DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDRÉS SALGADO ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
POPAYÁN
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDRÉS SALGADO ROMERO

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP PRUEBA DE HABILIDADES PRÁCTICAS – INGENIERÍA DE TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
POPAYÁN
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

POPAYAN, 22 de mayo de 2020

AGRADECIMIENTOS

En primer lugar doy gracias a Dios por mí existir, por regalarme la oportunidad y la sabiduría necesarias para salir adelante en esta carrera profesional que me propuse. Agradecimiento especial a mis padres, mis hermanas, y familiares que de una u otra manera han hecho posible la culminación de otra etapa más en mi vida. También agradezco a directivos, docentes y personal administrativo de la Universidad Nacional Abierta y a Distancia (UNAD) que han dado todos sus esfuerzos, conocimientos e interés para que cada uno de nosotros hayamos tenido logros positivos en este proceso. Así mismo, un agradecimiento a todos mis compañeros por su disposición y ánimo ya que esto permitió que el trabajo colaborativo fuese posible.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

CCNP: (Cisco Certified Network Professional) Es el nivel intermedio de certificación de la compañía cisco, por medio de este certificado se puede mejorar la calidad de montaje de escenarios mucho más complejos. Para la obtención de esta certificación, es necesario cursar y aprobar varias pruebas de conocimiento las cuales son divididas en 3 módulos.

ENRUTAMIENTO: El enrutamiento es el proceso en donde los Router aprenden sobre redes remotas, de esta manera encuentran y escogen todas las rutas posibles para llegar al destino de la manera más rápida y eficaz permitiendo el intercambio de datos entre estas rutas. O sea que los Router son los encargados de determinar y examinar las redes y direcciones ip de destino para enviar los paquetes de datos. Si por algún motivo el Router no determina ninguna ruta posible, por alguna falla en el enrutamiento este procede a descartar los paquetes que se envían y descarta el enrutamiento.

PROTOCOLO: Se refiere a las reglas y normas que ayudan en la regulación de la comunicación entre dos o más sistemas para la transmisión de información a través de medios físicos diversos. Se puede decir también, que son lenguajes o códigos de comunicación entre sistemas informáticos que se definen con base a una sintaxis, sincronización, semántica y métodos de recuperación de errores. Todo esto se implementa a través del hardware o software, o la combinación de ambos, brindando a cada participante en la comunicación una identidad y un método específico para el proceso de la información.

RED: Es un conjunto de dispositivos interconectados entre sí a través de un medio, los cuales intercambian información y comparten recursos en paquetes de datos transmitidos mediante impulsos eléctricos, ondas electromagnéticas o cualquier otro medio. Cuentan con un emisor, un receptor y un mensaje.

ROUTER: O enrutador, es un dispositivo que permite la interconexión de ordenadores en una red y opera en la capa 3, permitiendo que varias redes u ordenadores se conecten entre sí y de esta manera se comparta una misma conexión en los dispositivos de la red.

SWITCH: O conmutador, es un dispositivo de interconexión de redes informáticas y opera en la capa 2, permite filtrar y encaminar paquetes de datos entre segmentos de redes locales y ofrecer conexión a los equipos que conforman una subred LAN. Opera de manera similar a una pequeña central telefónica.

TOPOLOGÍA DE RED: Es la forma en que está diseñada la red, ya sea de manera física o lógica. También se puede definir como el conjunto de nodos interconectados entre si sobre un medio de comunicación. La topología de red está compuesta por dos partes, la topología física que es la disposición real de los cables y la topología lógica, que es la que define la forma en que los Host acceden a los medios.

VLAN: Es una expresión en ingles que significa Virtual Local Area Network, por lo que se puede afirmar que la idea de VLAN se refiere a una red de área local. Se utiliza para crear redes lógicas independientes dentro de una misma red física.

RESUMEN

“Prueba de habilidades prácticas” es una actividad evaluativa que se tiene en cuenta en el diplomado de profundización Cisco CCNP, identificando competencias y habilidades, donde se ponen a prueba niveles de comprensión y solución de problemas de networking. El desarrollo y solución de los dos escenarios se llevará a cabo con la utilización del simulador gráfico de red GNS3, el cual permite el diseño de topologías de redes complejas, como también poner en marcha simulaciones sobre ellas combinando dispositivos tanto reales como virtuales. El desarrollo de cada uno de los escenarios, tendrá su correspondiente descripción, de tal manera que se puede validar el correcto funcionamiento de los equipos y sus respectivas configuraciones. Todo esto está enmarcado dentro de las temáticas del programa de telecomunicaciones y el diplomado Cisco CCNP.

Palabras clave: Telecomunicaciones, Cisco CCNP, Redes, Networking, Protocolos

ABSTRACT

"Practical skills test" is an evaluative activity that takes into account the Cisco CCNP deepening diploma, identifying competencies and skills, where you can take a test of understanding levels and solving network problems. The development and solution of the two scenarios will be carried out with the use of the GNS3 graphical network simulator, which allows the design of complex network topologies as well as to run simulations on them combining both real and virtual devices. The development of each of the scenarios will have its corresponding description so that the correct operation of the equipment and its respective settings can be validated. All this is framed within the themes of the telecommunications program and the Cisco CCNP diploma.

Keywords: Telecommunications, Cisco CCNP, Networks, Networking, Protocols

INTRODUCCIÓN

Las telecomunicaciones son un pilar fundamental dentro del avance tecnológico y científico creado por el ser humano. Mediante las grandes redes de comunicación el mundo puede compartir información a, y desde grandes distancias, permitiendo que el conocimiento se esparza y que día tras día haya innovación tecnológica y por supuesto que la seguridad y la conexión de estas redes también se haga de manera detallada y que durante su proceso se vayan perfeccionando, de tal manera que la información enviada y recibida sea clara y sin ninguna clase de alteración.

Por lo tanto, el siguiente trabajo tiene como objetivo dar a conocer el desarrollo de la Evaluación – Prueba de habilidades prácticas CCNP, mediante la cual se busca identificar el grado de desarrollo de competencias y habilidades que ponen a prueba el nivel de comprensión y solución de escenarios de Networking, a través del desarrollo de tareas en los dos (2) escenarios que se proponen, y de esta manera, realizar los procesos de configuración de todos los dispositivos presentes en las topologías propuestas.

También se hace una descripción detallada de las etapas, procesos y verificación del uso de los comandos y configuraciones que sean aplicadas a los dispositivos presentes en la red.

1. DESARROLLO ESCENARIO 1

Descripción de escenarios propuestos para la prueba de habilidades

1.1 Topología Escenario 1

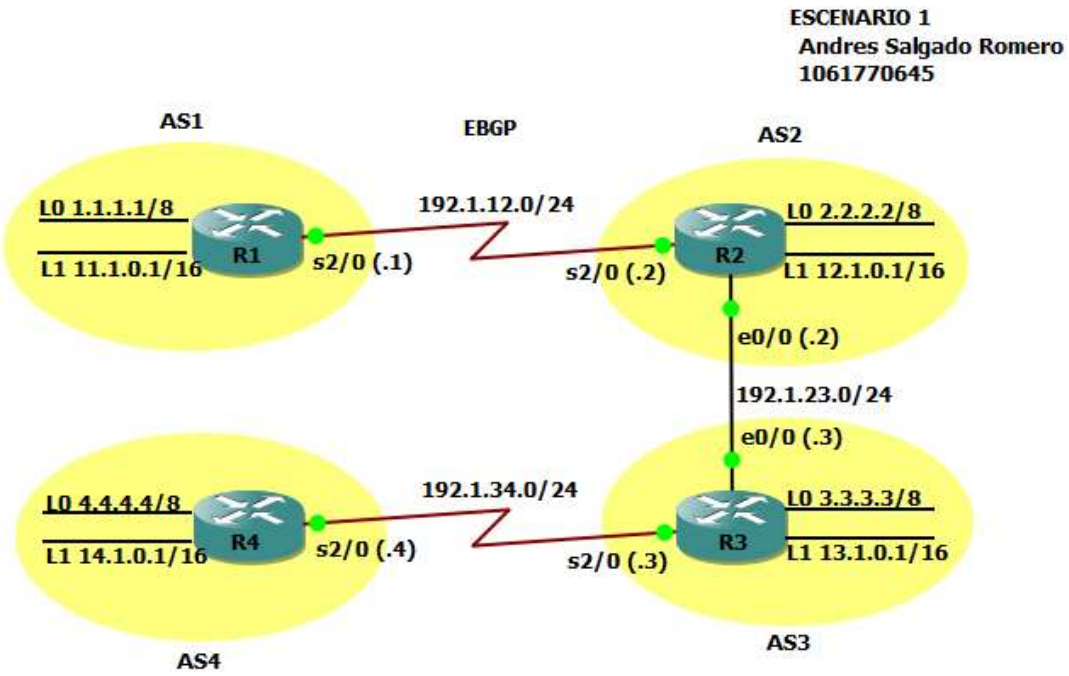

Figura 1 Topología escenario 1

En el escenario propuesto en la anterior ilustración se describe una topología de red LAN que hace uso de cuatro (4) Router para la comunicación entre sí.

Es así, que para esta topología se va a configurar el protocolo EBGP mediante el cual los Router podrán realizar el correcto direccionamiento y búsqueda de las respectivas rutas de cada Router vecino en la red y de esta manera establecer una conexión rápida y eficaz, permitiendo que los paquetes que sean enviados no sufran ningún tipo de pérdida y lleguen completamente a su destino.

Mediante el uso de los Loopback para cada Router se mantendrá latente el protocolo de enrutamiento EBGP, ya que al no configurarlo, después de cierto tiempo de inactividad en las interfaces de los Router estos proceden a descartar los protocolos configurados, haciendo que la conexión falle y no se pueda enviar ni recibir paquetes desde cualquier dispositivo.

1.2 Información para configuración de los Router

Tabla 1 Configuración R1

Interfaz	Dirección IP	Mascara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S2/0	192.1.12.1	255.255.255.0

Tabla 2 Configuración R2

Interfaz	Dirección IP	Mascara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S2/0	192.1.12.2	255.255.255.0
E0/0	192.1.23.2	255.255.255.0

Tabla 3 Configuración R3

Interfaz	Dirección IP	Mascara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E2/0	192.1.23.3	255.255.255.0
S0/0	192.1.34.3	255.255.255.0

Tabla 4 Configuración R4

Interfaz	Dirección IP	Mascara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S2/0	192.1.34.4	255.255.255.0

1.3 Configuración de relación de vecino BGP entre R1 y R2

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 Router 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***.

Se borran configuraciones previas en los Router y se configuran parámetros básicos en cada uno utilizando los siguientes comandos.

[R1]

```
R1#erase startup-config
R1#reload
Router>enable
Router#configure terminal
Router(config)#ip domain-name CCNP.NET
Router(config)#no ip domain lookup
Router(config)#line con 0
Router(config-line)#no exec-timeout
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#hostname R1
```

[R2]

```
R1#erase startup-config
R1#reload
Router>enable
Router#configure terminal
Router(config)#ip domain-name CCNP.NET
Router(config)#no ip domain lookup
Router(config)#line con 0
Router(config-line)#no exec-timeout
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#hostname R2
```

[R3]

```
R1#erase startup-config
R1#reload
Router>enable
Router#configure terminal
Router(config)#ip domain-name CCNP.NET
Router(config)#no ip domain lookup
Router(config)#line con 0
```

```
Router(config-line)#no exec-timeout
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#hostname R3
```

[R4]

```
R1#copy running-config startup-config
R1#erase startup-config
R1#reload
Router>enable
Router#configure terminal
Router(config)#ip domain-name CCNP.NET
Router(config)#no ip domain lookup
Router(config)#line con 0
Router(config-line)#no exec-timeout
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#hostname R4
```

Procedemos a realizar la respectiva configuración planteada en el punto 1.3

[R1]

```
R1#configure terminal
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
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)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```

[R2]

```
R2#configure terminal
R2(config)#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
R2(config-if)#interface serial 2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface ethernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
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
```

```
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
       a - application route
       + - 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, 00:01:07
      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, 00:01:07
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.1/32 is directly connected, Serial2/0
```

Figura 2 R1 - show ip router

```
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
       a - application route
       + - 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, 00:02:04
      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, 00:02:04
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.0.0/16 is directly connected, Loopback1
L        12.1.0.1/32 is directly connected, Loopback1
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.2/32 is directly connected, Serial2/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.2/32 is directly connected, Ethernet0/0
```

Figura 3 R2 - show ip router

Como se observa en las anteriores ilustraciones, el comando ***show ip route*** aplicado en R1 y R2 nos muestra las respectivas tablas de enrutamiento, con información sobre las direcciones de las redes a las cuales se encuentran directamente conectadas las interfaces. Igualmente se ven las direcciones de los Loopback y las direcciones de los Router vecinos. La interface s2/0 en este caso es reconocida como vía para las rutas del enlace físico y su dirección de red seria 192.1.12.0/24.

1.4 Configuración de una relación de vecino BGP entre R2 y R3

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]

```
R2#configure terminal
```

```
R2(config)#router bgp 2
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]

```
R3#configure terminal
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface ethernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
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)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

```
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
       a - application route
       + - 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, 00:11:29
      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, 00:00:21
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:11:29
      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, 00:00:21
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.2/32 is directly connected, Serial2/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.2/32 is directly connected, Ethernet0/0
```

Figura 4 R2 - show ip router

```
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
       a - application route
       + - 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, 00:01:18
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:18
      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 [20/0] via 192.1.23.2, 00:01:18
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:01:18
      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
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:01:18
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.3/32 is directly connected, Ethernet0/0
```

Figura 5 R3 - show ip router

Como se observa en las anteriores ilustraciones, al ejecutar el comando ***show ip route*** en R2 se actualiza la tabla de enrutamiento mostrando la ruta física y los Loopback que comunican con R3, mientras que en R3 la tabla de enrutamiento muestra solo las redes conocidas por el que son sus propios Loopback y la red física que tiene establecida con R2 y la ruta aprendida de R1 mediante BGP por su relación de adyacencia con R2.

1.5 Configuración de una relación de vecino BGP entre R3 y R4

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#configure terminal
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
```

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

[R4]

```
R4#configure terminal
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 2/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
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
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

Para que se puedan establecer correctamente las adyacencias mediante los Loopback, el Router vecino informa sobre el uso de la interfaz Loopback.

[R3]

```
R3#configure terminal
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
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)#neighbor 4.4.4.4 ebgp-multihop
```

[R4]

```
R4#configure terminal
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
```

```
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
       a - application route
       + - 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, 00:17:15
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:17:15
      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, 00:17:15
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:17:15
      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
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:17:15
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.3/32 is directly connected, Ethernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial2/0
L        192.1.34.3/32 is directly connected, Serial2/0
```

Figura 6 R3 - show ip route

```
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
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

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
      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, Serial2/0
L        192.1.34.4/32 is directly connected, Serial2/0
```

Figura 7 R4 - show ip route

Como se observa en las anteriores ilustraciones, al ejecutar el comando ***show ip route*** en R3 se actualiza la tabla de enrutamiento y ahora vemos que tiene comunicación hacia el Loopback0 de R4 mediante la vía de conexión física correspondiente a 192.1.34.4/24 que sería en este caso la interface s2/0.

En R4 podemos observar que se comunica hacia el Loopback0 de R3 mediante la vía del serial 2/0 en R3.

En R3 los demás vecinos no sufren alteraciones ya que las otras rutas no se ven afectadas por el cambio en las rutas estáticas creadas para el Loopback 0 del otro Router, por lo tanto las tablas de enrutamiento en esa parte siguen siendo iguales.

2. DESARROLLO ESCENARIO 2

2.1 Topología escenario 2

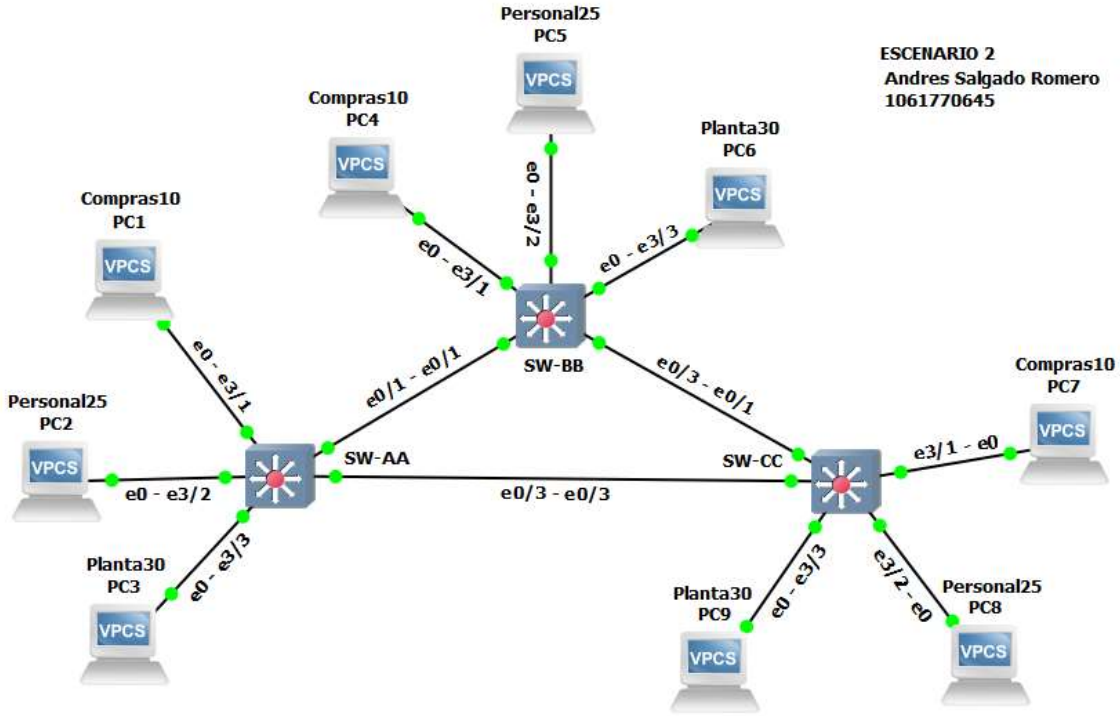

Figura 8 Topología escenario 2

En el escenario propuesto en la anterior ilustración, se describe una topología de red con 3 Switch, los cuales tienen conectados por la interfaces e3/1-3 equipos finales PC, cada equipo en el Switch estará alojado en una VLAN diferente para comunicarse solo entre equipos PC alojados en la misma VLAN y cada Switch se conectará a sus iguales por medio de un enlace troncal.

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.

Se borran configuraciones previas en los Switch y se configuran parámetros básicos en cada uno utilizando los siguientes comandos.

[SW-AA]

```
Switch#dir
```

```
Switch#delete nvram_00001
Switch#delete startup-config.cfg
Switch#reload
Switch>enable
Switch#configure terminal
Switch(config)#ip domain-name CCNP.NET
Switch(config)#no ip domain lookup
Switch(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname SW-AA
SW-AA(config)#interface range e0/1, e0/3, e3/1-3
SW-AA(config-if-range)#no shutdown
```

[SW-BB]

```
Switch#dir
Switch#delete nvram_00002
Switch#delete startup-config.cfg
Switch#reload
Switch>enable
Switch#configure terminal
Switch(config)#ip domain-name CCNP.NET
Switch(config)#no ip domain lookup
Switch(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname SW-BB
SW-BB(config)#interface range e0/1, e0/3, e3/1-3
SW-BB(config-if-range)#no shutdown
```

[SW-CC]

```
Switch#dir
Switch#delete nvram_00003
```

```
Switch#delete startup-config.cfg
Switch#reload
Switch>enable
Switch#configure terminal
Switch(config)#ip domain-name CCNP.NET
Switch(config)#no ip domain lookup
Switch(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname SW-CC
SW-CC(config)#interface range e0/1, e0/3, e3/1-3
SW-CC(config-if-range)#no shutdown
```

Procedemos a realizar la respectiva configuración planteada en el punto A. 1.

[SW-AA]

```
SW-AA#configure terminal
SW-AA(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco
```

[SW-BB]

```
SW-BB#configure terminal
SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco
```

[SW-CC]

```
SW-CC#configure terminal
SW-CC(config)#vtp mode client
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 capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
```

Figura 9 SW-AA show vtp status

```
SW-BB#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
```

Figura 10 SW-BB show vtp status

```
SW-CC#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
```

Figura 11 SW-CC show vtp status

B. Configurar DTP (Dynamic Trunking Protocol)

3. 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]

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

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

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
SW-AA#
```

Figura 12 SW-AA show interfaces trunk

```
SW-BB#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
```

Figura 13 SW-BB show interfaces trunk

5. 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

[SW-AA]

```
SW-AA#configure terminal
SW-AA(config)#interface ethernet 0/3
SW-AA(config-if)#switchport mode trunk
```

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

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       auto             n-802.1q       trunking      1
Et0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
Et0/3       1
```

Figura 14 SW-AA show interfaces trunk

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

[SW-CC]

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

C. Agregar VLANs y asignar puertos.

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

[SW-AA]

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

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#
```

Figura 15 SW-AA show interfaces trunk (Error crear vlan10)

[SW-BB]

```
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
```

9. Verifique que las VLANs han sido agregadas correctamente.

```
SW-AA#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 16 SW-AA show vlan brief

```
SW-BB#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 17 SW-BB show vlan brief

```
SW-CC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 18 SW-CC show vlan brief

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

Tabla 5 Puertos VLAN y direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
E3/1	VLAN 10	190.108.10.X/24
E3/2	VLAN 25	190.108.20.X/24
E3/3	VLAN 30	190.108.30.X/24

X = Número de cada PC particular

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

12. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

[SW-AA]

```
SW-AA#configure terminal
SW-AA(config)#interface ethernet 3/1
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface ethernet 3/2
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface ethernet 3/3
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

[SW-BB]

```
SW-BB#configure terminal
SW-BB(config)#interface ethernet 3/1
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#interface ethernet 3/2
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface ethernet 3/3
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
```

[SW-CC]

```
SW-CC#configure terminal
SW-CC(config)#interface ethernet 3/1
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface ethernet 3/2
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#interface ethernet 3/3
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

[PC1, PC2, PC3]

`ip 190.108.10.1/24` $\rightarrow vlan10$

`ip 190.108.20.2/24` $\rightarrow vlan25$

`ip 190.108.30.3/24` $\rightarrow vlan30$

[PC4, PC5, PC6]

`ip 190.108.10.4/24` → $vlan10$

`ip 190.108.20.5/24` → $vlan25$

`ip 190.108.30.6/24` → $vlan30$

[PC7, PC8, PC9]

`ip 190.108.10.7/24` → $vlan10$

`ip 190.108.20.8/24` → $vlan25$

`ip 190.108.30.9/24` → $vlan30$

D. Configurar las direcciones IP en los Switches.

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

Tabla 6 Direcciones IP para SVI en VLAN 99

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

[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
```

[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
```

[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

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

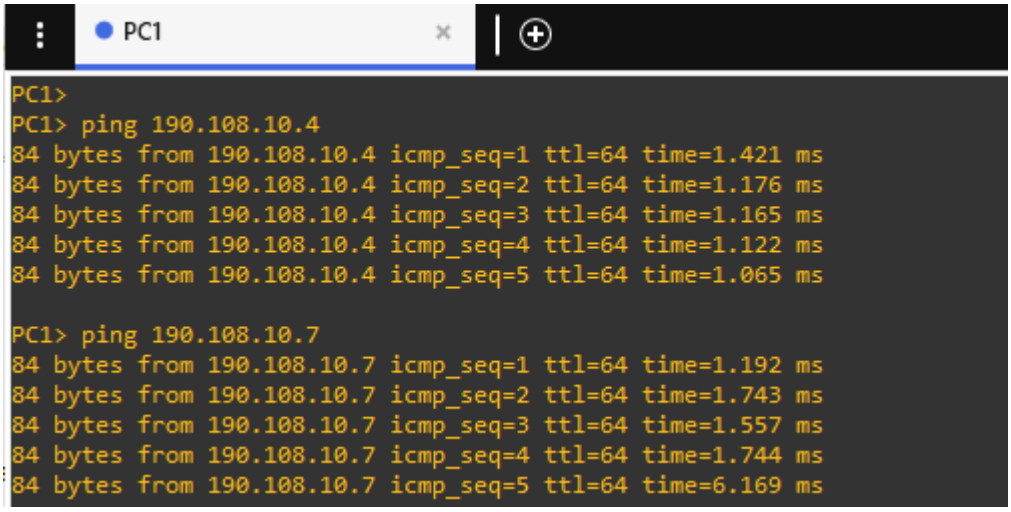

Figura 19 PC1 ping equipos VLAN 10

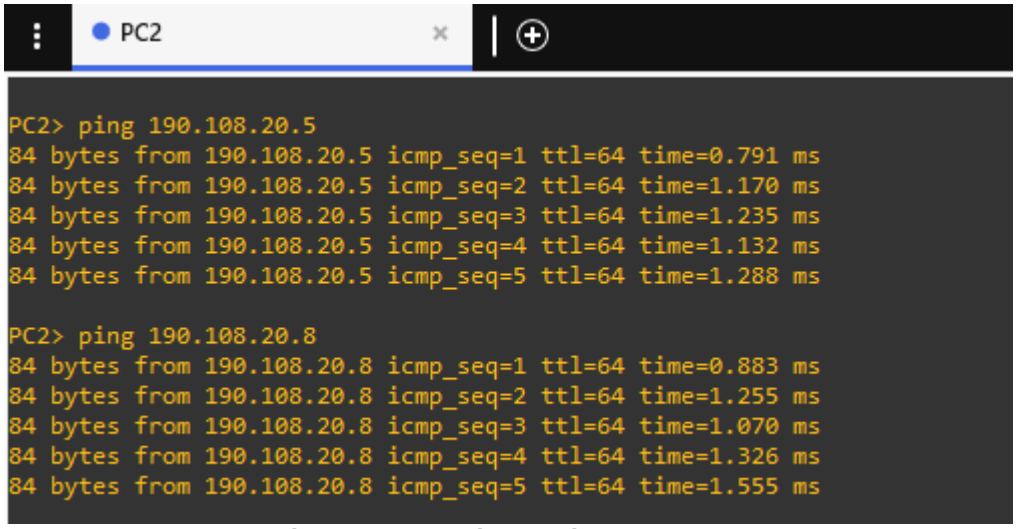

Figura 20 PC2 ping equipos VLAN 25

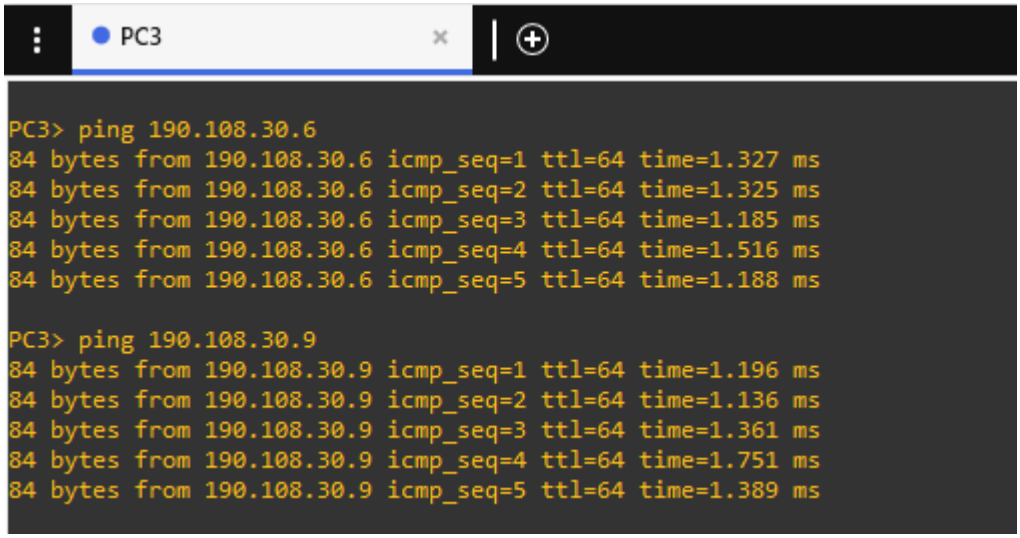

Figura 21 PC1 ping equipos VLAN 30

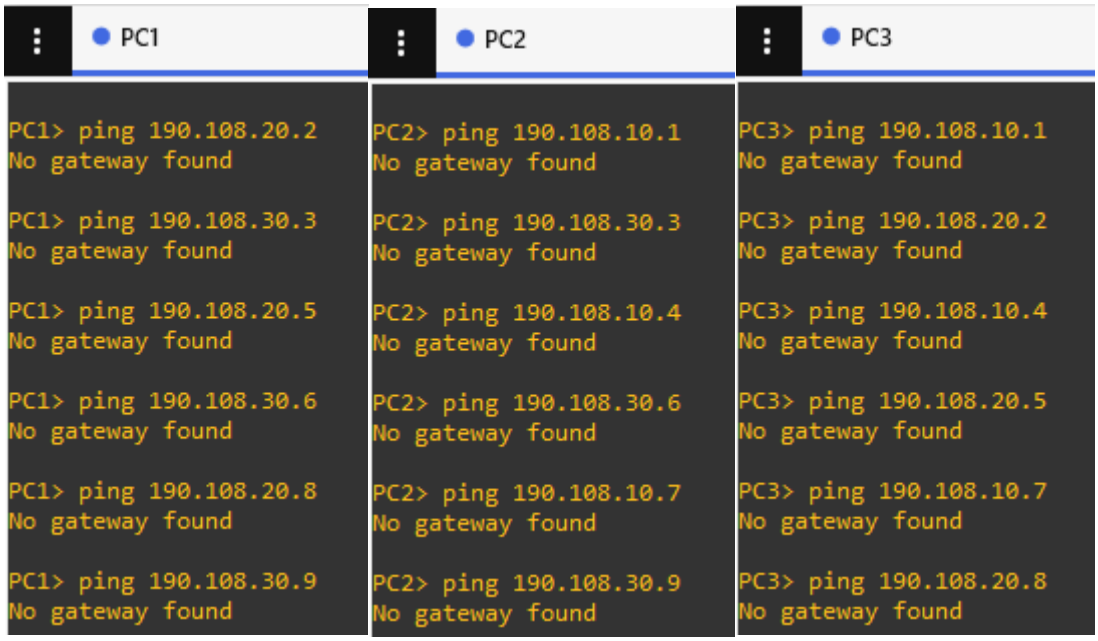

Figura 22 PC1 - PC2 -PC3 ping equipos de otras VLAN

En las ilustraciones podemos ver que al efectuar el comando ping entre equipos pertenecientes a las misma VLAN obtenemos una respuesta afirmativa, mientras que si efectuamos el ping hacia un equipo de una VLAN diferente la respuesta es errónea, estos resultado se obtienen ya que cada PC corresponde a un segmento de red diferente (VLAN10, VLAN25, VLAN30), dejando como resultado la respuesta afirmativa solo en los equipos pertenecientes a la misma VLAN y una respuesta negativa en los equipos pertenecientes a VLAN diferente.

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

Por motivos de compatibilidad en los comandos de la IOS de los Switch que utilice para realizar esta simulación no puede efectuar el ping de Switch a Switch en GNS3, por tal motivo migré toda la configuración a Packet Tracer, utilizando las mismas configuraciones que había realizado en GNS3 obteniendo los resultados esperados. De esta manera las capturas de pantalla que se ven a continuación son el producto de la simulación del ejercicio tal como fue programado en GNS3.

En el archivo .RAR final queda evidencia de las 2 simulaciones, tanto en GNS3 como en Packet Tracer.

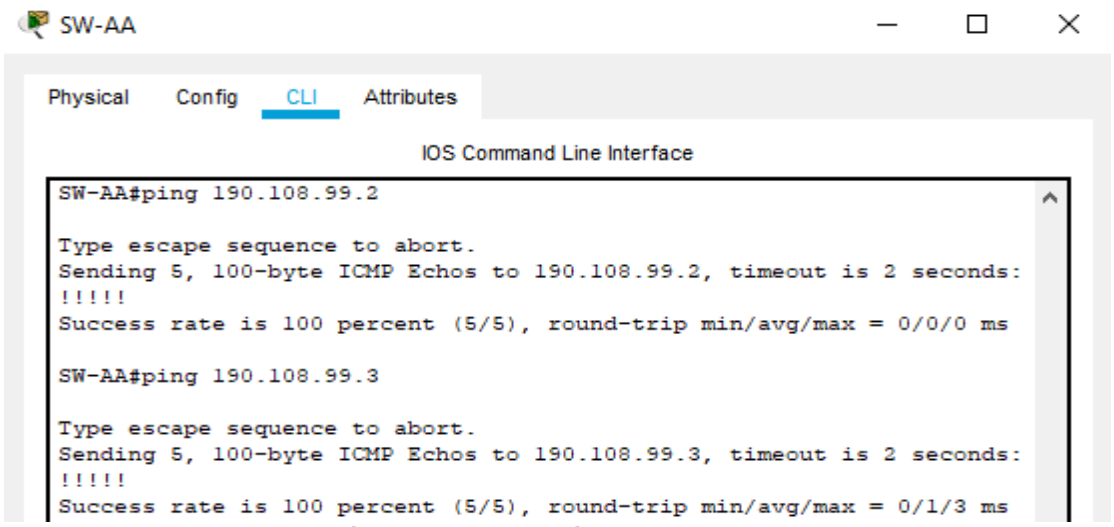

Figura 23 SW-AA ping a SW-BB y SW-CC

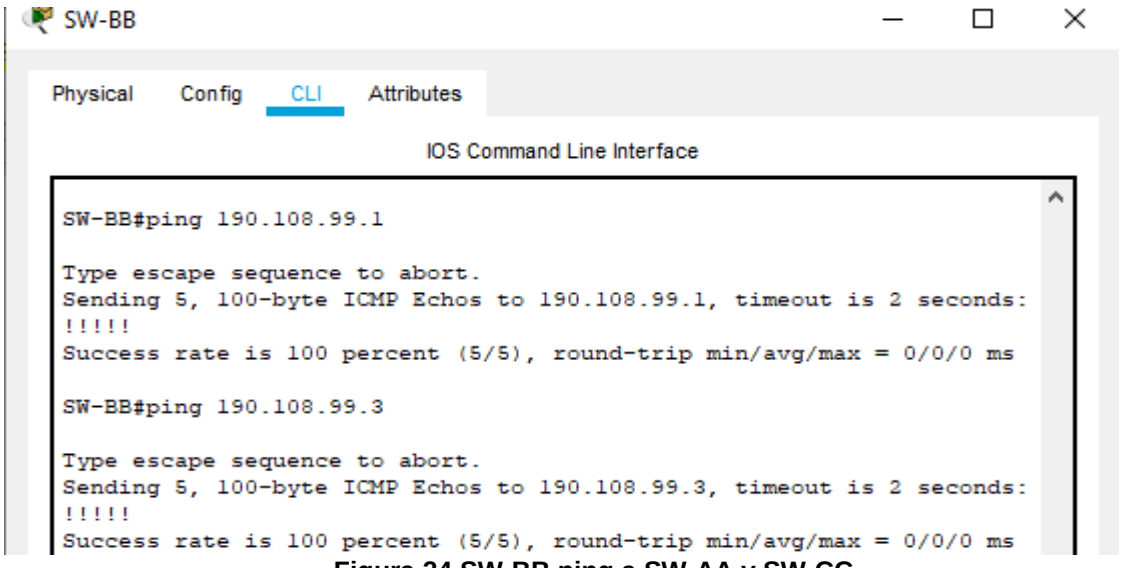

Figura 24 SW-BB ping a SW-AA y SW-CC

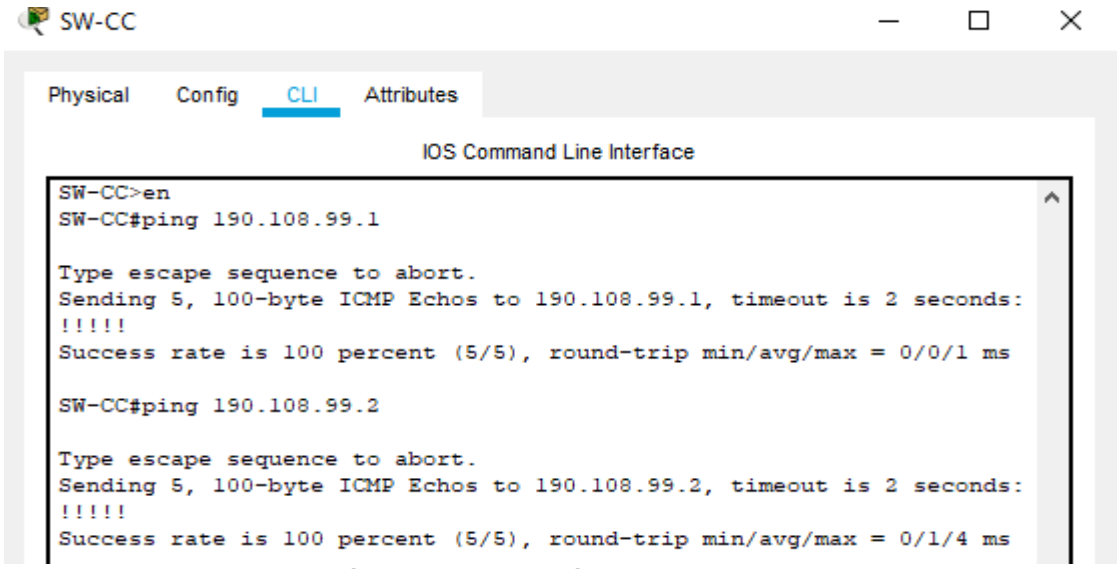

Figura 25 SW-CC ping a SW-AA y SW-BB

En las ilustraciones podemos ver que la prueba ping de Switch a Switch fue exitosa ya que los enlaces de los Switch están en modo ***trunk*** y los datos son enviados a través del protocolo ICMP, así como también el encapsulamiento que comparten los Switch es compatible en cada uno de ellos.

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

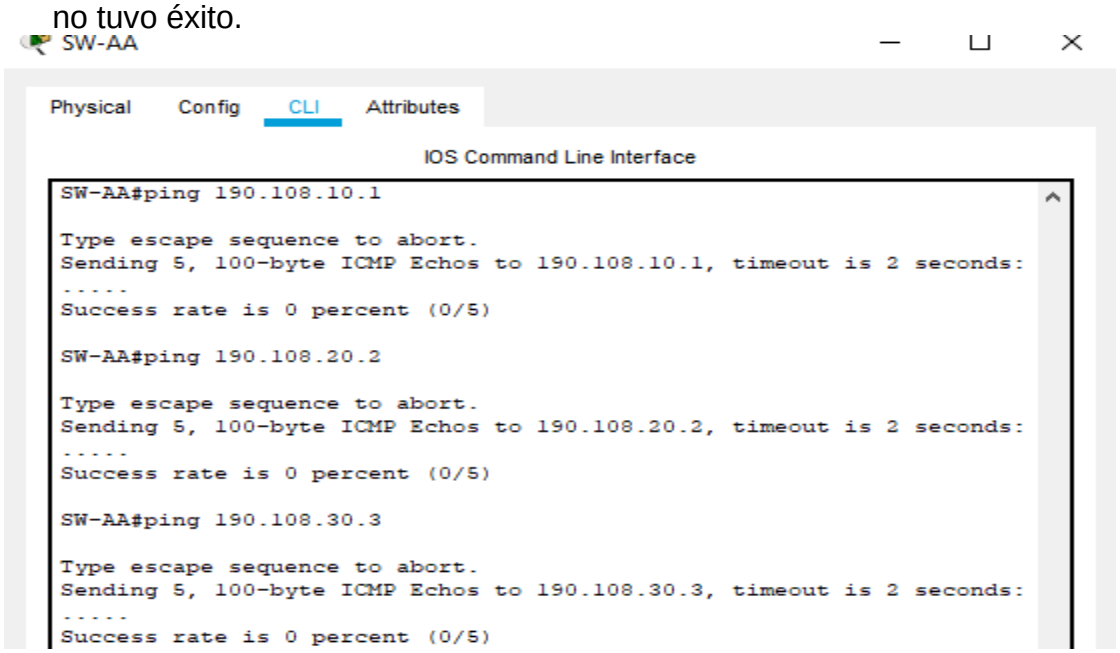

Figura 26 SW-AA ping equipos VLAN 10, 25, 30

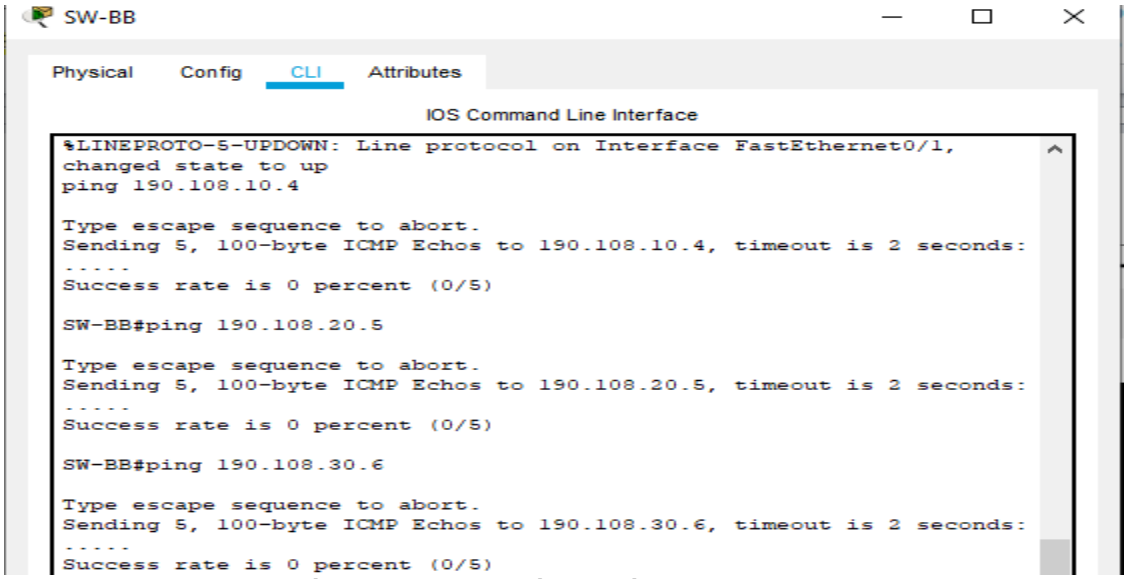

Figura 27 SW-BB ping equipos VLAN 10, 25, 30

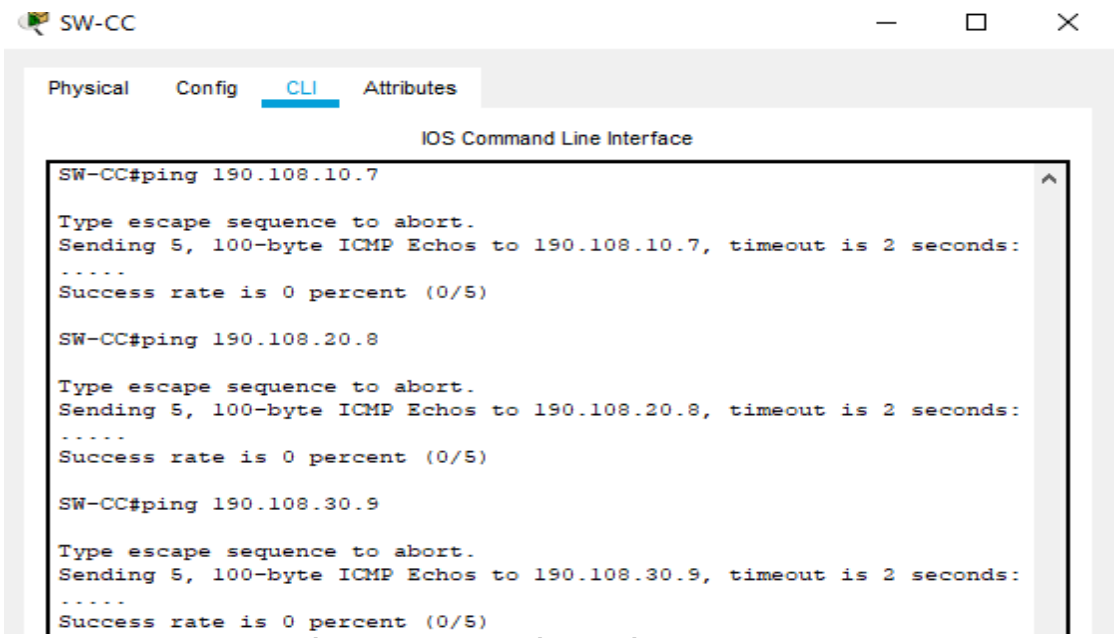

Figura 28 SW-CC ping equipos VLAN 10, 25, 30

En las ilustraciones podemos ver que la prueba ping Switch a PC no es exitosa, el motivo de que esto ocurra, es porque las VLAN presentes en la red no cuentan aún con direccionamiento IP, por ello para dar solución a este inconveniente sería necesario configurar dirección IP y máscara de subred en cada una de las interfaces de las VLAN en los Switch, teniendo siempre en cuenta utilizar los mismos segmentos de red de los equipos PC presentes en la red. Entonces los Switch en este caso sirven básicamente de carretera para el envió de información, ya sea entre ellos mismos o de PC a PC (en el mismo segmento de red).

CONCLUSIONES

La actividad Evaluación – Prueba de habilidades prácticas CCNP tiene una gran relevancia, puesto que mediante ella se han logrado profundizar los módulos Routing y Switching presentados por Cisco Networking Academy que son elementos formativos que permiten conocer la manera de gestionar redes para así aumentar la velocidad de acceso a la información y administrarla de manera eficiente. Esto permite que se puedan configurar y operar de manera simulada tanto pequeñas como grandes redes haciendo uso de diversos protocolos (BGP, VTP, OSPF, EIGRP, HSRP, GLBP, entre otros) y redes virtuales (VLAN), logrando una mejor administración de las redes propuestas.

La implementación de diversos protocolos de seguridad tienen como finalidad hacer que la comunicación sea clara, además de tener cuidado con la información enviada a través de las redes de telecomunicaciones o las redes limitadas en las que los usuarios pueden usar contraseñas y/o protocolos de lectura entre Routers que indican si se puede o no hacer el envío o recepción de la información. Dichos protocolos permiten que una comunicación sea rápida, certera y eficaz.

Además de lo anterior, se cuenta con redes LAN Virtuales (VLAN) que son un método que permite crear redes lógicas independientes dentro de una misma red física y tienen grandes beneficios ya que garantizan la seguridad y la administración de los equipos de manera eficaz. Un usuario puede tener varias VLAN dentro de un mismo Router. Las VLAN ayudan también a la reducción de sobrecarga de la CPU en cada dispositivo y evitan riesgos de que estos fallen. Otra ventaja que ofrecen las VLAN es mejorar la seguridad de los clientes que hacen envío de datos sensibles y para solucionar problemas de manera más rápida.

BIBLIOGRAFÍA

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

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

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

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

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

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

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

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

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. 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

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

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