DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FREDY YHOAM HERRERA SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
ZIPAQUIRA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FREDY YHOAM HERRERA SANCHEZ

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 – ECBTI
INGENIERÍA ELECTRONICA
ZIPAQUIRA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

ZIPAQUIRA, 22 de mayo de 2020

AGRADECIMIENTOS

Después de un periodo de aprendizaje lleno de angustias e incertidumbres, a causa de un problema que ha sido de magnitud global, escribo este apartado de agradecimientos para finalizar mi diplomado de profundización en CISCO CCNP. Ha sido un curso lleno de conocimientos que aportan a mi crecimiento personal y profesional, es por esto que quiero agradecer a todas aquellas personas que hicieron parte de este bello proceso.

Primero que todo, me gustaría agradecer a mis compañeros de curso, así como a mi Tutor con quienes hemos formado un grupo colaborativo excepcional para el desarrollo de las actividades que fueron planteadas. Particularmente me gustaría nombrar a mi esposa Erika Ballen, quien ha sido una persona con la cual puedo contar en cada paso que doy hacia mi formación como Ingeniero, a ella mucha gracias.

Finalmente agradecer a mis padres y a mi hijo por sus sabios consejos y su comprensión, por la dedicación y la moral que me han ofrecido para salir siempre adelante.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

EIGRP: es un protocolo propiedad de Cisco Systems, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace, es utilizado en redes TCP/IP de interconexión de sistemas abiertos (OSI).

ROUTER: es un dispositivo que permite la conexión de varias redes u ordenadores entre si, este enrutador se vale de un protocolo de enrutamiento para poder comunicarse y compartir información con otros enrutadores de una manera rápida y adecuada.

SWITCH: también conocido como conmutador, es un dispositivo que conecta múltiples equipos entre si para crear una red, en informática se puede considerar como un controlador de interconexión.

VLAN: (red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física, de esta manera el usuario puede obtener varias VLAN dentro de un mismo router o switch.

LAN: es una sigla que se refiere a una red de área local, muy usada por empresas para vincular computadoras que pueden compartir información entre ellas e incluso acceder a un periférico como lo es una impresora.

BGP: es un protocolo que permite crear ruteo de interdominios libre de loops entre sistemas autónomos, utiliza TCP como protocolo de transporte es por esto que se puede considerar que dos routers BGP forman una conexión TCP entre ellos, a estos se conocen como vecinos o “peers”.

RESUMEN

Es parte fundamental para un Ingeniero Electrónico, atacar las problemáticas frecuentes que se presentan en el ámbito tecnológico, es por esto que las herramientas ofrecidas en el curso de profundización CISCO CCNP, permiten el mejoramiento continuo para el desarrollo de las actividades encontradas en el ámbito industrial.

Este trabajo nos permite aplicar los conocimientos que fueron adquiridos al momento de desarrollar cada una de las actividades propuestas, además de abordar los temas de cursos anteriores, aplicándolos mediante el proceso de simulación y ejecución en dos escenarios de trabajo, que pondrán a prueba las habilidades practicas con las cuales se cuenta al finalizar el curso.

A través de las plataformas y los recursos que CISCO nos ofrece, se han evidenciado las características más importantes de conmutación y enrutamiento para redes. Con la adquisición de nuevos conceptos se ha ejecutado el desarrollo de estos escenarios, verificando así la importancia que tiene este tipo de temáticas.

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

ABSTRACT

It is a fundamental part for an Electronic Engineer to attack the frequent problems that arise in the technological field, which is why the tools offered in the CISCO CCNP deepening course allow continuous improvement for the development of activities found in the industrial field .

This work allows us to apply the knowledge that was acquired when developing each of the proposed activities, in addition to addressing the topics of previous courses, applying them through the simulation process and execution in two work scenarios, which will test the skills practices that are available at the end of the course.

Through the platforms and resources that CISCO offers us, the most important switching and routing characteristics for networks have been demonstrated. With the acquisition of new concepts, the development of these scenarios has been executed, thus verifying the importance of this type of theme.

Key Words: CISCO, CCNP, Routing, Switching, Networks, Electronics

INTRODUCCION

En el desarrollo de este trabajo se abordaron dos escenarios, diseñados como actividad final del curso diplomado de profundización CISCO CCNP, que permiten mostrar las habilidades adquiridas para el desarrollo de temáticas tales como la conmutación y el enrutamiento dentro de las redes.

Gracias a las herramientas brindadas dentro del curso, en especial el software Packet Tracer de CISCO, se pudo ejecutar la configuración de cada uno de los dispositivos que están dentro de los escenarios, verificando su funcionalidad y observando el comportamiento de cada uno a través de la interfaz presentada por dicho software.

Cabe resaltar la importancia que tiene el uso de los protocolos de enrutamiento, así pues, para el desarrollo de la actividad, se muestran las figuras con la arquitectura de cada escenario y la comprobación de comandos que permiten establecer el buen desarrollo en las programaciones realizadas a los dispositivos, también se muestra detalladamente cada línea de configuración con el fin de dar claridad a los procedimientos que se establecen dentro del escenario propuesto.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

