DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ALEJANDRO ROZO ONOFRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA ELECTRONICA

TOCANCIPA

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ALEJANDRO ROZO ONOFRE

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
TOCANCIPA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

TOCANCIPA, 22 de mayo de 2020

AGRADECIMIENTOS

A mis padres quienes me han motivado y apoyado sin descanso en cada uno de mis propósitos, logros y caídas, son la base de la persona que soy y seré en un futuro, gracias por sus consejos y enseñanzas siempre estaré inmensamente agradecido con ustedes.

A mis hermanos que al igual que yo hemos estado en una fase de aprendizaje constante, donde nos descubrimos como personas y profesionales, nuestros caminos siempre estarán unidos y solo miraremos atrás para nunca olvidar nuestras raíces

Al amor de mi vida quien cambio la forma en que veía el mundo siempre ayudándome hacer mejor persona, es un logro compartido y espero que los próximos agradecimientos en los que nos mencionen sean en tu grado.

A todos mis profesores por su paciencia, dedicación y forma de ver la vida, cambiando una por una la mente de sus estudiantes, por querer que nos superemos e implantarnos esa curiosidad por entender el mundo.

Cuando los sacrificios son grandes la satisfacción es infinita, la constancia, disciplina y perseverancia traen siempre buenos resultados.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL: es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Bloquea o permite que los usuarios accedan a los recursos específicos. Un ACL contiene los host que permiten el acceso o la negación al dispositivo de red. El router o el Switch examinan cada paquete para determinar si remitir o declinar el paquete, en base de los criterios especificados dentro de las listas de acceso. Los criterios de una lista de acceso pueden ser la dirección de origen del tráfico, la dirección destino del tráfico, el Upper-Layer Protocol u otra información.

Loopback: Es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y por lo tanto nunca se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento. Es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.

EEE 802.1X: Protocolo para el control de acceso y de autenticación que restringe los dispositivos no autorizados en la conexión con un LAN a través de los puertos públicos accesibles. 802.1x controla el acceso a la red por medio de la creación de dos puntos de acceso virtual distintas en cada puerto. Un Punto de acceso es un puerto incontrolado; el otro es un puerto controlado. Todo el tráfico a través del puerto único está disponible para ambos puntos de acceso. 802.1x autentica cada dispositivo del usuario que esté conectado con un puerto del switch y asigna el puerto a un VLAN antes de que haga disponible cualquier servicio que sea ofrecido por el Switch o el LAN.

Vlan: Son un mecanismo para permitir que los administradores de red creen dominios de broadcast lógicos que pueden abarcar un solo switch o varios switches múltiples, sin importar la proximidad física. Esta función es útil para reducir los tamaños de los dominios de broadcast o para permitir que los grupos o los usuarios se agrupen lógicamente sin necesidad de estar situados físicamente en el mismo lugar.

BGP: Es un protocolo de gateway exterior que permite que los Sistemas Autónomos intercambien información de ruteo entre sí. Un sistema autónomo es un conjunto de Routers bajo sola administración técnica. Los números de Sistema autónomo (AS) son asignados por el registro americano para los números de Internet.

RESUMEN

Las prácticas presentadas en este documento son el resultado de la apropiación de conocimientos en redes de comunicación, desde el diseño, creación, expansión y resolución de errores, todos los parámetros básicos de configuración de router se pudieron aplicar en el escenario 1 de este laboratorio así como la creación de un protocolo BGP para compartir las listas de acceso entre los equipos.

El análisis de redes requiere de la optimización de los recursos por ello se aplica un enlace troncal para el escenario 2 de comunicación entre switches, así mismo para redes independientes se crearon Vlan para comunicar dispositivos de comunicación final en este caso PCs, aunque todos estos parámetros se configuraron exitosamente, se evidencia que falta la asignación de ip para que las Vlan funcionen adecuadamente para cada switch.

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The practices presented in this document are the result of the appropriation of knowledge in communication networks, from the design, creation, expansion and resolution of errors, all the basic router configuration parameters will be applied in scenario 1 of this laboratory as well as creating a BGP protocol to share access lists between teams.

The analysis of networks requires the optimization of resources, for this a trunk link is applied for scenario 2 of communication between switches, also for independent networks it will be created in Vlan to communicate final communication devices in this case PC, although all these parameters If it was configured successfully, it is evident that the IP allocation is missing for the Vlan to work specifically for each switch.

