PRUEBA DE HABILIDADES PRÁCTICAS

JORGE LUIS GUERRERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA_UNAD
ESCUELA DE CIENCIAS BASICAS E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
POPAYAN CAUCA
MAYO 2020

PRUEBA DE HABILIDADES PRÁCTICAS

JORGE LUIS GUERRERO

DIPLOMADO DE PROFUNDIZACION CISCO CCNP

GERARDO GRANADOS ACUÑA
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA_UNAD
ESCUELA DE CIENCIAS BASICAS E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
POPAYAN CAUCA
MAYO 2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Popayán, 15 de mayo de 2020

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

CCNP: (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

DOMINIO: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

ETHERNET: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

FIREWALL: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

HOST: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas. Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

INTERFACE: Interfaz o interface es el punto de conexión ya sea dos componentes de hardware, dos programas o entre un usuario y un programa.

IP PRIVADO: Las IPs privadas sirven para proveer conectividad entre equipos internos sin que se pueda acceder directamente a Internet (se debería definir un NAT). Los routers descartan los paquetes con direccionamiento privado desde la interfaz outsider (salvo problema de seguridad) por lo que como mucho podríamos lanzar paquetes pero nunca podría contestar ya que no se podría saber cómo “volver“.

IPV6: Con el crecimiento exponencial de las computadoras, el sistema de direcciones IP, IPv4, se va a quedar sin direcciones IP. Entra en acción IPv6, también llamado IPng (IP Next Generation - IP de Nueva Generación); es la siguiente versión planificada para el sistema de direcciones IP.

PROTOCOLO: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

ROUTER: Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.

SWITCH: Un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

RESÚMEN

El presente informe tiene como finalidad dar a conocer los pasos correspondientes a la configuración de dos escenarios los cuales hacen parte de la prueba de habilidades prácticas del diplomado de profundización Cisco Certified Network Professional CCNP.

Además, describe detalladamente los pasos de las configuraciones, también contiene imágenes que corresponde a los comandos empleados y resultados obtenidos en cada uno de los escenarios.

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

ABSTRACT

The present work aims the steps corresponding to the configuration of two scenarios which are part of the practical skills test of the Cisco Certified Network Professional CCNP.

Also, it describes in detail the steps of the configurations, also contains images corresponding to the commands used and results obtained in each of the scenarios.

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

INTRODUCCIÓN

CCNP CISCO tiene un avanzado currículo que ayuda a desarrollar las habilidades necesarias para complementar con éxito títulos universitarios afines con las TIC, brinda una gran experiencia de aprendizaje con una carga tanto teórica como práctica que abarca habilidades avanzadas de Routing y Switching.

El diplomado de Cisco Certified Network Professional CCNP se encuentra diseñado para personas que deseen continuar con su preparación académica y seguir adquiriendo habilidades de gestión de redes orientadas hacia el mundo laboral, profesional y empresarial.

Teniendo en cuenta el concepto, además de tener claridad del objetivo de CCNP (Cisco Certified Network Professional), finalmente el presente trabajo pretende desarrollar los laboratorios propuestos en el diplomado CISCO CCNP y brindar solución a las configuraciones las cuales se desarrollaron en los programas de simulación GNS3 Y Packet Tracer.

1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1.1 Escenario 1

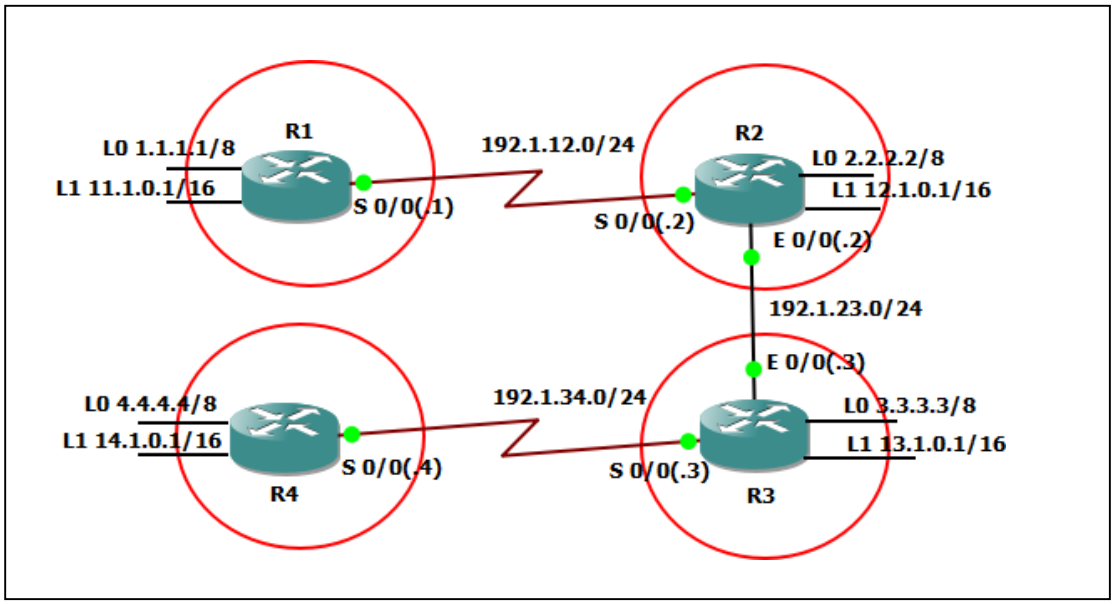

Figura 1. Topología1

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

Tabla 1. Router1

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 2. Router2

Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

Tabla 3. Router3

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

Tabla 4. Router 4.

Para este primer escenario usamos el simulador GNS3, por lo tanto, se configuran las interfaces asociadas a los 4 Routers:

R1#configure terminal
R1(config)#interface serial 0/0
R1(config-if)#ip address **192.1.12.1 255.255.255.0**
R1(config-if)#no shutdown
R1(config-if)#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)#exit

R2#configure terminal
R2(config)#interface serial 0/0
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)#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)#exit

R3#configure terminal
R3(config)#interface serial 0/0
R3(config-if)#ip address **192.1.34.3 255.255.255.0**
R3(config-if)#no shutdown
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 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)#exit

R4#configure terminal
R4(config)#interface serial 0/0
R4(config-if)#ip address **192.1.34.4 255.255.255.0**
R4(config-if)#no shutdown
R4(config-if)#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)#exit

1. *Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.*

Se procede a configurar el protocolo BGP en los routers 1 y 2.

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

R2(config)#router bgp 2
R2(config-router)#bgp router-id **33.33.33.33**
R2(config-router)#network **192.1.12.0 mask 255.255.255.0**
R2(config-router)#network **2.0.0.0 mask 255.0.0.0**
R2(config-router)#network **12.1.0.0 mask 255.255.0.0**
R2(config-router)#network **192.1.23.0 mask 255.255.255.0**
R2(config-router)#neighbor **192.1.12.1 remote-as 1**
R2(config-router)#neighbor **192.1.23.3 remote-as 3**

Por medio del comando *show ip route* tanto en R1 como en R2, se observan los resultados obtenidos en las tablas de enrutamiento, donde se encuentran las direcciones Loopback y las direcciones de las redes que están conectadas en forma directa, también, las interfaces Loopback de su

respectivo router vecino. Además, en la tabla de enrutamiento, se identifica un código B, el cual indica que las interfaces fueron aprendidas a través del protocolo BGP. Por último, la dirección 192.1.12.0/24 conectada a través de la interfaz serial 0/0, sirve como vía para alcanzar las diferentes rutas, ya que este enlace comunica físicamente ambos dispositivos.

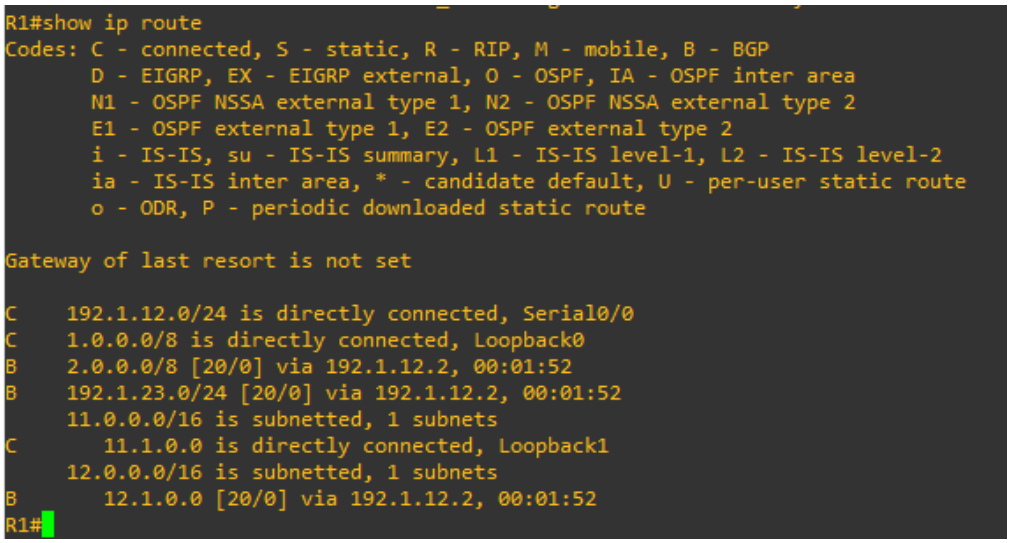

Figura 2. R1_show_ip_route

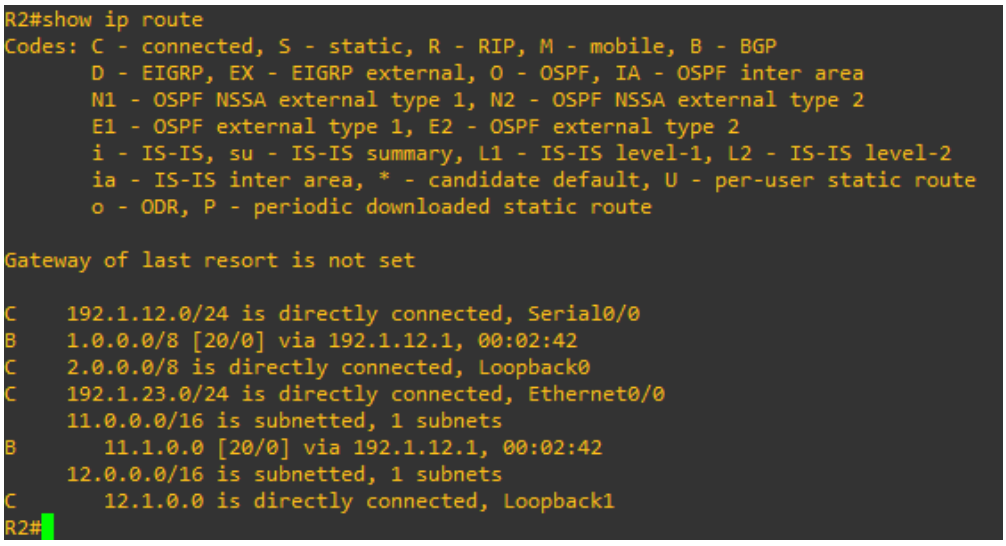

Figura 3. R2_show_ip_route

2. *Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como*

44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Se procede a configurar el protocolo BGP en el router 3.

R3(config)#router bgp 3
R3(config-router)#bgp router-id **44.44.44.44**
R3(config-router)#network **192.1.34.0 mask 255.255.255.0**
R3(config-router)#network **192.1.23.0 mask 255.255.255.0**
R3(config-router)#network **13.1.0.0 mask 255.255.0.0**
R3(config-router)#network **3.0.0.0 mask 255.0.0.0**
R3(config-router)#neighbor **192.1.34.4 remote-as 4**
R3(config-router)#neighbor **192.1.23.2 remote-as 2**

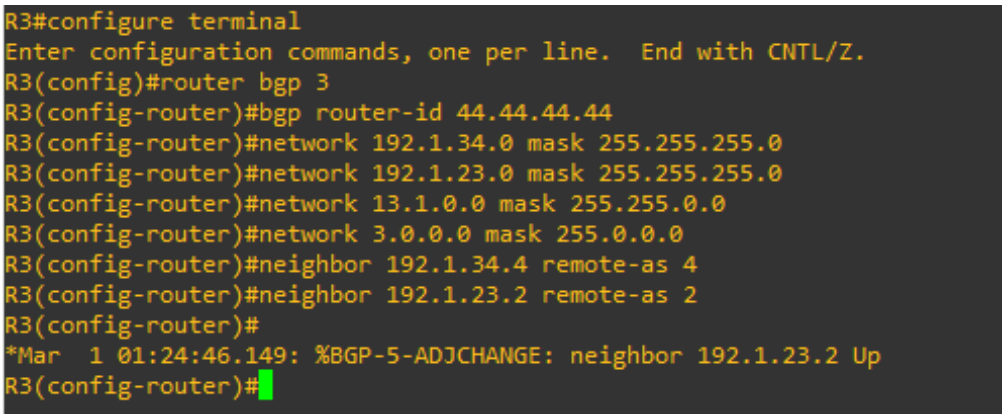

Figura 4. R3_BGP

A continuación, se usó el comando *show ip route* en el router 2, donde se ha actualizado su tabla de enrutamiento y ahora contiene las direcciones Loopback configuradas en el router 3, por lo tanto, contiene 4 rutas a través del protocolo BGP. También, usamos el mismo comando para el router 3, el cual muestra por medio de su tabla de enrutamiento las interfaces Loopback y las redes que lo comunican con los routers R2 y R4 mediante la interfaz Ethernet 0/0 y la interfaz serial 0/0 respectivamente. Además, el router R3 ha actualizado las direcciones de red de las interfaces Loopback que se configuraron en R2 y R1, las cuales aprendió por medio del protocolo BGP debido a la relación de adyacencia que se estableció con R2, también, encontramos la dirección de red que conecta los routers R1 con R2, el cual aprendió con el protocolo BGP.

```
R2#show ip route
Codes: 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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:46:53
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:01:17
C    192.1.23.0/24 is directly connected, Ethernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:46:53
B    192.1.34.0/24 [20/0] via 192.1.23.3, 00:01:17
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 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, 00:01:20
R2#
```

Figura 5. R2_show_ip_route

```
R3#show ip route
Codes: 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

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:02:11
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:02:11
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:02:11
C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:02:11
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:02:11
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Figura 6. R3_show_ip_route

3. *Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la*

Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Se procede a configurar el protocolo BGP en el router 4.

R4(config)#router bgp 4
R4(config-router)#bgp router-id **66.66.66.66**
R4(config-router)#network **192.1.34.0 mask 255.255.255.0**
R4(config-router)#network **14.1.0.0 mask 255.255.0.0**
R4(config-router)#network **4.0.0.0 mask 255.0.0.0**
R4(config-router)#neighbor **192.1.34.3 remote-as 3**
R4(config-router)#exit
R4(config)#ip route **3.0.0.0 255.0.0.0 192.1.34.3**

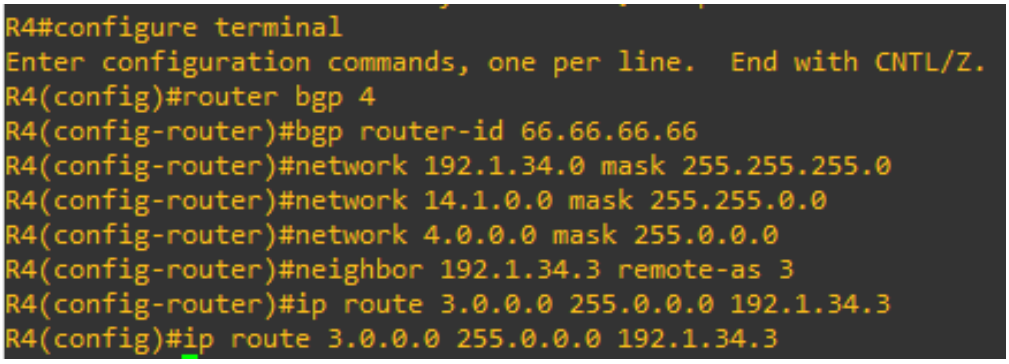

Figura 7. R4_BGP

Por medio del comando show ip route, se evidencia que el R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este dispositivo con R4 ha cambiado y ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática dado que así se estableció en el paso anterior, sin embargo, pese a que se usa la dirección lógica Loopback 0 para establecer la adyacencia, la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 0/0. Así también, se puede identificar que la dirección de red de la interfaz Loopback 1 se siegue aprendiendo mediante el protocolo BGP, pero ahora se alcanza mediante la interfaz Loopback 0 de R4 (4.4.4.4). Los demás resultados que nos muestra la tabla de enrutamiento permanecen iguales para el R3. Por otro lado, en el R4 la dirección con la que se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la interfaz Loopback 0 de R3. Por último, la tabla de enrutamiento nos muestra la ruta estática que se creó hacia R3.

```
R3#show ip route
Codes: 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

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:12:48
B    1.0.0.0/8 [20/0] via 192.1.23.2, 01:44:16
B    2.0.0.0/8 [20/0] via 192.1.23.2, 01:44:16
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:36:52
C    192.1.23.0/24 is directly connected, Ethernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 01:44:16
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 01:44:19
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.34.4, 00:36:57
R3#
```

Figura 8. R3_show_ip_route

```
R4#show ip route
Codes: 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

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:14:20
B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:38:25
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:38:25
S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is directly connected, Loopback0
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:12:27
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.34.3, 00:38:25
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.34.3, 00:38:27
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:38:27
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
R4#
```

Figura 9. R4_show_ip_route

Se ejecuta el comando *show ip bgp* en los 4 routers donde se evidencia que han aprendido las rutas Loopback de los demás de manera automática:

```
R1#show ip bgp
BGP table version is 30, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0                  0         32768 i
*> 2.0.0.0          192.1.12.2               0             0 2 i
*> 3.0.0.0          192.1.12.2                             0 2 3 i
*> 4.0.0.0          192.1.12.2                             0 2 3 4 i
*> 11.1.0.0/16      0.0.0.0                  0         32768 i
*> 12.1.0.0/16      192.1.12.2               0             0 2 i
*> 13.1.0.0/16      192.1.12.2                             0 2 3 i
*> 14.1.0.0/16      192.1.12.2                             0 2 3 4 i
*  192.1.12.0       192.1.12.2               0             0 2 i
*>                  0.0.0.0                  0         32768 i
*> 192.1.23.0       192.1.12.2               0             0 2 i
*> 192.1.34.0       192.1.12.2                             0 2 3 i
R1#
```

Figura 10. R1_Show_ip_bgp

```
R2#show ip bgp
BGP table version is 32, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          192.1.12.1               0             0 1 i
*> 2.0.0.0          0.0.0.0                  0         32768 i
*> 3.0.0.0          192.1.23.3               0             0 3 i
*> 4.0.0.0          192.1.23.3                             0 3 4 i
*> 11.1.0.0/16      192.1.12.1               0             0 1 i
*> 12.1.0.0/16      0.0.0.0                  0         32768 i
*> 13.1.0.0/16      192.1.23.3               0             0 3 i
*> 14.1.0.0/16      192.1.23.3                             0 3 4 i
*> 192.1.12.0       0.0.0.0                  0         32768 i
*                   192.1.12.1               0             0 1 i
*  192.1.23.0       192.1.23.3               0             0 3 i
*>                  0.0.0.0                  0         32768 i
*> 192.1.34.0       192.1.23.3               0             0 3 i
R2#
```

Figura 11. R2_Show_ip_bgp

```
R3#show ip bgp
BGP table version is 33, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          192.1.23.2                             0 2 1 i
*> 2.0.0.0          192.1.23.2                             0 2 i
*> 3.0.0.0          0.0.0.0                  0         32768 i
*> 4.0.0.0          192.1.34.4               0             0 4 i
*> 11.1.0.0/16      192.1.23.2                             0 2 1 i
*> 12.1.0.0/16      192.1.23.2               0             0 2 i
*> 13.1.0.0/16      0.0.0.0                  0         32768 i
*> 14.1.0.0/16      192.1.34.4               0             0 4 i
*> 192.1.12.0       192.1.23.2               0             0 2 i
*> 192.1.23.0       0.0.0.0                  0         32768 i
*                   192.1.23.2               0             0 2 i
*  192.1.34.0       192.1.34.4               0             0 4 i
*>                  0.0.0.0                  0         32768 i
R3#
```

Figura 12. R3_Show_ip_bgp

```
R4#show ip bgp
BGP table version is 44, local router ID is 66.66.66.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          192.1.34.3                             0 3 2 1 i
*> 2.0.0.0          192.1.34.3                             0 3 2 i
r> 3.0.0.0          192.1.34.3               0             0 3 i
*> 4.0.0.0          0.0.0.0                  0         32768 i
*> 11.1.0.0/16      192.1.34.3                             0 3 2 1 i
*> 12.1.0.0/16      192.1.34.3                             0 3 2 i
*> 13.1.0.0/16      192.1.34.3               0             0 3 i
*> 14.1.0.0/16      0.0.0.0                  0         32768 i
*> 192.1.12.0       192.1.34.3                             0 3 2 i
*> 192.1.23.0       192.1.34.3               0             0 3 i
*> 192.1.34.0       0.0.0.0                  0         32768 i
*                   192.1.34.3               0             0 3 i
R4#
```

Figura 13. R4_Show_ip_bgp

1.2 Escenario 2

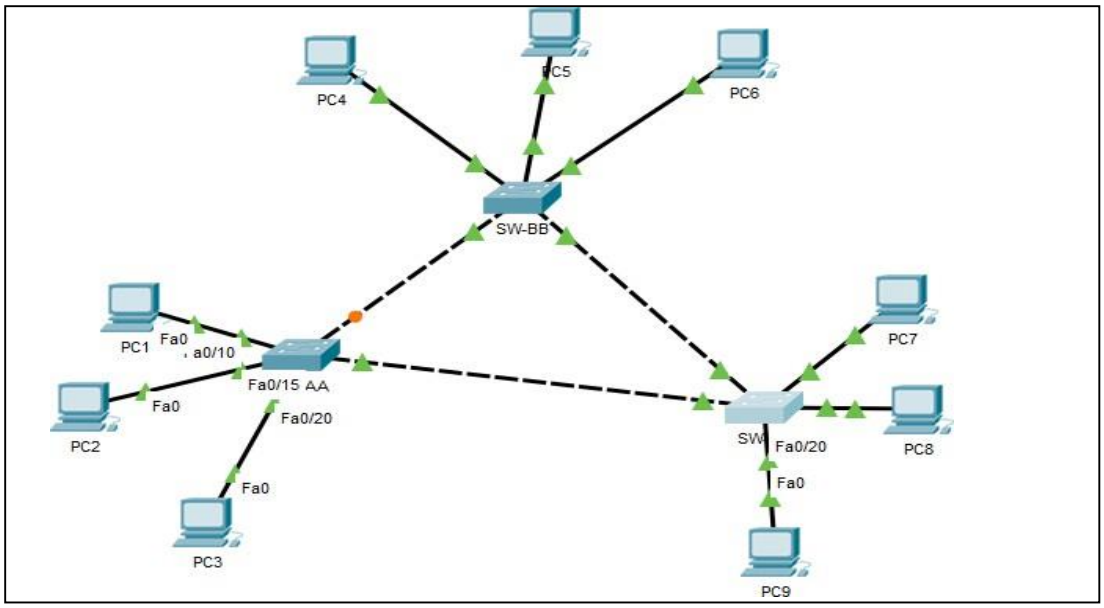

Figura 14. Topología 2

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.

Switch>enable
Switch#configure terminal
Switch(config)#hostname **SW-AA**
SW-AA(config)#vtp mode **client**
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
```

Figura 15. SW-AA_VTP_Client

Switch>enable
Switch#configure terminal
Switch(config)#hostname **SW-CC**
SW-CC(config)#vtp mode **client**
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#
```

Figura 16. SW-CC_VTP_Client

Switch>enable
Switch#configure terminal
Switch(config)#hostname **SW-BB**
SW-BB(config)#vtp mode **server**
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
```

Figura 17. SW-BB_VTP_Server

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

```
SW-AA#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#
```

Figura 18. SW-AA_Show_vtp_status

```
SW-BB#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
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)
SW-BB#
```

Figura 19. SW-BB_Show_vtp_status

```
SW-CC#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

Figura 20. SW-CC_Show_vtp_status

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.***

SW-BB>enable
Sw-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#**switchport mode dynamic desirable**

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable

SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SW-BB(config-if)#
```

Figura 21. SW-BB_mode_dynamic_desirable

5. 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
Fa0/1       auto         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
```

Figura 22. SW-AA_Show_interfaces_trunk

```
SW-BB#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
```

Figura 23. SW-BB_Show_interfaces_trunk

*6. 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>enable
Sw-AA#configure terminal
SW-BB(config)#interface fastEthernet 0/3
SW-BB(config-if)#**switchport mode trunk**

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

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

SW-AA(config-if)#
```

Figura 24. SW-AA_mode_trunk

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

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

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1
```

Figura 25. SW-AA_Show_interface_trunk.2

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

SW-CC>enable
Sw-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/1
SW-BB(config-if)#**switchport mode trunk**

```
SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk

SW-CC(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Figura 26. SW-CC_mode_trunk

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

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1
```

Figura 27. SW-CC_Show_interfaces_trunk

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

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1
```

Figura 28. SW-BB_Show_interfaces_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>enable
Sw-AA#configure terminal
SW-AA(config)#**vlan 10**

```
SW-AA>enable
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 29. SW-AA_vlan_10

SW-BB>enable
Sw-BB#configure terminal
SW-BB(config)#**vlan 10**
SW-BB(config-vlan)#name **Compras**
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name **Personal**
SW-BB(config-vlan)#**vlan 30**
SW-BB(config-vlan)#name **Planta**
SW-BB(config-vlan)#**vlan 99**
SW-BB(config-vlan)#name **Admon**
SW-BB(config-vlan)#exit

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#ex
SW-BB(config-vlan)#exit
```

Figura 30. SW-BB_vlans

10. Verifique que las VLANs han sido agregadas correctamente.

```
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, Fa0/10
                                                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
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
SW-BB#
```

Figura 31. SW-BB_Show_vlan_brief

```
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, Fa0/10
                                                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
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
SW-AA#
```

Figura 32. SW-AA_Show_vlan_brief

```
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, Fa0/10
                                                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
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
SW-CC#
```

Figura 33. SW-CC_Show_vlan_brief

11. 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

X = número de cada PC particular

Tabla 5. Parámetros de configuración puertos VLAN

12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN10.

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>enable
SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access **vlan 10**
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access **vlan 25**
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access **vlan 30**
SW-AA(config-if)#exit

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#ex
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
SW-AA(config)#
```

Figura 34.SW-AA_Switchport_mode_access

SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access

SW-BB(config-if)#switchport access **vlan 10**
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access **vlan 25**
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access **vlan 30**
SW-BB(config-if)#exit

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
SW-BB(config)#
```

Figura 35. SW-BB_Switchport_mode_access

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access **vlan 10**
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access **vlan 25**
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access **vlan 30**
SW-CC(config-if)#exit

```
SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
SW-CC(config)#
```

Figura 36. SW-CC_Switchport_mode_access

PC1: ip address 190.108.**10**.1 Subnet Mask: 255.255.255.0
PC2: ip address 190.108.**20**.2 Subnet Mask: 255.255.255.0
PC3: ip address 190.108.**30**.3 Subnet Mask: 255.255.255.0
PC4: ip address 190.108.**10**.4 Subnet Mask: 255.255.255.0
PC5: ip address 190.108.**20**.5 Subnet Mask: 255.255.255.0
PC6: ip address 190.108.**30**.6 Subnet Mask: 255.255.255.0
PC7: ip address 190.108.**10**.7 Subnet Mask: 255.255.255.0
PC8: ip address 190.108.**20**.8 Subnet Mask: 255.255.255.0
PC9: ip address 190.108.**30**.9 Subnet Mask: 255.255.255.0

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 intefáz.

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. Parámetros de configuración SVI

SW-AA>enable
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-AA(config-if)#exit

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

Figura 37. SW-AA_Vlan_99

SW-BB>enable
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-BB(config-if)#exit

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

Figura 38. SW-BB_Vlan_99

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#**interface vlan 99**
SW-CC(config-if)#**ip address 190.108.99.3 255.255.255.0**
SW-CC(config-if)#exit

```
SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

Figura 39. SW-CC_Vlan_99

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.

Al realizar Ping entre los diferentes PCs que pertenecen a la misma Vlan, se obtuvo éxito, en cambio para los PCs que perteneces a Vlans diferentes no fue así. La causa del problema de conexión entre PCs con diferente Vlans, se debe a que cada Pc pertenece a un segmento de red diferente. Por lo tanto, si se pretende lograr un enrutamiento entre Vlans, es necesario incluir un Switch de capa 3, de esta manera, se establece la comunicación entre PCs.

Ping de PC1 a PC4 y de PC1 a Pc6

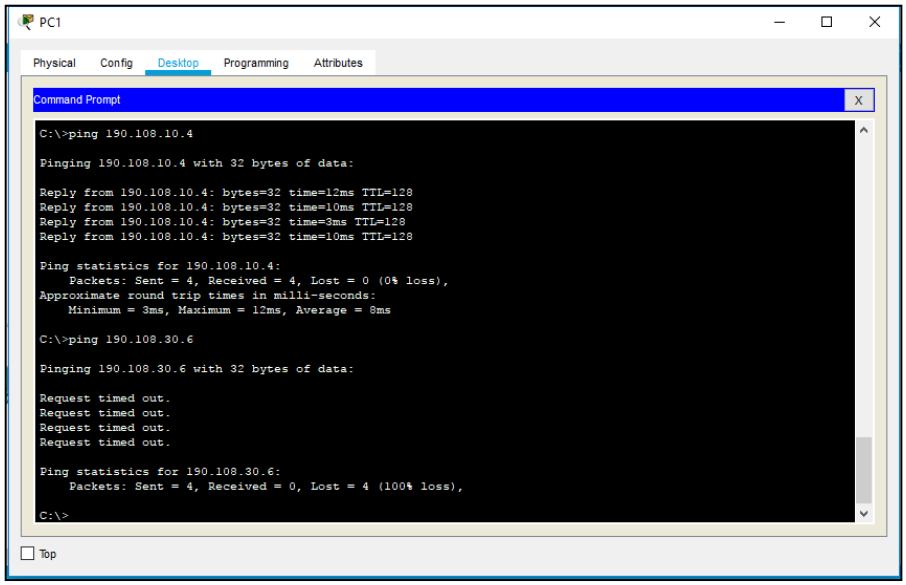

Figura 40. Ping_1

Ping de PC3 a PC9 y de PC3 a PC8

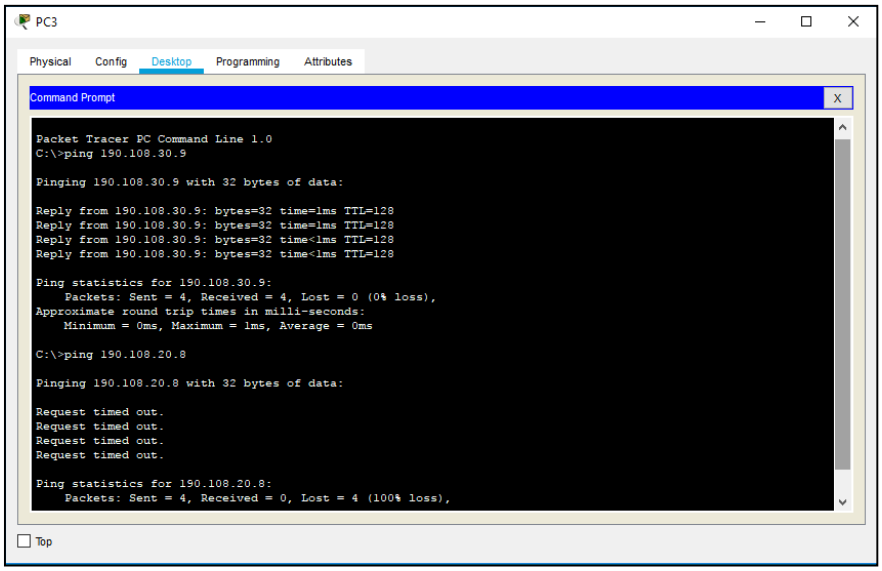

Figura 41. Ping_2

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

Se realizó con éxito el ping entre los diferentes Switches, debido a que las interfaces físicas que comunican los 3 Switches están configuradas en modo troncal, por medio del comando ***show interfaces trunk***, observamos que comparten el mismo tipo de encapsulamiento.

Ping SW-AA a SW-BB y SW-CC

```
SW-AA>enable
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 100 percent (5/5), round-trip min/avg/max = 0/0/1 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 100 percent (5/5), round-trip min/avg/max = 0/5/24 ms

SW-AA#
```

Figura 42. Ping_3

Ping SW-BB a SW-AA y SW-CC

```
SW-BB>enable
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 = 0/0/2 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 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

SW-BB#
```

Figura 43. Ping_4

Ping SW-CC a SW-BB y SW-AA

```
SW-CC>enable
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 = 0/0/1 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 = 0/8/42 ms

SW-CC#
```

Figura 44. Ping_5

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

El ping realizado entre los Switches y los PCS no obtuvo éxito, debido a que no se configuro un enrutamiento IP en las Vlans creadas. Por lo tanto, aunque estén habilitadas las Vlans en cada uno de los Switches y se configure cada interfaz en modo de acceso según su respectiva Vlan, también es necesario configurar una dirección IP y una máscara de subred en cada una de las interfaces Vlan de los Switches y además determinar una Vlan nativa para dichas interfaces.

Ping SW-AA a PC1, PC2 Y PC3

```
SW-AA>enable
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 190.108.20.2

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-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 0 percent (0/5)

SW-AA#
```

Figura 45. Ping_6

Ping SW-BB a PC1, PC2 Y PC3

```
SW-BB#ping 190.108.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#
```

Figura 46. Ping_7

Ping SW-CC a PC1, PC2 Y PC3

```
SW-CC>enable
SW-CC#ping 190.108.10.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.20.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.30.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#
```

Figura 47. Ping_8

2. CONCLUSIONES

CCNP (Cisco Certified Network Professional), provee la capacidad, el conocimiento y las habilidades necesarias para la implementar y mantener en óptimas condiciones una estructura de red integrada de servicios y aplicaciones. CCNP (Cisco Certified Network Professional), se ha diseñado para reflejar las habilidades y las responsabilidades laborales asociadas a los roles profesionales de ingeniero de Telecomunicaciones y demás profesiones afines.

La presente certificación además, ofrece una experiencia de aprendizaje con una gran carga académica, tanto teórica como práctica, llevando a cabo el desarrollo de simulaciones dentro del aula, abarcando así habilidades avanzadas de routing, switching y solución de problemas.

Mediante el uso de herramientas de simulación se realizó un análisis del comportamiento de distintos protocolos, utilizando comandos de administración de tablas de enrutamiento; identificando problemas propios de enrutamiento y conmutación, mediante el uso adecuado de estrategias y estadísticas de tráfico en las interfaces, todo esto soportado en los modelos de comunicación y con el fin de resolver problemas de configuración, conectividad y enrutamiento.

REFERENCIAS BIBLIOGRÁFICAS

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

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de http://www.birminghamcharter.com/ourpages/auto/2012/3/22/41980164/CCNA %20Electronic%20Book%206th%20edition.pdf

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado dehttp://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&A N=440032&lang=es&site=ehost-live

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/978158 7205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materia ls/Cisco-ICND2.pdf

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

UNAD (2015). SwitchCISCO Security Management[OVA]. Recuperado dehttps://1drv.ms/u/s!AmIJYei-NT1IlyVeVJCCezJ2QE5c

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