DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ANDRES JAIMES RUIZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ANDRES JAIMES RUIZ

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

____

____

____

____

____

____

____

____

Firma del Presidente del Jurado

____

Firma del Jurado

____

Firma del Jurado

BOGOTÁ, 22 de mayo 2020

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

BGP: Border Gateway Protocol es un protocolo de puerta de enlace exterior que permite a los sistemas autónomos intercambiar información de enrutamiento entre sí

VTP: son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco

Interfaz loopback: El dispositivo de red loopback es una interfaz de red virtual. Las direcciones del rango '127.0.0.0/8' son direcciones de loopback, de las cuales se utiliza, de forma mayoritaria, la '127.0.0.1' por ser la primera de dicho rango, añadiendo '::1' para el caso de IPv6 ('127.0.0.1::1'). Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers. y son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

DTP: (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE.

VLAN:Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

El Diplomado de Profundización CISCO CCNP busca proporcionar una visión general teórica detallada y avanzada acerca de los aspectos más relevantes del enrutamiento y la conmutación. Esta visión brinda el conocimiento y las habilidades necesarias para diseñar y apoyar redes empresariales. El desarrollo de la prueba de habilidades permite evidenciar el conocimiento adquirido a lo largo del diplomado desarrollando; en este caso específico, el uso y la configuración de dispositivos cisco virtualizados y simulados. Más concretamente, se usan los softwares de simulación de redes GNS3 y Paket tracer para el desarrollo de topologías de red usando los protocolos BGP, VTP y DTP. Finalmente, se obtuvo la correcta configuración y trazabilidad entre las distintas topologías de redes con dichos protocolos.

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

ABSTRACT

The CISCO CCNP Deepening Diploma seeks to provide a detailed and advanced theoretical overview of the most relevant aspects of routing and switching. This overview provides the knowledge and skills necessary to design and support business networks. The development of the skills test allows to demonstrate the knowledge acquired throughout the developing diploma; in this specific case, the use and configuration of simulated and virtualized cisco devices. More specifically, the simulation software of GNS3 and Paket tracer networks are used for the development of network topologies using the BGP, VTP and DTP protocols. Finally, the correct configuration and traceability between the different network topologies with these protocols was obtained.

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

INTRODUCCIÓN

En el presente documento se da paso al desarrollo de la prueba de habilidades correspondiente al diplomado CCNP. En esta prueba se pone en práctica los conocimientos adquiridos durante el diplomado identificando situaciones problémicas asociadas con aspectos de conmutación y enrutamiento. Se hace uso eficiente de estrategias basadas en comandos IOS y estadísticas de tráfico en las interfaces, con el fin de resolver conflictos de configuración y conectividad en contextos de redes LAN y WAN.

En trabajo se enmarca en dos escenarios, el primero corresponde a la configuración y uso de Border Gateway Protocol (BGP), el cual es un protocolo de gateway exterior que permite que los Sistemas Autónomos intercambien información de ruteo entres sí, a partir de una topología dada, usando el software de simulación GNS3. El segundo escenario corresponde al uso y configuración del protocolo troncal VLAN (VTP), usando es este caso el software Paket tracer.

DESARROLLO

1. Escenario 1

Figura 1.Simulación Escenario 1

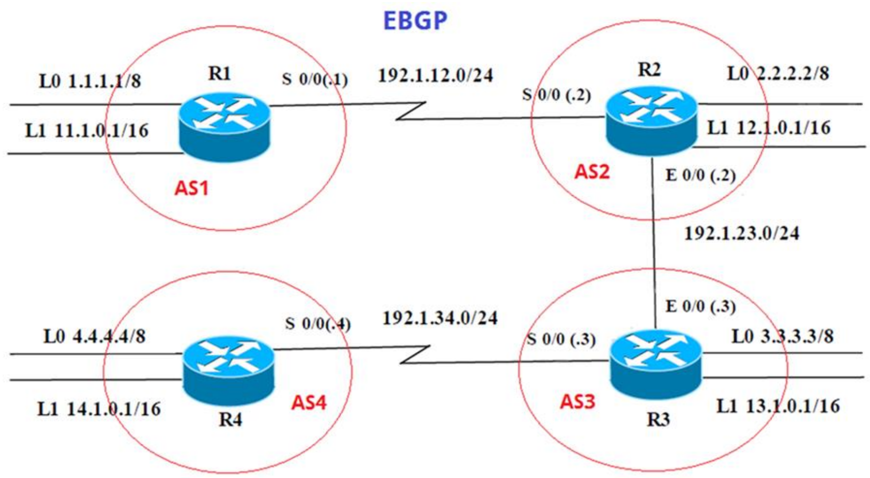


Figura 2. Información para configuración de los Routers

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

Configuración R1

- **R1(config)#int s1/0**
- **R1(config-if)#ip address 192.1.12.1 255.255.255.0**
- **R1(config-if)#no shutdown**
- **R1(config-if)#int loopback 0**
- **R1(config-if)#ip address 1.1.1.1 255.0.0.0**
- **R1(config-if)#int loopback 1**
- **R1(config-if)#ip address 11.1.0.1 255.255.0.0**
- **R1(config-if)#exit**

Configuración R2

- **R2(config)#int s1/0**
- **R2(config-if)#ip address 192.1.12.2 255.255.255.0**
- **R2(config-if)#no shutdown**
- **R2(config-if)#int g0/0**
- **R2(config-if)#ip address 192.1.23.2 255.255.255.0**
- **R2(config-if)#no shutdown**
- **R2(config-if)#int loopback 0**
- **R2(config-if)#ip address 2.2.2.2 255.0.0.0**
- **R2(config-if)#int loopback 1**
- **R2(config-if)#ip address 12.1.0.1 255.255.0.0**

Configuración R3

- **Configuración R3**
- **R3(config)#int s1/0**
- **R3(config-if)#ip address 192.1.34.3 255.255.255.0**
- **R3(config-if)#no shutdown**
- **R3(config-if)#int g0/0**

- **R3(config-if)#ip address 192.1.23.3 255.255.255.0**
- **R3(config-if)#no shutdown**
- **R3(config-if)#int loopback 0**
- **R3(config-if)#ip address 3.3.3.3 255.0.0.0**
- **R3(config-if)#int loopback 1**
- **R3(config-if)#ip address 13.1.0.1 255.255.0.0**

Configuración R4

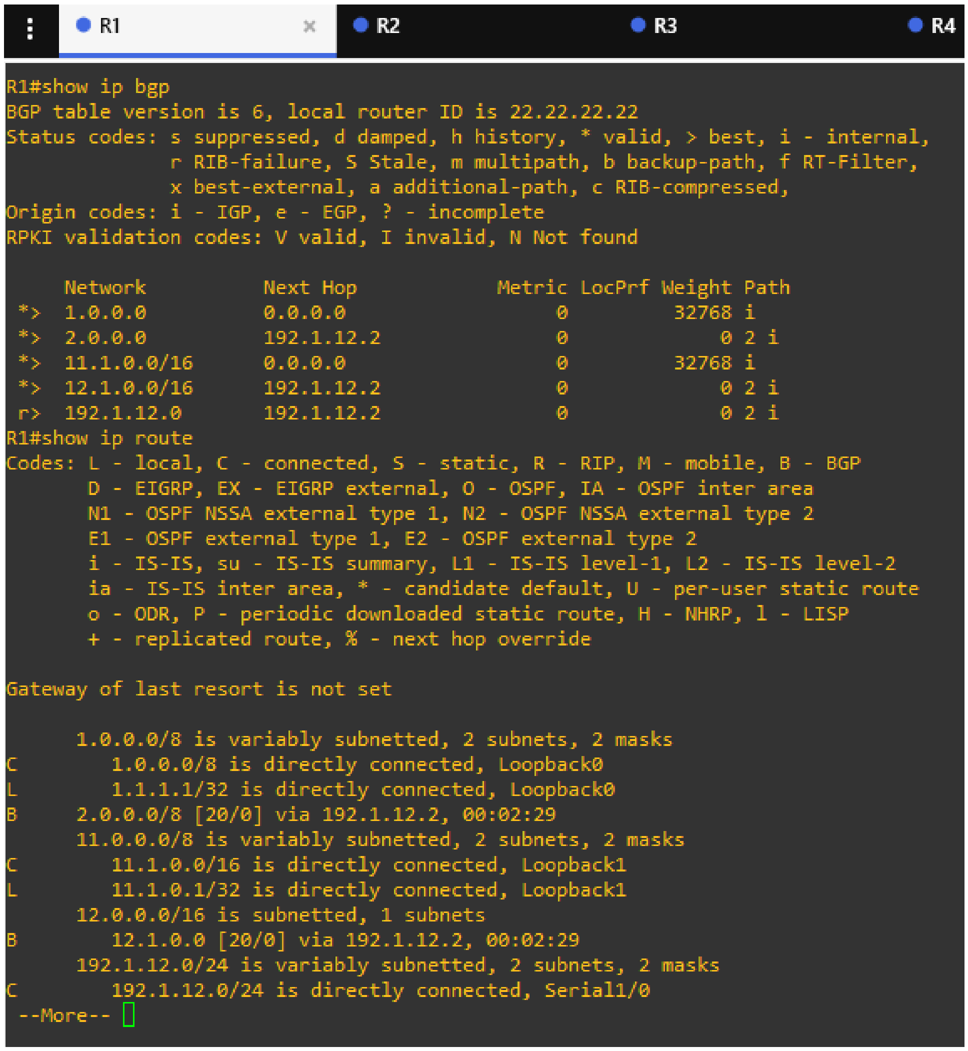
- **Configuración R4**
- **R4(config)#int s1/0**
- **R4(config-if)#ip address 192.1.34.4 255.255.255.0**
- **R4(config-if)#no shutdown**
- **R4(config-if)#int loopback 0**
- **R4(config-if)#ip address 4.4.4.4 255.0.0.0**
- **R4(config-if)#int lopback 1**
- **R4(config-if)#ip address 14.1.0.1 255.255.0.0**
- **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.***

- **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**

Se comprueba con el comando show ip bgp. Se evidencia las rutas con relación de vecinos.

Figura 3. Show ip bgp R1

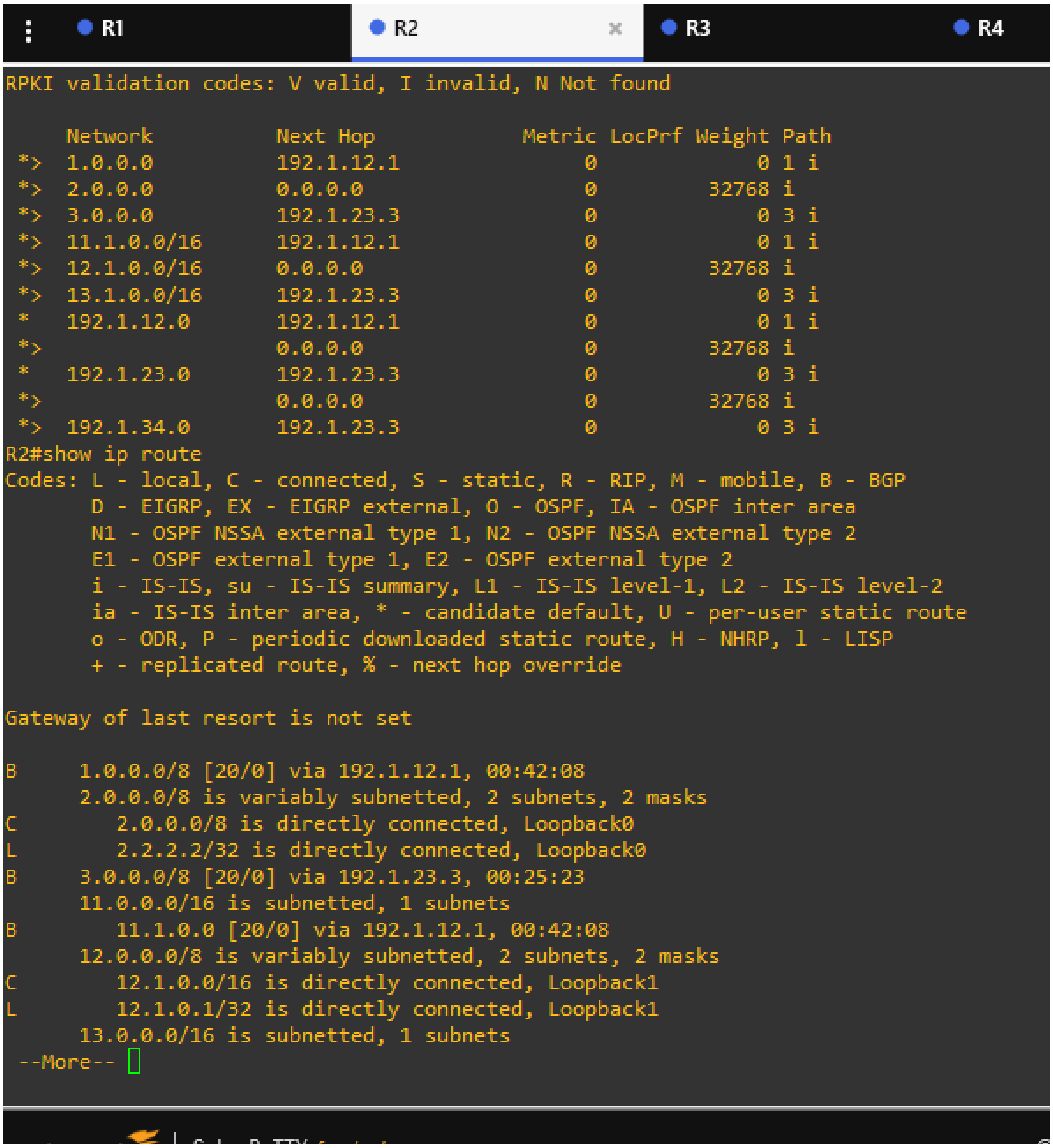



```
R1#show ip bgp
BGP table version is 6, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     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
 *>  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
 r>  192.1.12.0       192.1.12.2               0             0 2 i
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/8 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
B     2.0.0.0/8 [20/0] via 192.1.12.2, 00:02:29
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.1.0.0/16 is directly connected, Loopback1
L        11.1.0.1/32 is directly connected, Loopback1
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.12.2, 00:02:29
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
 --More--
```

- **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**

Se comprueba con el comando show ip bgp en R2. Se evidencia las rutas con relación de vecinos.

Figura 4. Show ip bgp R2

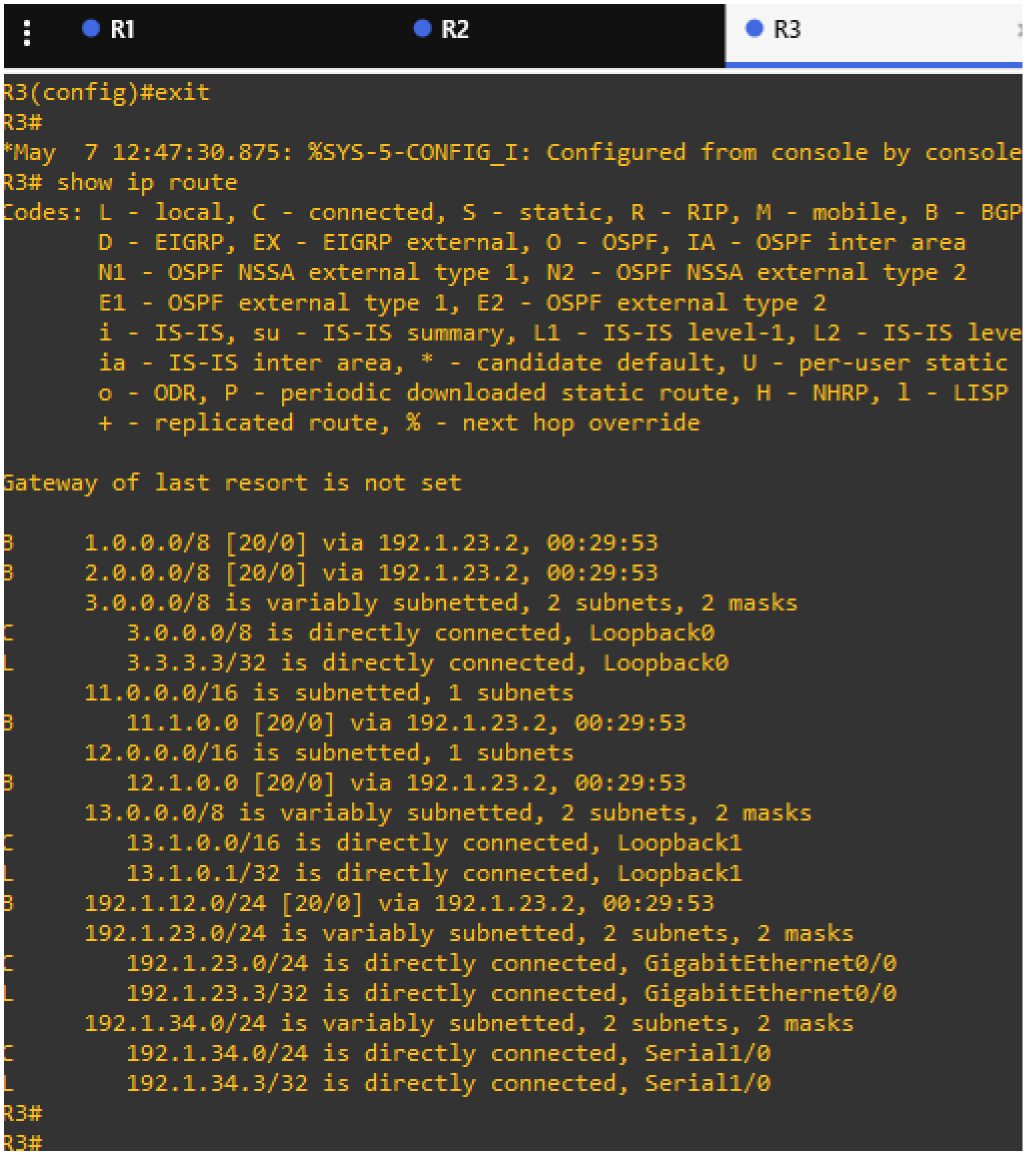


2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

- **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**

Se aplica el comando show ip route en R3. Se comprueba adyacencia de vecinos con los otros routers.

Figura 5. Show ip route R3



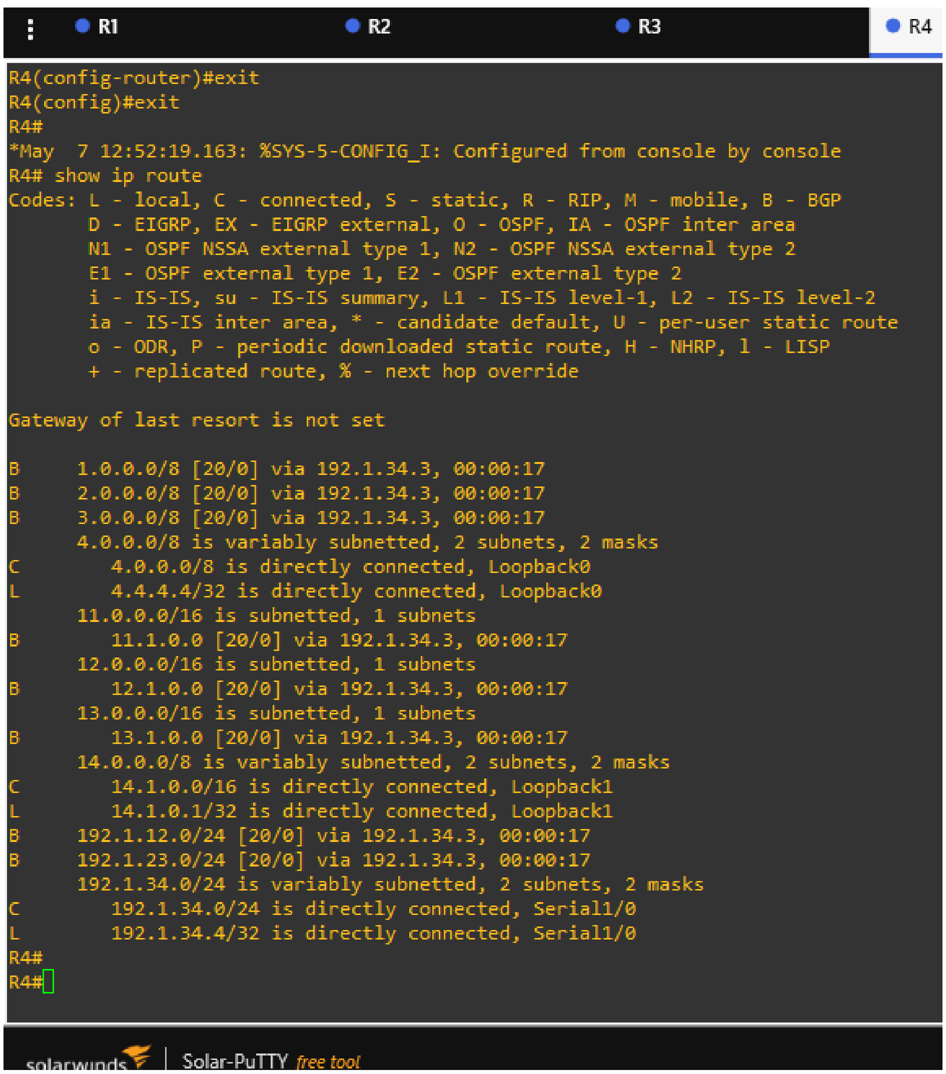

```
R3(config)#exit
R3#
*May  7 12:47:30.875: %SYS-5-CONFIG_I: Configured from console by console
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS leve
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:29:53
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:29:53
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.0.0.0/8 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:29:53
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:29:53
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.0.0/16 is directly connected, Loopback1
L        13.1.0.1/32 is directly connected, Loopback1
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:29:53
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.3/32 is directly connected, Serial1/0
R3#
R3#
```

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

- **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**

Se valida la configuración BGP.

Figura 6. Show ip route R4




```
R4(config-router)#exit
R4(config)#exit
R4#
*May  7 12:52:19.163: %SYS-5-CONFIG_I: Configured from console by console
R4# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:17
B     2.0.0.0/8 [20/0] via 192.1.34.3, 00:00:17
B     3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:17
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.0.0.0/8 is directly connected, Loopback0
L        4.4.4.4/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.34.3, 00:00:17
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.34.3, 00:00:17
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.34.3, 00:00:17
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.1.0.0/16 is directly connected, Loopback1
L        14.1.0.1/32 is directly connected, Loopback1
B     192.1.12.0/24 [20/0] via 192.1.34.3, 00:00:17
B     192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:17
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.4/32 is directly connected, Serial1/0
R4#
R4#
```

Se evidencia que se han aprendido las rutas loopback de forma automática.

Figura 7. Show bgp R1

```
R1#show bgp
BGP table version is 13, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - in
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-F
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     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       0.0.0.0                  0         32768 i
 *                    192.1.12.2               0             0 2 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 8. Show bgp R2

```
R2#show 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 - int
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Fi
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     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
R2#
```

Figura 9.Show bgp R3

```
*May  7 12:52:12.195: %BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up
R3#show bgp
BGP table version is 12, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - inte
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Fil
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     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
 *>  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 10. Show bgp R4

```
R4#
R4#show bgp
BGP table version is 12, local router ID is 66.66.66.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - inte
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Fil
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     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
 *>  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
R4#
```

Se hace ping de R1 a las loopback de los otros Routers y a serial 1/0.

Figura 11. Ping de R1 a las loopback

```
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 = 188/216/248 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 = 136/152/192 ms
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 = 60/80/104 ms
R1#ping 192.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/223/268 ms
R1#
```

solarwinds | Solar-PuTTY *free tool*

Figura 12. Ping de R1 a las loopback (continuacion)

```
 *>  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
R4#traceroute 11.1.0.1
Type escape sequence to abort.
Tracing the route to 11.1.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.1.34.3 56 msec 48 msec 96 msec
  2 192.1.23.2 [AS 3] 176 msec 140 msec 112 msec
  3 192.1.12.1 [AS 2] 212 msec 252 msec 184 msec
R4#traceroute 12.1.0.1
Type escape sequence to abort.
Tracing the route to 12.1.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.1.34.3 44 msec 68 msec 84 msec
  2 192.1.23.2 [AS 3] 196 msec 132 msec 136 msec
R4#trace route 13.1.0.1
Translating "route"
               ^
% Invalid input detected at '^' marker.

R4#traceroute 13.1.0.1
Type escape sequence to abort.
Tracing the route to 13.1.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.1.34.3 120 msec 36 msec 40 msec
R4#
```

Figura 13. Comprobación con show ip route R1

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level
       ia - IS-IS inter area, * - candidate default, U - per-user static r
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/8 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
B     2.0.0.0/8 [20/0] via 192.1.12.2, 01:07:10
B     3.0.0.0/8 [20/0] via 192.1.12.2, 00:50:02
B     4.0.0.0/8 [20/0] via 192.1.12.2, 00:16:00
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.1.0.0/16 is directly connected, Loopback1
L        11.1.0.1/32 is directly connected, Loopback1
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.12.2, 01:07:10
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.12.2, 00:50:02
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.12.2, 00:16:00
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.1/32 is directly connected, Serial1/0
B     192.1.23.0/24 [20/0] via 192.1.12.2, 00:50:32
B     192.1.34.0/24 [20/0] via 192.1.12.2, 00:50:02
R1#
```

Figura 14. Comprobación con show ip route R2

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS leve
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 01:08:04
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.0.0.0/8 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
B     3.0.0.0/8 [20/0] via 192.1.23.3, 00:51:19
B     4.0.0.0/8 [20/0] via 192.1.23.3, 00:16:54
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 01:08:04
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.0.0/16 is directly connected, Loopback1
L        12.1.0.1/32 is directly connected, Loopback1
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.23.3, 00:51:19
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.23.3, 00:16:54
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.2/32 is directly connected, Serial1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.2/32 is directly connected, GigabitEthernet0/0
B     192.1.34.0/24 [20/0] via 192.1.23.3, 00:51:19
R2#
```

Figura 15. Comprobación con show ip route R3

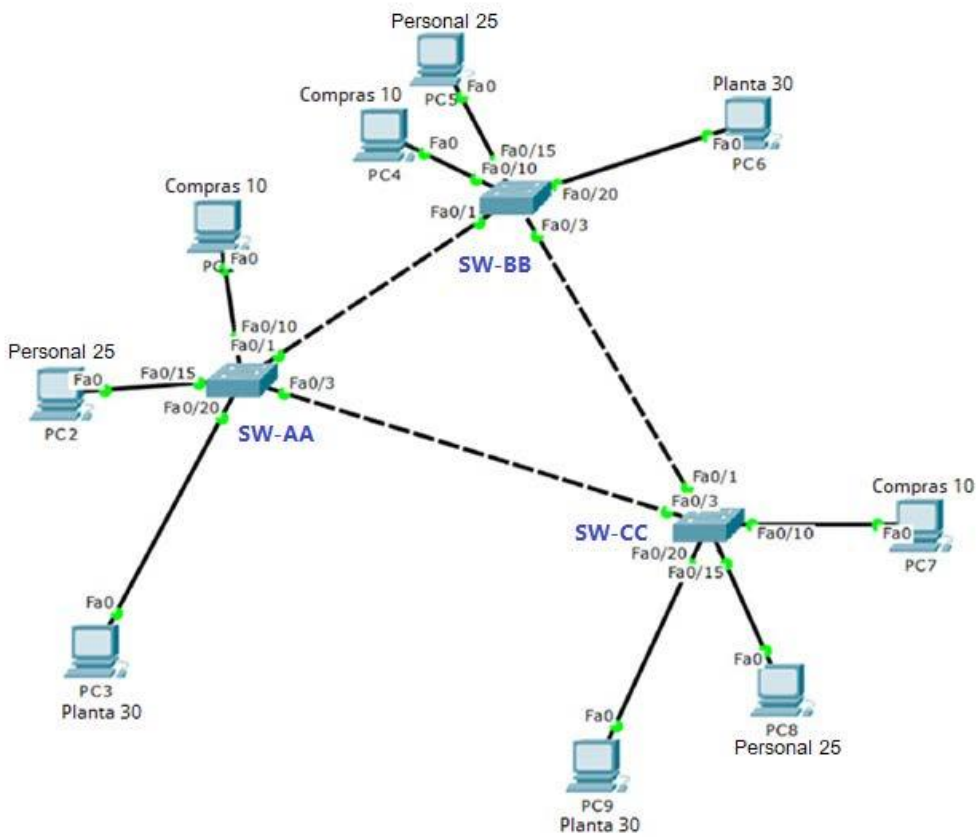
```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level
       ia - IS-IS inter area, * - candidate default, U - per-user static r
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:51:58
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:51:58
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.0.0.0/8 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
B     4.0.0.0/8 [20/0] via 192.1.34.4, 00:17:34
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:51:58
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:51:58
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.0.0/16 is directly connected, Loopback1
L        13.1.0.1/32 is directly connected, Loopback1
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.34.4, 00:17:34
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:51:58
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.3/32 is directly connected, Serial1/0
R3#
R3#
```

Figura 16. Comprobación con show ip route R4

```
R4# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS leve
       ia - IS-IS inter area, * - candidate default, U - per-user static
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.34.3, 00:18:06
B     2.0.0.0/8 [20/0] via 192.1.34.3, 00:18:06
B     3.0.0.0/8 [20/0] via 192.1.34.3, 00:18:06
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.0.0.0/8 is directly connected, Loopback0
L        4.4.4.4/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.34.3, 00:18:06
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.34.3, 00:18:06
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.34.3, 00:18:06
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.1.0.0/16 is directly connected, Loopback1
L        14.1.0.1/32 is directly connected, Loopback1
B     192.1.12.0/24 [20/0] via 192.1.34.3, 00:18:06
B     192.1.23.0/24 [20/0] via 192.1.34.3, 00:18:06
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.4/32 is directly connected, Serial1/0
R4#
R4#
```

2. Escenario 2

Figura 17. Simulación 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.

SW-BB
vtp mode servidor
SW-AA
vtp mode client
SW-CC
vtp mode client

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

Figura 18. Show vtp status SW-BB, SW-AA y SW-CC

```
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                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72
0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

```
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                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A C
0xA0 0x3A
```

```
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                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72
0xA0 0x3A
```

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***.

El puerto 0/1 de SW se deja desirable.

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

Figura 19. Show interfaces trunk SW-AA y SW-BB

```
SW-AA#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

```
SW-BB>show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

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

int 0/3
switchport mode trunk

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

Figura 20. Show interfaces trunk en SW-AA

```
SW-AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vla:
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       none
Fa0/3       1
```

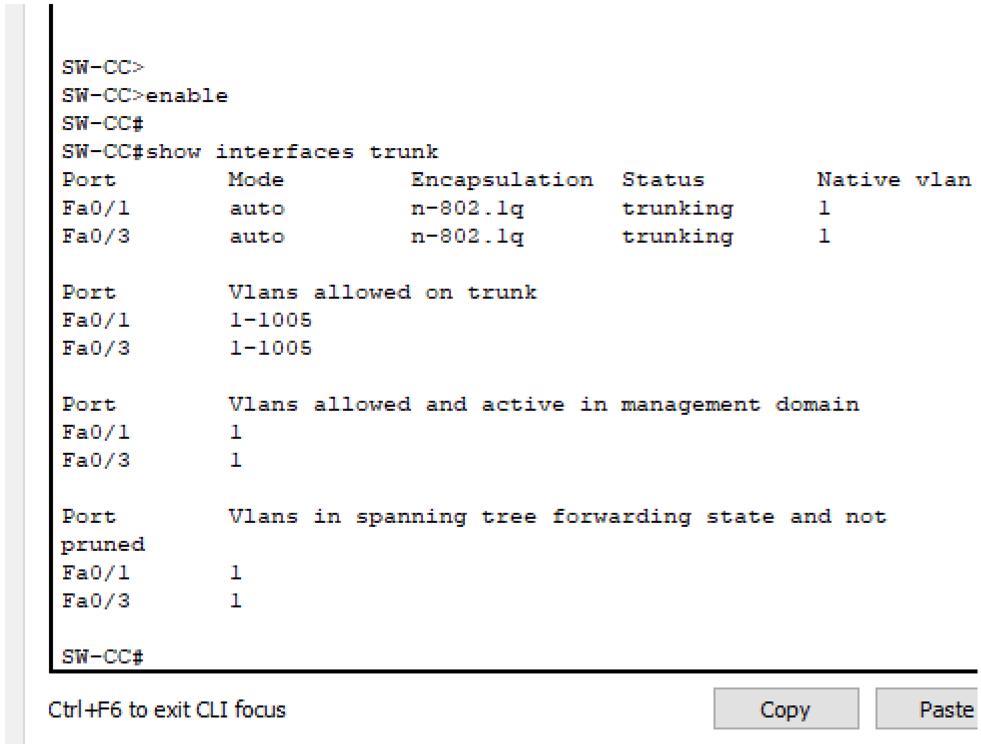
8. Configure un enlace "trunk" permanente entre SW-BB y SW-CC**.**

interface f0/3
switchport mode trunk

Figura 21. Show interfaces trunk en SW-BB

```
SW-BB#
SW-BB#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vla:
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       1

SW-BB#
```

Figura 22. Show interfaces trunk en SW-CC



```
SW-CC>
SW-CC>enable
SW-CC#
SW-CC#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         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

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

SW-CC#
```

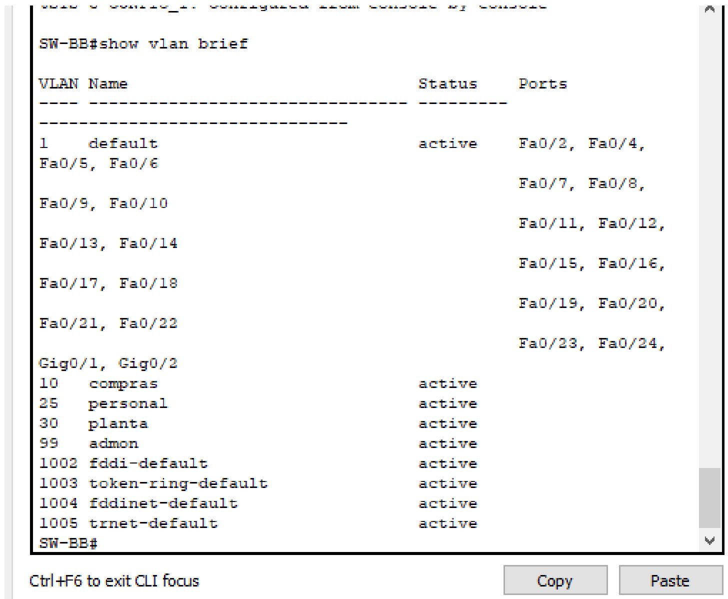

C. Agregar VLANs y asignar puertos.

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

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

10. Verifique que las VLANs han sido agregadas correctamente.

Figura 23. VLANS Compras, personal, planta



```
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#
```

Ctrl+F6 to exit CLI focus   Copy   Paste

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

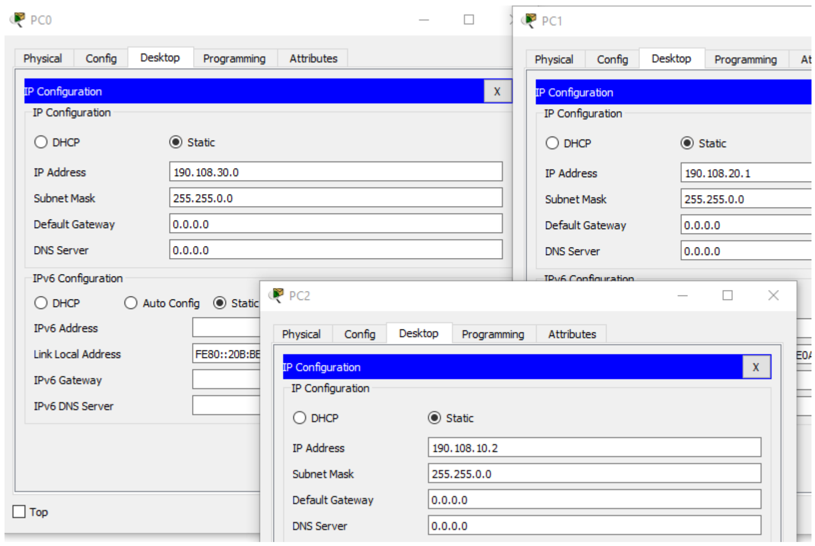
Figura 24. Direcciones IP para VLAN

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

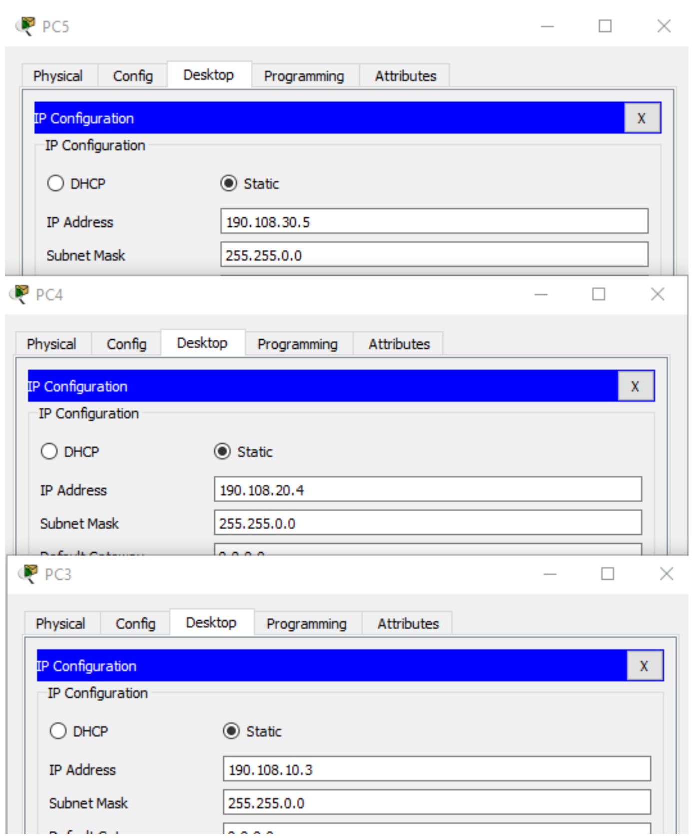
SW-AA

Figura 25. Direcciones IP en PC0



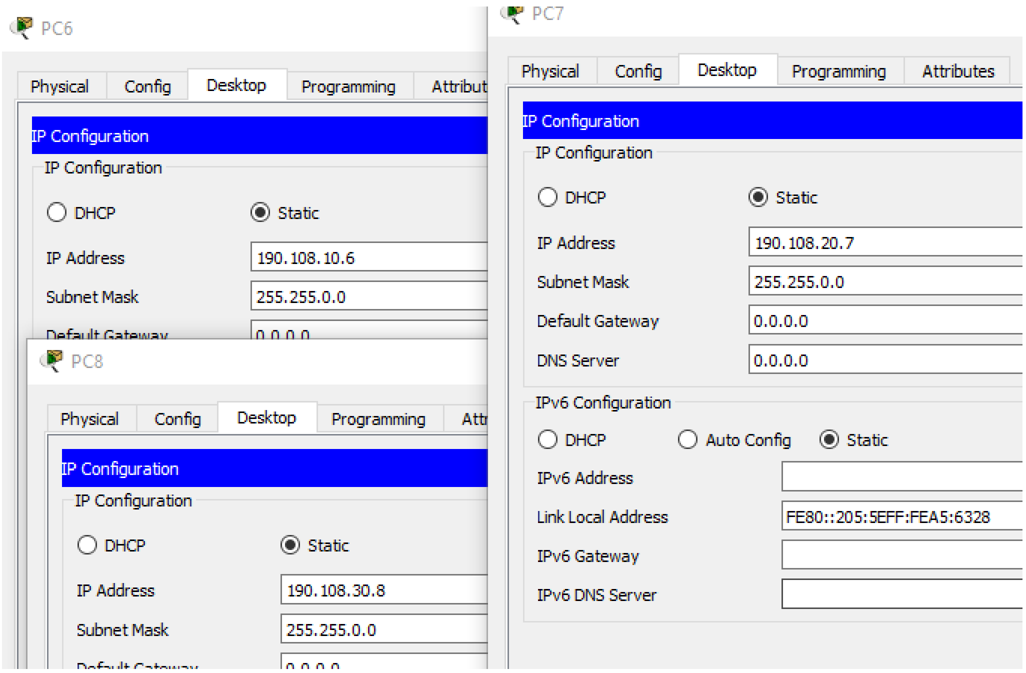
SW-BB

Figura 26. Direcciones IP en PC3, PC4 y PC5



SW-CC

Figura 27. Direcciones IP en PC6, PC7 y PC8



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.

SW-AA SW-BB SW-CC

interface f0/10
switchport mode access
switchport acces vlan 10

SW-AA SW-BB SW-CC

SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)##switchport access vlan 20 **^**
SW-CC(config-if)#switchport access vlan 25

SW-CC(config-if)#interface f0/20
SW-CC(config-if)#switchport mode access

SW-AA(config)#
SW-AA(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport acces vlan 20
SW-AA(config-if)#
SW-AA(config-if)#interface f0/20
SW-AA(config-if)#switchport mode access

SW-BB(config)#nterface f0/15 ^
SW-BB(config)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-BB(config-if)#nterface f0/20
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface f0/20
SW-BB(config-if)#switchport mode access

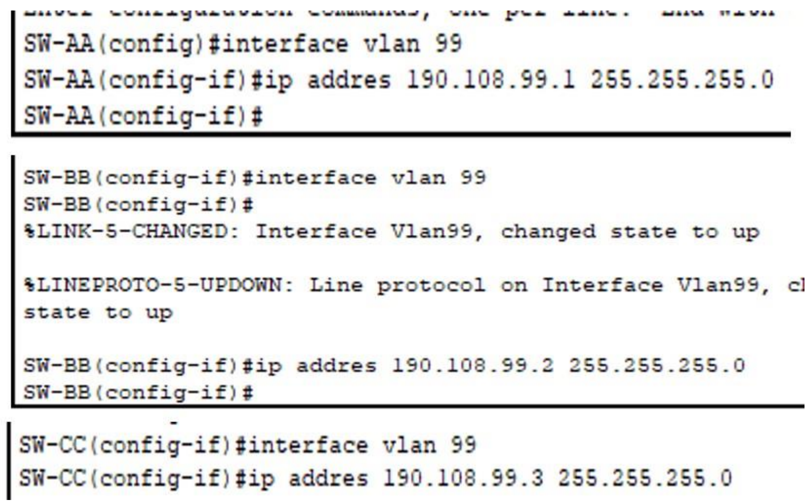
D. Configurar las direcciones IP en los Switches.

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.

Figura 28. Direccionamiento para Switches

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

Figura 29. Comprobación de direccionamiento de los switches

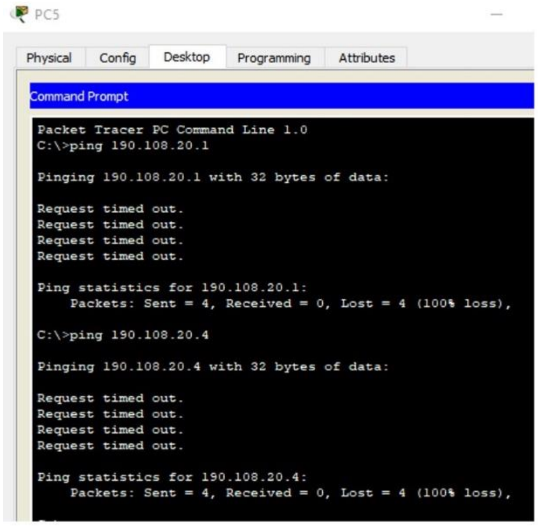


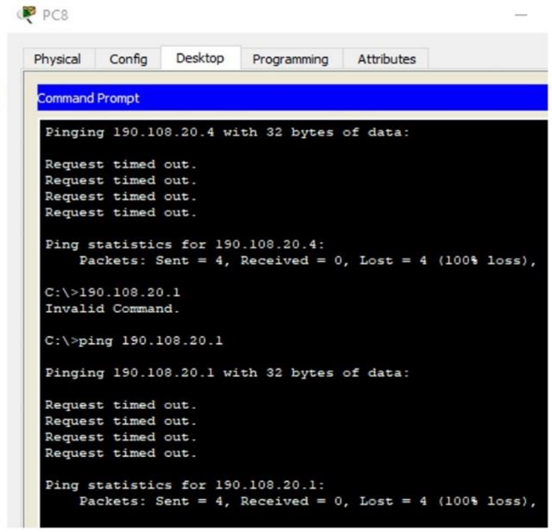
```
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip addres 190.108.99.1 255.255.255.0
SW-AA(config-if)#

SW-BB(config-if)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

SW-BB(config-if)#ip addres 190.108.99.2 255.255.255.0
SW-BB(config-if)#

SW-CC(config-if)#interface vlan 99
SW-CC(config-if)#ip addres 190.108.99.3 255.255.255.0
```

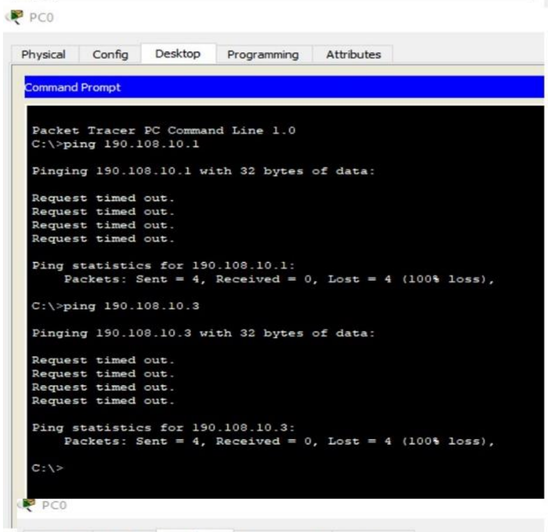
E. Verificar la conectividad Extremo a Extremo

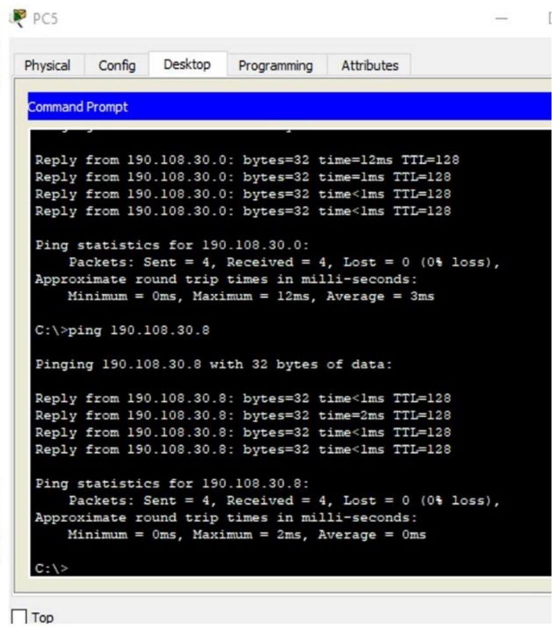
15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

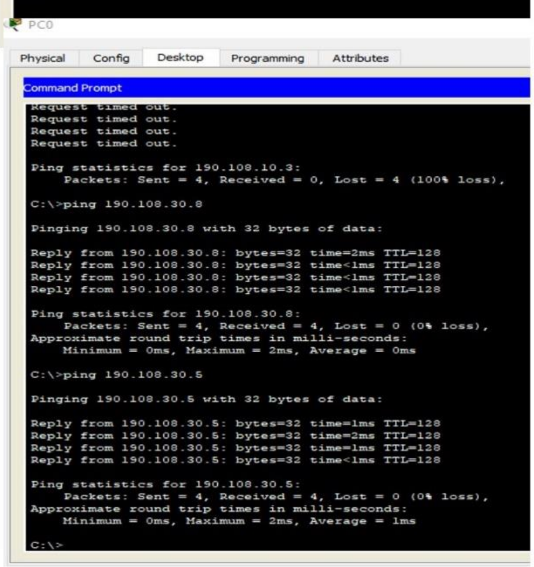
Figura 30. Ping desde cada PC


PC5
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.20.1
Pinging 190.108.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.20.4
Pinging 190.108.20.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),


PC8
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.20.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>190.108.20.1
Invalid Command.
C:\>ping 190.108.20.1
Pinging 190.108.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),


PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.1
Pinging 190.108.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.10.3
Pinging 190.108.10.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>


PC5
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 190.108.30.0: bytes=32 time=12ms TTL=128
Reply from 190.108.30.0: bytes=32 time=1ms TTL=128
Reply from 190.108.30.0: bytes=32 time<1ms TTL=128
Reply from 190.108.30.0: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.30.0:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
C:\>ping 190.108.30.8
Pinging 190.108.30.8 with 32 bytes of data:
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Reply from 190.108.30.8: bytes=32 time=2ms TTL=128
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.30.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>
Top


PC0
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.30.8
Pinging 190.108.30.8 with 32 bytes of data:
Reply from 190.108.30.8: bytes=32 time=2ms TTL=128
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Reply from 190.108.30.8: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.30.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>ping 190.108.30.5
Pinging 190.108.30.5 with 32 bytes of data:
Reply from 190.108.30.5: bytes=32 time=1ms TTL=128
Reply from 190.108.30.5: bytes=32 time=2ms TTL=128
Reply from 190.108.30.5: bytes=32 time=1ms TTL=128
Reply from 190.108.30.5: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.30.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\>

Se puede apreciar que los pings a los pc que pertenecen a las redes y vlan diferentes no son exitosos. Los pings que pertenecen a la misma red vlan son exitosos. Esto es porque los switches capa2 no pueden hacer ruteo InterVLAN,se necesitan routers que interconecten las diferentes redes.

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

Figura 31. Ping desde cada Switch

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

Los pings tienen éxito porque se configuraron las interfaces que los comunican como los enlaces troncales estáticos entre SW-AA y SW-CC y entre SW-BB y SW-CC

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

Figura 32. Ping desde SW-AA, -BB y -CC a cada PC

```
SW-AA>
SW-AA>enable
SW-AA#pin 190.108.30.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.0, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.10.2

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

SW-AA#
```

Ctrl+F6 to exit CLI focus   Copy

```
SW-BB#ping 190.108.30.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.8, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

```
SW-CC>
SW-CC>enable
SW-CC#190.108.30.0
Trying 190.108.30.0 ...
% Connection timed out; remote host not responding
SW-CC#
```

Los ping a los pc desde los switches no fueron exitosos por que las interfaces vlan no tiene configurado ningún direccionamiento IP que las comunique.

CONCLUSIONES

- Los sistemas autónomos suelen pertenecer a ISP u otras grandes organizaciones de alta tecnología, como empresas de tecnología, universidades, agencias gubernamentales e instituciones científicas. Cada sistema autónomo que desee intercambiar información de enrutamiento debe tener un número de sistema autónomo.

- Las rutas se intercambian y el tráfico se transmite a través de Internet utilizando BGP o eBGP externos. Los sistemas autónomos también pueden usar una versión interna de BGP para enrutar a través de sus redes internas, lo que se conoce como BGP interno o iBGP para abreviar. Cabe señalar que el uso de BGP interno NO es un requisito para usar BGP externo. Los sistemas autónomos pueden elegir entre varios protocolos internos para conectar los enrutadores en su red interna.

- El VLAN Trunk Protocol (VTP) reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo de propiedad de Cisco que está disponible en la mayoría de los productos de la serie Cisco

BIBLIOGRAFÍA

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

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

UNAD (2015). Switch CISCO Security Management [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IlyVeVJCCezJ2QE5c

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

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