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

INTRODUCCION

La comunicación entre dispositivos locales o remotos es cada vez más necesaria en un mundo digital que presenciamos actualmente, es por ello que el estudio de redes es indispensable para una correcta integración de equipos, ser eficaces y eficientes con los recursos que tenemos a mano para no crear costos incensarios. La presentación de esta prueba de habilidades nos muestra a groso modo problemáticas comunes presentes en la integración o creación de redes, la apropiación de los comandos de programación, aplicación de los parámetros y de cómo verificar el buen funcionamiento la red es el ovejito de este curso

Los escenarios presentados tienen el fin de afianzar los conocimientos adquiridos durante la fase de aprendizaje, es por ello que se propone la configuración de routers para establecer un protocolo de comunicación BGP entre ellos, al igual que BGP también existen otros protocolo de comunicación que se vieron atreves del curso como TCP/IP, OSPF, EIGRP, ISDN, STP y VTP todos destinados a cubrir las necesidades que se presenten según los equipos y tipos de enlaces que se requieren.

Para este curso se vio la importancia de la configuración de switch de capa 2 y 3, mediante la simulación en máquinas virtuales se pudo aprender la diferencia entre ellos, cuál es la correcta aplicación según el volumen de dados y protocolos de enrutamiento

DESARROLLO

Escenario 1

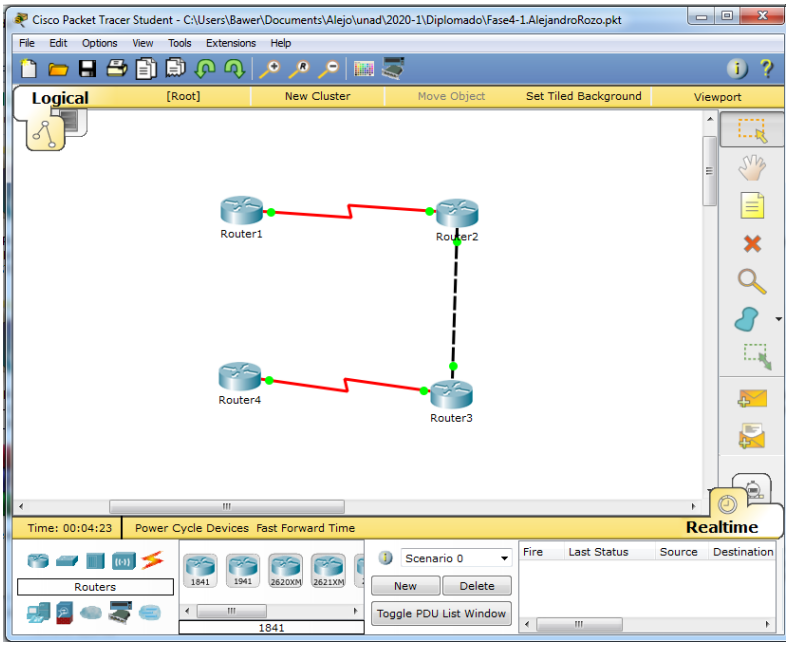

Ilustración 1 Escenario 1

Tablas para configuración de los Routers

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 1 Configuración inicial R1

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 1/0	192.1.23.2	255.255.255.0

Tabla 2 Configuración inicial R2

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
	S 0/0	192.1.34.2	255.255.255.0
	E 1/0	192.1.23.3	255.255.255.0

Tabla 3 Configuración inicial R3

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 4 Configuración inicial R4

Configuración inicial para cada uno de los routers en Packet Tracer

Parámetros de programación para el router R1

R1(config)#int s0/0

R1(config-if)#ip address 192.1.12.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#int lo 0

R1(config-if)#ip address 1.1.1.1 255.0.0.0

R1(config-if)#int lo 1

R1(config-if)#ip address 11.1.0.1 255.255.0.0

R1(config-if)#exit

Parámetros de programación para el router R2

R2(config)#int s0/0

R2(config-if)#ip address 192.1.12.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#int e1/0

R2(config-if)#ip address 192.1.23.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#int lo 0

R2(config-if)#ip address 2.2.2.2 255.0.0.0

R2(config-if)#int lo 1

R2(config-if)#ip address 12.1.0.1 255.255.0.0

Parámetros de programación para el router R3

R3(config)#int s0/0

R3(config-if)#ip address 192.1.34.3 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#int e1/0

R3(config-if)#ip address 192.1.23.3 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#int lo 0

R3(config-if)#ip address 3.3.3.3 255.0.0.0

R3(config-if)#int lo 1

R3(config-if)#ip address 13.1.0.1 255.255.0.0

Parámetros de programación para el router R4

R4(config)#int s0/0

R4(config-if)#ip address 192.1.34.4 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#int lo 0

R4(config-if)#ip address 4.4.4.4 255.0.0.0

R4(config-if)#int lo 1

R4(config-if)#ip address 14.1.0.1 255.255.0.0

R4(config-if)#exit

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.***

Parametros de programación para cada uno de los routers

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

```
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.3
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

Verificación con comando ***show ip route router R1***

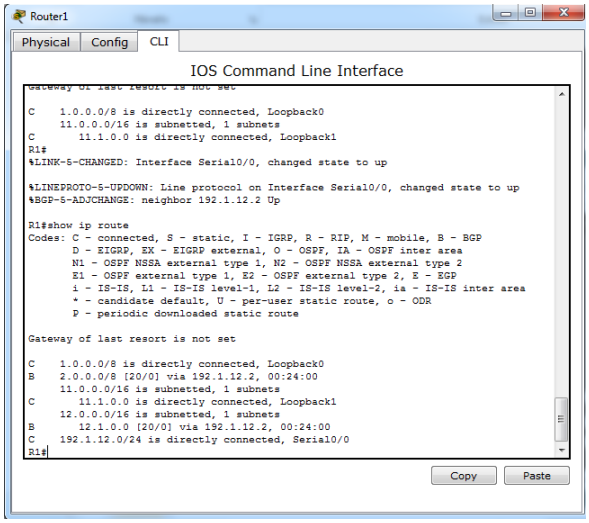

Ilustración 2 Show ip router R1

Verificación con comando ***show ip bgp router R1***

```
R1>enable
R1#show ip bgp
BGP table version is 13, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Ilustración 3 Show ip bgp router R1

Verificación con comando ***show ip route router R2***

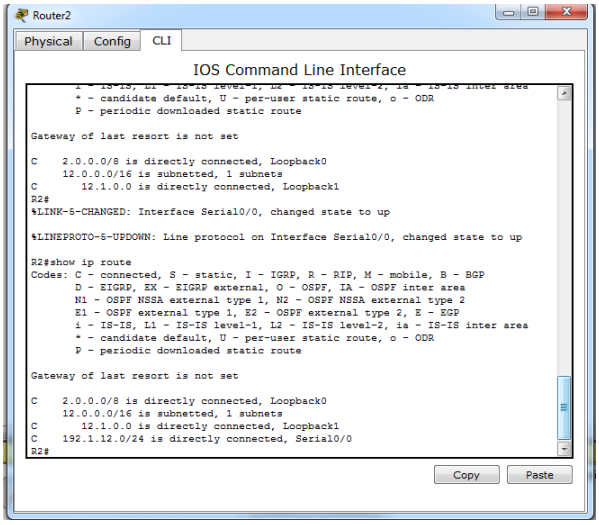

Ilustración 4 Ilustración 2 Show ip router R2

Verificación con comando ***show ip bgp router R2***

```
R2>enable
R2#show ip bgp
BGP table version is 14, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Ilustración 5 Show ip bgp router R2

1. 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.***

Parámetros de programación para el router

R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44

R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#neighbor 192.1.23.2 remote-as 2

Verificación con comando ***show ip route router R3***

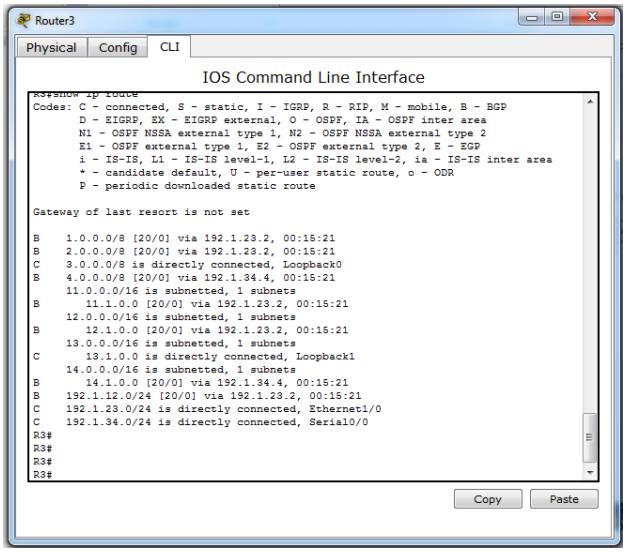

Ilustración 6 Show ip router R3

Verificación con comando ***show ip bgp router R3***

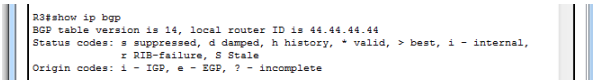

Ilustración 7 Show ip bgp router R3

1. 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 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.***

Parametros de programación para el router

R4(config)#router bgp 4

R4(config-router)#bgp router-id 66.66.66.66

R4(config-router)#network 192.1.34.0 mask 255.255.255.0

R4(config-router)#network 14.1.0.0 mask 255.255.0.0

R4(config-router)#network 4.0.0.0 mask 255.0.0.0

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

Verificación con comando ***show ip route router R4***

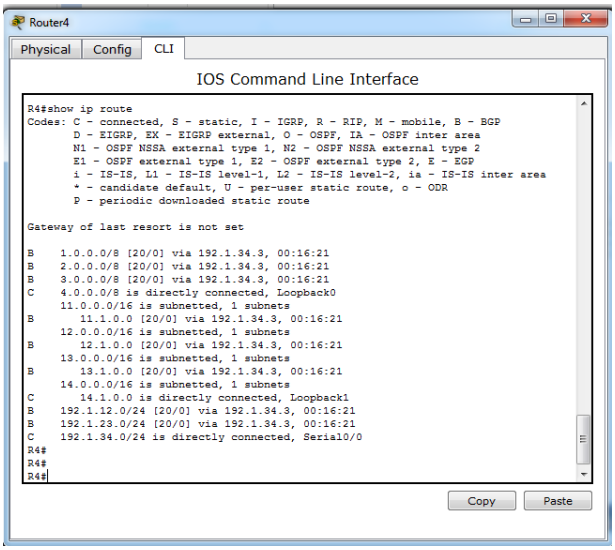

Ilustración 8 Show ip router R4

Verificación con comando ***show ip bgp router R4***

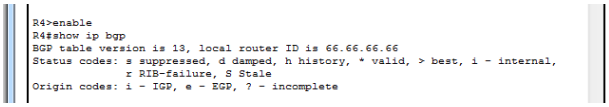

Ilustración 9 Show ip bgp router R4

Escenario 2

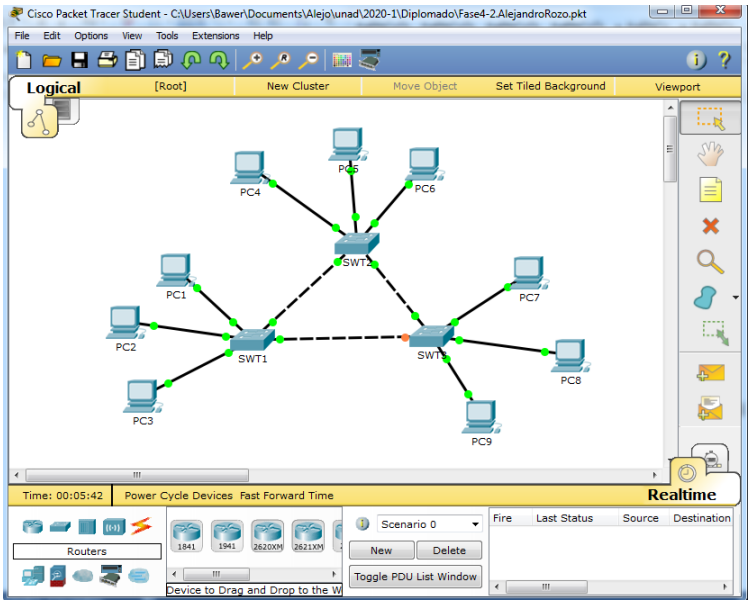

Ilustración 10 Escenario 2

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Parámetros de programación para el router

SW-AA#configure terminal
SW-AA (config)#vtp mode client Setting device to VTP CLIENT mode.
SW-AA (config)#vtp domain CCNP Changing VTP domain name from NULL to CCNP
SW-AA (config)#vtp password cisco Setting device VLAN database password to cisco

SW-BB#configure terminal
SW-BB(config)#vtp mode server Setting device to VTP SERVER mode.
SW-BB(config)#vtp domain CCNP Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco Setting device VLAN database password to cisco

SW-CC#configure terminal
SW-CC(config)#vtp mode client Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP Changing VTP domain name from NULL to CCNP

SW-CC(config)#vtp password cisco Setting device VLAN database password to cisco

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

Verificación con comando ***show vtp status SW-AA***

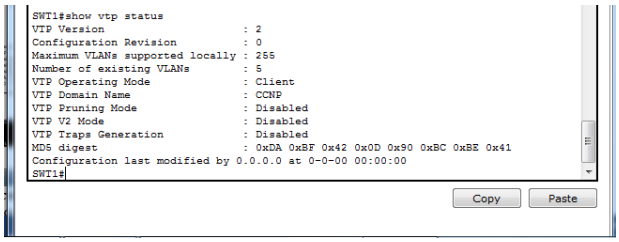

Ilustración 11 Show vtp status SW-AA

Verificación con comando ***show vtp status SW-BB***

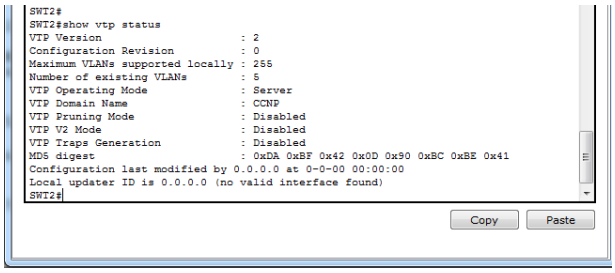

Ilustración 12 Show vtp status SW-BB

Verificación con comando ***show vtp status SW-CC***

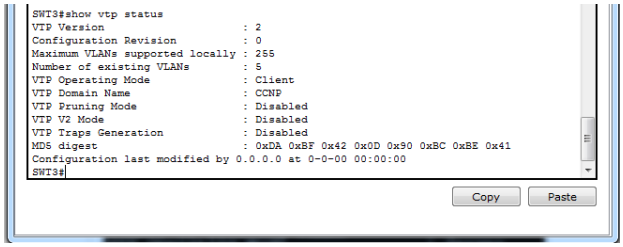

Ilustración 13 Show vtp status SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

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***.

