

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DARIO ORLANDO DITTA DIAZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DARIO ORLANDO DITTA DIAZ

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
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

AGRADECIMIENTOS

A Dios, Jesucristo y a la virgen María por darme la oportunidad de constituir este proyecto, en lo académico y personal, por brindarme fortaleza y sabiduría en los momentos difíciles.

A mi familia por estar siempre atentos a cualquier requerimiento que tuviera, brindándome herramientas para sacar adelante los imprevistos y ser un pilar principal para culminar esta etapa de formación académica.

A mis hijos Nahiomy Giselle y Emmanuel Dario Orlando por ser inspiración de continuar mis procesos de formación profesional y de esta manera ser ejemplo en sus proyectos de vida.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE IMÁGENES	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	9
DESARROLLO DEL ESCENARIO 1	11
DESARROLLO DEL ESCENARIO 2	18
A. CONFIGURACION VTP	19
B. CONFIGURACION DTP(DYNAMIC TRUNKING PROTOCOL)	20
C. AGREGAR VLANS Y ASIGNAR PUERTOS.	21
D. CONFIGURAR LAS DIRECCIONES IP EN LOS SWITCHES.	25
E. VERIFICAR LA CONECTIVIDAD EXTREMO A EXTREMO.	25
CONCLUSIONES	32
REFERENCIAS	33

Lista de tablas

	Pág
Tabla 1. Información para configurar R1.....	11
Tabla 2. Información para configurar R2.....	11
Tabla 3. Información para configurar R3.....	12
Tabla 4. Información para configurar R4.....	12
Tabla 5. Configuración puertos y dirección ip.	23
Tabla 6. Configuración de las direcciones Ip.	25

Lista de imágenes

	Pag
Imagen 1. Escenario uno.....	11
Imagen 2. Diseño de la topología.....	12
Imagen 3. Tabla de enrutamiento del Router 1.....	15
Imagen 5. Tabla de enrutamiento del Router 3.....	16
Imagen 4. Tabla de enrutamiento del Router 2.....	17
Imagen 6. Tabla de enrutamiento del Router 4.....	17
Imagen 7. Escenario 2.....	18
Imagen 8. Diseño de la topología.....	18
Imagen 9. Verificación de la configuración vtp.....	19
Imagen 10. Verificación de la configuración vtp.....	20
Imagen 11. Verificación de la configuración vtp.....	20
Imagen 12. Enlace troncal en SW-AA.....	20
Imagen 13. Enlace troncal en SW-BB.....	20
Imagen 14. Enlace troncal en SW-AA.....	21
Imagen 15. Enlace troncal en SW-BB.....	21
Imagen 16. Tabla con las VLANs agregadas correctamente en SW-AA.....	22
Imagen 17. Tabla con las VLANs agregadas correctamente en SW-BB.....	22
Imagen 18. Tabla con las VLANs agregadas correctamente en SW-CC.....	22
Imagen 19. Ping desde PC1 a PC2, PC3 y PC4.....	26
Imagen 20. Ping desde PC2 a PC7, PC8 y PC9.....	26
Imagen 21. Ping PC3 a PC4, PC5 y PC6.....	27
Imagen 22. Ping desde SW-AA a SW-BB y SW-CC.....	27
Imagen 23. Ping desde SW-BB a SW-AA y SW-CC.....	28
Imagen 24. Ping desde SW-CC a SW-AA y SW-BB.....	28
Imagen 25. Ping desde SW-AA a PC1, PC2, PC3.....	28
Imagen 26. Ping desde SW-AA a PC4, PC5, PC6.....	29
Imagen 27. Ping desde SW-CC a PC7, PC8, PC9.....	29
Imagen 28. Ping desde SW-AA a PC1, PC7 y PC9.....	30

GLOSARIO

Interfaz: Punto, área, o la superficie a lo largo de la cual dos cosas de naturaleza distinta convergen. Por extensión, se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común.

Proxy: Hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Red de área amplia (WAN): Una red que interconecta recursos de computadoras que están geográficamente ampliamente separadas (usualmente a más de 100 km). Esto incluye pueblos, ciudades, estados y condados. Un WAN cubre generalmente un área mayor que 5 millas (8 km) y puede considerarse que consiste en una colección de LAN

Switch: Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Un switch interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de los datagramas en la red. Un switch en el centro de una red en estrella.

VPN: (Virtual Private Network/Red Privada Virtual). Una conexión IP entre dos sitios sobre una red pública IP que tiene su tráfico de carga útil codificada de manera que sólo los nodos fuente y destino pueden descifrar los paquetes de tráfico. Una VPN permite a una red públicamente accesible ser usada para transmisiones de datos altamente confidenciales, dinámicas y seguras.

RESUMEN

Por medio del presente trabajo escrito se pretende dejar evidencia de las actividades requeridas para aplicar el conocimiento obtenido en la formación de ingeniería electrónica componente práctico indicadas en la guía de prueba de habilidades cuyo objetivo es que nosotros como estudiantes conozcamos, estudiemos, entendamos, comprendamos, apropiemos, y sobre todo apliquemos los conceptos que se han estudiado durante el desarrollo del presente Diplomado de profundización en la plataforma CISCO en redes para obtener la certificación CCNP de cuyos principales temas relacionó a continuación conmutación, enrutamiento.

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

ABSTRACT

By means of this written work it is intended to leave evidence of the activities required to apply the knowledge obtained in the practical component electronic engineering training indicated in the skills test guide whose objective is that we as students know, study, understand, understand, Let us adopt, and above all, apply the concepts that have been studied during the development of this Diploma of deepening in the CISCO platform in networks to obtain the CCNP certification of whose main topics it related switching, routing.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

El objetivo principal del diplomado CCNP es lograr que el estudiante adopte las capacidades requeridas para administrar dispositivos de red como routers y switches, a través del estudio de la arquitectura TCP/IP y la implementación de recursos y herramientas necesarias para lograr conectividad de red y solucionar las inconsistencias presentados.

Mediante el desarrollo de las actividades logramos el fortalecimiento de los fundamentos básicos para la implementación de plataformas de red escalables con el uso del modelo jerárquico de tres niveles, para mejorar el rendimiento de la red e incorporar eficientemente los protocolos de conmutación.

Los ejercicios planteados en la actividad para el desarrollo de habilidades nos dan la oportunidad de afianzar el conocimiento adquirido durante el diplomado de profundización en los conceptos de ROUTE y SWITCH plasmándolos en los diferentes programas que manejamos a lo largo del proceso de formación.

Con el desarrollo de esta actividad se coloca a prueba todo lo aprendido durante el semestre, esto con el fin de medir las capacidades. Lógica, comprensión y solución a diferentes escenarios propuestos, en esta actividad se tendrá dos escenarios los cuales serán desarrollados por medio del software GNS3 y Packet Tracer y por medio de este documento se mostrarán los procedimientos y resultados con comandos como show ip route, show vtp status, show vlan brief etc.

