UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Propuesta de solución para alta disponibilidad y balanceo de tráfico en GGSN/ PGW en una red celular.

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniera en Telecomunicaciones

P R E S E N T A

Samanta Magali Rivera Cruz

ASESOR DE INFORME

Juventino Cuellar González

Ciudad Universitaria, Cd. Mx., 2018

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 OBJETIVO

Este trabajo muestra mi desempeño como profesional en el diseño e implementación de proyectos, así como el desarrollo de los conocimientos aprendidos a lo largo de la carrera Ingeniería en Telecomunicaciones.

El objetivo de este trabajo profesional es presentar una propuesta realizada a un operador celular con el fin de brindarle una solución que contempla alta disponibilidad y balanceo de tráfico en sus elementos GGSN (Gateway GPRS Support Node) / PGW (Packet Gateway) [1], según la tecnología de tercera o cuarta generación celular, utilizando equipos F5 por medio de los módulos de LTM (Local Traffic Manager) y GTM (Global Traffic Manager).[2]

Al pertenecer a una empresa encargada de ofrecer soluciones tecnológicas, era necesario analizar y comprender las necesidades y oportunidades de negocio en la infraestructura de un cliente.

En base a eso, se encontró este punto de falla que no permitía una conmutación automática en uno de los elementos más importantes de la red, elemento encargado del ruteo hacia las redes externas e internas, así como del procedimiento que permite establecer una sesión de datos. Adicional se buscó ofrecer características adicionales que hicieran la diferencia con las soluciones que ofertaban otros proveedores.

[1] Para más información, véase Antecedentes
[2] El equipo F5 será explicado más a fondo en el subcapítulo 4.4

2 INTRODUCCIÓN

Una de las grandes necesidades en la actualidad para toda empresa u organización que haga uso de las tecnologías de la información es garantizar la alta disponibilidad en la operación de una compañía.

Para casos específicos, como proveedores de servicios, u operadores móviles de red, cada minuto de indisponibilidad puede afectar la confiabilidad de sus clientes, así como conllevar grandes pérdidas monetarias y sanciones administrativas

En una red celular, el GGSN/ PGW, según la tecnología ocupada, es un elemento de gran importancia, ya que desempeña la función de punto de enlace para distintos APNs (Access Point Name)3, otorga el direccionamiento a las terminales móviles, gestiona diversas políticas de cobro y facturación y de igual forma desempeña la funcionalidad de router o punto central de conexión entre el interior y el exterior de la red.

La propuesta de solución garantiza la alta disponibilidad mediante el monitoreo de los GGSN/PGW a través del protocolo GTP (GPRS Tunneling Protocol), al mismo tiempo que realizará balanceo de tráfico según la localización geográfica.

El equipo F5, puede equiparse con diversas funcionalidades de acuerdo a los módulos con los que se configure. El módulo de LTM nos permite el balanceo de carga y es el más común de la marca. Para este proyecto en particular, se implementó también el módulo GTM, modulo que está referido al protocolo DNS4 y es de esta forma que el monitoreo de los GGSN/PGW se ejecuta.

GPRS es un sistema celular que principalmente se basa en DNS, ya que este es el encargado de asignarle una dirección IP a los APN, y esta dirección es la que apunta a los GGSN/PGW.

[3] Véase en la sección 4.2.
[4] Véase sección GPRS y la explicación del elemento DNS

3 TRABAJO PROFESIONAL

3.1 DESCRIPCIÓN DE LA EMPRESA

La empresa en la que me desempeñe profesionalmente forma parte de un grupo originario de Perú, y que actualmente tiene presencia en diversos países de América Latina, es una empresa vanguardista en las tecnologías de la información que tiene asociaciones con líderes en producción de equipos de tecnología, marcas como CISCO, F5, BLUECAT, BARRACUDA, PALO ALTO, FORTINET, CITRIX, METASWITCH, VMWARE entre otras. En el área de las tecnologías de la información se caracteriza como una empresa vendedora de soluciones.

Su principal función es brindar a sus potenciales clientes propuestas de soluciones que busquen cubrir sus necesidades o nuevos requerimientos mediante la implementación de productos de las marcas antes mencionadas.

Mediante personal capacitado en los diferentes productos y tecnologías, ha logrado vender soluciones a importantes empresas del país, como proveedores de servicios, operadores móviles, entre otros.

3.2 MISIÓN DE LA EMPRESA

"Somos un grupo internacional que ofrece servicios de tecnología de la información con oficinas en Perú, México, Ecuador, Chile, Brasil y EEUU. Nos especializamos en tecnología aplicada que impulsa el progreso y ayuda a las organizaciones a prepararse para el futuro.

Somos partners de marcas líderes como Cisco, F5, Citrix, Bluecat, Airwatch, Bluecoat, Thales, RSA, entre otras. Nuestra práctica en la implementación de proyectos de tecnología de la información nos ha permitido desarrollar una experiencia de más de 23 años en diversos sectores a lo largo de distintas regiones, ofreciendo y garantizando soluciones prácticas y viables en casi todos los rubros del negocio: telecomunicaciones, banca, seguros, salud, minería, construcción, energía, pesquería, comercio y otros.

Nuestro personal capacitado y experimentado identificará sus necesidades para brindarle la mejor solución integrada para potenciar la productividad de su empresa y así obtener resultados concretos y positivos frente a los desafíos de negocio que enfrentan las compañías hoy en día." [5]

3.3 DESCRIPCIÓN DEL PUESTO

En la empresa desempeñe el puesto de Ingeniero de Soporte e Implementación, entre mis funciones estaban:

[5] Misión de la empresa obtenida de la página oficial de la compañía.

- ✓ Diseñar soluciones para satisfacer las necesidades o requerimientos de un cliente mediante los productos en los que se tiene capacitación.

- ✓ Ejecutar Demos, con las soluciones propuestas, en infraestructura del cliente y en ambientes.

- ✓ Formar parte de las brigadas encargadas de dar soporte 24X7 de primer nivel, hacer troubleshooting nivel 1 y buscar la solución de cualquier eventualidad.

- ✓ Implementación de equipos (Site Survey, Cableado y etiquetado, Pruebas de Red, Configuración del Proyecto, ATPs)

- ✓ Capacitarme en diferentes tecnologías y ser especialista, con el fin de ser capaz de ofrecer soporte en primer nivel.

4 ANTECEDENTES

4.1 HISTORIA DE LA TELEFONÍA MÓVIL CELULAR

La telefonía inalámbrica ha tenido gran aceptación a lo largo del tiempo, esta ha evolucionado al paso de los años, cambiando sus características, y mejorando algunas de las funcionalidades de la red, así como los elementos que la conforman.

Cuando recién empezó la telefonía a través de señales de radio, el servicio no presentaba la eficiencia que presentan los operadores en la actualidad, había problemas de interferencia y poca disponibilidad de canales, debido a que la utilización del espectro era ineficiente para la capacidad de troughput que demandaba la población.

El término celular se empezó a utilizar cuando el servicio comenzó a ofrecerse mediante celdas que permitían la reutilización de frecuencias, las células ofrecen algunos beneficios, como la posibilidad de usar transmisores de menor potencia y la optimización del espectro.

La evolución de la tecnología celular se clasifica por generaciones, véase Figura 1; aunque este trabajo profesional es funcional a partir de la generación 2.5, se hará una breve introducción de las características de cada una, ahondando más en los sistemas y elementos de red más relevantes para esta propuesta de solución.

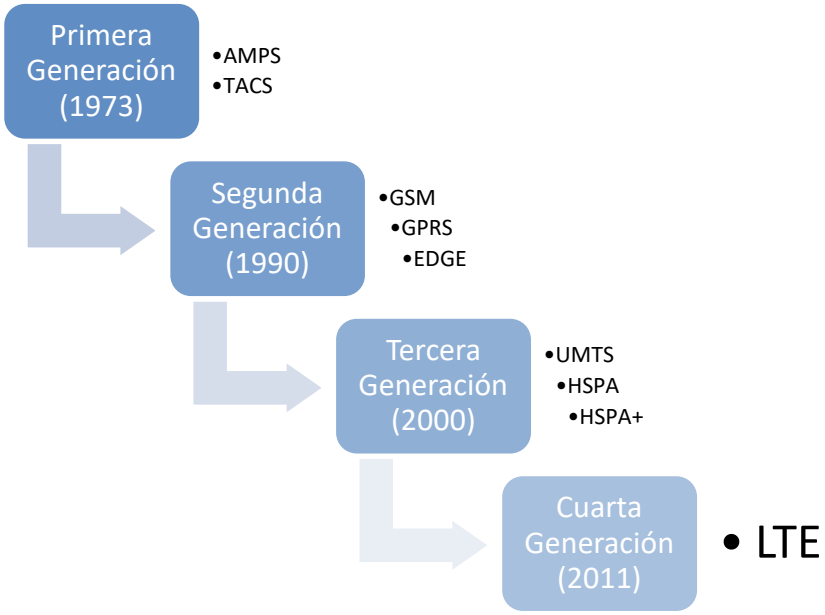

Figura 1.Evolución de la telefonía Móvil[6]

[6] Imagen de elaboración propia.

4.1.1 PRIMERA GENERACIÓN

La primera generación de telefonía móvil se caracterizaba por ser de carácter analógico, se basó en un conjunto de celdas o células interconectadas. Establece las bases y estructuras de los futuros sistemas como el roaming (Capacidad de cambiar de área de cobertura a otra sin perder señal) y el handover (Transferencia entre estaciones base) entre células. Esta generación utilizaba la técnica de FDMA.

Aunque representó grandes avances en la telefonía, aún contaba con varias desventajas considerables como: baja velocidad de transmisión, limitada capacidad con relación al número de suscriptores, alta necesidad de potencia, no contaba con seguridad y la calidad se consideraba deficiente.

La tecnología de la primera generación fue la AMPS (Advanced Mobile Phone System), se desarrolló en los laboratorios Bell, y entro en funcionamiento en 1979. Un ejemplo de esta arquitectura se muestra a continuación en la Figura 2

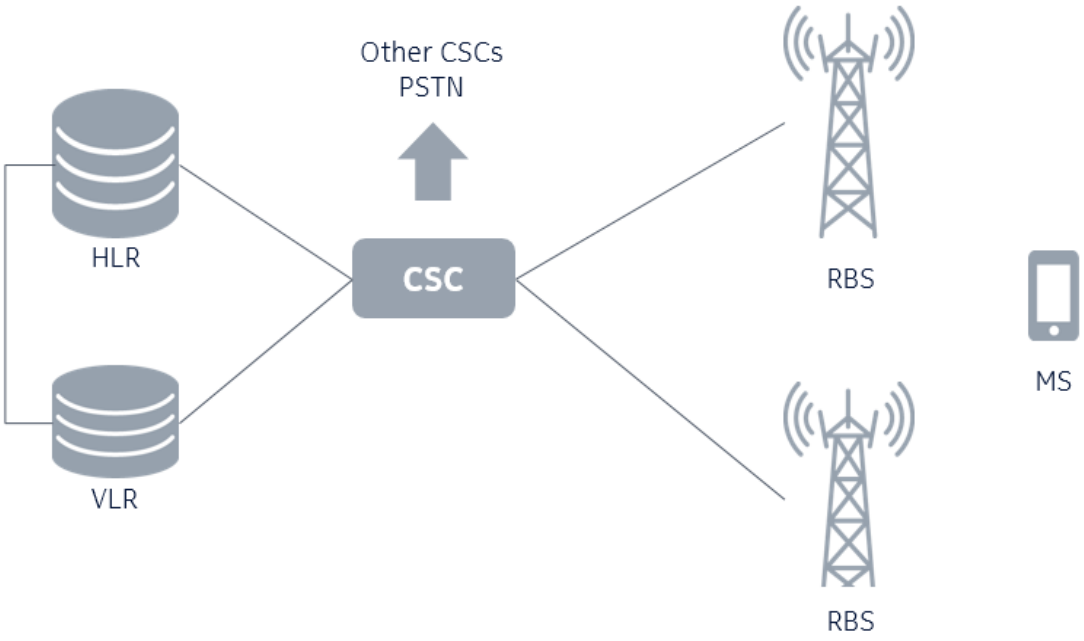

Figura 2. Arquitectura del sistema AMPS[7]

Sus elementos fueron los siguientes:

[7] Imagen de elaboración propia.

- MS Mobile Station / Estación Móvil

Terminal con la que interactúa el usuario, se identificaba por un MIN (Mobile Identification Number)

- RBS Radio Base Station / Estación Rádio Base

Elemento encargado de realizar la comunicación con los MS en determinada celda.

- CSC Conmutation and Switching Central /Central de Conmutación y Control

Encargada de la señalización y la conmutación en determinada área, ejecuta la conmutación con otras CSC, se tiene conexión a las bases de datos (HLR, VLR)

- HLR Home Location Register / Registro de Suscriptores Locales

Base de datos que almacena la información de todos los usuarios de un sistema celular

- VLR Visitor Location Register / Registro de Suscriptores Visitantes

Base de datos que contiene la información de los usuarios visitantes a un sistema celular.

4.1.2 SEGUNDA GENERACIÓN

Esta generación se caracterizó por dejar de ser analógica y ser digital, aparece la señalización que permite los SMS, un servicio bidireccional de intercambio de mensajes alfanuméricos de hasta 160 bytes.

La segunda generación de telefonía surge de la limitación de canales que había en la primera generación, con técnicas como TDMA (Time Division Multiple Access) y CDMA (Code Division Multiple Access), esto pudo combatirse.

La segunda generación trajo consigo la aparición de algunos sistemas como GSM (Global System for Mobile Communications), IS-136, y PDC (Personal Digital Communications)

La red GSM se basa en técnicas de conmutación de circuitos (Circuit Switched o CS). Introdujo varias ventajas con respecto a la primera generación, como una mejor calidad de voz, seguridad en la transmisión de la información, mayores tasas de transmisión (hasta 9.6 Kb/s), disminución de potencia en sus dispositivos, así como los SMS (Short Message Service). Se presenta el concepto de Handover (Intercambio entre Estaciones base), que permite la conmutación entre celdas y con ello, una movilidad ilimitada en la red.

A continuación, se muestra la arquitectura celular GSM, con algunas descripciones de sus elementos, GSM está conformado por 4 módulos o subsistemas, estos se muestran en la Figura 3, con cada uno de los elementos que los conforman.

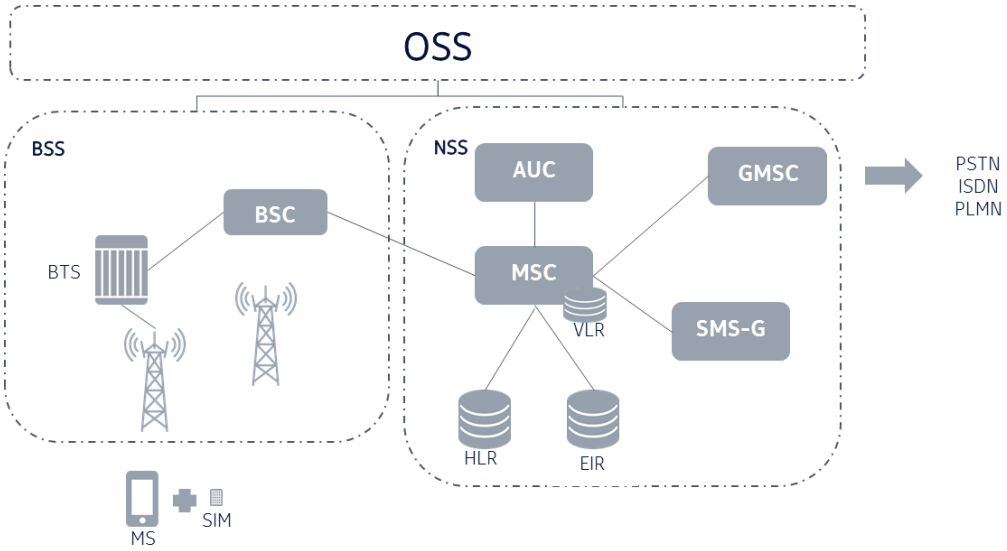

Figura 3 Arquitectura de Red GSM[8]

- MS: Mobile Station/Estación Móvil

Esta subestación consta de dos elementos, el equipo o terminal móvil, y la SIM, que permite hacer la identificación en la Red. Esta subestación es la que el usuario ve y con el que interactúa.

- BSS: Base Station Subsystem

Es el Subsistema de estaciones base, incluye las BTS y las BSC.

  - BTS: Base Transceiver Station / Estación Base

    Es la primera interacción con los móviles. Entre sus funciones están la recepción y transmisión de los canales de radio y la conversión de señales de radiofrecuencia en bits. Hay una BTS por celda. Se encarga del cifrado de la información.

  - BSC: Base Station Controller /Controlador de Estaciones Base

    Controla un grupo de BTSs, se encarga de su gestión y de la organización de los recursos de radio, de la asignación de canales.

- NSS: Network Switching Subsystem / Subsistema de Conmutación de Red

[8] Imagen de elaboración propia.

Este subsistema se encarga de la gestión, conmutación, e interconexión de otras redes. Representa el Core de la Red. Está conformado por los siguientes elementos: MSC, GMSC, AuC, HLR, VLR, EIR y G-SMS.

- MSC: Mobile Switching Center's / Centro de Servicios de conmutación móvil

  Es el principal elemento de la NSS, se encarga de la conmutación entre MSC, además de permitir el registro, la autenticación, la localización y enrutamiento de llamadas. Entre sus funciones se encuentra el control de los handover.

- GMSC: Gateway Mobile Switching Center / Gateway de Centro de Servicios de conmutación móvil.

  Elemento de la red que funciona como Gateway para la conmutación con redes externas, como la Red de Telefonía Fija, entre otros.

- AuC: Authentication Center / Centro de Autenticación

  Es una base que se utiliza para la autenticación y el cifrado en el canal de radio. Esta autentificación se lleva a cabo a través de triplets.

- HLR: Home Location Register / Registro de Suscriptores Locales

  Esta base de datos contiene la información administrativa de todos los suscriptores de una red. Contiene perfiles y servicios de todos los abonados de esa red celular.

- VLR: Visitor Location Register / Registro de Suscriptores Visitantes

  El VLR trabaja en conjunto con el MSC, contiene información específica del HLR acerca de los suscriptores que se encuentran alojados en ese momento en el MSC, es una base de datos temporal.

- EIR: Equipment Identity Register / Registro de Identidad de Equipo.

  Este elemento es el que tiene la capacidad de decidir si un elemento es bienvenido en la red. Cada equipo cuenta con un IMEI (International Mobile Equipment Identity) y estos son categorizados en 3 posibles listas, cada una con un estado asignado. Los posibles estados que le asigna el EIR a un móvil son los siguientes:

  - Permitido en la red

- Acceso prohibido
- En supervisión

➢ SMS-G: Short Message Service Gateway / Gateway de Sevicios de mensajes cortos

Tiene la funcionalidad de Gateway para los SMS, se encarga del procesamiento de los mensajes que son enviados o recibidos desde esa red.

❖ OSS: Operation Support Subsystem / Subsistema de apoyo y operación.

Entre las funciones del subsistema de Soporte y Operación la red, se encuentra el monitoreo y control, tienen interconexión con los subsistemas NSS y BSS.

4.1.3 GENERACIÓN 2.5

La generación 2.5 surge de la necesidad por parte de la población de emplear el servicio de navegación por internet, la segunda generación tenía limitaciones y aunque era más eficiente en voz, seguía presentando deficiencias en datos, lo que orillo a la creación de tecnologías como HSCSD, GPRS y EDGE.

La evolución de GSM hacia la tercera generación se dio por partes, esta evolución se describe con más detalle en la figura 4:

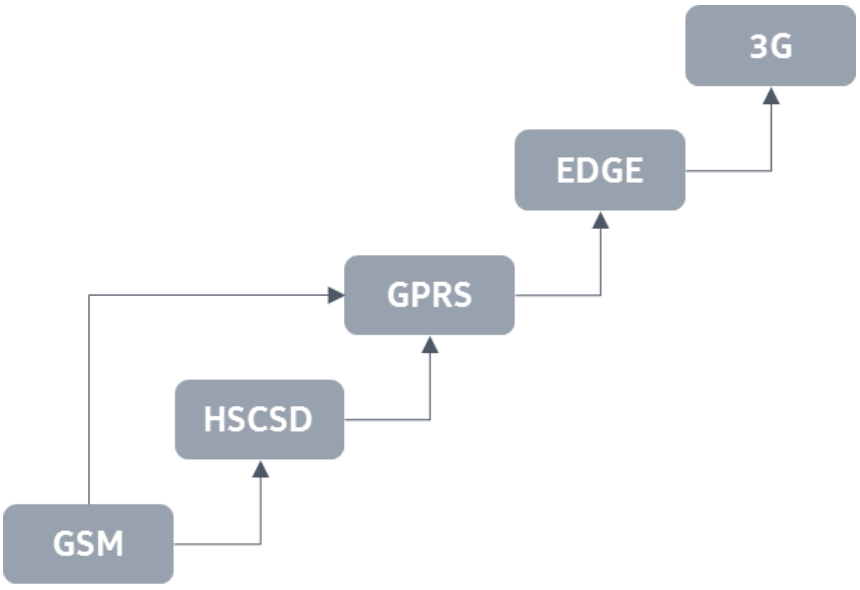

Figura 4 Evolución hacia la tercera generación[9]

[9] Imagen de elaboración propia.

Esta generación permite navegación por internet, aunque de manera limitada, para algunos operadores represento una opción en cuanto a actualización de tecnología.

Cada una de las tecnologías represento una mejora con respecto a la anterior, a continuación, se muestra un análisis comparativo de cada una de las tecnologías de acuerdo a sus velocidades de transmisión.

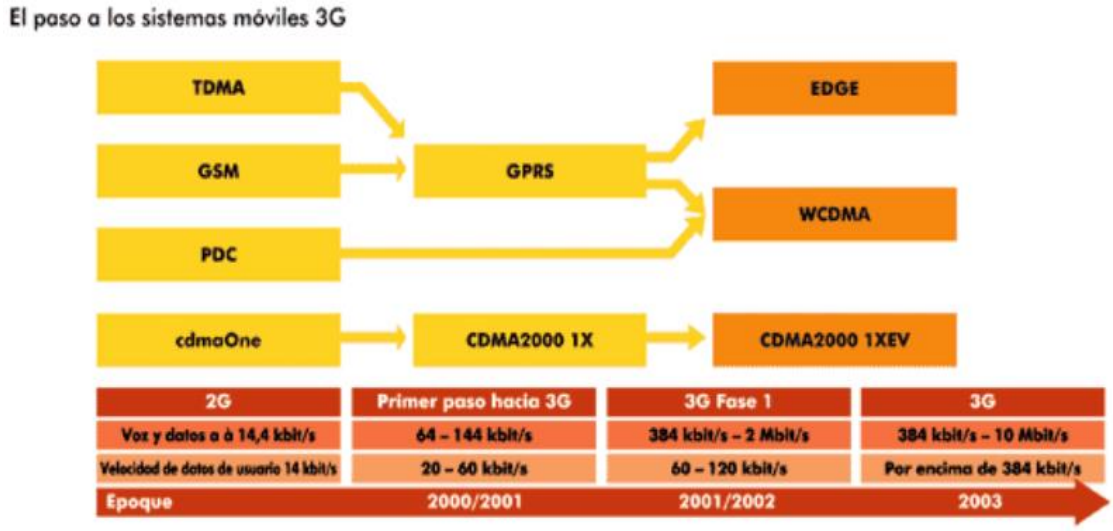

Figura 5. Tasas de transmisión en la evolución hacia 3G[10]

4.1.3.1 HSCSD (HIGH SPEED CIRCUIT SWITCHED DATA)

HSCSD surge como una evolución de GSM, permite la agrupación de 8 slots de GSM, consiguiendo tasas de transmisión de hasta 56.6 Kb/s. Seguía siendo una generación de conmutación de circuitos, cada uno de sus canales de radio podía ser utilizado para una conversación de voz, y para datos.

Una de las características de esta tecnología es contar con velocidades simétricas y asimétricas. Se permitieron varias aplicaciones como:

- ✓ Correo electrónico
- ✓ Transferencias de archivos

[10] Imagen obtenida de la página de noticias de la ITU [http://www.itu.int/itunews/issue/2003/06/thirdgeneration-es.html]

4.1.3.2 GPRS (GENERAL PACKET RADIO SYSTEM)

Este sistema representa las bases de la tercera generación, uno de los grandes avances fue la posibilidad de estar siempre conectados, ya que el cobro se empezó a hacer por kilobyte y no por tiempo, como se trabajaba en los sistemas anteriores. GPRS, de igual forma, trabaja como un sistema de conmutación de paquetes (PS).

En GPRS se integran la conmutación por circuitos con la conmutación de paquetes. La conmutación de circuitos permite tráfico en tiempo real, mientras que la conmutación por paquetes no.

Entre las características que se introducen en GPRS, es el aumento en el ancho de banda y en las velocidades de transferencia (desde 14.4 kb/s hasta 115 kb/s), la disminución de costos debido a la optimización de los recursos de la red. Se introduce el concepto de APN (Access Point Name).

El contenido ya permite la introducción de videoconferencias, imágenes móviles, chats, email, entre otros.

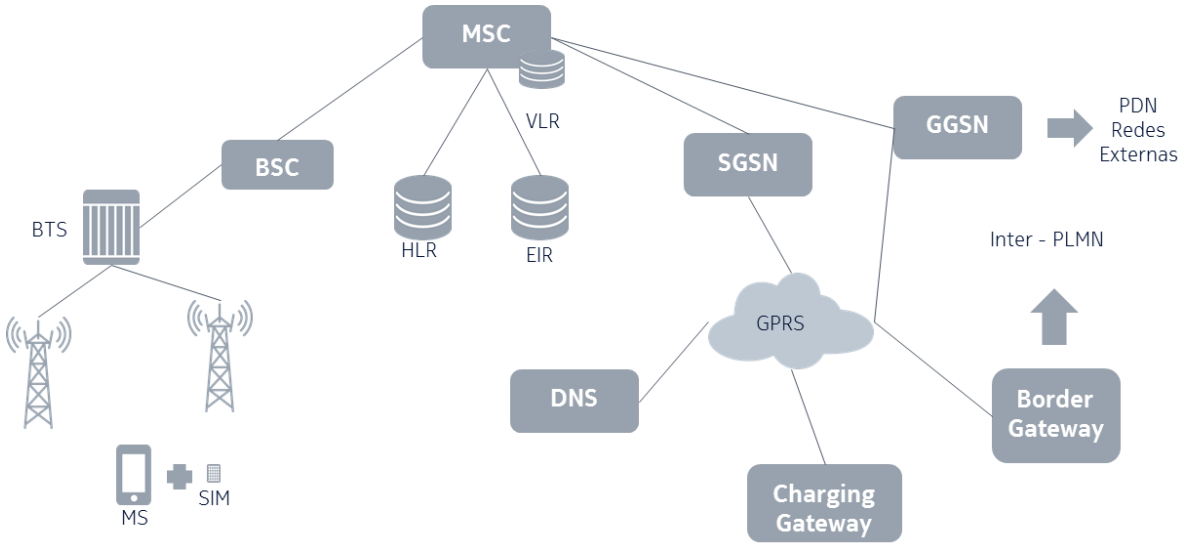

Figura 6. Arquitectura de GPRS[11]

Como se puede observar en la figura 5, GPRS es una evolución de GSM, conserva algunos de los elementos de su arquitectura, aunque en este sistema se incluyen nuevos, como el Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN), DNS (Domain Name Server), estos elementos serán explicados a profundidad, ya que son importantes en la presente propuesta de solución. También se integran en GPRS el Border Gateway (BG) y elementos de Billing como el CG (Charging Gateway).

[11] Imagen de elaboración propia.

- Serving GPRS Support Node (SGSN)

Este nodo de la red tiene algunas funcionalidades importantes, se encarga de la conmutación de paquetes, permite el handover, retransmisión de los datos entre las terminales móviles y el GGSN (permitiendo la comunicación bidireccional).

Entre las principales funciones del SGSN están las siguientes:

- Adaptación de los protocolos entre la red IP (la red de transporte) y los protocolos usados en la parte de RAN, SNDCP (Sub Network Dependent Convergence Protocol) y LLC (Logical Link Protocol)
- Este elemento tiene entre sus funciones principales, permitirle el acceso a la red a las terminales móviles
- Permite la interacción con los nodos encargados de las bases de datos (HLR y MSC/VLR), lo que hace posible el attach a la red de un abonado, y con esto, su autenticación y aceptación a la red móvil.
- Es el encargado de establecer los túneles a través del protocolo GTP con lo que garantiza el ruteo hacia otro elemento de la red: el GGSN.
- Permite que la conexión de un usuario con la red sea posible con (QoS)
- Cifrado y compresión de los datos.
- Manejo de la movilidad (Handover) y apoyo en la autenticación.
- Se encarga de la tarificación.

El nombre de las interfaces que interconectan los elementos de la red también cambia en comparación con GSM.

La interfaz GN es la que interconecta el GGSN y el SGSN, la comunicación a través de esta interfaz se lleva a cabo mediante el protocolo GTP.

Este dato es relevante para este proyecto, el protocolo GTP será explicado más adelante, debido a que es la interfaz que será monitoreada, y el monitoreo desde el F5 se llevará a cabo a través de este protocolo y sus parámetros.

- GGSN: Gateway GPRS Support Node

Este elemento es uno de los principales en la red debido a las múltiples e importantes funciones que realiza, es importante contar con alta disponibilidad en él.

Su función principal es conectar las terminales móviles a redes externas o a la Red de Core de GPRS, esto permite el acceso a Internet y su intranet respectivamente.

Entre sus funciones se encuentra:

- Funciona como punto de enlace, lo que permite ejecutar la conexión entre el exterior (Internet), la red de datos Interna, o redes corporativas.
- Intercambio de información y señalización de datos de usuario, lo que permite la ejecución del PDP Context.
- Recepción de paquetes de datos desde el SGSN o BG, y traducción del protocolo GTP.
- En este equipo se configuran los APNs con las características apropiadas de facturación (Prepago o Pospago)
- Asignación de IPs de manera dinámica o estática de acuerdo a las características del APN.
- Permite la configuración de políticas de cobro, así como la medición del volumen de datos, y la generación de CDRs, paquetes que representan los datos consumidos por los usuarios.
- Almacena información de los usuarios que se encuentran conectados.
- Permite configuración externa para autenticación como Radius o Diameter, que puede ser utilizada en servicios de valor agregado.

En este proyecto, se presenta una propuesta de solución utilizando equipos F5 para monitorear dos equipos GGSN/PGW, y garantizar que, en caso de falla en alguno de los equipos, el tráfico sea enviado al equipo que en ese momento se encuentre disponible, la alta disponibilidad se efectuara a nivel DNS, cambiando la dirección del GGSN/PGW a la que se apunta, simultáneamente, estos trabajarán en un esquema de alta disponibilidad Activo-Activo para diferentes regiones geográficas. Más adelante se explicará el proceso de activación de contexto de un móvil.

- DNS (Domain Name Server)

Un servidor DNS (Domain Name System) es un servidor cuya función es traducir nombres de dominio a IPs y viceversa.

Existen algunos tipos de registros de DNS, cada uno tiene funcionalidades diferentes, esto será explicado a continuación:

✓

- A: Este registro se utiliza para convertir nombres de dominio en direcciones IP.
- AAAA: Este registro es similar al tipo A, solo que es aplicable para el protocolo IPV6
- CNAME: Este registro puede usarse como un alias, se utiliza para crear nombres de host adicionales hacia una misma dirección IP.
- NS: indica los servidores de DNS autorizados para el dominio.
- SRV: Este registro utiliza un pool de los servidores para un solo dominio, usando balanceo de carga estatico, permitiendo señalar alguno de ellos como primario.
- NAPTR: El registro NAPTR es un registro de recursos, funciona en conjunto con los registros SRV.

La funcionalidad de un DNS en el esquema GPRS, es entregarle al SGSN la dirección IP del GGSN de acuerdo al APN configurado y a su autentificación con el nodo HLR previamente, esto se lleva a cabo cuando se ejecuta el proceso de activación del PDP Context, proceso que se explicará más adelante.

El SGSN pregunta por la dirección de un nombre de APN (este suele ser un nombre de dominio o un registro NAPTR en algunos casos), posteriormente el servidor DNS contesta con la dirección IP del GGSN.

Es importante notar, que los registros NAPTR permiten hacer cierto tipo de balanceo, sin embargo, este es estático y no ejecuta un monitoreo previo a eso.

➢ Border Gateway

Elemento encargado de establecer la comunicación con otros operadores u proveedores de servicios, suele ser normalmente un router que maneja un protocolo de ruteo externo en una de sus interfaces para que la comunicación sea segura por internet.

➢ Charging Gateway

Es el nodo de la red que se encarga de administrar los CDRs recolectados, (estos CDRs contiene información acerca de la cantidad de paquetes de navegación que ha usado un usuario), y después los pre-procesa y analiza para su posterior facturación.

En GPRS se llevan a cabo dos procesos de flujo importante, el Attach a la red, y el PDP Contexto, estos son viables e identificables gracias a un elemento llamado APN.

4.1.3.2.1 ATTACH A LA RED.

Cuando un usuario se conecta a la red ocurren los siguientes pasos, estos se ilustran en la Figura 7.

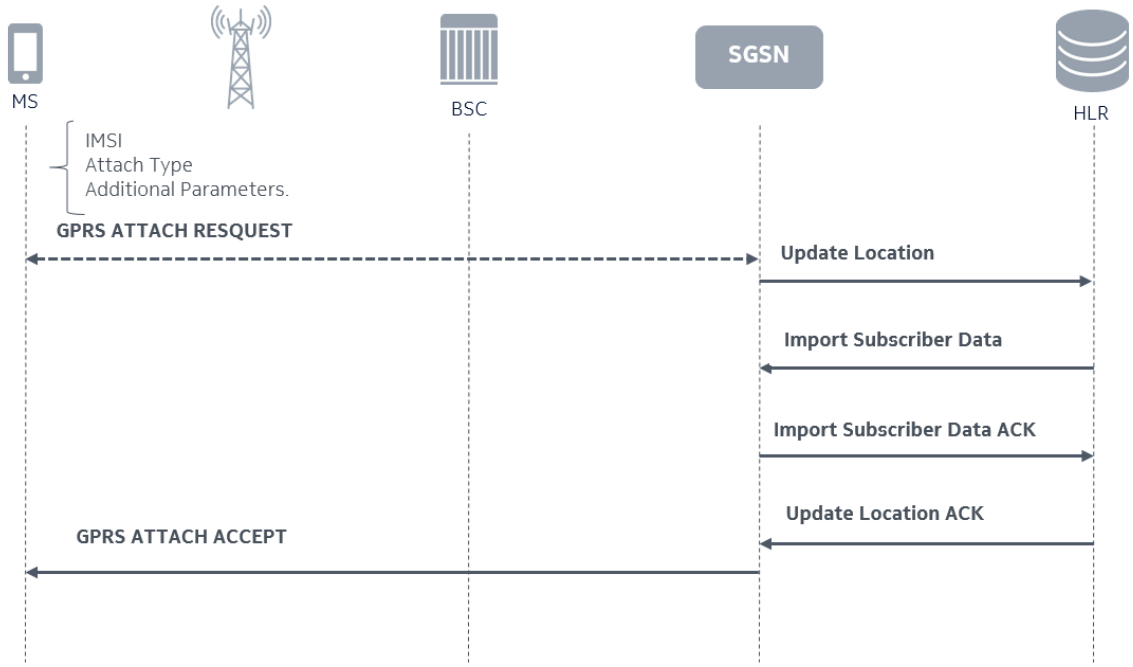

Figura 7.Attach a la Red[12]

1. Envía una petición de Attach a la Red. La terminal tiene previamente configurado parámetros que deben validarse en la red.
2. Esta es recibida por la parte de RAN (BTS y BSC) y transmitida a la parte de Core para su autentificación.

[12] Imagen de elaboración propia.

3. En la red de Core, es recibida por el SGSN, quién actualiza la conexión y ubicación del subscriptor.
4. Posteriormente el SGSN se encarga de interactuar con el HLR, con el fin de intercambiar información del subscriptor.
5. El HLR hace una revisión de la información de todos los datos, así como del perfil del usuario, y finalmente, valida la información si tiene autorización para ingresar a la red en el APN que está configurado.
6. El SGSN, al recibir confirmación del HLR, envía un mensaje de aceptación a la red y el proceso de Attach del Móvil es completado.

4.1.3.2.2 PDP CONTEXT

El proceso de PDP surge de la necesidad del usuario por solicitar una conexión a la red de Datos. Los pasos que se siguen en este procedimiento son los siguientes:

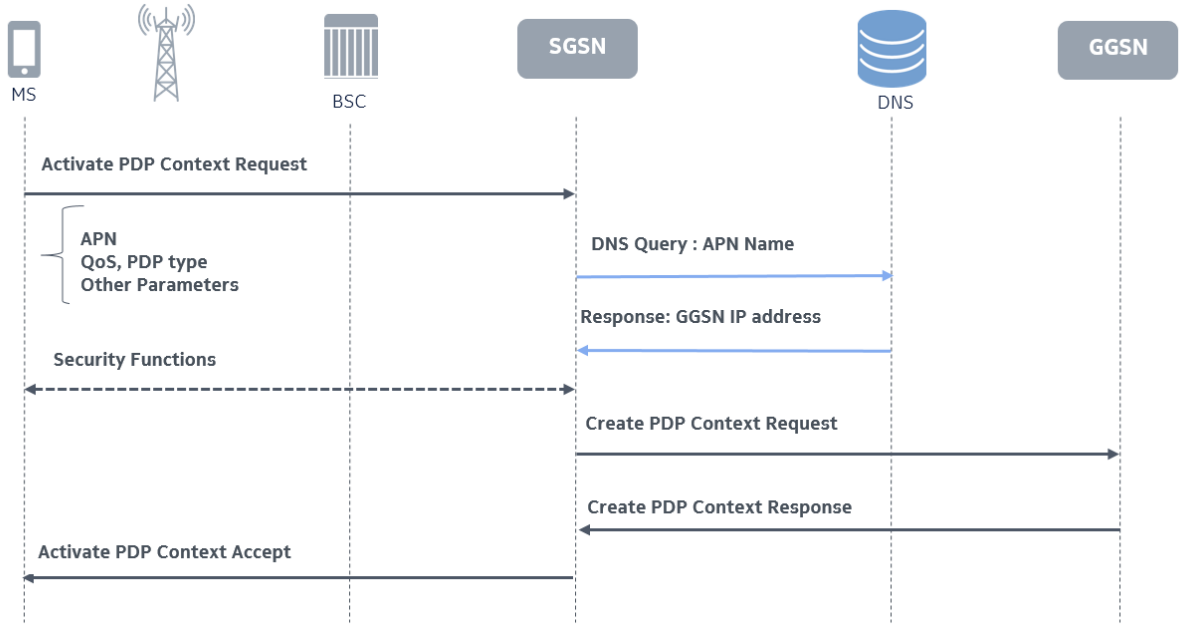

Figura 8. Procedimiento de PDP Context[13]

1. La terminal móvil, que tiene previamente configurado un APN (Los permisos de conexión a este APN ya han sido validados en el Attach), solicita una activación de PDP Context.

[13] Imagen de elaboración propia.

2. La petición atraviesa la parte de RAN, y de nueva cuenta son recibidos por el SGSN.
3. Este recibe la petición del usuario, esta petición solicita la conexión al APN configurado.
4. El SGSN hace una Query hacia el DNS, para traducir el nombre de dominio del APN en una dirección IP.
5. El DNS recibe la petición, consulta en su base de datos, y regresa la dirección IP del GGSN que tiene la configuración de ese APN.
6. EL SGSN, al recibir la respuesta, procede a enrutar la petición al GGSN correspondiente.
7. El GGSN, al tener la configuración de dicho APN, procede a analizar su configuración, y a validar las características de cobro del usuario (Se lleva a cabo de la validación de Saldo y si tiene permitida la navegación)
8. En caso de que la respuesta sea positiva, se retorna al GGSN la aceptación del PDP Context, y direccionamiento al usuario, lo que le permite la navegación a la Red Interna y a la PDN.

4.1.4 TERCERA GENERACIÓN

La tercera generación trajo la aparición de UMTS, sistema que representa una mejora espectral, así como la integración con GSM en una modalidad Dual que soporta ambos sistemas, con sus respectivas interfaces.

Entre las características de UMTS se encontraba integrar redes terrestres y satelitales.

La Tercera generación trajo consigo una estandarización a través de la 3GPP (3rd Generation Partnership Project), cuyo objetivo era representar un sistema estándar con sus especificaciones dentro del marco de la ITU.

UMTS representa la integración del sistema de paquetes con el de circuitos, dando servicios de datos y voz respectivamente.

Para el sistema de conmutación de circuitos, es decir, el tráfico en tiempo real, la arquitectura de UMTS utiliza elementos de GSM, como el MSC, GMSC, mientras que para el sistema de conmutación de paquetes se usan elementos de la Red GPRS, como el GGSN, SGSN, entre otros.

Entre una de las características que se pueden apreciar en la evolución de la Tercera generación es la separación de la señalización con el tráfico de datos, con la identificación de 2 planos: User Plane y Control Plane, ambos trabajando diferentes protocolos de acuerdo a su funcionalidad.

En la parte de Radio Access Network, se aprecia la incorporación de dos sistemas

- UTRAN: UMTS terrestrial Radio Access Network
- GERAN: GSM Edge Radio Access Network. (Segunda Generación)

Para la parte de acceso en radiofrecuencia UMTS se caracterizó por usar WCDMA (Wideband Code Division Multiple Access), cuyo funcionamiento se basa en usar la misma frecuencia, pero diferentes códigos de modulación, esto involucra eficiencia espectral. La terminal móvil ahora toma el nombre de UE (User Equipment).

Entre los beneficios que buscaba UMTS, se encontraba velocidad de transmisión alta, equipos más adaptables, pequeños y ofrecer una cobertura más amplia.

Entre los elementos que se observan en UMTS, están algunos que ya habíamos apreciado anteriormente y estos solo se mencionaran:

- RAN

  - Ue: User Equipment / Termina Mòvil

  - RNC: Radio Network Controller. / Controlador de la Red Radio
    Tiene bajo su control uno o más Nodos B, entre sus funciones esta gestionar los Handover. Tiene conexión al Core de Voz y de datos, mediante los elementos MSC o SGSN, respectivamente.

  - Node B / Nodo B
    Es un elemento similar al BTS de 2G, se encarga de la conversión de bits en ondas electromagnéticas.

- Core CS y Core PS

  - MSC (Mobile Switching Center)
  - GMSC (Gateway Mobile Switching Center)
  - GGSN (Serving GPRS Support Node)
  - GGSN (Gateway GPRS Support Node)
  - HLR (Home Location Register)
  - AuC Authentication Center)
  - EIR (Equipment Identify Register)

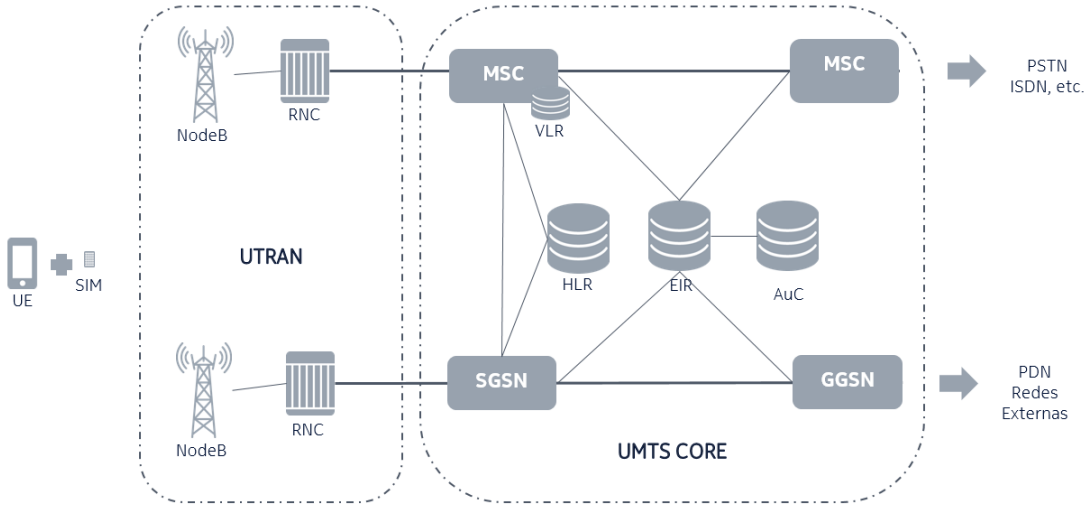

Figura 9. Diagrama de UMTS[14]

4.1.5 CUARTA GENERACIÓN

La tecnología de cuarta generación en Telecomunicaciones permite la transmisión de datos y de voz a altas velocidades a través de redes inalámbricas. Una de las características más representativas es la posibilidad de hacer la transmisión de paquetes en tiempo real, permitiendo la integración de VoIP.

Entre las tecnologías que se encuentran dentro de la cuarta generación se encuentran dentro de la cuarta generación están: LTE, LTE-Advanced y WiMax.

LTE fue creada por el 3GPP, sus siglas significan Long Term Evolution, suele ser la tecnología más representativa de la cuarta generación. Es una evolución de las arquitecturas GSM y UMTS.

La red de Acceso en radiofrecuencia se ve caracterizada por usar OFDM (Orthogonal Frequency Division Multiplexing), así como usar un ancho de banda dividido en numerosas subportadoras ortogonales entre sí.

De igual forma desaparece la red de conmutación de circuitos, y se vuelve una arquitectura basada en IP.

La arquitectura de LTE, se caracteriza por la integración de la E-UTRAN (Envolved – UTRAN), y EPC (Envolved Packet Core)

La parte de E-UTRAN ahora se compacta en un solo elemento:

- e-NodeB / Nodo B evolucionado

[14] Imagen de elaboración propia.

Entre sus funciones se encuentra gestionar los recursos de radio, gestión de movilidad y handovers, así como el cifrado, compresión, modulación y demodulación.

En la arquitectura EPC, el Core si tiene elementos nuevos, ahora está conformado por:

- MME Mobility Management Entity / Entidad de gestión de la movilidad

Este elemento tiene funciones de control parecidas al GGSN, se encarga de la gestión de la movilidad, tambièn gestiona la autenticación y autorización.

- S- GW Serving – Gateway

Se encarga de la gestión del canal y de la transferencia del User Plane, es responsable de sus propios recursos, sin embargo, el MME, al estar a cargo del Control puede comandarlo.

- P-GW Packet Data Network Gateway

Es el elemento que tiene funcionalidades parecidas al GGSN, se encarga de administrar configuración de IP a las terminales móviles.
En este equipo es donde se encuentran configurados los APNs, por lo que cumple la función de DHCP con los usuarios de una red de telefonía celular, proporcionándoles, direccionamiento, servidor DNS, tipos de cobro, entre otras características.

Puede tener interacción directa con un elemento conocido como PCRF, que se encarga de las políticas de control y cobro, así como validar si el usuario tiene permitida la navegación o no.

Es el elemento que funciona como Gateway de la red, y tiene la capacidad de enrutar hacia otros sistemas u operadores, así como redes externas o internas.

- PCRF Policy and Charging Resource Function / Función de politica y reglas de carga.

Se encarga de gestionar y manejar las políticas de control en la Red, así como de manejar la calidad de servicio de acuerdo a diferentes perfiles de usuario.

- HSS Home Subscriber Server / Servidor de Subscriptores Base

Este elemento es una base de Datos, tiene capacidades similares al elemento HLR de generaciones pasadas. Contiene el registro de datos de suscripción de todos los usuarios, así como su ubicación.

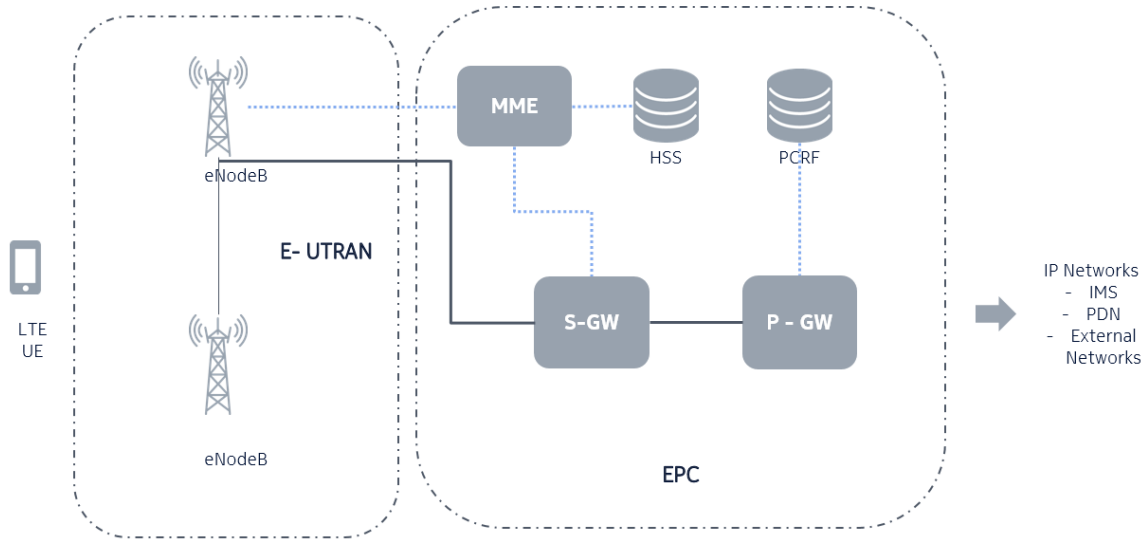

Figura 10. Diagrama LTE[15]

4.2 ESTRUCTURA DE APN

Un APN es un elemento lógico mediante el cual una terminal móvil se va a conectar a una red de datos celular.

Un usuario tiene configurado cierto APN, en primera instancia se valida si este usuario tiene permitido el acceso a este APN en la base de datos del HLR para el procedimiento de Attach a la red, en caso de que este sea exitoso para la navegación en la red de datos, se utiliza otro procedimiento, el PDP Context (Packet Data Protocol), donde de igual forma se ocupa el nombre del APN, este es consultado vía DNS a través de un Query para que posteriormente el servidor DNS regrese la respuesta a la petición con la dirección IP del GGSN que tiene la configuración de ese APN y pueda proceder con la navegación.

El formato de la estructura del nombre de dominio de un APN se muestra en la Figura 11.

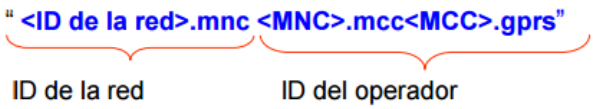

Figura 11. Estructura de un APN

[15] Imagen de elaboración propia.

4.3 GTP (INTERFACES GN)

La interfaz GN es la que interconecta el GGSN y el SGSN, la comunicación a través de esta interfaz se lleva a cabo mediante el protocolo GTP.

El protocolo GTP (GPRS Tunneling Protocol) es un protocolo usado en algunas redes tecnológicas importantes como GSM, UMTS, LTE. Se utiliza para encapsular datos de usuario al pasar a través de la red, así como llevar tráfico de señalización. Se puede categorizar en tres modalidades:

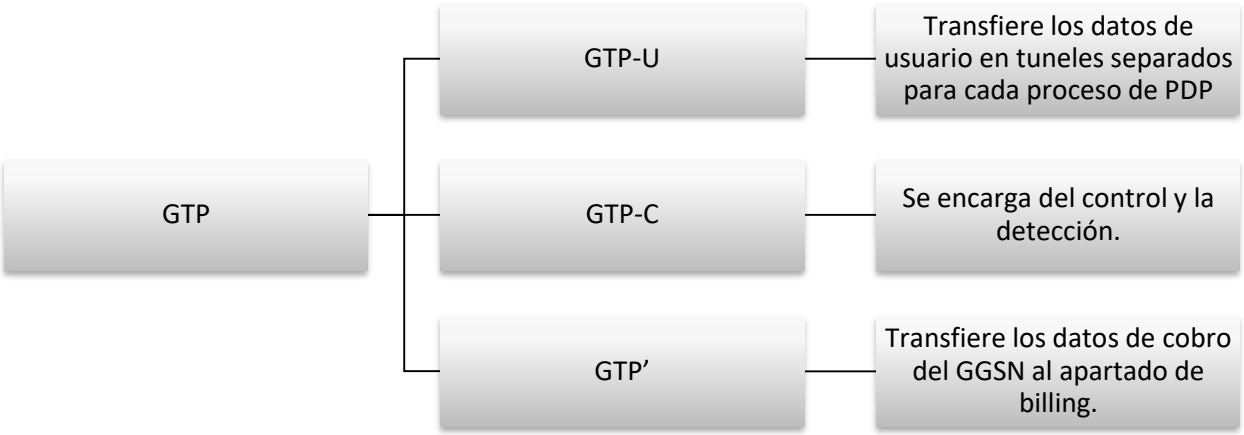

Tabla 1. Protocolo GTP[16]

4.4 EQUIPO BIG IP F5

La plataforma F5 BIG-IP, es una mezcla de software y hardware que consiste en un equilibrador de carga y un proxy completo. Tiene la funcionalidad de proporcionar la visibilidad de todo el tráfico que pasa por la red, así como la posibilidad de controlarlo.

[16] Tabla de elaboración propia

F5 tiene presencia en el mercado de las telecomunicaciones en una gran diversidad de campos:

➢ Seguridad

Las soluciones de F5 ofrecen una visibilidad de las amenazas de identidad y de los controles necesarios para mitigar los riesgos. Además, dichas soluciones potencian la seguridad de aplicaciones de cualquier infraestructura, desde datacenters tradicionales a entornos de cloud. Esto permite que los usuarios accedan a los datos desde cualquier dispositivo, en cualquier entorno y en cualquier momento.

Las soluciones de seguridad tradicionales se centran en la protección de la red y, por lo tanto, ignoran el contenido de la aplicación.

La ubicación en la red de un servidor F5 proporciona la visibilidad y el análisis necesarios para todo el tráfico de las aplicaciones, lo que le permite tomar decisiones según los riesgos potenciales para la aplicación, así como tomar las medidas necesarias contra la actividad malintencionada. Las soluciones de seguridad se ofrecen donde los negocios las necesitan (en dispositivos de software, de hardware independiente y virtuales, así como desde la cloud).

Entre las soluciones que ofrece F5 están:

- Visibilidad de SSL
- Protección contra DDoS
- Gestión de acceso e identidad
- Firewall para aplicaciones Web.

➢ Distribución de aplicaciones

La distribución de aplicaciones incluye el equilibrio de carga tradicional para distribuir cualquier aplicación, además de una gama de servicios de seguridad, rendimiento y gestión.

Es posible para F5 ofrecer una arquitectura que proporciona seguridad, estabilidad y agilidad para cada una de las aplicaciones que se administren, independientemente de dónde y cómo se implementen.

Se pueden implementar servicios de distribución de aplicaciones avanzados como la protección contra DDoS, WAF, DNS, optimización de TCP y equilibrio de carga de servidores globales para mantener la seguridad, la velocidad y la disponibilidad de las aplicaciones de manera constante.

➢ Cloud

F5 ofrece servicios de aplicaciones programables que se pueden integrar en una gran pila de soluciones de cloud públicas, privadas híbridas o de colocación. Le permiten proporcionar servicios de una forma automatizada y basada en políticas que cumple los requisitos de seguridad y conformidad sin ralentizar su equipo de desarrollo ni crear dependencia en un entorno de cloud determinado.

Aunque la cloud hace posible la innovación y la agilidad, no resuelve los estándares de seguridad y conformidad a los que están sujetos los equipos de TI. Para mantener el ritmo, los desarrolladores a menudo pierden tiempo en resolver estos problemas en lugar de aprovecharlo para trabajar en las funciones que generan ingresos. La plataforma F5 ofrece el rendimiento, seguridad y disponibilidad para las aplicaciones en la cloud.

F5 cuenta con diferentes módulos, cada una con diferentes características, lo que permite su explotación para una gran diversidad de soluciones. Los módulos se muestran en la Figura 12.

Los dos módulos a utilizar en esta propuesta de solución son LTM y GTM, ambos tienen características de configuración propias, mientras LTM ofrece redundancia HA y balanceo de carga, GTM se encarga del funcionamiento de DNS en un nivel local y global. Estos módulos serán los únicos que se explicarán con más detalle a continuación:

Figura 12. Módulos de F5[17]

4.4.1 BIG-IP LOCAL TRAFFIC MANAGER (LTM)

Este módulo de F5 ofrece un conocimiento del tráfico que circula a través de la red, transforma el caótico volumen de tráfico de red en flujos de datos ensamblados y, a continuación, toma decisiones inteligentes sobre la gestión del mismo mediante la selección del destino correcto según el rendimiento del servidor, la seguridad y la disponibilidad.

[17] Imagen obtenida de la página oficial de la marca [https://f5.com/es/products]

Dado que BIG-IP LTM es un proxy completo, puede inspeccionar, gestionar e informar sobre el tráfico que entra y sale de su red. Desde decisiones básicas sobre el equilibrio de carga a decisiones complejas sobre la gestión del tráfico según cada cliente, el servidor o el estado de la aplicación.

Por excelencia este módulo desarrolla la función de ser un balanceador de carga, al ser funcional como un full proxy tiene la ventaja de agregar seguridad.

Un proxy o servidor proxy, es un servidor que funciona o hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor. Entre sus funciones se encuentran:

- Abrir sesiones TCP o UDP de cada lado.
- Es la interconexión para dos dispositivos.
- Ser Full Proxy es mantener tablas separadas de cada lado de la conexión.

Los principales elementos en una arquitectura de LTM son los Nodos, Pool Members, Pools y Virtual Server.

- ✓ Nodo: Es un objeto lógico en el equipo que identifica la dirección IP o nombre de dominio de un recurso físico en la red.

- ✓ Pool Member: Es un objeto lógico que representa un nodo físico en la red. La diferencia con un Nodo es que el Pool Member está referido a un servicio, es decir, a un socket, mientras que el nodo puede ser exclusivamente la dirección IP o nombre de dominio.

- ✓ Pool: Es un conjunto lógico de servidores o elementos representados por los Pool members. A cada Pool se le asigna un método de balanceo que define la manera en que asignará las conexiones con los Pool Members.

- ✓ Virtual Server: Es uno de los elementos principales de configuración en el módulo de LTM y el sistema F5 en general, ya que es un objeto de gestión de tráfico. Se representa a través de una dirección IP virtual y un servicio (Puerto de escucha).
  Coloquialmente, se podría decir que el Virtual Server es el elemento que escucha el tráfico de la red. A este elemento es al que se le suelen realizar las peticiones, y es la IP que representa un Proxy, posteriormente, después dirige el tráfico según los elementos lógicos que tenga configurados, es decir, Pool y sus respectivos miembros.

  El principal propósito de un Virtual Server es distribuir el tráfico entre un conjunto de servidores o miembros de acuerdo a un método de balanceo, sea estático o dinámico. Cuando se crea un servidor virtual se especifica el o los Pools que se desean utilizar como destino para cualquier tráfico que reciba ese virtual server. También es posible configurar sus propiedades generales, perfiles, traducción de direcciones IP, monitoreo y algunas otras características como iRules o tipos de persistencia de sesión.

Una de las características de un sistema F5, es poder realizar monitoreo personalizado a cada uno de sus elementos de acuerdo a sus características.

El estado de cada uno se indica mediante varios iconos que se distinguen por la forma y el color. La forma del icono indica el estado que ha informado el monitoreo para ese nodo. Hay 4 tipos diferentes de estado:

- Up/ Available
  Se representa por medio de un circulo de color verde y se muestra cuando el elemento responde satisfactoriamente al monitoreo que le fue asignado.

- Down/ Offline
  Contrario al estado disponible ocurre cuando los parámetros de monitoreo no muestran respuestas satisfactorias. Se representa con un diamante o rombo color rojo.

- Upknown
  Representado por medio de un cuadrado azul, aparece principalmente cuando no se ha asignado un monitoreo al elemento por lo que el sistema F5 no puede determinar si este es disponible o no.

- Connection Limit /Unavailable
  Se representa por un triángulo amarillo, los elementos que se muestran en este estado son los que se encuentran saturados debido a que ya están ocupando sus sesiones disponibles.

La Figura 13 muestra gráficamente cada uno de los estados.

Como se ha mencionado anteriormente, la principal función de este módulo es el Balanceo de Carga, existen varias formas o métodos de llevar a cabo el balanceo.

Figura 13.Tipos de Estado para el monitoreo de Elementos F5[18]

[18] Imagen obtenida de la página https://www.fir3net.com/Loadbalancers/F5-BIG-IP/big-ip-ltm-health-monitors.html

Como se ha mencionado anteriormente, la principal función de este módulo es el Balanceo de Carga, existen varias formas o métodos de llevar a cabo el balanceo.

Un método de balanceo de carga es un algoritmo o fórmula que el sistema F5 utiliza para determinar el nodo al que se enviará el tráfico. El balanceo de carga puede efectuarse de diferentes maneras según el algoritmo que se configure, existen 2 tipos de balanceo: estático y dinámico.

- Estático
  - Round Robin.
    Este es el método predeterminado. El modo Round Robin pasa cada nueva petición de conexión al siguiente servidor en línea, distribuyendo conexiones uniformemente.
  - Ratio.
    En este método se distribuyen las conexiones entre los Pool Members de acuerdo con los pesos de relación que se les configura, donde el número de conexiones que cada nodo recibe a lo largo del tiempo es proporcional a la relación de peso que se define para cada uno.
- Dinámico
  - Least Connections
    El método de Least Connections es relativamente simple, el sistema F5 pasa una nueva conexión al nodo que tiene el menor número de conexiones actuales.
  - Fastest
    Este método establece una nueva conexión basada en el número mínimo de solicitudes de capa 7 pendientes a un Pool Member y el número de conexiones abiertas de capa 4. Este método es útil cuando los nodos están distribuidos a través de diferentes redes lógicas.
  - Observed
    El método de balanceo Observed es muy similar al de Least Connections, ya que se encarga de distribuir el tráfico al nodo que tenga el menor número de conexiones. La principal diferencia entre ambos, es que Least Connections mide el número de conexiones al momento del balanceo, mientras que Observed está continuamente monitoreando el tiempo de la sesión.
  - Predictive
    El método predictivo también se basa en la observación, las conexiones se distribuyen según el número de conexiones actuales. Sin embargo, el equipo F5 analiza la tendencia de la distribución a lo largo del tiempo, determinando si el rendimiento de los nodos está

mejorando o disminuyendo. Los nodos con mejor rendimiento reciben una mayor proporción de las conexiones.

- Dynamic Ratio
  Es similar al método de Ratio excepto por que los pesos de relación se basan en el monitoreo continuo de los servidores y por lo tanto estos se encuentran cambiando continuamente. Este método distribuye conexiones basadas en diversos aspectos del análisis del rendimiento del servidor en tiempo real.

4.4.2 BIG-IP GLOBAL TRAFFIC MANAGER (GTM)

El módulo de Global Traffic Manager permite supervisar la disponibilidad y el rendimiento de los recursos globales y utilizar esa información para gestionar los patrones de tráfico de la red. GTM utiliza algoritmos de equilibrio de carga, enrutamiento basado en topología e inclusive permite la configuración de iRules (Reglas mediante código que se configuran para requerimientos específicos), para controlar y distribuir el tráfico según políticas específicas.

Si se analiza como un centro de datos de múltiples infraestructuras tiene la funcionalidad de permitir configuración para resolver el tráfico entrante de diferentes maneras. El GTM también incluye otras características avanzadas como DNSSEC y resolución inteligente basada en muchos algoritmos diferentes.

GTM distribuye solicitudes de resolución de nombres DNS mediante su funcionalidad como servidor "DNS Inteligente", GTM selecciona el mejor recurso disponible utilizando un método de equilibrio de carga estático o dinámico.

Utilizando un método de equilibrio de carga estática, GTM selecciona un recurso basado en un patrón predefinido.

Utilizando un método dinámico de balanceo de carga, GTM selecciona un recurso basado en las métricas de rendimiento actuales recopiladas por los agentes que se ejecutan en cada centro de datos.

Para que el sistema Global Traffic Manager funcione eficazmente, debe definir los componentes que conforman los segmentos de su red. Estos componentes incluyen componentes físicos como centros de datos y servidores, así como componentes lógicos tales como direcciones IP, direcciones y agrupaciones. Al definir estos componentes se crea un mapa de red que puede utilizar el servidor F5 para dirigir el tráfico del DNS al mejor recurso disponible.

Los componentes que se definen en Global Traffic Manager se pueden dividir en dos categorías básicas:

- **Componentes físicos**

Los componentes físicos son aquellos que se configuran en el módulo de GTM y tienen una correlación directa con una ubicación física o un dispositivo en la red.
Estos componentes son:

- ✓ **Data Centers (Centro de datos):**
  Los centros de datos son el nivel superior de la configuración de una red física. Es necesario configurar un centro de datos para cada ubicación física en la red global. Cuando se crea un centro de datos en Global Traffic Manager se definen los servidores (tanto los pertenecientes a LTM como a GTM) que residen en esa ubicación.

- ✓ **Servers (Servidores):**

Un servidor es un dispositivo físico en el que se puede configurar uno o más servidores virtuales. Los servidores que se definen pueden incluir sistemas F5 o servidores externos.

- ✓ Links (Enlaces):

Un enlace es una representación lógica de un dispositivo físico que conecta su red a Internet. Es posible asignar varios enlaces a cada centro de datos asociando lógicamente vínculos a una colección de servidores para administrar el acceso a sus fuentes de datos. La configuración de enlaces es opcional, aunque son muy útiles para determinar la disponibilidad de recursos.

- ✓ Virtual Server (Servidores Virtuales):

Un servidor virtual, en el contexto de Global Traffic Manager, es una combinación de una dirección IP y un número de puerto que apunta a un recurso que proporciona acceso a una aplicación o fuente de datos en su red. Los servidores virtuales son el destino final para las solicitudes de conexión.

- ❖ Componentes lógicos

Además de los componentes físicos de su red, GTM también maneja el tráfico de DNS sobre componentes lógicos. Los componentes de red lógicos consisten en elementos de red que no representan una ubicación física o un dispositivo. Los componentes lógicos son:

- ✓ Listeners:

Es un objeto que supervisa la red para las consultas DNS y por lo tanto, es crítico para la gestión del tráfico global. El Listener instruye al sistema para supervisar el tráfico de red destinado a una dirección IP específica. Este elemento es similar al Virtual Server del módulo de LTM. A un Listener se le pueden asignar métodos de Balanceo y Recursos, como Pool, con Servidores asociados.

- ✓ Pools:

Es una colección de servidores virtuales que pueden residir en varios servidores de red. En un Pool se definen los servidores virtuales a los que el módulo GTM dirigirá el tráfico DNS. Es posible configurar métodos de equilibrio de carga, monitores, iRules y otras opciones de configuración en cada uno de los Pool que se configuren.

- ✓ Wide IPs:

Este elemento es uno de los más importantes en la configuración de GTM y en este proyecto. Una Wide IP asigna un nombre de dominio completo (FQDN) a uno o más Pools de servidores virtuales que alojan el contenido de los dominios. A cada Wide IP se le debe configurar que Grupos o Pools de servidores están aptos para responder a una solicitud, y que métodos de balanceo de carga son los adecuados. De tal manera, cuando se recibe una petición a determinada Wide IP, el servidor F5 estará capacitado para su resolución.

- ✓ Distributed applications:

  Una aplicación distribuida es una colección de una o más Wide IPs, centros de datos y enlaces que sirven como una sola aplicación a un visitante. Una aplicación distribuida es el componente de nivel más alto que admite GTM. Se puede configurar Global Traffic Manager para que la disponibilidad de aplicaciones distribuidas dependa de un centro de datos, enlace o servidor específico. Por ejemplo, si cierto elemento se desconecta (como un centro de datos), esta información hace que la wide IP y su aplicación distribuida correspondiente no estén disponibles. En consecuencia, el sistema no envía solicitudes de resolución a ninguno de los recursos de aplicación distribuida hasta que toda la aplicación esté disponible de nuevo.

Global Traffic Manager proporciona un sistema de equilibrio de carga en niveles en el que el equilibrio de carga se produce en más de un punto durante el proceso de solicitud de resolución de nombres.

Los niveles dentro de Global Traffic Manager que permiten balanceo de tráfico son los siguientes:

- Wide IP-level load balancing

  Se realiza el balanceo entre uno o más Pools

- Pool-level load balancing

  El balanceo, en este caso, se lleva a cabo entre varios servidores.

Al igual que en el módulo de Local Traffic Manager existe el balanceo estático y dinámico, los métodos difieren de acuerdo a las características para que sean aplicables, es decir, los métodos de equilibrio para Wide IP-level load balancing, no son los mismos que los funcionales para Pool-level load balancing.

Para un escenario Wide IP-level load balancing, solo se permiten los métodos de equilibrio de carga estáticos y solo hay 4 de ellos que son aplicables, mientras que para Pool-level load balancing las opciones son más bondadosas permitiendo escoger entre 8 métodos estáticos, más 10 métodos de balanceo dinámicos.

Global Traffic Manager admite tres tipos de métodos de equilibrio de carga para Pool-level load balancing:

- Preferido,
- Alternativo
- Fallback

El método de equilibrio de carga preferido es el modo de equilibrio de carga que el sistema intenta utilizar en primer lugar. Si el método preferido no proporciona un recurso válido, el sistema utiliza el método de equilibrio de carga alternativo. Si el método de balanceo de carga alternativo no proporciona un recurso válido, el sistema utiliza el método de fallback.

En la tabla siguiente se explica lo anterior, así como una identificación previa de los métodos de balanceo y en qué caso estos pueden ser aplicados, entre ellos se reconocen algunos que se habían visto previamente en Local Traffic Manager.

		Wide-level load balancing	Pool-level load balancing		
			Preferido	Alternativo	Fallback
Estático	Drop Packet		*	*	*
	Fallback IP		*	*	*
	Global Availability	*	*	*	*
	Ratio	*		*	*
	Return to DNS		*	*	*
	Round Robin	*	*	*	*
	Static Peristent		*	*	*
	Topology	*	*	*	*
Dinámico	Completion Rate		*		*
	CPU		*		*
	Hops		*		*
	Kbps/Second		*		*
	Leats Connection		*		*
	Packet Rate		*	*	*
	Quality of Service		*		*
	Round Trip Time		*		*
	Virtual Server Score		*	*	*
	VS Capacity		*	*	*

Tabla 2. Métodos de balanceo GTM

A continuación, algunos de los métodos de la tabla anterior son explicados mejor.

- **Estático**
  - **Fallback IP.**

Cuando se especifica el modo de equilibrio de carga Fallback IP, Global Traffic Manager devuelve una dirección IP específica, funciona como IP de respaldo para las consultas. Es posible especificar una dirección IPv4 y una dirección IPv6 como dirección IP de respaldo. Aunque es posible configurar este método de varias formas, se aconseja que solo se ocupe como Método Fallback.

- Global Availability.

  El modo de equilibrio de carga Global Availability utiliza los servidores virtuales incluidos en un Pool en el orden en que se enumeran. Para cada solicitud de conexión este método comienza en la parte superior de la lista y envía la conexión al primer servidor virtual disponible en la lista. Sólo cuando el servidor virtual actual está lleno o no disponible, el modo Global Availability se mueve al siguiente servidor virtual de la lista.

- Topology.

  El modo de equilibrio de carga de Topología le permite dirigir o restringir el flujo de tráfico mediante la adición de registros de topología a una declaración de topología en el archivo de configuración.

  Es posible configurar el Administrador de tráfico GTM para cargar el equilibrio entre las peticiones de conexión entrantes y un recurso basado en la proximidad física del recurso al cliente que realiza la solicitud. También puede configurar el sistema para entregar contenido específico por región, a un cliente que realiza una solicitud desde una ubicación específica.

  Un registro de topología es un conjunto de características que mapea el origen de una solicitud de conexión a un destino específico. Se crean registros de topología en el Administrador de tráfico global que indican al sistema dónde se deben encaminar las solicitudes de conexión.

  Cada registro de topología contiene los siguientes elementos:

  - Una instrucción de fuente de solicitud que define el origen de una solicitud de conexión.
  - Una instrucción de destino que define el recurso al que el GTM dirigirá la solicitud de conexión.
  - Un peso asignado por el sistema a un objeto servidor durante el proceso de equilibrio de carga.

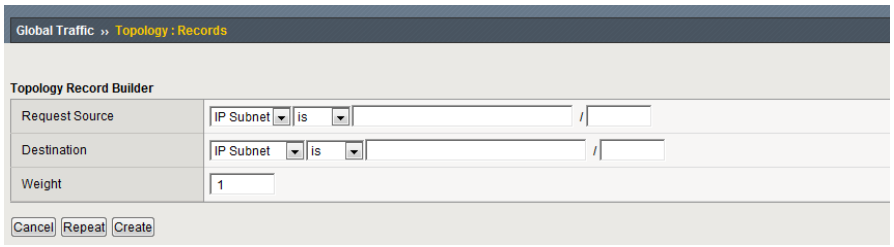

Figura 14. Configuración de un registro de topología.[19]

De forma predeterminada, cada vez que se carga la configuración del sistema, Global Traffic Manager clasifica automáticamente los registros de topología en una lista ordenada basada en el algoritmo de clasificación de coincidencias más largo de la topología.

Cuando una solicitud de conexión llega al sistema, la decisión de equilibrio de carga se basa en el siguiente proceso:

1. Para cada petición de conexión, el sistema realiza una iteración a través de una lista ordenada de registros de topología de la primera a la última y asigna un peso a cada objeto.
2. El sistema localiza el primer registro de topología que más específicamente coincide con el objeto de servidor y asigna la puntuación de topología en el registro al objeto.
3. Si la iteración a través de la lista no encuentra un registro de topología que coincida, a ese objeto de servidor se le asigna una puntuación cero.
4. El servidor F5 direcciona la solicitud de conexión al objeto con la puntuación más alta

❖ Dinámico

- Completion Rate

  El modo de equilibrio de carga de Completion Rate selecciona el Virtual server que actualmente mantiene el menor número de paquetes eliminados durante una transacción entre un Pool Member y el cliente.

- CPU

  En este método de balanceo se elige el Virtual Server que actualmente tiene el mayor tiempo de procesamiento de la CPU disponible para gestionar solicitudes de resolución de nombres.

- Hops

  El modo Hops selecciona un Virtual Server en el centro de datos basándose en el que tiene menos saltos.

[19]Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm-topology-lb-configuring-11-0-0/1.html]

- Packet Rate

  El modo de equilibrio de carga de velocidad de paquetes selecciona el recurso que está procesando actualmente el menor número de paquetes por segundo.

- Quality of Service

  El modo de equilibrio de carga de Quality of Service utiliza información de rendimiento actual para calcular una puntuación global para cada servidor virtual y, a continuación, distribuye conexiones basadas en las puntuaciones.

  Una de las ventajas es que toma como referencia muchos factores como lo son:

  - Tiempo de viaje
  - Saltos
  - Puntuación de servidor virtual
  - Tasa de paquetes
  - Topología
  - Capacidad de enlace
  - Capacidad de Virtual Server
  - Kilobytes / Segundo

- Round Trip Times

  Este modo de balanceo de carga selecciona el servidor virtual con el tiempo de ida y vuelta medido más rápido entre un Servidor y un cliente.

- Virtual Server Score

  El modo de equilibrio de carga de Virtual Server Score instruye al GTM para asignar solicitudes de conexión a servidores virtuales basándose en un sistema de clasificación definido por el usuario.

5 DEFINICIÓN DEL PROBLEMA.

5.1 SITUACIÓN INICIAL

Para efectuar el PDP Context, el cliente cuenta con configuración de DNSs tipo A y NAPTR, el flujo de configuración es el siguiente:

Registros Tipo A

1) El SGSN pregunta al DNS por la dirección del APN que el usuario tenga configurado, y haya sido validado.
2) El DNS, responde con una dirección IP al ser un registro tipo A. Esta dirección corresponde al GGSN/ PGW que está configurado para ese APN.

Registro tipo NAPTR

1) El SGSN pregunta al DNS por la dirección del APN que el usuario tenga configurado, y haya sido validado.
2) El DNS analiza su configuración de registro NAPTR (que tiene asociado un registro SRV que a su vez cuenta con un pool de GGSN / PGW, aunque con prioridades establecidas), y regresa una dirección de igual manera estática de un grupo de servidores para su redirección al GGSN/PGW de prioridad más alta.

5.2 PROBLEMÁTICA

Al obtener respuestas de carácter estático por parte de los servidores DNS, no hay manera en que se haga una conmutación automática en caso de que un GGSN o PGW presente problemas.

Suponiendo que un GGSN/ PGW fallara y no pudiera ejecutar sus funciones, la solución sería modificar los registros que apuntan hacia ese GGSN/PGW de manera manual, o en su defecto, cambiar el direccionamiento IP de los GGSN/PGW para suplirlo por otro que sea funcional.

Para un registro tipo A, modificar la dirección IP de todos los RR. Es importante mencionar que el número de registros a modificar sería considerable, y el tiempo de recuperación del servicio sería proporcional a esta cantidad.

Para un registro tipo NAPTR es modificar de igual manera la prioridad.

En el supuesto de que se escogiera modificar el elemento de red, se tendría que realizar cambios en varios equipos, en direccionamiento.

La problemática principal, es que la reactivación del servicio es dependiente del personal humano, y la solución o alternativas a la problemática actualmente son de carácter reactivo, es decir, ya que sucedió la falla, se procede a actuar.

Para un operador móvil o service provider es vital la operación y funcionalidad de todos los elementos de su red, que se presente una falla en un equipo que se encarga de gran parte de las funcionalidades del Core de la Red significa, en la gran mayoría de los casos, baja del servicio y perdida de la operación.

Cuando se presenta una falla en un equipo o elemento de la red, se procede a intentar, mitigar el problema, y que el servicio vuelva a operar lo más rápidamente posible.

En este caso, la solución que involucra la modificación de los registros en el DNS conlleva una gran cantidad de tiempo, de esfuerzo y de gran parte de su personal trabajando hasta que el problema se contenga.

La opción que involucra los cambios en la configuración de red, aunque parecen más simples, pueden presentar más riesgos a la red, y no es fácil que se aprueben debido a las afectaciones en políticas de firewalls y demás nodos de la red, lo que involucra la participación de más áreas y departamentos.

5.3 PROPUESTA DE SOLUCIÓN

La propuesta de solución surgió después de analizar las necesidades que presentaba nuestro potencial cliente, estudiar la tecnología con la que contábamos y trabajar sobre un laboratorio con equipo nuestro para realizar pruebas y ver lo que estaba en nuestras posibilidades ofrecer.

En el mundo de las tecnologías de la información es común que los vendedores de soluciones en primera instancia, realicen DEMOs o maquetas en nodos y equipos reales del cliente, principalmente debido a que las soluciones son costosas y para los clientes es importante probar las soluciones en su infraestructura y su red, analizar el comportamiento y validar su funcionamiento antes de proceder con la compra. En ocasiones, son varios los proveedores que proponen sus soluciones y tecnologías, en este caso, el cliente valora cuál le es más funcional y se entra a concurso.

Para esta propuesta de solución, el cliente contaba con un laboratorio equipado con los equipos necesarios de la red que nos permitieron hacer pruebas e implementaciones de este tipo, se nos permitió integrar parte de la configuración necesaria para este proyecto e interactuar con algunos de sus elementos:

- 2 nodos GGSN
- 2 servidores DNSs
- 1 SGSN

Por parte de nosotros se aprovisionaron dos F5 virtualizados en servidores que formaban parte de su infraestructura, ambos configurados en un hypervisor VMware. Los dos F5 contaban con licenciamiento para utilizar los módulos LTM y GTM.

La propuesta de solución implica configurar un clúster de 2 equipos F5, que funcionarán como un servidor proxy entre el SGSN y el DNS. A su vez, monitoreará los GGSN /PGW y hará una resolución inteligente de DNS basada en disponibilidad.

La propuesta de solución garantiza los siguientes puntos que se irán desglosando a continuación:

- Utilización de F5 como Proxy. Resolución de DNS Inteligente mediante monitoreo de DNS.

  El módulo GTM brinda las herramientas para la resolución de DNS inteligente. En el equipo F5 se configurará un pool que cuente con los GGSN/PGW disponibles, este pool estará relacionado con los nombres de dominio correspondientes a los APN que requieran alta disponibilidad en los GGSN/PGW.

  Al Pool de los GGSN/ PGW se le asignará un monitor de GTP que enviará constantemente mensajes GTP Echo a los GGSN/PGW, estos mensajes son equivalentes a un keepalive, por lo que cuando deje de recibir respuesta de un miembro del pool, declarará a ese GGSN/PGW como inactivo.
  El Pool se configurará con el método de balanceo Global Availability, es decir, se escogerá un GGSN/PGW como primario y procesará el tráfico a menos que este deje de estar disponible.

Esta funcionalidad permite que el DNS sea dinámico, que la respuesta a un DNS Query este en función de la disponibilidad de los GGSN/PGW y que en caso de que el GGSN/PGW primario deje de estar disponible, la conmutación sea automática y en segundos, es decir, que la respuesta al DNS Query muestre la dirección IP del GGSN/PGW secundario.

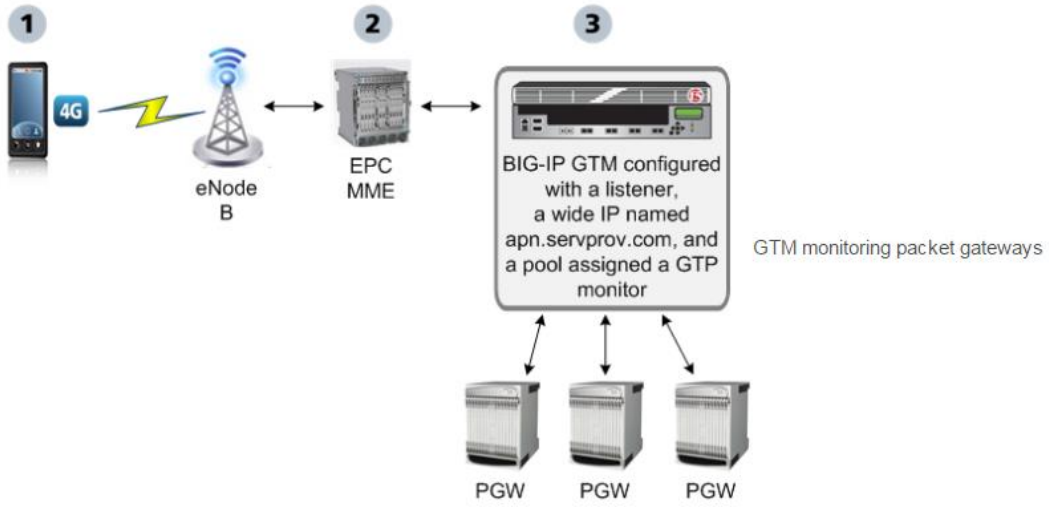

Figura 15. Solución de F5 como DNS Inteligente[20]

En la Figura 15 se muestra al F5 funcionando como DNS Inteligente en una arquitectura celular de cuarta generación, la cual es parte de la propuesta de solución que se configuró.

- Balanceo de Trafico de los servidores DNS que actualmente están funcionando.

A través del módulo GTM, el sistema F5 funcionaría como un DNS inteligente. Sin embargo, nos enfrentamos a la situación de que no se podía desechar la infraestructura de DNS con la que el cliente contaba debido a que tenía poco tiempo de haberse comprado, por lo que se buscó un escenario que pudiera adaptarse.

Nuestra propuesta fue habilitar la funcionalidad de DNS del equipo F5 exclusivamente para cuestiones de movilidad en el PDP Context para los APN que requieran alta disponibilidad, de tal forma que los DNS actuales puedan resolver los nombres de dominio que tengan la característica de ser funcionales estáticamente en segundo plano. Es decir, que el equipo F5 solo los redireccione con cierto método de balanceo previo, esto también serviría para no sobrecargar los servidores F5 con más procesamiento, permitiendo que los servidores DNS actuales funcionen óptimamente.

[20] Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm-implementations-11-5-0/9.html]

El módulo de GTM permite configurar diferentes características de resolución de DNS, por lo que el servidor F5 tiene ciertas prioridades al momento de recibir tráfico en el puerto 53. En primera instancia revisa si el nombre de dominio que se ha solicitado en un DNS Query está contenido en su base de datos, en caso de que lo encuentre, este se encarga de la resolución de acuerdo a su configuración. Sin embargo, en caso de que no lo encuentre lo redirecciona a cierto Pool de Servidores. En este Pool se configurarán los DNS actuales.

Esto significa que las peticiones de DNS se harán hacia la dirección que se encuentra configurada en el equipo F5 como puerto de escucha, posteriormente el servidor F5 será el encargado de decidir qué hacer con el tráfico.

Al momento de configurar un Pool debe establecerse también un método de balanceo, para este caso se configuro el método de Round Robin, ya que al ser todos los DNS de características similares, es funcional. El pool se configura con monitoreo de DNS Query, si detecta que todos los servidores DNS están respondiendo bien al monitoreo los sigue considerando al momento de hacer el balanceo, en caso de que uno de ellos deje de responder, este será descartado al momento de hacer el balanceo Round Robin y se pondrá en Estado no disponible.

- Balanceo de carga en GGSN/PGW según la localización geográfica, optimizando la funcionalidad activo-activo de ambos GGSN/PGW

Como se comentó en un inicio, uno de los propósitos de este proyecto es que se cuente con alta disponibilidad en los equipos GGSN/PGW sin embargo, en ocasiones al configurar alta redundancia, queda un equipo funcionando y otro equipo en standby. En este caso se hizo la propuesta con ambos equipos en estado activo a través de un balanceo por localización geográfica en la resolución de DNS

Para casos de esta propuesta se trabajó con dos supuestos:

- Región Norte
- Región Sur

Para cada una de las regiones se le asignará un GGSN/PGW como elemento primario, y el otro como secundario. Es decir, para la región Norte, el GGSN/PGW A será el elemento primario y el GGSN/PGW B el secundario, para la Región Sur la definición será a la inversa, el GGSN/PGW B será el elemento primario y el GGSN/PGW A el secundario.

Al momento de que los usuarios de determinada región soliciten un DNS Query al F5, este les responderá con el GGSN que tengan asignado como primario.

Esta configuración se logra mediante la creación de dos Pools de GGSN/PGW, cada uno con el método de balanceo de High Availability.

Un Pool tiene al GGSN/PGW A configurado en primer lugar, y el otro Pool tiene al GGSN/PGW B.

Ahora bien, a nivel Listener o Virtual Server (Que es el elemento que funciona como punto de escucha y el que recibe todo el tráfico) se ha configurado el método de balanceo Topology.

Esto permite que a los usuarios de cierta región geográfica se le asigne un pool y a los usuarios de la otra región geográfica se les asigne el otro, teniendo así ambos GGSN/PGW funcionando y en una configuración Activo-Activo.

En caso de que uno de los dos GGSN/PGW llegará a fallar, todo el tráfico lo tomaría el GGSN/PGW funcional debido al monitoreo constante que se está ejecutando por el F5.

- Configuración de alta disponibilidad en equipos F5 configurando un clúster HA.

Al vender una solución de TI, es importante garantizar su funcionalidad el 100% del tiempo, por lo que se debe considerar una solución de redundancia.
Un sistema redundante es un tipo de configuración del sistema F5 que permite continuar con el procesamiento de tráfico en caso de que un sistema F5 no esté disponible. Un sistema redundante F5 consta de dos unidades de configuración idéntica.
Cuando se produce un evento o incidente que impide que una de las unidades procese el tráfico de red, la unidad equivalente en el sistema redundante comienza inmediatamente a procesar ese tráfico y los usuarios no experimentan interrupción en el servicio.

El proceso de conmutación se llama Failover. Este se explica mejor con la siguiente imagen:

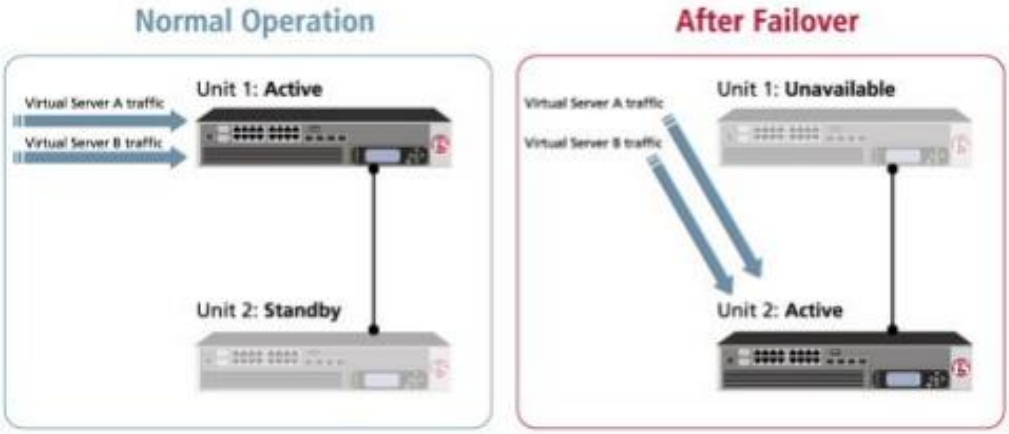

Figura 16. Proceso Failover de un sistema redundante F5.[21]

Es necesaria la configuración de una IP flotante en un sistema de redundancia. Una IP flotante es una dirección compartida entre dos sistemas F5.

[21] Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_0_0/tmos_high_avail.html]

Cuando dos unidades comparten una dirección IP propia flotante, el tráfico en ambos lados del proxy se puede enviar a esa dirección en lugar de una dirección IP automática estática. Si la unidad primaria de destino no está disponible, la unidad de redundancia puede recibir y procesar ese tráfico.

6 DESARROLLO DE LA CONFIGURACIÓN

NOTA: Debido a políticas de la empresa, y a que la realización de este proyecto se llevó a cabo en equipos del cliente, con direccionamiento y configuración relevante, las imágenes que se muestran son ejemplos de configuración tomadas de las páginas oficiales de soporte y foros de la marca, donde usuarios que configuran F5 pueden exponer preguntas, configuraciones y dudas.

Por otra parte, también se mostrará la guía de configuración vía CLI.

❖ CONFIGURACIÓN DE RED EN EQUIPO F5 Y CLUSTER DE ALTA DISPONIBILIDAD

Para que un equipo F5 se integre a la red, es importante hacer ciertas configuraciones de Red, entre las más importantes está el direccionamiento IP, Vlans, entre otros. Debido a que se está trabajando en un clúster de alta disponibilidad que integra 2 equipos, esto se debe realizar en cada uno de ellos, posteriormente se ejecutará y explicará la integración.

- Vlans.

En primer lugar, es necesario configurar las Vlans, la configuración más común incluye 2 Vlans, Interna y externa, esta se muestra a continuación.

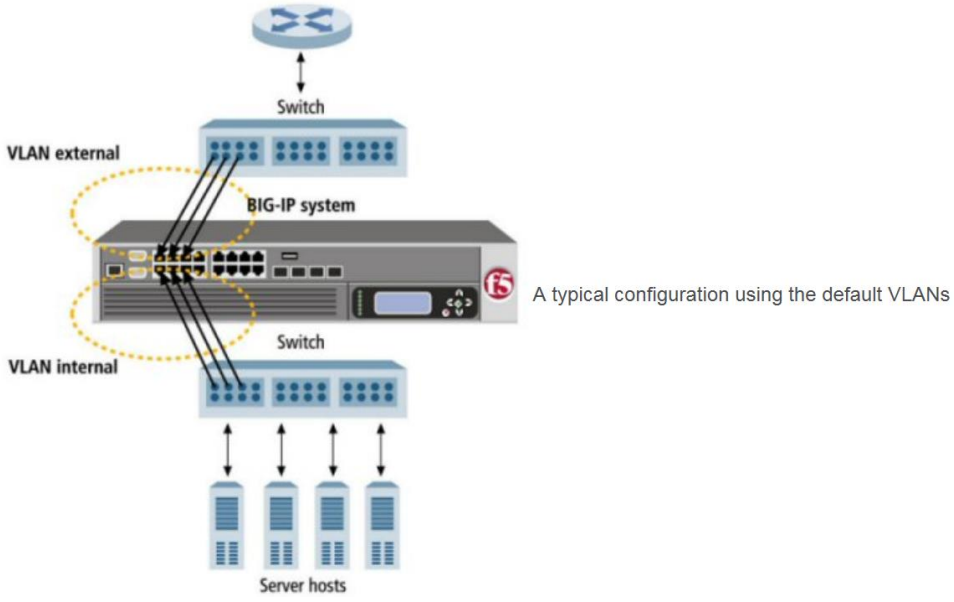

Figura 17. Configuración de Vlans.[22]

[22] Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1/tmos_vlans.html]

Típicamente, se suele usar esta configuración para el balanceo de carga, es más seguro contar con un lado para servidores, y otro para usuarios

Por el lado, en la Vlan interna se configura direccionamiento IP para que tenga contacto directo con los servidores entre los cuales se va a balancear.

Mientras, que en la Vlan externa es la comunicación con los usuarios que solicitaran las conexiones. De este lado se configuran los Virtual Server o Listener (Según la tecnología LTM o GTM).

En la Vlan, se configura Nombre, las interfaces que estarán configuradas para recibir tráfico de esta Vlan, si el tráfico será etiquetado o no (Tagged o Untagged).

Para la configuración de este proyecto se configuro solo una Vlan, debido a la característica de laboratorio y al direccionamiento que nos asignaron, sin embargo, para el ambiente de producción, si se aconsejó la creación de 2 Vlans.

NOTA: Es importante señalar que la creación de 2 Vlan se realizó para cumplir el requerimiento de Balanceo de Trafico de los servidores DNS que actualmente se encontraban funcionando, es decir, los servidores Bluecat.

Del lado de la Vlan Interna se configurarían estos, mientras que de la externa el GGSN /PGW que haría la petición. En caso de que no existieran estos servidores Bluecat, podría bastar con una sola, debido a que todas las resoluciones las haría el F5, y solo se necesitaría comunicación de un lado.

La configuración de las Vlans, se lleva a cabo en la pestaña de Network > VLANs.

Es posible configurar Vlans vía CLI con los siguientes comandos, ingresando a la herramienta TMSH propia del equipo Big-IP F5de la siguiente manera. La configuración siguiente ilustra la creación de 2 Vlans, una interna (Vlan_Interna) conectada en la interfaz 1.1 y una externa (Vlan_Externa) cuyo enlace es la interfaz 1.2.
Ambas Vlans estarán etiquetadas con las Vlans, 100 y 200, respectivamente.

Finalmente, la configuración se guarda. La configuración debe realizarse en cada uno de los equipos.

```
root@tmsh
root@(tmos)#create /net vlan Vlan_Interna interfaces add {1.1 {tagged}} tag 100
root@(tmos)#create /net vlan Vlan Externa interfaces add {1.2 {tagged}} tag 200
root@(tmos)#save /sys config
```

- Self IP

La creación de una Self-IP es posterior a una Vlan, ya que, al momento de la creación, es necesario que esta sea asociada a una. La Self IP, representa el direccionamiento que se le da a una interfaz, y es lo que hace el equipo alcanzable en la red.

La creación de Self- Ip es en Network > Self IPs.
Para cada una de las Self Ip es importante configurar nombre identificativo, la dirección IPv4 o Ipv6, máscara de red, se elige la Vlan a la que esta IP será asociada, así como se configura el bloqueo de puerto, de acuerdo a las características restrictivas de seguridad.

Existen 2 tipos de Self IP, las físicas y las flotantes, esta característica se configura en el campo Traffic Group. En este caso, como están referenciadas a una interfaz se consideran físicas.

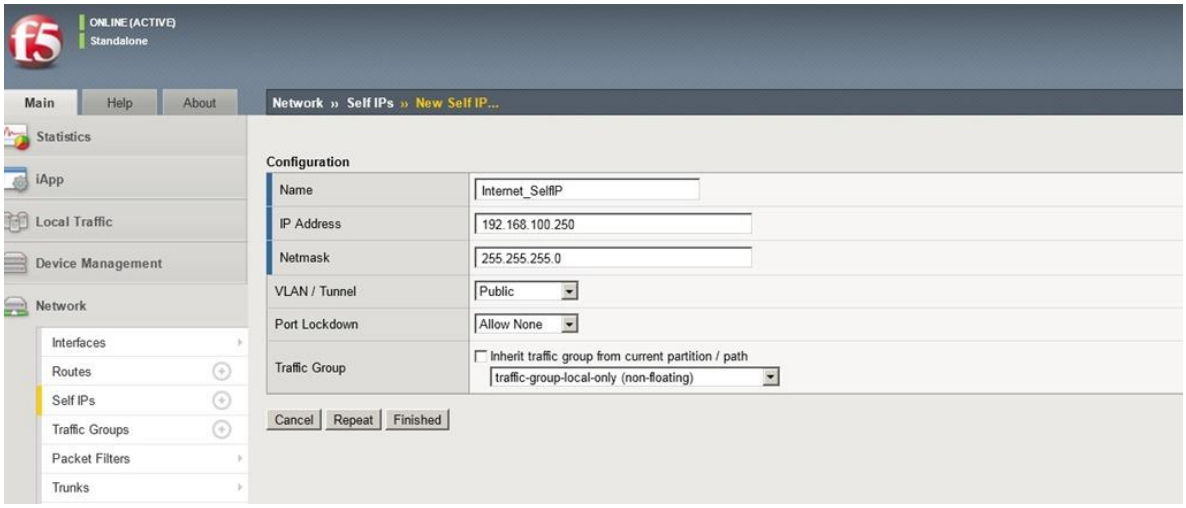

Figura 18. Ejemplo de creación de una Self IP[23]

Como se va a llevar a cabo, la creación de un clúster de HA, es necesaria la creación de una Self IP Flotante.
Una dirección Self IP flotante es una dirección IP que se comparte entre dos sistemas o entre dos unidades de un sistema redundante. Esta Ip es necesaria, para que, en caso de una falla, no haya dificultad con el envío y recepción de paquetes, ya que considera al equipo como uno solo.

A continuación, se mostrará la configuración de Self IPs en un equipo vìa CLI, este contendrà dos Self IPs físicas (Una por cada Vlan) y 2 Self IP flotantes (Debido a que son cluster).
El comando contiene las vlans a las que pertenecen, así como el nombre que le configura.
La distinción la hace el grupo de tráfico, las Ips físicas deben pertenecer al traffic-group-local-only, mientras que las flotantes son parte del traffic-group-1.

[23] Imagen obtenida del foro oficial de la marca [https://devcentral.f5.com/articles/quick-start-application-delivery-fundamentals]

```
root@ tmsh

root@(tmos)# create /net self IP Interna 10.10.10.1/24 vlan Vlan Interna traffic-group traffic-
group-local-only allow-all

root@(tmos)# create /net self IP_Externa 20.20.20.1/24 vlan Vlan_Externa traffic-group traffic-
group-local-only allow-all

root@(tmos)# create /net self IP_Interna_Flotante 10.10.10.3/24 vlan Vlan_Interna traffic-
group traffic-group-1 allow-all

root@(tmos)# create /net self IP_Externa_Flotante 20.20.20.3/24 vlan Vlan_Externa traffic-
group traffic-group-1 allow-all

root@(tmos)#save /sys config
```

- Ruteo estático o dinámico

Como un equipo con configuración en la capa 3 de red, es necesario contar con ruteo para saber qué hacer con el tráfico de datos. Cuando se configura una Self IP, el equipo automáticamente actualiza la tabla de enrutamiento con esa subred, sin embargo, es importante contar con un Gateway
El ruteo estático, o dinámico se configura en la siguiente pestaña: Network > Routes.
Es posible configurar un Default Gateway, Pool o Vlan, para que el equipo redirecciones el tráfico que no esté incluido en su tabla de enrutamiento.

Con esta información previamente configurada en cada uno de los dos equipos, se procede a la configuración del clúster.

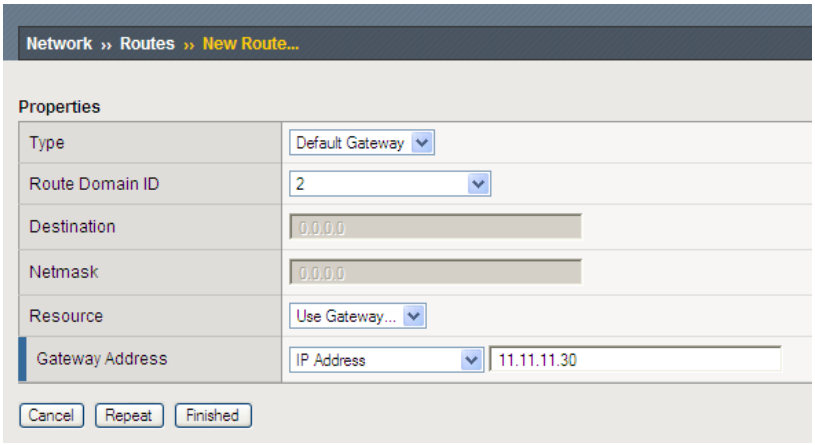

Figura 19. Ejemplo de configuración de Rutas[24]

La configuración de rutas estáticas se usa principalmente para configurar rutas por defecto, los siguientes comandos ilustran como se configura la ruta Default, tomando como Default Gateway una IP de la Vlan externa.

[24] Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1/tmos_routes.html]

```
root@ tmsh
root@(tmos)# create /net route Ruta DG 0.0.0.0/0 gw 20.20.20.254 vlan Vlan Externa
root@(tmos)#save /sys config
```

- Clúster De Alta Disponibilidad

Para la creación de un clúster de HA, es posible ir guiándose en la herramienta de Setup Utility que ofrecen los servidores F5.
En un principio solicita la creación de las Vlan Interna y externa, así como de una Vlan exclusiva para HA (Esta Vlan es opcional y tiene como propósito principal el intercambio de información de sincronización entre ambos dispositivos sin interferir en las interfaces que manejan el tráfico de datos, puede ocuparse alguna de las ya creadas).

Posteriormente se requiere un intercambio de certificados de seguridad entre ambos dispositivos. Desde uno de ellos, se realiza la petición hacia el otro dispositivo en la pestaña Devices > Peer List.
Para hacer el intercambio se solicitan las credenciales del otro equipo, asì como su dirección IP, ya que se ha aceptado, aparece una imagen como la siguiente, donde se aprecia que el equipo local es el bigip1.example.com y el elemento que ya aparece dentro de sus Peer es el bigip2.example.com.

Como aún es necesaria más configuración, en la parte superior izquierda aparece el estado de Disconnect.

Posteriormente se lleva a cabo la creación de un grupo o cluster de equipos F5, para formar el grupo de alta disponibilidad.
Se configura el nombre, tipo de failover, así como los miembros que lo conforman, si se desea la sincronización automática o no.

Después de cierto tiempo en el que se lleva a cabo la sincronización, ambos equipos aceptan la configuración y se sincronizan, su estado pasa de desconectado a Online.

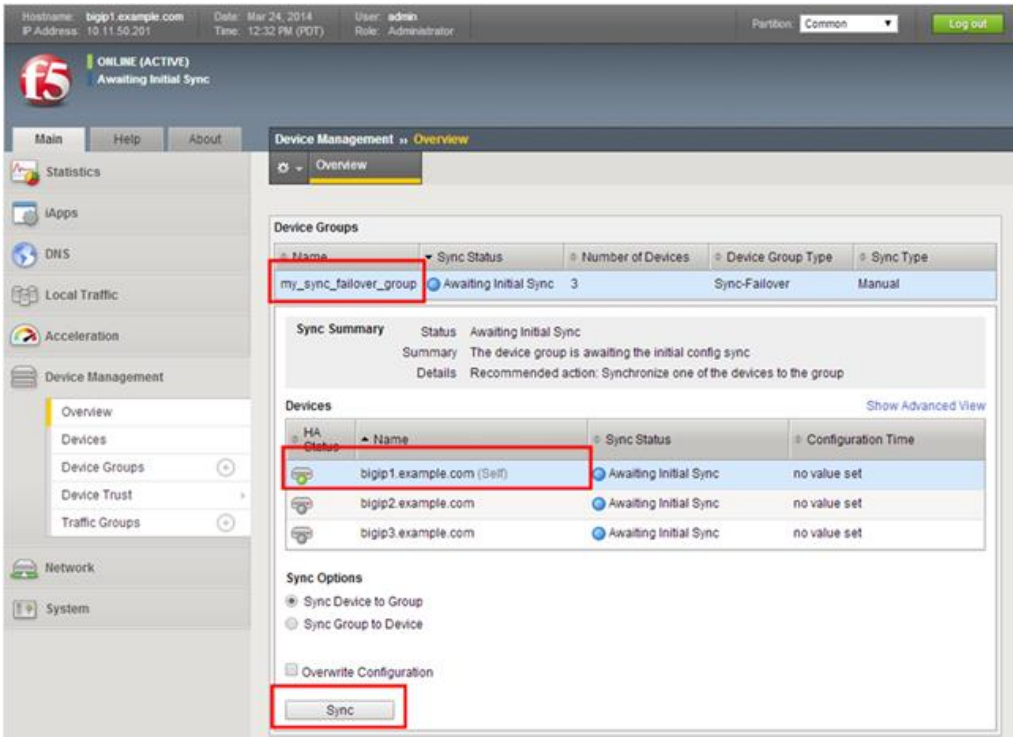

Figura 20. Ejemplo de creación de grupo de failover F5[25]

La configuración vía línea de comados se lleva a cabo de manera similar, se identifica el equipo, con su nombre, así como la IP que funionará como IP de Failover y de cluster HA, en este caso la perteneciente a la Vlan Interna, posteriormente se solicita el intercambio de certificados de seguridad, donde es necesario introducir las credenciales del otro equipo, y posteriormente son agrupados en el Cluster.

El penúltimo comando pretende ejecutar la sincronización.

```
root@(tmos)#modify /cm device equipo1.prueba.demo configsync-ip 10.10.10.1

root@(tmos)#modify /cm device equipo1.prueba.demo unicast-address {{ ip 10.10.10.1 }}

root@(tmos)#modify /cm trust-domain /Common/Root add-device { device-ip 192.168.0.1 device-
name equipo2.prueba.demo username admin password admin

root@(tmos)#list /cm trust-domain

root@(tmos)#create /cm device-group Grupo_HA devices add { equipo1.prueba.demo
equipo1.prueba.demo } type sync-failover

root@(tmos)#run /cm config-sync to-group Grupo HA

root@(tmos)#save /sys config
```

[25] Imagen obtenida del foro oficial de la marca [https://devcentral.f5.com/articles/scalen-a-network-architect-engineers-unofficial-guide-to-scalen-clustering]

❖ UTILIZACIÓN DE F5 COMO PROXY. RESOLUCIÓN DE DNS INTELIGENTE MEDIANTE MONITOREO A LOS GGSN/PGW Y BALANCEO DE CARGA EN GGSN/PGW SEGÚN LA LOCALIZACIÓN GEOGRÁFICA

Los proveedores de servicios pueden configurar el sistema BIG-IP GTM para aumentar la disponibilidad de sus servicios. Una forma es configurando un monitor GTP para medir la disponibilidad de una serie de equipos GGSN/ PGW. El monitor GTP emite una solicitud de eco a dicha serie de equipos. Si un GGSN/ PGW no responde a la solicitud de eco de GTP, se marca como no disponible y se elimina de la lista de sistemas GGSN/ PGW disponibles que se devuelven a un SGSN/ MME en una respuesta de DNS.

GTM gestiona sólo los registros A y AAAA para el balanceo global de carga del servidor (GSLB).

El siguiente diagrama muestra al F5 funcionando como DNS Inteligente, en una arquitectura celular de cuarta generación, que es parte de la propuesta de solución que se configuró.

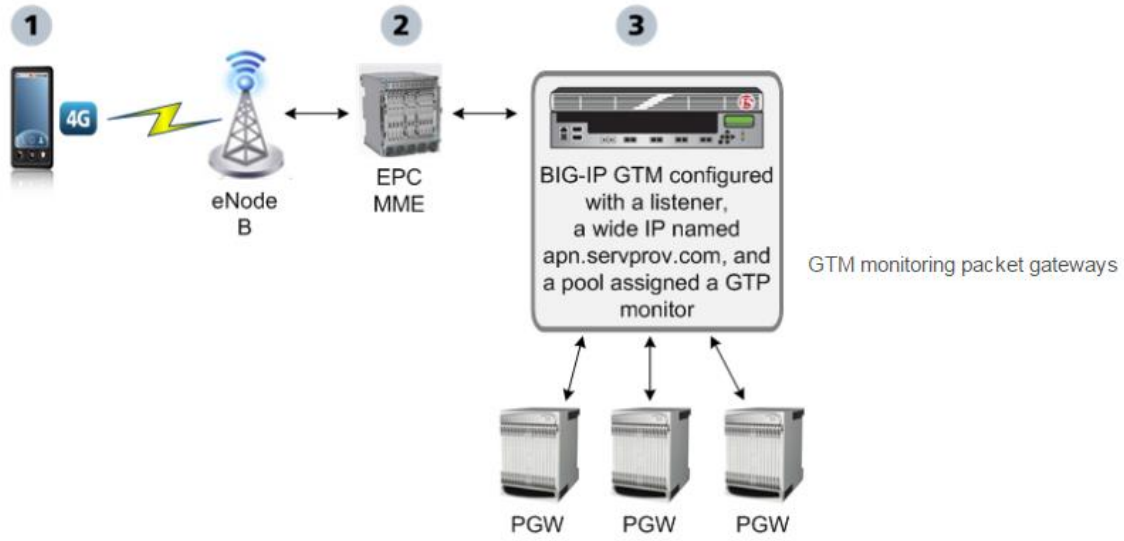

Figura 21. Solución de F5 como DNS Inteligente[26]

Los pasos a seguir para la configuración de esta solución son los siguientes, y se aplican en el módulo de DNS > GSLB

1. Definir un Data Center

Se crea un Data center que contenga los servidores que tomarán un representarán los equipos en una subred de las que se configurarán. Es posible configurar Nombre, Locación y el Punto de Contacto. En este caso, se configuraron 3, uno representando al Cluster de equipos F5, otro al GGSN 1 y otro al GGSN 2.

[26] Imagen obtenida de la página oficial de soporte de la marca [https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm-implementations-11-5-0/9.html]

```
root@ tmsh

root@(tmos)#create gtm datacenter GGSN1 GGSN2 Cluster

root@(tmos)#save /sys config
```

2. Definir Sistemas BIG-IP GTM y LTM

En este apartado se configura un objeto de servidor para representar el propio sistema GTM, así como los sistemas LTM involucrados. Se lleva a cabo en la configuración de Servers.

Se deben configurar previamente los Data Center, ya que estos se vinculan.

A cada sistema se le configura Nombre, Tipo de Producto (En este apartado es posible configurar si es un Sistema simple o en redundancia), dirección o direcciones IP del servidor.

NOTA: No es posible configurar la IP de Management de un servidor.

Se escoge el Data Center, monitores de disponibilidad, así como servidores virtuales asociados al servidor. Es indispensable contar, al menos con uno para su funcionamiento.

La configuración incluyó 2 equipos que conforman el clúster LTM-GTM.

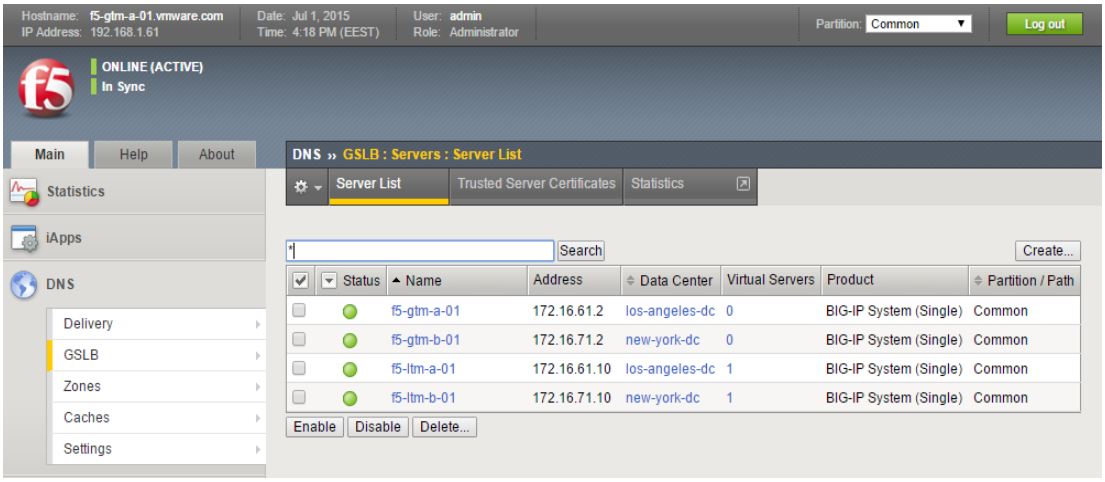

Figura 22. Ejemplo configuración de equipos LTM y GTM F5[27]

Los siguientes comandos muestran la creación de los dos servidores pertenecientes al cluster.

```
root@ tmsh

root@(tmos)# create gtm server gtm-ltm1 addresses add { 10.10.10.1 } monitor bigip datacenter
Cluster virtual-servers add { 10.10.10.1:80 }

root@(tmos)# create gtm server gtm-ltm2 addresses add { 10.10.10.2 } monitor bigip datacenter
Cluster virtual-servers add { 10.10.10.2:80 }

root@(tmos)#save /sys config
```

[27] Imagen obtenida de un foro de TI [http://kaloferov.com/blog/geo-location-based-traffic-management-with-f5-big-ip-for-vmware-products-poc-f5-big-ip-gtm-configuration/]

3. Definición de Sistemas GGNS/PGW

De manera similar al paso anterior, se configura un objeto lógico Server por cada uno de los GGSN/PGW con los que se trabajara.

A cada uno se le asigna un nombre, el tipo de producto (En este caso se configura como Generic Host, al no ser un equipo F5), la dirección IP, el Data Center Asociado a cada uno, monitores asociados, en el campo de servidores virtuales, se solicita la creación de uno, es decir, una dirección y un puerto o servicio (socket).

NOTA: Aunque es posible la adición del monitor de GTP desde este punto, lo recomendable, para mejores prácticas es adicionarlo en la configuración del Pool de Servidores.

```
root@ tmsh

root@(tmos)#create gtm server GGSN1 addresses add { 20.20.20.100 } monitor none datacenter
GGSN1 virtual-servers add { 20.20.20.100:* }

root@(tmos)#create gtm server GGSN2 addresses add { 20.20.20.200 } monitor none datacenter
GGSN2 virtual-servers add { 20.20.20.200:* }

root@(tmos)#save /sys config
```

4. Creación de Listeners para identificar el tráfico de DNS hacia un APN

La creación de Listener se hace para identificar tráfico DNS hacia un nombre de punto de acceso específico (APN). La mejor práctica es crear dos Listener: uno que se encargue de manejar el tráfico UDP y otro que maneje el tráfico TCP, sin embargo, es posible su funcionamiento con uno solo.

En la opción de DNS > Delivery, se configuran los Listener, para cada uno de ellos es posible asignarle un nombre, la dirección de escucha (A la que se enviarán las peticiones para su procesamiento), El protocolo a utilizar (UDP o TCP), en caso de que se configure uno solo, lo recomendable es configurar UDP.

Se mostrará la guía de configuración vía línea de comandos, y la Figura 23 muestra las opciones de configuración vía Interfaz gráfica.

```
root@ nano /config/bigip local.conf

/config/bigip_local.conf

virtual address 10.10.10.100 {
   floating disable
   unit 0
}
virtual Listener DNS {
   destination 10.10.10.100:53
   ip protocol udp
   translate address automap
   translate service disable
   profile dns DNS TP
}

root@ bigip load
```

La configuración vía comandos, en este caso es diferente, debido a que se edita un archivo, facilitando la configuración del listener. Pueden configurarse tantos parámetros, como se decida, los parámetros que no sean agregados al archivo, tomarán los valores por default.

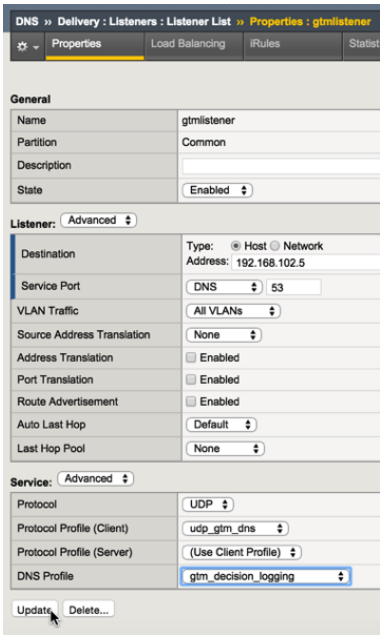

Figura 23. Ejemplo Creación de Listener.[28]

5. Creación de un monitor GTP personalizado.

Se crea un monitor GTP personalizado para detectar la presencia y la integridad de un GGSN o PGW. El monitor GTP emite una solicitud de eco GTP y si el sistema GGSN o PGW no responde, se marca automáticamente como No disponible y se elimina de la lista disponible de sistemas GGSN/PGW que el sistema BIG-IP devuelve a un SGSN/MME.

En el apartado DNS > GSLB > Monitors, es posible configurar diversos tipos de monitores

Para esta configuración en particular, será de GTP. Se le debe asignar un nombre, en el campo de Type, se selecciona GTP.

En el campo Interval, se indica el número en segundos, con qué el sistema emitirá la comprobación del monitor. El valor predeterminado es 30 segundos.

En el campo Timeout, se debe configurar en segundos, cuánto tiempo el destino tiene para no responder a la comprobación del monitor. El valor predeterminado es 120 segundos. Si el objetivo no responde dentro del período de tiempo configurado, se considera No disponible.

Se escribe un número en el campo Versión de protocolo que indica la versión del protocolo GTP que el sistema utiliza. El valor predeterminado es 1.

[28] Imagen obtenida de la página oficial de soporte de la marca [https://devcentral.f5.com/articles/configuring-decision-logging-for-the-f5-big-ip-global-traffic-manager]

6. Creación de un Pool de sistemas GGSN / PGW

Después de configurar los servidores que representarán a los GGSN/PGW, y el monitor que se les configurará, es posible proceder a la configuración del Pool.

Un Pool se crea en la sección DNS> GSLB> Pools.

Se le debe configurar un nombre que lo identifique, se selecciona el o los monitores aplicables (En este caso el monitor GTP que se creó anteriormente).

También se debe configurar el método de Balanceo aplicable al Pool.

Finalmente, se agregan los miembros que conforman este Pool, y entre los cuáles se efectuará el balaceo.

De acuerdo a la solución propuesta, se configuraron dos Pool, ambos con el método Global Availability seleccionado, sin embargo, uno de los Pool tenía al GGSN 1 configurado en primer lugar y al GGSN 2 en segundo lugar, mientras el otro, contenía el orden invertido.

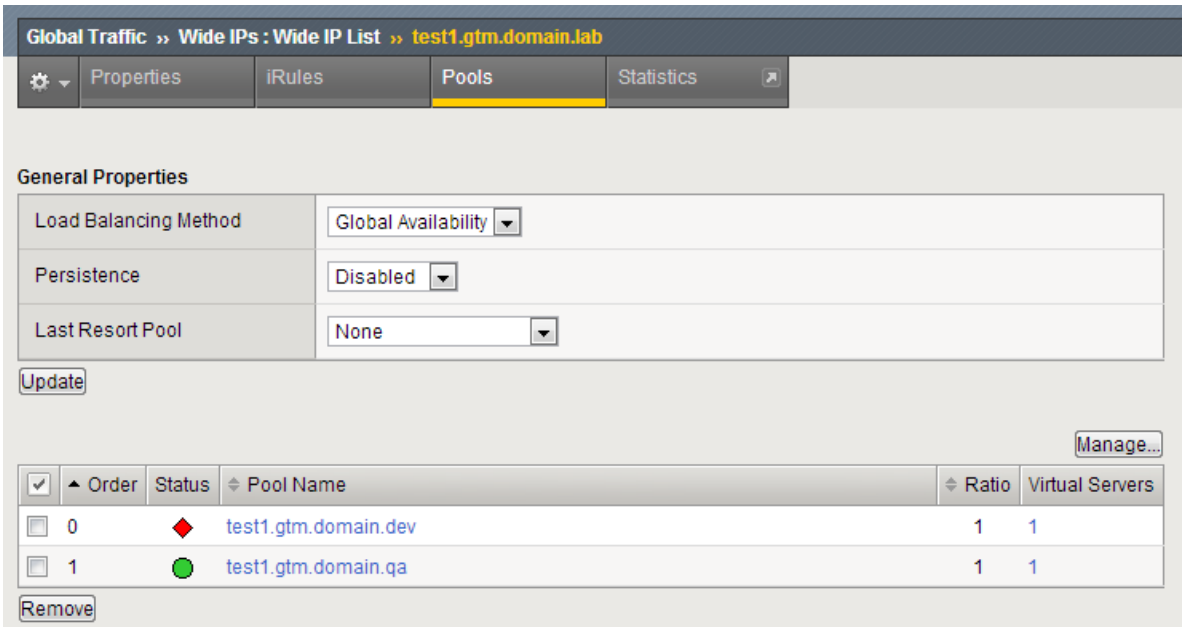

Figura 24. Ejemplo Pool con método de balanceo Global Availability.[29]

En el ejemplo se observan dos miembros pertenecientes al Pool, debido al método configurado, se debe escoger siempre el primer elemento, a menos que este no esté disponible, como es el caso en la imagen, en ese caso todas las conexiones serán enviadas al elemento en verde.

La creación vía Línea de comando, se realizaría de la siguiente manera, de igual forma configurando dos pools, considerando cada elemento con diferente valor de ratio em cada uno de ellos.

[29]Imagen obtenida de la página oficial de soporte de la marca [https://devcentral.f5.com/questions/gtm-global-availability-load-balancing-to-down-pool]

```
root@ tmsh

root@(tmos)#create gtm pool Pool Region Norte members add { 20.20.20.100:* {ratio 1}
20.20.20.200:* {ratio 2} } load-balancing-mode global-availability verify-member-availability
GTP_Monitor

root@(tmos)#create gtm pool Pool_Region_Sur members add { 20.20.20.200:* {ratio 1}
20.20.20.100:* {ratio 2} } load-balancing-mode global-availability verify-member-availability
GTP_Monitor

root@(tmos)#save /sys config
```

7. Configuración de Registro de Topología.

El registro de Topología, se lleva a cabo en el apartado de Global Traffic, cada registro requiere:
Una instrucción Source de solicitud que define el origen de una solicitud de conexión. Una instrucción de destino que define el recurso al que el equipo F5 dirigirá la solicitud de conexión. Un peso (puntaje de topología) asignado por el sistema a un objeto servidor durante el proceso de equilibrio de carga.

Para el proyecto en particular se configuraron como fuente 2 subredes diferentes, una que representaba terminales móviles de la región norte, y otra que representaba usuarios de la región sur.

Como destino a cada uno se le configuro un Pool creado en el paso anterior, es decir, al registro que identificaba la primera subred se le configuro el Pool que tenía configurado el método de balanceo Global Availability con el GGSN 1 en primer lugar, y al GGSN 2 en segundo.

Al segundo registro de topología se le configuro el otro Pool, uno que contenía de igual forma el método de balanceo Global Availability con el GGSN 2 como primario, y al GGSN 1 como secundario. Se muestran las opciones de configuración vía CLI y vía GUI.

```
root@ tmsh

root@(tmos)#create gtm topology ldns: subnet 1.1.1.1/10 server: pool /Common/Pool_Region_Norte
{order 1}

root@(tmos)#create gtm topology ldns: subnet 2.2.2.2/10 server: pool /Common/Pool Region Sur
{order 2}

root@(tmos)#save /sys config
```

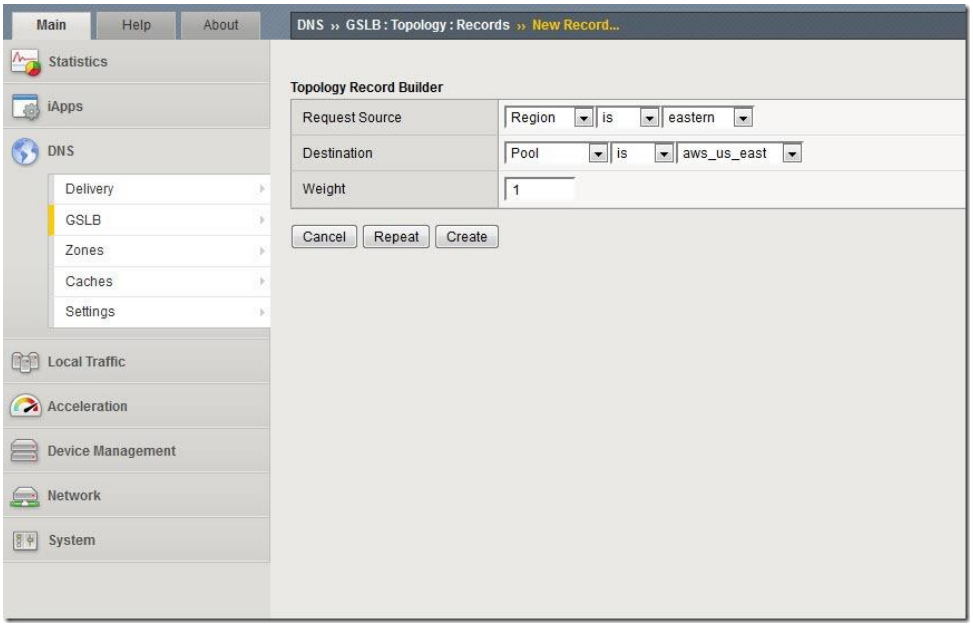

Figura 25. Ejemplo creación Registros Topología.[30]

8. Configuración de una Wide IP para el nombre de un APN

En la pestaña correspondiente a DNS> GSLB> Wide IPs, se procede a configurar una Wide IP. Para su configuración, en el apartado del nombre, se configura el APN, la dirección a la que preguntarán los móviles.

De igual forma se seleccionan el o los Pools que se deseen configurar, y el método de balanceo seleccionado.

De acuerdo a la solución propuesta, en esta sección se eligió el método de balanceo Topology, y se agregaron los dos Pools que se habían configurado en pasos anteriores, al actuar el método de balanceo, este efectuará el balanceo de acuerdo a los registros de Topología que se crearon en el punto anterior.

```
root@ tmsh

create gtm wideip apn.prueba.demo pool-lb-mode topology pools add { Pool_Region_Norte { ratio
1 } Pool_Region_Sur { ratio 2 } }

root@(tmos)#save /sys config
```

[30] Imagen obtenida de la página oficial de soporte de la marca [https://devcentral.f5.com/articles/using-big-ip-gtm-to-integrate-with-amazon-web-services]

- **Balanceo de Trafico de los servidores DNS que actualmente están funcionando.**

  Finalmente, un requerimiento de este proyecto era que los equipos que actualmente se encontraban funcionando siguieran siendo útiles, lo que permitía optimizar los equipos evitando que estos se cargarán con más procesamiento.

  Para esta configuración, se configuro el Balanceo más común en F5, Un Pool con los servidores DNS actuales, con el método de balanceo estático Round Robin.

  En el Listener, se configuro como Default Pool, el que contenía estos elementos, de tal forma, al momento de hacer una petición, el F5 revisa si contenía el Registro en su base de datos, en caso de que no, este redirigía la petición a cualquiera de los miembros de este Pool de acuerdo a su método de balanceo de carga.

```
root@ tmsh

root@(tmos)# modify /gtm listener Listener_DNS address 10.10.10.100:53 ip-protocol udp pool
Pool_DNS_Bluecat translate-address automap translate service disable profile dns DNS_TP

root@(tmos)#save /sys config
```

7 CONCLUSIONES

Este documento retrata mi desempeño como profesional en la administración e implementación de proyectos. La presentación de esta DEMO; significo el primer proyecto a mi cargo como Ingeniero de Diseño e Implementación.

Este proyecto consistió en el desarrollo de una solución de las muchas que día a día se ofrecen en el mercado de las tecnologías de la información. Siempre buscando mejorar el rendimiento, la operación o las velocidades de transmisión, la evolución en la telefonía móvil ha sido constante y apresurada.

La demanda por un mejor servicio, mayor calidad y la alta disponibilidad que exigen los usuarios finales obligan a los operadores de redes celulares a estar en constante actualización de tecnología, así como buscar soluciones que cubran sus necesidades y deficiencias actuales.

Los retos principales de un Vendedor de soluciones es visualizar oportunidades de negocio, en los puntos débiles de la infraestructura del cliente. Esta propuesta surgió al observar un punto de falla, la necesidad de una conmutación automática en caso de que un elemento importante en el Core de la red (GGSN o PGW, según la tecnología) dejara de funcionar

Después de hacer un análisis detallado de los recursos tecnológicos que podíamos ofrecer, presentamos una solución que cubría sus necesidades y que inclusive presentaba algunas características adicionales como la optimización de los recursos por medio del balanceo de tráfico.

La presente propuesta fue configurada en la infraestructura del cliente, se presentaron y se explicaron los detalles de la configuración y se hicieron pruebas para validar su correcto funcionamiento.

Es importante remarcar que en este proceso estábamos compitiendo con otro vendor que ofrecía una solución que pretendía cubrir la misma necesidad el cliente de contar con redundancia.

Finalmente, la propuesta fue comprada por el cliente.

A lo largo de

Aunque el día de hoy, ya no me desempeño profesionalmente en esta empresa, el pertenecer a una empresa pequeña, me dio la oportunidad de desempeñar diferentes actividades, en las áreas de soporte, diseño e implementación en una variedad de áreas de las telecomunicaciones.

Obtuve conocimientos en Servidores Linux, Servidores DNS, Virtualización, Recuperación y Alta Disponibilidad em ambientes virtualizados,

8 REFERENCIAS

BIBLIOGRAFICAS

- GSM - Architecture, Protocols and Services, Jörg Eberspächer,Hans-Joerg Vögel,Christian Bettstetter,Christian Hartmann.
- Manual de Telefonía. Telefonía Fija y Móvil. José Manuel Huidobro Moya. Ed. Paraninfo. 1998
- GPRS Networks, Sanders Geoff, Thorens Lionel, Reisky Manfred, Rulik Olver, Deylitz Stefan, Editorial Wiley.

ARTÍCULOS

- GSM Network Architecture by Ian Poole.
- SISTEMA EMBEBIDO PARA LA CONEXIÓN DE UN PLC SIEMENS S7-200 A LA RED GSM, Velasco Martos, Nicolás
- High Speed Circuit Switched Data Joint SMG1, SMG2, SMG3, SMG4 Workshop. Publicado por ETSI. e-REdING, Trabajos y proyectos fin de estudios de la E.T.S.I.

ELECTRONICAS

- https://f5.com/products/big-ip/local-traffic-manager-ltm
- https://f5.com/products/big-ip/global-traffic-manager-gtm
- http://www.cisco.com/c/es_mx/support/docs/wireless/mme-mobility-management-entity/119015-technote-mme-00.html
- https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_0_0/tmos_high_avail.html
- https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1/tmos_selfips.html
- https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm_config_guide_10_1/gtm_loadbal.html
- https://support.f5.com/kb/en-us/products/big-ip_gtm/manuals/product/gtm_config_guide_10_1/gtm_topology_newest.html#1028268
- http://www.itu.int/itunews/issue/2003/06/thirdgeneration-es.html
- https://support.f5.com/csp/article/K7117

ANEXO 1. ESPECIFICACIONES DE HARDWARE F5

BIG-IP System
HARDWARE DATASHEET

Deliver More Applications for More Users

BIG-IP® Application Delivery Networking platforms can manage even the heaviest traffic loads at both layer 4 and layer 7. By merging high performance switching fabric, specialized hardware, and advanced software, F5 provides the flexibility to make in-depth application decisions without introducing bottlenecks.

With the high performance you get from BIG-IP platforms, you can consolidate devices— saving management costs, electricity, space, and cooling—and still have room to grow.

Key Benefits

Consolidate your infrastructure with purpose-built hardware

BIG-IP hardware platforms are designed specifically for application delivery. One device can be configured for server load balancing, global data center load balancing, web application firewall, HTTP acceleration, spam filtering, and WAN optimization.

Offload application servers

BIG-IP systems feature high-performance SSL and compression hardware as well as advanced connection management to remove processingintensive tasks from application servers and use these resources more efficiently.

Secure your network

Instantly add a layer of security with BIG-IP systems, providing default deny security and a full packet filter engine that can limit access in a very granular way.

Reduce your operating costs

Spend less time on configuration, upgrades, and maintenance with the simple-to-manage BIG-IP hardware, featuring out-of-band management, front-panel management, warm upgrades, remote boot, and USB support.

Maximize uptime

Ensure your critical infrastructure is built on reliable hardware with hot-swappable components, redundant power supplies, redundant fans, compact flash, multi-boot support, and always-on management.

8900 Series

6900 Series

Specifications	8900 Series	6900 Series
Traffic Throughput:	12 Gbps	6 Gbps
Hardware SSL:	Included: 500 TPS Maximum: 58,000 TPS, 9.6 Gbps bulk encryption	Included: 500 TPS Maximum: 25,000 TPS, 4 Gbps bulk encryption
FIPS SSL:		FIPS 140-2 Level 2 (option) 20,000 TPS
Hardware Compression:	Included: 50 Mbps Maximum: 8 Gbps	Included: 50 Mbps Maximum: 5 Gbps
Processor:	Dual CPU, quad core (8 processors)	Dual CPU, dual core (4 processors)
Memory:	16 GB	8 GB
Hard Drive	Two 320 GB drives	Two 320 GB drives
Gigabit Ethernet CU Ports:	16	16
Gigabit Fiber Ports (SFP):	8 LX; SX or copper (4 SX included)	8 LX; SX or copper (4 SX included)
10 Gigabit Fiber Ports (SFP+):	2 SR (sold separately)	
Power Supply:	Dual 850W included	Dual 850W included
Typical Consumption:	450W (110V input)	300W (110V input)
Input Voltage:	90-246 VAC +/- 10% auto switching, 50/60hz	90-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	1536 BTU/hour (110V input)	1024 BTU/hour (110V input)
Dimensions:	3.5”H x 17.3”W x 21.4”D 2U industry standard rack-mount chassis	3.5”H x 17.75”W x 20.75”D 2U industry standard rack-mount chassis
Weight:	45.5 lbs. (dual power supply)	45.5 lbs. (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2	32° to 104° F (0° to 40° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Relative Humidity:	5 to 85% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2	5 to 85% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2
Safety Agency Approval:	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950 EN 60950	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950 EN 60950

Certifications/ Susceptibility Standards:	EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A	EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A

BIG-IP System

3900 Series

3600 Series

1600 Series

Specifications	3900 Series	3600 Series	1600 Series
Traffic Throughput:	4 Gbps	2 Gbps	1 Gbps
Hardware SSL:	Included: 500 TPS Maximum: 15,000 TPS, 2.4 Gbps bulk encryption	Included: 500 TPS Maximum: 10,000 TPS, 2 Gbps bulk encryption	Included: 500 TPS Maximum: 5,000 TPS, 1 Gbps bulk encryption
Software Compression:	Included: 50 Mbps Maximum: 3.8 Gbps	Included: 50 Mbps Maximum: 1 Gbps	Included: 50 Mbps Maximum: 1 Gbps
Processor:	Quad core CPU	Dual core CPU	Dual core CPU
Memory:	8 GB	4 GB	4 GB
Hard Drive	300 GB, 10K RPM	320 GB	320 GB
Gigabit Ethernet CU Ports:	8	8	4
Gigabit Fiber Ports (SFP):	4 optional LX, SX, or copper	2 optional LX, SX, or copper	2 optional LX, SX, or copper
Power Supply:	One 300W included, dual power option	One 300W included, dual power option	One 300W included, dual power option
Typical Consumption:	175W (110V input)	165W (110V input)	150W (110V input)
Input Voltage:	90-240 VAC +/- 10% auto switching	90-240 +/- 10% VAC auto switching	90-240 +/- 10% VAC auto switching
Typical Heat Output:	598 BTU/Hour (110V input)	563 BTU/hour (110V input)	512 BTU/hour (110V input)
Dimensions:	1.75”H x 17”W x 21”D (per unit) 1U industry standard rack-mount chassis	1.75”H x 17”W x 21”D (per unit) 1U industry standard rack-mount chassis	1.75”H x 17”W x 21”D (per unit) 1U industry standard rack-mount chassis
Weight:	20 lbs. (one power supply)	20 lbs. (one power supply)	20 lbs. (one power supply)
Operating Temperature:	32° to 104° F (0° to 40° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2	32° to 104° F (0° to 40° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2	32° to 104° F (0° to 40° C) per Telcordia GR-63-CORE 5.1.1 and 5.1.2

Humidity:	10 to 90% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2	10 to 90% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2	10 to 90% @ 40º C, per Telcordia GR-63-CORE 5.1.1 and 5.1.2 Relative
Safety Agency Approval:	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950	UL 60950 (UL1950-3) CSA-C22.2 No. 60950-00 (bi-national standard with UL 60950) CB TEST CERTIFICATION TO IEC 950
Certifications/ Susceptibility Standards:	EN 60950 EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A	EN 60950 EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A	EN 60950 EN55022 1998 Class A EN55024 1998 Class A FCC Part 15B Class A VCCI Class A

More Information

Visit these resources on F5.com to learn more about the BIG-IP family of products.

Datasheets

BIG-IP® Local Traffic Manager™

BIG-IP® Global Traffic Manager™

BIG-IP® Application Security Manager™

BIG-IP® Link Controller™

BIG-IP® Secure Access Manager™

BIG-IP® WebAccelerator™

Reports

F5 Application Delivery Controller Performance Report

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447
www.f5.com

F5 Networks, Inc.
Corporate Headquarters
emeainfo@f5.com

F5 Networks
Asia-Pacific
f5j-info@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

F5 Networks
Japan K.K.
info@f5.com
info.asia@f5.com

IT agility. Your way.