```
SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

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

Verificación con comando ***show interface trunk SW-AA***

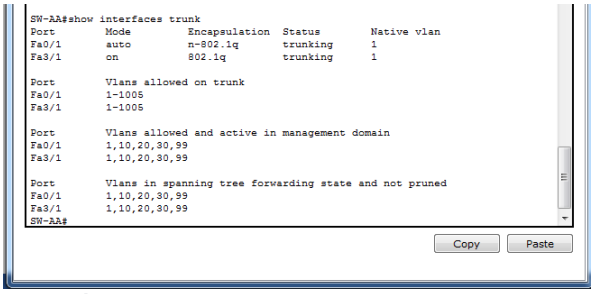

Ilustración 14 Show interface trunk SW-AA

Verificación con comando ***show interface trunk SW-BB***

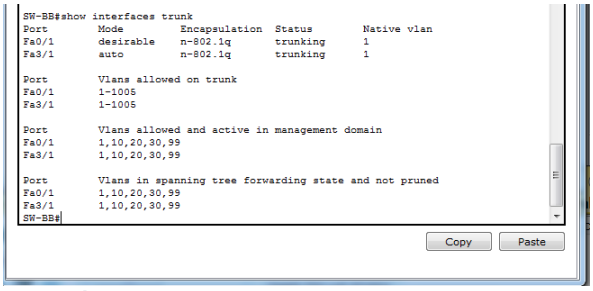

Ilustración 15 Show interface trunk SW-BB

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

SW-AA#configure terminal
SW-AA (config)#interface fastEthernet 3/1
SW-AA (config-if)#switchport mode trunk

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

Verificación con comando ***show interface trunk SW-AA***

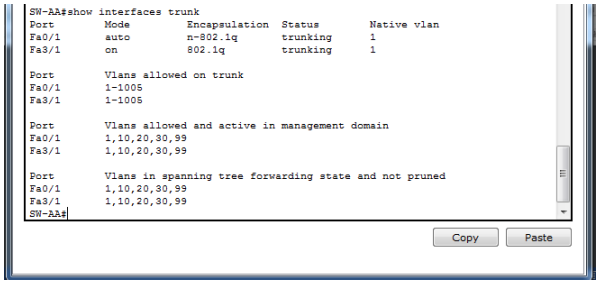

Ilustración 16 Show interface trunk SW-AA

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

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config)#switchport mode trunk

Verificación con comando ***show interface trunk SW-CC***

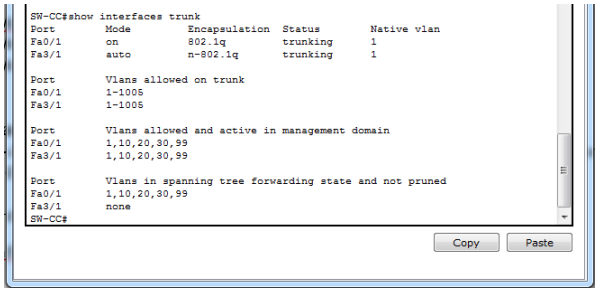

Ilustración 17 Show interface trunk SW-CC

C. Agregar VLANs y asignar puertos.

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

```
SW-AA#configure terminal
SW-AA(config)#vlan 10

SW-BB#configure terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#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
```

8. Verifique que las VLANs han sido agregadas correctamente.

Verificación con comando ***show vlan brief SW-BB***

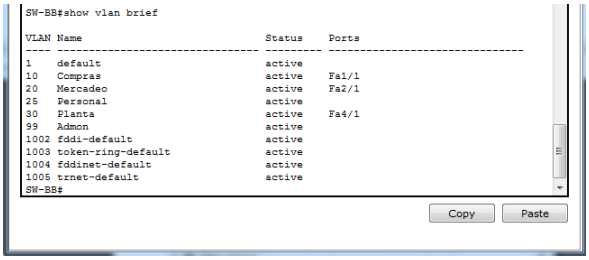

Ilustración 18 Show vlan brief SW-BB

Verificación con comando ***show vlan brief SW-AA***

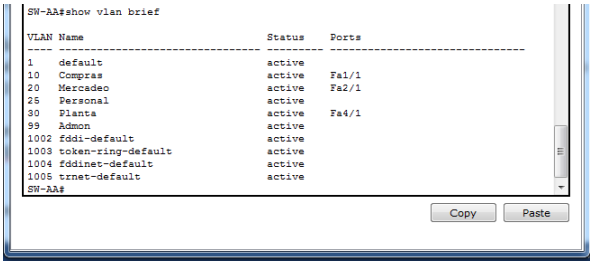

Ilustración 19 Show vlan brief SW-AA

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

Interfaz	**VLAN**	**Direcciones IP de los PCs**
F1/1	VLAN 10	190.108.10.X / 24
F2/1	VLAN 25	190.108.20.X /24
F4/1	VLAN 30	190.108.30.X /24

Tabla 5 Configuracion Vlan e IPs

X = número de cada PC particular

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

Parámetros de programación para SW-AA

```
SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 1/1
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config)#interface fastEthernet 2/1
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config)#interface fastEthernet 4/1
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

11. 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.

Parámetros de programación para SW-BB

```
SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 1/1
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
```

```
SW-BB(config)#interface fastEthernet 2/1
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config)#interface fastEthernet 4/1
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
```

Parámetros de programación para SW-CC

```
SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 1/1
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config)#interface fastEthernet 2/1
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config)#interface fastEthernet 4/1
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

Tabla de direcciones IP PCs

PC	Direccion IP	Mascara
1	190.108.10.1	255.255.255.0
2	190.108.20.2	255.255.255.0
3	190.108.30.3	255.255.255.0
4	190.108.10.4	255.255.255.0
5	190.108.20.5	255.255.255.0
6	190.108.30.6	255.255.255.0
7	190.108.10.7	255.255.255.0
8	190.108.20.8	255.255.255.0
9	190.108.30.9	255.255.255.0

Tabla 6 Direccionamiento de PCs

D. **Configurar las direcciones IP en los Switches.**

12. 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.

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

Tabla 7 Direccionamiento de switches

Parámetros de programación para SW-AA

SW-AA#configure terminal

SW-AA(config)#interface vlan 99

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

Parámetros de programación para SW-BB

SW-BB#configure terminal

SW-BB(config)#interface vlan 99

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

Parámetros de programación para SW-CC

SW-CC#configure terminal

SW-CC(config)#interface vlan 99

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

E. Verificar la conectividad Extremo a Extremo

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

Las pruebas indican que solo existe comunicación efectiva con las pc que tienen la misma dirección Ip en sus primeros 8 dígitos, con el resto de Pcs no existe comunicación, esto se debe que están haciendo uso de las Vlan para comunicación, para establecer una comunicación efectiva con todos los Pcs utilizando un switch para encaminar el tráfico hacia el equipo deseado, también en la trama de envió se debe incluir una etiqueta con el destino para que el enrutador reconozca con quien se requiere la comunicación.

