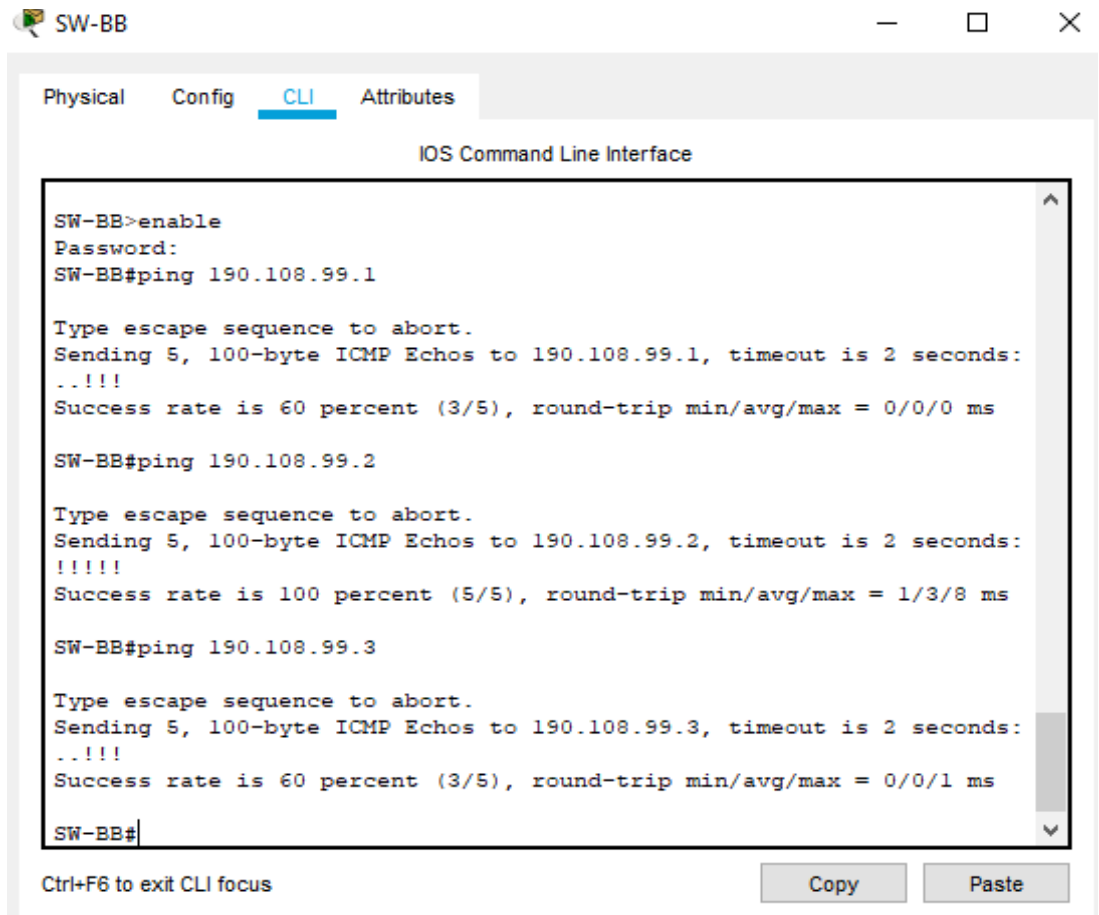


Ilustración 31 Verificación del ping desde el switch SW-BB

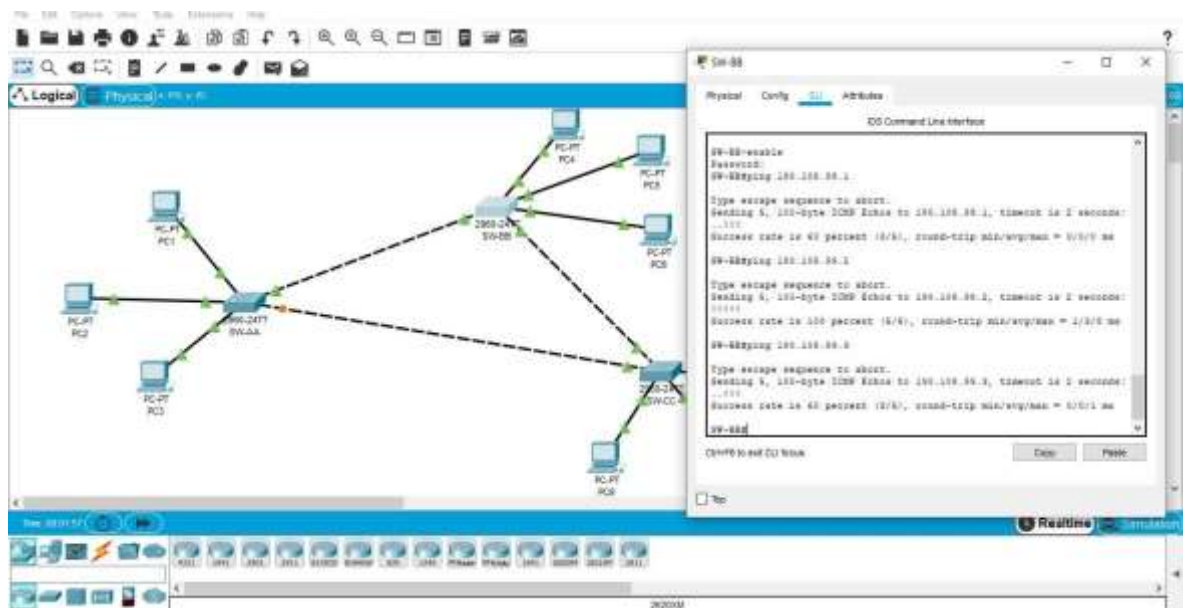
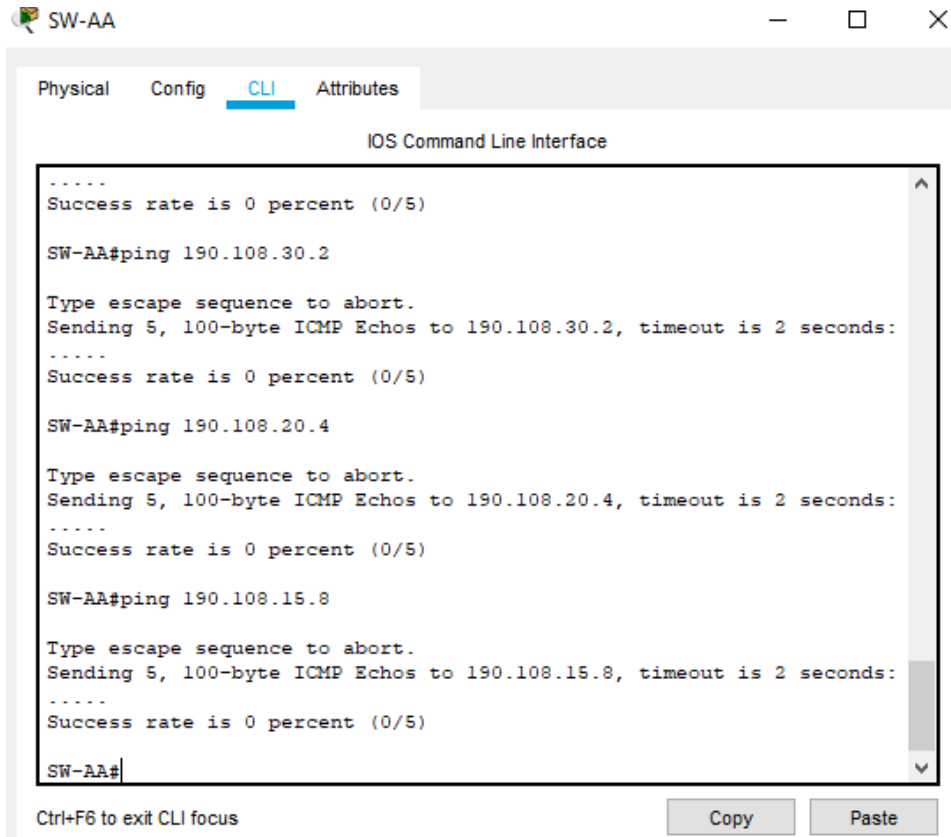


