

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO STIVEL RUBIO MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
22 de mayo de 2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DIEGO STIVEL RUBIO MORENO

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

DIRECTOR:
MSc: GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
22 de mayo de 2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C, 22 de mayo de 2020

AGRADECIMIENTOS

Este esfuerzo lo dedico a mi familia, a mis padres y hermana por su apoyo incondicional e incansable para hoy poder llegar a un logro más, agradecimientos a los instructores de la Universidad Nacional Abierta y a Distancia – UNAD por sus esfuerzos, conocimiento y guía académica para ser de nosotros profesionales íntegros que podamos aportar positivamente al desarrollo de nuestras comunidades y país, igualmente agradecer a la universidad por la modalidad de estudios virtuales implementada ya que presentan gran oportunidad a muchas personas que poseen dificultades para acceder a educación presencial.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO	11
1. Escenario 1	11
2. Escenario 2	22
CONCLUSIONES	39
BIBLIOGRAFÍA	40

LISTA DE TABLAS

Tabla 1. Interfaces loopback para crear R1 -----	12
Tabla 2. Interfaces loopback para crear R2 -----	12
Tabla 3. Loopback para crear R3 -----	12
Tabla 4. Loopback para crear R4 -----	12
Tabla 5. Configuración direcciones IP en los terminales-----	31
Tabla 6. Configurar las direcciones IP en los switch -----	35

LISTA DE FIGURAS

Figura 1. Escenario 1 -----	11
Figura 2. Simulación de escenario 1 -----	11
Figura 3. R1 después de ser configurado adecuadamente -----	13
Figura 4. R2 después de ser configurado adecuadamente -----	14
Figura 5. R3 después de ser configurado adecuadamente -----	15
Figura 6. R4 después de ser configurado adecuadamente -----	16
Figura 7. Relación del vecino BP entre R1 y R2 -----	17
Figura 8. Salida del comando show ip route -----	17
Figura 9. Salida del comando show ip bgp -----	18
Figura 10. Salida del comando show ip bgp -----	19
Figura 11. Salida del comando show ip route -----	19
Figura 12. Salida del comando show ip bgp -----	20
Figura 13. Salida del comando show ip route -----	21
Figura 14. Escenario 2 -----	22
Figura 15. Simulación de escenario 2 -----	22
Figura 16. Salida del comando show vtp status switch SS-AA -----	24
Figura 17. Salida del comando show vtp status switch SS-BB -----	24
Figura 18. Salida del comando show vtp status switch SS-CC -----	25
Figura 19. Salida del comando show interface trunk -----	26
Figura 20. Salida del comando show interface trunk -----	26
Figura 21. Verificación vlan configuradas comando show vlan switch SW-AA ---	29
Figura 22. Verificación vlan configuradas comando show vlan switch SW-BB ---	30
Figura 23. Ping verificación pc SW-AA a SW-BB y SW-CC -----	36
Figura 24. Ping verificación pc SW-BB a SW-AA y SW-CC -----	36
Figura 25. Ping verificación pc SW-CC a SW-BB y SW-AA -----	37
Figura 26. Ping verificación switch SW-AA a SW-BB y SW-CC -----	37
Figura 27. Ping verificación switch SW-BB a SW-AA y SW-CC -----	38
Figura 28. Ping verificación switch SW-CC a SW-BB y SW-AA -----	38

GLOSARIO

NETWORKING: El término hacer contactos, o el anglicismo networking, se usa en el mundo de los negocios para hacer referencia a una actividad socio económica en la que profesionales y emprendedores se reúnen para formar relaciones empresariales, crear y desarrollar oportunidades de negocio, compartir información y buscar clientes potenciales.

LOOPBACK: La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback, en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

PING: Como programa, ping es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP. Se vale del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

CCNP: Certificación de enrutamiento y conmutación CCNP.

La certificación de enrutamiento y conmutación Cisco Certified Network Professional (CCNP) valida la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia y trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, inalámbrica y video.

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. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa OSI 3 y 4).

RESUMEN

Este trabajo tiene como objetivo desarrollar la prueba de habilidades prácticas que es una herramienta de evaluación del Diplomado de profundización de Cisco CCNP, con la cual se busca medir las habilidades y competencias que el estudiante logró alcanzar mediante el desarrollo del diplomado y cada una de sus actividades.

Esta actividad final contara con dos escenarios en la cual cada estudiante realizará cada una de las configuraciones necesarias, apoyándose en los conocimientos adquiridos en conmutación, enrutamiento, redes y electrónica para dar solución a los dos problemas planteados, el estudiante contara con el apoyo de software especializado y pondrá en ejecución lo aprendido en el transcurso del curso.

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

ABSTRACT

This work aims to develop the practical skills test, which is an evaluation tool of the Cisco CCNP Deepening Diploma, which seeks to measure the skills and competences that the student achieved through the development of the diploma and each of its activities.

This final activity will have two scenarios in which each student will perform each of the necessary configurations, relying on the knowledge acquired in switching, routing, network design and electronics to solve the two problems posed, the student will have the support specialized software and will implement what has been learned during the course.

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

INTRODUCCIÓN

Este trabajo presenta el desarrollo de la prueba de habilidades prácticas la cual es una herramienta de evaluación del Diplomado de profundización Cisco CCNP, para optar el título de ingeniero. El desarrollo de esta actividad se llevará a cabo poniendo en práctica los conocimientos tanto teóricos y prácticos adquiridos a lo largo del curso en los dos módulos trabajados, (Módulo CCNP ROUTE y Módulo CCNP SWITCH). Empleando la metodología adquirida a lo largo del diplomado la cual consistió en estudiar y entender la parte teórica para luego llevarla a la práctica mediremos nuestro conocimiento mediante la solución de dos problemas que abarcan el diseño, implementación y configuración de redes de datos, protocolos de enrutamiento, programación, normas preparándonos e instruyéndonos para que seamos capaces de asumir retos en nuestra vida laboral y profesional, la cual como futuro ingeniero de Telecomunicaciones podrá aplicar estos conocimientos en la transformación, mejoramiento y expansión de redes de nueva generación y de la tecnología que nos rodea.

El primer escenario abarca lo estudiado y aprendido en el módulo CCNP ROUTE. Consiste en la aplicación del protocolo de puerta de enlace de frontera - EIGRP, a la red conformada por cuatro routers, teniendo como objetivo el intercambio de información de encaminamiento entre sistemas autónomos. Para la c

El segundo escenario abarca lo estudiado y aprendido en el módulo CCNP SWITCH. Teniendo como objetivo la aplicación del protocolo troncal VLAN (VTP) a una red de 3 switch, cada switch se identifica por un nombre y una función diferente, en este caso el switch SW-BB se configura como servidor y los switch SW-AA y SW-CC se configuran como clientes. Cada switch se conectará con 3 terminales por medio de la creación de VLAN e interfaces utilizadas, teniendo en cuenta las direcciones IP asignadas.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1 - EBG

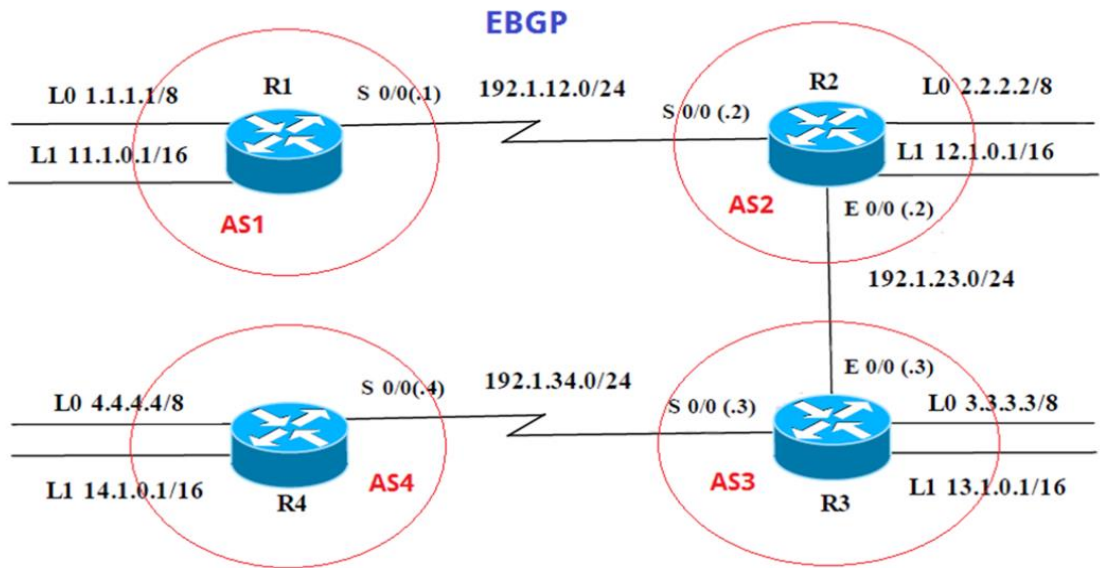
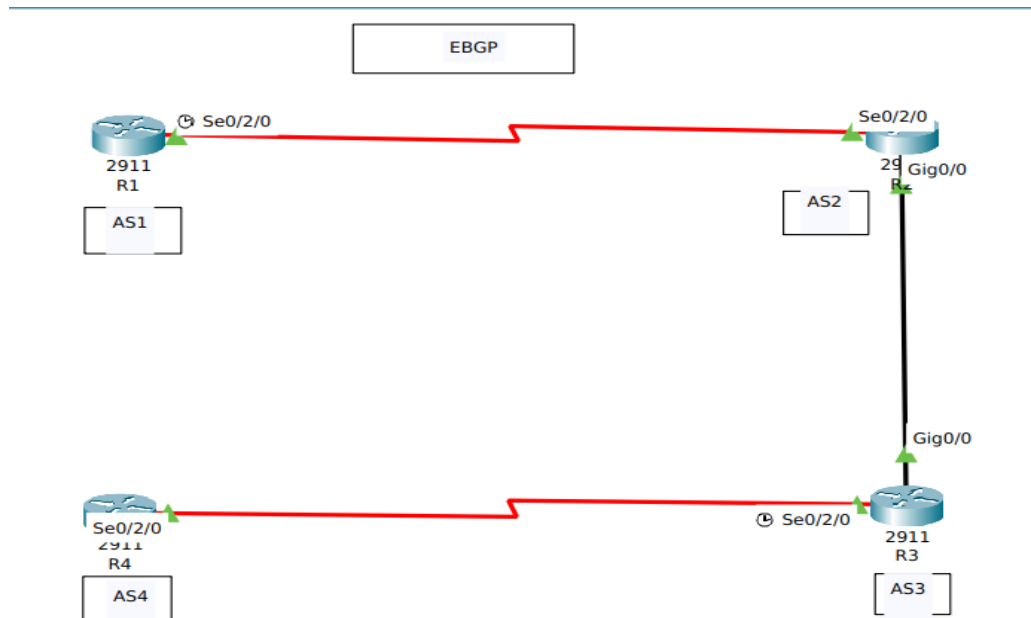


Figura 2. Simulación escenario 1



Información para Configuración de routers:

Tabla 1 Información para configuración de R1 y R2

	Interfaz	Dirección IP	Máscara
R1	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	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

Tabla 2 Información para configuración de R3 y R4

	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0
R4	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

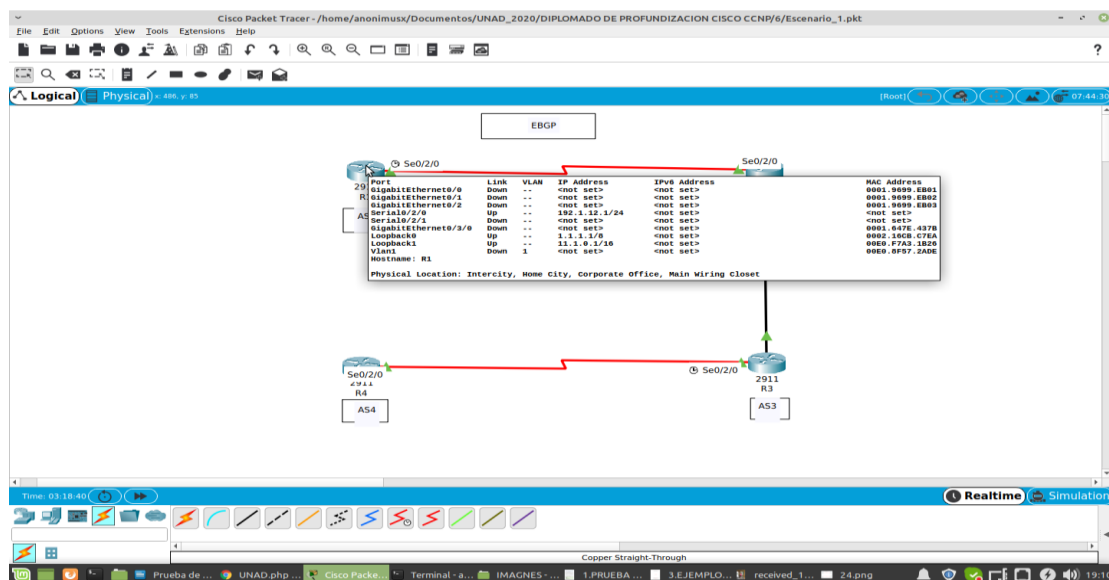
1.1 Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3 Y R4 según el diagrama. No se asigna passwords en los routers.

Configurar las interfaces con las direcciones que se muestran en la topología de red.

Se procede a configurar cada uno de los enrutadores: R1, R2, R3 y R4. Se asignan nombres y protocolos de comunican mediante EBGP que fueron asignados. Se adjunta código y pantallazos con veracidad de código.

```
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#interface loopback 1
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#interface serial0/2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#exit
R1(config)#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 3. R1 después de ser configurado adecuadamente

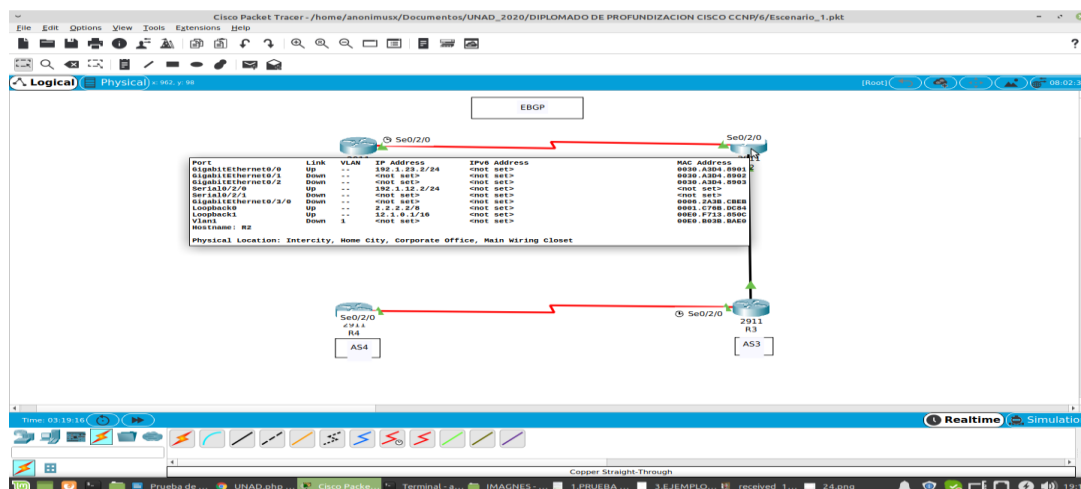


```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface loopback 0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#interface loopback 1
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#interface serial 0/2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#exit
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#exit
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

```

Figura 4. R2 después de ser configurado adecuadamente

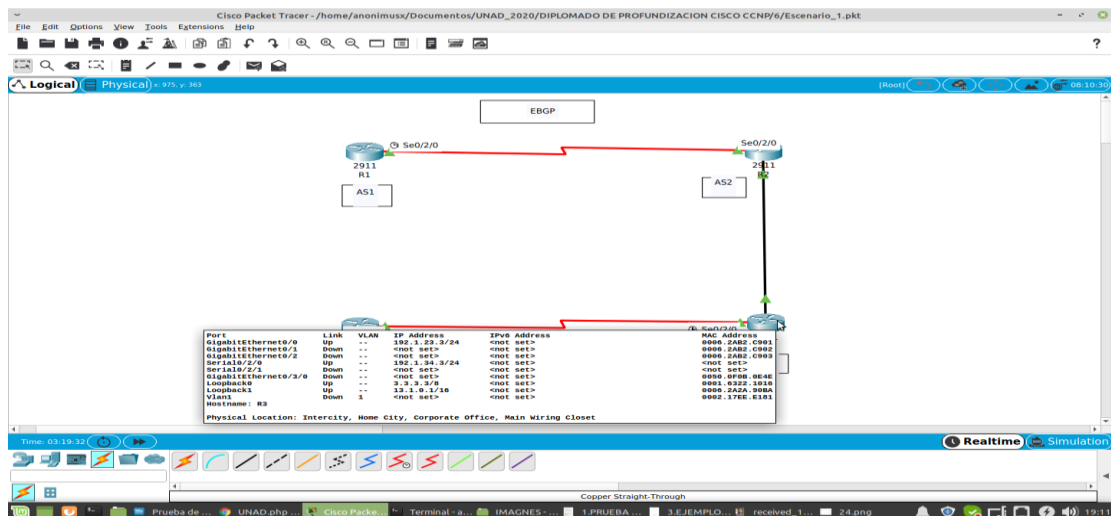


```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#interface loopback 0
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#interface loopback 1
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#interface GigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#exit
R3(config)#interface serial 0/2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#

```

Figura 5. R3 después de ser configurado adecuadamente

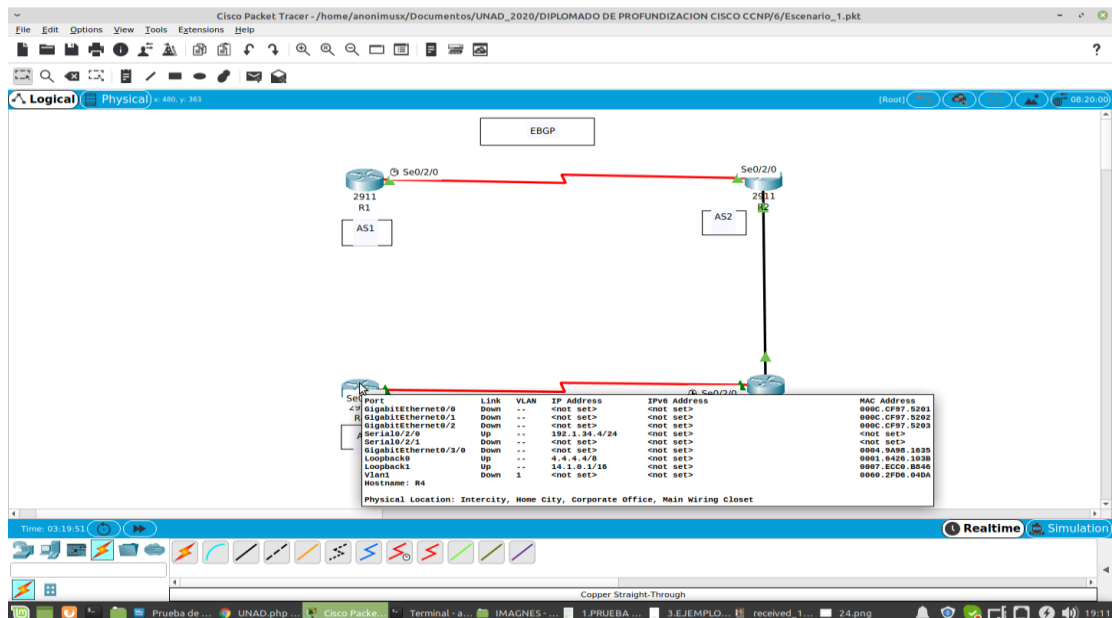


```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#interface loopback 0
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#interface loopback 1
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R4(config-if)#ip address 14.1.0.1 255.255.255.0
R4(config-if)#exit
R4(config)#interface serial 0/2/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#exit
R4(config)#

```

Figura 6. R4 después de ser configurado adecuadamente



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#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.1 mask 255.0.0.0
R1(config-router)#exit
R1(config)#exit
```

Figura 7. Relación de vecino BGP entre R1 y R2

```
R1#show ip bgp
BGP table version is 16, 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
*> 1.0.0.0/8        0.0.0.0           0      0 32768 i
*> 3.0.0.0/8        192.1.12.2        0      0      0 2 3 i
*> 4.0.0.0/8        192.1.12.2        0      0      0 2 3 4 i
*> 13.1.0.0/16     192.1.12.2        0      0      0 2 3 i
*> 14.1.0.0/16     192.1.12.2        0      0      0 2 3 4 i
-----
```

Figura 8. salida del comando show ip route

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

Gateway of last resort is not set

 1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
 C    1.0.0.0/8 is directly connected, Loopback0
 L    1.1.1.1/32 is directly connected, Loopback0
 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
 192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
 C    192.1.12.0/24 is directly connected, Serial0/2/0
 L    192.1.12.1/32 is directly connected, Serial0/2/0
```

```

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 1.1.1.0
R2(config-router)#network 11.1.0.0
R2(config-router)#exit
R2(config)#exit

```

Figura 9. salida del comando show ip bgp

```

R2>enable
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
*> 3.0.0.0/8        192.1.23.3          0         0     0 3 i
*> 4.0.0.0/8        192.1.23.3          0         0     0 3 4 i
*> 13.1.0.0/16     192.1.23.3          0         0     0 3 i
*> 14.1.0.0/16     192.1.23.3          0         0     0 3 4 i

```

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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
R3(config-router)#neighbor 192.1.12.2 remote-as 2
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 4.4.4.4 mask 255.0.0.0
R3(config-router)#network 14.1.0.1 mask 255.0.0.0
R3(config-router)#network 2.2.2.2 mask 255.0.0.0
R3(config-router)#network 12.1.0.1 mask 255.255.0.0
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#exit

```

Figura 10. salida del comando show ip bgp

```
R3#show ip bgp
BGP table version is 14, 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
*> 1.0.0.0/8        192.1.23.2         0      0      0 2 1 i
*> 3.0.0.0/8        0.0.0.0           0      0 32768 i
*                   192.1.34.4         0      0      0 4 i
*> 4.0.0.0/8        192.1.34.4         0      0      0 4 i
*>                   0.0.0.0           0      0      0 3 i
*> 13.1.0.0/16     0.0.0.0           0      0 32768 i
*                   192.1.34.4         0      0      0 4 i
*> 14.1.0.0/16     192.1.34.4         0      0      0 4 i
*>                   0.0.0.0           0      0      0 3 i
```

Figura 11. salida del comando 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    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
C    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
C    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
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/2/0
L    192.1.34.3/32 is directly connected, Serial0/2/0
```

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>enable
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
R4(config-router)#neighbor 192.1.23.3 remote-as 3
R4(config-router)#neighbor 192.1.23.2 remote-as 2
R4(config-router)#neighbor 192.1.12.2 remote-as 2
R4(config-router)#neighbor 192.1.12.1 remote-as 1
R4(config-router)#network 3.3.3.3 mask 255.0.0.0
R4(config-router)#network 13.1.0.1 mask 255.255.0.0
R4(config-router)#network 12.1.0.1 mask 255.255.0.0
R4(config-router)#network 2.2.2.2 mask 255.0.0.0
R4(config-router)#network 11.1.0.1 mask 255.255.0.0
R4(config-router)#network 4.4.4.4 mask 255.0.0.0
R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#exit
R4(config)#exit
R4#
%SYS-5-CONFIG_I: Configured from console by console

```

Figura 12. salida del comando show ip bgp

```

R4>enable
R4#show ip 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 - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 1.0.0.0/8        192.1.34.3          0      0      0 3 2 1 i
*> 3.0.0.0/8        192.1.34.3          0      0      0 3 i
*>                  0.0.0.0             0      0      0 4 i
*> 4.0.0.0/8        0.0.0.0             0      0 32768 i
*                   192.1.34.3          0      0      0 3 i
*> 13.1.0.0/16      192.1.34.3          0      0      0 3 i
*>                  0.0.0.0             0      0      0 4 i
*> 14.1.0.0/16      0.0.0.0             0      0 32768 i
*                   192.1.34.3          0      0      0 3 i

```

Figura 13. salida del comando show ip route

```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
     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
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/2/0
L    192.1.34.4/32 is directly connected, Serial0/2/0
```

2. ESCENARIO 2

Figura 14. Escenario 2

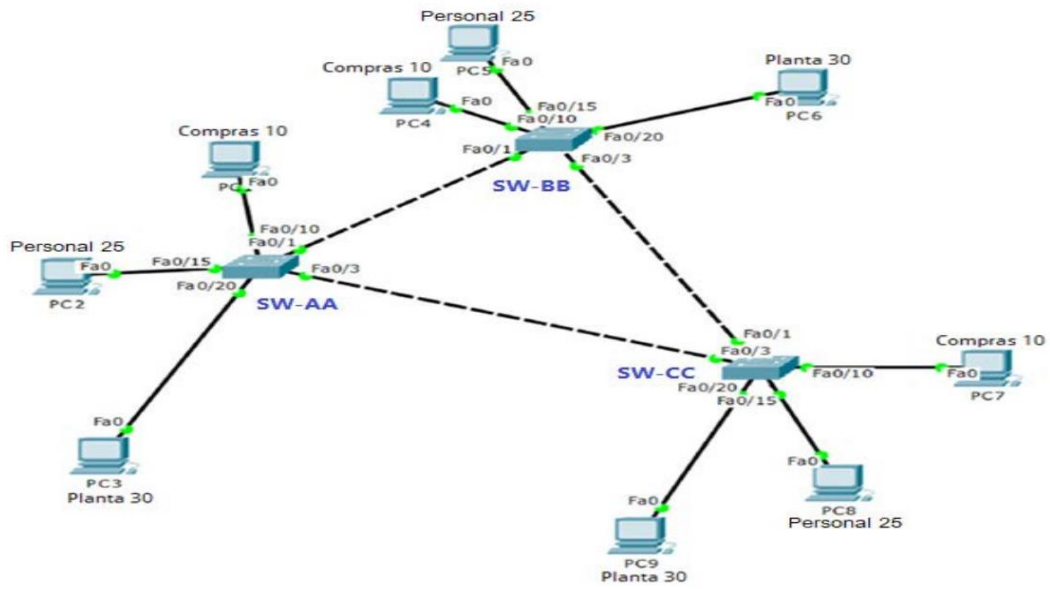
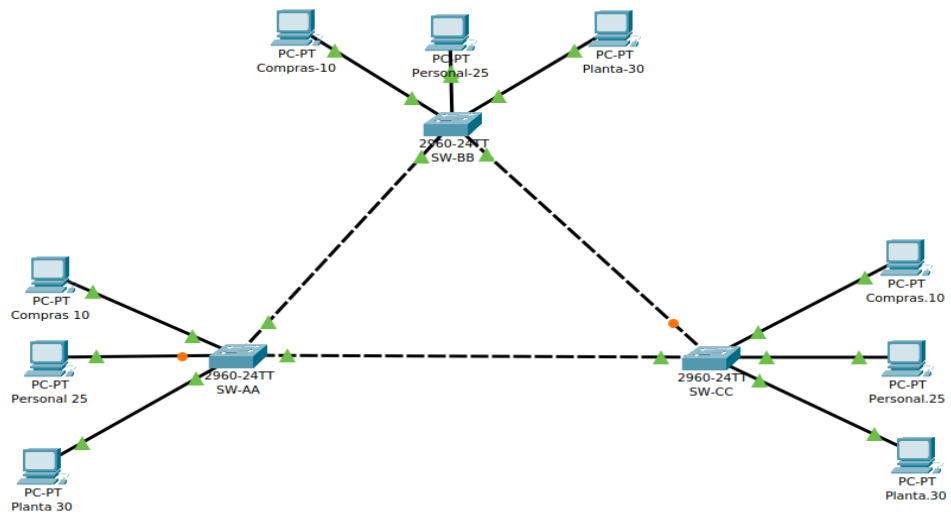


Figura 15. Topologia escenario 2 – cisco packet tracer



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.

SS-AA

```
Switch>ENABLE
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SS-AA
SS-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SS-AA(config)#vtp version 2
SS-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SS-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SS-AA(config)#
```

SS-BB

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SS-BB
SS-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SS-BB(config)#vtp version 2
SS-BB(config)#vtp mode server
Device mode already VTP SERVER.
SS-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SS-BB(config)#
```

SS-CC

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SS-CC
SS-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SS-CC(config)#vtp version 2
SS-CC(config)#vtp mode client
```

Setting device to VTP CLIENT mode.
SS-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SS-CC(config)#

3. Verifique las configuraciones mediante el comando show vtp status.

Figura 16. salida del comando show vtp status – switch SS-AA

```
SS-AA#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x94 0x7D 0x70 0xAD 0xCC 0x47 0xA7 0x66
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:21
SS-AA#
```

Figura 17. salida del comando show vtp status – switch SS-BB

```
SS-BB#
SS-BB#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x40 0xD3 0x8E 0x51 0x3D 0x8E 0xBA 0x7D
Configuration last modified by 0.0.0.0 at 3-1-93 00:10:13
Local updater ID is 0.0.0.0 (no valid interface found)
SS-BB#
```


Figura 18. salida del comando show vtp status – switch SS-CC

```
SS-CC#
SS-CC#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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                 : Enabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xF5 0x34 0x72 0x2F 0x37 0xEC 0x45 0x7D
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:15
SS-CC#
```

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.

```
SS-AA#
```

```
SS-AA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SS-AA(config)#interface FastEthernet 0/1
```

```
SS-AA(config-if)#switchport mode dynamic desirable
```

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

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

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

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

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

Figura 19. salida del comando show interface trunk

```
SS-AA#
SS-AA#show interface 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

SS-AA#
```

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

SS-AA#

SS-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-AA(config)#interface FastEthernet 0/3

SS-AA(config-if)#switchport mode trunk

SS-AA(config-if)#

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

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

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

Figura 20. salida del comando show interface trunk

```
SS-AA#
SS-AA#show interface 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

SS-AA#
```

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

SS-BB#

SS-BB#enable

SS-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-BB(config)#interface FastEthernet 0/3

SS-BB(config-if)#switchport mode trunk

SS-BB(config-if)#

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

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

SS-CC#

SS-CC#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-CC(config)#interface FastEthernet 0/1

SS-CC(config-if)#switchport mode trunk

SS-CC(config-if)#exit

SS-CC(config)#end

SS-CC#

%SYS-5-CONFIG_I: Configured from console by console

C. Agregar VLANs y asignar puertos.

SS-AA

SS-AA#enable

SS-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-AA(config)#vlan 10

VTP VLAN configuration not allowed when device is in CLIENT mode.

SS-AA(config)#

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

SS-BB#

SS-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-BB(config)#vlan 10

SS-BB(config-vlan)#name Compras

SS-BB(config-vlan)#vlan 25

SS-BB(config-vlan)#name Personal

SS-BB(config-vlan)#vlan 30

SS-BB(config-vlan)#name Planta

SS-BB(config-vlan)#vlan 99

SS-BB(config-vlan)#name Admon

SS-BB(config-vlan)#exit

SS-BB(config)#

10. Verifique que las VLANs han sido agregadas correctamente.

En SW-AA: No se puede crear la vlan 10 ya que en el switch 1 tiene un vtp en modo cliente, lo que no permite crear la Vlan.

Figura 21. verificación vlan configuradas - comando show vlan switch SW-AA

```

SS-AA#
SS-AA#show vlan

VLAN Name                Status    Ports
-----
1    default                active   Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                   Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                   Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                   Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   Compras                active
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

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet     100001   1500  -     -     -     -     -     0     0
10   enet     100010   1500  -     -     -     -     -     0     0
25   enet     100025   1500  -     -     -     -     -     0     0
30   enet     100030   1500  -     -     -     -     -     0     0
99   enet     100099   1500  -     -     -     -     -     0     0
1002 fddi     101002   1500  -     -     -     -     -     0     0
1003 tr      101003   1500  -     -     -     -     -     0     0
1004 fdnet  101004   1500  -     -     -     ieee  -     0     0
1005 trnet  101005   1500  -     -     -     ibm   -     0     0

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
SS-AA#

```

Figura 22. verificación vlan configuradas - comando show vlan switch SW-BB

```

SS-BB#
SS-BB#show vlan

VLAN Name                Status    Ports
-----
1    default                active   Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                         Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                         Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                         Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                         Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                         Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   Compras                active
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

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001   1500  -     -     -     -   -         0      0
10   enet  100010   1500  -     -     -     -   -         0      0
25   enet  100025   1500  -     -     -     -   -         0      0
30   enet  100030   1500  -     -     -     -   -         0      0
99   enet  100099   1500  -     -     -     -   -         0      0
1002 fddi  101002   1500  -     -     -     -   -         0      0
1003 tr   101003   1500  -     -     -     -   -         0      0
1004 fdnet 101004   1500  -     -     -     -   ieee      0      0
1005 trnet 101005   1500  -     -     -     -   ibm       0      0

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----
SS-BB#

```

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

Tabla 3. Información para configuración vlan y direcciones ip

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

SS-AA#

SS-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-AA(config)#interface vlan 10

SS-AA(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

SS-AA(config-if)#ip address 190.108.10.1 255.255.255.0

SS-AA(config-if)#exit

SS-AA(config)#interface vlan 25

SS-AA(config-if)#

%LINK-5-CHANGED: Interface Vlan25, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up

SS-AA(config-if)#ip address 190.108.20.1 255.255.255.0

SS-AA(config-if)#exit

SS-AA(config)#interface vlan 30

SS-AA(config-if)#

%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

SS-AA(config-if)#ip address 190.108.30.1 255.255.255.0

SS-AA(config-if)#exit

SS-BB#

SS-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-BB(config)#interface vlan 10

SS-BB(config-if)#

```
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SS-BB(config-if)#ip address 190.108.10.2 255.255.255.0
SS-BB(config-if)#exit
SS-BB(config)#interface vlan 25
SS-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan25, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up
SS-BB(config-if)#ip address 190.108.20.2 255.255.255.0
SS-BB(config-if)#exit
SS-BB(config)#interface vlan 30
SS-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
SS-BB(config-if)#ip address 190.108.30.2 255.255.255.0
SS-BB(config-if)#exit
```

SS-CC>

```
SS-CC>enable
SS-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SS-CC(config)#interface vlan 10
SS-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SS-CC(config-if)#ip address 190.108.10.3 255.255.255.0
SS-CC(config-if)#exit
SS-CC(config)#interface vlan 25
SS-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan25, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up
SS-CC(config-if)#ip address 190.108.20.3 255.255.255.0
SS-CC(config-if)#exit
SS-CC(config)#interface vlan 30
SS-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
SS-CC(config-if)#ip address 190.108.30.3 255.255.255.0
SS-CC(config-if)#exit
SS-CC(config)#
12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y
asígnelo a la VLAN 10.
```


SS-AA#

SS-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-AA(config)#interface FastEthernet 0/10

SS-AA(config-if)#switchport mode access

SS-AA(config-if)#switchport access vlan 10

SS-AA(config-if)#exit

SS-AA(config)#

SS-BB#

SS-BB#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-BB(config)#interface FastEthernet 0/10

SS-BB(config-if)#switchport mode access

SS-BB(config-if)#switchport access vlan 10

SS-BB(config-if)#exit

SS-BB(config)#

SS-CC#

SS-CC#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-CC(config)#interface FastEthernet 0/10

SS-CC(config-if)#switchport mode access

SS-CC(config-if)#switchport access vlan 10

SS-CC(config-if)#exit

SS-CC(config)#exit

SS-CC#

%SYS-5-CONFIG_I: Configured from console by console

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.

SS-AA#

SS-AA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SS-AA(config)#interface FastEthernet 0/15

SS-AA(config-if)#switchport mode access

SS-AA(config-if)#switchport access vlan 25

SS-AA(config-if)#exit

SS-AA(config)#interface FastEthernet 0/20

SS-AA(config-if)#switchport mode access

```
SS-AA(config-if)#switchport access vlan 30
SS-AA(config-if)#
```

SS-BB#

```
SS-BB#enable
SS-BB#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
SS-BB(config)#interface FastEthernet 0/15
SS-BB(config-if)#switchport mode access
SS-BB(config-if)#switchport access vlan 25
SS-BB(config-if)#no shutdown
SS-BB(config-if)#exit
SS-BB(config)#interface FastEthernet 0/20
SS-BB(config-if)#switchport mode access
SS-BB(config-if)#switchport access vlan 30
SS-BB(config-if)#exit
```

SS-CC#

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

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.

Tabla 4 Información para configuración switch virtual interface

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

SS-AA#

```
SS-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SS-AA(config)#interface vlan 99
SS-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SS-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SS-AA(config-if)#exit
SS-AA(config)#
```

SS-BB#

```
SS-BB#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
SS-BB(config)#interface vlan 99
SS-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SS-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SS-BB(config-if)#exit
```

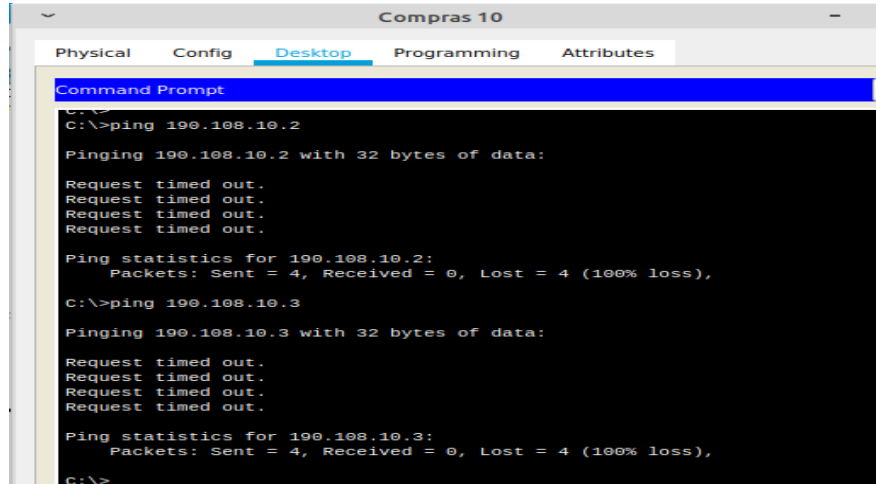
SS-CC>

```
SS-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SS-CC(config)#interface vlan 99
SS-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SS-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SS-CC(config-if)#exit
SS-CC(config)#
```

E. Verificar la conectividad Extremo a Extremo

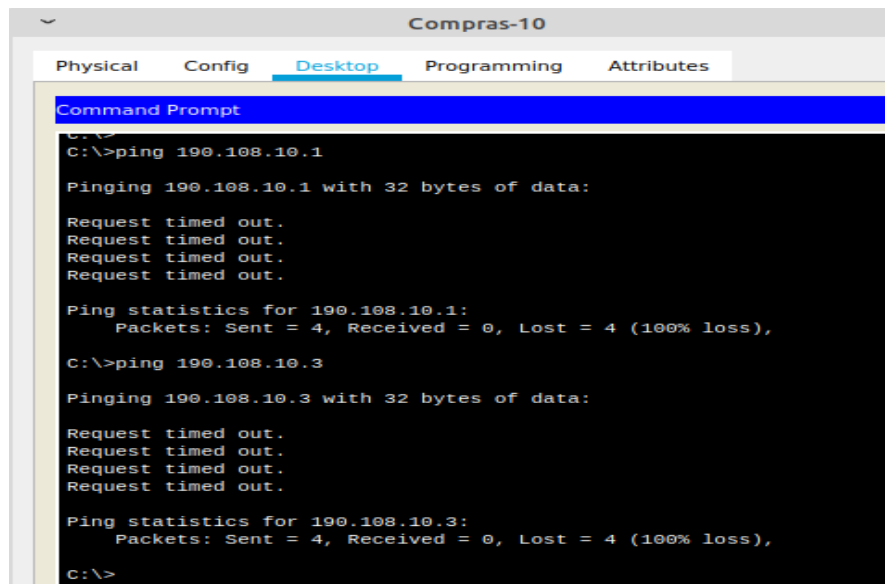
15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Figura 23. ping verification pc SW-AA a pc SW-BB y pc SW-CC



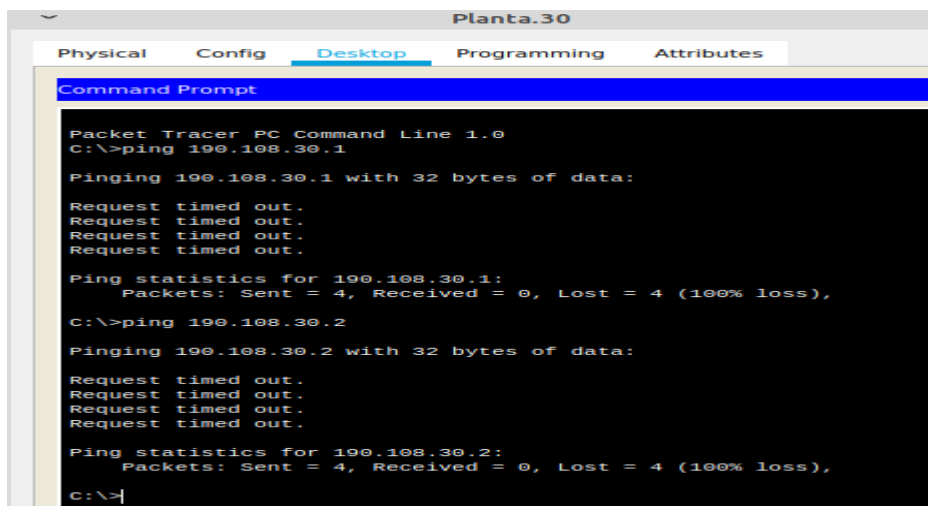
```
Compras 10
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.10.2
Pinging 190.108.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% 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:\>
```

Figura 24. ping verificación pc SW-BB a pc SW-AA y pc SW-CC



```
Compras-10
Physical Config Desktop Programming Attributes
Command Prompt
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:\>
```

Figura 25. ping verificación pc SW-CC a pc SW-BB y pc SW-AA



```
Planta.30
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.30.1
Pinging 190.108.30.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.30.2
Pinging 190.108.30.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>|
```

SOLUCIÓN: El ping realizado entre cada una de las PC es correcto solo si hacen parte de la misma Vlan, de lo contrario el ping es incorrecto como en este caso podemos observar.

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

Al ejecutar un ping de cada ping a los demás, el resultado es exitoso, debido a que se reconoce el direccionamiento de la Vlan 99, entonces, al realizar un ping desde un switch a la Vlan 99 de otro switch, el pingo es exitoso. A continuación se evidencia:

Figura 26. ping verificación sw-aa a sw-bb y sw-cc

```
SS-AA#
SS-AA#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 = 0/2/8 ms
SS-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 = 0/0/0 ms
SS-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 = 0/0/1 ms
SS-AA#|
```

Figura 27. ping verificación SW-BB a SW-AA y SW-CC

```
SS-BB>enable
SS-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 = 0/0/0 ms

SS-BB#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 = 2/3/7 ms

SS-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

SS-BB#
```

Figura 28. ping verificación SW-CC a SW-AA y SW-B

```
SS-CC#
SS-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 = 0/0/0 ms

SS-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 = 0/3/18 ms

SS-CC#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/10 ms

SS-CC#
```

CONCLUSIONES

Por medio del desarrollo de los laboratorios planteados comprendimos como se implementa y configura una red que este soportada por VLAN con el uso de los protocolos VTP y STP, donde se pueda diseñar las plantillas de configuración para su uso en múltiples dispositivos, configurar troncales y vlan usando el protocolo VTP, los EtherChannel Link en red de switches interconectados, entro otros usos.

Reforzamos diversos conocimientos adquiridos a través de la realización de las guías y laboratorios desarrollados durante el transcurso del curso Diplomado de profundización cisco CCNP y la solución de las lecciones evacuativas en el entorno de cisco (Netacad).

Con el desarrollo adecuada de la topología establecida en el escenario 1, pudimos obtener información detallada de las direcciones ip, interfaz y máscara de red, en esta topología de red implementamos la configuración de vecinos BGP, anuncio de direcciones y identificación de router (ID) , verificamos la correcta configuración por medio de show ip route.

Con el desarrollo adecuada de la topología establecida en el escenario 2, identificamos la topología de red y configuramos VTP para actualización de VLAN, verificamos por medio de show vtp estatus. Configuramos DT para los switches 1 y 2, y observamos cómo funcionan los enlaces troncales, adicionamos VLAN y asignación de puertos, por medio de los pc realizamos pruebas de diagnóstico de comunicación de red (ping) entre la red, los computadores de la red se configuraron con ip estática, de acuerdo a criterios establecidos.

REFERENCIAS BIBLIOGRÁFICAS

Froom, R., Frahim, E. (2015). CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1InWR0hoMxgBNv1CJ>

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!AmlJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>