Prueba ping entre Pc1 – Pc3 / Pc1 – Pc7

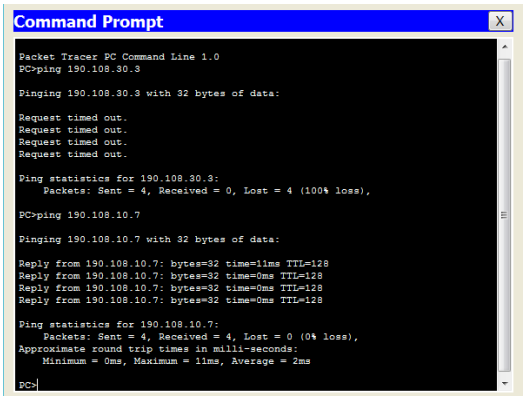

Ilustración 20 Ping PC1

Prueba ping entre Pc6 – Pc3 / Pc6 – Pc2

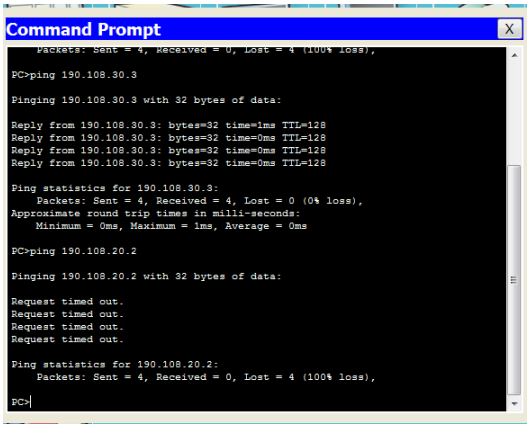

Ilustración 21 Ping PC6

Prueba ping entre Pc8 – Pc5 / Pc8 – Pc1

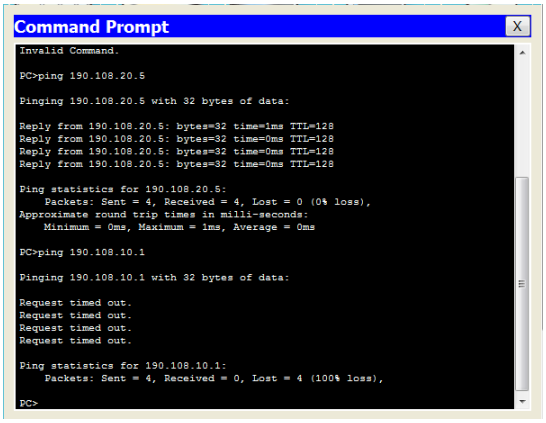

Ilustración 22 Ping PC8

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

La prueba de comunicación entre switches fue exitoso ya que la comunicación entre ellos está en modo Trunk por lo tanto el encapsulamiento funciona entre ellos.

Prueba ping entre SW-AA /SW-BB/SW-CC

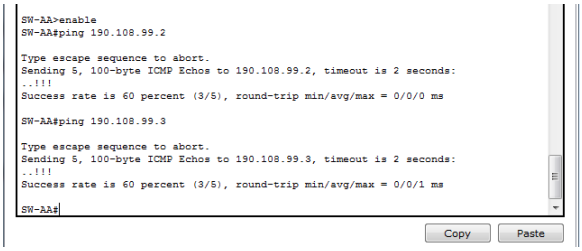

Ilustración 23 Ping SS-AA

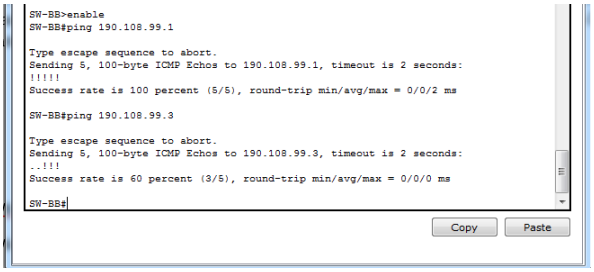

Ilustración 24 Ping SS-BB

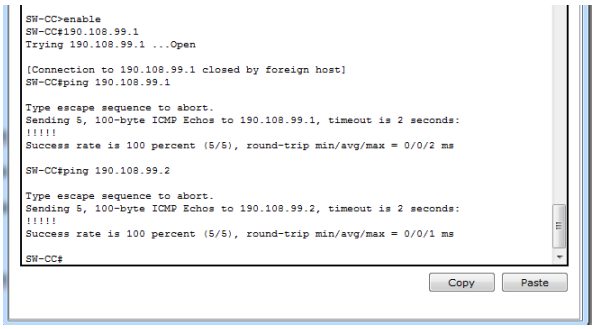

Ilustración 25 Ping SS-CC

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

La prueba de comunicación entre Switches y pc no tuvo éxito, esto se debe a que aunque están configuradas las Vlan en los Switches también se deben relacionas las direcciones IP de cada PC, esto se debe realizar para los tres Switches con sus respectivas PCs