Ilustración 32 Verificación del ping desde los switch

3. Ejecute un Ping desde cada Switch a cada PC.

Al comprobar en los switch **NO** se tuvo éxito, no hay comunicación ya que ni el switch ni el pc tienen configurada una dirección IP, haciendo que los PC's no se encuentren dentro de la red.

La dirección IP es fundamental ya que permite a cada dispositivo ser reconocido dentro de la misma red y así poder enviar y recibir información.



```
SW-AA#ping 190.108.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.15.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.15.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Ilustración 33 Verificación del ping desde el switch SW-AA

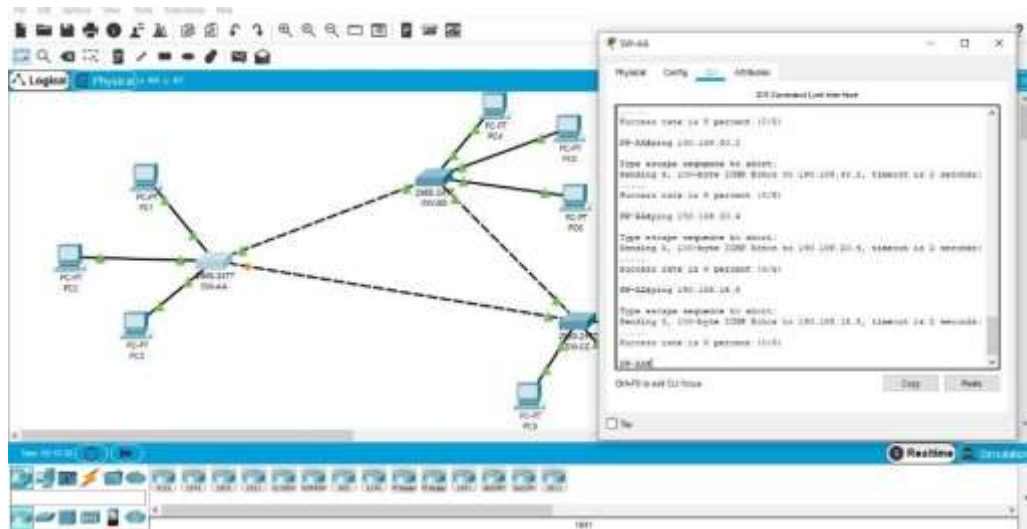


Ilustración 34 Verificación del ping desde los switch a las PC's

CONCLUSIONES

Se desarrolló cada escenario con los respectivos procedimientos de la solución, a través de la herramienta Packet Tracer, logrando obtener la simulación deseada para cada ejercicio propuesto.

La descripción detallada de todo el procedimiento para solucionar los escenarios propuestos permitió aclarar y precisar aún más los conocimientos aprendidos con respecto a los protocolos EIGRP, EBGP OSPF, la redistribución de rutas; en el módulo de CCNP SWITCH, las configuraciones de cada uno de los dispositivos como los Router, los switch, los PC's, además de los procesos de verificación y de conectividad mediante el uso y aprendizaje de los comandos requeridos para llevar a cabo la solución.

A lo largo del diplomado de profundización en CCNP se alcanzaron distintas habilidades de redes y comunicaciones que van orientadas hacia el mundo profesional ya que se abordaron diferentes temas importantes e interesantes en el mundo actual, los cuales permitirán dar soluciones a problemas de conectividad que se presenten con los softwares, para de esta manera garantizar la seguridad de la información en las organizaciones.

A través de la realización de estas simulaciones nos dimos cuenta de las ventajas que tiene una red de comunicaciones, porque al interconectar varios sistemas podemos transportar la información de una manera más fácil y segura.

REFERENCIAS

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). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing 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>

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