DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YELISA VILLERO RIVERA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YELISA VILLERO RIVERA

Diplomado de opción de grado presentado para optar el título de INGENIERO ELECTRONICO

DIRECTOR:

MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

VALLEDUPAR, 22 de Mayo del 2020

AGRADECIMIENTOS

A DIOS primeramente autor de todas las cosas que me ha permito llegar donde estoy sin él no somos nada Gracias Dios por permitirme llegar hasta donde tú me tienes ahora.

A mis queridos padres que con su amor y sacrificio me heredaron la mejor educación y me supieron guiar por el camino correcto, a mi familia que día a día nos apoyan y siempre están junto a nosotros, y a nuestros amigos por su amistad y empuje.

A la Universidad Nacional Abierta y a Distancia y su cuerpo de docentes, por todos los conocimientos adquiridos a lo largo de esta hermosa carrera.

Tabla de contenido

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP: es el protocolo de encaminamiento EGP más utilizado en Internet. Es un protocolo que funciona sobre TCP por el puerto 179. BGP permite el encaminamiento de los paquetes IP que se intercambian entre los distintos AS. Para ello, es necesario el intercambio de prefijos de rutas entre los diferentes AS de forma dinámica, lo cual se lleva a cabo mediante el establecimiento de sesiones BGP inter-AS sobre conexiones TCP. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa.

DTP (Dynamic Trunking Protocol): es un protocolo que automatiza la configuración de trunking en enlaces Ethernet. Su función es gestionar de forma dinámica la configuración del enlace troncal al conectar dos switches, introduciendo los comandos del IOS en la configuración del dispositivo de forma automática sin que el administrador intervenga. Por defecto, DTP está habilitado y las interfaces de sus conmutadores estarán en modo "dinámico automático" o "dinámico deseable". Esto significa que siempre que reciba un paquete DTP que solicite formar una troncal, su interfaz estará en modo troncal.

VTP (VLAN Trunking Protocol): es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP.

Enlace Troncal: Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-

Gigabit Ethernet. Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

VLAN: Se conoce como Virtual LAN o VLAN a una división de carácter lógico del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. Se trata, por tanto, de una agrupación de un conjunto de dispositivos que pueden mantener comunicación entre sí. Es importante destacar que aquellos dispositivos que pertenecen a VLANs diferentes no pueden establecer una comunicación entre ellas. Las VLAN son un mecanismo que permite a los administradores de red crear dominios de transmisión lógica que pueden abarcar un solo conmutador o múltiples conmutadores, independientemente de la proximidad física.

RESUMEN

El presente proyecto de grado se fundamenta en el desarrollo de 2 escenarios de configuración de redes VLAN y el protocolo BGP donde aplican los conocimientos adquiridos a lo largo del curso. Para el desarrollo del escenario 1 se implementar el protocolo de enrutamiento BGP usado para intercambiar información de enrutamiento entre los routers, configurando los sistemas autónomos y al mismo tiempo se intercambian sus tablas de rutas a través del protocolo BGP. Se añadirá a cada router un identificador "remote-as" y se le indicará cual es la red que queda detrás de él, del mismo modo se le indicará también cuáles son sus routers vecinos con los que intercambiará la información de routing a través de BGP.

Para el escenario 2, se configuran los switches en modo VTP y DTP, implementando las VLAN 10, 25 y 30. Si se configura un switch como servidor VTP sin un nombre de dominio VTP, no será posible configurar una VLAN en el switch. Todos los dispositivos en el mismo dominio de administración reciben información acerca de cualquier nueva VLAN que se haya configurado en el dispositivo. Los switches configurados en modo transparente también difunden la información por sus puertos troncales, pero no la utilizan para su propia configuración. En el switch servidor de VTP se crearán todas las VLANs, el resto de los switches serán clientes. En el switch definido como cliente no hay que definir o crear las VLANs, sólo habrá que asignar los puertos a las VLANs.

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

ABSTRACT

This degree project is based on the development of 2 configuration scenarios for VLAN networks and the BGP protocol where they apply the knowledge acquired throughout the course. For the development of scenario 1, the BGP routing protocol used to exchange routing information between the routers will be implemented, configuring the autonomous systems and at the same time their route tables are exchanged through the BGP protocol. A "remote-as" identifier will be added to each router and it will be indicated which is the network that is behind it, in the same way it will also be indicated which are its neighboring routers with which it will exchange routing information through BGP .

For Scenario 2, the switches are configured in VTP and DTP mode, implementing VLANs 10, 25, and 30. If a switch is configured as a VTP server without a VTP domain name, it will not be possible to configure a VLAN on the switch. All devices in the same management domain receive information about any new VLANs that have been configured on the device. Switches configured in transparent mode also broadcast the information through their trunk ports, but do not use it for their own configuration. All VLANs will be created on the VTP server switch, the rest of the switches will be clients. In the switch defined as client, it is not necessary to define or create the VLANs, it will only be necessary to assign the ports to the VLANs.

Key Words: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCION

El desarrollo del diplomado de profundización CISCO CCNP tiene como objetivo proveer herramientas y habilidades que debe tener el profesional en redes de telecomunicaciones para detectar, y resolver fallas en redes complejas, abarcando todos los conceptos y tecnologías asociadas al enrutamiento y conmutación enfatizado en el uso de dispositivos de Cisco. El diplomado está enfocado a la implementación de soluciones de conmutación en un entorno de red con dispositivos de red. Los futuros profesionales desarrollarán capacidades necesarias para cumplir con las responsabilidades laborales de técnicos, administradores e ingenieros de red.

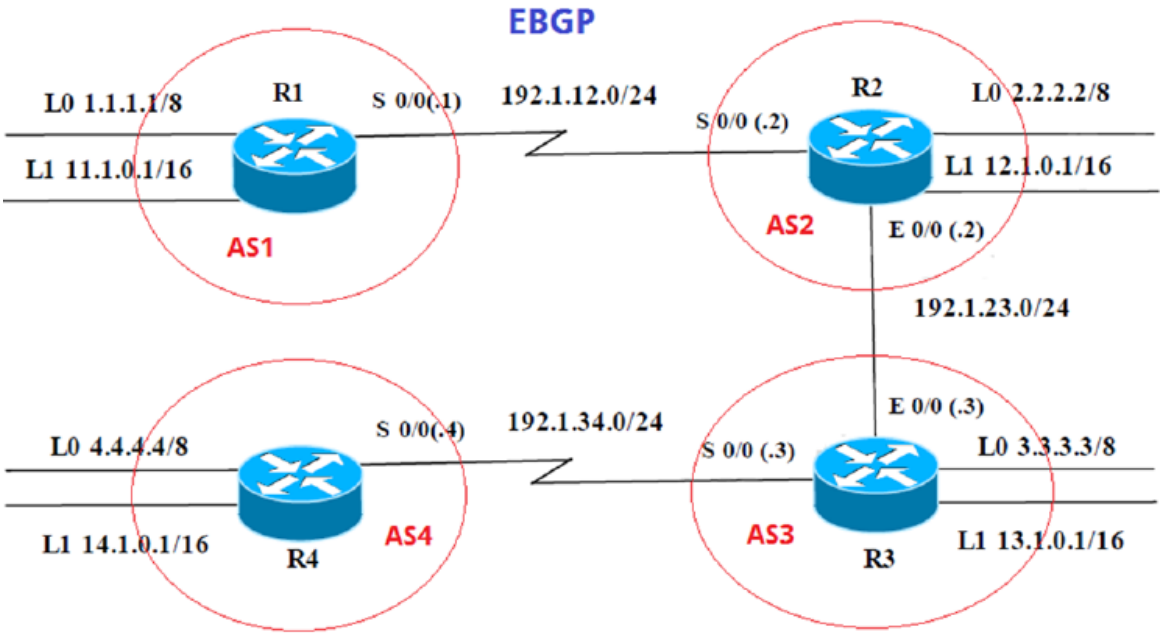
En el desarrollo del escenario 1, se realiza la conexión y configuración de una red constituida por 4 routers. El primer paso consiste en realizar la respectiva configuración de sus puertos seriales y FastEthernet mediante las tablas asignadas, de igual forma, se establecen las interfaces loopbacks configurando el protocolo de comunicación BGP. Las tablas de encaminamiento de BGP almacenan rutas para alcanzar redes. Para que la sesión BGP se establezca, el neighbor debe ser perfectamente alcanzable por la IP, sin embargo, las rutas a anunciar deben existir en la tabla de ruteo del router local o no serán enviadas en las actualizaciones, por tal razón las rutas aprendidas serán propagadas por defecto. Un dato importante a tener en cuenta es que al momento de establecer más sesiones BGP, simplemente se agregan más comandos ***neighbor***, el cual nos permite identificar un vecino con el cual el router local establecerá la sesión. Hay que destacar que cuando el protocolo BGP se ejecuta entre routers que pertenecen a dos AS diferentes, esto se llama BGP externo o eBGP, como veremos en el desarrollo de los pasos en la configuración del escenario 1. Una vez emitida la configuración correspondiente, los routers BGP se convierten en vecinos después de que los routers establezcan una conexión TCP entre ellos. Una vez establecida la conexión TCP y se encuentre activa, los routers comenzarán a enviar mensajes de apertura para intercambiar valores, dichos valores que intercambian los routers incluyen el número de AS, la versión de BGP que ejecutan los routers, el ID de router BGP, entre otros. Hay que aclarar que las direcciones IP que se utilizan con en el comando *neighbor* de los routers de deberán poder alcanzarse entre sí.

Para el desarrollo del escenario 2, se realiza la conexión y configuración de una red VLAN constituidas por: compras (VLAN 10), personal (VLAN 25) y planta (VLAN 30), que a su vez estarán conectadas mediante 3 switches. Inicialmente se

hace uso de un enlace troncal de VLAN, que se caracteriza por ser un enlace de capa 2 del modelo OSI entre dos switches que transporta el tráfico para todas las VLAN. Para configurar un puerto de switch en un extremo de un enlace troncal en el escenario 2, se implementó el comando ***switchport mode trunk*** cambiando la interfaz a modo de enlace troncal permanente, donde se establece una negociación de protocolo de enlace troncal dinámico para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio. Sin embargo, también se hace uso del comando ***switchport mode dynamic desirable*** el cual hace que la interfaz intente convertir el enlace en un enlace troncal de manera activa, de este modo, la interfaz se convierte en una interfaz troncal aun si la interfaz vecina se establece en modo de enlace troncal, deseado o automático.

ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1.1 ESCENARIO 1



Información para configuración de los Routers:

R1

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

R2

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

R3

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

R4

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

Tabla 1. Interfaces asociadas a los 4 routers

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***.
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***.
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 realizar las respectivas conexiones entre los 4 router y sus interfaces en el simulador GNS3, como se ilustra en la figura 1.

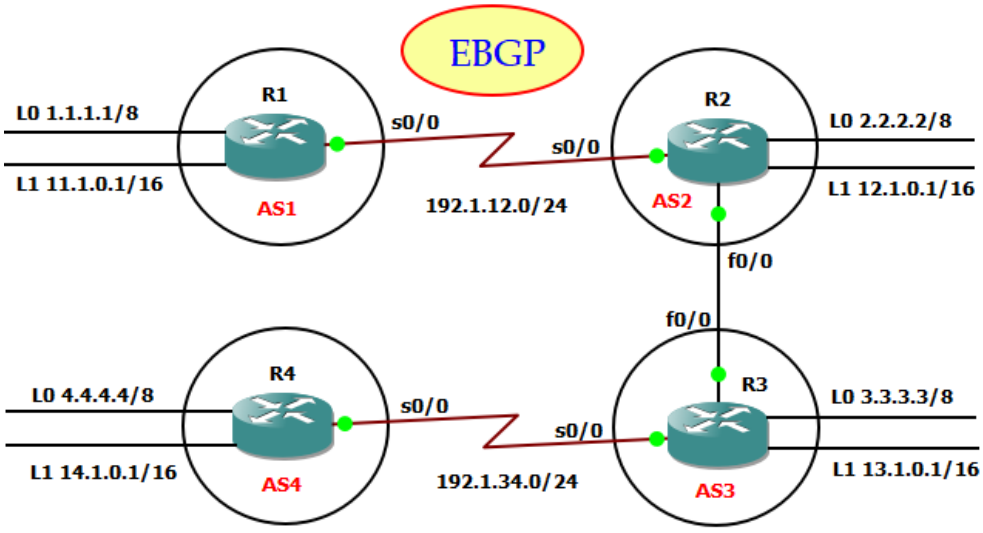


Figura 1. Conexión de los Routers en GNS3

1.1.1 Configuración de vecino BGP entre R1 y R2

En primer lugar, se configuran las interfaces Loopback y Serial asociada a cada router, luego se realiza la configuración de los router en modo BGP, es decir, definimos el proceso BGP, el número de AS al que el router pertenece y la vecindad que forma R1 con R2, R2 con R1 y R3. Una vez se inicia el proceso BGP se procede a configurar las redes o información que se van a transportar mediante el protocolo BGP. El comando utilizado para enseñar redes es el siguiente: ***network "IP network" mask "mascara de la red"***:

```
R1#configure terminal
R1(config)#interface L0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface L1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface s0/0
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
R1(config-router)#exit
R1(config)#
```

```
R2#configure terminal
R2(config)#interface L0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface L1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface s0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface f0/0
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)#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
R2(config-router)#exit
R2(config)#
```

Un aspecto que es necesario a tener en cuenta es que la dirección IP configurada con el comando ***neighbor*** en cada router sean alcanzables entre sí. Una vez finalizado el proceso de configuración anterior, el siguiente paso es verificar si los router quedaron bien configurados con sus respectivas interfaces y proceso BGP mediante el comando ***show ip route***.

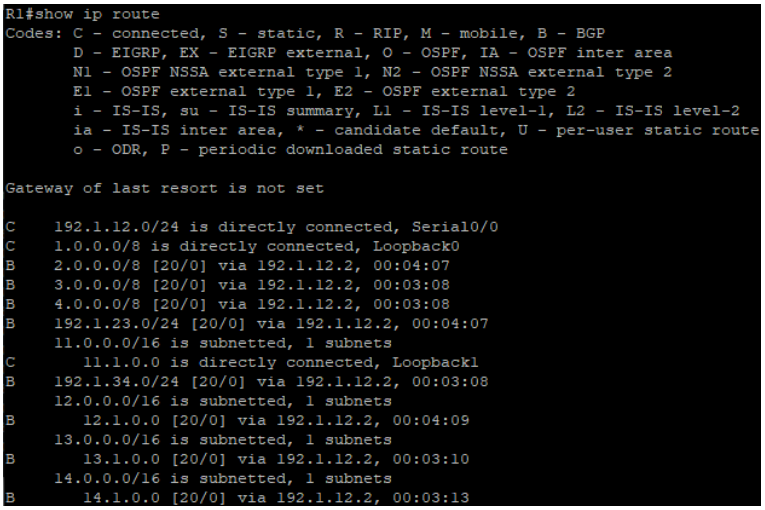


Figura 2. Verificación en R1 de las Interfaces configuradas

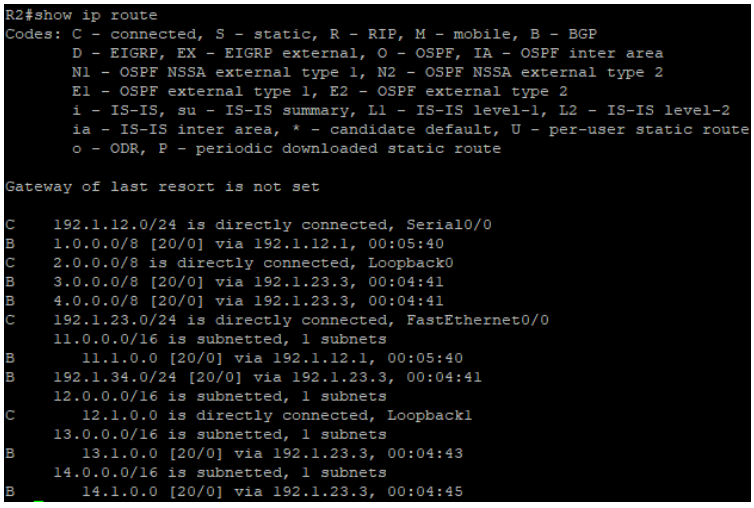
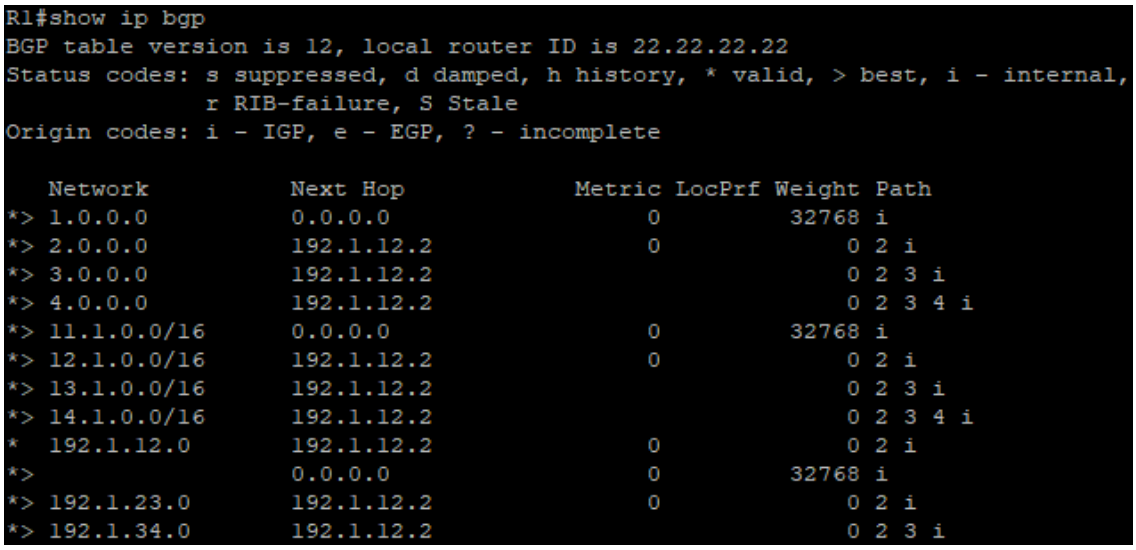


Figura 3. Verificación en R2 de las Interfaces configuradas

R1 guardará la ruta 192.1.12.0/24 en su tabla de encaminamiento y la anunciará al router R2 incluso si no dispone de un camino IGP para llegar. Se observa que los routers BGP intercambian información sobre la posibilidad de alcance de la red, debido a que la formación de vecinos BGP indica que los routers intentarán comunicarse vía BGP.

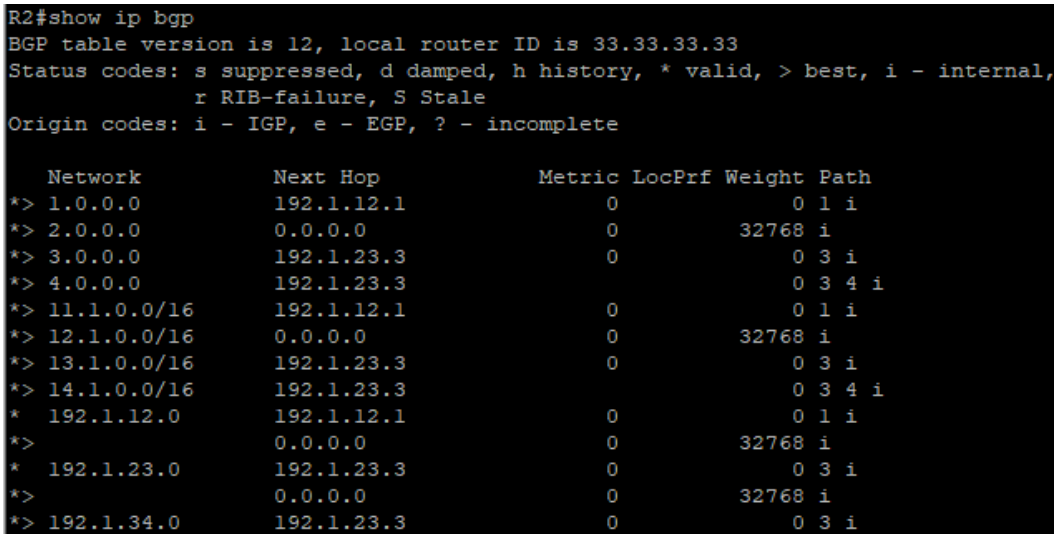
Se ejecuta el comando ***show ip bgp*** en ambos routers para evidenciar que han aprendido las rutas loopback de los demás de manera automática:



```
R1#show ip bgp
BGP table version is 12, 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
```

Figura 4. Rutas aprendidas en R1



```
R2#show ip bgp
BGP table version is 12, 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       192.1.12.1               0             0 1 i
*>                  0.0.0.0                  0         32768 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
```

Figura 5. Rutas aprendidas en R2

1.1.2 Configuración de vecino BGP entre R2 y R3

Como R2 ya fue configurado en el paso anterior, no es necesario realizar de nuevo el procedimiento, por tal motivo se procede solo a configurar las interfaces Loopback, Serial y FastEthernet asociada al router 3, y al igual que el paso anterior, se realiza la configuración del router en modo BGP, es decir, definimos el proceso BGP y el número de AS al que el router pertenece y la vecindad que forma con R2 y R4:

```
R3#configure terminal
R3(config)#interface L0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface L1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface s0/0
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)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit
R3(config)#
```

Una vez finalizada la configuración en R3, es necesario afirmar que el comando ***network*** funciona si el router conoce la red que estamos anunciando, ya sea conectada, estática o detectada dinámicamente, por tal motivo, el router R3 al igual que los routers R1 y R2, aprendieron las tablas de rutas de los demás router. Los routers intentarán conversar con su neighbor, por lo tanto éste debe poder ser alcanzado, y ya que está directamente conectado, no necesita de otro protocolo.

Por otro lado, no es necesario que los vecinos estén directamente conectados, razón por la cual se configuran las interfaces loopbacks para el establecimiento de la sesión TCP entre los routers. Una vez establecida la adyacencia entre R2 y R3, se verifica mediante los comandos ***show ip route*** y ***show ip 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, 07:17:12
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 01:27:47
B    4.0.0.0/8 [20/0] via 192.1.23.3, 01:27:19
C    192.1.23.0/24 is directly connected, FastEthernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 07:17:12
B    192.1.34.0/24 [20/0] via 192.1.23.3, 06:47:32
     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, 06:55:34
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.23.3, 01:30:30
```

Figura 6. Verificación en R3 de las Interfaces configuradas

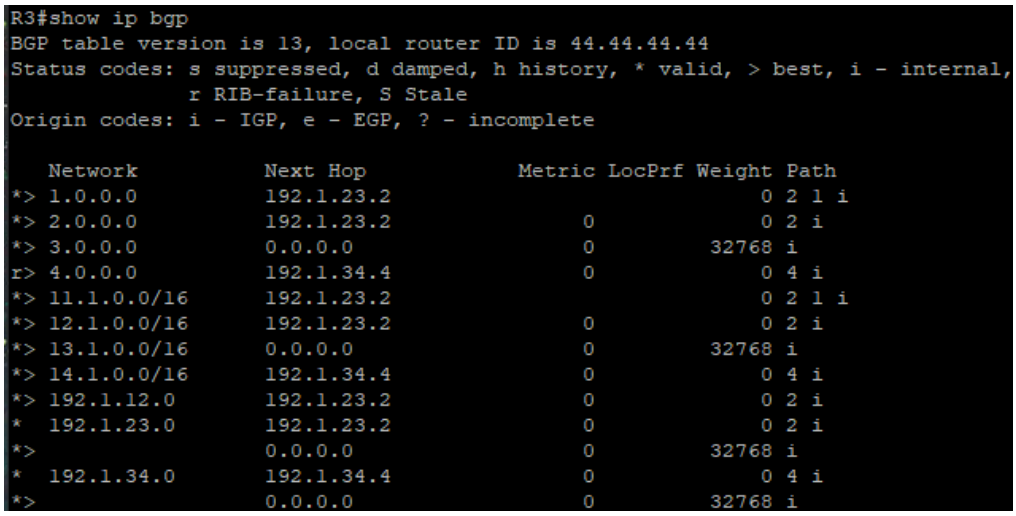
```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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, 06:59:42
B    1.0.0.0/8 [20/0] via 192.1.23.2, 06:59:42
B    2.0.0.0/8 [20/0] via 192.1.23.2, 06:59:42
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, FastEthernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 06:59:42
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, 06:59:43
     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, 01:31:44
R3#
*Mar  1 07:59:23.254: %BGP-3-NOTIFICATION: received from neighbor 4.4.4.4 2/2 (p
eer in wrong AS) 2 bytes 0003
```

Figura 7. Verificación en R3 de las Interfaces configuradas

Ahora se mostraran todas las rutas recibidas desde los routers BGP mediante el comando ***show ip bgp***.



```
R3#show ip bgp
BGP table version is 13, 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             0 2 i
*> 3.0.0.0          0.0.0.0                  0         32768 i
r> 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       192.1.23.2               0             0 2 i
*>                  0.0.0.0                  0         32768 i
*  192.1.34.0       192.1.34.4               0             0 4 i
*>                  0.0.0.0                  0         32768 i
```

Figura 8. Rutas aprendidas en R3

1.1.3 Configuración de vecino BGP entre R3 y R4

Como R3 ya fue configurado en el paso anterior, no es necesario realizar de nuevo el procedimiento, por tal motivo se procede solo a configurar las interfaces Loopback y Serial asociada al router 4, y al igual que el paso anterior, se realiza la configuración del router en modo BGP, es decir, definimos el proceso BGP y el número de AS al que el router pertenece y la vecindad que forma con R3:

```
R4#configure terminal
R4(config)#interface L0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface L1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface s0/0
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 255.0.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#exit
R4(config)#
```

Una vez finalizada la configuración del router, se emite el comando ***show ip route*** para verificar los parametros establecidos:

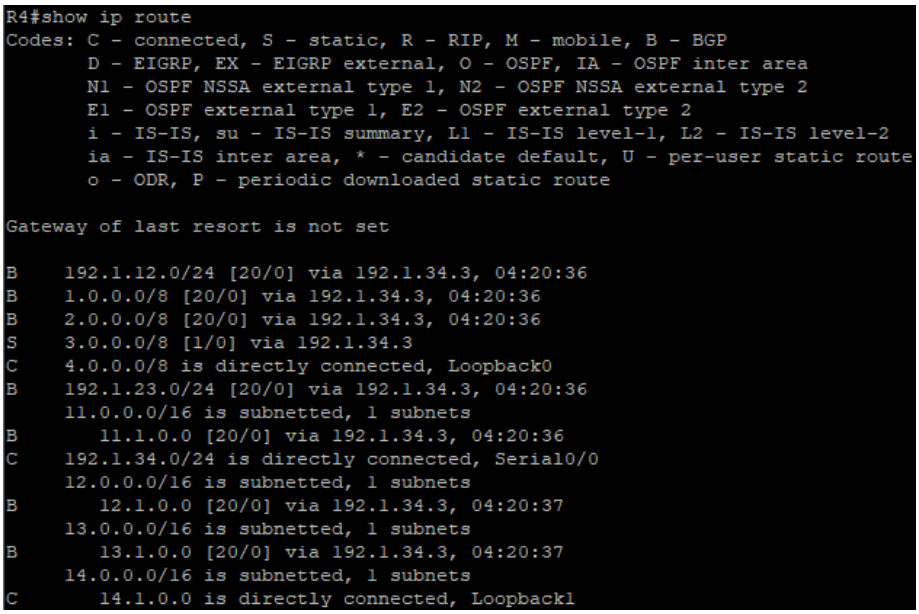


Figura 9. Verificación en R4 de las Interfaces configuradas

Por defecto, la sesión BGP entre routers se establece mediante la dirección IP de la interfaz del router vecino. Sin embargo, CISCO proporciona el comando ***update-source*** que permite que cualquier interfaz indicada, incluida la de loopback, pueda ser utilizada para establecer una sesión BGP. Por otro lado, para la configuración de las sesiones IBGP se utilizan normalmente interfaces ***loopback***, las cuales permiten asegurar las sesiones IBGP indicando una dirección IP virtual para un vecino mediante el comando ***neighbor***, de manera que dicha dirección IP sea independiente a las interfaces físicas del router vecino y se pueda establecer la sesión IBGP por una o por otra interfaz física.

Para establezca las relaciones de vecino con base en las direcciones de Loopback 0, crear rutas estáticas para alcanzar la Loopback 0 del otro router y no anunciar la Loopback 0 en BGP, los routers deben estar directamente conectados cuando utilizan eBGP. Si no están conectados directamente, el comando vecino del ***ebgp-multihop*** debe ser utilizado y una trayectoria a través de un IGP o de una ruta estática para alcanzar ambos routers y así obtener una relación de vecino. A continuación se realiza una configuración adicional en R3 y R4:

```
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 l0
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop
R3(config-router)#exit
R3(config)#

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 l0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#exit
R4(config)#
```

Una vez finalizada la configuración adicional, se emite el comando show ip route y show bgp en R3 y R4 para conocer los cambios en las tablas de rutas de cada router:

```
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, 04:31:11
B    1.0.0.0/8 [20/0] via 192.1.23.2, 04:31:11
B    2.0.0.0/8 [20/0] via 192.1.23.2, 04:31:11
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, FastEthernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 04:31:11
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, 04:31:14
     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, 04:31:16
```

Figura 10. Modificaciones de la tabla de ruteo en R3

```
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, 04:34:42
B    1.0.0.0/8 [20/0] via 192.1.34.3, 04:34:42
B    2.0.0.0/8 [20/0] via 192.1.34.3, 04:34:42
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, 04:34:42
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.34.3, 04:34:42
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, 04:34:44
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 04:34:44
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
```

Figura 11. Modificaciones de la tabla de ruteo en R4

Se ejecuta el comando ***show ip bgp*** en routers R3 y R4 donde se evidencia que han aprendido las rutas loopback de los otros routers de manera automática:

```
R3#show ip bgp
BGP table version is 13, 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             0 2 i
*> 3.0.0.0          0.0.0.0                  0         32768 i
r> 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       192.1.23.2               0             0 2 i
*>                  0.0.0.0                  0         32768 i
*  192.1.34.0       192.1.34.4               0             0 4 i
*>                  0.0.0.0                  0         32768 i
R3#
```

Figura 12. Nuevas rutas aprendidas en R3

```
R4#show ip bgp
BGP table version is 29, 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          192.1.34.3                             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       192.1.34.3               0             0 3 i
*>                  0.0.0.0                  0         32768 i
```

Figura 13. Nuevas rutas aprendidas en R4

Un aspecto que es necesario tener en cuenta es que las direcciones IP configuradas con el comando ***neighbor*** en cada router sean alcanzables entre sí. Para verificarlo, una forma segura es mediante el uso del comando ***ping*** forzando al router a que utilice como dirección IP fuente la especificada en el comando ***neighbor*** en lugar de la dirección IP de la interfaz por la que realmente se envía el ping. Para comprobarlo, se hace ping desde e router R1 a las Loopbacks 0 de los demás routers:

```
R1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/29/124 ms
R1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/48 ms
R1#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/41/60 ms
```

Figura 14. Ping desde R1 a las L0 de R2, R3 y R4

Otra manera de saber a qué AS y ***neighbor*** pertenece cada router, se hace uso del comando ***traceroute*** desde el router R4 a las Loopbacks 1 de R1, R2 y R3:

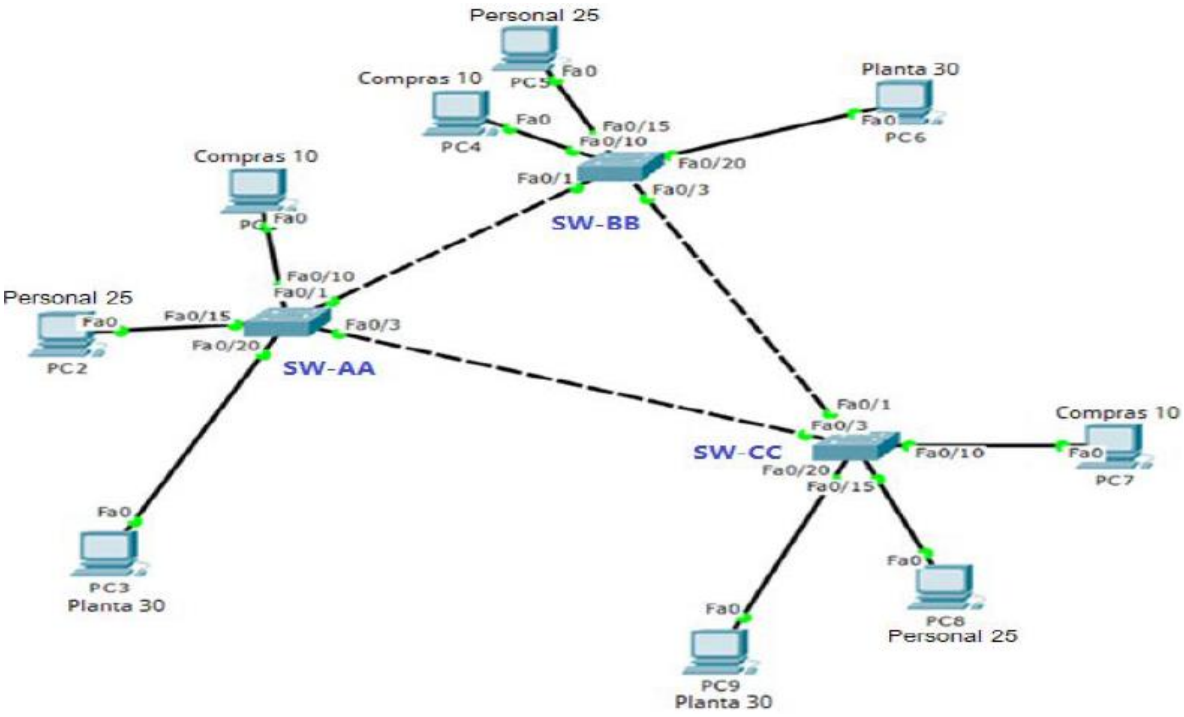
```
R4#traceroute 11.1.0.1

Type escape sequence to abort.
Tracing the route to 11.1.0.1

  1 192.1.34.3 32 msec 0 msec 0 msec
  2 192.1.23.2 [AS 3] 44 msec 20 msec 20 msec
  3 192.1.12.1 [AS 2] 72 msec 40 msec 28 msec
R4#
*Mar  1 08:08:29.797: %BGP-3-NOTIFICATION: sent to neighbor 3.3.3.3 2/2 (peer in
 wrong AS) 2 bytes 0003
```

Figura 15. Uso del comando ***traceroute*** para verificar el AS de cada router

1.2 ESCENARIO 2



A. Configurar VTP

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

2. Verifique las configuraciones mediante el comando ***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***.

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

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

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

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)

10. Verifique que las VLANs han sido agregadas correctamente.

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 2. Puertos VLAN y direcciones IP de los PCs

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

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

D. Configurar las direcciones IP en los Switches.

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

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 3. Direcciones IP de los Switches

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.

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

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

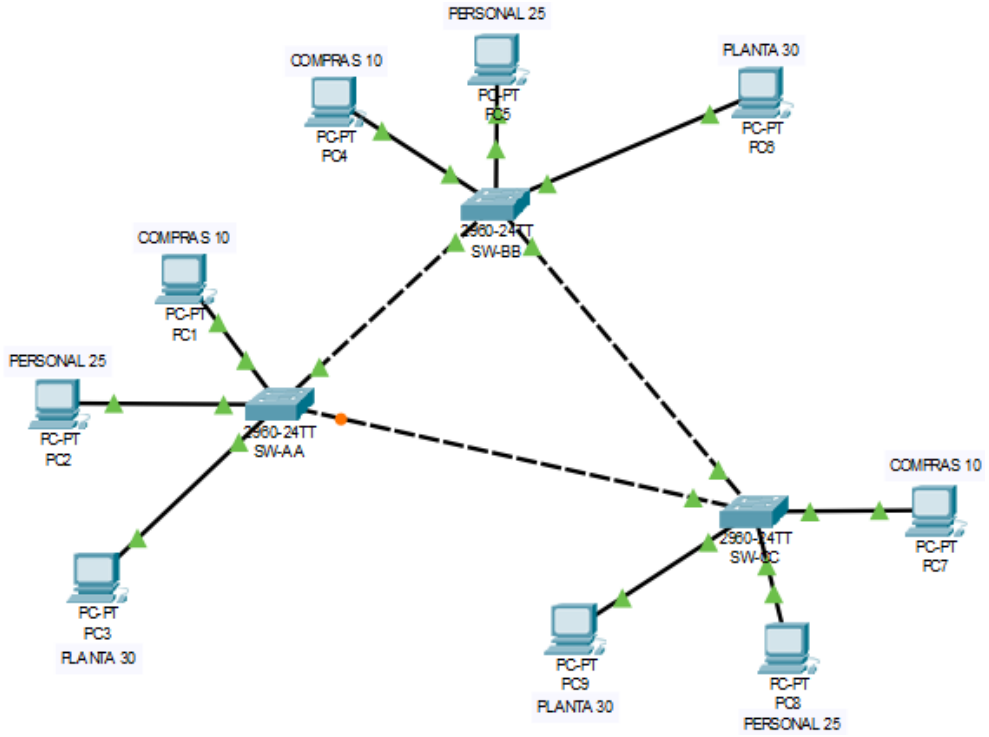


Figura 16. Red VLAN-Conexión de los PCs a los Switches

1.2.1 Configuración VTP

Inicialmente se configuran todos los switches para usar VTP y obtener 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)#exit
SW-AA#configure terminal
SW-AA(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco
SW-AA(config)#exit

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

switch>enable
switch#configure terminal
switch(config)#hostname SW-CC
SW-CC(config)#exit
SW-CC#configure terminal
SW-CC(config)#vtp mode server
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco
SW-CC(config)#exit
```

El protocolo VTP facilita la configuración de VLANs en múltiples switches de manera simultánea solo con la configuración del switch denominado como servidor (***server***), encargados de crear y mantener la información de todas las VLANs en la red y son los encargados de pasar esta información al resto de switches. En el modo Cliente (***client***) no se puede hacer ninguna modificación en las VLANs y mantienen la información de VLANs gracias a los mensajes que son enviados desde los servidores. A continuación, usamos el comando ***show vtp status*** para obtener información sobre el dominio VTP de los switches previamente configurados:

```
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
```

Figura 17. Estado VTP de SW-AA

```
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
```

Figura 18. Estado VTP de SW-BB

```
SW-CC#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
```

Figura 19. Estado VTP de SW-CC

1.2.2 Configuración DTP

Se procede a configurar un enlace troncal dinámico entre SW-AA y SW-BB, solo se configura un lado del enlace como ***dynamic desirable***.

```
SW-BB#configure terminal
SW-BB(config)#interface f0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

Usamos el comando `show interfaces trunk` para observar el estado de la interfaz f0/1:

```
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

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

Figura 20. Verificando la activación del enlace troncal ***dynamic desirable*** en SW-BB

```
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

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

Figura 21. Estado de la Interfaz Fa0/1 en SW-AA

En las figuras 20 y 21, se observa que el comando ***switchport mode dynamic desirable*** hace que la interfaz de SW-BB intente convertir el enlace en un enlace troncal de manera activa. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal, deseado o automático, para nuestro caso, en el switch SW-AA la interfaz se estableció en automático.

- El siguiente paso es configurar un enlace trocal estático entre SW-AA y SW-BB utilizando el comando ***switchport mode trunk*** en la interfaz F0/3 de SW-AA.

```
SW-AA#configure terminal
SW-AA(config)#interface f0/3
SW-AA(config-if)#switchport mode trunk
```

Usamos el comando `show interfaces trunk` para observar el estado de la interfaz f0/3:

```
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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       none
```

Figura 22. Estado de la Interfaz Fa0/3 en SW-AA

El comando `switchport mode trunk` usado en la figura 22 coloca la interfaz en modo de enlace troncal permanente y al mismo tiempo, la interfaz se convierte en una interfaz de enlace troncal, incluso si la interfaz vecina no es una interfaz de enlace troncal

- Como último paso, se configure un enlace troncal permanente entre SW-BB y SW-CC. Como SW-BB y SW-CC comparten conexión mediante 2 interfaces distintas, la configuración del enlace troncal debe realizarse en ambas interfaces, haciendo uso del comando `switchport mode trunk` en SW-CC en la interfaz f0/1 y en SW-BB en la interfaz f0/3:

```
SW-CC#configure terminal
SW-CC(config)#interface f0/1
SW-CC(config-if)#switchport mode trunk

SW-BB#configure terminal
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk
```

Una vez finalizada la configuración de las interfaces, emitimos el comando `show interfaces trunk` para observar el estado de la interface f0/3 en SW-BB el estado de la interfaz f0/1 en SW-CC:

```
SW-BB$show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1
```

Figura 23. Estado de la Interfaz Fa0/3 en SW-BB

```
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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1
```

Figura 24. Estado de la Interfaz Fa0/1 en SW-CC

En las figuras 23 y 24, el enlace entre los switches SW-BB y SW-CC se convierte en un enlace troncal porque el puerto f0/1 del switches SW-CC esta encendido para omitir todos los anuncios de DTP, así como para aparecer y permanecer en modo de puerto de enlace troncal. Los puertos f0/3 de los switches SW-BB y SW-CC se establecieron en modo ***desirable*** y automático. La interfaz se considera que está en un estado de enlace troncal (siempre activado). Por tal motivo, el puerto local termina en estado de enlace troncal sólo si el modo de enlace troncal del puerto remoto ha sido configurado para estar activo o si es conveniente. Es por eso que el comando ***switchport mode trunk*** hace que la interfaz se convierta en un enlace troncal, pero sin que genere tramas DTP.

1.2.3 Agregar VLANs y asignar puertos

En el switch SW-AA se agrega la VLAN 10, en el switch SW-BB se agregan 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(config)#exit

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
```

Se emite el comando ***show vlan brief*** para mostrar el contenido del archivo vlan.dat asociado a cada switch:

```
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
```

Figura 25. Estado de las VLANs en SW-AA

```
SW-BB#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 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
```

Figura 26. Estado de las VLANs en SW-BB

```
SW-CC#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 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
```

Figura 27. Estado de las VLANs en SW-CC

En las figuras 25, 26 y 27 se observa que las interfaces fueron creadas con éxito en los 3 switches y en estado activo.

El siguiente paso es asociar los puertos a las VLAN y configure las direcciones IP. Se configurara el puerto f0/10 en modo de acceso para SW-AA, SW-BB y SW-CC asignándolo a la VLAN 10, este mismo proceso se realiza para los puertos f0/15 y f0/20 en SW-AA, SW-BB y SW-CC. Por último, se asignan las VLANs y las direcciones IP de los PCs de acuerdo con la tabla 2:

```
SW-AA>enable
SW-AA#configure terminal
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 15
SW-AA(config-if)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit

SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
```

```
SW-BB(config-if)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 15
SW-BB(config-if)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 15
SW-CC(config-if)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
```

El siguiente paso es asignar las direcciones IP y mascara de subred asociada a cada puerto, teniendo en cuenta el diagrama de conexión de la red VLAN y los datos de la tabla 2. Como cada switch maneja 3 PCs enumerados, demos definir la interfaz con la cual están conectados al switch:

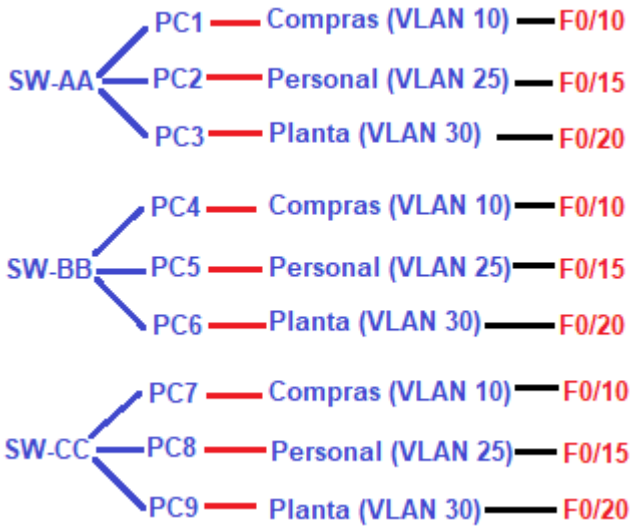


Figura 28. VLAN asociadas a cada PC

Teniendo en cuenta el diagrama esquemático de la figura 28 y la tabla 6 de direcciones IP, se proceden a configurar los PCs asociados a cada switch:

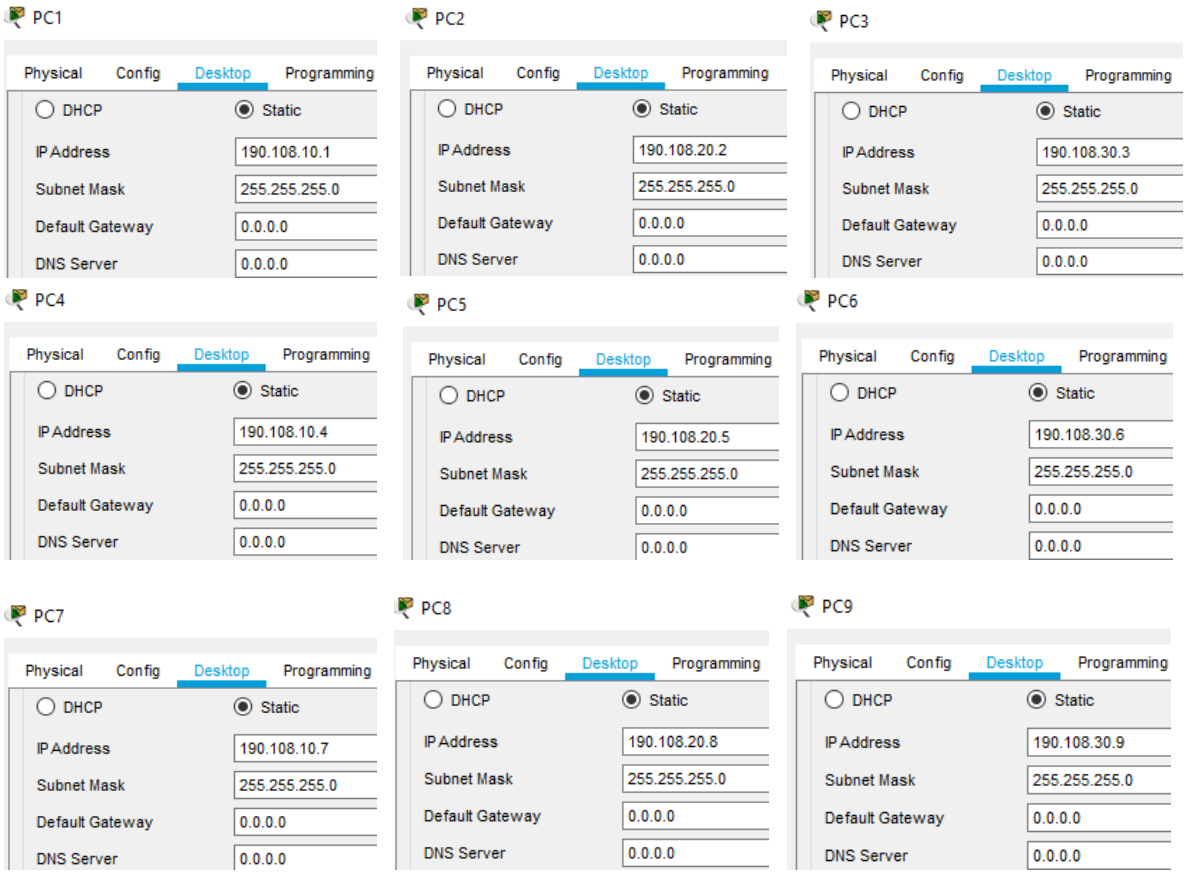


Figura 29. Configuración de las IP en los PCs

1.2.4 Configurar las direcciones IP en los Switches

En cada uno de los Switches se asigna una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la tabla 6 de direccionamiento, y al mismo tiempo se activa la interfaz.

```
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)#no shutdown

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)#no shutdown

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)#no shutdown
```

1.2.5 Verificar la conectividad Extremo a Extremo

Para comprobar la conectividad entre los PCs, se ejecute un ***ping*** desde cada PC a los demás.

- Ejecutamos ping desde el PC1 hacia PC2 y PC4:

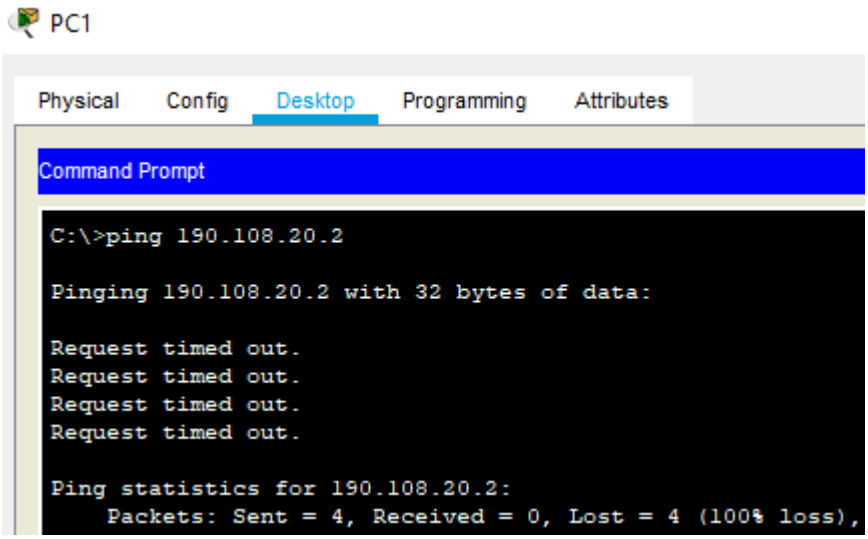


Figura 30. Ping desde PC1 a PC2

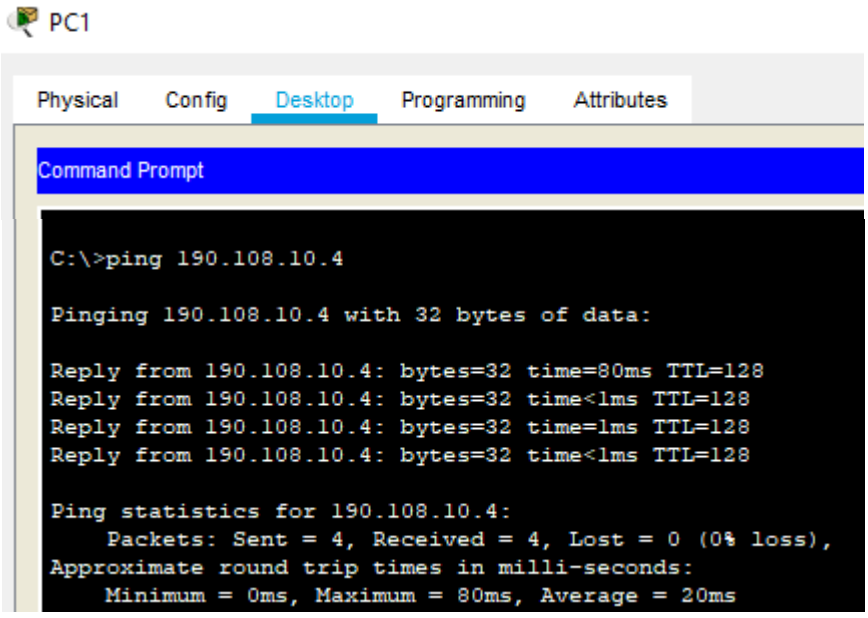


Figura 31. Ping desde PC1 a PC4

En la figura 30, se observa que el ping desde PC1 a PC2 falla, mientras que en la figura 31 se observa que el ping de PC1 a PC4 fue satisfactorio, esto se debe a que PC2 está en una VLAN distinta a la de PC1 y PC4. Si hacemos ping de PC1 hacia PC4 y PC7, estos serán satisfactorios, debido a que están dentro de la misma VLAN, como se muestra en las figuras 32 y 33:

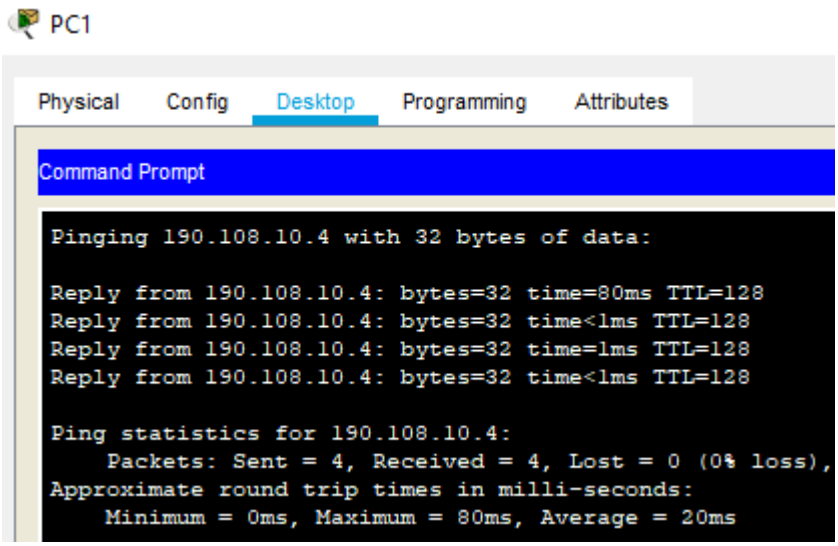


Figura 32. Ping satisfactorio de PC1 a PC4

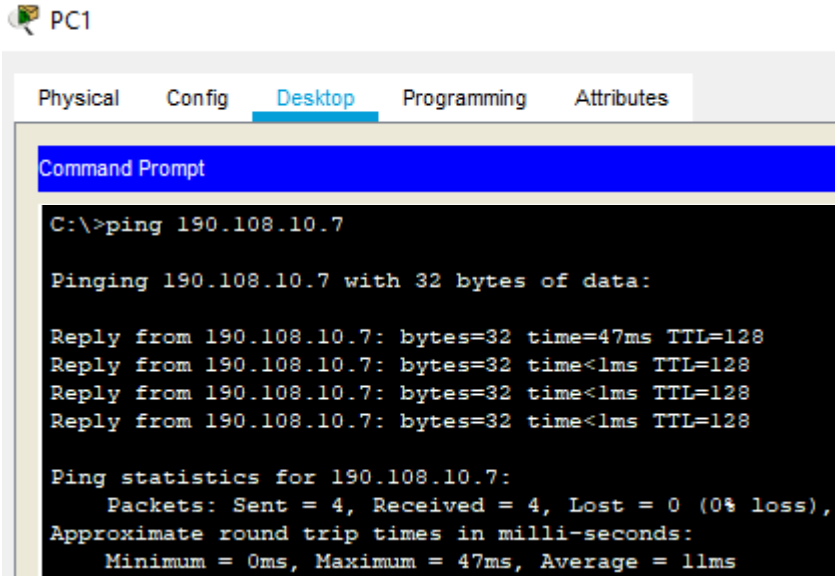


Figura 33. Ping satisfactorio de PC1 a PC7

- Ejecutamos ping desde el PC2 hacia PC5, PC8 y PC6:

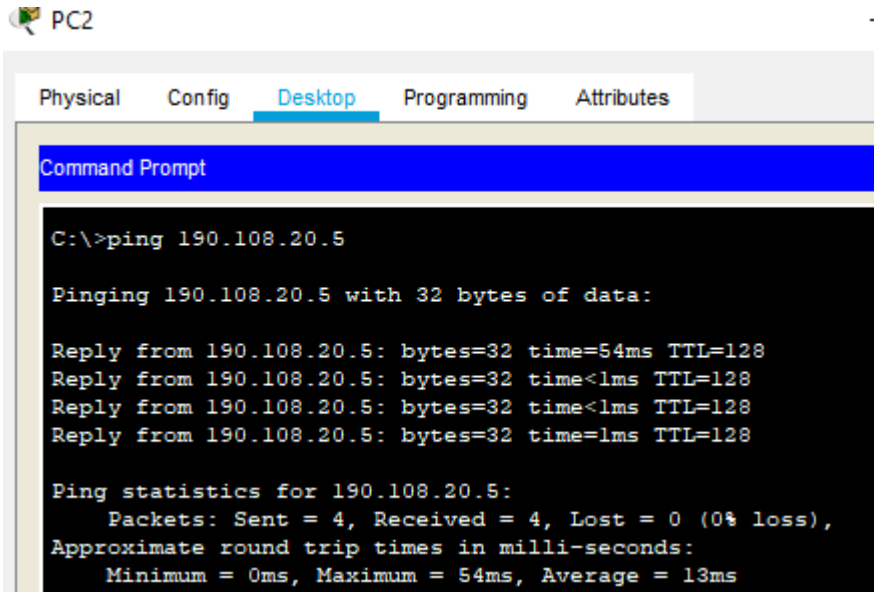


Figura 34. Ping de PC2 a PC5

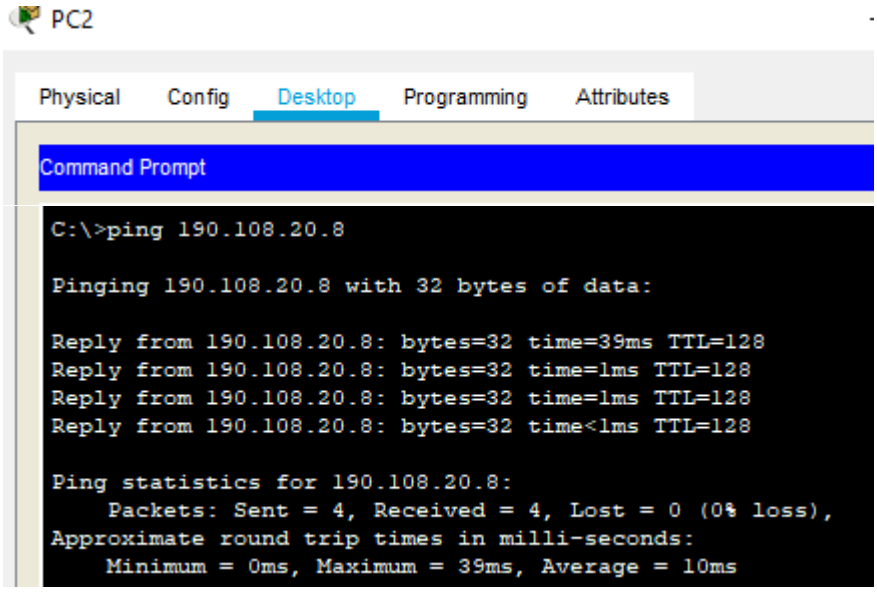


Figura 35. Ping de PC2 a PC8

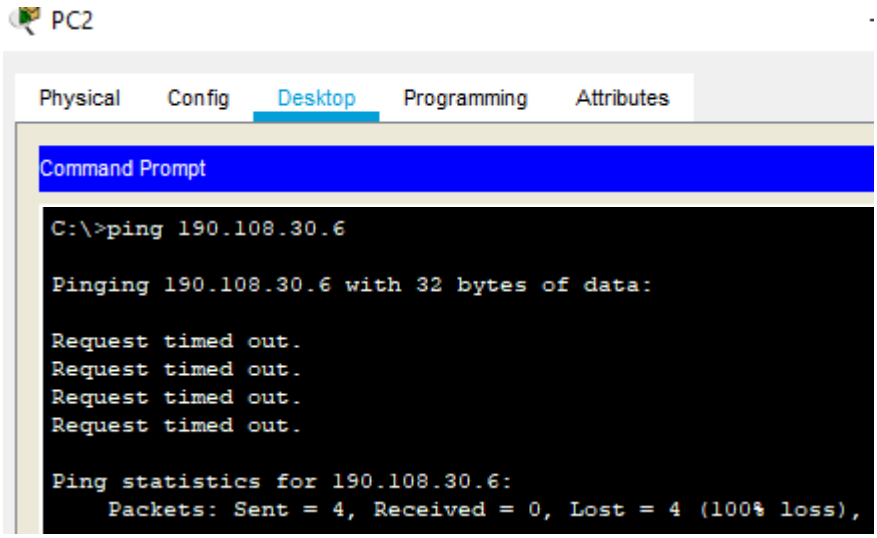


Figura 36. Ping de PC2 a PC6

En las figuras 34 y 35, se observa que el ping desde PC2 a PC5 y PC8 son satisfactorios debido a estos PCs están dentro de la misma VLAN, mientras que en la figura 36 se observa que el ping de PC2 a PC6 ha fallado, esto se debe a que PC6 está en una VLAN distinta a la de PC2, PC5 y PC8. Como conclusión, los pings solo serán satisfactorios en los PCs que estén dentro de la misma VLAN.

Ahora se ejecuta un Ping desde cada Switch hacia los demás:

```
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 = 0/0/3 ms
```

Figura 37. Ping de SW-AA hacia SW-BB y SW-CC

```
SW-BB#ping 190.108.99.1

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

Figura 38. Ping de SW-BB hacia SW-AA y SW-CC

```
SW-CC#ping 190.108.99.1

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

Figura 39. Ping de SW-CC hacia SW-AA y SW-BB

En las figuras 37, 38 y 39 se observa que en este caso el ping ha sido satisfactorio, los cinco paquetes de prueba han llegado correctamente, esto se debe a que los 3 switches se encuentran configurados dentro de la misma VLAN, en este caso la vlan 99, que les permite cambiar información entre ellos mediante los enlaces troncales que fueron configurados inicialmente.

Ahora se ejecute un Ping desde cada Switch a cada PC:

```
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)
```

Figura 40. Fallo del pin de SW-AA 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)
```

Figura 41. Fallo del pin de SW-BB a PC4, PC5 y PC6

```
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)
```

Figura 42. Fallo del pin de SW-CC a PC7, PC8 y PC9

En las figuras 40, 41 y 42 se evidencia el que de la comunicación entre los switches y los PCs es fallida, los ping emitidos fallaron, debido a que los switches no permiten el tráfico de información de un punto a otro.

CONCLUSIONES

Para las configuraciones del escenario 1 se debe tener en cuenta que las rutas a anunciar deben existir en la tabla de ruteo del router local o no serán enviadas en las actualizaciones para que las rutas aprendidas puedan ser propagadas por defecto, teniendo en cuenta que la configuración e implementación del protocolo BGP es de suma importante en el momento de crear las sesiones BGP, y al momento de introducir las direcciones IP de los vecinos BGP se debe hacer de manera correcta, esto para evitar inconvenientes en el momento de establecer sesión BGP con los routers. En el proceso de configuración de las redes BGP realizado para el primer escenario, se concluye que una vez establecida la sesión BGP el router empieza a intercambiar información de encaminamiento con sus vecinos BGP, al recibir esta información se realiza la selección y almacenamiento de las rutas más óptimas, de manera que primero son insertadas todas las rutas en la tabla de BGP.

En el marco del desarrollo del escenario 2 hay que resaltar que el comando ***switchport mode trunk*** cambia el modo de enlace del puerto de acceso a trunk para permitir su operación como puerto troncal, del mismo modo, se pudo observar que a pesar de usarse enlaces troncales entre los switches, no se logró con éxito la respectiva comunicación entre los distintos PCs conectados a su respectiva VLAN, esto se debe a que los PCs no están conectados todos a la misma VLAN, lo que ocasiona que el ping falle, sin embargo, solo habrá comunicación entre aquellos PCs que estén dentro de la misma VLAN.

En el caso de la comunicación entre los switches y los PCs, los ping emitidos fallaron, debido a que los switches no permiten el tráfico de información de un punto a otro, pero este tipo de inconvenientes se logra mediante la implementación de un switch de capa 3, donde se puede mencionar que una de las capacidades de los switch de capa tres o switch multicapas es que se pueden usar distintos tipos de interfaces con las que se puede comunicar diferentes redes desde el switch multicapa, sencillamente trabaja en capa 3 para intercambiar información de una vlan a otra.

BIBLIOGRAFIA

Ariganello, E., Sevilla, E. Redes CISCO. CCNP a fondo. Guía de estudio para profesionales. Editorial RA-MA S.A Editorial y Publicaciones. Madrid. Pág. 201-225

Duggna, M. Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs. Pearson Education. Third Edition

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101

Edgeworth, R., Foss, A., Rios, R. (2015). CISCO Press (Ed). IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols.

Hucaby, D., McQuerry, S. (2003). CISCO Press (Ed). Cisco Field Manual: Catalyst Switch Configuration. A complete, concise reference for implementing the most features of the Cisco family of switches.

Jack, T. (2004). CCNP: Building Cisco MultiLayer Switched Networks Study Guide

Froom, R., Sivasubramanian, B., Frahim, E. (2010). CISCO Press (Ed) Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide Foundation Learning for SWITCH 642-813