Prueba ping entre SW-AA /PC-1/PC-2/PC-3

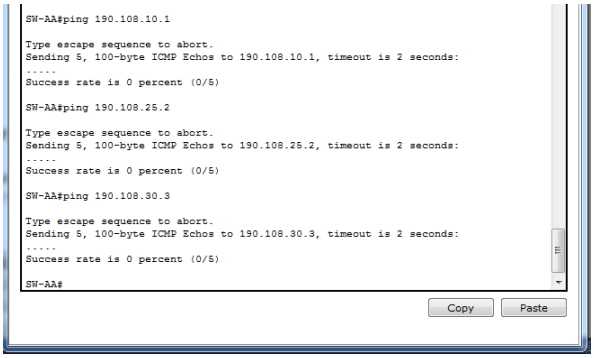

Ilustración 26 Ping SS-AA / PC

Prueba ping entre SW-BB /PC-4/PC-5/PC-6

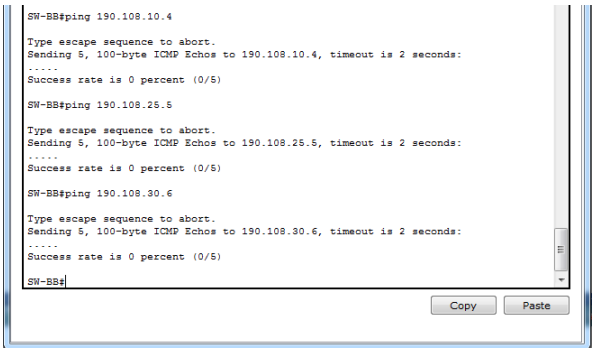

Ilustración 27 Ping SS-BB / PC

Prueba ping entre SW-BB /PC-7/PC-8/PC-9

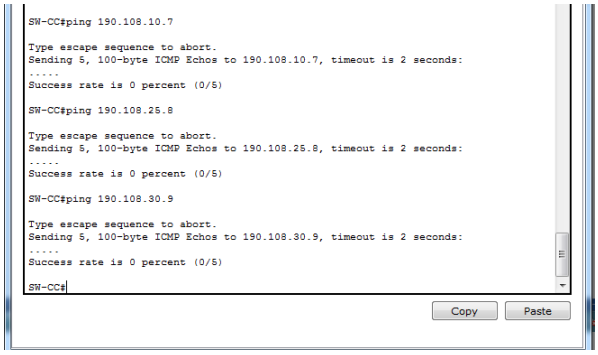

Ilustración 28 Ping SS-CC / PC

CONCLUSIONES

- Por medio de los ejercicios realizados se consolidan los conocimientos adquiridos durante el desarrollo del diplomado, verificamos los comandos básicos de configuraciones como asignación de Ip, configuración de protocolo BGP para intercambio de rutas en sistemas autónomos y enrutamiento de comunicación por medio del comando Trunk y creación de Vlan.

- Para que el protocolo BGP sea efectivo se requiere que los router de la red tengan asociadas referencias AS, asi se crea una malla con los router vecinos para reconociendo, un router configurado con un AS especifico aceptara solo tramas con esa etiqueta que envíen los demás equipos.

- El enlace troncal es efectivo y funciona correctamente para el escenario 2, pero se requiere que los equipos de las Vlan estén asociados por medios de sus IPs, de esta forma la comunicación será efectiva.

BIBLIOGRAFIA

- BGP Case Studies. (s. f.). Cisco. Recuperado 18 de mayo de 2020, de https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html
- Cisco Nexus 5000 Series NX-OS Software Configuration Guide—Configuring Access and Trunk Interfaces [Cisco Nexus 5000 Series Switches]. (s. f.). Cisco. Recuperado 18 de mayo de 2020, de https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.html
- Configure el puerto a las configuraciones del interfaz del VLA N en un conmutador con el CLI. (s. f.). Cisco. Recuperado 18 de mayo de 2020, de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html
- Ejemplo de configuración de iBGP y eBGP con o sin dirección de loopback. (s. f.). Cisco. Recuperado 18 de mayo de 2020, de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/13751-23.html
- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. 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). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx