DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRÁCTICAS CCNP

GUSTAVO ALEXANDER CEPEDA GUTIÉRREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA
INGENIERIA ELECTRONICA (RESOLUCIÓN 13155)
YOPAL - CASANARE
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

GUSTAVO ALEXANDER CEPEDA GUTIÉRREZ

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

DIRECTOR:
MSc. GERARDO GRANADOS A

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA
INGENIERIA ELECTRONICA (RESOLUCIÓN 13155)
YOPAL - CASANARE
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Yopal, 22 de mayo de 2020

AGRADECIMIENTOS

Este logro lo dedico principalmente a Dios, por inspirarme y darme fuerzas para llegar hasta éste punto en la formación y obtener así el fruto de uno de los tan anhelados sueños.

Agradecimiento especial a mi Madre, que más que mi progenitora fue mi motor y apoyo para alcanzar tan apreciado logro, con sus consejos, su apoyo emocional, económico e incondicional fueron la base fundamental para hoy compensar el esfuerzo que se tuvo durante el proceso con la satisfacción del resultado obtenido.
Quiero agradecer de gran manera a todos y cada uno de mis formadores académicos, tutores, monitores, orientadores, apoyos remotos y locales del CEAD de Yopal, cuerpo administrativo y de coordinación del programa, consejería y demás personas que fueron apoyo incondicional en cada una de los obstáculos y dudas presentadas durante el periodo de formación.

Agradezco también comedidamente al director del diplomado de profundización en Cisco y los diferentes tutores, por su conocimiento impartido durante éste proceso, por compartir sus experiencias técnicas basadas en redes y en los temas tratados académicamente en torno al trascurso del diplomado.

A mis compañeros y demás personas vinculadas en el proceso mi agradecimiento especial, con sus aportes, su apoyo y orientación en los obstáculos presentados fueron pieza clave en la solución de problemas a los cuales me vi enfrentado en lo que concierne al plan de formación, a cada uno de ellos mi manifestación rotunda de agradecimiento.

¡Gracias!

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ADYACENCIA: Nos dice cuando existe una conexión directa entre dos nodos de la red en un grafo. Es una matriz cuadrada y binaria, donde un valor 0 indica la ausencia de relaciones entre dos nodos, y un valor 1 indica que dos nodos están directamente relacionados. Usualmente se considera que los elementos de la diagonal principal son cero.

BGP: En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol)es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos..

DOT1Q: El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

EIGRP: EIGRP (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de Vector de distancias.

ENCAPSULATION: En redes de ordenadores, encapsulación es un método de diseño modular de protocolos de comunicación en el cual las funciones lógicas de una red son abstraídas ocultando información a las capas de nivel superior.

OSPF: OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio.

ROUTING: Es el proceso de seleccionar una ruta para el tráfico en una red o entre varias redes o entre ellas. En términos generales, el enrutamiento se realiza en muchos tipos de redes, incluidas las redes con conmutación de circuitos, como la red telefónica pública conmutada (PSTN) y las redes informáticas, como Internet.

SPANNING-TREE: En comunicaciones, STP (del inglés Spanning Tree Protocol) es un protocolo de red de capa 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

SWITCH: Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

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).

VTP: VTP son las siglas de 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.

VTY (Telnet): Telnet (Telecommunications Network) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.

RESUMEN

El presente trabajo se realiza en base a los conocimientos adquiridos en el contenido del Diplomado de profundización en Cisco CCNP para optar el título de Ingeniero Electrónico, done se aplican conceptos de enrutamiento y conmutación a partir de equipos que soportan configuraciones de protocolos de la Capa 2 y Capa 3 del modelo OSI, éstos lineamientos permiten no solo la adyacencia entre switch que se comportan como enrutadores, sino que también permiten aplicar modelos de seguridad para la estructura de redes de comunicación.

Este trabajo se realiza mediante el desarrollo de dos Escenarios, los cuales fueron sugeridos como prueba de habilidades prácticas del conocimiento adquirido durante el desarrollo del curso, para ello se emplea el uso de herramientas de emulación y simulación como lo es Packet Tracer y GNS3 de acuerdo a la necesidad y estructura del laboratorio sugerido realizando conexiones a Routers y Switches para que interactúen entre si y al finalizar comprobar su correcto funcionamiento y la propagación de las interfaces virtuales mediante los protocolos requeridos.

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

ABSTRACT

This work is carried out based on the knowledge acquired in the content of the Cisco CCNP in-depth Diploma in order to opt for the title of Electronic Engineer, where routing and switching concepts are applied from equipment that supports Layer 2 protocol configurations and Layer 3 of the OSI model, these guidelines allow not only the adjacency between switches that behave like routers, but also allow the application of security models for the structure of communication networks.

This work is carried out through the development of two Scenarios, which were suggested as a test of practical skills of the knowledge acquired during the development of the course, for which the use of emulation and simulation tools such as Packet Tracer and GNS3 according to to the need and structure of the suggested laboratory making connections to routers and switches so that they interact with each other and at the end check their correct operation and the propagation of virtual interfaces using the required protocols.

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

INTRODUCCIÓN

Existen diversos métodos y protocolos de red que permiten la interconexión de dispositivos generando un proceso de comunicación para facilitar el diseño de las arquitecturas de las redes con dispositivos de acuerdo al modelo OSI en Capa 2 y Capa 3, éstos modelos no solo permiten que los dispositivos se relacionen entre sí, sino que también facilitan la estructura del tráfico que debe interactuar en la red. Es de conocimiento que la manufacturera y fabricante de los equipos más comunes es Cisco, que a través de su lenguaje en sistemas operativos complejos y compactos como lo es iOS, propio de la compañía, permiten que a través de los avances y mejoras en los equipos se realicen una serie de protocolos que facilitan la interacción y permiten un mejor diseño en las redes promoviendo la seguridad de la información.

Para el desarrollo del presente documento se tuvieron en cuenta dos escenarios, en el primer escenario se realizará la configuracion y montaje de una red basada en la conexión de cuatro Routers todos ellos usando un protocolo BGP que es un protocolo mediante el cual se intercambia información de orientación 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, en el caso del primer escenario se hará que el protocolo de enrutamiento BGP permita la interacción entre los equipos y haremos que se comuniquen entre sí.

En el segundo escenario veremos la interacción entre Switches de características similares, en ellos se configurará protocolos de troncalización de puertos como VTP y DTP, se hará la creación e interfaces LAN virtuales, conocidas en redes como VLAN, se asignarán puertos troncales donde se propagarán las VLAN a través de la red y puertos de acceso donde se conmutarán para la conexión de usuarios finales, se realizaran en todos los casos la configuracion básica de los equipos y el direccionamiento correspondiente de acuerdo a la topología y tablas de red sugeridas, se harán prueba de conectividad y respuesta mediante comandos propios del lenguaje iOS que determinan la interacción de los equipos en las redes.

DESARROLLO

Descripción general de la prueba de habilidades

La evaluación 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 es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante debe 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.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer, GNS3 o SMARTLAB.

• Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL y OBLIGATORIA.

• Toda evidencia de copy-paste o plagio (de la web o de otros informes) será penalizada con severidad.

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1. Escenario 1

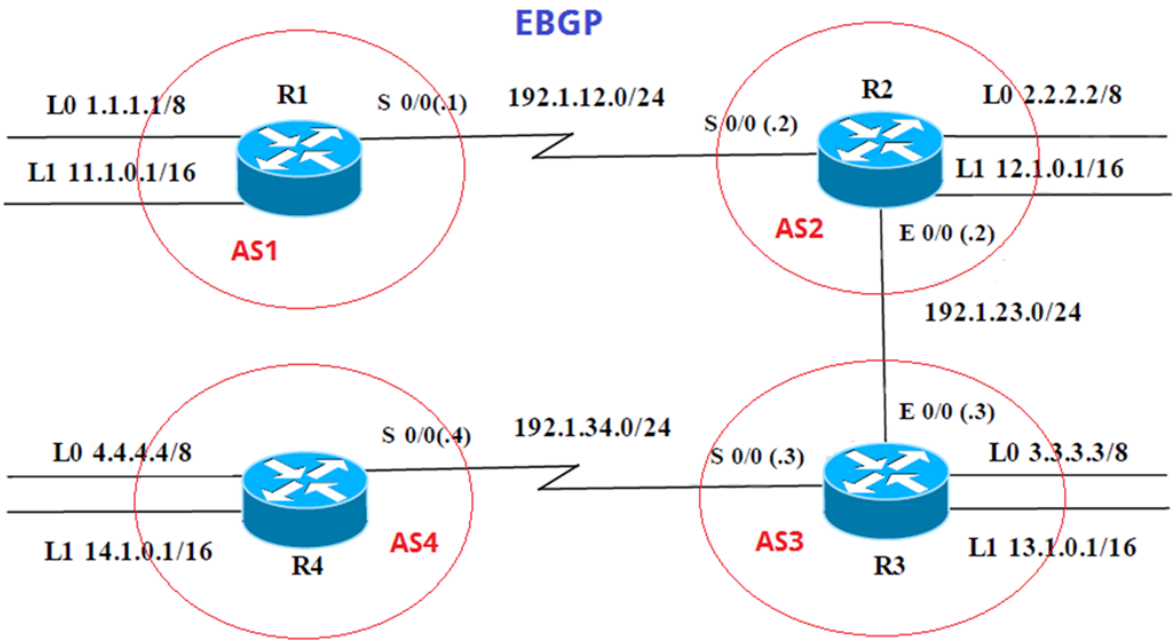


Figura 1. Diagrama de Red Escenario 1.

