DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RODRIGO SANTANA VILLEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA TELECOMUNICACIONES
IBAGUÉ
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RODRIGO SANTANA VILLEGAS

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA TELECOMUNICACIONES
IBAGUÉ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del jurado

_____
Firma del jurado

IBAGUÉ, 17 de mayo de 2020

AGRADECIMIENTOS

Agradezco primero que todo a la vida por darme la oportunidad de estar aquí, a mis padres Ruby Villegas y German Santana por ser ese apoyo incondicional, y a mi esposa Melissa y el hijo que viene en camino por encender de nuevo este motor.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

SWITCH: es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos, puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto según su configuración, puede funcionar en la capa 2 o capa 3 del modelo OSI.

PROTOCOLOS DE RED: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

ROUTER: enrutador, o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

VLAN: 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.

LOOPBACK: es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento.

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.

OSPF: Open Shortest Path First (OSPF), es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF mantiene actualizada la capacidad de encaminamiento entre

los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos.

EIGRP: Es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP.

BGP:(Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

VTP: VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

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.

RESUMEN

El diplomado Cisco Certified Network Professional (CCNP) nos equipa con los conocimientos y las habilidades necesarios para planificar, implementar, asegurar, mantener y solucionar problemas de redes empresariales convergentes.

En este curso se obtienen el conocimiento para monitorear y mantener servicios de enrutamiento en una red empresarial, planear, configurar, y verificar la implementación de una LAN y WAN empresarial compleja con soluciones de enrutamiento usando un rango de protocolos de enrutamiento ambientes IPv4 e IPv6 como EIGRP, OSPF y BGP.

Del mismo modo, se planea, configura, y verificar la implementación de una red compleja conmutada. Cubriendo soluciones de conmutación segura junto con la integración de VLANs, VoIP, LAN inalámbrica y vídeo dentro del campus.

Finalmente, las habilidades adquiridas por medio de este curso son planeamiento y ejecución del mantenimiento de una red regular, así como el soporte y solución de problemas usando procesos basados en tecnologías y mejores prácticas. Estos bajo enfoques sistemáticos y reconocidos por el mercado de telecomunicaciones.

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

ABSTRACT

The Cisco Certified Network Professional (CCNP) Diploma equips us with the knowledge and skills required to implement, ensure, maintain, and resolve converged business network problems.

In this course you will gain the knowledge to monitor and maintain routing services in an enterprise network, plan, configure, and verify the implementation of a complex enterprise LAN and WAN with routing solutions using a range of routing protocols in IPv4 and IPv6 environments such as EIGRP, OSPF and BGP.

Similarly, the implementation of a complex switched network is planned, configured, and verified. Covering secure switching solutions along with the integration of VLAN, VoIP, wireless LAN and video within the campus.

Finally, the skills acquired through this course are planning and executing the maintenance of a regular network, as well as the support and solution of problems using processes processed in technologies and best practices. These low systematic approaches and recognized by the telecommunications market.

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

INTRODUCCIÓN

La siguiente actividad denominada Prueba de habilidades prácticas, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial al desarrollar el paso a paso es poner a prueba los niveles de comprensión y resolución de problemas relacionados con diversos aspectos de Networking que se vieron en el transcurso de los diferentes módulos del diplomado.

A través de este diplomado y el desarrollo de cada una de sus actividades se pretende alcanzan objetivos como, el desarrollo del pensamiento crítico y habilidades para resolver problemas mediante equipamientos reales y simulados (packet Tracer o GNS3), el diseño de redes LAN simples, realizando configuraciones básicas de switches y routers con implementación de esquemas de asignación de IP, resolución de problemas e inconvenientes comunes de routing de VLAN en redes ipv4 e ipv6, trabajar con routers y switches mediante los protocolos OSPF, EIGRP, BGP y STP en redes ipv4 e ipv6, configurar las tecnologías de WAN y los servicios de red requeridos por las aplicaciones convergentes en redes complejas, entre otros con el fin de preparándonos para aplicar a las pruebas de certificación CISCO, ampliando nuestro portafolio de conocimientos y creando profesionales más competitivos para el mercado laboral en el área de telecomunicaciones.

Para esta actividad, se solicita realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros comandos de visualización.

En el escenario uno (1), tenemos el caso de una red conformada por cuatro (4) routers conectados entre sí físicamente por puertos seriales y ethernet respectivamente. Cada router debe ser configurado con dos interfaces lógicas internas lookback (las cuales no se asigna a un puerto físico debido a que son interfaces de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento) y su respectivo direccionamiento IPv4 el cual es asignado por el ejercicio. Después es necesario configurar relación de vecinos BGP (Border Gateway Protocol, protocolo de puerta de enlace exterior que

permite que los Sistemas Autónomos intercambien información de ruteo entre sí), donde se anuncia las direcciones lookback de los routers para logra la conectividad extremo a extremo, y entre dispositivos vecinos. Finalizado cada proceso se solicita realizar pruebas de conectividad y visualización de configuración de cada dispositivo que interviene en la red, a través de los comandos que se encuentran al interior de la Prueba de habilidades prácticas y adquiridos durante el transcurso del diplomado.

En el escenario dos (2), tenemos el caso de una red conformada por tres (3) switches, en donde se solicita configurar en cada una de ellos VTP (VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco), con el fin de centralizar y simplificar la administración en un dominio de VLANs, facilitando crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos, esta configuración nos pide la Prueba de habilidades prácticas tener un servidor y dos clientes, configurados bajo un mismo dominio.

Es necesario configurar enlaces troncales DTP (Dynamic Trunking Protocol es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking) bajo el modo dynamic desirable en uno de los lados y creación de troncales permanentes.

A través de parámetros de configuración que se encuentran en la Prueba de habilidades prácticas, se debe configurar las VLANS (redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única) asociando los puertos y conectando los equipos usuarios a las interfaces asignadas respectivamente.

Por ultimo en cada uno de los Switches se debe asignar una dirección IP al SVI (Switch Virtual Interface) para una VLAN determinada de acuerdo con la tabla especificada en el documento la cual nos permitirá tener acceso a los parámetros de configuración de los dispositivos.

Se debe realizar pruebas de conectividad y configuración a través de los comandos solicitados en el trabajo y adquiridos durante el transcurso del diplomado.

Se llevara a cabo el desarrollo de la Prueba de Habilidades Prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización CCNP, se sustenta el desarrollo de cada escenario con los respectivos procesos documentando paso a paso la solución correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción

detallada de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de los comandos requeridos para cada caso brindados por el documento o adquiridos en el transcurso del diplomado, empleando la herramienta de simulación como packet tracert y GNS3.

DESARROLLO

Escenario 1

Figura 1 Ejemplo de escenario 1

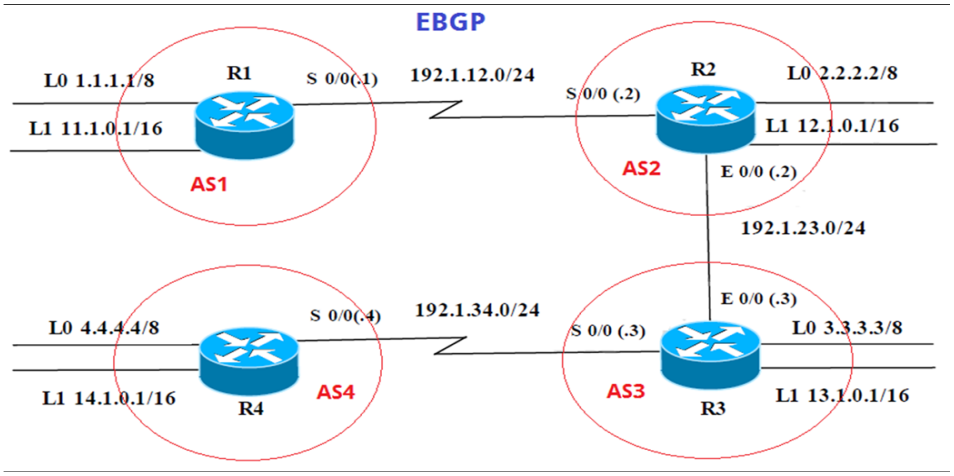


Tabla 1 Información para la configuración de los routers

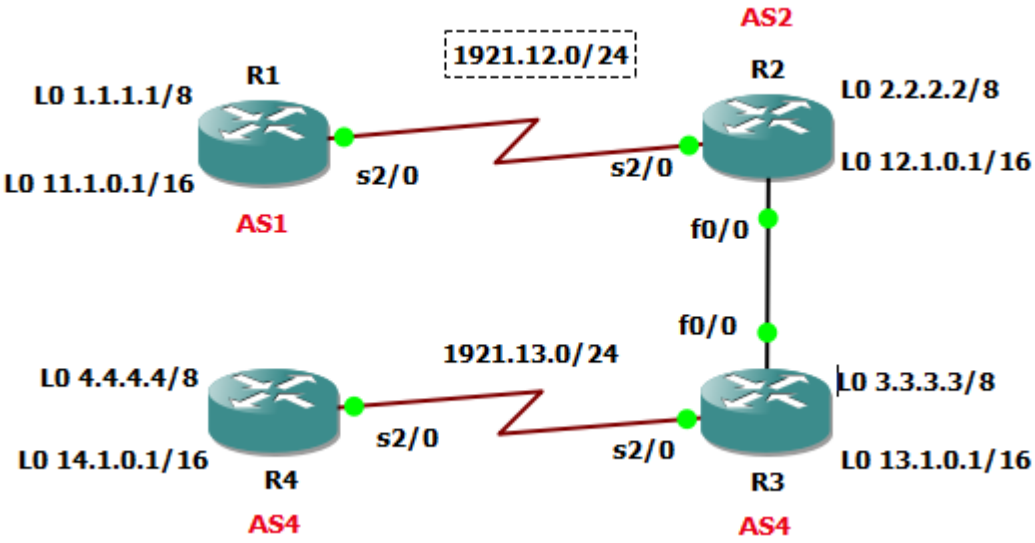
	Interfaz	Direccion IP	Mascara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0

	Interfaz	Direccion IP	Mascara
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

	Interfaz	Direccion IP	Mascara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	S 0/0	192.1.23.3	255.255.255.0
	E 0/0	192.1.34.3	255.255.255.0

	Interfaz	Direccion IP	Mascara
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

Figura 2 Topología de escenario 1



Se realiza la configuración en los routers según la tabla 1

R1#configure terminal
R1(config)#interface s 2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Loopback 0
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)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit

Figura 3 Show ip interface brief

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES unset  administratively down down

FastEthernet0/1            unassigned      YES unset  administratively down down

FastEthernet1/0            unassigned      YES unset  administratively down down

Serial2/0                  192.1.12.1      YES manual up                    down

Serial2/1                  unassigned      YES unset  administratively down down

Serial2/2                  unassigned      YES unset  administratively down down

Serial2/3                  unassigned      YES unset  administratively down down

Loopback0                  1.1.1.1         YES manual up                    up

Loopback1                  11.1.0.1        YES manual up                    up
```

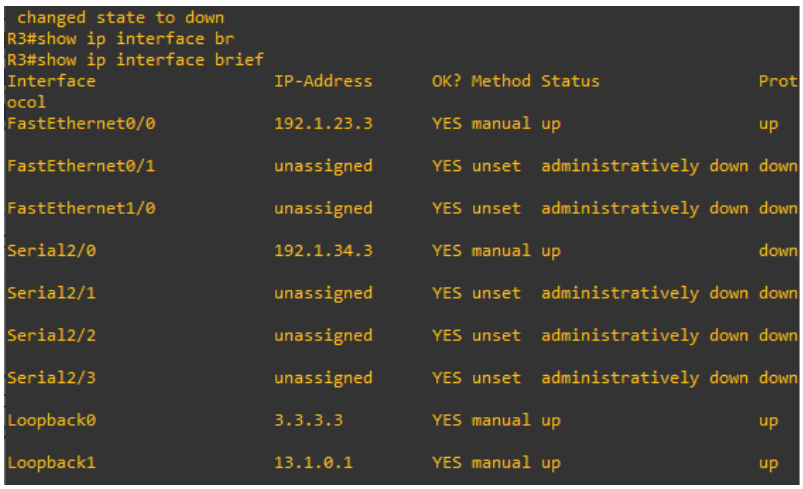
R2# configure terminal
R2(config)#interface lo 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#inter lo 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#inter s 2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit R2(config)#inter f 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown

Figura 4 Show ip interface brief

```
R2#show ip int
R2#show ip interface br
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            192.1.23.2      YES manual up                    up

FastEthernet0/1            unassigned      YES unset  administratively down down

FastEthernet1/0            unassigned      YES unset  administratively down down

Serial2/0                  192.1.12.2      YES manual up                    up

Serial2/1                  unassigned      YES unset  administratively down down

Serial2/2                  unassigned      YES unset  administratively down down

Serial2/3                  unassigned      YES unset  administratively down down

Loopback0                  2.2.2.2         YES manual up                    up

Loopback1                  12.1.0.1        YES manual up                    up
```

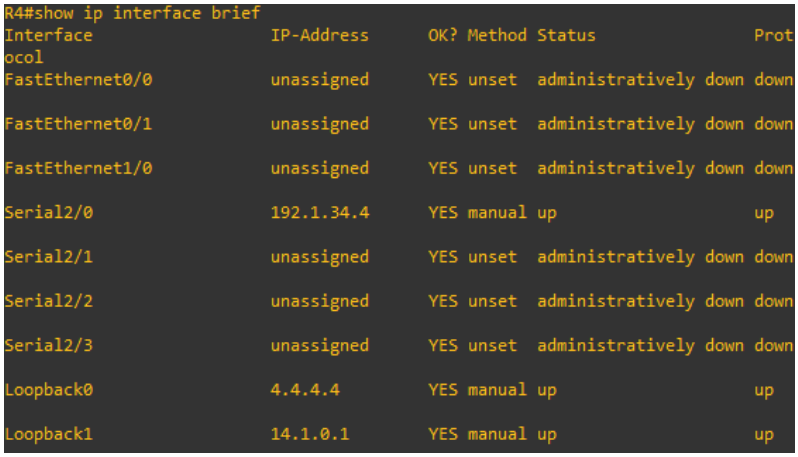
R3#configure t
R3(config)#inter Lo 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)# inter Lo1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#inter f 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#inter s 2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown

Figura 5 Show ip interface brief



R4#configure t
R4(config)#inter lo 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#int Lo1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#inter s 2/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown

Figura 6 Show ip interface brief



```
R4#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES unset  administratively down down

FastEthernet0/1            unassigned      YES unset  administratively down down

FastEthernet1/0            unassigned      YES unset  administratively down down

Serial2/0                  192.1.34.4      YES manual up                    up

Serial2/1                  unassigned      YES unset  administratively down down

Serial2/2                  unassigned      YES unset  administratively down down

Serial2/3                  unassigned      YES unset  administratively down down

Loopback0                  4.4.4.4         YES manual up                    up

Loopback1                  14.1.0.1        YES manual up                    up
```

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

   Se configure el vecino BGP para R1 y R2: R1:

   R1(config)#router bgp 100
   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 200

   R2(config)#router bgp 200
   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 100
   R2(config-router)#neighbor 192.1.23.3 remote-as 300

   comprueba el funcionamiento de la relación BGP establecida:

Figura 7 Ping de R1 a R2

```
R1#ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/26/36 ms
R1#
```

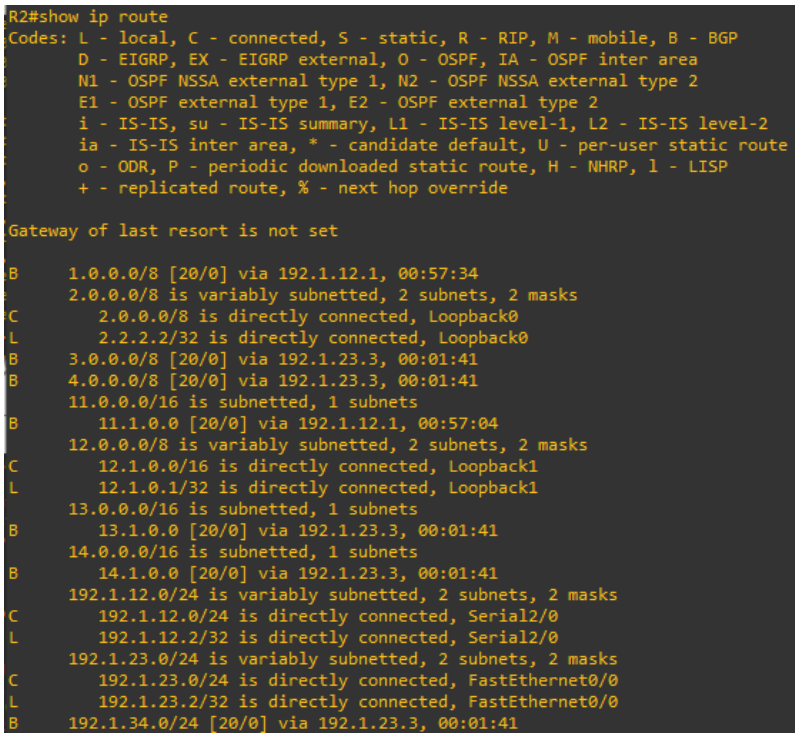
Figura 8 Ping de R2 a R1

```
R2#ping 192.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/23/44 ms
R2#
```

Figura 9 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 ro
       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, 00:54:06
B     3.0.0.0/8 [20/0] via 192.1.12.2, 00:00:36
B     4.0.0.0/8 [20/0] via 192.1.12.2, 00:00:36
      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, 00:53:37
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.12.2, 00:00:36
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.12.2, 00:00:36
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.1/32 is directly connected, Serial2/0
B     192.1.23.0/24 [20/0] via 192.1.12.2, 00:52:43
B     192.1.34.0/24 [20/0] via 192.1.12.2, 00:00:36
```

Figura 10 Show ip route R2



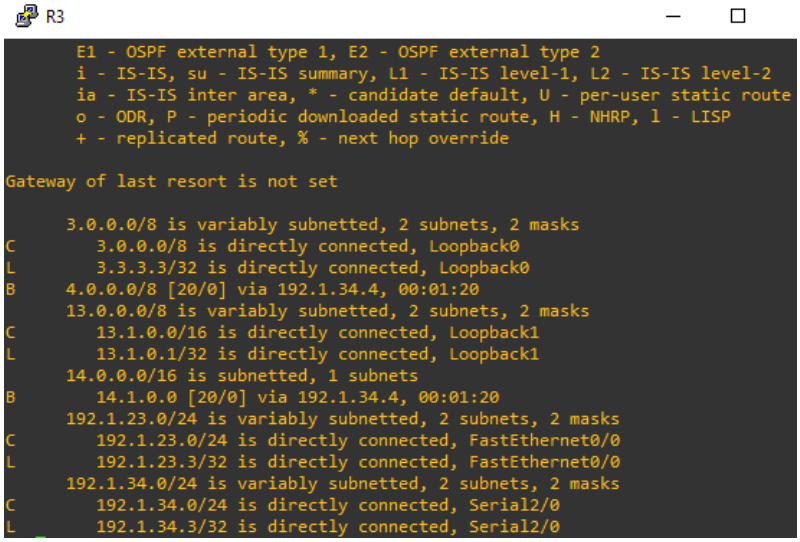
```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS 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 192.1.12.1, 00:57:34
      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, 00:01:41
B     4.0.0.0/8 [20/0] via 192.1.23.3, 00:01:41
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:57:04
      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, 00:01:41
      14.0.0.0/16 is subnetted, 1 subnets
B        14.1.0.0 [20/0] via 192.1.23.3, 00:01:41
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.2/32 is directly connected, Serial2/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, FastEthernet0/0
L        192.1.23.2/32 is directly connected, FastEthernet0/0
B     192.1.34.0/24 [20/0] via 192.1.23.3, 00:01:41
```

1. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

   Se configura:

   R3(config)#router bgp 300
   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 400
   R3(config-router)#neighbor 192.1.23.2 remote-as 200

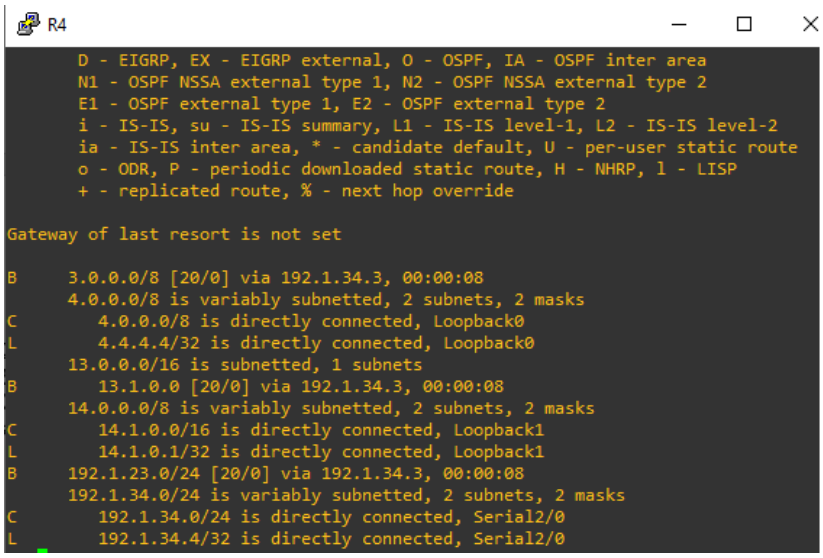
Figura 11 Show ip route R3



2. 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. Creerutas 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 delcomando show ip route.

   R4(config)#router bgp 400
   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 300

Figura 12 Show ip route R4



Se ejecuta el comando show ip bgp en los 4

Figura 13 Show ip bgp R1

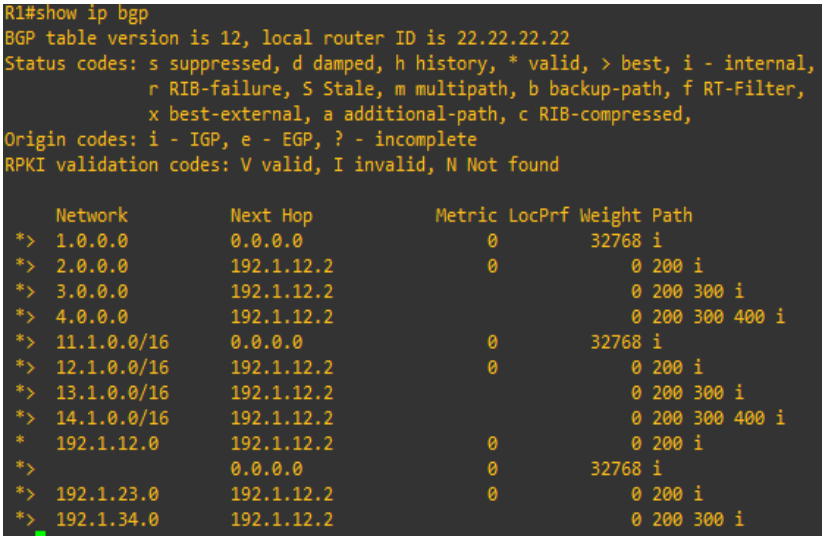


Figura 14 Show ip bgp R2

```
R2#show ip bgp
BGP table version is 13, 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, 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          192.1.12.1               0             0 100 i
 *>  2.0.0.0          0.0.0.0                  0         32768 i
 *>  3.0.0.0          192.1.23.3               0             0 300 i
 *>  4.0.0.0          192.1.23.3                             0 300 400 i
 *>  11.1.0.0/16      192.1.12.1               0             0 100 i
 *>  12.1.0.0/16      0.0.0.0                  0         32768 i
 *>  13.1.0.0/16      192.1.23.3               0             0 300 i
 *>  14.1.0.0/16      192.1.23.3                             0 300 400 i
 *>  192.1.12.0       0.0.0.0                  0         32768 i
 *                    192.1.12.1               0             0 100 i
 *   192.1.23.0       192.1.23.3               0             0 300 i
 *>                   0.0.0.0                  0         32768 i
 *>  192.1.34.0       192.1.23.3               0             0 300 i
```

Figura 15 Show ip bgp R3

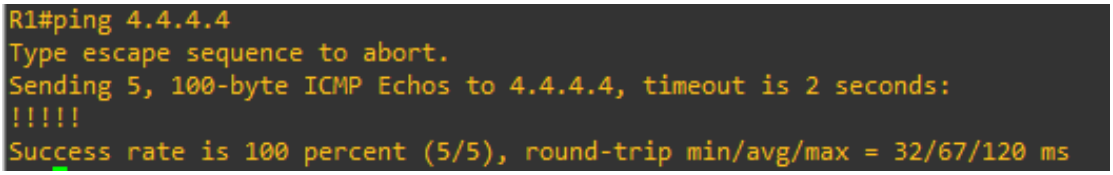
```
R3#show ip bgp
BGP table version is 12, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
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          192.1.23.2                             0 200 100 i
 *>  2.0.0.0          192.1.23.2               0             0 200 i
 *>  3.0.0.0          0.0.0.0                  0         32768 i
 *>  4.0.0.0          192.1.34.4               0             0 400 i
 *>  11.1.0.0/16      192.1.23.2                             0 200 100 i
 *>  12.1.0.0/16      192.1.23.2               0             0 200 i
 *>  13.1.0.0/16      0.0.0.0                  0         32768 i
 *>  14.1.0.0/16      192.1.34.4               0             0 400 i
 *>  192.1.12.0       192.1.23.2               0             0 200 i
 *   192.1.23.0       192.1.23.2               0             0 200 i
 *>                   0.0.0.0                  0         32768 i
 *   192.1.34.0       192.1.34.4               0             0 400 i
 *>                   0.0.0.0                  0         32768 i
```

Figura 16 Show ip bgp R3

```
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, 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          192.1.34.3                             0 300 200 100 i
 *>  2.0.0.0          192.1.34.3                             0 300 200 i
 *>  3.0.0.0          192.1.34.3               0             0 300 i
 *>  4.0.0.0          0.0.0.0                  0         32768 i
 *>  11.1.0.0/16      192.1.34.3                             0 300 200 100 i
 *>  12.1.0.0/16      192.1.34.3                             0 300 200 i
 *>  13.1.0.0/16      192.1.34.3               0             0 300 i
 *>  14.1.0.0/16      0.0.0.0                  0         32768 i
 *>  192.1.12.0       192.1.34.3                             0 300 200 i
 *>  192.1.23.0       192.1.34.3               0             0 300 i
 *   192.1.34.0       192.1.34.3               0             0 300 i
 *>                   0.0.0.0                  0         32768 i
```

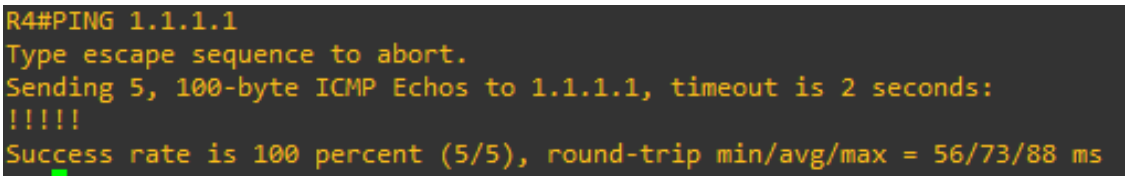
Se realiza ping de R1 A loopback R4 para comprobar conectividad de extremo a extremo

Figura 17 Ping R1 – R4



Se realiza ping de R4 A loopback R1 para comprobar conectividad de extremo a extremo

Figura 18 Ping R4 – R1



Configuración de rutas estáticas

R3(config)#ip route 14.1.0.0 255.255.0.0 192.1.34.4
R3(config)#ip route 13.1.0.0 255.255.0.0 192.1.34.3

Escenario 2

Figura 19 Ejemplo de escenario 1.

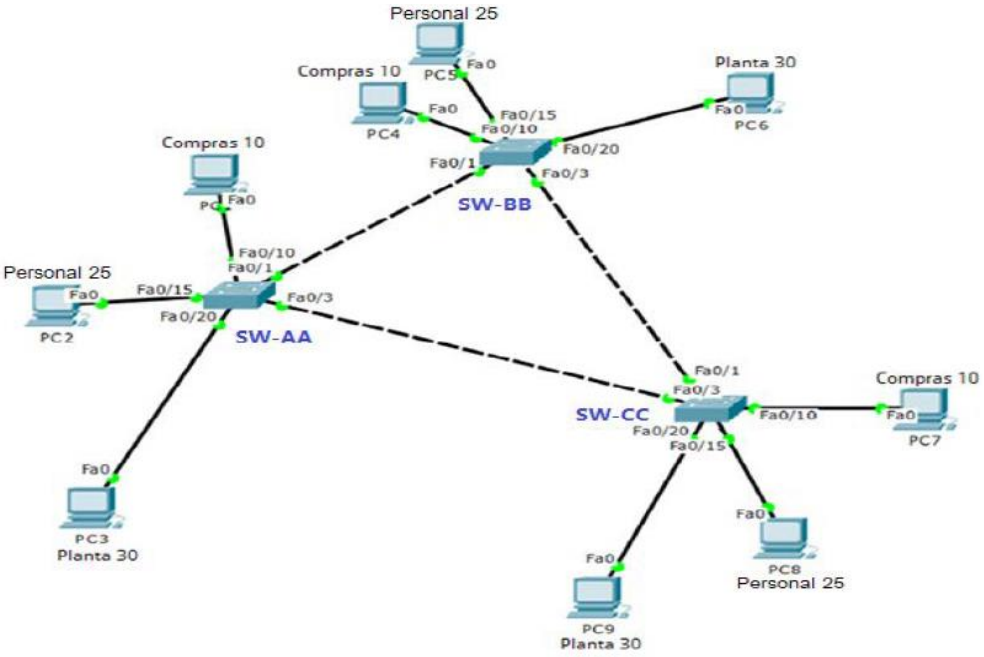
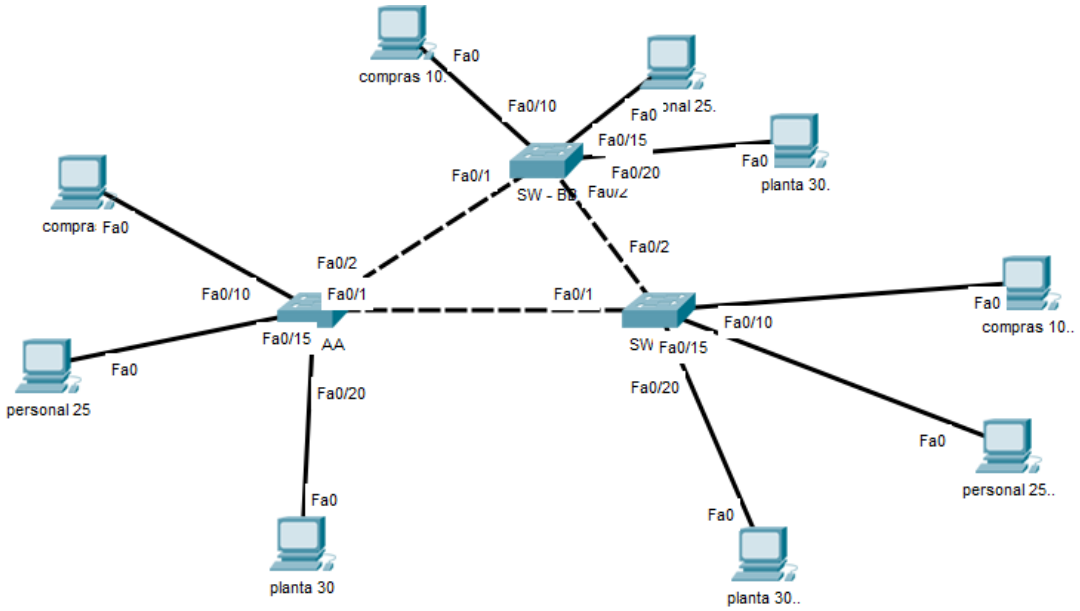


Figura 20 Topología escenario 1



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-AA (config)#vtp domain CCNP
   SW-AA (config)#vtp pass cisco
   SW-AA(config)#vtp mode client

   SW-CC(config)#vtp domain CCNP
   SW-CC(config)#vtp pass cisco
   SW-CC(config)#vtp mode client

   SW-BB(config)#vtp domain CCNP
   SW-BB(config)#vtp pass cisco
   SW-BB(config)#vtp mode server

   Verifique las configuraciones mediante el comando show vtp status.

Figura 21 show vtp status SW-AA

```
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 0xA6 0x0E 0x9A 0x72 0xA0
0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Figura 22 show vtp status SW-CC

```
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
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Figura 23 show vtp status SW-BB.

```
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
Local updater ID is 0.0.0.0 (no valid interface found)
```

B. Configurar DTP (Dynamic Trunking Protocol)

4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

SW-AA(config)#interface FastEthernet 0/2
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#switchport mode Dynamic desirable

SW-BB(config)#interface FastEthernet 0/1
SW-BB(config-if)#switchport mode trunk

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

Figura 24 show interfaces trunk.SW-AA

```
SW-AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       1
```

Figura 25 show interfaces trunk SW-BB

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

Port        Vlans allowed on trunk
Fa0/1       1-1005

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

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

6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/1 de SW-AA

SW-AA(config)#interface FastEthernet 0/1
SW-AA(config-if)#switchport mode trunk

SW-BB(config)#interface FastEthernet 0/1
SW-BB(config-if)#switchport mode trunk

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

Figura 26 show interfaces trunk SW-AA

```
SW-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/2       1
```

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

SW-CC(config)#interface fastEthernet 0/2
SW-CC(config-if)#switchport mode trunk

SW-BB(config)#interface FastEthernet 0/2
SW-BB(config-if)#switchport mode trunk

Figura 27 show interfaces trunk SW-AA

```
SW-CC$show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/2       1
```

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

SW-AA(config)#interface vlan 10

SW-BB#conf terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name admon

10. Verifique que las VLANs han sido agregadas correctamente.

Figura 28 show vlan brief SW-BB

```
SW-BB#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, 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
```

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

Tabla 2 Información para la configuración de los PC

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

Figura 29 Configuración IP EQUIPOS SW-AA

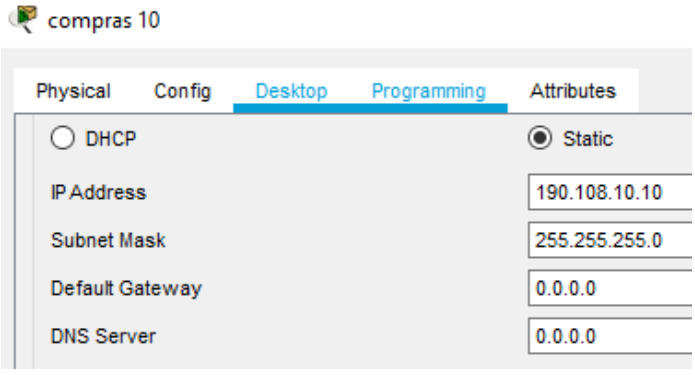


Figura 30 Configuración IP EQUIPOS SW-AA

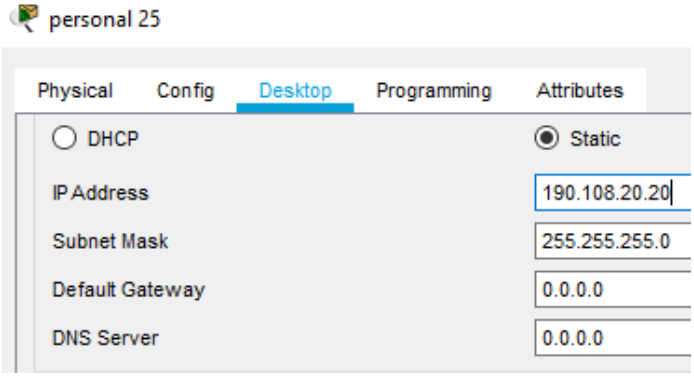


Figura 31 Configuración IP EQUIPOS SW-AA

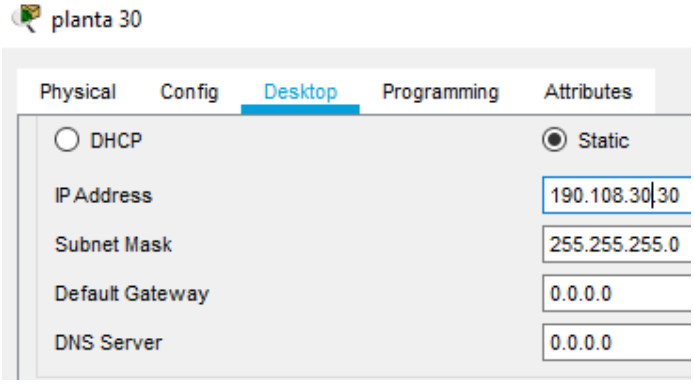


Figura 32 Configuración IP EQUIPOS SW-BB

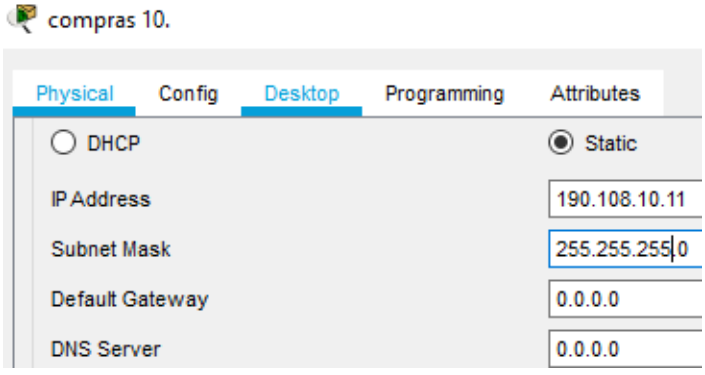


Figura 33 Configuración IP EQUIPOS SW-BB

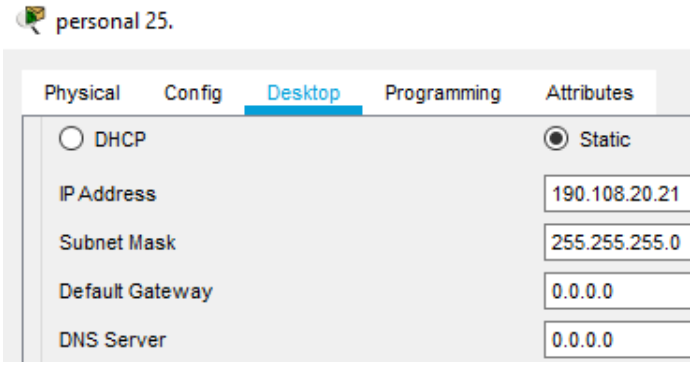


Figura 34 Configuración IP EQUIPOS SW-BB

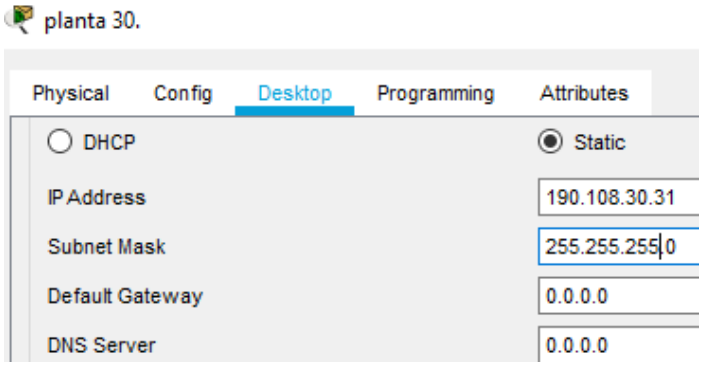


Figura 35 Configuración IP EQUIPOS SW-CC

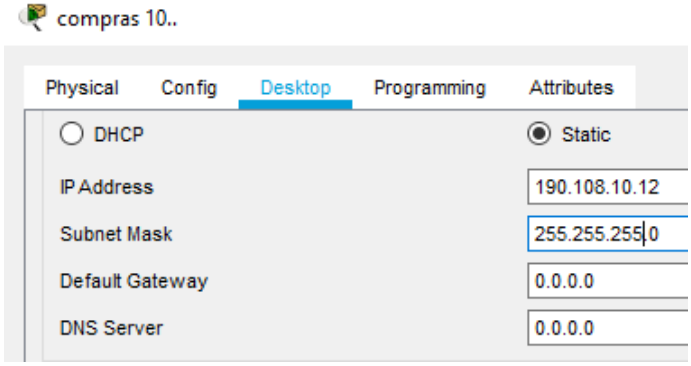


Figura 36 Configuración IP EQUIPOS SW-CC

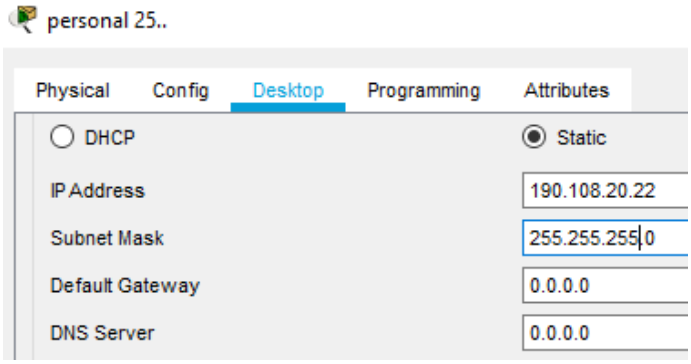
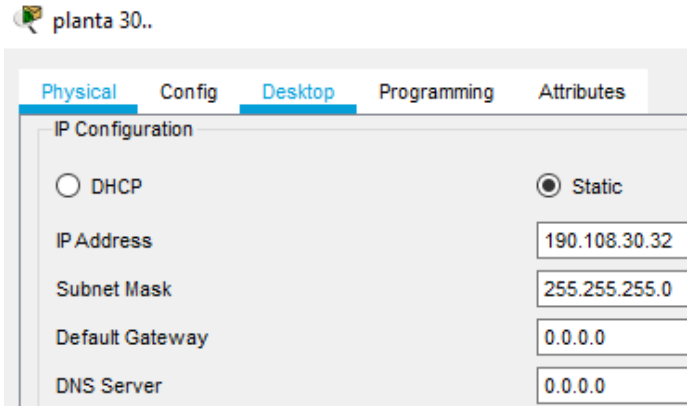


Figura 37 Configuración IP EQUIPOS SW-CC



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

El proceso completo esta en el punto 13

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(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#no shutdown
SW-AA(config-if)#interface fastEthernet 0/15
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#no shutdown
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport access vlan 30
```

SW-AA(config-if)#no shutdown

SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shutdown
SW-BB(config-if)#interface fastEthernet 0/15
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#no shutdown
SW-BB(config-if)#interface fastEthernet 0/20
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#no shutdown

SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#no shutdown
SW-CC(config-if)#interface fastEthernet 0/15
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#no shutdown
SW-CC(config-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#no shutdown

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 3 Información para la configuración de 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

SW-AA(config)#configure terminal
SW-AA (config)#vlan 99
SW-AA (config-vlan)#exit
SW-AA (config)#interface vlan 99

```
SW-AA (config-if)#no shutdown
SW-AA (config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA (config-if)#exit

SW-BB(config)#configure terminal
SW-BB(config)#vlan 99
SW-BB(config-vlan)#exit
SW-BB(config)#interface vlan 99
SW-BB(config-if)#no shutdown
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#exit

SW-BB(config)#configure terminal
SW-BB(config)#vlan 99
SW-BB(config-vlan)#exit
SW-BB(config)#interface vlan 99
SW-BB(config-if)#no shutdown
SW-BB(config-if)#ip address 190.108.99.3 255.255.255.0
SW-BB(config-if)#exit
```

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.

Cuando se realiza ping a equipos que están en diferentes segmentos o VLANS, estos no responden.

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

Si tiene éxito ya que se configura una VLAN común para todos, la de administración y en este caso se tiene comunicación desde allí.

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

No se tuvo éxito ya que ni el switch ni el pc tienen configurada una dirección ip, esto hace que los equipos no se encuentren dentro de la red. La dirección ip es

primordial ya que permite a cada dispositivo ser reconocido dentro de la misma red y así poder enviar y recibir información.

CONCLUSIONES

En el desarrollo de la Prueba de Habilidades Prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización CCNP, se puede medir el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del curso, poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

El BGP, permite crear un enrutamiento entre dominios sin bucles entre sistemas autónomos (AS). Un AS es un conjunto de enrutadores bajo una sola administración técnica. Los enrutadores en un AS pueden usar múltiples Protocolos de Pasarela Interior (IGP) para intercambiar información de enrutamiento dentro del AS. Los enrutadores pueden usar un protocolo de puerta de enlace exterior para enrutar paquetes fuera del AS.

Las rutas estáticas se utilizan a menudo, cuando no hay ninguna ruta dinámica a la dirección IP de destino o cuando se desea anular la ruta detectada dinámicamente.

La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y se la considera una interfaz de software. Es útil para probar y administrar un dispositivo asegurando que por lo menos una interfaz esté siempre disponible. Se pueden habilitar varias interfaces loopback en un router con la condición de que su dirección IP debe ser única y no la debe usar ninguna otra interfaz.

VTP, VLAN Trunk Protocol reduce la administración en una red conmutada. Cuando configuramos una nueva VLAN en un servidor VTP, la VLAN se distribuye a través de todos los conmutadores en el dominio, reduciendo la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo propiedad de Cisco.

DTP, protocolo de enlace dinámico se utiliza para negociar la formación de una troncal entre dos dispositivos. Las interfaces troncales Ethernet soportan diferentes modos de trunking. Una interfaz se puede establecer en trunking o no trunking, o para negociar trunking con la interfaz vecina. La negociación de troncales es gestionada por el protocolo de enlace dinámico, que funciona de forma punto a punto únicamente.

La importancia de los comandos de visualización de configuración en la

implementación de Networking es innegable, el desarrollo de este trabajo fue una de las herramientas mas valiosas, con estos podemos detectar errores de configuración además de llevar la traza de los procesos.

REFERENCIAS BIBLIOGRÁFICAS

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

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

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