

Universidad Popular Autónoma del Estado de Puebla
Departamento de Ingenierías



Facultad de Tecnologías de Información

“Enrutamiento Para Conectividad De Access Point Name”

Trabajo Terminal:

Para Obtener El Grado De Licenciatura En
Ingeniería En Computación Y Sistemas

Presenta:

Raúl Alberto Ramírez Martínez

Director de Proyecto Terminal:

Dra. Alejandra Aldrette Malacara

Puebla, México

Julio, 2016



UPAEP – Secretaría General

Dirección General de Apoyos Académicos

Dirección del Centro de Recursos para el Aprendizaje y la Investigación.

Biblioteca Central - **Karol Wojtyla**

Tesis Digitales Restricciones de uso:

DERECHOS RESERVADOS ©

PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de textos, imágenes, gráficas, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente de donde la obtuvo mencionando el autor o autores involucrados en el documento.

Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS:

A mis formadores/as:

Por colaborar con mi formación académica.

A mi Asesora:

Por el tiempo, dedicación, paciencia y orientación en la elaboración de este trabajo.

DEDICATORIA

A mis Padres:

Carlos Raúl Ramírez Guzmán y Soledad Daria Martínez González, por sus consejos, apoyo incondicional, por motivarme constantemente para alcanzar mis metas, por enseñarme que con esfuerzo, trabajo y constancia todo se puede, por ser mi ejemplo a seguir, instruyéndome siempre por el camino de los buenos principios, por su amor y por ser los mejores padres.

A mi Hermana:

Karla Brenda Ramírez Martínez, por su apoyo incondicional, por siempre escucharme, aconsejarme y siempre estar conmigo.

INDICE

I.- INTRODUCCION	1
II.- OBJETIVOS	2
III.- ANTECEDENTES	3
IV.- PLANTEAMIENTO DEL PROBLEMA	4
V.- MARCO TEÓRICO.....	5
1.- REDES.....	6
1.1- LAN	6
1.2.- WAN	7
1.3. MAN	7
2.- RUTEO.....	8
2.1 - OSPF	9
2.2.- BGP	11
2.3. -HSRP	13
2.4. -Policy-Based Routing.....	14
2.5. - Virtual Routing and Forwarding.....	15
VI.- DESCRIPCION DEL TRABAJO	16
VII. - RESULTADOS	25
VIII. - CONCLUSIONES	27
IX. - BIBLIOGRAFIA.....	28

INDICE DE ILUSTRACIONES

FIGURA 1 . - ARQUITECTURA ACTUAL DE LA RED	4
FIGURA 2 . - ELEMENTOS OSPF	10
FIGURA 3 . - CONCEPTO IBGP Y EBGp	11
FIGURA 4 . - ROUTER REFLECTOR	12
FIGURA 5 . - HSRP	14
FIGURA 6 . - VRF	15
FIGURA 7 . - TOPOLOGÍA DE CONECTIVIDAD	17
FIGURA 8 . - COMUNICACIÓN DE OSPF	18
FIGURA 9 . - RUTEO CORE	21
FIGURA 10 . - PROCESO DE APLICACIÓN DE CONFIGURACIONES	26

INDICE DE TABLAS

TABLA 1.- DIRECCIONAMIENTO VLAN 56.....	19
TABLA 2. - DIRECCIONAMIENTO VLAN 57	19
TABLA 3. - DIRECCIONAMIENTO EQUIPOS TL_6500	21
TABLA 4. - DIRECCIONAMIENTO EQUIPOS RT_TL	23

I. - INTRODUCCION

Hoy en día la tecnología es una parte muy importante en nuestra vida diaria, ya sea para realizar tareas personales como revisar el correo, navegar en internet, o simplemente redactar un documento, por lo que hoy en día sería muy difícil imaginarnos sin esta herramienta, pero no sólo se ha vuelto indispensable para nosotros, también para las empresas se ha vuelto de gran importancia para su crecimiento, para realizar sus tareas diarias, la oportunidad de ofrecer nuevos servicios y la creación de nuevas oportunidades de trabajo.

Considerado esto, es que para una empresa es muy importante mantenerse conectada con todas sus sucursales, clientes y con el resto del mundo, por así decirlo tener una "red" de comunicación donde todos puedan acceder a recursos que se encuentren en diferentes lugares, automatizar procesos, comunicarse entre ellos y poder estar siempre actualizados.

En este trabajo se muestra uno de los muchos servicios que puede proporcionar una empresa de telecomunicaciones, en este caso la comunicación de dispositivos móviles con otras plataformas de la red o conexión a internet, así como también los diferentes tipos de protocolos de ruteo que se utilizan en la red para poder implementar esta comunicación.

En el capítulo II se mencionará brevemente el objetivo por el que se realiza el ruteo para la comunicación de los dispositivos móviles.

En capítulo III se explicará lo que es un Access Point Name, cómo funciona, los elementos que forman parte de él, así como las funciones que tienen cada uno de estos elementos que lo integran.

En el capítulo IV "planteamiento del problema" se detallarán los requerimientos solicitados por el cliente, así como cuál será la forma en que se resolverá esta solicitud.

En el capítulo V "Marco Teórico" se explicará la forma en que funcionan los protocolos que se utilizarán para realizar las configuraciones y lograr la comunicación deseada.

En el capítulo VI "Descripción del trabajo" se realizará la asignación de las vlans (Virtual LAN), direccionamiento Ip, protocolos de ruteo, así como también se detallará cómo estará conformada la topología de la red, y los equipos que estarán involucrados en las configuraciones.

En el capítulo VII "Resultados" se explicará cuál fue el resultado de la aplicación de las configuraciones en los equipos de la red y los procesos de validación una vez aplicadas estas.

En el capítulo VIII "Conclusiones" se mencionará porque hoy en día es muy importante el uso de esta tecnología, y la razón por la cual se decidió resolver la solicitud de esta manera, existiendo otras formas de realizar estas configuraciones.

II. - OBJETIVOS

Establecer enrutamiento de un APN (Access Point Name) para dispositivos móviles, mediante el uso de diferentes protocolos de ruteo entre los equipos de la red CORE IP, para lograr la comunicación con plataformas específicas de la red y conexión a internet.

A través de asignación de direccionamiento iP, Vlans y ruteo se realizará la comunicación entre los dispositivos móviles y los equipos de la red de datos, a lo que se llamara como el Backbone o el CORE, los cuales serán los encargados de proporcionar el camino que deben de recorrer los datos para que puedan tener comunicación los dispositivos móviles con las plataformas internas de la empresa o algún servicio que se encuentre en internet con el cual deseen tener comunicación.

III. - ANTECEDENTES

Los primeros sistemas de comunicaciones móviles empleaban tecnología analógica y estaban orientados esencialmente hacia la telefonía.

El paso hacia una segunda generación de telefonía móvil viene marcado por la migración hacia la tecnología digital, lo que le da la posibilidad de integrar los servicios de voz con una gran variedad de servicios de datos.

Debido al gran crecimiento que está existiendo en la actualidad en el uso de los dispositivos móviles y su necesidad de conectarse a internet y plataformas, el incremento en el uso de este tipo de implementaciones está creciendo de manera muy rápida, ya que antes los dispositivos que necesitaban tener conectividad a internet eran muy pocos, cada vez es mayor la necesidad de los usuarios de conectarse a la red cuando no se encuentra en casa o en la oficina así como desplazarse mientras lo utilizan.

Con la aparición de los dispositivos móviles, televisiones inteligentes, terminales de cobro etc. la necesidad para conectarse a internet ha aumentado por lo que también las redes han evolucionado, con el objetivo de dar respuesta a las necesidades de los usuarios surgió “IP Móvil” para extender el protocolo IP y adaptarlo al ámbito de las terminales móviles, con el uso de diferentes tipos de protocolos de ruteo y tecnologías que permiten la comunicación entre estos dispositivos móviles.

Los dispositivos de enrutamiento toman la decisión sobre la ruta que debe seguir un paquete hacia su destino final basándose en la dirección IP de destino que contiene el dispositivo móvil, por lo que todo dispositivo que desea acceder a los recursos de una red interna o externa debe contar con una dirección IP.

IV. - PLANTEAMIENTO DEL PROBLEMA

Para la implementación del ruteo del Access Point Name, se tiene que tomar en cuenta varios factores existentes dentro de la topología actual en la red. Actualmente dentro de la red CORE IP donde se necesita realizar el enrutamiento, existen otros APN's y servicios enrutados de diferentes clientes, así como servicios y plataformas propias de la empresa.

Se debe elegir qué tipo de enrutamiento se realizará (Dinámico o Estático), así como si debe ir dentro de la tabla de ruteo global o dentro de alguna VRF (Virtual Routing and Forwarding), ya que dentro de la red existen diferentes tablas de ruteo. Para la asignación de un pool de IPs dentro de la red se toma en cuenta para que tipo de servicio es, ya que las IPs se asigna según el tipo de servicio y dependiendo en que equipos se realizaran las configuraciones.

Para esta solicitud donde se desea tener comunicación con plataformas propias de la red y además contar con salida de internet, también se debe involucrar dentro de la implementación a la gerencia de Seguridad en particular al área de Gestion de Firewall, quienes que tendrá que aplicar las políticas, aplicar ruteo y aplicar un NAT (Network Address Translation) dentro de los Firewall, para poder tener la comunicación con IPs que no están dentro de la propia red.

A continuación se anexa un diagrama (ver Figura 1), donde se observa la topología actual de la red de CORE IP donde se necesita realizar el ruteo, para lograr la comunicación de los dispositivos móviles con las plataformas de la red e internet.

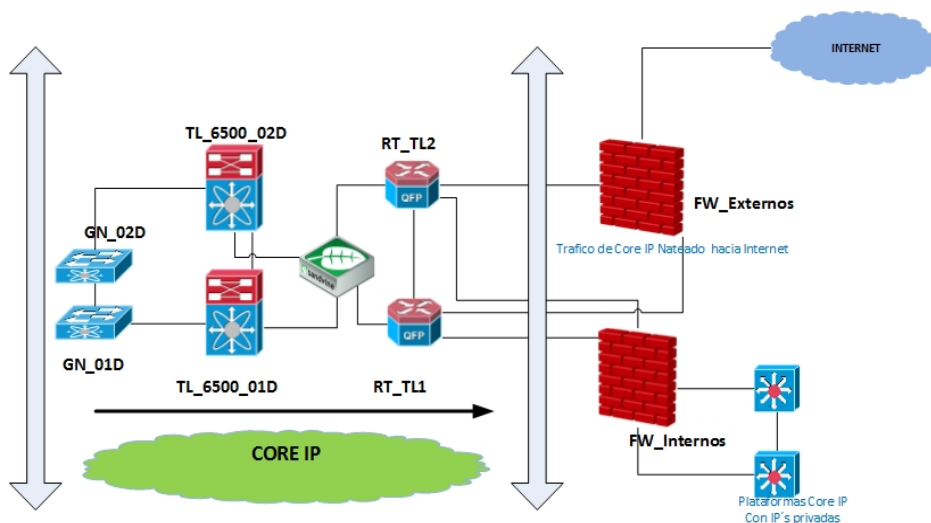


Figura 1. - Arquitectura Actual de la Red

V.- MARCO TEÓRICO

Para poder tener la comunicación deseada, se debe hacer uso de diferentes protocolos de comunicación, para hacer el ruteo necesario, entre ellos son OSPF, HSRP, BGP así como de rutas estáticas.

Por ello es que se dará una pequeña explicación de cómo funcionan estos protocolos.

¿Qué es un ACCESS POINT NAME?

Es el nombre que se le da a un punto de acceso o también por sus iniciales se le llama "APN", este puede Proporcionar Acceso a una Red pública de Datos (PDN) , una red Privada o Corporativa, además que puede proporcionar varios tipos servicios como Internet, o también para hacer uso de servicios específicos de alguna plataforma, esto haciéndolo mediante el uso de la red existente de la compañía ya sea mediante el uso de una red GPRS o una tecnología más rápida como 2G y 3G.

La estación Móvil se conecta con el SGSN el cual envía un mensaje de solicitud para establecer la conexión al GGSN, del cual obtiene la configuración necesaria para establecer la conexión solicitada y además podrá obtener una dirección IP válida mediante del DNS (Domain Name System) el cual se encarga de otorgar IPs a los dispositivos móviles, con la cual podrá acceder a los servicios que requiere.³

GGSN: Gateway GPRS Support Node, los APN son soportados por el GGSN, el cual es el encargado de responder la solicitud de los usuarios, brindándoles el establecimiento de la sesión solicitada, asignándoles una IP para el uso del dispositivo móvil.⁵

SGSN: Service GPRS Support Node, es el responsable de establecer la comunicación con el GGSN, por medio de un mensaje Packet Data Protocol (PDP), así como también el cifrado, comprensión y ruteo de datos hacia el GGSN.⁷

El APN está compuesto de 2 partes:³

- **Network ID:**
El identificador de Red, es una parte muy importante del APN ya que identifica a cual GGSN se conectara, esta parte es obligatoria.³
- **Operator ID:**
El identificador del operador es una parte opcional del APN, identifica la red móvil terrestre pública por su nombre en inglés "Public Land Mobile Network (PLMN)" en la que se encuentra el GGSN.³

Un protocolo de comunicación es un conjunto de reglas que especifican cómo se llevará a cabo el intercambio de datos u órdenes durante la comunicación de los dispositivos que conforman parte de la red.⁹

1.- REDES

Una red de computadoras o una red informática es un conjunto de equipos interconectados entre sí, por medios de cables, ondas, señales o cualquier otro medio de transporte de datos que sirven para compartir recursos, archivos, datos y servicios, tales como el internet, impresoras, bases de datos, archivos o simplemente juegos.⁹

Algunos de los objetivos de las redes es compartir recursos, para que cualquier nodo de la red que participe en ella pueda hacer de su uso cuándo lo solicite, por ello mismo otro de sus objetivos es contar con alta fiabilidad, es decir contar con fuentes alternas dentro de la red que puedan proporcionar el recurso solicitado y no depender solamente de un equipo.⁸

Las Redes se pueden clasificar según el tamaño de su cobertura y cantidad de usuarios conectados a ésta.

- LAN
- MAN
- WAN

1.1- LAN

Red de Área Local (Local Área Network), es una red que conecta dispositivos en un área relativamente pequeña en una única área geográfica, pueden ser dentro de una empresa pequeña, un campus o una casa.⁸

Una LAN por lo general es administrada por una sola organización, también puede compartir los recursos con cualquier otro dispositivo conectado a la LAN.

1.2. - WAN

Red de área Metropolitana (Wide Área Network), es una red que conecta varias redes locales (LAN), las cuales los miembros no se encuentran en una misma área geográfica, por lo cual una WAN es de gran tamaño y puede estar formada por una o varias empresas, o simplemente por el Proveedor de servicios de internet (ISP) para ofrecerle conectividad a sus clientes.

Una WAN se extiende por un área geográfica muy extensa y en ocasiones en un país, y su función es interconectar equipos que se encuentran ubicados a grandes distancias.⁸

1.3. - MAN

Red de Área Metropolitana (Metropolitan Área Network) es una red de alta velocidad que da cobertura a una área geográfica extensa conecta redes de 2 o más LANS pero que no se extiende más allá de la región.⁸

2. - RUTEO

Es la forma en como buscar todos los posibles caminos en una red de datos para llegar a un destino, no sólo consiste en saber llegar sino encontrar la mejor ruta para llegar al destino.

Los protocolos de enrutamiento proporcionan diferentes tipos de mecanismos para poder construir una tabla de enrutamiento que contenga la información de cómo llegar a los diferentes routers de la red, así como diferentes formas de determinar la mejor ruta para llegar al nodo remoto. Dentro de un ruteador pueden existir diferentes tipos de protocolos de enrutamiento a la vez.⁶

Enrutamiento Estático:

El principal problema del enrutamiento estático es mantener las tablas de enrutamiento actualizadas, ya que esto resulta en tener que introducir manualmente en todos los ruteadores de la red la información de cómo llegar de un router a otro⁶, imaginándonos que en una red de gran tamaño puede haber por lo menos 300 equipos.

Enrutamiento Dinámico:

Este tipo de protocolo dinámico mantiene las tablas de enrutamiento actualizadas por medio de mensajes de actualización que están configurados determinado cierto de tiempo, o cuando se presenta cambios en la topología de la red, indicándole al router que la información de sus tablas debe ser actualizada.⁶

A continuación se mencionan los protocolos de enrutamiento que se utilizarán para este proyecto.

2.1. - OSPF

Por sus siglas en ingles Open Shortest Path First, es un protocolo de enrutamiento jerárquico, que usa el algoritmo Dijkstra estado de enlace, para calcular la mejor ruta para llegar a su destino.

La medida que utiliza para determinar qué camino es el mejor para llegar a su destino es el *costo* el cual toma parámetros de medida, el ancho de banda y la congestión de los enlaces.¹

OSPF usa una jerarquía de áreas de 2 capas:

Backbone Área:

Será la que interconecte todas las áreas existentes dentro de la red, lo que quiere decir es que las rutas entre las diferentes áreas siempre tendrán que pasar por de esta, si no es posible que una NonBackbone área pueda conectarse al área 0 directamente, se puede crear un enlace virtual entre las áreas, para poder conectarse al Backbone.

Dos principales requerimientos para el área Backbone es que debe conectar todas las áreas que no son Backbone y que debe ser un área continúa.⁴

NonBackbone área:

Su función primaria es conectar usuarios finales y recursos, como lo mencionamos antes las áreas NonBackbone deben pasar por el área Backbone para poder lograr la comunicación con los demás usuarios finales de las demás áreas.⁴

Los Routers que participan en un mismo enlace eligen a un Router como el Designated Router (DR) y un Router Designado secundario (BDR) que actúa como backup, esto se hace para poder reducir el tráfico que puedan generar los mensajes de actualización entre los diferentes routers que participen en este proceso, y así el único encargado de enviar mensajes de actualización a todos los routers es el router DR.⁴

OSPF utiliza routers especiales con los cuales puede mantener la información de sus tablas más completa. En una topología multi-área se utilizan comúnmente los términos ABR Y ASRBR, como se muestra en la *figura 2*.

Routers fronterizos de área (ABR):

Este tipo de router mantiene la información completa de su área y conecta con otras áreas, permitiendo así rutear paquetes entre las diferentes áreas. Este router tiene interfaces conectadas en al menos 2 diferentes áreas de OSPF. ⁴

Router fronterizos de Sistemas autónomos (ASBR):

Es un ruteador que es el border con otros protocolos de Ruteo, es decir que tiene al menos una interfaz conectada a un área de OSPF y al menos una de sus interfaces conectada a un dominio diferente al de OSPF. ⁴

Router Internos:

Es un router que tiene todas sus interfaces conectadas a solo un área de OSPF. ⁴

Backbone Router:

Es un router que tiene al menos una de sus interfaces conectadas al área de Backbone. ⁴

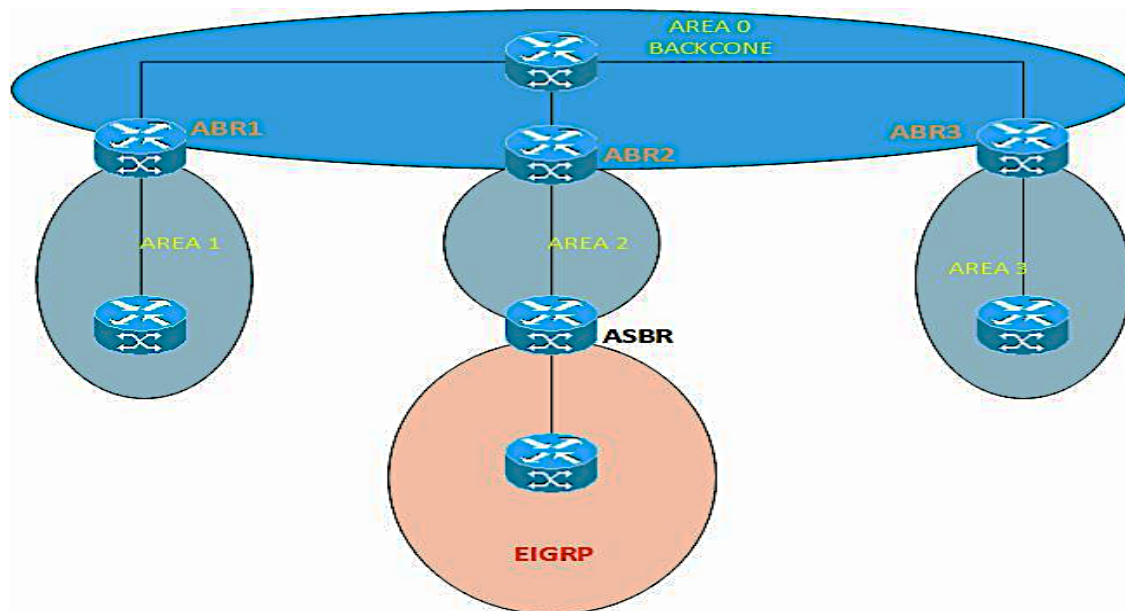


Figura 2 . - Elementos OSPF

2.2.- BGP

Es un protocolo de enrutamiento por vector distancia usado comúnmente para enrutar paquetes entre dominios. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos (SA).⁶

- Un Sistema Autónomo es un grupo de redes bajo una misma administración.

Aunque BGP es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un Sistema Autónomo como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP dentro de un mismo SA son denominadas BGP interno (iBGP), mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo (eBGP). Los routers pueden correr solo un proceso BGP a la vez.⁴ Podemos observar estos elementos representados en la *figura 3*.

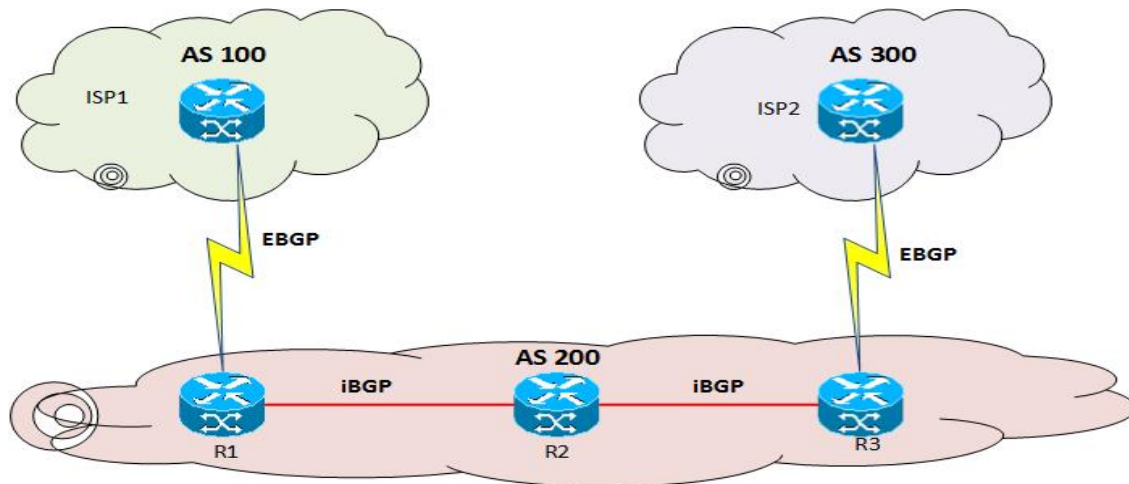


Figura 3 . - Concepto iBGP y eBGP

Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dice que son iguales BGP. En principio, los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Después de que los vecinos ya han intercambiado sus rutas, después de eso solo enviarán actualizaciones incrementales para propagar nuevas rutas.⁴

A diferencia de los protocolos de Gateway Internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda o retardo, en cambio BGP, toma decisiones de enrutamiento basándose en políticas de la red, número de

sistemas autónomos distintos por lo que tiene que pasar, en cuanto menor sea la distancia mejor será la ruta.¹

BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles.

BGP usa 3 tipos de base de datos, las 2 primeras son para BGP específicamente, la tercera es compartida por todos los procesos de ruteo existentes en el router.¹

Neighbor Database:

Es una lista con todos los vecinos de BGP configurados.¹

BGP Database:

Es una lista de todas las redes conocidas por BGP, con sus caminos y atributos.

¹

Routing Table:

Es una lista que contiene todas las redes conocidas por el router, así como el camino que deben tomar para poder llegar a ellas.¹

En topologías donde pueden existir más de 50 routers, el intercambio de rutas entre vecinos puede ocasionar que se congestione la red, es por eso que existe la opción de poder configurar un equipo como el Router Reflector y los demás como clientes, esto en lo que ayuda es que al haber un cambio en la red en un router configurado como cliente, este mande la actualización sólo al router reflector en lugar de mandar la actualización a todos los equipos existentes en la red, el router reflector se encargara de enviar la actualización ocurrida hacia todos los demás routers clientes (ver figura 4), esto ayuda a disminuir el número de mensajes enviados en la red así evitando la congestión que podrían ocasionar esta gran cantidad de mensajes.

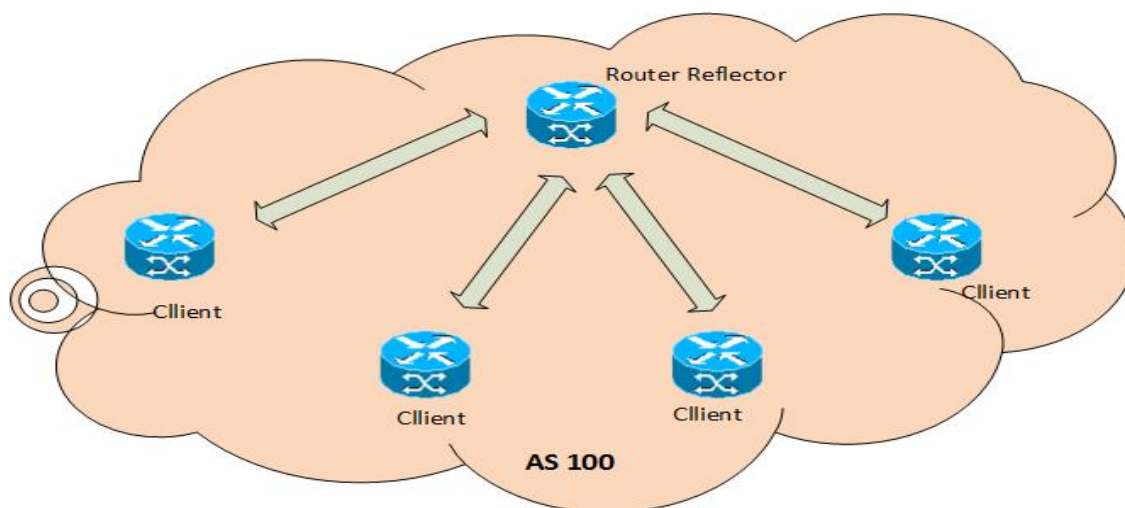


Figura 4. - Router Reflector

2.3. - HSRP

Hot Standby Router Protocol es un protocolo propiedad de Cisco que permite que varios routers o equipos multicapa, parezcan como un solo Gateway de iP. Lo que permite este protocolo es que se cuente con redundancia en los equipos de red, asignado la iP del Gateway a varios equipos que participan en un mismo grupo de HSRP. Para su funcionamiento, un Router es elegido como el primario o activo, otro es elegido como Standby Router, si además de estos 2 router existen más, los routers restantes se quedarán en el estado de “listen”.²

El Rango de grupo HSRP puede ser asignados de 0 a 255, recordando que los routers que participen en un mismo grupo deben tener asignado el mismo número de grupo.²

Para mejor administración de estos grupos, se recomienda que si se están asignando grupos de HSRP para vlans, el grupo de HSRP debe ser el mismo que el número de la Vlan.

Elección del Router Activo:

HSRP elige el router activo en base a la prioridad (0 a 255) que está configurada en cada router en el grupo. Por defecto la prioridad en cada router es de 100. El equipo que tenga la prioridad más alta será el router Activo del grupo. Si todas las prioridades de los routers es igual, entonces el router con mayor iP en la interface donde está el proceso de HSRP se volverá el Router Activo.²

Los routers intercambian paquetes de “hello” en un intervalo de 3 segundos, esto para descubrir la existencia de otro equipo así como para estar seguro de que el Router Primario sigue activo, si pasan 10 segundos sin recibir “hellos” del router activo esto indica que está “down”, entonces el router que está como Standby pasará a ser el router Activo. Normalmente cuando el router que estaba activo falla y el router Standby se vuelve el activo, el router que originalmente estaba como activo, no puede inmediatamente volver a ser el activo cuando se recupera de su falla, aunque este tenga la prioridad más alta. Para que esto pueda pasar y vuelva a ser el router activo se debe configurar con la opción “preempt”, lo que hace es que cuando se recupera de su falla, inmediatamente vuelve a tener el rol de activo.²

El modo en que se configura HSRP para que funcione, es que cada router en el grupo de HSRP tiene su propia y una única iP asignada a su interfaz, a la que se le llama iP física, y también cuenta con una iP Virtual que tiene en común los routers del grupo de HSRP, que es la que se asigna como Gateway iP, en el siguiente diagrama podemos observar el concepto de HSRP (ver *figura 5*).

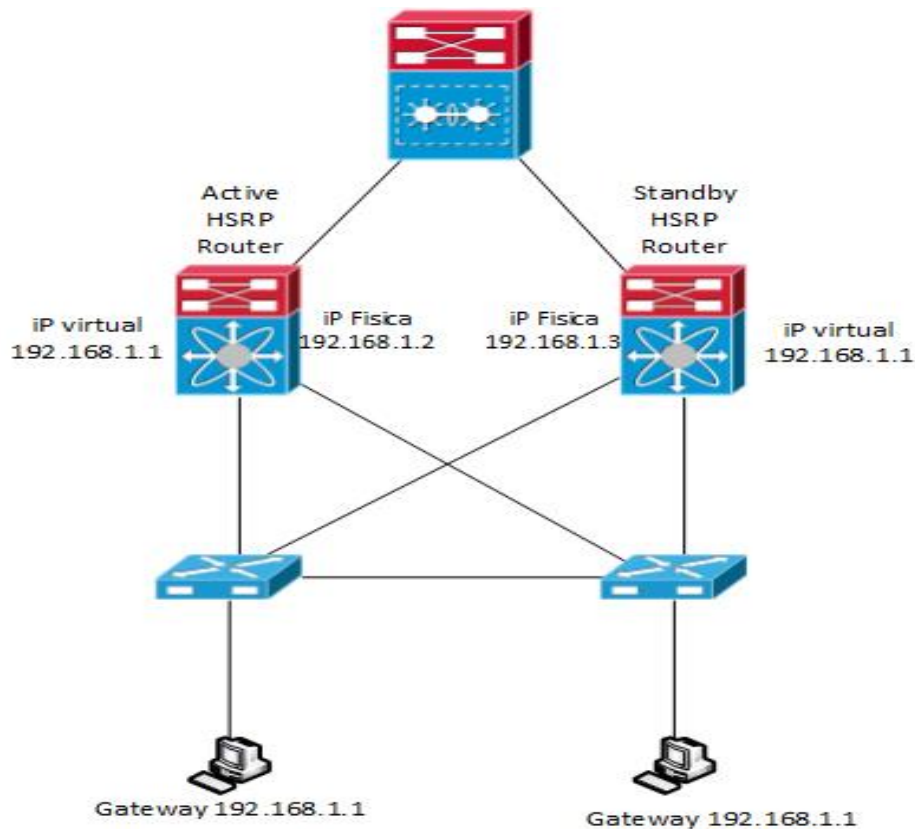


Figura 5.- HSRP

2.4. - Policy-Based Routing

Cuando un paquete llega a una interfaz del router, el proceso del router ejecuta varios pasos para procesar el paquete, se des encapsula el paquete para revisar que no contenga errores.

Cuando se descarta que no tenga errores, el router compara la iP destino del paquete con la tabla de ruteo existente, para poder así enviar el paquete basándose en su tabla de ruteo.¹

Policy- Based Routing (PBR) lo que realiza es que no hace caso del destino natural del siguiente salto a realizar basado en la tabla de ruteo, PBR intercepta el paquete después de su des encapsulación en la interfaz por la que ingresa, entonces PBR escoge como es que se enviará el paquete, usando los criterios establecidos cuando se configure el PBR, y no en base a la tabla de ruteo del router.

PBR escoge como enviar el paquete usando los criterios lógicos usados dentro del route-map y la lista de acceso, que se utilizan para filtrado de tráfico o manipulación de él.¹

2.5. - Virtual Routing and Forwarding

VRF (Virtual Routing and Forwarding) permite que un router soporte múltiples instancias de routers virtuales, esto permite que cada instancia tenga su propia configuración y sus propios procesos de ruteo.⁴ Al crear routers virtuales se crean diferentes tablas de ruteo para cada router virtual, lo que permite segmentar tráfico y controlar el camino que pueden tomar.

La capacidad de aislar una red de otra tiene muchos beneficios en la seguridad, ya que esto permite que se pueda separar tráfico, por ejemplo al separar tráfico de los empleados del tráfico de los visitantes, es muy importante porque se evita que pueda haber un riesgo de que un intruso pueda acceder a archivos privados de la empresa. Una representación de esta tecnología la podemos observar en la *figura 6*.

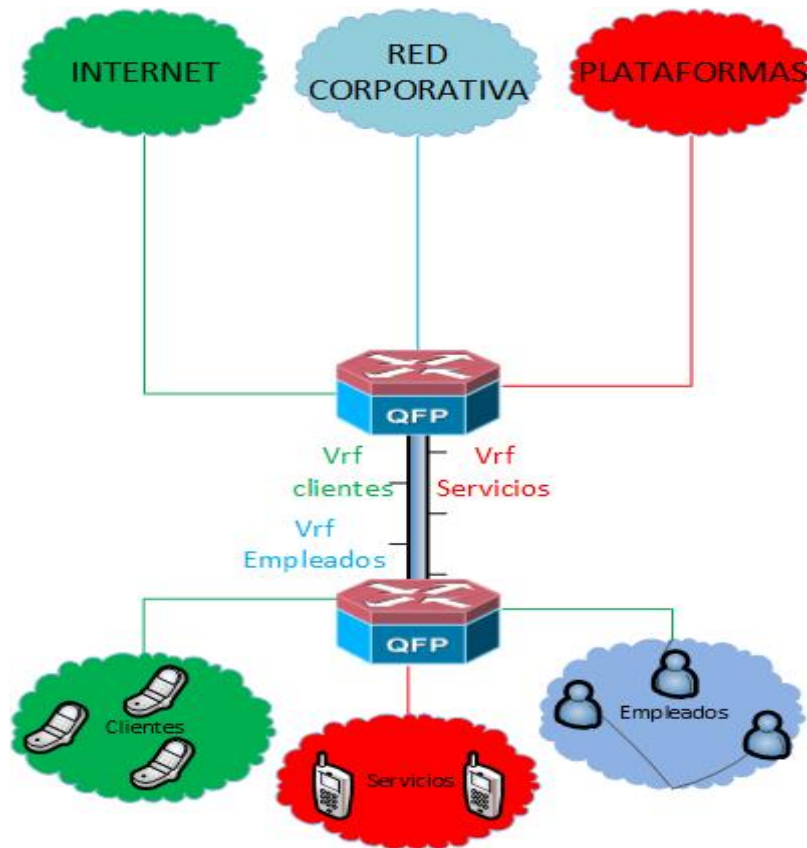


Figura 6. - VRF

VI. - DESCRIPCION DEL TRABAJO

Para la implementación del APN, se asignó al usuario un pool de IPs las cuales son las que utilizarán sus dispositivos móviles que tendrán salida a internet o acceso a plataformas de la red. Para ello el cliente solicito 30 IPs para sus dispositivos que utilizara.

Las IPs que se le asignaran estarán dentro del rango de IPs privadas, y pertenecerán a la VRF de clientes, para que estas no se mezclen con IPs existentes en la red interna del Backbone y también para separar trafico perteneciente a clientes con el tráfico existente de la red.

En base a lo solicitado el cliente, se le pudo haber asignado direccionamiento con capacidad de 32 IPs una máscara /27 que cuenta con dicha capacidad, pero se le asignó una máscara /26 con capacidad de 64 IPs considerando un posible crecimiento futuro en caso de requerirse, y en caso de que después el cliente solicite mas IPs, este proceso de asignación y ruteo sea más eficiente , debido a los procesos que se llevan en la empresa y así poder acelerar tiempo de respuestas a la solicitud del usuario.

El pool de IPs asignado al cliente fue el:

- **10.217.193.0 /26**

Lo que otorga un rango de IPs usables desde: 10.217.193.1 hasta la 10.217.193.254.

Para empezar con las configuraciones se mostrará un diagrama de la conectividad que existe entre el Equipo GGSN hasta los equipos de CORE , que son en los que se realizará el ruteo para lograr la conexión para la conectividad hacia internet, pasando antes por los Firewalls donde el área de gestión de Firewalls son los encargados de realizar la aplicación de las políticas donde se puede especificar que IPs son las permitidas en tener la conectividad a internet , además de los protocolos y puertos de los cuales pueden hacer uso, sin olvidarse también que dentro de los Firewall se realizara el NAT, asignándole a las IPs privadas del cliente una IP pública para que puedan salir a internet, ya que las IPs privadas no son ruteables en una red pública como internet. En el siguiente diagrama podemos observar la topología por donde cursara el tráfico de los dispositivos móviles (ver *figura 7*).

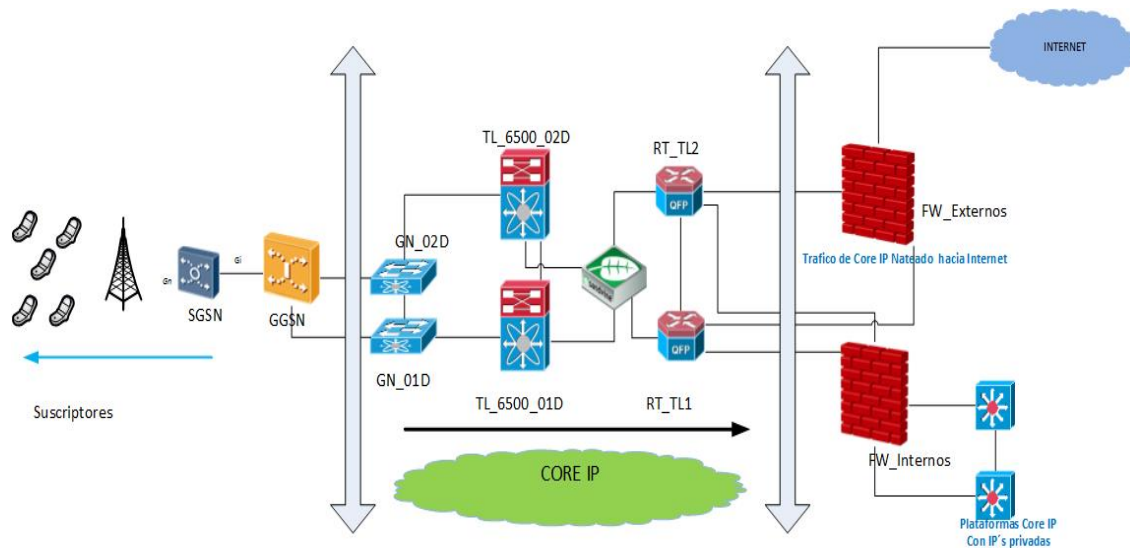


Figura 7 . - Topología de Conectividad

Primero lo que se necesita hacer es que los equipos de CORE que son el borde con el GGSN, tengan comunicación entre ellos para poder así nosotros conocer las IPs privadas asignadas que utilizarán los dispositivos móviles.

Para ello los equipos del CORE que son el TL_6500_01d y TL_6500_02d se comunican con el GGSN por medio del protocolo de ruteo OSPF, por lo que se debe lograr una vecindad con el GGSN para que por medio de este protocolo el GGSN nos anuncie las IPs de los suscriptores y nosotros anunciarle al GGSN el camino por donde tendrá que irse para su conectividad.

Para esto se asignó direccionamiento IP, vlans y procesos de OSPF de uso interno en los equipos del CORE, para conectar el GGSN con los equipos TL6500_01D y TL_6500_02D, y estos a su vez con los con los equipos RT_TL1 y RT_TL2, las vlans asignadas serán usadas para que por medio estas curse el tráfico del usuario, por lo que estas vlans serán propagadas en los equipos en capa 2 y capa 3.

Dentro de las vlans se usará el protocolo HSRP para brindar redundancia a la comunicación y en caso de que un equipo falle el otro asuma el rol de activo, es por eso que los equipos tiene el nombre 01D, 02D o TL1 y TL2.

En el siguiente diagrama se observan los equipos que estarán involucrados en el proceso de OSPF (ver figura 8).

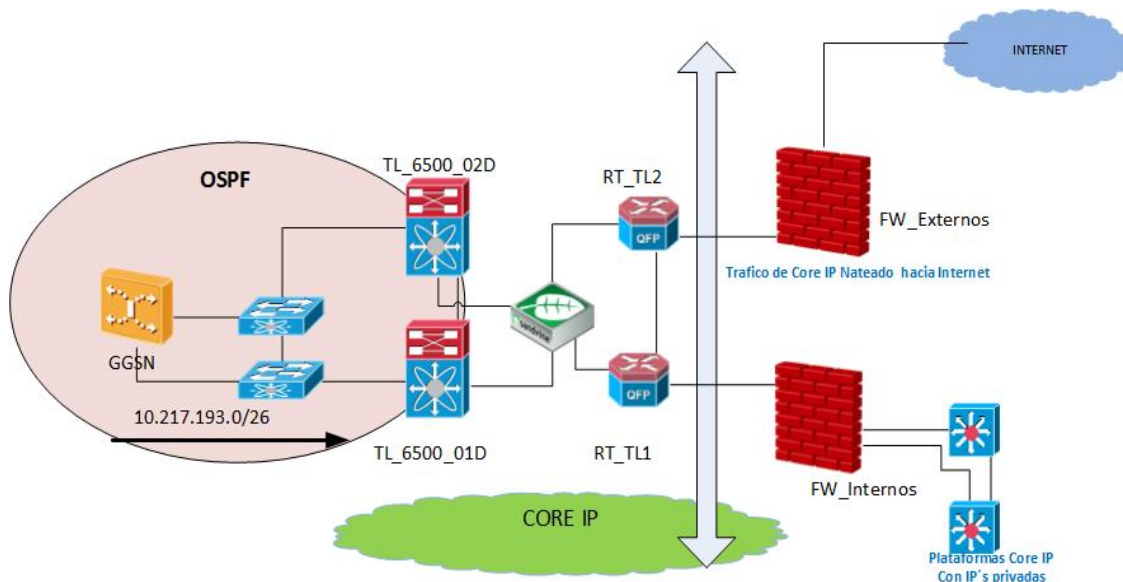


Figura 8 . - Comunicación de OSPF

A continuación se enlistan las IPs, vlans, proceso de OSPF grupo de HSRP etc. que se utilizaran:

VLANS:

- VLAN 56 nombre: APN_VIRUTAL_1.
- VLAN 57 nombre: APN_VIRTUAL_2.

Direccionamiento para las vlans.

- 10.223.187.0 /29
- 10.223.187.8/29

Grupos de HSRP:

- Grupo de HSRP: 56 para la Vlan 56.
- Grupo de HSRP: 57 para Vlan 57.

Nombre de la vrf:

- vrf APN_CLIENTES.

Proceso de BGP:

- 7428.

Primero se crean las vlans 56 y 57, son 2 para generar redundancia y se crean en ambos equipos TL_6500_01D Y 02, con su respectivo grupo.

Las 3 primeras IPs usables en ambas vlans se utilizarán en los equipos de CORE, recordando que la primera es usada para la red y la última para el broadcast.

En la *tabla 1 y 2*, podemos observar el direccionamiento asignado para las vlans 56 y 57.

Para Vlan 56:

IP virtual	iP Física equipo 01d	iP Física equipo 02d	Grupo HSRP	área OSPF	router-id
10.223.187.1	10.223.187.2	10.223.187.3	56	120	10.223.187.0

Tabla 1.- Direccionamiento Vlan 56

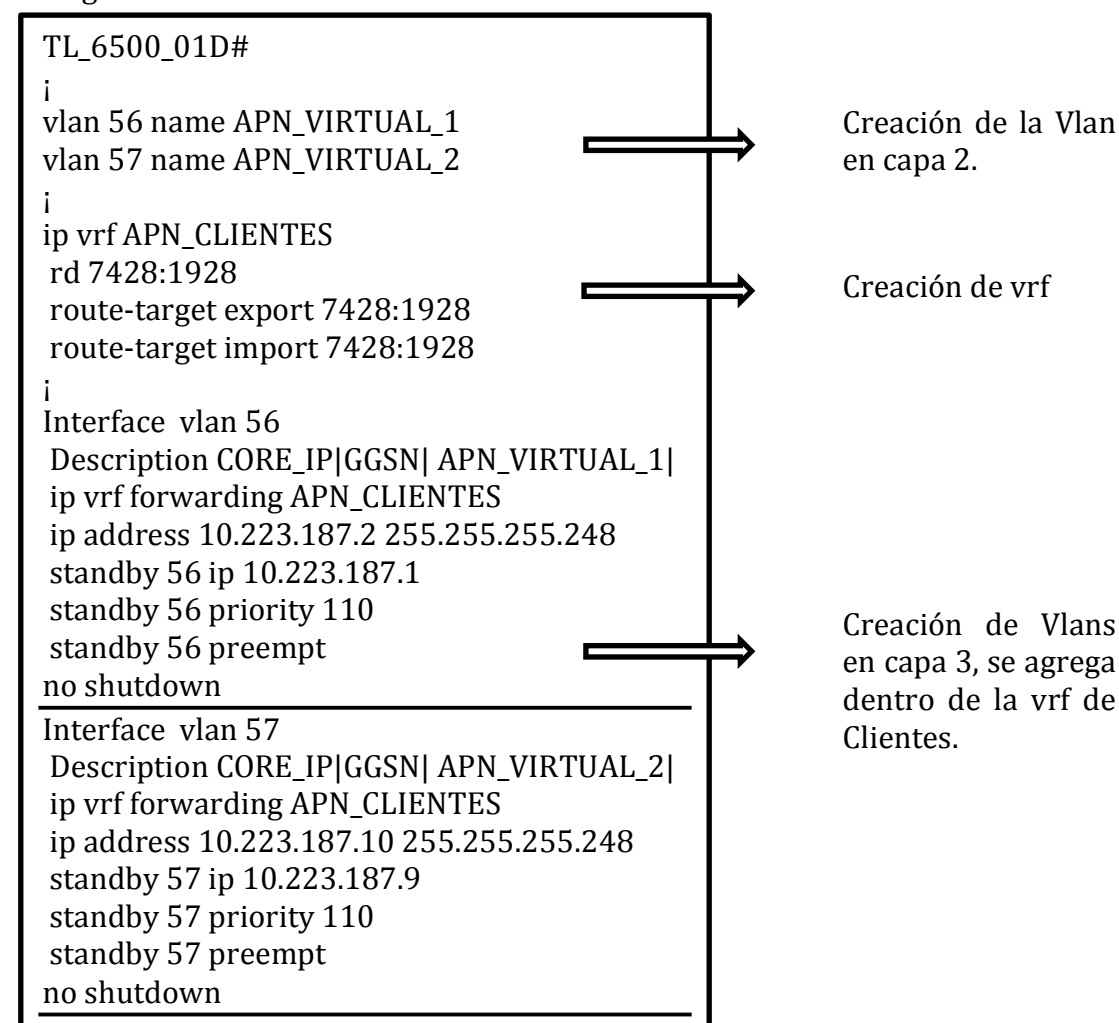
Para Vlan 57:

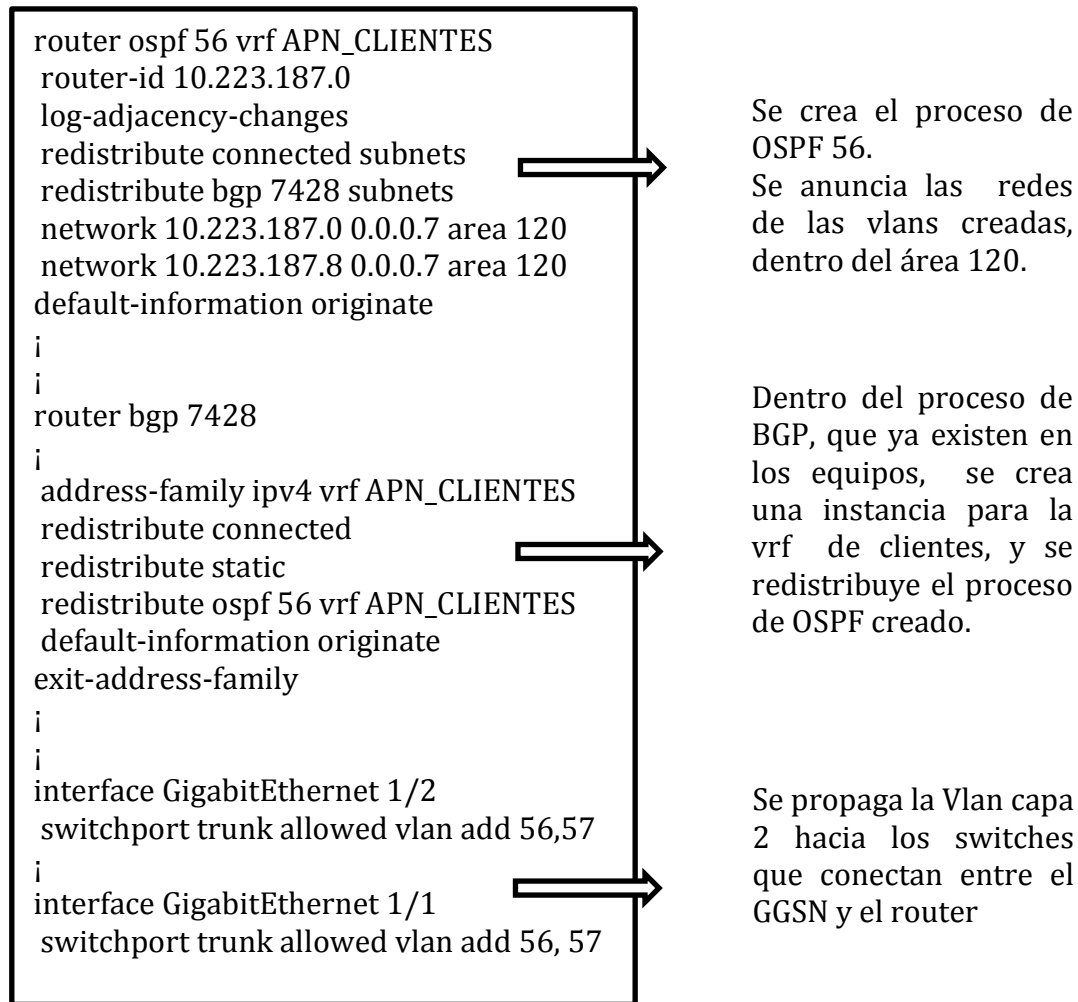
IP virtual	iP Física equipo 01d	iP Física equipo 02d	Grupo HSRP	área OSPF	router-id
10.223.187.9	10.223.187.10	10.223.187.11	57	120	10.223.187.0

Tabla 2. - Direccionamiento Vlan 57

Las IPs restantes en ambas vlans serán configuradas del lado del equipo GGSN, así también el equipo GGSN deberá configurar su proceso de OSPF en la misma área, ya que si no está en la misma área, la adyacencia entre los equipos no levantará y por lo tanto OSPF no logrará la comunicación.

Configuraciones:





Esta configuración se aplica también en el equipo TL_6500_02d, solo cambiando las IPs físicas de ambas vlans, asignándole la IP física que le corresponde, según las tablas 1 y 2.

Para el proceso de OSPF el router-id deberá cambiar a 10.223.187.8. Esto porque cada router debe tener un único router-id, si se llegara el mismo router-id en ambos routers, esto provocaría que se mostraran mensajes de log indicando una duplicidad, lo que causaría consumo de CPU en los equipos. Con esta configuración se conseguirá tener comunicación con el equipo GGSN, lo que hará esta comunicación, es que anunciara las IPs de los dispositivos móviles, para que así se conozca donde se encuentra este direccionamiento, así como también con esta comunicación se le anunciara al GGSN el camino por el cual tendrá la salida de internet, y la conexión a las plataformas de la red.

El siguiente paso es realizar el ruteo para la comunicación entre los equipos de CORE, es decir se realizara el camino que debe recorrer la conexión desde los equipos de CORE (TL_6500_01DY 02D) hasta la salida de internet y las plataformas.

A continuación se muestra un diagrama (ver *figura 9*), donde se puede observar los equipos donde debe pasar la comunicación.

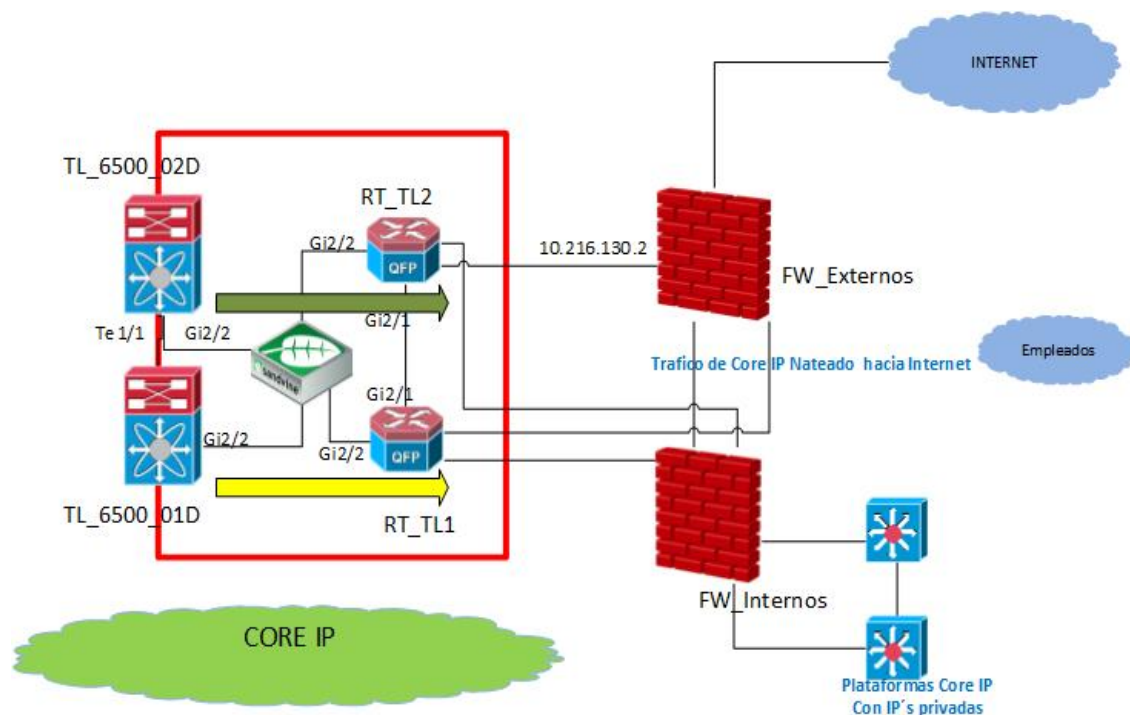


Figura 9. - Ruteo CORE

Para la interconexión de los 4 equipos involucrados, se asignó una Vlan y direccionamiento para esta.

- Vlan 59 nombre: interconexión_APN
- Direccionamiento: 10.223.187.16 /29

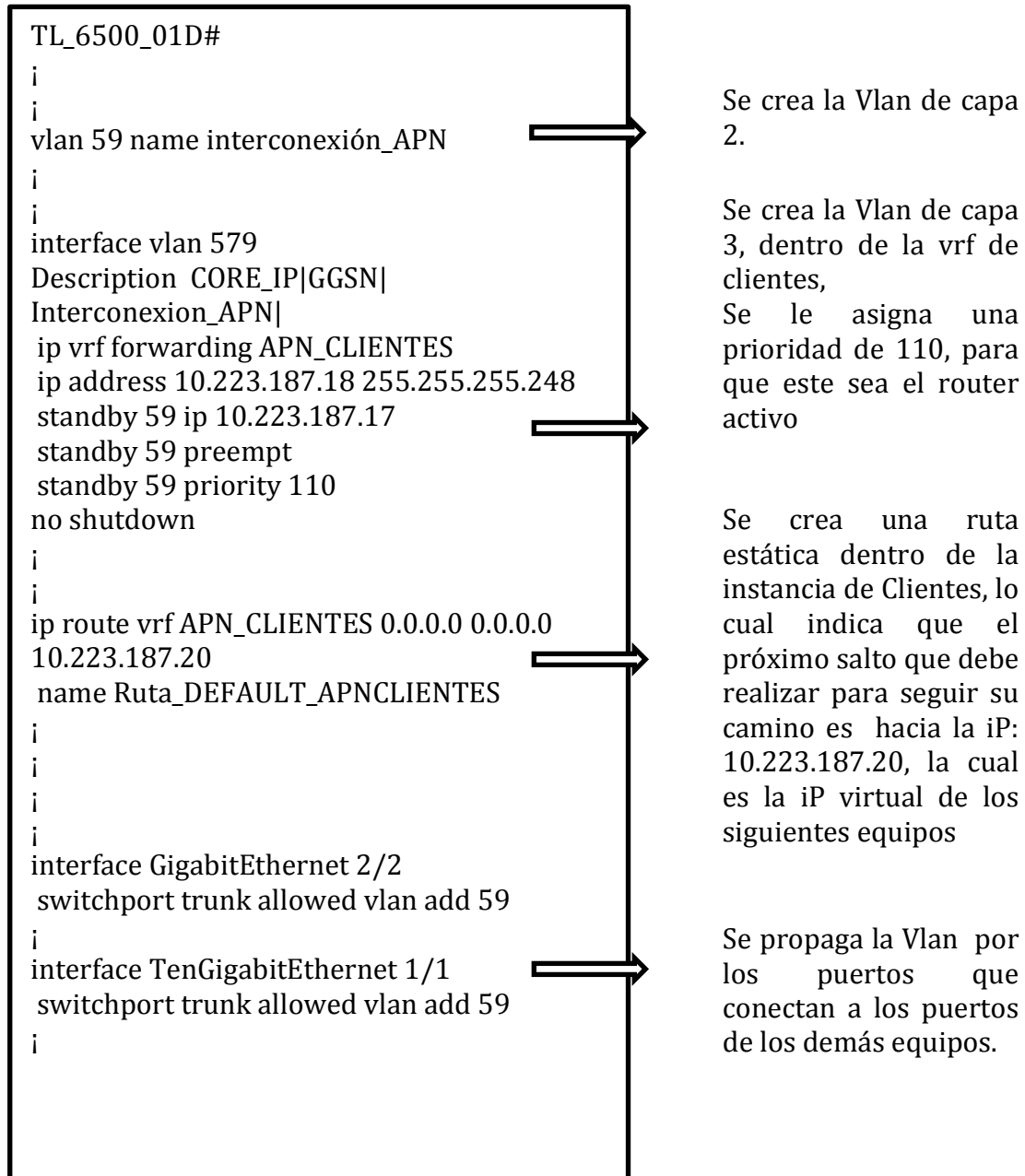
Quedando distribuido de la siguiente manera para los equipos TL_6500 (ver *tabla 3*):

Vlan	Equipo	Red	iP Virtual	iP Física	Grupo HSRP
59	TL_6500_01D	10.223.187.16	10.223.187.17	10.223.187.18	59
59	TL_6500_02D	10.223.187.16	10.223.187.17	10.223.187.19	59

Tabla 3. - Direccionamiento equipos TL_6500

Teniendo el direccionamiento para cada equipo, se realizarán las siguientes configuraciones en los equipos, empezando con los TL_6500.

Configuraciones:



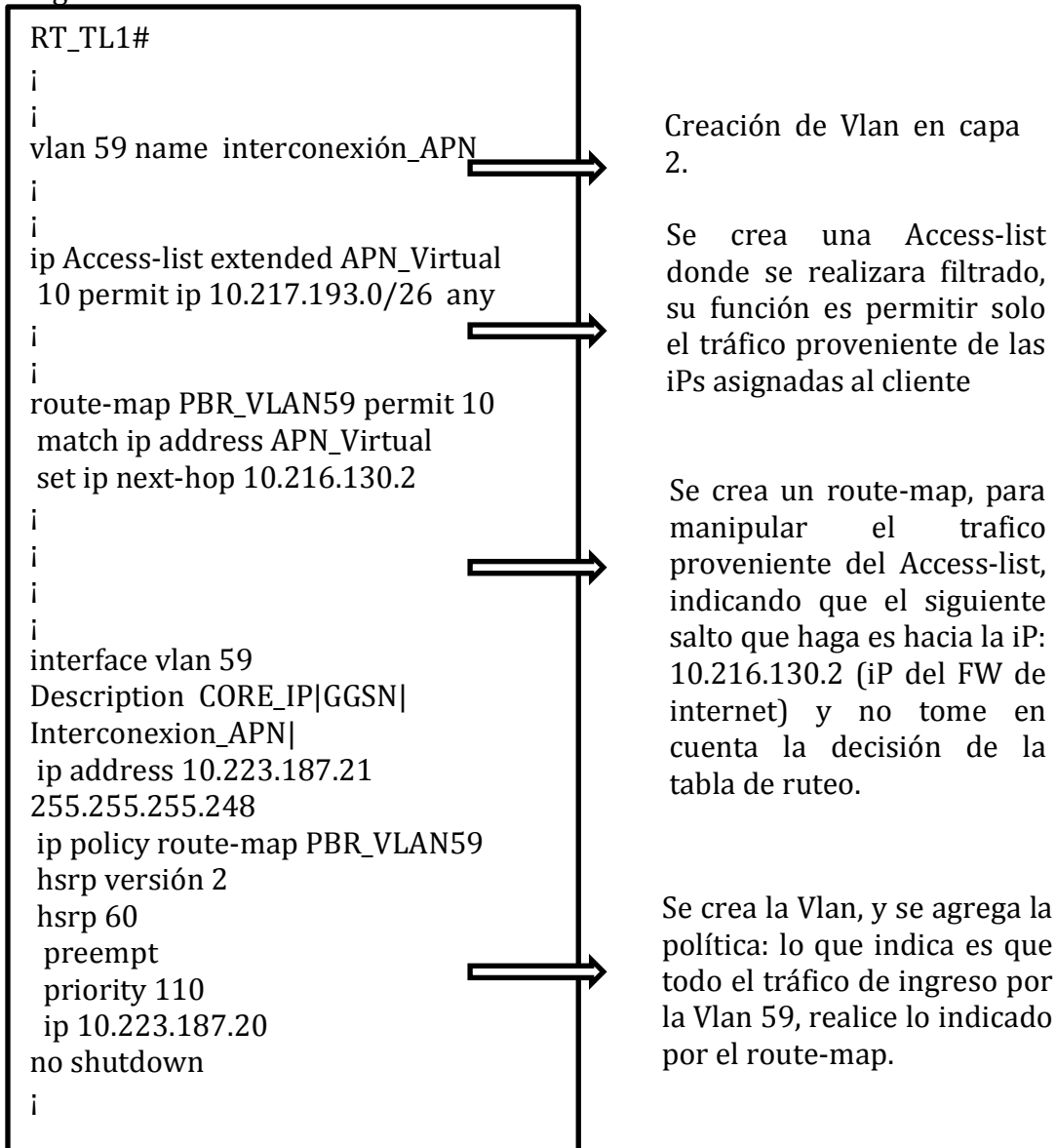
Para la configuración del equipo backup TL_6500_02D, es igual a la del master, sólo cambiando la IP física según como viene la tabla 3, y sin ponerle la prioridad de 110 al grupo de HSRP, ya que a este se le puso una prioridad más alta que la de default, para que fuera el router master.

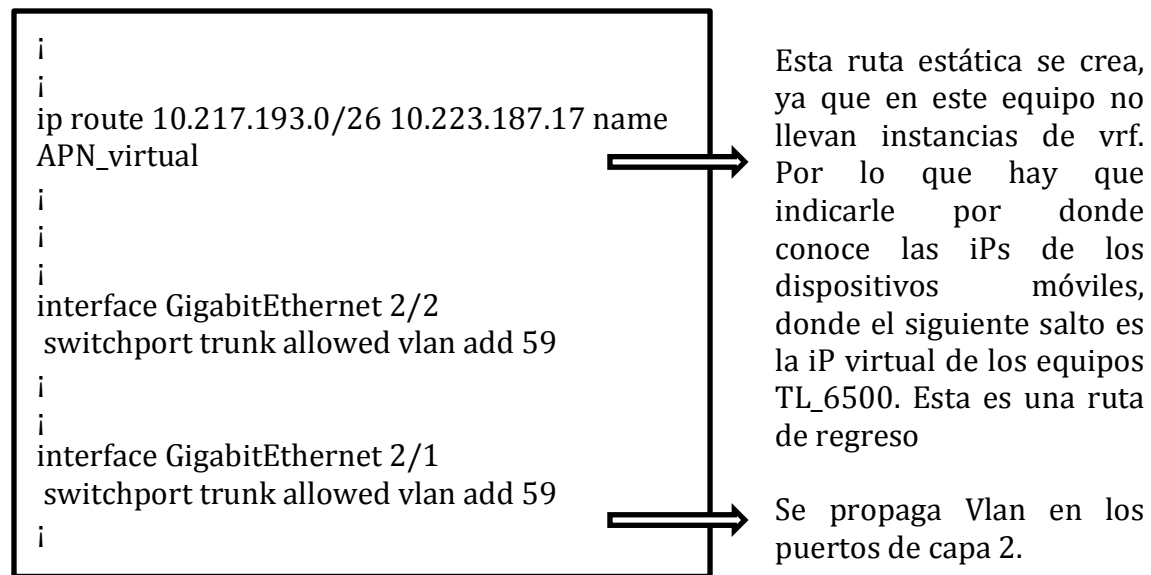
El siguiente paso será configurar los equipos RT_TL. Con el direccionamiento asignado a la Vlan 59, el cual quedo repartido de la siguiente manera (ver *tabla 4*):

Vlan	Equipo	Red	iP Virtual	iP Física	Grupo HSRP
59	RT_TL1	10.223.187.16	10.223.187.20	10.223.187.21	60
59	RT_TL2	10.223.187.16	10.223.187.20	10.223.187.22	60

Tabla 4. - Direccionamiento Equipos RT_TL

Configuraciones:





Esta misma configuración se aplica en el equipo de backup RT_TL2, sólo cambiando la IP física de la Vlan tomando de referencia la tabla 4 , así como también omitiendo la configuración de la prioridad, para dejarle la prioridad por default, para que el equipo RT_TL1 sea el master.

Con el route-map creado se especificó que todo el tráfico proveniente de las IPs asignadas al cliente, se mande a la dirección IP: 10.216.130.2, la cual pertenece al firewall que da la salida a internet, una vez las configuraciones correspondientes al firewall serán realizadas por el área de gestión de firewall, que serán los encargados de realizar el NAT, y aplicar las políticas indicado que puertos o protocolos se permitirán para esta comunicación.

VII. - RESULTADOS

Al dar inicio a la actividad de configuración del ruteo del APN en los equipos de red, se realiza una conferencia telefónica con las áreas involucradas en la actividad, así como también con el cliente. La realización de la actividad se ejecuta en horario nocturno (ventana), que es el horario permitido para realizar cambios en la red, ya que es cuando menos tráfico cursa por esta, por este motivo se lleva a cabo en este horario por si existe alguna afectación en el tráfico de datos, se evita que el impacto en la red sea menor. Al momento en que el área de OPERACIONES iP termina de aplicar las configuraciones de los scripts en los equipos de datos, se realiza las validaciones de que el proceso de OSPF formen adyacencia con los equipos vecinos, el ruteo funcione correctamente y el protocolo de HSRP haya convergido de manera correcta. Al comprobar que todos los protocolos se comunican correctamente y que no se presentaron fallas, como resultado de las pruebas realizadas se dan por exitosas las configuraciones aplicadas en la red de datos CORE IP.

Por consiguiente el cliente procede a efectuar pruebas de conectividad entre sus dispositivos móviles y los equipos de la red CORE IP, al llevar a cabo sus pruebas de conexión a internet, y comunicación con las plataformas deseadas, logra obtener la conectividad deseada, la actividad se da por concluida como exitosa.

En caso de que el enrutamiento del APN solicitada por el cliente no fuera exitoso, se tendría que aplicar ROLLBACK, lo cual es borrar las configuraciones aplicadas en los equipos, y dejarlos tal y como estaban antes de empezar la actividad, y se tendría que reprogramar la actividad para otra fecha y hacer las modificaciones al script si es que tuviera errores, lo cual atrasaría mucho el tiempo de implementación de la solicitud del cliente

Basado al trabajo realizado para el enrutamiento del APN y con las pruebas realizadas con el cliente durante la actividad, se pudo concluir que el enrutamiento realizado fue exitoso ya que se consiguió la comunicación entre los dispositivos móviles del cliente con las plataformas de la empresa y comunicación con internet, y que además el cliente quedo satisfecho con la pronta solución a su solicitud ya que la conexión de sus dispositivos móviles se pudo llevar a cabo en solo una actividad y no hubo rollback's que retrasaran su proyecto.

Como se muestra en el diagrama (ver *figura 10*) podemos observar el proceso que se lleva a cabo en la actividad, para aplicar las configuraciones y validar que la actividad sea exitosa.

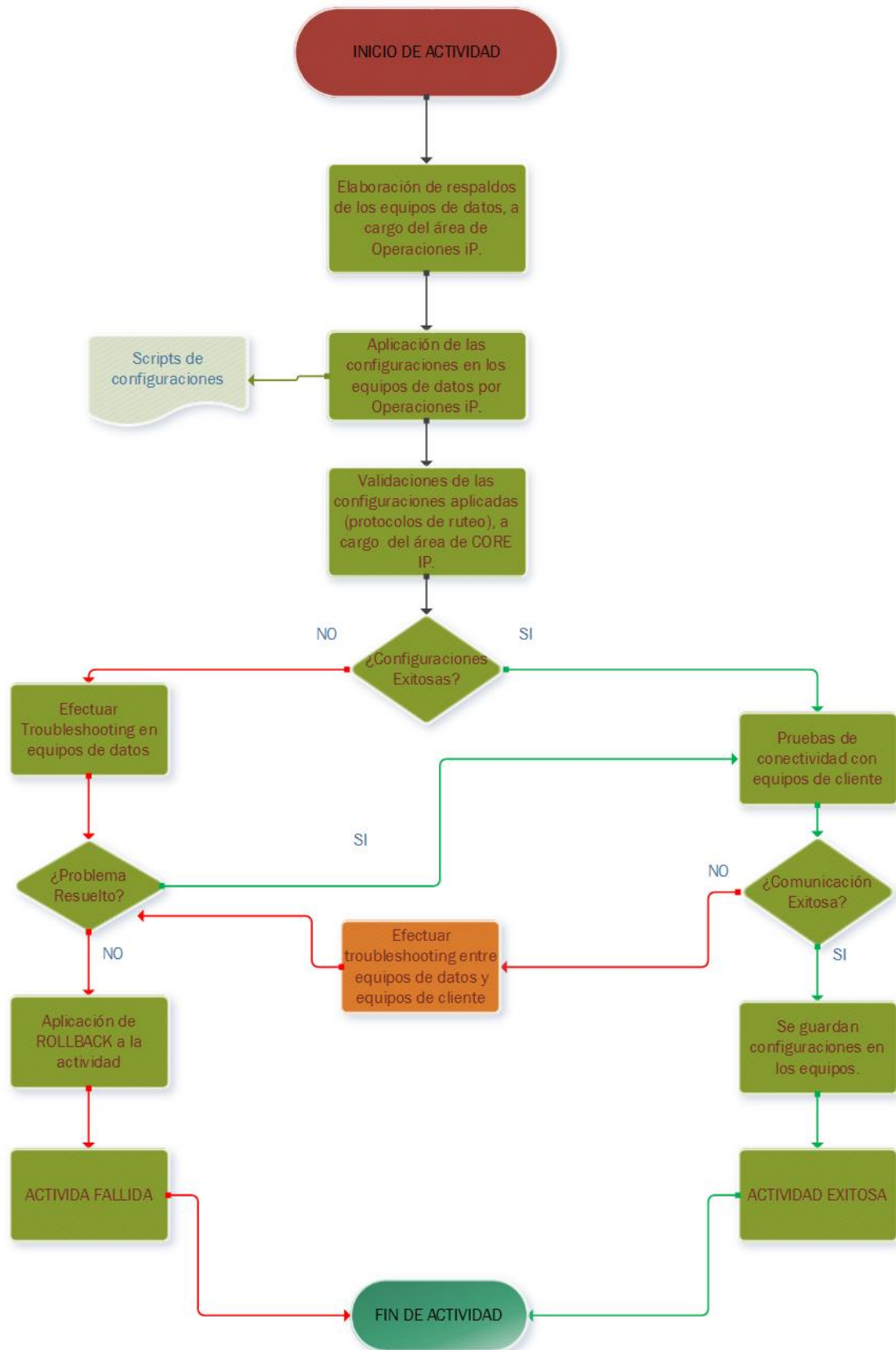


Figura 10 . - Proceso de aplicación de Configuraciones

VIII. - CONCLUSIONES

Actualmente en todo el mundo es muy importante mantenerse comunicado e informado, por lo cual la tecnología se ha vuelto muy importante en nuestra vida. Es por eso que hoy en día es imprescindible mantenerse actualizado en las nuevas tecnologías, ya que éstas se actualizan constantemente, y más con la aparición del internet el cual ha sido un gran detonante en nuestra sociedad, ya que la mayoría de los dispositivos que usamos se conectan a internet y hacen uso de direcciones IP para lograr su comunicación, las cuales se están terminando, es por eso que para enrutar el APN, se usa direccionamiento privado, y solo se le asigna una IP publica a la cual se le aplica un NAT para que pueda representar a todo el pool de direcciones asignadas dentro de Internet.

Otra manera en que se podría resolver esta solicitud de APN, es que en lugar de utilizar ruteo dinámico, se utilizara ruteo estático, pero esto no es una buena práctica ya que se tendría que poner rutas estáticas en cada equipo, y al utilizar el ruteo estático en los equipos, estos no comparte su tabla de ruteo con los demás equipos, y en caso de que ocurra alguna falla en la red, los routers no tienen la capacidad de reacción ante la falla y se podría perder la comunicación entre ellos, y se tendría que realizar el enrutamiento manualmente para resolver la falla presentada, lo cual podría llevar mucho tiempo encontrar el problema en una red amplia.

Es por este motivo que se usa enrutamiento dinámico, ya que en caso de alguna falla o algún cambio en la red, la convergencia de la red se realizaría más rápido y no se necesitaría intervención manual, ya que la convergencia se haría de forma automática.

IX. – BIBLIOGRAFIA

1. - Kevin Wallace. (2015). CCNP Routing and Switching ROUTE 300-101. Indianapolis: Cisco Press.
2. - David Hucaby. (2015) CCNP Routing and Switching SWITCH 300-115. Indianapolis: Cisco Press.
3. - Cisco Systems, Inc. (2011). CISCO GGSN Release 9.0 Configuration Guide, San Jose, CA: Americas Headquarters.
4. - Denise Donohue, (2015) Routing and Switching, ROUTE 300-101 Quick Reference, Indianapolis: Cisco Press.
5. - <https://supportforums.cisco.com/es/discussion/11358361>
6. - http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
7. - <http://es.slideshare.net/lonely113/general-packet-radio-service-10642934>
8. - <http://www.redusers.com/noticias/que-es-una-red-informatica/>
9. - http://www.ecured.cu/Red_de_computadoras