Desarrollo del escenario 1

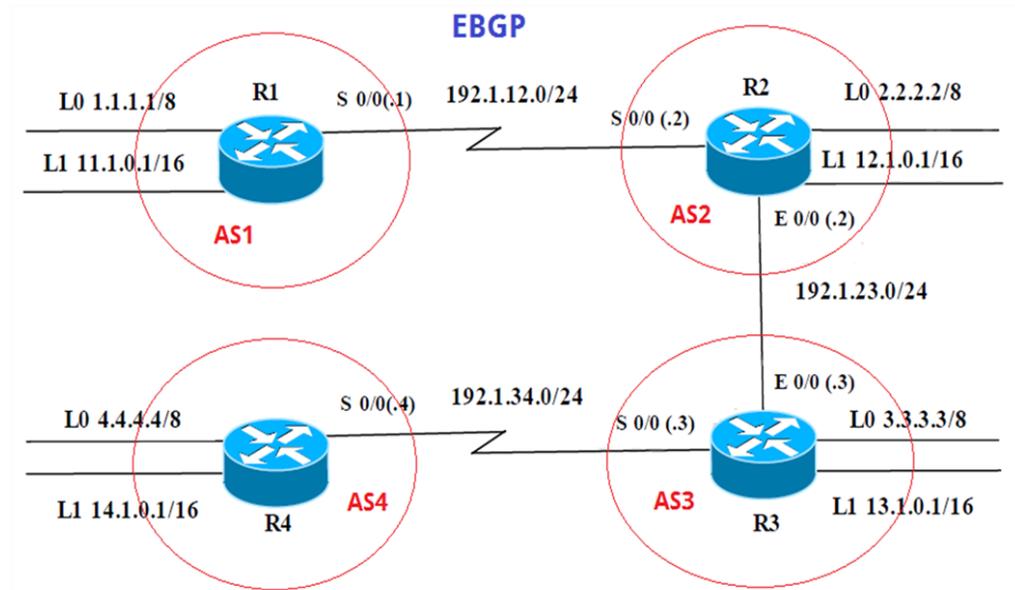


Imagen 1. Escenario uno.

	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

Tabla 1. Información para configurar R1.

	Interfaz	Dirección IP	Máscara
R2	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 2. Información para configurar R2.

	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

R3

Tabla 3. Información para configurar R3.

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

R4

Tabla 4. Información para configurar R4.

Solución

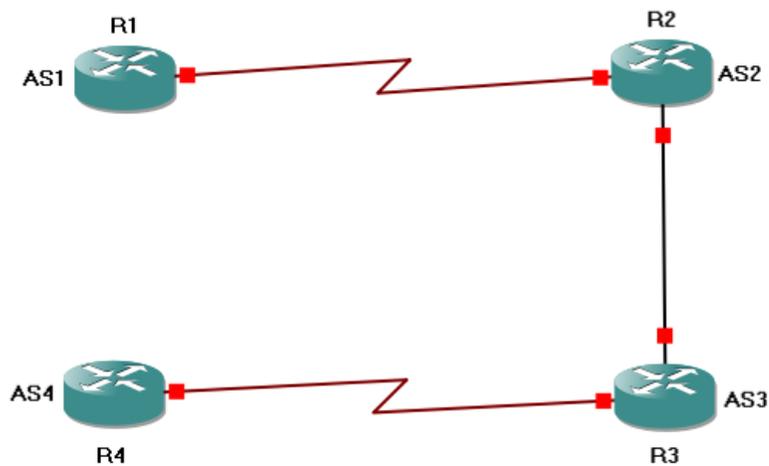


Imagen 2. Diseño de la topología.

Se configura la dirección IP a en cada interfaz de los routers.

R1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#int loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config)#int loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config)#int serial 1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

R2#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)# int loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config)# int loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config)#int serial 1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
```

R3#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)# int loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config)# int loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config)#int serial 1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface FastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
```

R4#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R4(config)# int loopback 0
```

```
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config)# int loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config)#int serial 1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
```

1. Configure 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*.

```
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```

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

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*.

```
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

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

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

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*.

```
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)#exit
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
```

```
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#neighbor 3.3.3.3 remote-as 3
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
```

Después de configurar los routers con las especificaciones de cada punto se procede a mostrar la tabla de enrutamiento de cada router como lo indica cada punto, se decidió mostrar las cuatro tablas después de configurar cada router para verlas actualizadas y con su configuración final.

```

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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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
B       2.0.0.0/8 [20/0] via 192.1.12.2, 00:05:35
    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
    12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:05:35
    13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.12.2, 00:05:35
    14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.12.2, 00:05:35
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial1/0
L       192.1.12.1/32 is directly connected, Serial1/0
B       192.1.23.0/24 [20/0] via 192.1.12.2, 00:05:35
B       192.1.34.0/24 [20/0] via 192.1.12.2, 00:05:35
R1#

```

Imagen 3.Tabla de enrutamiento del Router 1.

