DIPLOMADO DE PROFUNDIZACION
PRUEBA DE HABILIDADES PRACTICAS CCNP

ROGER ALBERTO GARCIA BELTRAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECTBI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2020

DIPLOMADO DE PROFUNDIZACION
PRUEBA DE HABILIDADES PRACTICAS CCNP

ROGER ALBERTO GARCIA BELTRAN

Diplomado de opción de grado presentado para optar el
Título de INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
MSc. Gerardo Granados Acuña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECTBI
INGENIERIA DE TELECOMUNICACIONES
BOGOTA
2020

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 22 mayo de 2020

AGRADECIMIENTOS

Al finalizar este trabajo académico, quiero ante todo dar gracias a Dios dador de la inteligencia y la sabiduría, ser mi guía y acompañarme en el transcurso de todo mi proceso académico, y así culminar con éxito mi proceso educativo. A mi esposa por ser el pilar fundamental en el esfuerzo y haberme apoyado incondicionalmente, aun cuando por momentos quería desfallecer en el proceso, a mis hijos que son mi motor y para quienes quiero ser su mayor ejemplo, quienes han sido mi principal motivación para este proceso; a mi padre que es un ejemplo de tenacidad, y a mis demás familiares de quienes recibí apoyo y lograr así finalizar con éxito el desarrollo de este diplomado.

Así mismo a mis tutores Efraín Alejandro Perez que con su amplia experiencia y conocimiento me orientaron el desarrollo y culminación con éxito este diplomado y a la universidad Nacional Abierta y a Distancia UNAD, la cual me permitirá obtener el título profesional de Ingeniero En Telecomunicaciones.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Backbone:Porción de la red que administra el tráfico de alto volumen. El backbone puede conectar varias sedes o edificios de una organización, así como las pequeñas redes LAN que posea.Caching Técnica consistente en duplicar datos de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en el caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso aparente al dato sea menor.

DoS:(del inglés Denial of Service / Denegacion del Servicio). Es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea innaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Middleware:Lógica de la Mediación. Capa de programas que oculta a los desarrolladores de aplicaciones distribuidas los detalles de la plataforma física incluyendo su heterogeneidad. Gracias a ella, el entorno de ejecución aparenta ser un sistema uniforme. Los desarrolladores pueden concentrarse en los aspectos relevantes de la aplicación, la cual puede ser implantada en cualquier plataforma sobre la que se instale la lógica de mediación.

Socket: Mecanismo de comunicación entre procesos. Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadores distintos) pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada. Un socket queda definido por una dirección IP, un protocolo y un número de puerto. Ejemplo: ftp://201.45.23.45:21

TCP:(del inglés Transmission Control Protocol, Protocolo de Control de Transmisión). Protocolo que fue creado entre los años 1973 - 1974 (por Vint Cerf y Robert Kahn) es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por computadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

WDM - Multiplexación por división de longitud de onda:Un método de multiplexión usado con cables de fibra óptica. Este implica la transmisión simultánea de fuentes de luz sobre un solo canal de fibra óptica. Las fuentes de luz de diferentes longitudes de onda son combinadas por un multiplexor WDM y transmitidas sobre una sola línea. Cuando llegan las señales, un desmultiplexor las separa y las transmite a sus respectivos receptores de destino.

RESUMEN

Las destrezas adquiridas en el desarrollo del diplomado Cisco CCNP (Cisco Certified Networking Proffesiona se ven reflejada en la actividad de la prueba habilidades las cuales busca medir el nivel de conocimiento e identificar el grado de competencia que fueron adquirido a lo largo del curso para esto se trabajó con dos módulos de CCNP ROUTER y CCNP SWITCH avansados *Cisco Networking Academy* mediamente dos escenarios propuestos donde se configuraron y se les dio el enrutamiento a rauter y swintch en la herramienta Packer tracer teniendo en cuenta los principios básicos de la redes y los protocolos de enrutamiento de gateway interior mejorado (EIGRP), el protocolo Primer camino más corto (OSPF) y el protocolo de puesta de enlace de frontera (BGP). Para esto fue nesario examinar las mejores prácticas de seguridad electrónica que nos permitieran monitoreo y administración de la conmutación en una arquitectura de redes y la utilización de switch de capas 2 capas 3 implementamos VLANs en las redes que se plantearon en los dos escenarios para poder implementar las características de seguridad en redes WAN Y LAN que permitan instalar configurar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de redes
En los escenarios se asocian aspectos de conmutación y enrutamiento mediante estrategias basadas en comandos IOS configura plataformas de conmutación basadas en switches, mediante el uso de protocolos como STP mediante el uso de comandos de administración avanzados.

Palabras Clave en el RESUMEN: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The skills gained in the development of Cisco CCNP(Cisco Certified Networking Proffesiona) are reflected in the skills test activity which seeks to measure the level of knowledge and identify the degree of competence that was acquired throughout the course for this worked with two modules of CCNP ROUTER and CCNP SWITCH advanced Cisco Networking *Academy* half two proposed scenarios where they were configured and given the rauter and swintch routing in the Packer tracer tool taking into account the basic principles of the networkis and enhanced internal gateway routing protocols (EIGRP), the Shortest First Path Protocol (OSPF), and the BGP border laying protocol y se les do el enrutamiento a (BGP). For this it was necessary to examine the best practices of el Electronics security that would allow us to monitor and manage switching in a re-des architecture and the use of layer 2 layer 3 switch we implement VLANs in the networks that were raised in the two scenarios to be able to implement the security features on WAN and LAN networks that allow to install, monitor, and troubleshoot computers belonging to the Networking infrastructure

The scenarios associate aspects of switching and routing using IOS command-based strategies to configure switch-based switching platforms, using protocols such as STP by using advanced management commands.

Keywords in the SUMMARY: CISCO, CCNP, Switching, Routing, Networks, Electronics, Networking.

INTRODUCCION

El siguiente trabajo presenta el desarrollo de dos escenarios propuestos en la prueba de habilidades practicas del curso CISCO CCNP La cual es una actividad evaluación del diplomado de profundización que tiene como propósito que el estudiante demuestre los logros alcanzados mediante el desarrollo del curso y afianzar los conocimientos adquiridos para poder implementar en la etapa profesional.

Atreves de este componente practico el diplomado CISCO CCNP en la prueba de habilidades practicas, se utilizaran la herramienta Packet Tracer para la configuración de inicial de los routers y switches, seguridad de credenciales de acceso, enrutamiento (EIGRP y OSPF), creación de VLANs y verificación de conectividad mediante el uso de comandos como ping, show ip route, show vtp status, show interfaces trunk, entre otros.

Con Este proyecto consolidamos el proceso de conceptualización de los diversos temas del área de networking y abordan temáticas como el enrutamiento dinámico a través de los protocolos OSPF y EIGRP, así como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback un tema con demasiada importancia que cada día es relevante a momento de implementar una red.

DESARROLLO

ESCENARIO 1

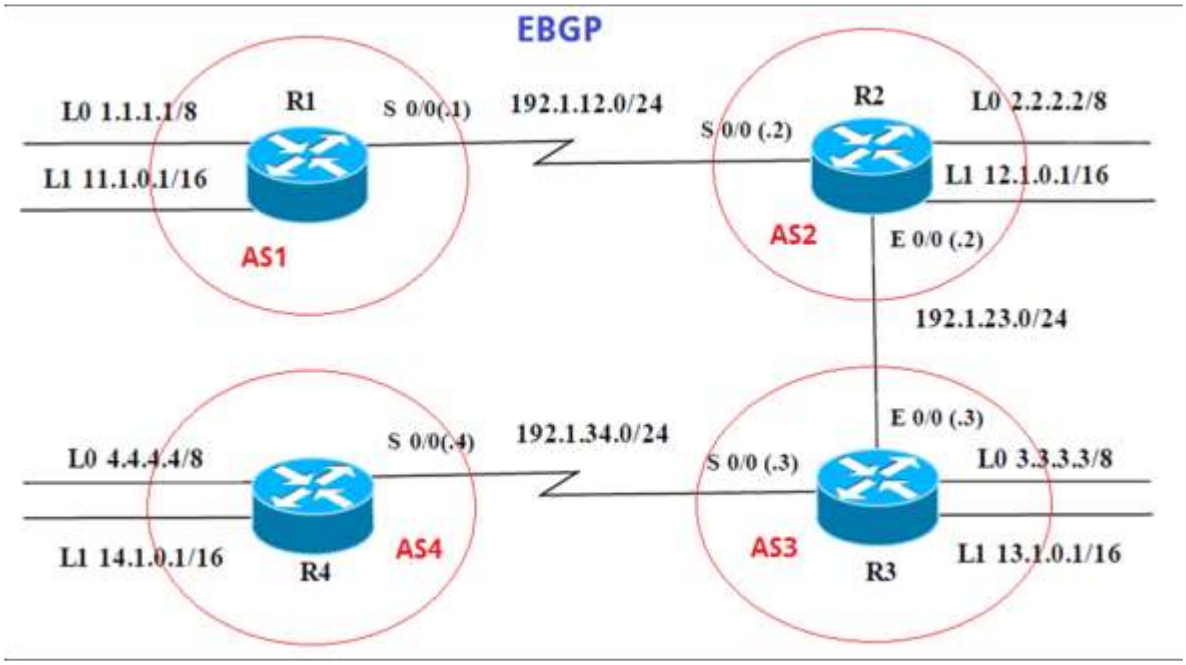


Figura 1. Escenario 1

Información 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
S0/0	192.1.12.1	255.255.255.0

Tabla 1. Router 1

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
S0/0	192.1.12.2	255.255.255.0
E0/0	192.1.23.2	255.255.255.0

Tabla 2. Router 2

	interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E0/0	192.1.23.3	255.255.255.0
	S0/0	192.1.34.3	255.255.255.0

Tabla 3. Router 3

	interfaz	Dirección IP	Máscara
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S0/0	192.1.34.4	255.255.255.0

Tabla 4. Router 4

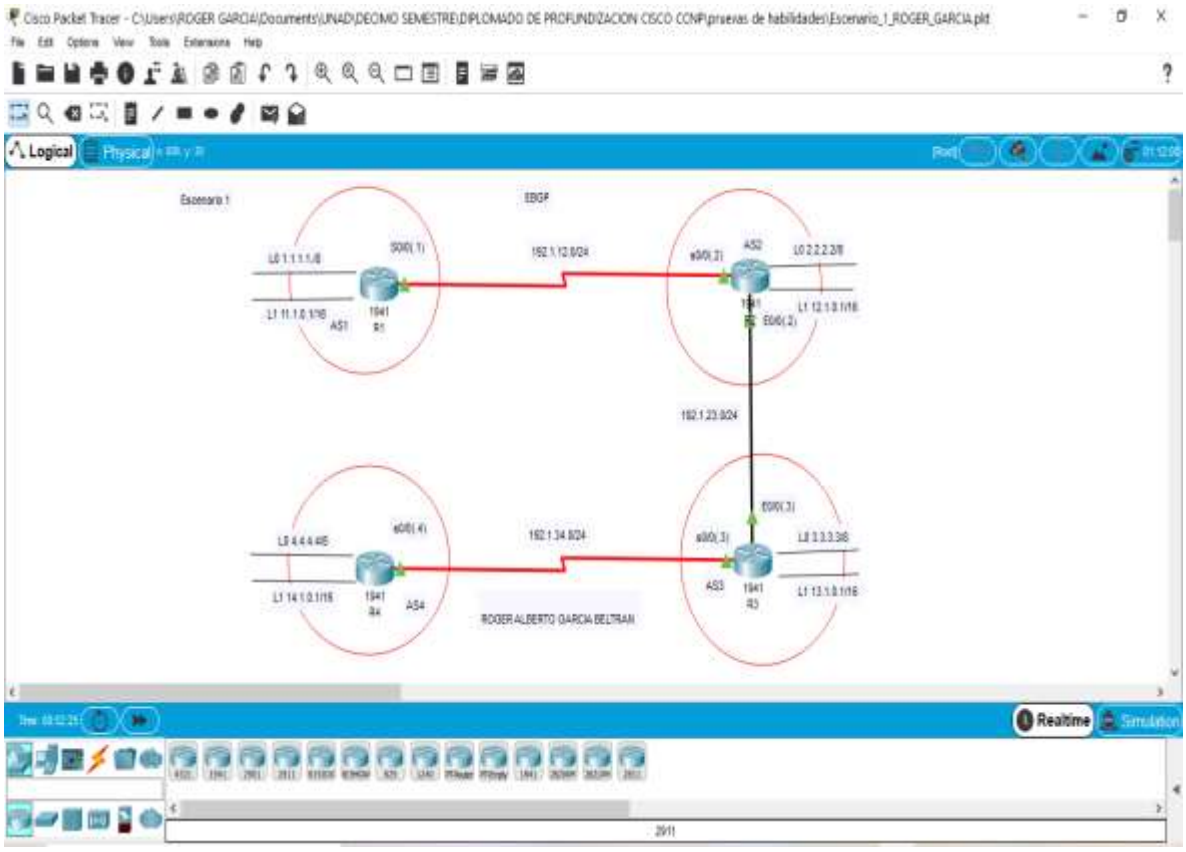


Figura 2. Montaje Escenario 1

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.***

R1

```
R1(config)# int s0/0/0
R1(config-if)# ip add 192.1.12.1 255.255.255.0
R1(config-if)# clockrate 64000
R1(config-if)#no shutdown
R1(config-if)#int loopback 0
R1(config-if)#ip add 1.1.1.1 255.0.0.0
R1(config-if)#int loopback 1
R1(config-if)#ip add 11.1.0.1 255.255.0.0
R1(config-if)#exit
```

R2

```
R2(config)# interface s 0/0/0
R2(config-if)# ip address 192.1.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface G0/0
R2(config-if)# ip address 192.1.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface loopback 0
R2(config-if)# ip address 2.2.2.2 255.0.0.0
R2(config-if)# interface loopback 1
R2(config-if)# ip address 12.1.0.1 255.255.0.0
```

R3

```
R3(config)#int s0/0/0
R3(config-if)#ip add 192.1.34.3 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config)#int g0/0
R3(config-if)#ip add 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
```

```
R3(config)#int loopback 0
R3(config-if)#ip add 3.3.3.3 255.0.0.0
R3(config-if)#int loopback 1
R3(config-if)#ip add 13.1.0.1 255.255.0.0
```

R4

```
R4(config)#int s0/0/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#int loopback 0
R4(config-if)#ip add 4.4.4.4 255.0.0.0
R4(config-if)#int loopback 1
R4(config-if)#ip add 14.1.0.1 255.255.0.0
```

CONFIGURACION BGP

R1

```
R1(config)#router bgp 1
R1(config-router)#no synchronization
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
```

R2

```
R2(config)#router bgp 2
R2(config-router)#no synchronization
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
```

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
     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       12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.1/32 is directly connected, Serial0/0/0

R1>
```

Figura 3. Tabla de enrutamiento R1

```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       2.0.0.0/8 is directly connected, Loopback0
L       2.2.2.2/32 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.1.0.0/16 is directly connected, Loopback1
L       12.1.0.1/32 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
 --More--
```

Figura 4. Tabla de enrutamiento R2

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.***

Configuración BGP

R2

R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3

R3

R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#no synchronization
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0

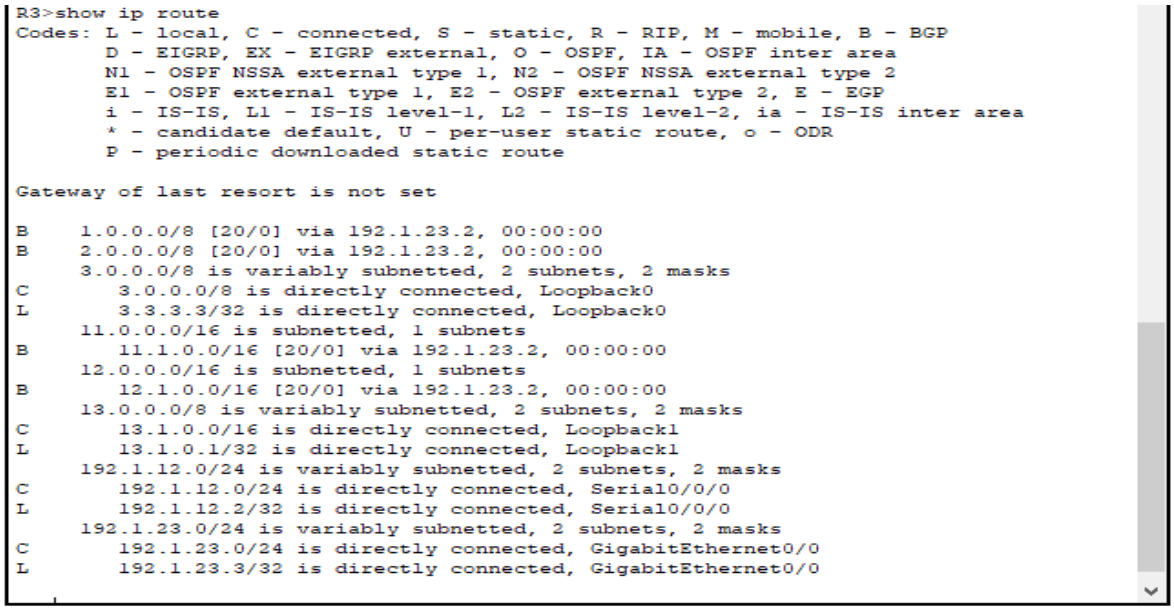
```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.0.0.0/8 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
B     3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.0.0/16 is directly connected, Loopback1
L        12.1.0.1/32 is directly connected, Loopback1
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial0/0/0
L        192.1.12.2/32 is directly connected, Serial0/0/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.2/32 is directly connected, GigabitEthernet0/0

R2>
```

Figura 5. Tabla de Enrutamiento 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
     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
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       13.1.0.0/16 is directly connected, Loopback1
L       13.1.0.1/32 is directly connected, Loopback1
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.2/32 is directly connected, Serial0/0/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.23.0/24 is directly connected, GigabitEthernet0/0
L       192.1.23.3/32 is directly connected, GigabitEthernet0/0
```

Figura 6. Tabla de enrutamiento R3

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

R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4

R4

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

```
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.0.0/16 is directly connected, Loopback1
L        13.1.0.1/32 is directly connected, Loopback1
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial0/0/0
L        192.1.12.2/32 is directly connected, Serial0/0/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
```

Figura 7. Tabla de enrutamiento 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     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
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       14.1.0.0/16 is directly connected, Loopback1
L       14.1.0.1/32 is directly connected, Loopback1
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.34.0/24 is directly connected, Serial0/0/0
L       192.1.34.4/32 is directly connected, Serial0/0/0

R4>
```

Figura 8. Tabla de enrutamiento R4

ESCENARIO 2

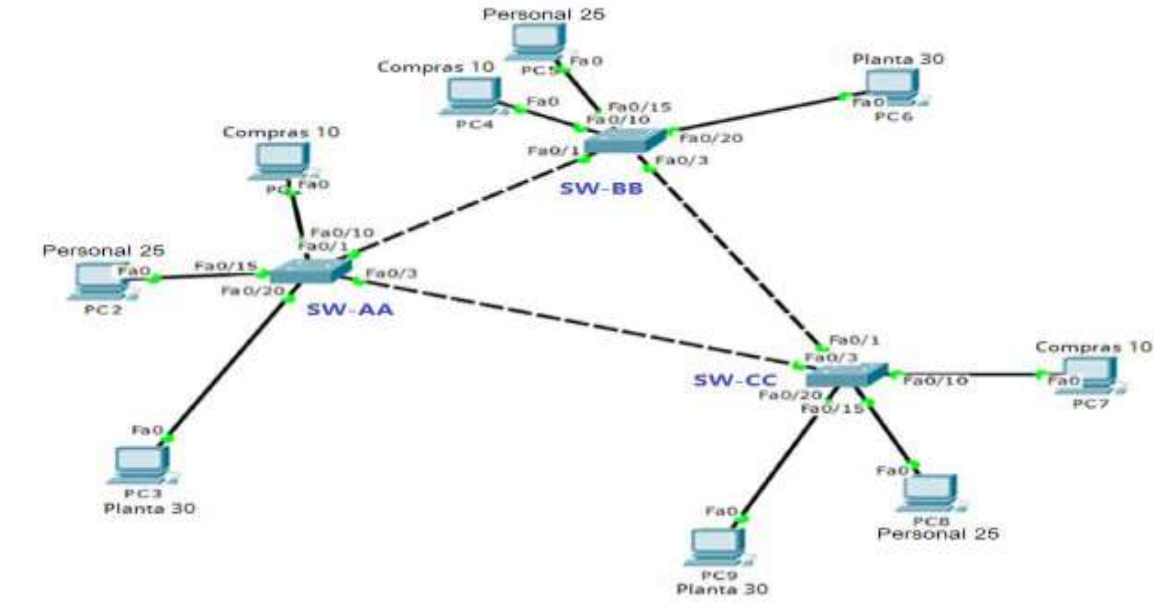


Figura 9. Escenario 2

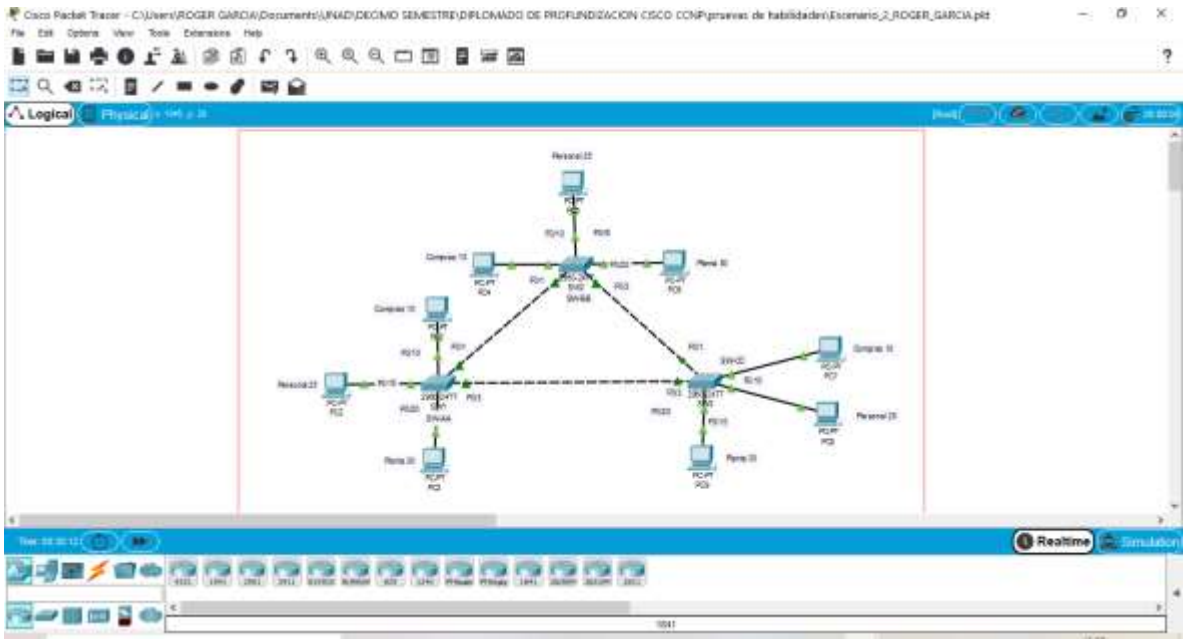


Figura 10. Montaje Escenario 2

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.

SW1

SW1(config)#vtp domain CCNP
SW1(config)#vtp mode client
SW1(config)#vtp password cisco
SW1(config)#vtp version 2

SW2

SW2(config)#vtp domain CCNP
SW2(config)#vtp mode server
SW2(config)#vtp password cisco
SW2(config)#vtp version 2

SW3

SW3(config)#vtp domain CCNP
SW3(config)#vtp mode client
SW3(config)#vtp password cisco
SW3(config)#vtp version 2

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

```
SW1>show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA4 0x20 0x0E 0x8B 0xB2 0xC2 0x9A
0x46
Configuration last modified by 0.0.0.0 at 3-1-93 02:31:24
SW1>
```

Figura 11 Estado vtp SW1

```
SW2>show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA4 0x20 0x0E 0x8B 0xB2 0xC2 0x9A
0x46
Configuration last modified by 0.0.0.0 at 3-1-93 02:31:24
Local updater ID is 190.108.99.2 on interface Vl99 (lowest numbered
VLAN interface found)
SW2>
```

Figura 12 Estado vtp SW2

```
SW3>show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA4 0x20 0x0E 0x8B 0xB2 0xC2 0x9A
0x46
Configuration last modified by 0.0.0.0 at 3-1-93 02:31:24
SW3>
```

Figura 13 Estado vtp SW3

B. Configurar DTP (Dynamic Trunking Protocol)

4. 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***.

SW1

SW1(config)#int fa0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport mode dynamic desirable

SW2

SW2(config)#int fa0/1
SW2(config-if)#switchport mode trunk

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

```
SW1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

SW1#
```

Figura 14 Interface trunk en SW1

```
SW2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

Figura 15. Interface trunk en SW2

6. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz F0/3 de SW-AA

SW1

SW1(config)#int f0/3
SW1(config-if)#switchport mode trunk

SW3

SW3(config)#int fa0/3
SW3(config-if)#switchport mode trunk

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

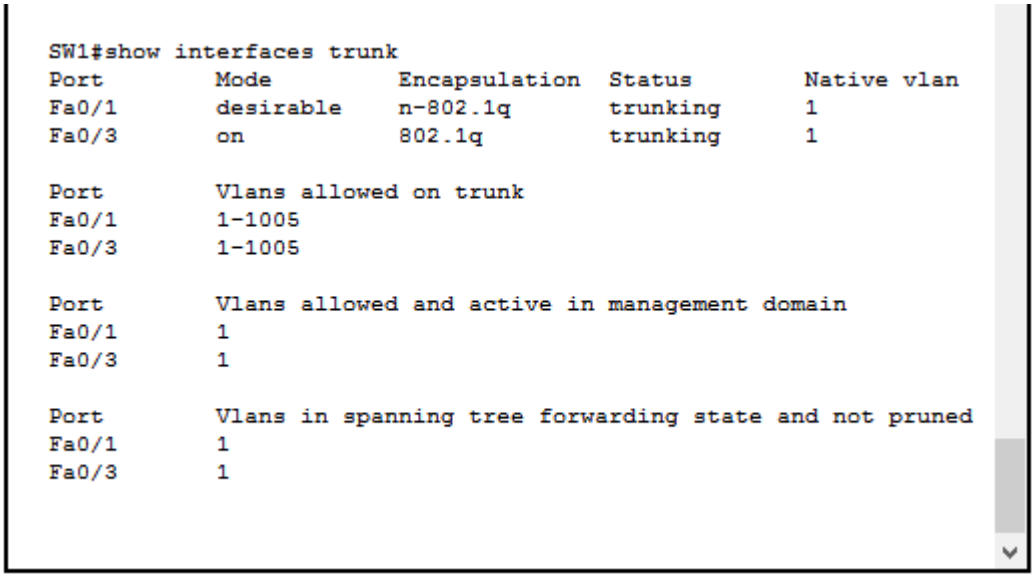


Figura 16 Interface trunk en SW-AA

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

SW2

SW2(config)#int fa0/3
SW2(config-if)#switchport mode trunk

SW3

SW3(config)#int fa0/1
SW3(config-if)#switchport mode trunk

C. Agregar VLANs y asignar puertos.
9. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

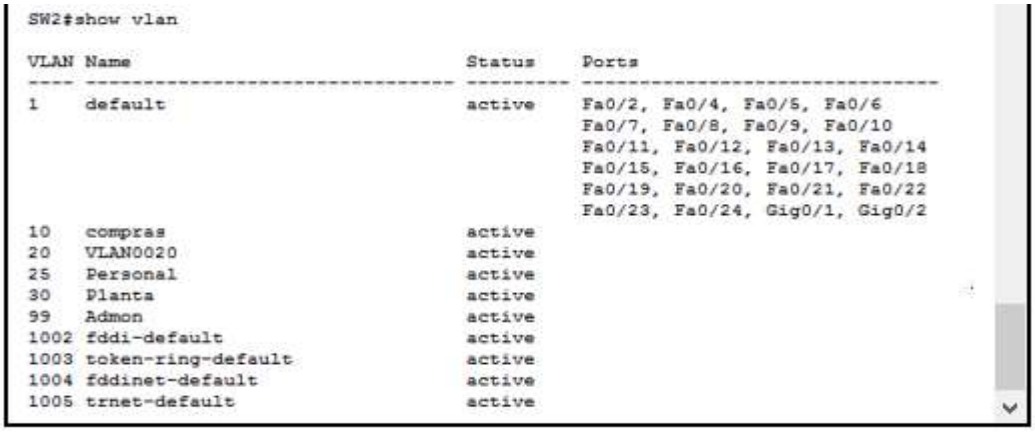
SW-AA

SW1(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.

SW-BB

SW2(config)#vlan 10
SW2(config-vlan)#name compras
SW2(config-vlan)#vlan 25
SW2(config-vlan)#name Personal
SW2(config-vlan)#vlan 30
SW2(config-vlan)#name Planta
SW2(config-vlan)#vlan 99
SW2(config-vlan)#name Admon