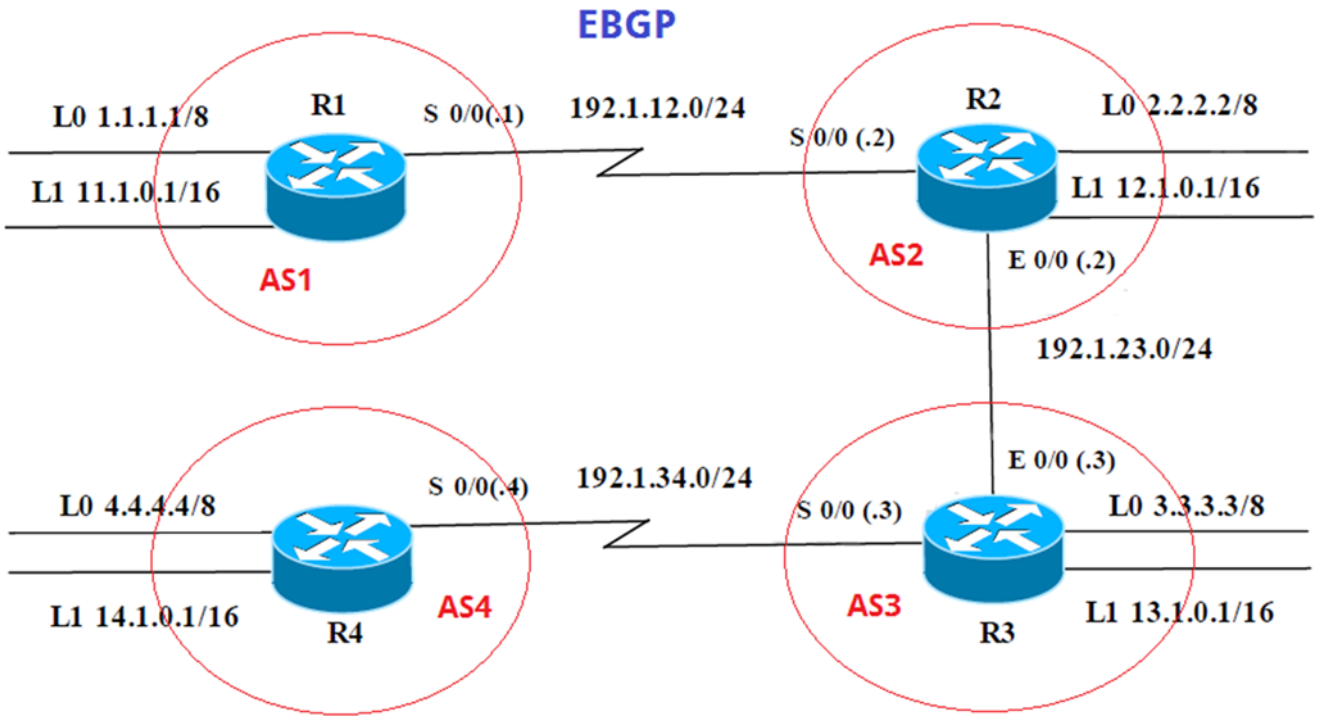


Tabla 1. Información para configuración de R1

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

Tabla 2. Información para configuración de 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

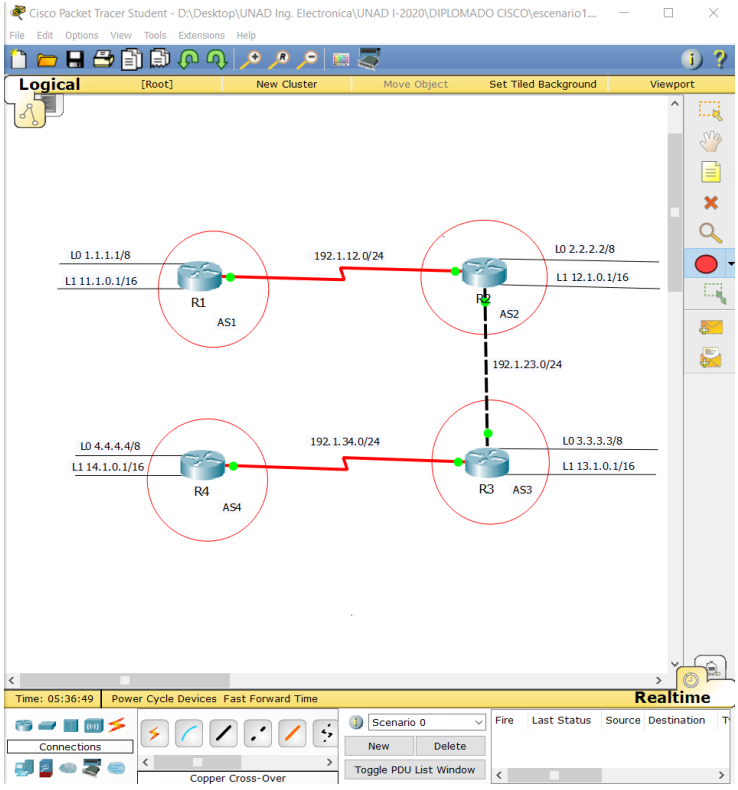
Tabla 3. Información para configuración de R3

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

Tabla 4. Información para configuración de 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

Figura 2. Simulación de Escenario 1



1.1. 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.***

Empezamos habilitando y configurando el hostname de cada Router:

R1
Router>enable *ingreso a modo privilegiado*
Router#config t *ingreso al modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1 *asigno el nombre del Router*
R1(config)#

R2
Router>enable *ingreso a modo privilegiado*
Router#config t *ingreso al modo configuracion*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2 *asigno el nombre del Router*
R2(config)#

R3
Router>enable *ingreso a modo privilegiado*
Router#config t *ingreso al modo configuracion*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3 *asigno el nombre del Router*
R3(config)#

R4
Router>enable *ingreso a modo privilegiado*
Router#config t *ingreso al modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4 *asigno el nombre del Router*
R4(config)#

Debemos ingresar las redes que pertenecen al vecindario BGP1

R1(config)#router bgp 1 *habilita el BGP en el router*
R1(config-router)#network 1.1.1.1 mask 255.0.0.0 *anunciamos las direcciones loopback*
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#bgp router-id 22.22.22.22 *definimos la ID del router BGP*
R1(config-router)#end

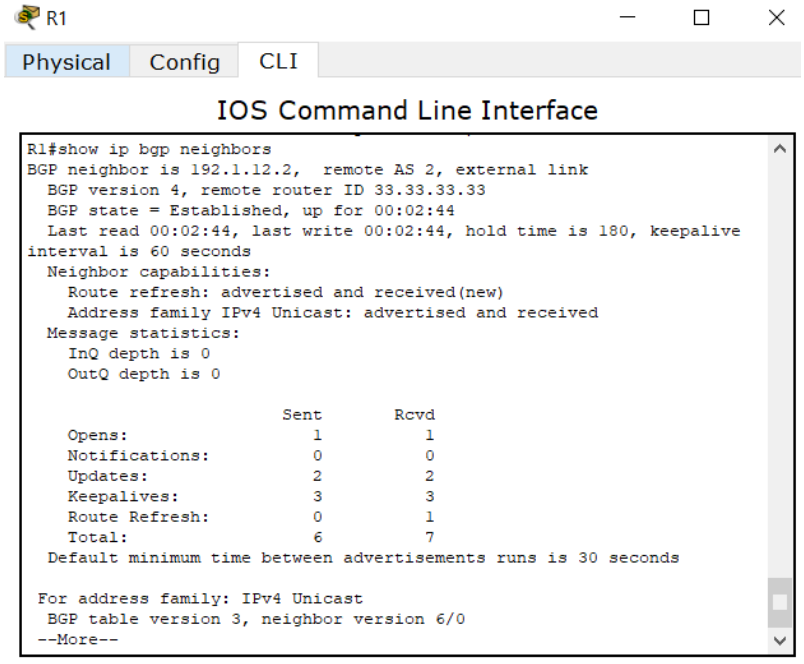
Debemos ingresar las redes que pertenecen al vecindario BGP2

R2(config)#router bgp 2 *habilita el BGP en el router*
R2(config-router)#network 2.2.2.2 mask 255.0.0.0 *anunciamos las direcciones loopback*
R2(config-router)#network 12.1.0.1 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#bgp router-id 33.33.33.33 *definimos la ID del router BGP*
R2(config-router)#end

Establecemos los vecinos por medio del siguiente comando para R1 y R2

R1(config-router)#neighbor 192.1.12.2 remote-as 2 *establecemos la conexión TCP*
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
R2(config-router)#neighbor 192.1.12.1 remote-as 1 *establecemos la conexión TCP*
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

Figura 3. Comando Show ip bgp neighbors R1



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

Se realiza la configuración de las redes en BGP 3

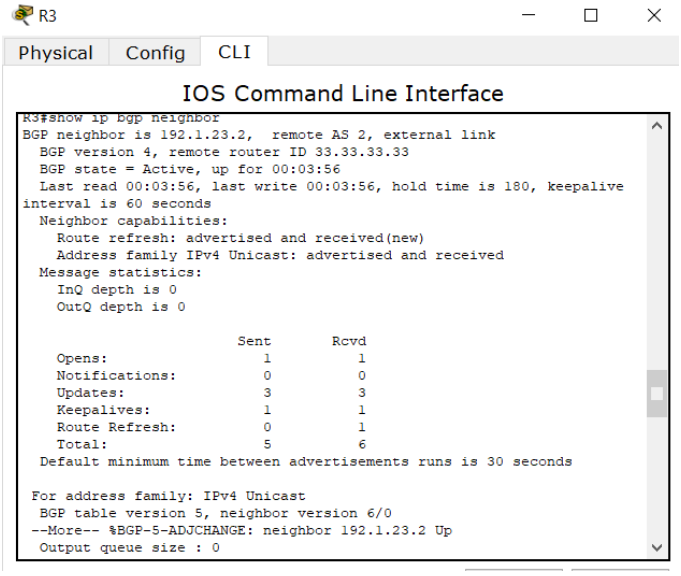
R3(config)#router bgp 3 *habilita el BGP en el router*
R3(config-router)#network 3.3.3.3 mask 255.0.0.0 *anunciamos las direcciones loopback*
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#bgp router-id 44.44.44.44 *definimos la ID del router BGP*

Se procede a establecer las conexiones con el vecino BGP entre R2 y R3

R2(config)#router bgp 2 *habilita el BGP en el router*
R2(config-router)#network 192.1.23.0 mask 255.255.255.0 *anunciamos la dirección loopback*

R2(config-router)#neighbor 192.1.23.3 remote-as 3 *establecemos la conexión TCP*
R3(config-router)#neighbor 192.1.23.2 remote-as 2 *establecemos la conexión TCP*

Figura 4. Comando Show ip bgp neighbors R3



1.3. 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.

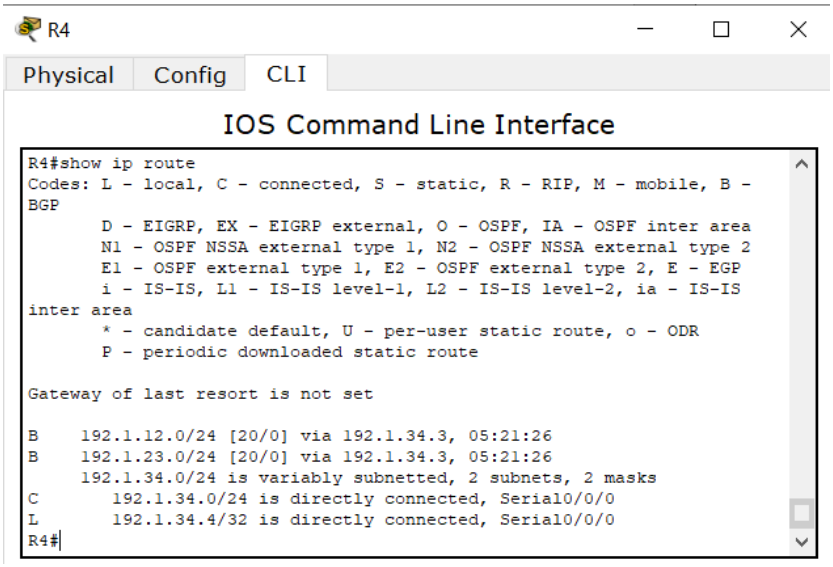
Se procede a configurar R4, para mostrar cada una de las redes solicitadas:

R4(config)#router bgp 4 *habilita el BGP en el router*
R4(config-router)#network 4.4.4.4 mask 255.0.0.0 *anunciamos las direcciones loopback*
R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#bgp router-id 66.66.66.66 *definimos la ID del router BGP*

Se establece la conexión con el vecino BGP para R3 y R4

R3(config)#router bgp 3 *habilita el BGP en el router*
R3(config-router)#neighbor 192.1.34.4 remote-as 4 *establecemos la conexión TCP*
R4(config-router)#neighbor 192.1.34.3 remote-as 3 *establecemos la conexión TCP*
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up

Figura 5. Comando Show ip route R4



2. ESCENARIO 2

Figura 6. Escenario 2

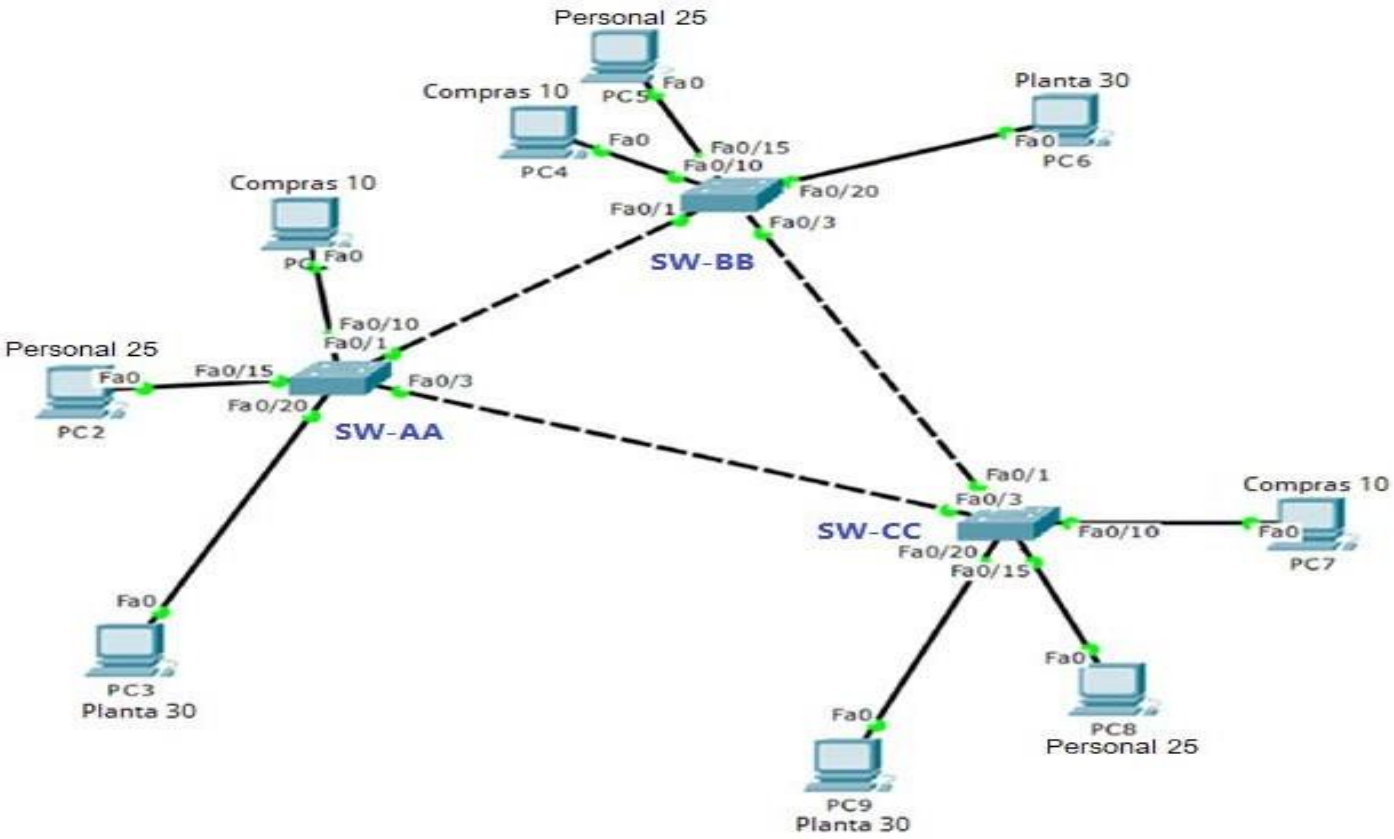
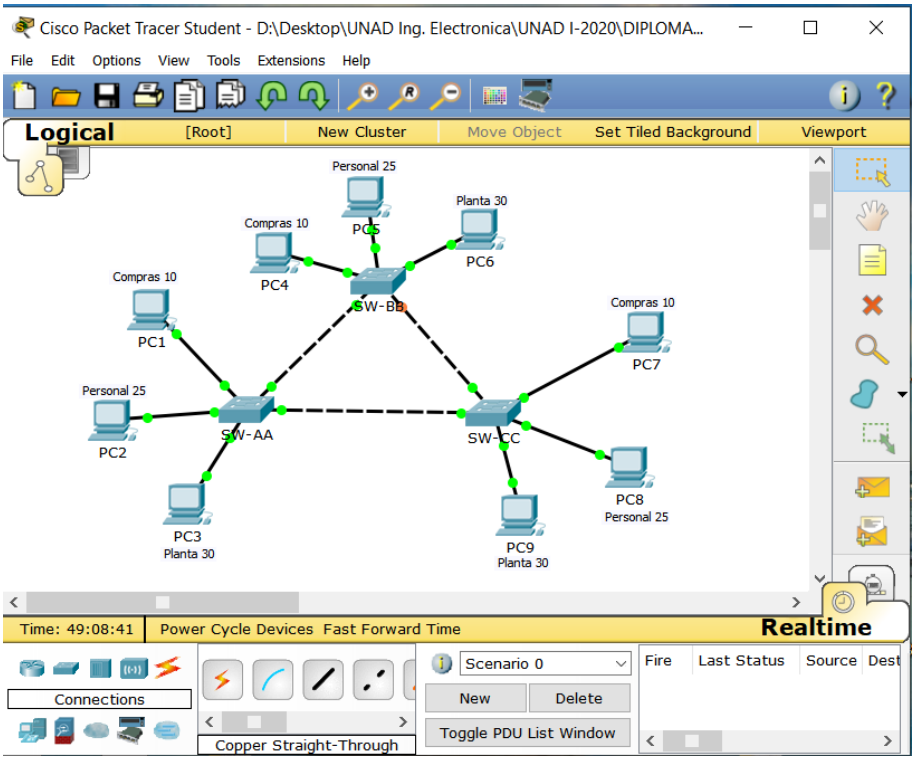


Figura 7. Simulación del escenario 2



A. Configurar VTP

2.1. 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.

Empezamos a configurarlos switches:

SW-AA

Switch>enable *ingreso a modo privilegiado*
Switch#config terminal *ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA *asigno nombre del switch*
SW-AA(config)#vtp domain CCNP *asigno nombre del dominio*
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp mode client *configuramos el switch en modo cliente*

Setting device to VTP CLIENT mode.
SW-AA(config)#vtp password cisco *asignamos la contraseña cisco*
Setting device VLAN database password to cisco

SW-BB

Switch>enable *ingreso a modo privilegiado*
Switch#config terminal *ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB *asigno nombre del switch*
SW-BB(config)#vtp domain CCNP *asigno nombre del dominio*
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp mode server *configuramos el switch en modo servidor*
Device mode already VTP SERVER.
SW-BB(config)#vtp password cisco *asignamos la contraseña cisco*
Setting device VLAN database password to cisco

SW-CC

Switch>enable *ingreso a modo privilegiado*
Switch#config terminal *ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC *asigno nombre del switch*
SW-CC(config)#vtp domain CCNP *asigno nombre del dominio*
Changing VTP domain name from client to CCNP
SW-CC(config)#vtp mode client *configuramos el switch en modo cliente*
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco *asignamos la contraseña cisco*
Password already set to cisco

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

Figura 8. Show vtp status en SW-AA

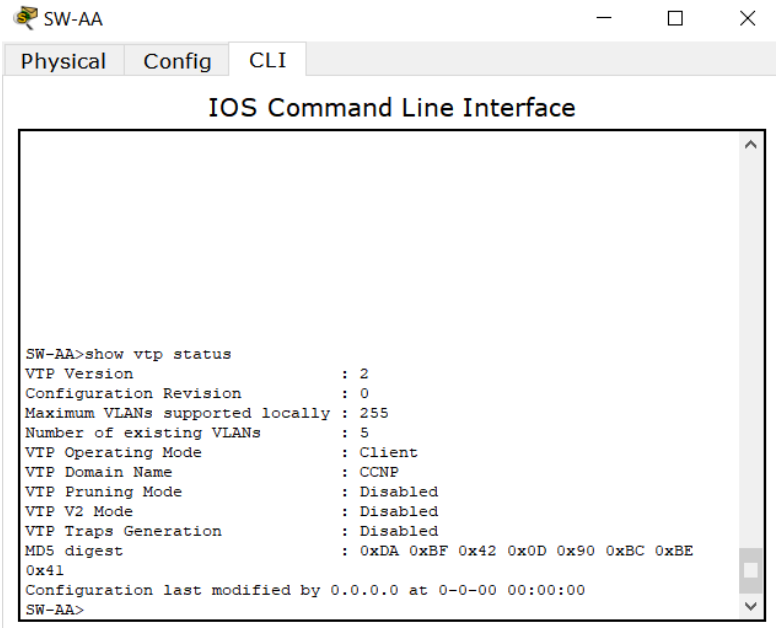


Figura 9. Show vtp status en SW-BB

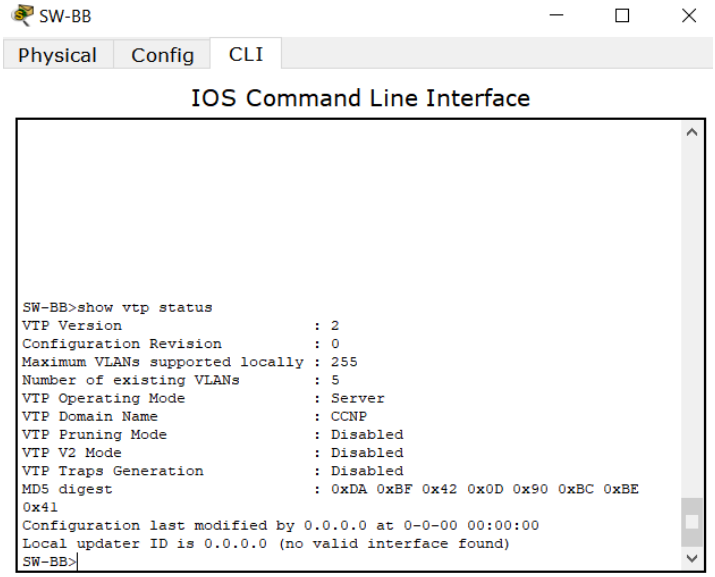
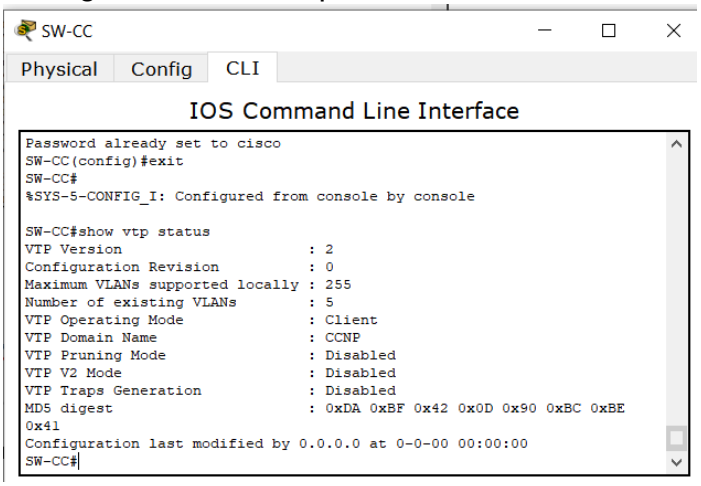


Figura 10. Show vtp status en SW-CC



B. Configurar DTP (Dynamic Trunking Protocol)

2.2. 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***.

Se configura los enlaces troncales en los switch dejando la configuración del ***dynamic desirable*** en SW-AA

SW-AA

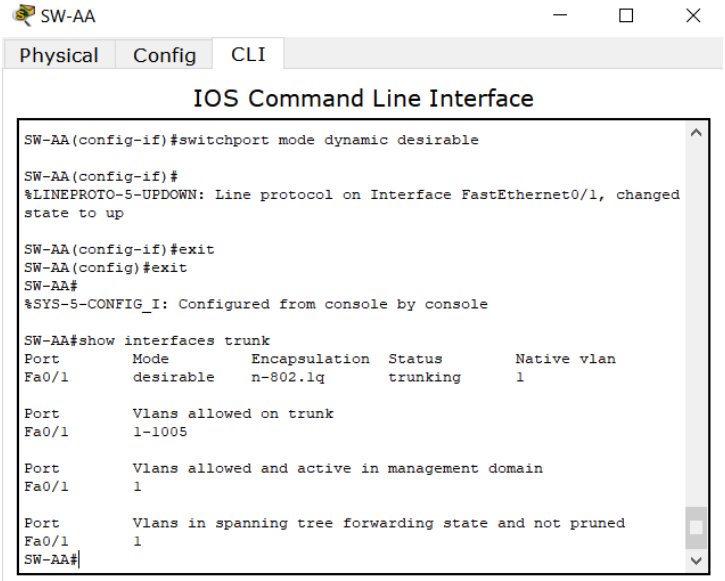
SW-AA(config)#interface fa0/1 *modo configuración del puerto ethernet 0/1*
SW-AA(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal*
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
SW-AA(config-if)#switchport mode dynamic desirable *configuramos el enlace troncal dinamico*
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SW-BB

SW-BB(config)#interface fa0/1 *modo configuración del puerto ethernet 0/1*
SW-BB(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal*
SW-BB(config-if)#

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

Figura 11. Show interfaces trunk en SW-AA



2.4. 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

Se realiza la aplicación del comando en los dos switchs

SW-AA

SW-AA#config terminal *ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fa0/3 *modo configuración del puerto ethernet 0/3*
SW-AA(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal estático*
SW-AA(config-if)#

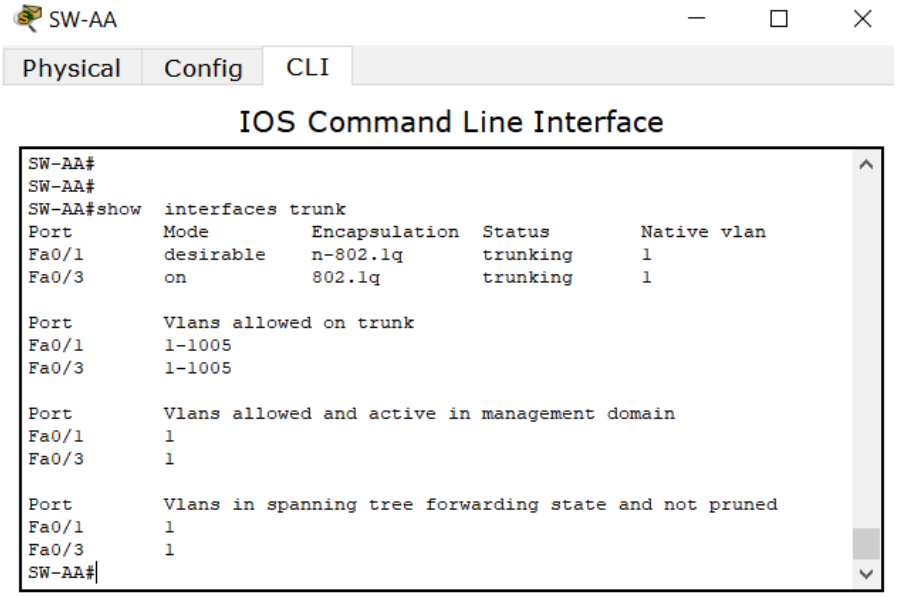
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to

SW-BB

SW-BB#config terminal *ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface fa0/3 *modo configuración del puerto ethernet 0/3*
SW-BB(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal estático*
SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

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

Figura 12. Show interfaces trunk en SW-AA



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

Se realiza la aplicación del comando en los dos switchs

SW-BB

SW-BB(config)#interface fa0/3 *modo configuración del puerto ethernet 0/3*
SW-BB(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal estático*
SW-BB(config-if)#

SW-CC

SW-CC(config)#interface fa0/1 *modo configuración del puerto ethernet 0/1*
SW-CC(config-if)#switchport mode trunk *configuramos el puerto como enlace troncal*
SW-CC(config-if)#

Agregar VLANs y asignar puertos.

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

Agregamos las VLAN en los Switchs

SW-AA

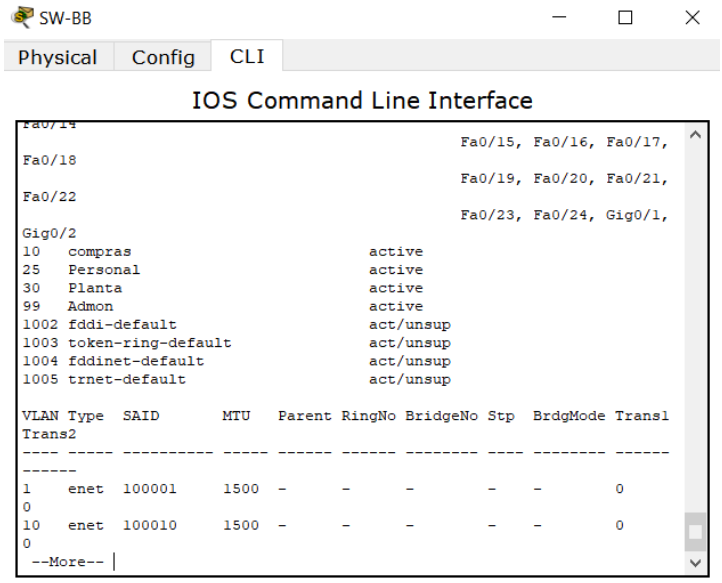
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#

SW-BB

SW-BB(config)#vlan 10 *configuramos como vlan 10*
SW-BB(config-vlan)#name compras *damos el nombre a la vlan 10*
SW-BB(config-vlan)#vlan 25 *configuramos como vlan 25*
SW-BB(config-vlan)#name Personal *damos el nombre a la vlan 25*
SW-BB(config-vlan)#vlan 30 *configuramos como vlan 30*
SW-BB(config-vlan)#name Planta *damos el nombre a la vlan 30*
SW-BB(config-vlan)#vlan 99 *configuramos como vlan 99*
SW-BB(config-vlan)#name Admon *damos el nombre a la vlan 99*

2.7. Verifique que las VLANs han sido agregadas correctamente.

Figura 13. Show vlan en SW-BB



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

Tabla 5. Interfaz, VLAN y Direcciones IP de los PCs

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

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

Se configura en cada uno de los Switchs

SW-AA

SW-AA(config)#interface fa0/10 *modo configuración del puerto ethernet 0/10*
SW-AA(config-if)#switchport access vlan 10 *configuramos el puerto para acceso vlan 10*
SW-AA(config-if)

SW-BB

SW-BB(config)#interface fa0/10 *modo configuración del puerto ethernet 0/10*
SW-BB(config-if)#switchport access vlan 10 *configuramos el puerto para acceso vlan 10*
SW-BB(config-if)#

SW-CC

SW-CC(config)#interface fa0/10 *modo configuración del puerto ethernet 0/10*
SW-CC(config-if)#switchport access vlan 10 *configuramos el puerto para acceso vlan 10*
SW-CC(config-if)#

2.10. 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 PCs de acuerdo con la tabla de arriba.

SW-AA

SW-AA(config)#interface fa0/15 *modo configuración del puerto ethernet 0/15*
SW-AA(config-if)#switchport access vlan 25 *configuramos el puerto para acceso vlan 25*
SW-AA(config-if)#exit *salimos de la configuración del puerto*
SW-AA(config)#interface fa0/20 *modo configuración del puerto ethernet 0/20*
SW-AA(config-if)#switchport access vlan 30 *configuramos el puerto para acceso vlan 30*

SW-BB

SW-BB(config)#interface fa0/15 *modo configuración del puerto ethernet 0/15*
SW-BB(config-if)#switchport access vlan 25 *configuramos el puerto para acceso vlan 25*
SW-BB(config-if)#exit *salimos de la configuración del puerto*
SW-BB(config)#interface fa0/20 *modo configuración del puerto ethernet 0/20*
SW-BB(config-if)#switchport access vlan 30 *configuramos el puerto para acceso vlan 30*

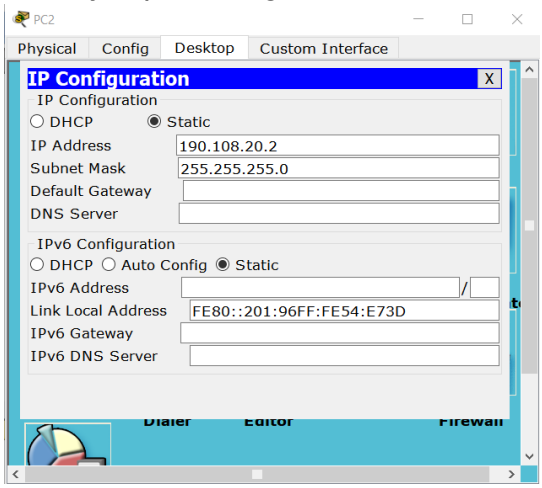
SW-CC

SW-CC(config)#interface fa0/15 *modo configuración del puerto ethernet 0/15*
SW-CC(config-if)#switchport access vlan 25 *configuramos el puerto para acceso vlan 25*
SW-CC(config-if)#exit *salimos de la configuración del puerto*
SW-CC(config)#interface fa0/20 *modo configuración del puerto ethernet*

0/20
SW-CC(config-if)#switchport access vlan 30 *configuramos el puerto para acceso vlan 30*

La configuración de la IP en los pc se ha realizado de acuerdo a la tabla anterior, como ejemplo tenemos la siguiente imagen:

Figura 14. Ejemplo configuración IP en los PC



C. Configurar las direcciones IP en los Switches.

2.11. 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 6. Direccionamiento para los switch

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

Se realiza la configuración en cada uno de los Switchs

SW-AA
SW-AA(config)#interface vlan 99 *modo configuración vlan 99*

SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0 *agregamos dirección IP*
SW-AA(config-if)#no shutdown *activamos la interfaz*
SW-AA(config-if)#exit *salimos*

SW-BB

SW-BB(config)#interface vlan 99 *modo configuración vlan 99*
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0 *agregamos dirección IP*
SW-BB(config-if)#no shutdown *activamos la interfaz*
SW-BB(config-if)#exit

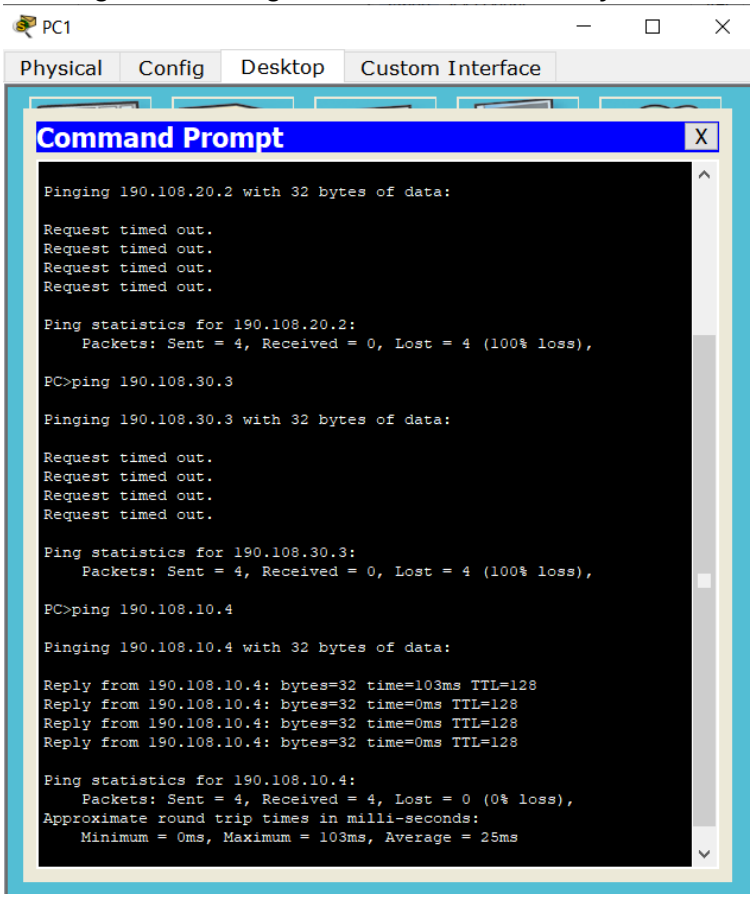
SW-CC

SW-CC(config)#interface vlan 99 *modo configuración vlan 99*
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0 *agregamos dirección IP*
SW-CC(config-if)#no shutdow *activamos la interfaz*
SW-CC(config-if)#exit *salimos*

D. Verificar la conectividad Extremo a Extremo

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

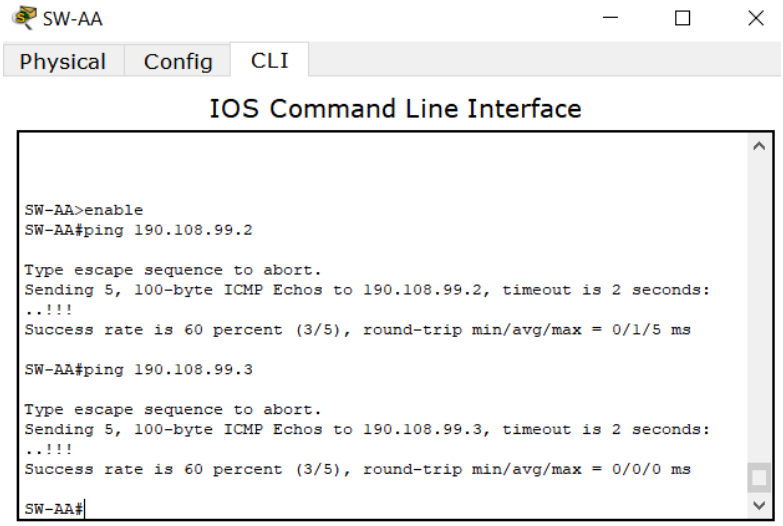
Figura 15. Ping PC1 hacia PC2, PC3 y PC4



Al realizar ping desde el PC1 hacia el PC2 y PC3 no es posible obtener una respuesta, debido a que estos PC se encuentran en una VLAN diferente, esto se pudo comprobar cuando hacemos ping de PC1 hacia PC4 y PC7 que están dentro de la misma VLAN existe una respuesta de enrutamiento.

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

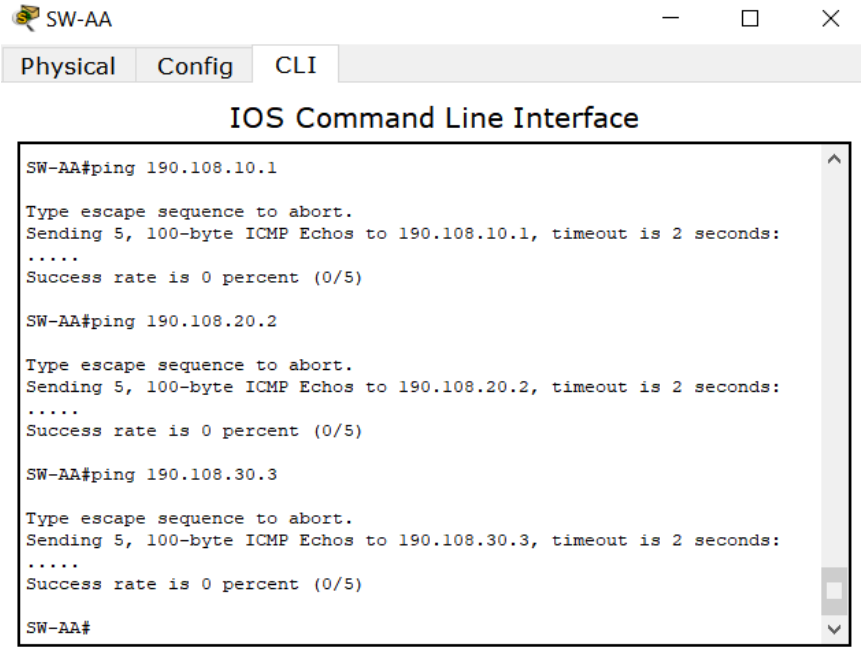
Figura 16. Ping SW-AA hacia SW-BB y SW-CC



Al realizar ping entre los switchts se puede apreciar que existe comunicación debido a que se ha configurado las direcciones IP dentro de la misma VLAN.

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

Figura 17. Ping de SW-AA hacia los PC



Al realizar ping de cualquiera de los switchs hacia los PC se puede verificar que

no existe ninguna respuesta, debido a que no se ha configurado ninguna de las direcciones IP de los PC en la VLAN que fue asignada para los switchs.

CONCLUSIONES

En el desarrollo del curso diplomado de profundización CISCO CCNP, se logró observar la importancia que tiene cada una de las temáticas abordadas, para lograr con éxito la configuración y el montaje de escenarios o topologías de red que son muy frecuentes en el ámbito laboral.

El software PACKET TRACER, es una herramienta fundamental para el desarrollo de las actividades, es muy amigable por su interfaz, además proporciona un aspecto muy amigable al momento de ejecutar las simulaciones, como por ejemplo él envió de datos.

Las habilidades alcanzadas en el curso, afianzan los conocimientos que fueron adquiridos en cursos anteriores.

Se logra comprender en cada uno de los módulos la importancia de los protocolos de comunicación, en especial el EIGRP y OSPF.

La aplicación de VLAN, acceso de usuarios y la configuración global de un switch es de gran ayuda para formar grandes redes multidispositivo.

Sin duda el manejo activo de estas temáticas, fortalece y enriquece la formación académica para el Ingeniero Electrónico, manteniéndolo siempre dispuesto y con todo el conocimiento al momento de enfrentar problemáticas relacionadas con estos temas.

BIBLIOGRAFIA

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

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Soto, E. (2008). Soporte de Tecnologias CISCO. Notas Tecnicas de Troubleshooting. Estudio de casos BGP. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

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