```

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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B       1.0.0.0/8 [20/0] via 192.1.12.1, 00:14:08
    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 [20/0] via 192.1.12.1, 00:14:08
    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
    13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:14:08
    14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.23.3, 00:14:08
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial1/0
L       192.1.12.2/32 is directly connected, Serial1/0
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.23.0/24 is directly connected, FastEthernet0/0
L       192.1.23.2/32 is directly connected, FastEthernet0/0
B       192.1.34.0/24 [20/0] via 192.1.23.3, 00:14:08
R2#

```

```

R3#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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:11:45
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:11:45
     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
S    4.0.0.0/8 [1/0] via 192.1.34.4
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:11:45
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:11:45
     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
     14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 4.4.4.4, 00:11:46
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:11:45
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.3/32 is directly connected, FastEthernet0/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#

```

```

R4#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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:15:52
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:15:52
S    3.0.0.0/8 [1/0] via 192.1.34.3
     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
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 3.3.3.3, 00:15:52
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:15:52
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:16:22
     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
B    192.1.12.0/24 [20/0] via 3.3.3.3, 00:15:52
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:16:22
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.4/32 is directly connected, Serial1/0
R4#

```

Imagen 6. Tabla de enrutamiento del Router 4.

Desarrollo del escenario 2

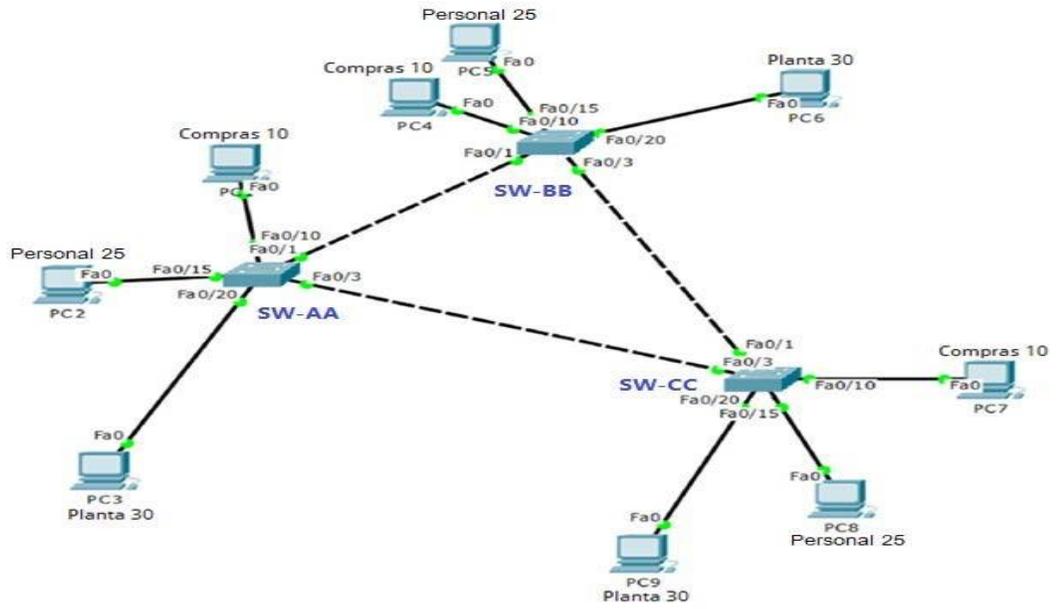


Imagen 7. Escenario 2.

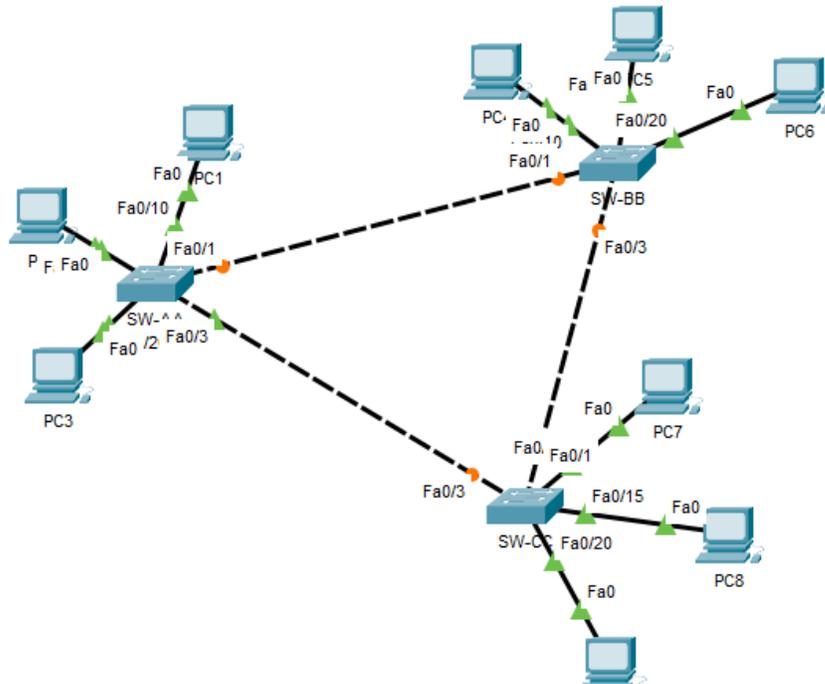


Imagen 8. Diseño de la topología.

A. Configuración 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 VTP llamado CCNP y usando la contraseña cisco.

SW-AA #config terminal

Enter configuration commands, one per line. End with CNTL/Z.

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

Setting device to VTP CLIENT mode.

```
SW-AA(config)#vtp domain CCNP
```

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

SW-BB #config terminal

Enter configuration commands, one per line. End with CNTL/Z.

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

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

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

SW-CC #config terminal

Enter configuration commands, one per line. End with CNTL/Z.

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

Setting device to VTP CLIENT mode.

```
SW-CC(config)#vtp domain CCNP
```

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

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

```
SW-AA#show vtp status
VTP Version                : 2
Configuration Revision     : 8
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
```

Imagen 9. Verificación de la configuración vtp.

```
SW-BB#show vtp status
VTP Version                : 2
Configuration Revision     : 8
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : CCNP
```

Imagen 10. Verificación de la configuración vtp.

```
SW-CC#show vtp status
VTP Version           : 2
Configuration Revision : 8
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode    : Client
VTP Domain Name       : CCNP
```

Imagen 11. Verificación de la configuración vtp.

B. Configuración DTP(Dynamic Trunking Protocol)

1. 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-AA#config terminal
SW-AA(config)#int FastEthernet 0/1
SW-AA(config-if)#switch mode dynamic desirable
SW-AA(config-if)#exit
```

Ya que la configuración por defecto que trae el Switch es el modo dynamic auto no se configura el SW-BB si no que se deja la configuración por defecto.

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

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

Imagen 12. Enlace troncal en SW-AA.

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

Imagen 13. Enlace troncal en SW-BB.

3. 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#config terminal
SW-AA(config)#int FastEthernet 0/3
SW-AA(config-if)#switchport mode trunk
```

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

```
SW-AA#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1
```

Imagen 14. Enlace troncal en SW-AA.

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

```
SW-BB#config terminal
SW-BB(config)#int FastEthernet 0/3
SW-BB(config-if)#switchport mode trunk
```

```
SW-BB#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1
```

- C. Agrega  *Imagen 15. Enlace troncal en SW-BB.*

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

En el momento que se intenta agregar la vlan 10 al Switch SW-AA muestra un mensaje el cual hace referencia a que la configuración del vlan vtp no se permite cuando el dispositivo está en el modo cliente.

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

Se procede a realizar la configuración en el Switch SW-BB el cual esta configuradora como servidor.

```

SW-BB#config 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

```

2. Verifique que las VLANs han sido agregadas correctamente.

```
SW-AA#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10 Compras	active	Fa0/10
25 Personal	active	Fa0/15
30 Planta	active	Fa0/20
99 Admon	active	

Imagen 16. Tabla con las VLANs agregadas correctamente en SW-AA.

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

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10 Compras	active	Fa0/10
25 Personal	active	Fa0/15
30 Planta	active	Fa0/20
99 Admon	active	

Imagen 17. Tabla con las VLANs agregadas correctamente en SW-BB.

```
SW-CC#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10 Compras	active	Fa0/10
25 Personal	active	Fa0/15

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

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

Tabla 5. Configuración puertos y dirección ip.

Se configura cada una de las direcciones ip de los PC según la tabla anterior, la configuración queda de la siguiente forma.

VLAN 10

PC1: 190.108.10.1

PC4: 190.108.10.2

PC7: 190.108.10.3

VLAN 25

PC2: 190.108.20.1

PC5: 190.108.20.2

PC8: 190.108.20.3

VLAN 30

PC3: 190.108.30.1

PC6: 190.108.30.2

PC9: 190.108.30.3

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
5. 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#config terminal
```

```
SW-AA(config)#int FastEthernet 0/10
```

```
SW-AA(config-if)#switchport mode access
```

```
SW-AA(config-if)#switchport access vlan 10
```

```
SW-AA(config-if)#int FastEthernet 0/15
```

```
SW-AA(config-if)#switchport mode access
```

```
SW-AA(config-if)#switchport access vlan 25
```

```
SW-AA(config-if)#int FastEthernet 0/20
```

```
SW-AA(config-if)#switchport mode access
```

```
SW-AA(config-if)#switchport access vlan 30
```

```
SW-BB#config terminal
```

```
SW-BB(config)#int FastEthernet 0/10
```

```
SW-BB(config-if)#switchport mode access
```

```
SW-BB(config-if)#switchport access vlan 10
```

```
SW-BB(config-if)#int FastEthernet 0/15
```

```
SW-BB(config-if)#switchport mode access
```

```
SW-BB(config-if)#switchport access vlan 25
```

```
SW-BB(config-if)#int FastEthernet 0/20
```

```
SW-BB(config-if)#switchport mode access
```

```
SW-BB(config-if)#switchport access vlan 30
```

```
SW-CC#config terminal
```

```
SW-CC(config)#int FastEthernet 0/10
```

```
SW-CC(config-if)#switchport mode access
```

```
SW-CC(config-if)#switchport access vlan 10
```

```
SW-CC(config-if)#int FastEthernet 0/15
```

```
SW-CC(config-if)#switchport mode access
```

```
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#int FastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

D. Configurar las direcciones IP en los Switches.

14. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

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 6. Configuración de las direcciones Ip.

```
SW-AA#config terminal
SW-AA(config)#int vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
```

```
SW-BB#config terminal
SW-BB(config)#int vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SW-CC#config terminal
SW-CC(config)#int vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

E. Verificar la conectividad Extremo a Extremo.

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

```
C:\>ping 190.108.20.1

Pinging 190.108.20.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.1

Pinging 190.108.30.1 with 32 bytes of data:
```

Imagen 19. Ping desde PC1 a PC2, PC3 y PC4.

```
C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:

Reply from 190.108.20.3: bytes=32 time<lms TTL=128
Reply from 190.108.20.3: bytes=32 time=lms TTL=128
Reply from 190.108.20.3: bytes=32 time=lms TTL=128
Reply from 190.108.20.3: bytes=32 time<lms TTL=128

Ping statistics for 190.108.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Imagen 20. Ping desde PC2 a PC7, PC8 y PC9.

```

C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.2

Pinging 190.108.30.2 with 32 bytes of data:

Reply from 190.108.30.2: bytes=32 time<1ms TTL=128
Reply from 190.108.30.2: bytes=32 time=3ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

```

Imagen 21. Ping PC3 a PC4, PC5 y PC6.

Después de realizar unas pruebas haciendo ping desde un PC a otro se puede evidenciar que el ping tiene éxito con los PC que se encuentra en la misma VLAN, como se puede apreciar en la imagen 17 al momento de hacer ping con el PC1 solo fue exitoso el ping con el PC4 ya que estos comparten la misma VLAN 10.

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

```

SW-AA#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

```

Imagen 22. Ping desde SW-AA a SW-BB y SW-CC.

```

SW-BB#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

SW-BB#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

```

Imagen 23. Ping desde SW-BB a SW-AA y SW-CC.

```

SW-CC#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW-CC#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

```

Imagen 24. Ping desde SW-CC a SW-AA y SW-BB.

Todos los pings fueron exitosos, esto se debe gracias a la configuración de los enlaces troncales y a la configuración del direccionamiento ip de la Vlan 99.

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

```

SW-AA#ping 190.108.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

Imagen 25. Ping desde SW-AA a PC1, PC2, PC3.

```
SW-BB#ping 190.108.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#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)
```

Imagen 26. Ping desde SW-AA a PC4, PC5, PC6.

```
SW-CC#ping 190.108.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.20.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Imagen 27. Ping desde SW-CC a PC7, PC8, PC9.

Se probó realizar ping desde los Switches a cada PC que están conectados directamente, también se intentó hacer ping desde los otros PC, pero los resultados fueron fallidos, esto se debe a que aún no se configura un enrutamiento IP en las VLANs creadas.

A continuación, se procede a realizar el enrutamiento IP a cada VLANs.

```
SW-AA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 10
SW-AA(config-if)#ip address 190.108.10.4 255.255.255.0
SW-AA(config-if)#interface vlan 25
SW-AA(config-if)#ip address 190.108.20.4 255.255.255.0
SW-AA(config-if)#interface vlan 30
SW-AA(config-if)#ip address 190.108.30.4 255.255.255.0
```

```
SW-BB#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.108.10.5 255.255.255.0
SW-BB(config-if)#interface vlan 25
SW-BB(config-if)#ip address 190.108.20.5 255.255.255.0
SW-BB(config-if)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.5 255.255.255.0
```

```
SW-CC#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 10
SW-CC(config-if)#ip address 190.108.10.6 255.255.255.0
SW-CC(config-if)#interface vlan 25
SW-CC(config-if)#ip address 190.108.20.6 255.255.255.0
SW-CC(config-if)#interface vlan 30
SW-CC(config-if)#ip address 190.108.30.6 255.255.255.0
```

```
SW-AA#ping 190.108.10.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
SW-AA#ping 190.108.10.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
SW-AA#ping 190.108.30.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/10 ms
```

Imagen 28. Ping desde SW-AA a PC1, PC7 y PC9.

Como se puede apreciar en la siguiente prueba, después de la configuración del enrutamiento IP de las VLAN se procede a realizar ping desde diferentes PC y se obtiene en todos los resultados un ping exitoso, esto pasa en todos los Switches.

Conclusiones

Mediante el desarrollo del diplomado de profundización adquirimos diferentes habilidades prácticas y cognitivas, las cuales nos dan la oportunidad de avanzar en temas de actualidad y que a lo largo de nuestra carrera como profesionales vamos a tener la oportunidad de compartirlas y aplicarlas en otros ámbitos.

En la actualidad el manejo y estructuración de las redes nos permiten tener acceso a un mundo globalizado que día a día requiere acortar distancias y ejecutar tareas de forma efectiva y constantes, es el caso del uso de herramientas empleadas para el desarrollo de las tareas asignadas a lo largo del diplomado como Packet tracer, Gns3, las cuales permiten tener una amplia vista de la aplicabilidad de lo aprendido durante todo el camino de formación profesional.

Al realizar esta prueba de habilidades pudimos aclarar dudas que se generaron a lo largo del diplomado pues el contenido de estos dos ejercicios resume los módulos que lo conforman ROUTERS Y SWITCH en los cuales aplicamos las configuraciones requeridas para el desarrollo adecuado de la topología de red y necesidades de los usuarios.

Referencias

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD>

Gallo, M. A. H., Gallo, W. M. M. A., & Hancock, W. M. (2002). Glosario. Comunicación entre computadoras y tecnología de redes. Thomson. Recuperado de: <http://go.galegroup.com/ps/i.do?id=GALE%7CCX4059900177&v=2.1&u=unad&it=r&p=GVRL&sw=w&asid=ebb3f06c3e49cace676a520de3807353>

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2>

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>