10. Verifique que las VLANs han sido agregadas correctamente.



```
SW2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   compras                          active
20   VLAN0020                         active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figura 17 Verificar VLAN en SW-BB

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

Interfaz	VLAN	Direcciones IP's de los PC's
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 VLAN'S

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

SW-AA

SW1(config)#int fa0/10
SW1(config-if)#switchport access vlan 10

SW-BB

SW2(config)#int fa0/10
SW2(config-if)#switchport access vlan 10

SW-CC
SW3(config)#int fa0/10
SW3(config-if)#switchport access vlan 10

13. 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

SW1(config)#int fa0/15
SW1(config-if)#switchport access vlan 20
SW1(config-if)#int fa0/20

SW1(config-if)#switchport access vlan 30

SW-BB

SW2(config)#int fa0/15
SW2(config-if)#switchport access vlan 20
SW2(config-if)#int fa0/20
SW2(config-if)#switchport access vlan 30

SW-CC

SW3(config)#int fa0/15
SW3(config-if)#switchport access vlan 20
SW3(config-if)#int fa0/20
SW3(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. Dirección IP Switches

SW-AA

SW1(config)#int vlan 99
SW1(config-if)#ip add 190.108.99.1 255.255.255.0
SW1(config-if)#no shutdown

SW-BB

SW2(config)#int vlan 99
SW2(config-if)#ip add 190.108.99.2 255.255.255.0
SW2(config-if)#no shutdown

SW-CC

SW3(config)#int vlan 99
SW3(config-if)#ip add 190.108.99.3 255.255.255.0
SW3(config-if)#no shutdown

E. Verificar la conectividad Extremo a Extremo

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

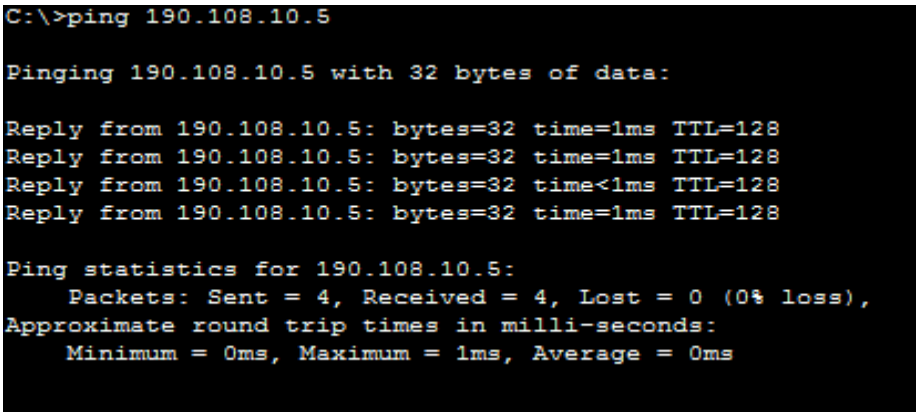


Figura 18 Ping errado

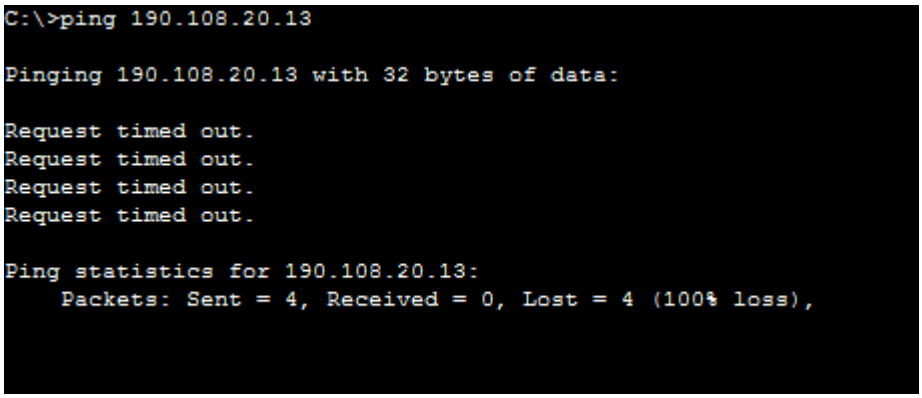


Figura 19 Ping Responde

El ping realizado entre los PCs pertenecientes a diferentes Vlans no tuvo éxito, sin embargo, los pings realizados a PCs que perteneces a la misma Vlan, si tuvieron éxito. El error en los PCs pertenecientes a diferentes Vlans se presenta ya que cada PC pertenece a un segmento de red diferente.

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