Información para configuración de los Routers

R1

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

Tabla 1. Direccionamiento IP Router R1 – Esc1.

R2

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

Tabla 2. Direccionamiento IP Router R2 - Esc1.

R3

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

Tabla 3. Direccionamiento IP Router R3 - Esc1.

R4

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

Tabla 4. Direccionamiento IP Router R4 - Esc1.

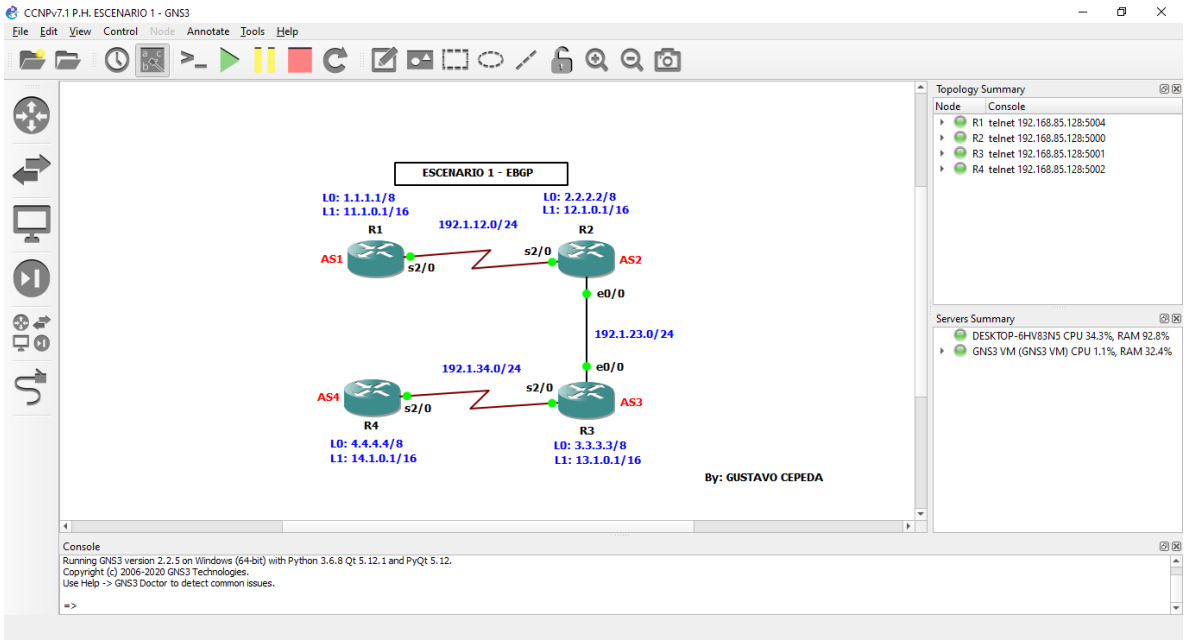


Figura 2. Montaje de la Red en GNS3 - Esc1.

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.***

SOLUCIÓN:

Configuración:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface loopback 0
R1(config-if)#ip a
*May 12 21:22:10.964: %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)#interface loopback 1
R1(config-if)#
*May 12 21:22:41.610: %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)#interface s2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
*May 12 21:24:13.345: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*May 12 21:24:14.429: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R1(config-if)#exit
R1(config)#router bgp 1
*May 12 21:24:36.477: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#exit
R1(config)#exit
R1#wr
*May 12 21:27:07.440: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#

R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface loopback 0
```

```
R2(config-if)#ip
*May 12 21:32:02.361: %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)#interface loopback 1
R2(config-if)#ip a
*May 12 21:32:33.635: %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)#interface s2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*May 12 21:33:51.644: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*May 12 21:33:52.652: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R2(config-if)#interface e0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#e
*May 12 21:34:29.748: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May 12 21:34:30.753: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 255.0.0.0
                          ^
% Invalid input detected at '^' marker.

R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#exit
R2(config)#exit
R2#
*May 12 21:37:44.760: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]

*May 12 21:37:47.994: %BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

Building configuration...
[OK]

Verificación:

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - 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, 00:00:58
      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, 00:00:58
      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
R1#
```

Figura 3. Comando "show ip route" en R1 - Esc1.

```
R2#sh 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
       a - application route
       + - 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, 00:01:09
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:01:09
      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
      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, Ethernet0/0
L        192.1.23.2/32 is directly connected, Ethernet0/0
R2#
```

Figura 4.Comando "show ip route" en R2 - Esc1.

Explicación:
Al configurar el protocolo BGP en los Router R1 y R2 y su direccionamiento IP de acuerdo a la tabla, evidenciamos mediante la verificación que existe adyacencia entre los Router identificada en el código B, allí podemos ver que creó la adyacencia mediante las Interfaces correspondientes y las vías creadas a través de la Interfaz fisica serial 2/0.

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.***

SOLUCIÓN:

Configuracion:

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#end
R2#wr
Building configuration...

*May 12 22:03:12.736: %SYS-5-CONFIG_I: Configured from console by console[OK]
R2#
```

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface loopback 0
R3(config-if)#ip
*May 12 23:30:44.905: %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)#interface loopback 1
R3(config-if)#ip
*May 12 23:31:12.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R3(config-if)#ip address 13.1.0.1 255.255.255.0
R3(config-if)#interface e0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
```

*May 12 23:32:09.925: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May 12 23:32:11.721: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R3(config-if)#interface s2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
*May 12 23:32:50.957: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*May 12 23:32:51.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#
*May 12 23:33:21.250: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#end
R3#
*May 12 23:35:52.787: %BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
R3#w
*May 12 23:35:53.861: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#

Verificación:

```
R2#sh 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
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 01:59:32
      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, 00:01:27
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 01:59:32
      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
      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, Ethernet0/0
L        192.1.23.2/32 is directly connected, Ethernet0/0
R2#
```

Figura 5. Comando "show ip route" en R2 - Esc1

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

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:01:41
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:41
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.0.0.0/8 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:01:41
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:01:41
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.0.0/24 is directly connected, Loopback1
L        13.1.0.1/32 is directly connected, Loopback1
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:01:41
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.3/32 is directly connected, Ethernet0/0
R3#
```

Figura 6. Comando "show ip route" en R3 - Esc1

Explicación:
Al configurar la adyacencia entre R2 y R3 evidenciamos que ya encontró una ruta por la cual tiene comunicación entre sí los dos Router, eso nos garantiza la interacción entre los Router, vemos que R2 ya ha actualizado su tabla de enrutamiento y ha aprendido 4 rutas, dos con los Loopback correspondientes hacia R1 y 2 adicionales hacia R3 a través de las interfaces fisicas correspondientes.

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.***

SOLUCIÓN:

Configuración:

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#end
R3#wr
*May 13 00:12:47.012: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Building configuration...
[OK]
R3#
```

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface loopback 0
R4(config-if)#
*May 13 00:15:02.515: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R4(config-if)#ip add 4.4.4.4 255.0.0.0
R4(config-if)#interface loopback 1
R4(config-if)#
```

*May 13 00:15:31.029: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R4(config-if)#ip add 14.1.0.1 255.255.0.0
R4(config-if)#interface s2/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
*May 13 00:16:25.042: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*May 13 00:16:26.048: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#end
R4#wr
*May 13 00:18:04.193: %SYS-5-CONFIG_I: Configured from console by console
R4#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R4#
*May 13 00:18:07.796: %BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
R4#

Es necesario realizar una configuracion adicional para que los Router creen la condición de adyacencia mediante las vías del Loopback más que no lo haga mediante las interfaces fisicas seriales, para ello configuramos lo siguiente en R3 y R4.

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#

*May 13 00:23:48.831: %BGP-3-NOTIFICATION: sent to neighbor 192.1.34.4 6/3 (Peer De-configured) 0 bytes
R3(config-router)#
*May 13 00:23:48.840: %BGP_SESSION-5-ADJCHANGE: neighbor 192.1.34.4 IPv4 Unicast topology base removed from session Neighbor deleted
*May 13 00:23:48.840: %BGP-5-ADJCHANGE: neighbor 192.1.34.4 Down Neighbor deleted
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop
R3(config-router)#end
R3#w
*May 13 00:25:34.510: %SYS-5-CONFIG_I: Configured from console by console
R3#wr
Building configuration...
[OK]
R3#

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
*May 13 00:29:07.896: %BGP-3-NOTIFICATION: sent to neighbor 3.3.3.3 passive 2/2 (peer in wrong AS) 2 bytes 0003
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
*May 13 00:29:07.896: %BGP-4-MSGDUMP: unsupported or mal-formatted message received from 3.3.3.3:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0039 0104 0003 00B4 2C2C 2C2C 1C02 0601
0400 0100 0102 0280 0002 0202 0002 0246 0002 0641 0400 0000 03
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#
*May 13 00:29:12.315: %BGP-5-NBR_RESET: Neighbor 3.3.3.3 passive reset (BGP Notification sent)
*May 13 00:29:12.319: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 passive Down BGP Notification sent

R4(config-router)#
*May 13 00:29:15.434: %BGP-3-NOTIFICATION: sent to neighbor 3.3.3.3 active 2/2 (peer in wrong AS) 2 bytes 0003
R4(config-router)#end
R4#
*May 13 00:29:15.434: %BGP-4-MSGDUMP: unsupported or mal-formatted message received from 3.3.3.3:
FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0039 0104 0003 00B4 2C2C 2C2C 1C02 0601
0400 0100 0102 0280 0002 0202 0002 0246 0002 0641 0400 0000 03
R4#wr
*May 13 00:29:16.565: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[OK]
R4#

Verificación:

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

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:59:39
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:59:39
      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
S     4.0.0.0/8 [1/0] via 192.1.34.4
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:59:39
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:59:39
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.0.0/24 is directly connected, Loopback1
L        13.1.0.1/32 is directly connected, Loopback1
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:59:39
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.3/32 is directly connected, Ethernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial2/0
L        192.1.34.3/32 is directly connected, Serial2/0
R3#
```

Figura 7. Comando "show ip route" en R3 - Esc1

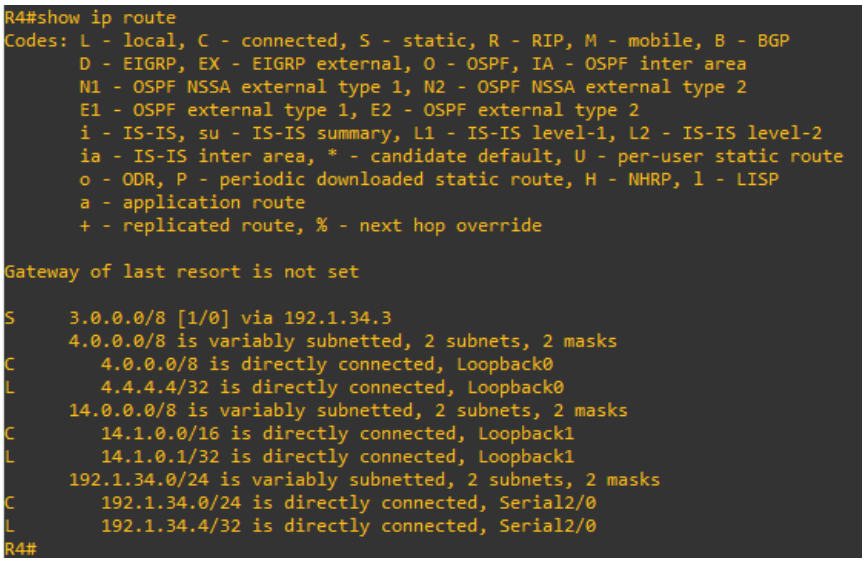


Figura 8. Comando "show ip route" en R4 - Esc1

Explicación:

Se crearon las adyacencias entre los Router R3 y R4, el Router R3 aprendió dos rutas adicionales, para R4 también fueron creadas las rutas a través de las Interfaces Loopback correspondientes, por tanto fue necesario precisar que la comunicación y la vía de la ruta fuera a través de las interfaces Loopback mas no fueran las interfaces seriales fisicas, para ello se eliminó de la configuracion la adyacencia a través de esas rutas y se crearon mediante las rutas del Loopback.

2. Escenario 2

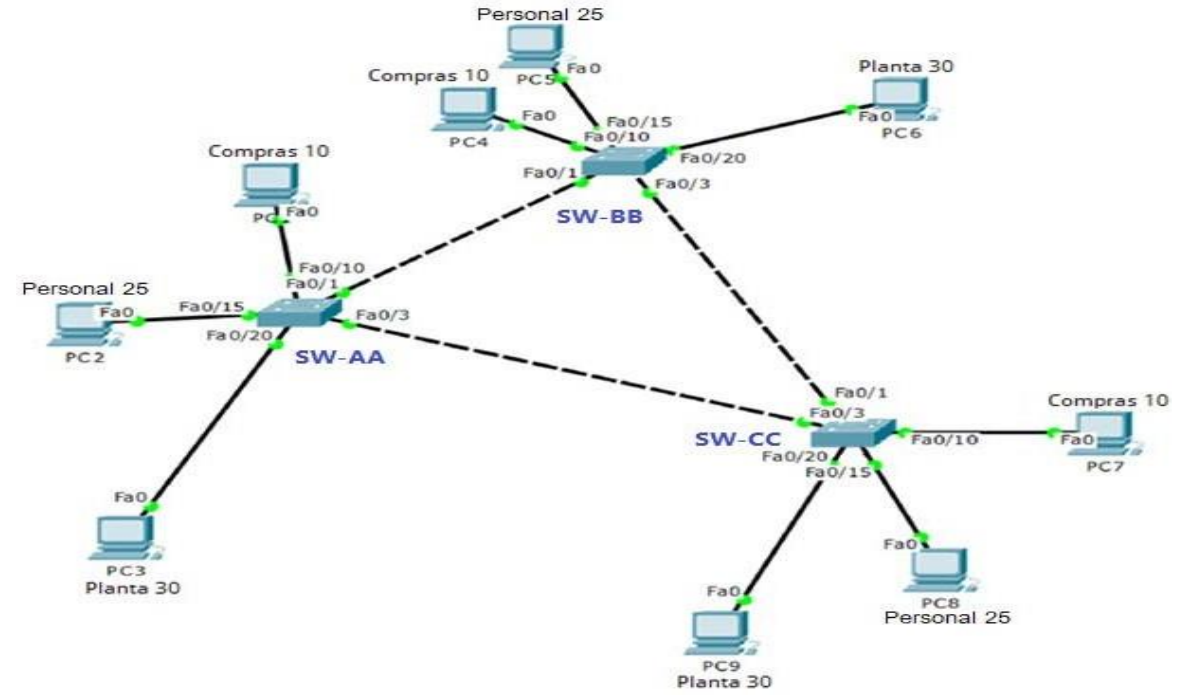


Figura 9. Diagrama de Red Escenario 2.

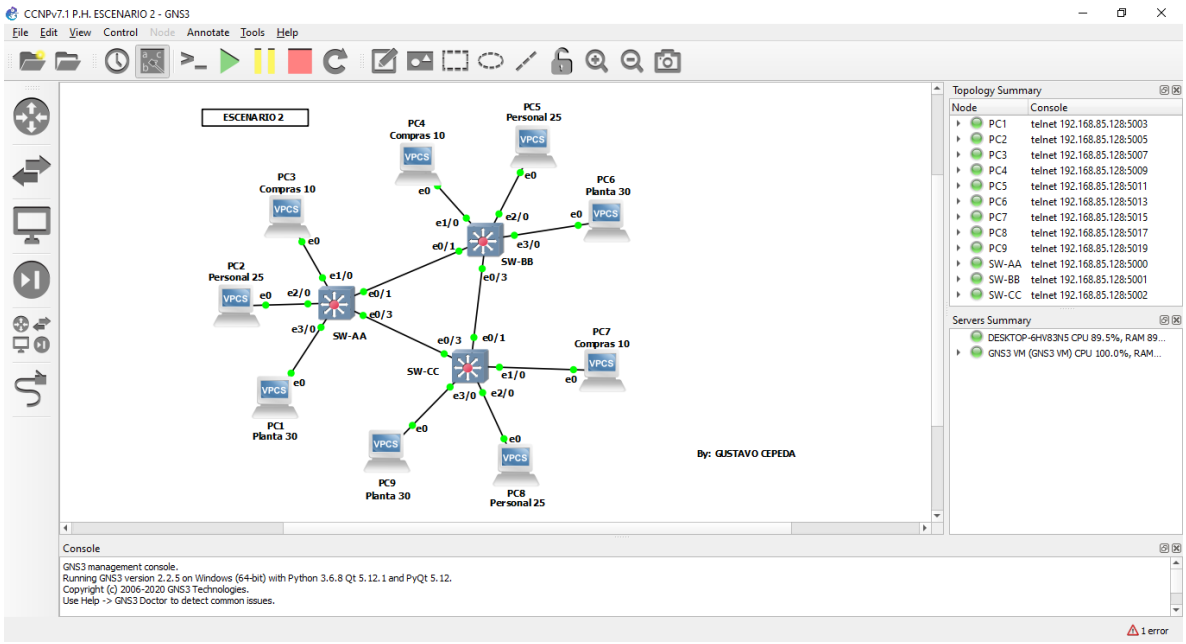


Figura 10. Montaje de la Red en GNS3 - Esc2

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.

SOLUCIÓN:

SW-AA.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VTP password to cisco
SW-AA(config)#end
SW-AA#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
*May 13 01:54:48.257: %SYS-5-CONFIG_I: Configured from console by console
[confirm]
Building configuration...
Compressed configuration from 1362 bytes to 826 bytes[OK]
SW-AA#
```

SW-BB.

```
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#vtp mode server
Device mode already VTP Server for VLANS.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VTP password to cisco
SW-BB(config)#end
SW-BB#wr
*May 13 02:00:38.152: %SYS-5-CONFIG_I: Configured from console by console
SW-BB#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
```

by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1362 bytes to 825 bytes[OK]
SW-BB#

SW-CC.

SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VTP password to cisco
SW-CC(config)#end
SW-CC#
*May 13 02:03:52.271: %SYS-5-CONFIG_I: Configured from console by console
SW-CC#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1362 bytes to 824 bytes[OK]
SW-CC#

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

SOLUCIÓN:

SW-AA.

```
SW-AA#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99

SW-AA#
```

Figura 11. Verificación VTP en SW-AA - Esc2.

SW-BB.

```
SW-BB#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 5-13-20 02:17:21
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
MD5 digest                        : 0x00 0xEB 0x55 0x51 0x26 0xDA 0x0B 0xEE
                                    0xBA 0x03 0xAF 0x5C 0xC4 0x35 0xD8 0x37

SW-BB#
```

Figura 12. Verificación VTP en SW-BB - Esc2

SW-CC.

```
SW-CC#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99

SW-CC#
```

Figura 13. Verificación VTP en SW-CC - Esc2

B. Configurar DTP (Dynamic Trunking Protocol)

3. 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.***

SOLUCIÓN:

SW-AA.

SW-AA#conf t

Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#int e0/1
SW-AA(config-if)#swit
SW-AA(config-if)#switchport trunk enc
SW-AA(config-if)#switchport trunk encapsulation do
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#end
SW-AA#wr
*May 13 02:31:33.078: %SYS-5-CONFIG_I: Configured from console by console
SW-AA#wr
Building configuration...
Compressed configuration from 1400 bytes to 850 bytes[OK]
SW-AA#
*May 13 02:32:34.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*May 13 02:32:35.755: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up

SW-BB.

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface e0/1
SW-BB(config-if)#switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#end
SW-BB#wr
Building configuration...

*May 13 02:32:35.429: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 1435 bytes to 873 bytes[OK]

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

SOLUCIÓN:

SW-AA.

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
SW-AA#
```

Figura 14. Verificación de Interfaces Virtuales en SW-AA - Esc2.

SW-BB.

```
SW-BB#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
SW-BB#
```

Figura 15. Verificación de Interfaces Virtuales en SW-BB - Esc2.

4. 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

SOLUCIÓN:

SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface e0/3
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#end
SW-AA#wr
Building configuration...
Compressed configuration from 1461 bytes to 883 bytes[OK]
SW-AA#
*May 13 03:05:50.859: %SYS-5-CONFIG_I: Configured from console by console
SW-AA#

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

SOLUCIÓN:

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       auto             802.1q         trunking      1
Et0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
Et0/3       none
SW-AA#
```

Figura 16. Verificación enlace troncal en la Interfaz e0/3 - SW-AA - Esc2.

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

SOLUCIÓN:

SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface e0/1
SW-CC(config-if)#switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#end
SW-CC#wr
Building configuration...

*May 13 03:12:52.074: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 1423 bytes to 868 bytes[OK]
SW-CC#

```
SW-CC#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       on               802.1q         trunking      1
Et0/3       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       none
Et0/3       1
SW-CC#
```

Figura 17. Verificación enlace troncal en la Interfaz e0/1 - SW-CC - Esc2.

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       auto             802.1q         trunking      1
Et0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
Et0/3       1
SW-AA#
```

Figura 18. Verificación enlace troncal en la Interfaz e0/3 - SW-AA - Esc2.

C. Agregar VLANs y asignar puertos.

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

SOLUCIÓN:

SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.

SW-AA(config)#

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#end
SW-BB#wr
*May 13 03:23:40.948: %SYS-5-CONFIG_I: Configured from console by console
SW-BB#wr
Building configuration...
Compressed configuration from 1435 bytes to 874 bytes[OK]
SW-BB#

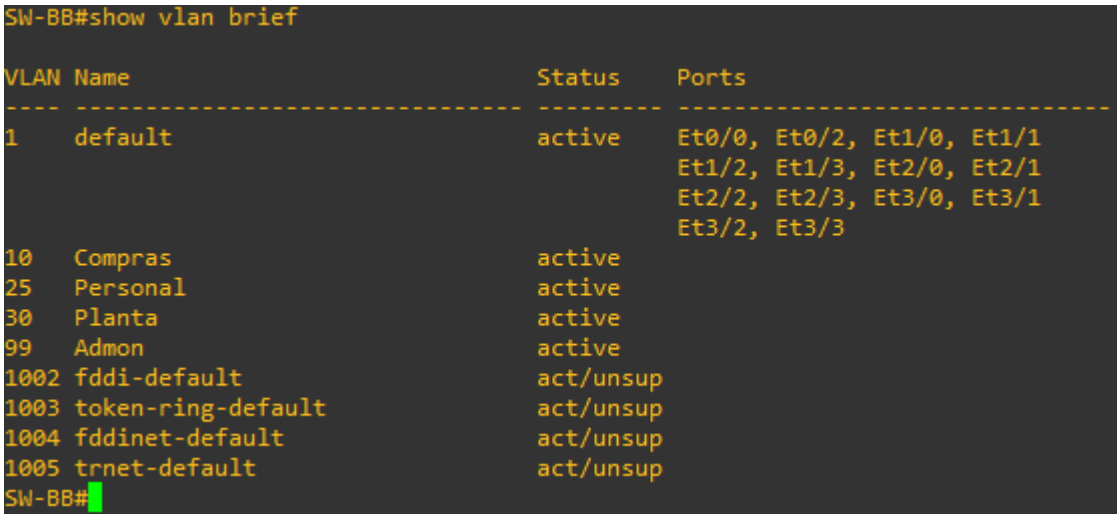
9. Verifique que las VLANs han sido agregadas correctamente.

SOLUCIÓN:

```
SW-AA#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW-AA#
```

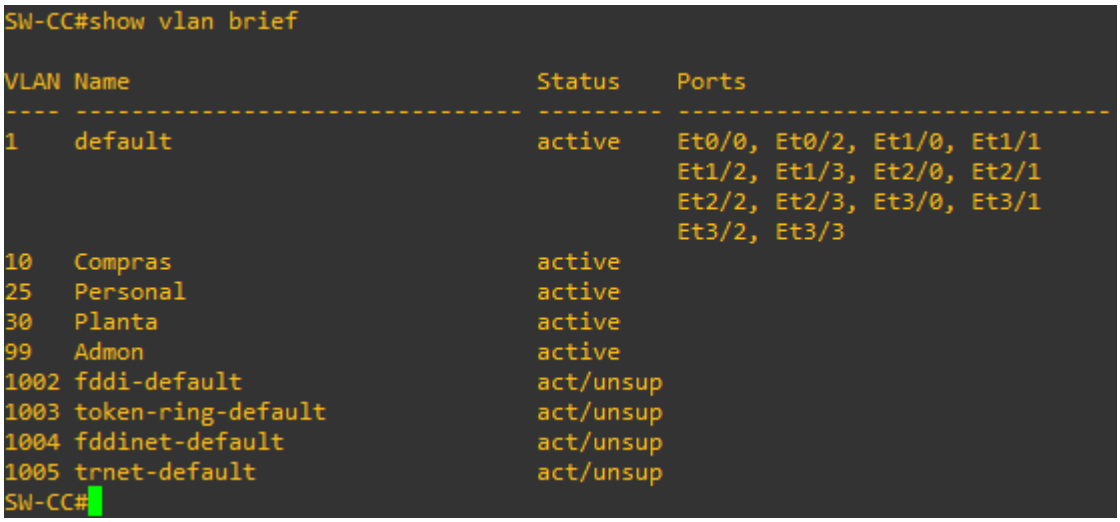
Figura 19. Verificación listado de VLAN agregadas en SW-AA – Esc2.



```
SW-BB#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW-BB#
```

Figura 20. Verificación listado de VLAN agregadas en SW-BB – Esc2.



```
SW-CC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW-CC#
```

Figura 21. Verificación listado de VLAN agregadas en SW-CC – Esc2.

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

Interfaz	VLAN	Direcciones IP de los PC's
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

Tabla 5. Listado de VLAN y Direccionamiento IP para PC´s - Esc2.

X = número de cada PC particular.

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

12. 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 PC's de acuerdo con la tabla de arriba.

SOLUCIÓN:

SW-AA.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface e1/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#interface e2/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface e3/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
SW-AA(config)#end
SW-AA#wr
Building configuration...
Compressed configuration from 1614 bytes to 949 bytes[OK]
SW-AA#
*May 13 03:37:58.602: %SYS-5-CONFIG_I: Configured from console by console
SW-AA#
```

SW-BB.

```
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface e1/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#interface e2/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
```

SW-BB(config-if)#exit
SW-BB(config)#interface e3/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
SW-BB(config)#end
SW-BB#wr
Building configuration...
*May 13 03:39:41.884: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 1588 bytes to 940 bytes[OK]
SW-BB#

SW-CC.

SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface e1/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#interface e2/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface e3/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
SW-CC(config)#end
SW-CC#wr
Building configuration...
Compressed configuration from 1576 bytes to 931 bytes[OK]
SW-CC#
*May 13 03:41:34.544: %SYS-5-CONFIG_I: Configured from console by console
SW-CC#

PC1.

PC1> ip 190.108.30.1 24
Checking for duplicate address...
PC1 : 190.108.30.1 255.255.255.0

PC1>

PC2.

PC2> ip 190.108.20.2 24
Checking for duplicate address...
PC1 : 190.108.20.2 255.255.255.0

PC2>

PC3.

PC3> ip 190.108.10.3 24
Checking for duplicate address...
PC1 : 190.108.10.3 255.255.255.0

PC3>

PC4.

PC4> ip 190.108.10.4 24
Checking for duplicate address...
PC1 : 190.108.10.4 255.255.255.0

PC4>

PC5.

PC5> ip 190.108.20.5
Checking for duplicate address...
PC1 : 190.108.20.5 255.255.255.0

PC5>

PC6.

PC6> ip 190.108.30.6 24
Checking for duplicate address...
PC1 : 190.108.30.6 255.255.255.0

PC6>

PC7.

PC7> ip 190.108.10.7 24
Checking for duplicate address...
PC1 : 190.108.10.7 255.255.255.0

PC7>

PC8.

```
PC8> ip 190.108.20.8 24
Checking for duplicate address...
PC1 : 190.108.20.8 255.255.255.0

PC8>
```

PC9.

```
PC9> ip 190.108.30.9 24
Checking for duplicate address...
PC1 : 190.108.30.9 255.255.255.0

PC9>
```

D. Configurar las direcciones IP en los Switches.

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

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

Tabla 6. Listado de VLAN y Direccionamiento IP para Switch - Esc2.

SOLUCIÓN:

SW-AA.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#i
*May 13 04:05:16.881: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#end
SW-AA#wr
Building configuration...
```

Compressed configuration from 1682 bytes to 992 bytes[OK]
SW-AA#
*May 13 04:05:53.061: %SYS-5-CONFIG_I: Configured from console by console
SW-AA#

SW-BB.

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip a
*May 13 04:06:13.233: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#end
SW-BB#wr
Building configuration...
Compressed configuration from 1656 bytes to 984 bytes[OK]
SW-BB#
*May 13 04:06:31.362: %SYS-5-CONFIG_I: Configured from console by console
SW-BB#

SW-CC.

SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip add
*May 13 04:06:47.753: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#end
SW-CC#wr
*May 13 04:07:02.269: %SYS-5-CONFIG_I: Configured from console by console
SW-CC#wr
Building configuration...
Compressed configuration from 1644 bytes to 974 bytes[OK]
SW-CC#

E. Verificar la conectividad Extremo a Extremo

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

SOLUCIÓN:

PC1.

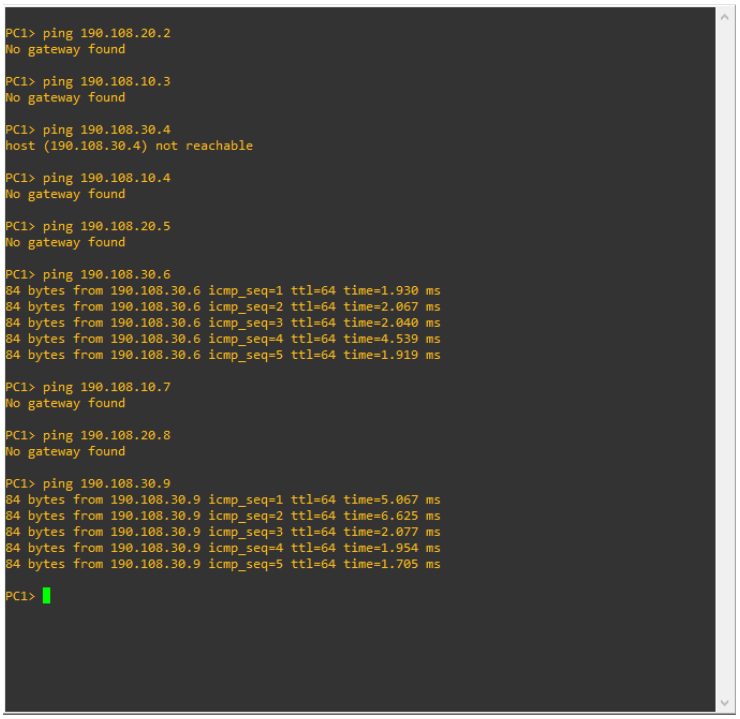


Figura 22. Respuesta de Ping desde PC1 a otros PC´s - Esc2.

PC2.

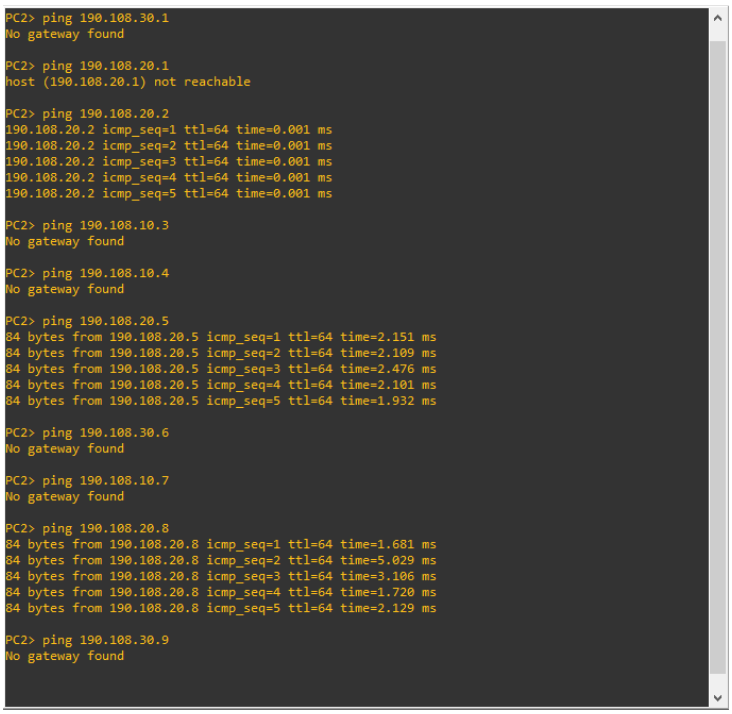


Figura 23. Respuesta de Ping desde PC2 a otros PC´s - Esc2.

PC3.

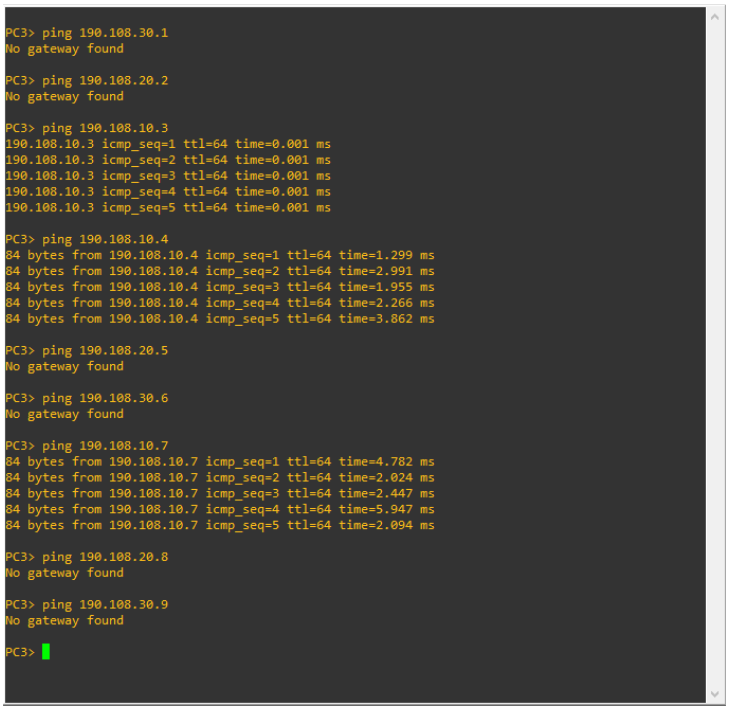


Figura 24. Respuesta de Ping desde PC3 a otros PC´s - Esc2.

PC4.

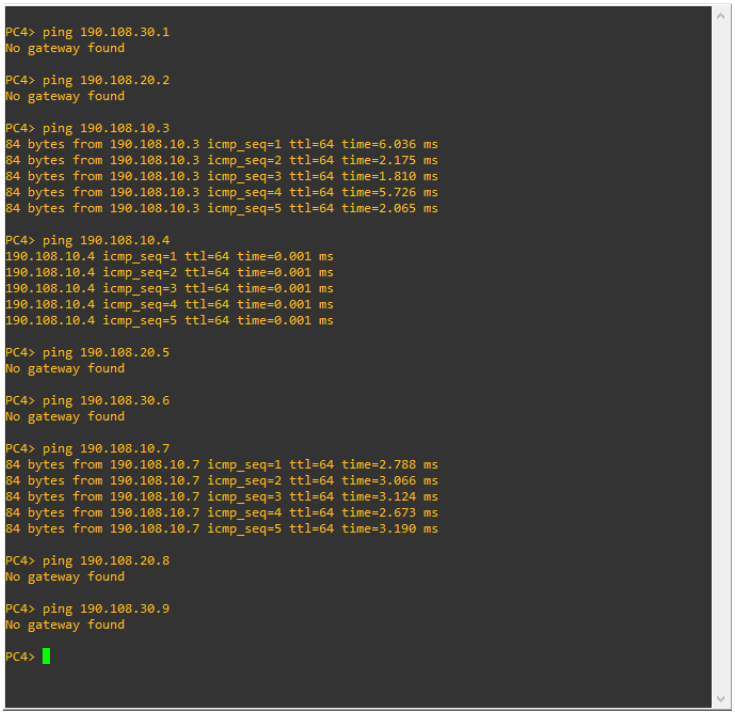


Figura 25. Respuesta de Ping desde PC4 a otros PC´s - Esc2.

PC5.

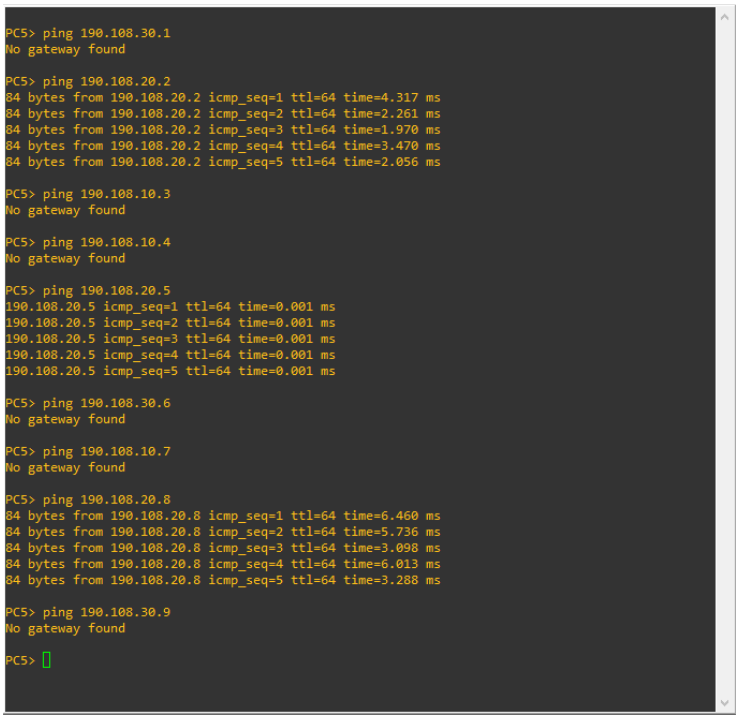


Figura 26. Respuesta de Ping desde PC5 a otros PC´s - Esc2.

PC6.

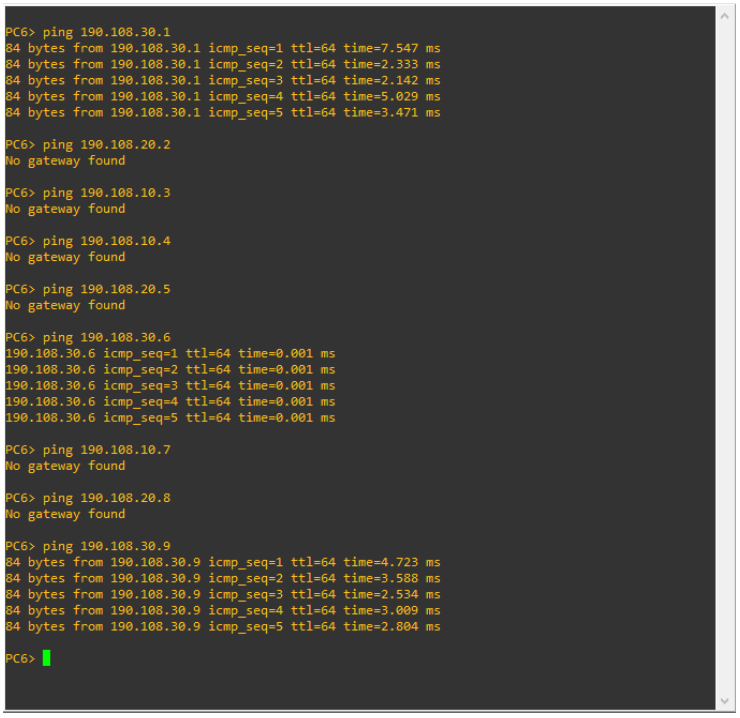


Figura 27. Respuesta de Ping desde PC6 a otros PC´s - Esc2.

PC7.

```
PC7> ping 190.108.30.1
No gateway found

PC7> ping 190.108.20.2
No gateway found

PC7> ping 190.108.10.3
84 bytes from 190.108.10.3 icmp_seq=1 ttl=64 time=1.616 ms
84 bytes from 190.108.10.3 icmp_seq=2 ttl=64 time=1.885 ms
84 bytes from 190.108.10.3 icmp_seq=3 ttl=64 time=1.824 ms
84 bytes from 190.108.10.3 icmp_seq=4 ttl=64 time=2.003 ms
84 bytes from 190.108.10.3 icmp_seq=5 ttl=64 time=2.625 ms

PC7> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=64 time=4.902 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=64 time=2.259 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=64 time=2.337 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=64 time=2.525 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=64 time=2.383 ms

PC7> ping 190.108.20.5
No gateway found

PC7> ping 190.108.30.6
No gateway found

PC7> ping 190.108.10.7
190.108.10.7 icmp_seq=1 ttl=64 time=0.001 ms
190.108.10.7 icmp_seq=2 ttl=64 time=0.001 ms
190.108.10.7 icmp_seq=3 ttl=64 time=0.001 ms
190.108.10.7 icmp_seq=4 ttl=64 time=0.001 ms
190.108.10.7 icmp_seq=5 ttl=64 time=0.001 ms

PC7> ping 190.108.20.8
No gateway found

PC7> ping 190.108.30.9
No gateway found

PC7>
```

Figura 28. Respuesta de Ping desde PC7 a otros PC´s - Esc2.

PC8.

```
PC8> ping 190.108.30.1
No gateway found

PC8> ping 190.108.20.2
84 bytes from 190.108.20.2 icmp_seq=1 ttl=64 time=2.603 ms
84 bytes from 190.108.20.2 icmp_seq=2 ttl=64 time=2.150 ms
84 bytes from 190.108.20.2 icmp_seq=3 ttl=64 time=2.850 ms
84 bytes from 190.108.20.2 icmp_seq=4 ttl=64 time=2.164 ms
84 bytes from 190.108.20.2 icmp_seq=5 ttl=64 time=2.382 ms

PC8> ping 190.108.10.3
No gateway found

PC8> ping 190.108.10.4
No gateway found

PC8> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=64 time=2.387 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=64 time=2.274 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=64 time=7.672 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=64 time=2.453 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=64 time=2.273 ms

PC8> ping 190.108.30.6
No gateway found

PC8> ping 190.108.10.7
No gateway found

PC8> ping 190.108.20.8
190.108.20.8 icmp_seq=1 ttl=64 time=0.001 ms
190.108.20.8 icmp_seq=2 ttl=64 time=0.001 ms
190.108.20.8 icmp_seq=3 ttl=64 time=0.001 ms
190.108.20.8 icmp_seq=4 ttl=64 time=0.001 ms
190.108.20.8 icmp_seq=5 ttl=64 time=0.001 ms

PC8> ping 190.108.30.9
No gateway found

PC8>
```

Figura 29. Respuesta de Ping desde PC8 a otros PC´s - Esc2.

PC9.

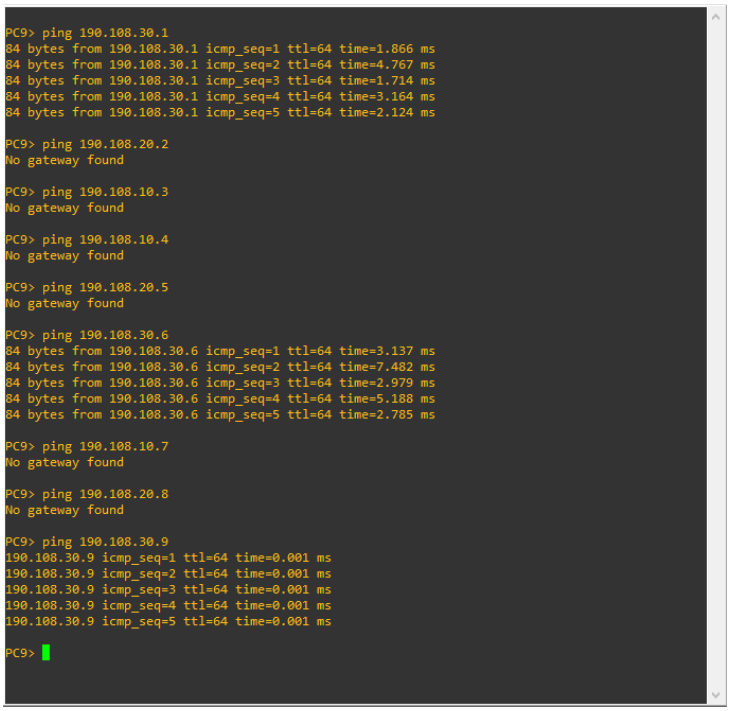


Figura 30. Respuesta de Ping desde PC9 a otros PC´s - Esc2.

Explicación:
Todos los Host que se encontraban en la misma VLAN tuvieron respuesta satisfactoria porque se encuentran con el mismo direccionamiento IP, pero para lograr que todos los Host tengan comunicación entre sí se debe configurar una puerta de enlace o mediante enrutamientos con equipos Capa 3 para realizar configuracion de enrutamiento con privilegios de dispersión y adyacencias de VLAN para conmutar todas las interfaces troncales hacia puertas de enlaces válidas.

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

SOLUCIÓN:

SW-AA.

```
SW-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 = 5/5/6 ms
SW-AA#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/7 ms
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/8 ms
SW-AA#
```

Figura 31. Respuesta de Ping desde SW-AA hacia SW-BB y SW-CC - Esc2.

SW-BB.

```
SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/6/9 ms
SW-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 = 4/6/11 ms
SW-BB#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/5/7 ms
SW-BB#
```

Figura 32. Respuesta de Ping desde SW-BB hacia SW-AA y SW-CC - Esc2

SW-CC.

```
SW-CC#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/5/7 ms
SW-CC#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/10 ms
SW-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 = 4/4/5 ms
SW-CC#
```

Figura 33. Respuesta de Ping desde SW-CC hacia SW-AA y SW-BB - Esc2

Explicación:
Todos los Switch tuvieron respuestas satisfactorias ya que se encuentran compartiendo el mismo direccionamiento IP, se encuentran en el mismo segmento de red y sus conexiones locales pertenecen a la misma VLAN de gestión, así que cuentan con condiciones de red en común que permiten la interacción satisfactoria entre los tres switch.

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

SOLUCIÓN:

Explicación:
La respuesta desde los Switch hacia los PC´s no fue satisfactoria debido a que los puertos que conectan los PC´s se encuentran modo acceso con la VLAN correspondiente a cada uno de los Host, la VLAN de gestión o administrativa es la VLAN 99 la cual no se encuentra propagada en la red de los usuarios finales, el direccionamiento no es el adecuado y falta una puerta de enlace que comunique los PC´s con la dirección del enrutamiento.

SW-AA.

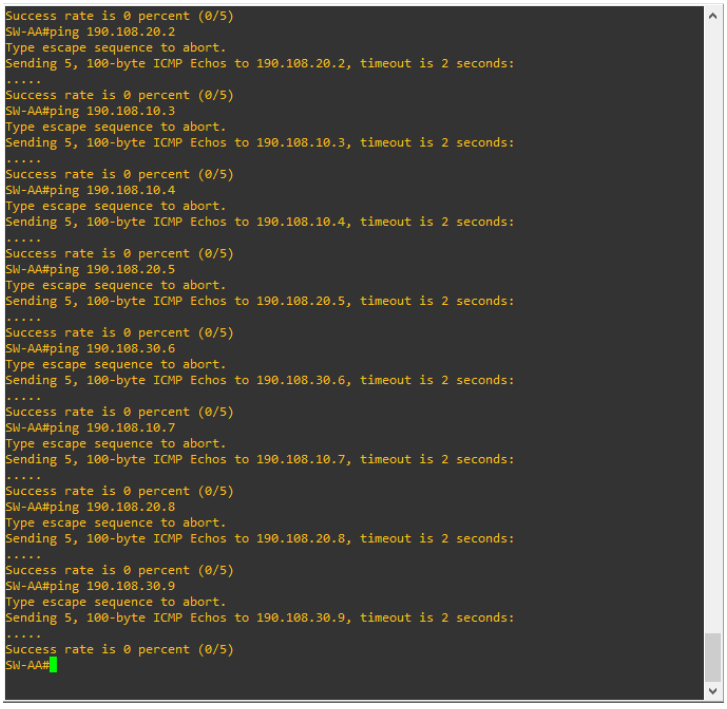


Figura 34. Respuesta de Ping desde SW-AA hacia los PC´s - Esc2

SW-BB.

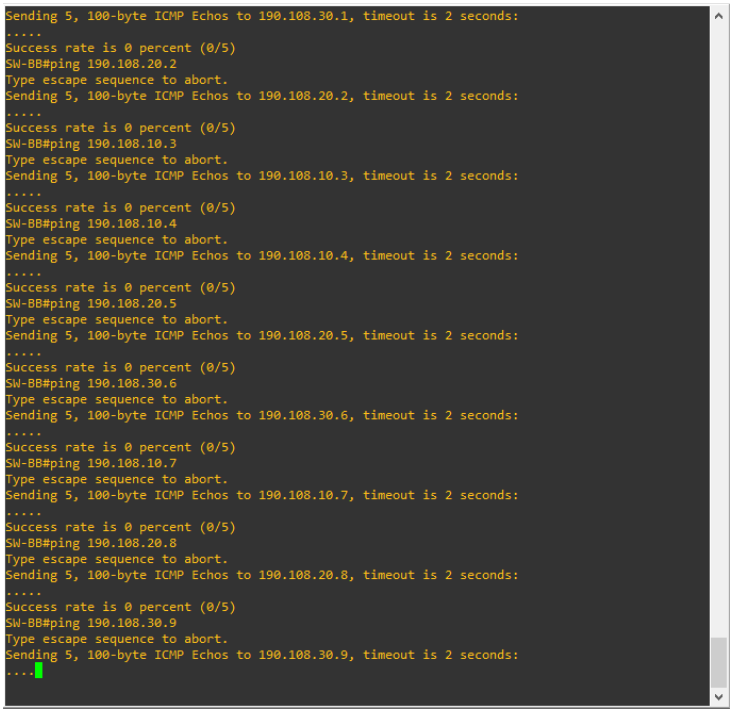


Figura 35. Respuesta de Ping desde SW-BB hacia los PC´s - Esc2

SW-CC.

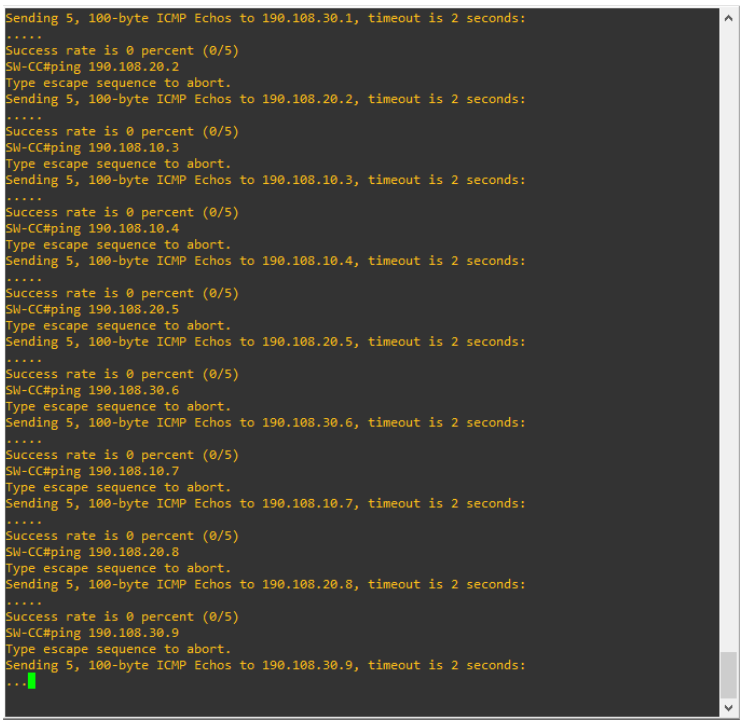


Figura 36. Respuesta de Ping desde SW-CC hacia los PC´s - Esc2

CONCLUSIONES

Mediante el desarrollo del presente documento se logró.

Se identificó la importancia de un protocolo de enrutamiento que permita la adyacencia de Router para la creación de una red que interactúe con los equipos broadcast y los usuarios finales a través de la aplicación de conceptos básicos como lo son el enrutamiento bajo configuracion BGP para interconectar Router y de esa forma crear tablas de enrutamiento en IPv4 para la topología de red sugerida, a su vez se aplicaron los conocimientos adquiridos en el diplomado de profundización CCNP mediante esta prueba de habilidades prácticas que integró configuraciones básicas hasta modelos de Switching y Routing para mejorar la configuracion lógica en las redes y garantizar sistemas más robustos, aplicables, seguros y sobre todo funcionales que dan solución a necesidades de comunicación entre redes.

Mediante el montaje, configuración y desarrollo del escenario 1, aplicamos la conceptualización y funcionalidad del protocolo BGP que mediante su interacción autónoma permite compartir información e interactuar con otros equipos siguiendo un proceso de continuidad con identificación de cada equipo enrutador para alcanzar el proceso de la red en general, es decir, este protocolo tiene la facilidad de dar continuidad una secuencia de los enrutadores que se relacionen entre sí, de ésta manera se puede agregar a la red cuantos enrutadores sean necesarios sin tener que modificar los servicios que ya se encuentren activos de la red principal.

El escenario 2, nos acercó más a conceptos de Switching mediante la creación de tablas de VLAN para la segmentación de servicios particulares de la red, acá se aplicó conceptos como interfaces troncales que son las que permiten la propagación de múltiples VLAN por las mismas tramas de conectividad, interfaces de acceso, éstas creadas para usuarios finales, donde se aterriza la VLAN propagada a través de la red que permitirá al usuario interesado de ese segmento compartir e interactuar con información particular sin conmutar con otros servicios, la adyacencia de Switch capa 2 no permite el Routing para la comunicación entre equipos de la red LAN y los usuarios finales, pero identificamos que al usar un equipo Capa 3 para tal fin se podría integrar el Switching con el Enrutamiento de la gestión y administración de los servicios para interconectarlos entre si y lograr una mejor comunicación teniendo acceso a todos los equipos relacionados en la red.

BIBLIOGRAFIA

Boix, R. (2002). Instrumentos de análisis de redes en economía urbana: Caracterización de redes de ciudades mediante el análisis de cuatro estructuras urbanas simuladas. Oviedo: V Encuentro de Economía Aplicada.

Border Gateway Protocol. (2019, 25 de junio). Wikipedia, La enciclopedia libre. Fecha de consulta: 19:17, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Border_Gateway_Protocol&oldid=116944498.

Conmutador (dispositivo de red). (2020, 18 de febrero). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:44, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Conmutador_(dispositivo_de_red)&oldid=123644479.

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

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

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

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

Encapsulación (redes). (2019, 6 de agosto). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:31, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Encapsulaci%C3%B3n_(redes)&oldid=118044480.

Enhanced Interior Gateway Routing Protocol. (2020, 10 de enero). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:28, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Enhanced_Interior_Gateway_Routing_Protocol&oldid=122645809.

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

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

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

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

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

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

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

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

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

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

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

IEEE 802.1Q. (2020, 21 de enero). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:26, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=IEEE_802.1Q&oldid=122942750.

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

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

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

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

Miranda, C. V. (2014). Redes telemáticas. Ediciones Paraninfo, SA.

Open Shortest Path First. (2019, 22 de diciembre). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:35, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Open_Shortest_Path_First&oldid=122207190.

Spanning Tree. (2020, 4 de marzo). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:41, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Spanning_tree&oldid=123997674.

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). Enterprise Internet Connectivity. 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). Implementing a Border Gateway Protocol (BGP). 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). Manipulating Routing Updates. 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

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

Telnet. (2020, 7 de marzo). Wikipedia, La enciclopedia libre. Fecha de consulta: 18:00, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=Telnet&oldid=124075840.

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg

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

VLAN Trunking Protocol. (2019, 30 de julio). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:54, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=VLAN_Trunking_Protocol&oldid=117869416.

VLAN. (2020, 26 de febrero). Wikipedia, La enciclopedia libre. Fecha de consulta: 17:51, mayo 12, 2020 desde https://es.wikipedia.org/w/index.php?title=VLAN&oldid=123853979.

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl

Wikipedia contributors. (2020, May 4). Routing. In Wikipedia, the Free Encyclopedia. Retrieved 17:39, May 12, 2020, from https://en.wikipedia.org/w/index.php?title=Routing&oldid=954840640