```
SW1#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
```

Figura 20. Ping Switches

```
SW1#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
```

Figura 21 Ping Switches

Se tiene conectividad ya que pertenecen a la misma VLAN

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

```
SW1#ping 190.108.20.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 22 Ping Switch a PC

El ping a diferente pc no tiene respuesta, debido a que no se tiene una interfaz wan dentro de la misma vlan configurada en el Switch, el tráfico se encuentra diferenciado entre vlan, no es posible que desde switch se obtenga respuesta a ping a cualquier PC.

CONCLUSIONES

Como resultado del desarrollo de los escenarios propuestos en la prueba de habilidades, es importante tener en cuenta la sintaxis a la hora de configurar los comandos en los activos de la topología para poder contextualizar los conocimientos teóricos y las habilidades practicas construidas a través del curso se realiza la aplicación y el uso de diferentes protocolo de enrutamiento con el fin anunciar rutas que se aprenden por otros medios para esto utilizamos una herramienta, Packet Tracer y SmartLab de cisco que nos permite realizar simulaciones configuraciones requeridas para cada dispositivo Al aplicar VLAN Trunking Protocol, se determina que es un protocolo usado para configurar y administrar VLANs en equipos Cisco. Los switches pueden operar en tres modos VTP diferentes Servidor–Cliente–Transparente. Así también, se logran determinar fallos y dar solución a estos, comprobando la configuración y la existencia de conexión lógica entre los dispositivos de las redes propuestas, empleando el protocolo ICMP y analizando el resultado obtenido con comandos show como: show running-config, show ip route, show interfaces trunk, show vtp status, show vlan brief. Entre otros.

En el módulo CCNP ROUTE y CCNP SWITCH se abordaron conceptos principales que son necesarios para el diseño de redes escalables mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red así realizar enrutamiento inter vlan como una mayor velocidad del tráfico de red, ya que, al no usarse toda la capacidad de la red, el router permite una comunicación de las subredes que pasan a través de sus interfaces.

Este diplomado nos permite conocer temas sobre redes de campus, que describen e implementan conceptos avanzados de VLANS y enrutamiento en la implementación de enrutadores Cisco escalables y altamente seguros que están conectados a LAN, WAN e IPv6. y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones

REFERENCIAS BIBLIOGRAFICAS

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de

https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP. Recuperado de https://repository.unad.edu.co/handle/10596/24419

García, V. S. (04 de Julio de 2017). Diseño de Redes con BGP. Obtenido de Universitat Politècnica de València: https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20-

%20Dise%C3%B1o%20de%20redes%20con%20BGP.pdf?sequence=1

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

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {Enlínea}.{Consultado junio 2009}. Disponibleen: http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otro_trabajos_de_grado/compendio_de_tesis_y_otros_trabajos_de_grado.asp?CodIdioma=ESP.

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

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

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de

https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl