Red Celular para la Conectividad de Soluciones IoT y M2M

Angela Natalia Noguera Valdes

Director: Dr. Luis Eduardo Tobón Llano

Pontificia Universidad Javeriana Cali
Facultad de Ingeniería y Ciencias.
Ingeniería Electrónica.
Trabajo de grado.

Tabla de contenido

Tabla de Ilustraciones

GLOSARIO

3GPP: por las siglas de 3rd Generation Partnership Project, dedicado a definir las especificaciones sistema global de comunicaciones de tercera generación 3G para teléfonos móviles.

Ancho de banda: Se trata de la capacidad máxima y la cantidad de datos que se pueden transmitir a través de una conexión (de internet, por ejemplo), en un momento determinado.

APN: Access Point Name, es el nombre de un punto de acceso que hay que configurar para que un dispositivo se pueda conectar a Internet usando las redes de una operadora y también para poder recibir y enviar mensajes multimedia.

B2B: Business to Business, es el marketing hacia las empresas.

B2C: Business to Consumer, es el marketing hacia consumidores.

CSP: Communications Service Provider, proveedor de servicios de comunicaciones es un proveedor de servicios que transporta información electrónicamente, por ejemplo, un proveedor de servicios de telecomunicaciones

EDGE: Enhanced Data Rates for GSM Evolution (tasas de Datos Mejorada para la Evolución del GSM) y también conocida como Enhanced GPRS (EGPRS) o GPRS Mejorado. Es una tecnología de telefonía móvil celular, que actúa como puente entre las redes 2G y 3G.

ETSI: El Instituto Europeo de Normas de Telecomunicaciones, es una organización de normalización independiente, sin fines de lucro de la industria de las telecomunicaciones de Europa.

FDMA: El acceso múltiple por división de frecuencia, también conocido como FDMA es una técnica de multiplexación usada en múltiples protocolos de comunicaciones, tanto digitales como analógicos, principalmente de radiofrecuencia, y entre ellos en los teléfonos móviles de redes GSM

GGSN: Gateway GPRS Support Node, este nodo se encarga de «enrutar» los paquetes de datos a los diferentes usuarios que en cada momento se encuentran conectados.

GPRS: General Packet Radio Service, es un servicio basado en la conmutación de paquetes que permite tasas de transferencia de 56 a 114 Kbps y una conexión continua a Internet desde un teléfono móvil o un ordenador. A GPRS se le considera como 2.5G.

GPS: Global Positioning System, surgido en el año 1993, permite determinar dónde se encuentra situado un objeto determinado, ya sea persona, vehículo o nave, de manera muy precisa.

GRE: Generic Routing Encapsulation, es un protocolo para el establecimiento de túneles a través de Internet. Está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar hasta 20 protocolos del nivel de red distintos.

GSM: Global System for Mobile Communications, se la conoce como la segunda generación de telefonía móvil (2G). Esta especificación de telefonía móvil digital buscaba consolidarse como el estándar europeo de telefonía celular, de forma que se pueda utilizar un mismo teléfono en cualquier país del continente.

HSCSD: Servicios de Datos Conmutados por Circuito de Alta Velocidad.

IMSI: es el acrónimo de International Mobile Subscriber Identity. Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

IoT: Internet of Things, conecta todo tipo de sistemas y objetos. Es el concepto general que abarca la red de dispositivos físicos, vehículos, electrodomésticos y otros elementos integrados con dispositivos electrónicos, software, sensores y conectividad a Internet que permiten que dichos dispositivos se conecten e intercambien datos.

IP: La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

LAN: Local Area Network, es una red de comunicación de datos que está situada habitualmente en un mismo edificio (no tiene grandes dimensiones) y que posibilita que las máquinas conectadas transmitan información de unas a otras mediante alguno de los protocolos existentes.

M2M: Machine to Machine, es un concepto genérico que se refiere al intercambio de información o comunicación en formato de datos entre dos máquinas remotas.

MCC: son las siglas en inglés de Mobile Country Code, es un código numérico usado juntamente con el MNC para identificar el país y los operadores de telefonía móvil que utilizan ya sea GSM, CDMA, UMTS, LTE y ciertas redes satelitales. Ambos códigos quedan definidos en la ITU E.212.

MMS: El servicio de mensajería multimedia, es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video o fotos.

MNC: son las siglas en inglés de Mobile Network Code, es un código numérico usado juntamente con el MCC para identificar el país y los operadores de telefonía móvil que utilizan ya sea GSM, CDMA, UMTS, LTE y ciertas redes satelitales. Ambos códigos quedan definidos en la ITU E.212.

MPLS: MultiProtocol Label Switching, es un mecanismo de transporte de datos. La tecnología MPLS ofrece una función de etiquetado para el tráfico IP que fluye en toda una red. Con éste, los administradores pueden controlar y dar forma al tráfico y permitir la QoS de extremo a extremo.

Packet Tracer: es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red.

PDH: es una tecnología usada en telecomunicación tradicionalmente para telefonía que permite enviar varios canales telefónicos sobre un mismo medio usando técnicas de multiplexación por división de tiempo y equipos digitales.

PDP: Protocolo de Paquetes de Datos, proporcionando al SGSN la dirección del GGSN por el que acceder al servicio.

PSTN: Public Switched Telephone Network, Red Telefónica Pública Conmutada.

QoS: Quality of Service, calidad de un servicio de trasmisión en base a las tasas de transferencia y los errores durante la comunicación.

RAB: Radio Access Bearer, Un servicio portador es un enlace entre dos puntos, que se define por un cierto conjunto de características. Siempre que a un equipo de usuario (UE) se le proporcione cualquier servicio (servicio CS / PS), el servicio debe estar asociado con un portador de radio que especifique la configuración para la capa 2 y la capa física para tener su QoS claramente definida.

RDSI: Red Digital de Servicios Integrados, servicio telefónico digital de alta velocidad que puede aumentar sustancialmente la velocidad de conexión a Internet o a una LAN corporativa.

SDH: es un conjunto de protocolos de transmisión de datos, que trabaja realizando multiplexación por división el tiempo. Toma pequeñas ranuras de tiempo y las ubica en forma ordenada en una ranura de tiempo más grande.

SGSN: Serving GPRS Support Node, este nodo se encarga de «enrutar» los paquetes de datos a los diferentes usuarios que en cada momento se encuentran conectados.

SIM: Subscriber Identity Module, es una tarjeta que contiene un chip de computadora, que mantiene un registro de un número telefónico, los servicios

incluidos en una suscripción, los nombres y números de los contactos, entre otras cosas.

SMS: Short Message Service, es un método para recibir y enviar mensajes de teléfono móvil a teléfono móvil.

TDMA: Time Division Multiple Access, Acceso de Multiplexación por División de Tiempo, permite que a cada uno de los terminales se le asigne un período de tiempo concreto para que pueda acceder al sistema de comunicaciones.

UICC: son unas tarjetas con chip usadas en teléfonos móviles en redes GSM y UMTS

VPN: Virtual Private Network, es una extensión de una red privada que abarca vínculos encapsulados, cifrados y autenticados en redes públicas o compartidas. Las conexiones VPN pueden proporcionar acceso remoto y conexiones enrutadas a redes privadas a través de Internet.

WAP: Wireless Application Protocol, Protocolo de Aplicaciones Inalámbricas, es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo: acceso a servicios de Internet desde un teléfono móvil.

RESUMEN

El proyecto desarrolla un estudio de la utilización de la red celular en la comunicación de las soluciones M2M e IoT, cuya definición y componentes se introducen al inicio del documento para luego realizar un enfoque hacia el ámbito de conectividad, particularmente el uso de las redes celulares, como medio de transporte para la información de los dispositivos que forman parte de las soluciones M2M e IoT.

En los primeros capítulos se hace una apropiación del marco teórico de las redes celulares, iniciando con los estándares que sirven como fuente para el presente documento, para luego realizar una aproximación a las generaciones de redes celulares con el fin llegar a la definición de la arquitectura base y la caracterización de sus principales componentes. Una vez se ha establecido el marco teórico del documento, se profundiza en los factores que se recomienda tener en cuenta dentro del diseño y la implementación de la conectividad para soluciones de M2M e IoT.

Entre los factores que se recomienda, se encuentran aspectos de configuración dentro de la red celular y alternativas de integración de la red celular con redes externas, los cuales se utilizan en el planteamiento de tres casos de uso dentro del documento. Posteriormente, con el conocimiento recopilado, se establece un flujo de opciones básicas, encaminadas a buscar el diseño apropiado según las necesidades de cada solución, concluyendo que con el uso de la tecnología celular en la conectividad de soluciones M2M e IoT se aportan, no solo todas las bondades de la tecnología móvil, sino que además es posible su integración con redes externas generando un mayor crecimiento en posibilidades de conexión al mundo M2M e IoT.

1. INTRODUCCIÓN

Las tecnologías de la información y las telecomunicaciones, hace ya varios años vienen experimentado evoluciones, que abren el camino a la aparición de nuevas soluciones y herramientas, que se integran de forma cada vez más importante en la ejecución de diversas actividades cotidianas en ámbitos de trabajo, educación y consumo.

En la aparición de estas nuevas soluciones, son las telecomunicaciones una pieza clave para potencializar su despliegue, por ejemplo, con el incremento en el uso de las tecnologías de comunicaciones inalámbricas, entre las cuales la más destacada es la comunicación vía red celular, que debido a su economía respecto a otro tipo de tecnologías como la satelital, proporcionando además mayor cobertura y ancho de banda. Aunque en su momento, la tecnología celular fue pensada solo para la transmisión de voz, la convergencia e integración de redes y servicios, han orientado su evolución a la generación de nuevos sistemas de gestión de datos con crecientes capacidades a menores costos, frente a los servicios convencionales. Todo esto ha reforzado cada vez más su uso e impacto en las tareas diarias de la sociedad.

A la par con la evolución de la red celular, se han desarrollado simultáneamente, avances tecnológicos hacia terminales inteligentes y almacenamiento de información en la nube, los cuales se integran para permitir procesar, transmitir y acceder a la información de manera rápida, eficaz, desde cualquier lugar y momento. Como producto de estas integraciones aparecen por ejemplo las soluciones Machine-to-Machine (en adelante, M2M) o Internet of Things (en adelante, IoT), que aprovechan el crecimiento en redes móviles y su empleabilidad entre las personas para permitir que las empresas obtengan información de los servicios y/o productos que prestan actualmente, permitiéndoles tener mayor visibilidad de su negocio y además, generen nuevos nichos de mercado con el único fin de aportar al crecimiento sostenible de las organizaciones, de los países y de su ciudadanía[1].

Actualmente existen compañías de sectores como el productivo, salud o educación, que han integrado las soluciones celulares a su gestión corporativa, al representar

[1] ITU: Internet de las cosas podría ser la "clave de conectividad" de bajo coste que transforme las vidas en los países en desarrollo. En: ITU [en línea]. Disponible en:http://www.itu.int/net/pressoffice/press_releases/2016/02-es.aspx#.V1DglvnhDIU > [Citado en Junio de 2016]

una alternativa flexible, escalable y de bajo costo, logrando diferenciarse en el mercado con una ventaja competitiva para quien lo haga parte de su motor de desarrollo. Permitiendo, por ejemplo, establecer comunicaciones remotas entre máquinas, logrando unificar a través de accesos inalámbricos las bases de datos y las aplicaciones empresariales, propiciando nuevos servicios en telemedicina, telemetría, seguimiento vehicular, entre otros.

Esta tendencia de las compañías y el mercado refuerza el que se pueda hablar de redes celulares y soluciones M2M e IoT al mismo tiempo ya que al integrar estos mundos se maximizan las ventajas en los diferentes campos de la sociedad. De allí que el objetivo del presente documento es apropiarse de la teoría necesaria para entender los elementos de comunicaciones que toman partido de esta integración y el cómo este conocimiento aplicado a problemas reales permite generar soluciones flexibles, operando en el mundo de las redes celulares, las redes tradicionales y los servicios M2M e IoT.

Los elementos antes mencionados, contienen una gran cantidad de componentes, buscaremos comprender su papel dentro de la integración, profundizando especialmente en los que conforman el Comunication Service Provider (en adelante CSP), que son los encargados de establecer la comunicación entre los elementos de la solución. De igual manera, como aporte y conociendo que no se cuenta con simuladores de redes celulares, se buscará emular en el software Packet Tracer, el comportamiento de algunos dispositivos de redes para aproximarnos a una configuración que permita entender el papel que desempeñan los APN en la interconexión entre redes móviles y las redes fijas, que al final es lo que permite maximizar las aplicaciones de soluciones de M2M e IoT. Al final del trabajo se buscará comprender y explotar las ventajas que estas soluciones tienen en el día a día de las empresas y de las personas, a través del análisis de tres tipos de servicios de M2M e IoT que son usados en la actualidad, donde se revisara las formas de personalización dependiendo del negocio, dando así alternativas para que cualquier compañía pueda interiorizar, diseñar y usar, soluciones M2M e IoT utilizando la red celular.

2. SOLUCIONES M2M e IoT

Las soluciones M2M e IoT, han aparecido en el mercado de las soluciones digitales, como una alternativa de comunicación que aporta mayor valor a los servicios de conectividad tradicional, permitiendo ofrecer nuevas y novedosas alternativas. Aunque los conceptos de M2M e IoT puede llegarse a considerar como iguales, es importante precisar a qué corresponde cada uno. Las soluciones de IoT se han convertido en un término ampliamente utilizado para el conjunto de tecnologías y sistemas asociados a las cosas conectadas a Internet y, por otro lado, M2M es propio de las soluciones que involucran la comunicación entre máquinas.

Tomando como referencia el concepto anterior, es posible suponer que la principal diferencia entre ambos tipos de soluciones se enfoca en los dispositivos finales que se emplean, los puntos que se abordarán en el presente trabajo ofrecen una visión general en el papel que las redes de comunicaciones y la conexión con redes externas juega en la implementación de soluciones IoT y M2M.

Con el fin de comprender las interacciones entre los diferentes componentes dentro de las soluciones, se plantea iniciar desde una arquitectura general hasta llegar a los elementos de interés del presente trabajo. Para lo anterior, se toma con referencia a nivel de arquitectura de alto nivel la definida por ETSI, donde se segmenta las soluciones M2M en: dominio de aplicaciones, dominio red y dominio dispositivos. Ilustración 1 Arquitectura Simple de M2M ETSI.

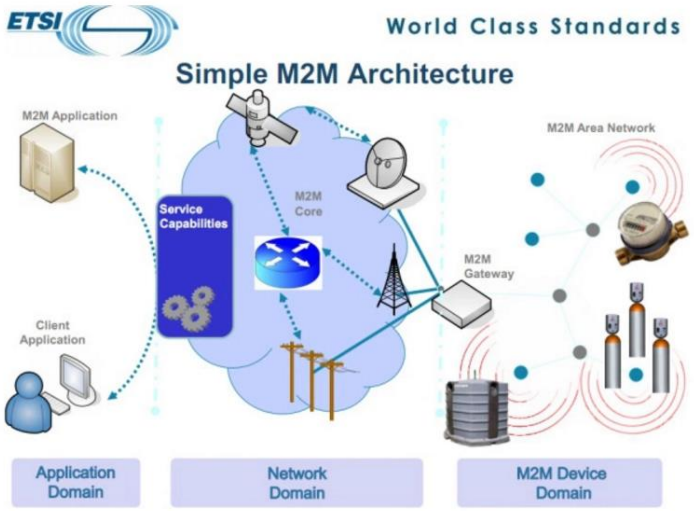

Ilustración 1 Arquitectura Simple de M2M ETSI[2]

Basados en la arquitectura definida, se puede observar como el dominio de redes, representa el punto intermedio de la solución, y sus componentes serán el foco principal del presente trabajo, como se verá más adelante. Dado que el tráfico ingresa a la red utilizando ciertos protocolos y bajo ciertas consideraciones, es viable tratarlo de la misma manera independiente del tipo de solución, por lo que son aplicables tanto para los servicios M2M como IoT.

Como ya se mencionó, las redes de comunicaciones proporcionan la infraestructura necesaria para conectar todos los elementos de la solución, antes de continuar desglosando los elementos de red es importante revisar la cadena de valor como se muestra en la Ilustración 2 y que se listan a continuación:

- Dispositivos
- Comunicaciones
- Aplicaciones
- Servidores

[2]Omar Elloumi, Susana Sabater, David Boswarthick. (14 de junio de 2010). *ETSI TC Machine to Machine Where Smart Grids meet M2M* [Diapositiva de PowerPoint]. SlideShare. https://www.slideserve.com/niran/etsi-tc-machine-to-machine-where-smart-grids-meet-m2m > [Citado en Junio de 2016]

Ilustración 2 Componentes de la cadena de valor soluciones M2M e IoT. Fuente Propia

2.1. Dispositivos

Se encuentran dentro del dominio de dispositivos M2M de la arquitectura ETSI y hace referencia a la máquina o elemento conectado al activo de interés, proporciona la capacidad de detección y actuación; dependiendo del nivel de complejidad, el dispositivo se compone de un sensor y de una capa de comunicación requerida para interactuar con la red.

El sensor, por ejemplo, en el caso del seguimiento vehicular estaría compuesto por un módulo con GPS que permita recopilar los datos de su posición, acoplado a un hardware que los trasmita a la red. Dependiendo de las funcionalidades de la solución, se emplearán sensores de temperatura, aceleración u otros según la información requerida.

En la capa de comunicación, se debe establecer una comunicación con la máquina, que será el elemento para monitorear, y por el otro con la red de acceso hacia los dispositivos o servidores que lo requieran, es decir que debe ser provisto por una capa de conexión a un red cableada o inalámbrica.

En el caso de que se utilice la red móvil para el transporte de los datos, los dispositivos deben poseer la electrónica necesaria para incorporar una tarjeta SIM como medio para establecer la conexión hacia la red móvil. Normalmente las tarjetas SIM empleadas en este tipo de soluciones son más robustas que las que se emplean para establecer las comunicaciones entre usuarios a través de la red móvil, esto debido a que probablemente estarán expuestas a condiciones ambientales y de movimiento que requieran mayor exigencia física y durabilidad.

En la medida en que se estandariza y maximiza el intercambio de información utilizando tecnologías de comunicaciones celulares a través de aplicaciones que se usan en muchos contextos de la vida, también se incrementa el desarrollo e inclusión de dispositivos en soluciones M2M e IoT, los cuales pueden ir desde computadoras personales, servidores y hardware dedicado de conmutación de paquetes, teléfonos inteligentes, televisores, dispositivos para propósitos específicos entre otros.

2.2. Aplicaciones

Están dentro del dominio de aplicaciones dentro de la arquitectura ETSI y son la capa de software que permite proporcionar una solución integral M2M e IoT adaptada a requerimientos específicos. Este software puede ir desde la interfaz en interacción con el usuario final hasta contener toda la inteligencia necesaria para interpretar los datos provistos por los sensores y otros elementos de la solución. Es importante qué en el desarrollo de una aplicación, bien sea especifica o la adaptación de una genérica, se contemple la unificación con el dispositivo en el cual se implementará, para garantizar no solo su integración, sino también su mayor desempeño.

2.3. Servidor

Para efectos del presente trabajo, se discriminan los servidores en representación del punto de recolección y almacenamiento de la información que puede ser aplicable en diferentes tipos de soluciones. El servidor normalmente se encuentra alojado en la red LAN (Local Área Network) del cliente o proveedor, ya que habitualmente interconecta los sistemas de operación de la organización, esto dependerá de la solución que se esté manejando.

2.4. Comunicaciones

Como se mencionó anteriormente, dentro del dominio de comunicaciones de la arquitectura ETSI, se encuentran la infraestructura de comunicaciones, la cual tanto en las soluciones M2M como IoT se podría emplear redes cableadas o inalámbricas para establecer comunicación entre los elementos que la componen, la comunicación principal generalmente se realiza a través de la red de transporte que proveen las empresas de telecomunicaciones, encargadas de proveer la conectividad necesaria para enlazar todos los elementos que se requieren integrar.

El segmento de comunicación es el elemento intermedio entre los dispositivos. Comúnmente las tecnologías de tipo inalámbricas son las más usadas para enlazar el dispositivo con los servidores o para llevar la información de la aplicación al destino según se haya establecido en el diseño. Al igual que con el resto de los componentes es vital para el funcionamiento de M2M e IoT, conocer y comprender su función y demás consideraciones para tener en cuenta para asegurar que sea la adecuada para un correcto desempeño. Este elemento es el que se tratara en detalle en este documento, centrado en la red móvil, qué elementos, configuraciones y diseños se usan para interconectar el mundo de aplicaciones/dispositivos con los servidores. No será parte del objeto de este trabajo la comunicación del sensor con la máquina y el dispositivo.

3. PAPEL DE LAS REDES CELULARES EN LAS SOLUCIONES M2M E IoT

El presente trabajo está orientado al componente de comunicaciones, que en adelante llamaremos, Communication Service Provider (CSP) y que hace referencia al servicio ofrecido normalmente por los proveedores de telecomunicaciones para establecer la comunicación dentro de la solución. Para el caso práctico de las soluciones en estudio, es importante analizar dos frentes: la conexión de los dispositivos a la red, y la integración de dicha conexión con redes externas como las redes LAN de las organizaciones que podrían formar parte de la solución y donde podrían estar alojados los servidores de datos.

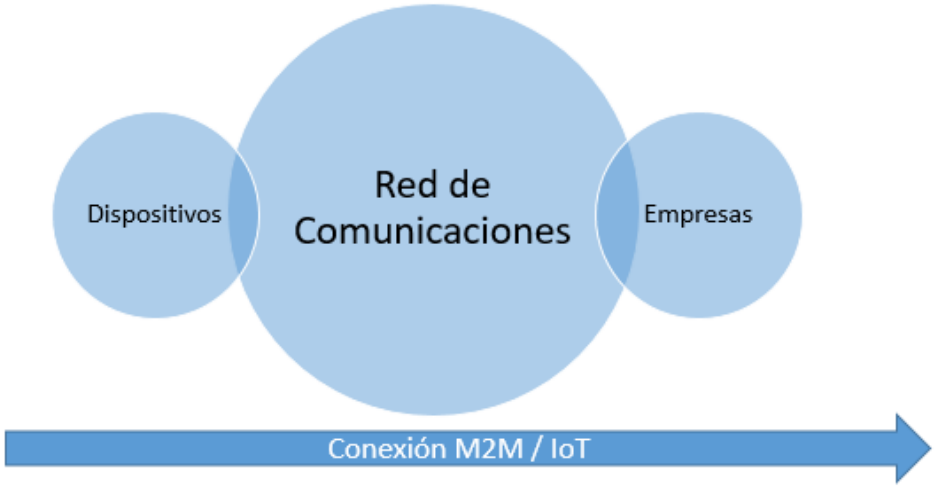

Ilustración 3 Relación de las conexiones en una solución M2M e IoT. Fuente propia

Como se observa en la Ilustración 3, la red de comunicaciones es el elemento central que permite la interconexión entre los dispositivos y las demás redes. En ambos extremos el tipo de tecnología de comunicación pueden ser cableadas o inalámbricas, sin embargo, emplear tecnología inalámbrica, sobre todo del lado de los dispositivos, facilita el poder incursionar en soluciones novedosas ya que facilita el despliegue e implementación en lugares de difícil acceso para las redes cableadas. Lo anterior permite reducir además los costos de inversión, en cuanto a infraestructura y soporte de la operación.

De allí que el crecimiento en el uso de redes celulares como mecanismo de comunicación en los servicios de M2M e IoT, permite maximizar el aporte de dichas soluciones en entornos donde no se cuenta con conexiones fijas, cobrando así mayor valor para el usuario que pueda acceder a servicios independientemente del lugar, cubriendo así zonas en las cuales hace unos años sería imposible o sumamente costoso llegar con los servicios.

En la actualidad las conexiones M2M e IoT emplean la red celular para soluciones en campos como: telemetría, gestión de flotas, seguridad, servicios financieros y nuevos servicios que se incorporan cada vez más a la sociedad. A su vez, han aparecido subgrupos de servicio clasificados según el tipo de cliente final que hace uso de servicio, es decir, modelos Business a Business (en adelante, B2B), donde

se desarrollará un gran porcentaje del mercado M2M e IoT, Business a Consumer (en adelante, B2C) que exigen mejoras a los modelos anteriores B2B o generan integraciones como B2B2C.

Dadas las ventajas que estas integraciones proporcionan, se ha apalancado el crecimiento en el uso de aplicaciones y dispositivos M2M e IoT, teniendo un crecimiento que se puede considerar proporcional al crecimiento en la cantidad de usuarios con acceso a la red móvil, marcando una tendencia en las continuas mejoras en el desempeño de los dispositivos y permitiendo nuevas funcionalidades, que a su vez aportan en la aparición de nuevas soluciones y usuarios al mundo M2M e IoT. Esta dinámica, conlleva constantes exigencias en los diferentes eslabones de la cadena de servicio, con múltiples requisitos en términos de tasa de intercambio de datos, computación y comunicaciones.

Para facilitar y mejorar el desempeño de la conexión de los dispositivos a la red de comunicaciones, se debe conocer los mecanismos disponibles para transportar la información de punta a punta incluyendo además la integración con soluciones empresariales, las cuales pueden llegar a requerir una personalización ajustada a las necesidades, llevando el análisis más allá de las soluciones genéricas o soluciones horizontales hacia soluciones particulares o soluciones verticales, es decir, aplicaciones orientadas a un único y específico mercado.

Como se menciona anteriormente, en el campo de las soluciones verticales, se ha hecho necesarias exigencias particulares para las redes de los CPS, que, si bien ya han adaptado las soluciones empresariales a sus redes tradicionales, ahora deben hacer lo propio para incorporar las redes celulares. Esto ha generado la necesidad de modelos específicos en términos de tecnología y plataformas, que permitan la interoperabilidad con el resto de los servicios del mercado, haciendo necesaria la definición y utilización de estándares, que logren suplir no solo las necesidades de las soluciones verticales, sino que además puedan coexistir con el resto de los servicios y así garantizar el crecimiento futuro.

Esto implica contemplar diseños de soluciones donde se puede utilizar, por ejemplo, la tecnología MPLS (Multiprotocolo Label Switching) como un actor con el cual sea necesario integrar las redes celulares. Esta integración se puede llevar a cabo a través de diferentes medios, el cual se selecciona tomando en cuenta una serie de consideraciones técnicas y económicas. Técnicamente, el medio seleccionado para

la integración debe cubrir por el ejemplo el ancho de banda requerido para la transacción o el tipo de comunicación, si se requiere que sea bidireccional o unidireccional, entre otros aspectos necesarios para garantizar la viabilidad y funcionalidad de las soluciones. Simultáneamente, las diferentes soluciones tecnológicas requieren también consideraciones de tipo económicas y operativas, tales como el costo de despliegue y mantenimiento de la infraestructura de red. Por ejemplo, una integración utilizando fibra óptica como medio de conexión puede conllevar inversiones de instalación y operativas importantes si la zona que se requiere cubrir es una amplia región geográfica.

Para abordar de la mejor manera las distintas situaciones y alternativas que se pueden presentar en el momento de diseñar una solución con una integración que involucre la red celular, se considera importante conocer los elementos básicos que componen este tipo de tecnología y así comprender que opciones se tiene para trabajar con ellos de la mejor manera. Con el fin de aportar al entendimiento de estos elementos, en los siguientes capítulos realizaremos una apropiación de la teoría básica en sistemas celulares.

4. SISTEMAS CELULARES

Las redes celulares están conformadas por celdas distribuidas geográficamente para dar cobertura a una zona o región específica. Con el paso del tiempo han evolucionado, integrando nuevas funcionalidades, dando paso a servicios convergentes de transmisión de voz y datos entre redes celulares y hacia redes externas; entre las características más importantes de los sistemas celulares, está el proporcionar movilidad a los usuarios, a través de funcionalidades de traspaso entre celdas y la reutilización de frecuencias.

Es precisamente esta propiedad de movilidad la que podríamos considerar la principal característica de las redes celulares ya que brinda la posibilidad de que un usuario activo pueda moverse dentro de la red, pasando de una celda a otra estableciendo vías de comunicación entre el teléfono móvil y la celda inmediatamente actual. Permitiendo así que los usuarios puedan acceder a los servicios independientemente del lugar y el momento.

Los siguientes capítulos, resumen conceptos de la red celular, que es importante conocer, para entender cómo se establece la comunicación entre el dispositivo la

red móvil y cómo dicha red, a su vez, se conecta con la red externa que puede albergar los servidores o la red LAN de las empresas. Finalmente, estos conocimientos de red móvil permitirán comprender como se establece un contexto PDP, con el uso de un APN y como el túnel tipo GRE facilitan las conexiones con una red celular.

4.1. Estándares de los Sistemas Celulares

La aparición de los sistemas celulares representó un importante avance a nivel de sistemas de comunicaciones, en sus inicios se utilizaban diferentes estándares dependiendo de la región, esto complicó la interconexión entre sistemas de diferentes proveedores de servicios, dado que no existía la posibilidad de roaming; en consecuencia, se limitaba la movilidad y la penetración de los servicios celulares.

Con el crecimiento en la demanda de los servicios celulares, se entendió la importancia de generar estándares globales, que permitieran la interoperabilidad de los diferentes sistemas celulares y con ello el crecimiento y la diversidad de servicios. Los diferentes estándares que han aparecido se pueden agrupar en redes de 2da, 3ra, 4ta y 5ta generación, cada uno incorporando cambios a su generación predecesora; de cada cambio, hizo parte importantes organizaciones que formaron grupos encargados de analizar lo actual y el futuro de la tecnología celular.

En el presente documento se da especial preferencia a la bibliografía de los diferentes estándares generados, además de literatura de apoyo para comprender los temas más relevantes de las diferentes generaciones.

Entre los organismos de estandarización que se encargan de la normalización de las Tecnologías de la Información y la comunicación (TICs), está ETSI la cual *"produce estándares globalmente aplicables para la Información y Tecnologías de la Comunicación (TIC), incluyendo telefonía fija, móvil, radio y convergentes, tecnologías de difusión e Internet"*[3]. Dependiendo del fin ETSI produce estándares puntuales distribuidos de la siguiente manera:

- Norma Europea (EN).
- ETSI estándar (ES).

[3] ETSI, About ETSI [en línea].< http://www.etsi.org/about > [Citado en noviembre de 2015]

- Guía ETSI (EG).
- ETSI Especificación Técnica (TS).
- Informe técnico del ETSI (TR).
- Informe Especial del ETSI (SR).
- ETSI Grupo de Especificación (GS).

Adicional a ETSI, entre las organizaciones se suma un grupo de organizaciones conformado en 1998, denominado 3GPP, que se enfocó en las especificaciones técnicas globalmente aplicables a sistemas móviles de tercera generación y sus evoluciones.

> *El 3GPP está formado por (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) y abarca las tecnologías de redes de telecomunicaciones móviles, incluidas las de acceso de radio, la red básica de transporte, y las capacidades de servicio - incluyendo trabajos sobre codecs, seguridad, calidad de servicio - y por lo tanto proporciona las especificaciones del sistema completo. Las especificaciones también ofrecen ganchos para el acceso sin radio a la red principal, y para la interoperabilidad con redes Wi-Fi*[4]*.*

El 3GPP se organiza en grupos de trabajo llamados Grupo de Especificaciones Técnicas (GTE o TSG – Technical Specification Groups), los grupos se reúnen con cierta periodicidad donde exponen, valoran y aprueban información en torno a diferentes áreas entre las cuales se destacan las siguientes:

- Redes de Acceso Radio (RAN).
- Servicios & Sistemas Aspectos (SA).
- Red Central y Terminales (TC).
- EDGE Radio Access Networks GSM (GERAN).

Al finalizar el proceso de estandarización se documenta publicaciones “Releases” (Rel), donde se encuentran las especificaciones del trabajo realizado.

4.2. Generación de los sistemas celulares

En la 2da generación se incorpora el uso de señales digitales, esto aumentó la capacidad e introduce el uso de servicios de datos como navegación WAP, SMS y MMS, dentro de esta generación se destaca la tecnología GSM y EDGE.

[4] 3GPP, About 3GPP [en línea].< http://www.3gpp.org/about-3gpp > [Citado en noviembre de 2015]

El estándar “Global System for mobile communications” (GSM), aparece como resultado del trabajo de un grupo cuyo nombre se denomina por las mismas siglas “Groupe Spécial Mobile” (GSM), el cual se originó a partir de la necesidad de contar con un estándar global de telecomunicaciones móviles.

GSM fue diseñado principalmente para la telefonía de voz, pero se definió una serie de servicios portadores (un subconjunto de las disponibles para línea fija redes digitales de servicios integrados, RDSI), lo que permite conexiones de datos con conmutación de circuitos a velocidades de hasta 9600 bits / s. En el momento del diseño original del sistema, este ritmo se compara favorablemente con los disponibles a través de conexiones fijas. Sin embargo, con el paso del tiempo, las velocidades de datos de conexión fijos aumentaron dramáticamente. La estructura de canal y modulación técnica GSM no permitió velocidades más rápidas, y por lo tanto el servicio de conmutación de circuitos de alta velocidad de datos (HSCSD) se introdujo en la Fase 2+ GSM.[5]

Aunque GSM solucionó varias de las limitaciones de los sistemas analógicos, no estaba orientada a la transmisión de datos, por lo cual se manejaba velocidades bajas impactando la experiencia del usuario en el uso de servicios de Internet, entonces surge “General Packet Radio Service (GPRS)” como una opción para la transmisión de datos a través de la conmutación de paquetes, incorporando a la arquitectura de GMS elementos como el “Nodo de Soporte de Servicio GPRS”(SGSN) y “Nodo de soporte GPRS pasarela”(GGSN) para la gestión de datos; si bien GPRS fue un importante avance en su momento, provocaba un uso ineficiente de la red ya que los recursos permanecen ocupados en tanto se realiza la transferencia de datos.

A pesar de las mejoras que se tuvo con GPRS, la velocidad no era suficiente para permitir el acceso de manera satisfactoria para los servicios emergentes y como producto de la búsqueda de nuevas tecnologías, aparece “Enhanced Data rate for Global Evolution (EDGE), con mejoras en la capa física proporcionando mayor velocidad de transmisión de datos respecto a la tecnología GSM.
Estos cambios pueden ser encontrados a nivel de literatura, bajo el nombre de GERAN, que es el nombre dado a los sistemas de segunda generación como una combinación de GSM, EDGE y “Radio Access Network” (GERAN) de 3GPP.

La siguiente generación desarrollada por 3GPP, fue conocida como “Universal Mobile Telecommunications System” (UMTS) y se basa en la división de código de banda ancha de acceso múltiple (W-CDMA) y ofrece una mayor eficiencia espectral y mayor ancho de banda que GSM. Esta tecnología de radio utilizada entre los

[5] ETSI, Mobile technologies GSM [en línea].< http://www.etsi.org/technologies-usters/technologies/mobile/gsm> [Citado en noviembre de 2015]

terminales móviles y las estaciones base de los sistemas, se conoce genéricamente como “Terrestre Universal de Acceso de Radio” (UTRA) y la red de acceso como “Radio Terrestre Red de Acceso Universa” (UTRAN).

Esta generación, es conocida también como el sistema 3G y 3.5G, el cual aporto significativas mejoras en términos de calidad y servicios multimedia. En esta generación nos detendremos para detallar los sistemas que la componen, describiendo los elementos más relevantes de la arquitectura.

Sin bien posterior surgió la generación Long Term Evolution (LTE) también conocidas como 4G, que con la incorporación de “Orthogonal Frequency Division Multiple Access” (OFDMA), *LTE se centró en mejorar el acceso radio terrestre de UMTS (UTRA) y la optimización de la arquitectura 3GPP de acceso radio. En el enlace descendente se obtendrían velocidades de datos de usuario de 100 Mbit/s (de tres a cuatro veces superior a lo proporcionado HSDPA en la Rel-6) y de 50 Mbit/s en el ascendente (de dos a tres veces las prestaciones de HSUPA).*[6]

En LTE la red de acceso está formada por un único nodo llamado eNB y accede a la red de core a través del Serving Gateway (SGW), lo que en la red UMTS se realizaba a través del SGSN y las funciones originales del GGSN son implementadas por el PDN Gateway (PGW). Por lo cual las aplicaciones presentadas en este trabajo, es viable implementarse sobre una red LTE, verificando además de acuerdo con la información de CISCO el protocolo GRE es soportado por el GGSN y PGW.[7]

4.3. Arquitectura de la red celular

Los sistemas de comunicaciones digitales celulares contemplan una arquitectura que va desde los equipos de acceso, administración y registro de abonados, hasta interfaces con otro tipo de redes.

La red de comunicaciones celulares ofrece enlaces de comunicación entre usuarios del servicio de comunicaciones móviles de su misma red e incluso si se encuentran en células distintas o en el dominio de diferentes operadores, así como conexiones

[6] HUIDOBRO, José Manuel. Funcionamiento de GPRS En: Comunicaciones Móviles Sistemas GSM, UMTS y LTE. 1ed. Mexico: Editorial Alfaomega Grupo Editor S.A, 2012.p. 261.

[7] CISCO, P-GW Administration Guide, StarOS Release 21.1[en línea]. <https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-1/PGW/21-1-PGW-Admin/21-PGW-Admin_chapter_01010.html> [Citado en abril de 2021]

entre usuarios del servicio de comunicaciones móviles y usuarios de las redes fijas (red telefónica conmutada, RDSI, red pública de conmutación de paquetes, etc.).

En cuanto a la cobertura, puede ser de metros hasta kilómetros dependiendo del diseño, este y otros aspectos son determinados por la torre de radio con que cuenta cada celda. La torre de radio es responsable de establecer los canales de comunicación con los teléfonos móviles a través de una interfaz de radio. La capacidad de la torre de radio se mide en términos de los canales simultáneos que puede soportar al igual que con el número simultáneo de usuarios móviles que se espera que esté activo dentro de la región atendida por la torre de radio.

El rango de frecuencia asignado en el espectro para el operador de la red celular, es descompuesto en sub-bandas que son asignadas una a cada celda, con el fin de evitar interferencias, utilizando así FDMA para evitar la interferencia entre celdas y TDMA para que los usuarios dentro de la misma celda accedan a los servicios a través de la misma sub-banda de frecuencia; con el fin de optimizar el uso de las frecuencias asignadas, entre celdas vecinas no se utiliza la misma sub-banda de frecuencia, generando así el reúso de frecuencias, siendo esta una de las características importantes entre las redes móviles.

El reusó de frecuencias es una de las funcionalidades de la red celular que hace posible la movilidad del usuario a través de la red. Como respuesta al constante movimiento del usuario es necesario conocer en todo momento la ubicación del móvil utilizando protocolos de señalización. Es importante tener en cuenta que el uso de esto protocolos incorporan a la red una carga de señalización importante, incrementándose cuando se trata de celdas pequeñas ya que la cantidad de traspasos aumentan. Para disminuir el efecto causado por la carga de señalización es impórtate dentro del diseño de la red de celdas se estudie el radio de cobertura vs las estadísticas de tráfico para determinar la mejor ubicación de las torres de radio.

En las siguientes secciones se analizará los principales componentes de la red celular, que se integran para dar paso a las funcionalidades descritas arriba a través de los diferentes servicios.

4.3.1. Mobile Station

Dentro de la arquitectura GSM, los terminales móviles se conocen como “Mobile Station” (MS), que son los elementos usados para acceder a la red móvil. Estos pueden ser desde teléfonos simples hasta Smartphone, PC y tablets conectados con un modem USB a la red móvil, o terminales para comunicaciones M2M. Su

comunicación con la red tiene lugar vía la interfaz de radio “Um”, conocida también como “interfaz área”.

De acuerdo con TS 142.017, la estación móvil, se divide en dos partes, “Mobile Equipment (ME)” y “Subscriber Identity Module (SIM)”[8]

La SIM es una tarjeta inteligente, que contiene la lógica necesaria para establecer la comunicación con la red móvil del proveedor al que este asociado el usuario, es decir los códigos de identificación en el móvil. La SIM es un módulo removible, que contiene el International “Mobile Subscriber Identity” (IMSI) que identifica inequívocamente un abonado.

Sin un IMSI, el servicio GSM no es accesible, el cual de acuerdo con el 3GPP TS 23.003 tiene la estructura de la Ilustración 4 Estructura de IMSI.

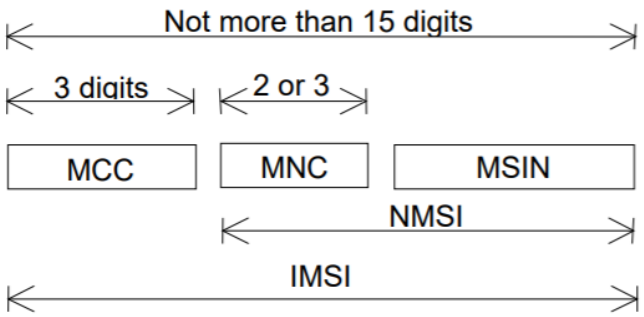

Ilustración 4 Estructura de IMSI[9]

MCC: Mobile Country Code. Identifica el país al que pertenece en la red móvil terrestre pública (PLMN)
MNC: Mobile Network Code. Identifica una PLMN particular dentro de un país
MSIN: Mobile Subscriber Identification Number, identifica el abonado dentro de la PLMN

El proveedor de servicios del abonado móvil proporciona el acceso dependiendo de la información de verificación contenida en la SIM.

[8] ETSI, TS 142 017 [en línea].< http://www.etsi.org/deliver/etsi_ts/142000_142099/142017/04.00.00_60/ts_142017v040000p.pdf > [Citado en noviembre de 2015]
[9] ETSI, TS 123 003 [en línea].<https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/10.05.00_60/ts_123003v100500p.pdf > [Citado en marzo de 2021]

Todos estos datos se utilizan para permitir el acceso y la movilidad del abonado a través de la red, sin embargo, como se mencionó anteriormente existe una carga de señalización asociada a estos accesos; con el fin de disminuir la carga de señalización en la red, asociada a la actualización de ubicación de la MS, se decidió agrupar una o más celdas bajo el concepto de “Location Area” (LA). Para esto se modifica el procedimiento de actualización de ubicación, enviando la actualización de ubicación solo si la MS cambia de LA; a través del procedimiento de paginación se identifica la celda exacta del ME en el LA, es decir en la que se cree esta la MS, por su parte la MS responde el mensaje de búsqueda de tal manera que se pueda conocer la celda exacta donde existe dicha MS.

Luego en GPRS, se introdujo la agrupación de nuevas secciones bajo el nombre de “Routing Area” (RA) como un concepto análogo a LA, las RA son un subconjunto de LA y como su nombre lo sugiere es el área de cobertura para el encaminamiento de paquetes o se puede entender como el área de cobertura de un SGSN. De manera similar con la aparición de UMTS apareció las áreas de cobertura “UTRAN”, se conoce como URA (Utran Registration Areas), todas estas sectorizaciones forman las áreas de servicio que conviven dentro de la red como se observa en la Ilustración 5 Áreas de Servicio en una red celular.

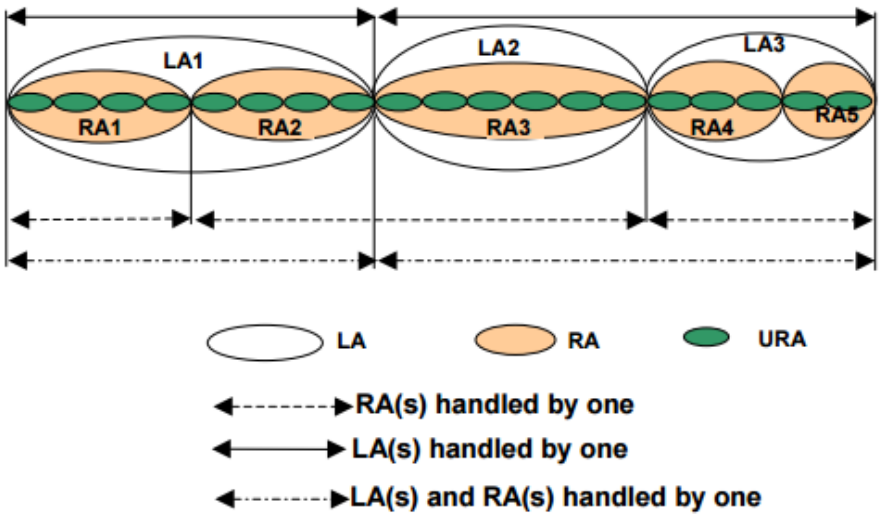

Ilustración 5 Áreas de Servicio en una red celular.[10]

[10] ETSI, TS 123 221 [en línea].< https://www.etsi.org/deliver/etsi_ts/123200_123299/123221/04.01.00_60/ts_123221v040100p.pdf> [Citado en marzo de 2021]

Por su lado el ME, está compuesto del “Terminal equipament” (TE) y el “Mobile termination” (MT) que hace parte del TE, pero se encarga específicamente de terminar la transmisión de radio y la administración de la movilidad.

4.3.2. Public Land Mobile Network (PLMN)

Introduciendo los componentes de la arquitectura de red, se encuentra el más alto nivel de la jerarquía en GSM hasta UMTS llamado PLMN, cuyo propósito específico es el suministro de servicios integrados con características similares a los de una red fija incluyendo además funciones de movilidad. Una PLMN se interconecta con otras PLMN y con la PSTN para proveer los servicios de voz y datos.

La PLMN es lo primero que se encuentra el móvil al acceder a través de la interfaz de radio utilizando las BTS, ya dentro de la PLMN el transporte de paquetes utiliza un identificador que contiene el código móvil del país (MCC) y el código de red móvil (MNC).

4.3.3. Access Network (AN)

La Red de Acceso se encarga de todas las funciones de acceso, está compuesta por el BTS (Base Transceiver Station) y BSC (Base Station Controller).

Dadas las similitudes entre la arquitectura de GSM y UMTS, el acceso a redes se puede realizar desde dos entidades, el BSS (Base Station Subsystem) y el RNS (Radio Network Sub-system), siendo el BSS una entidad proveniente de GSM y RNS la entidad adicional para la tecnología de UTRAN, como se muestra en la Ilustración 6 BSS y RNS. En el caso del RNS, la BTS es sustituida por el Nodo B y el BSC es sustituido por el RNC (Radio Network Controller).

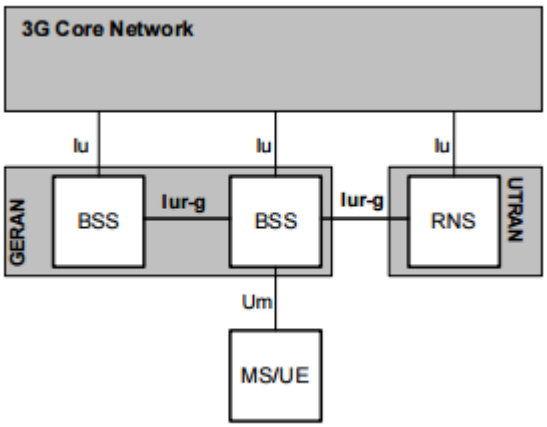

Ilustración 6 BSS y RNS[11]

Es importante tener en cuenta que los protocolos de comunicaciones entre las entidades de GSM/GPRS son diferentes a los de UMTS, esto debido a la introducción de una interfaz de aire basado en WCDMA en la Red de Acceso de UMTS, esto implica que para que un móvil pueda acceder a UMTS debe ser compatible, sin embargo, no ocurre lo mismo si un móvil quiere acceder de UMTS a GSM/GPRS, ya que lo puede hacer sin problemas.

4.3.3.1. Base Station Subsystem (BSS)

En GSM, el subsistema de estación base, contiene a “Base Station Controller” y una o más “Base Terminal Station”, estos elementos desarrollan principalmente todas las funciones para la administración de los recursos para la transmisión vía radio, recibe el acceso de radio provenientes de las MS que se encuentran en su área de cobertura y lo transmiten al Core Network (CN).

La interfaz de conexión entre una BTS y su correspondiente BSC se denominada interfaz Abis.

[11] ETSI, TS 143.130 [en línea]: https://www.etsi.org/deliver/etsi_ts/143100_143199/143130/16.00.00_60/ts_143130v160000p.pdf > [Citado en enero de 2016]

4.3.3.2. Base Terminal Station" (BTS)

Las BTS son las encargadas de establecer y mantener el enlace entre la MS y la BSC, realizan funciones de codificación de canal y cifrado/descifrado en la interfaz de radio. Las BTS reciben instrucciones de las BCS y a su vez entregan información a las BSC para controlar el acceso a los recursos de la red cumpliendo funciones de traspaso entre celdas y control de potencia.

4.3.3.3. Base Station Controller (BSC)

El BSC es el encargado de la gestión y mantenimiento del servicio. Una tarea específica es la asignación de estaciones dentro de un área de cobertura, los BSC también son los encargados de ejecutar las funciones de traspaso entre las estaciones base de su área, cada estación base debe conocer las estaciones móviles residentes y las visitantes para que las estaciones de control puedan determinar su posición en cualquier momento.

4.3.3.4. Radio Network Subsystem (RNS)

El RNS, también conocido como Red de Acceso por Radio Terrestre Universal (UTRAN), consta de un Controlador de Red de Radio (RNC) y uno o más Nodos B. El RNC es el análogo del BSC, mientras que el Nodo B es similar a la BTS. Las interfaces abiertas de RNS permiten que RNS y el Nodo B de diferentes proveedores operen entre sí.

4.3.4. Nodo B

Los Nodo B de manera análoga a las BTS es el responsable de la transmisión/recepción en una o más células a y desde la un UE compatible.

4.3.5. Radio Network Controller (RNC)

El Controlador de Red de Radio es el equipo en el RNS encargado de controlar el uso y la integridad de los recursos, tiene el control general de los recursos lógicos

de su nodo B, ofreciendo la asignación y la liberación de recursos de radio específicos para establecer medios de conexión entre un UE y la UTRAN.[12]

4.3.6. Core Network (CN)

En UMTS, la red principal consiste en las entidades que prestan apoyo a las diferentes funciones y servicios de red, como, movilidad, gestión, control de llamadas, conmutación, gestión de sesiones, enrutamiento, autenticación y la identificación del equipo.

Basado en el hecho de que la Red Central UMTS es una red núcleo GSM / GPRS evolucionado, se divide en dos dominios: el circuito conmutado (CS, Circuit Switched) y el dominio de conmutación de paquetes (PS, Packet Switched). El dominio CS presta servicios relacionados con la transferencia de voz, el dominio PS se relaciona con la transferencia de datos.

En la red se maneja dos clases de tráfico que son manejadas por la red principal, voz y datos. Las "redes móviles 2G, al igual que las redes GSM, fueron diseñados principalmente para la voz, en cambio las redes GPRS proporcionan capacidad para la transferencia de datos, por lo cual se segmentaron los dominios por tipo de servicio, es decir voz y datos.

4.3.7. Dominio CS

El dominio CS se refiere al conjunto de todas las entidades que realizan funciones importantes para la gestión de la movilidad. Estas entidades establecen conexiones llamadas "conexión CS" en las cuales se utilizan recursos para establecer una conexión y liberar los recursos cuando la conexión termina. El dominio CS está compuesto por el MSC, GMSC, VLR.

12 ETSI, TS 25.401 [en línea] :http://www.etsi.org/deliver/etsi_ts/125400_125499/125401/03.01.00_60/ts_125401v030100p.pdf > [Citado en enero de 2016]

4.3.7.1. Centros de conmutación (MSC)

Con el fin de establecer una “conexión CS”, liberar recursos y conmutar flujos de voz, se requiere una entidad de conmutación. El MSC (Mobile Switching Centres, o Centros de Conmutación de Servicio Móviles) es el encargado de manejar el circuito de servicios conmutados hacia y desde las estaciones móviles. Además, constituye la interfaz entre el sistema de radio y las redes fijas. El centro de conmutación realiza todas las funciones de conmutación y señalización teniendo en cuenta, el impacto de la asignación de recursos de radio y la procedencia del móvil a través de procedimientos para el registro de localización y traspaso.

4.3.7.2. The Gateway MSC (GMSC)

Como parte del CS y como puerta de enlace está el centro de conmutación móvil (GMSC), que proporciona conectividad a las redes externas del CS, incluyendo el dominio CS de otras redes UMTS y las redes PSTN.

Si una red entrega una llamada a la PLMN no puede interrogar al HLR, la llamada se encamina a un MSC. Este MSC interroga al HLR correspondiente y luego encamina la llamada al MSC donde se encuentra la estación móvil. El MSC que realiza la función de enrutamiento para la ubicación real de la MS se llama el MSC de pasarela (GMSC).[13]

4.3.7.3. Visitor Location Register (VLR).

Junto con el MSC, hay otra entidad en el dominio CS, llamado el Registro de posición de visitantes (VLR). El VLR contiene el perfil de abonado obtenido del Home Location Register (HLR). MSC consulta el VLR para obtener información de abonado y proporciona servicios al abonado sobre la base de la información consultada.

[13] ETSI, TS 123.002 [en línea] : < http://www.etsi.org/deliver/etsi_ts/123000_123099/123002/13.05.00_60/ts_123002v130500p.pdf

Un VLR puede estar a cargo de una o varias áreas de MSC, el VLR contiene también la información necesaria para manejar las llamadas de la configuración recibida por la MS registrada en su base de datos, contiene además parámetros de servicios suplementarios conectados al abonado móvil y recibido desde el HLR.

Cuando una estación móvil (MS) entra en una nueva área de servicio, se inicia un procedimiento de registro, el MSC a cargo identifica el área de servicio e inicia la transferencia al VLR el MS se encuentra.

4.3.8. Dominio PS

El dominio PS está compuesto por diversas interfaces de redes del tipo “conexión PS”, encargados de proporcionar los elementos necesarios para el tráfico de datos y apoyar la señalización del tráfico de usuarios. Los componentes básicos del dominio de PS son los nodos de soporte GPRS (GSN), el Soporte de Servicio GPRS nodos (SGSN) y los nodos de soporte de pasarela GPRS (GGSN), estos últimos elementos se conectan entre sí utilizando una IP-backbone donde los paquetes son transportados a través de una conexión tipo túnel utilizando el GSN. El SGSN y el GGSN se apoyan en el HLR para obtener información de los abonados que intentan registrarse en la red, cada uno obtiene información independiente entre sí.

El dominio PS utiliza conexiones de conmutación de paquetes (PS) para la comunicación entre el UE y el destino. Un aspecto importante de conexión PS es que los recursos no están reservados para una conexión; más bien, son una mejor utilización de los recursos. Un ejemplo de conexión PS es la transferencia sin conexión de datagramas IP en Internet.

4.3.8.1. Nodo de Soporte de Servicio GPRS (SGSN).

Con el fin de encaminar los paquetes en el dominio PS, se hizo necesario de una entidad para el enrutamiento, el nodo de soporte GPRS de servicio (SGSN) hace las veces VLR/MSC del dominio CS, realizando tanto las funciones de encaminamiento como de almacenamiento. El nodo SGSN es la entidad de control principal en la red central, cuando un UE se enciende y se conecta a la red se le registra en un SGSN específico dependiendo de su ubicación.

El tráfico del usuario se transporta a través de la SGSN, el cual se encarga de autenticar y autorizar los UE de acuerdo con la información de suscripción obtenida a través de la interface Gr desde el HLR, después de aprobada la autenticación también determina la ruta que debe tomar el tráfico con base en la ubicación física de la UE y el GGSN adecuado para el tipo de servicio que se esté solicitando.

Cuando un UE solicita una sesión, el SGSN establece un túnel, llamado "**PDP Context**", los datos y el control del tráfico de la UE a encaminar, durante la sesión, el SGSN almacena la información del tráfico del usuario y el perfil de acuerdo con el plan asignado, en caso de exceder los fondos, el SGSN termina la sesión.

El SGSN a su vez apoya el proceso de paginación, cuando se requiere establecer una sesión hacia un UE desde una red externa. De igual manera para que un MS pueda comunicarse con entidades de redes externas de datos, que debe tener una dirección que pueda ser comprendida, las conexiones más comunes son las basadas en el protocolo de Internet (IP); un MS debe tener una dirección IP para la comunicación con otras entidades en una red externa de datos.

Una dirección IP es asignada de forma estática o dinámicamente por el GGSN. En el caso de las direcciones estáticas, estas son asignadas por el operador de red de la PLMN es decir con carácter permanente. Sin embargo, dado que las direcciones de red son un recurso limitado, las direcciones se asignan generalmente de forma dinámica a menos de que sea estrictamente necesario.

Las direcciones IP dinámicas se asignan durante la activación del contexto PDP, establecido entre el UE, SGSN y GGSN. La activación de un contexto PDP se refiere a la creación del contexto PDP al UE, al SGSN y al GGSN, después de que la comunicación termina el contexto PDP se desactiva. El SGSN también es responsable de las funciones relacionadas con la gestión de movilidad.

4.3.8.2. Nodo de soporte GPRS pasarela (GGSN).

El dominio PS, tiene la puerta de enlace (Gateway) GPRS nodo de Soporte (GGSN), que se encarga de funciones similares a las de GMSC, proporciona conectividad a las redes PS externas, como Internet o el IMS. La elección del GGSN que debe

atender la solicitud de un UE, depende del servicio que el usuario tiene la intención de utilizar. Cuando un UE no tiene una sesión activa no hay ningún GGSN asociado con este UE.

El GGSN almacena información sobre los abonados y la información de enrutamiento necesaria para establecer un túnel para el tráfico de paquetes de datos, generando los contextos PDP y estableciendo el túnel de GTP. Una vez hecho esto, todo lo que tiene que hacer el GGSN es mantenerlas.

4.3.9. The Home Location Register (HLR).

El Home Location Register (HLR) es la base de datos maestra de un abonado. El HLR mantiene y proporciona los datos de abonado a otras entidades de red de datos, por ejemplo, cuando un dato es modificado por el operador, el HLR envía el dato a las entidades de red, siendo una entidad común tanto en el dominio CS, como en el dominio PS.

El tipo de datos almacenados puede ser permanente o dinámico. Los datos permanentes son los proporcionados por el operador de la red y los datos temporales son los obtenidos a través de otras entidades de la red. Los datos temporales se utilizan para los procedimientos dinámicos, por ejemplo, la dirección VLR es un dato dinámico que almacena el HLR y se utiliza para el enrutamiento de una sesión.

4.3.10. The Equipment Identity Register (EIR)

El “Registro de Identidad de Equipo” (EIR), es el encargado en la red de validar la identidad de un UE a través de consulta en el registro de IMEI en los sistemas. Los IMEI son clasificados en bases de datos dependiendo del tipo de registro, es decir, "lista blanca"(son los IMEI que tienen permiso de uso), "lista gris"(IMEI que está restringido en la red por alguna razón), "lista negra"(IMEI que tienen prohibido su uso). [14]

[14] 3GPP, TS 22.016 Release 13 [en línea]: < http://www.3gpp.org/DynaReport/22016.htm> [Citado en enero de 2016]

4.3.11. The Authentication Center (AuC)

El Centro de autenticación (AuC) es una entidad que almacena datos de cada abonado móvil, para permitir que el IMSI pueda ser autenticado. El AuC contiene la clave secreta que se comparte entre el AuC y la SIM de la UE. Esta clave asociada con un IMSI es utilizada para la autenticación y se comparte entre la tarjeta SIM y la AUC.

Las AuC, no participan en la autentificación, esa función es realizada por el VLR para CS dominio y SGSN para el dominio PS. El papel de las AuC es proporcionar VLR y al SGSN la información necesaria que puede ser utilizada por este último para la autenticación

4.3.12. Diagrama base de la arquitectura celular

Luego de repasar los elementos relevantes de la arquitectura celular, se presenta en la Ilustración 7 un diagrama general, el cual puede variar según el diseño de cada CSP, pero seguramente mantendrá los elementos básicos presentados.

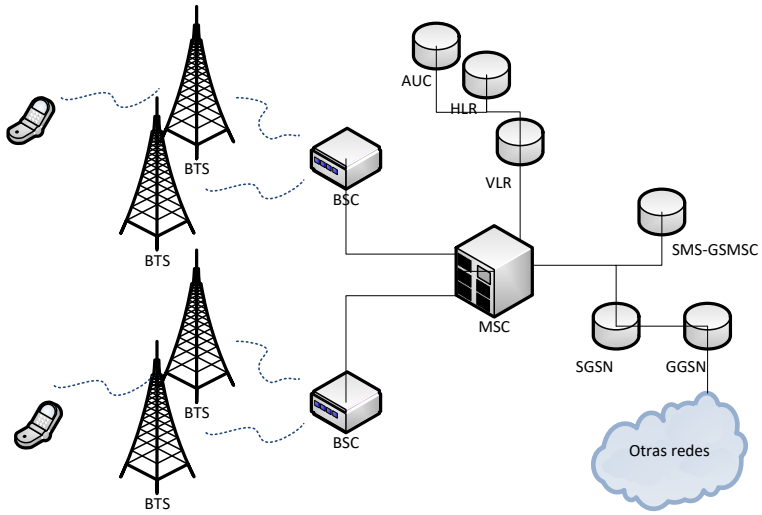

Ilustración 7 Diagrama general sobre los componentes de una red celular. Fuente propia

Comprender este diagrama facilitara la compresión de los procesos que se verán a continuación, donde profundizaremos en el flujo de comunicación dentro de la red celular, para luego explorar las alternativas de conexión hacia redes externas.

5. ASPECTOS ESPECIFICOS DE REDES CELULARES PARA SOLUCIONES M2M E IoT

La red celular, había sido tradicionalmente usada para servicios masivos de usuarios residenciales; sin embargo, existen factores diferenciales que se pueden ajustar y que aportan a una solución M2M e IoT con el fin de gestionar el transporte de información y que se pueden aprovechar en la planificación de los requerimientos de red orientados a obtener un mejor desempeño del servicio, crecimiento y despliegue.

Después de la introducción realizada en los capítulos anteriores sobre conceptos relevantes de las redes celulares, a continuación, se profundizará en los factores seleccionados por su aporte a las soluciones M2M e IoT, específicamente el encaminamiento del tráfico, protocolos que facilitan la comunicación con redes externas y algunos aspectos para tener en cuenta en el momento de escoger la SIM card a utilizar.

Para detallar como se puede lograr lo anterior, a continuación, se iniciará explicando el proceso para establecer un contexto PDP con el que inicia la transferencia de datos.

5.1. Proceso para establecer un contexto PDP

Un contexto PDP es un proceso de activación de la sesión de datos, que se lleva a cabo para autorizar a un “User Equipment” (UE) dentro de la red y que este puede hacer uso de esta, bajo ciertos parámetros definidos. Este proceso sucede antes de que el APN se establezca entre el SGSN y el GGSN.

A continuación, se esquematiza a partir de la arquitectura de la Ilustración 8, el paso a paso para establecer un contexto PDP que, en otras palabras, se puede entender como una sesión de datos que se establece dentro de la red celular.

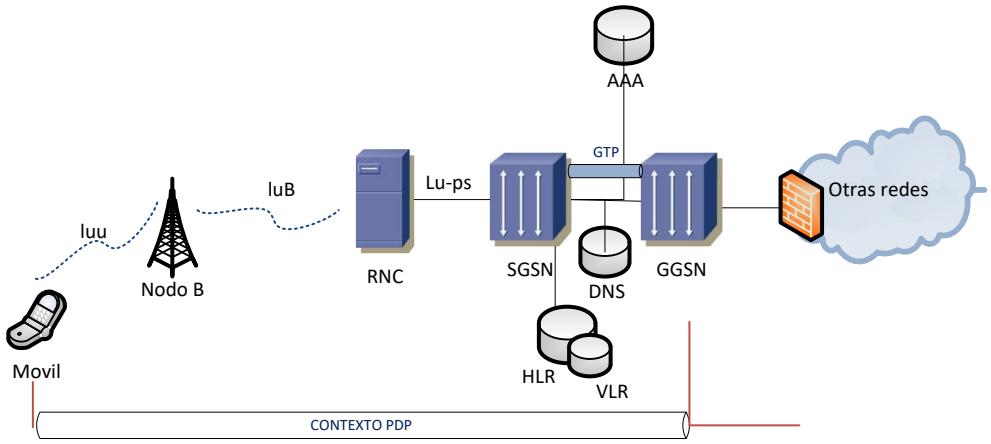

Ilustración 8 Establecimiento contexto PDP. Fuente propia

Paso 0: Cuando un UE que se encuentra en una zona de cobertura requiere establecer una sesión de datos, envía una solicitud al nodo B, que se encuentra dentro de su zona, a través de la interfaz de aire. En ese momento, se inicia la negociación con las diferentes entidades del core de la red, para determinar las características de la sesión de datos a establecer, de acuerdo con el siguiente proceso de validaciones. Como se muestra en la Ilustración 9.

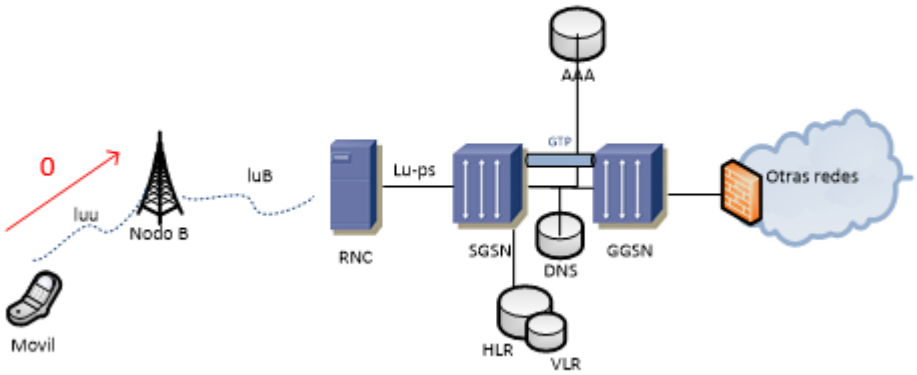

Ilustración 9 Establecimiento contexto PDP petición inicial. Fuente propia

Paso 1: El nodo B, el nodo de cobertura de la celda, donde está registrado el usuario, envía la solicitud del usuario móvil a la RNC, a la que pertenece. La comunicación entre el nodo B y la RNC se puede realizar a través de aire, vía microondas o por fibra a través de las tecnologías PDH, SDH, MPLS. Estos son parámetros de Core que define y varían según las definiciones de cada CSP.

En este punto se establecen canales de control entre el UE, el nodo B y la RNC. Todo esto con el fin de asignar un RAB (Radio Access Bearer) y poder establecer el contexto PDP. Si el RAB no se ha establecido no se puede establecer contexto PDP. Como se muestra en la Ilustración 10.

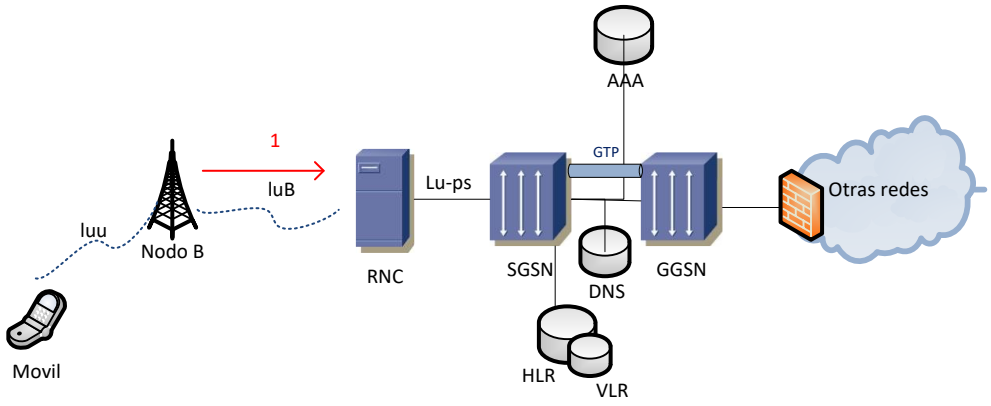

Ilustración 10 Establecimiento contexto PDP paso 1. Fuente propia

Paso 2: La RNC toma la solicitud del UE, y la envía al SGSN que ella tiene asignado, con el fin de intentar establecer la sesión de datos. El SGSN es el equipo del core que ayudará a establecer el contexto PDP, para que puedan fluir los datos del UE a través de la red móvil del operador. Como se muestra en la Ilustración 11.

El SGSN toma la solicitud y primero se comunica con el HLR, con el fin de revisar que servicios tiene aprovisionados la línea, revisar el QoS y si el usuario tiene saldo para poder establecer la sesión de datos.

En el HLR debe estar aprovisionado el APN (véase sección 5.3). Si no está aprovisionado el APN, el usuario nunca va a poder establecer una sesión de datos.

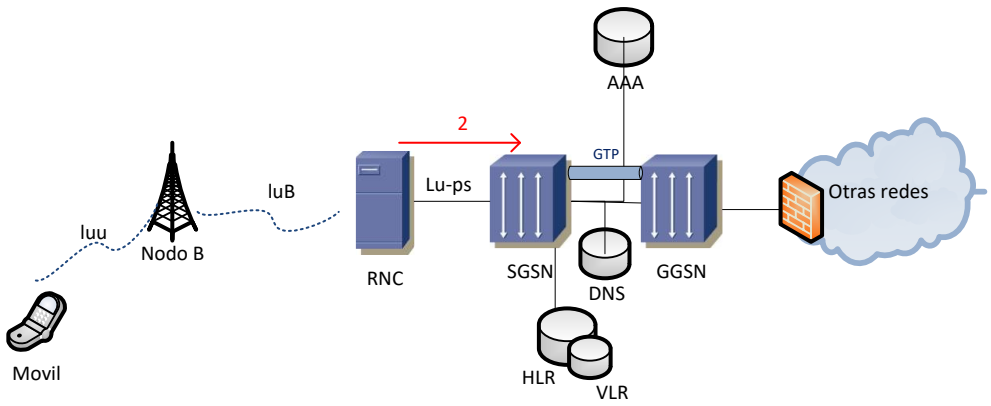

Ilustración 11 Establecimiento contexto PDP paso 2. Fuente propia

Paso 3: Una vez el SGSN valida el perfil del UE en el HLR, realiza una copia del VLR del HLR al VLR del SGSN.

Recordemos que el VLR es la base de datos donde se almacena la ubicación del UE, un UE no puede tener servicio si no tiene VLR, lo que pasaría si esto sucede es que no se encontraría al UE en la red. Como se muestra en la Ilustración 12.

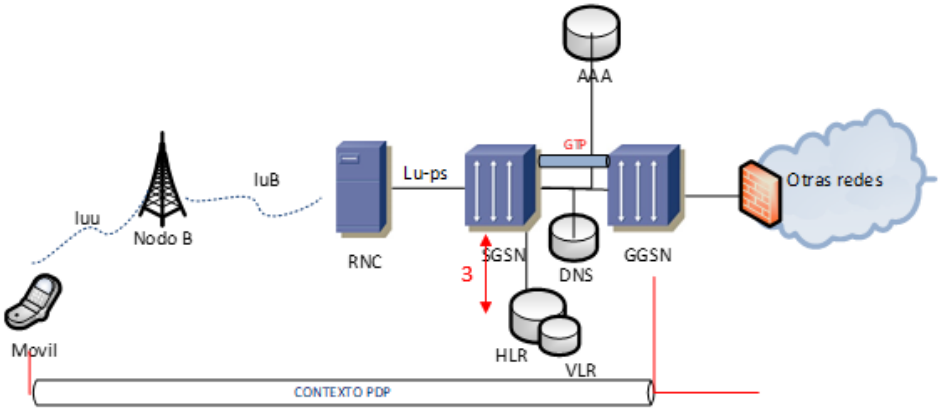

Ilustración 12 Establecimiento contexto PDP paso 3. Fuente propia

Paso 4: Con la información del perfil de la SIM, se debe autenticar el UE en la red. El SGSN envía una solicitud al AAA para que autentique la SIM en la red. Como se muestra en la Ilustración 13.

El AAA, autenticará la SIM revisando los pap user y pap password que tenga aprovisionados el terminal.

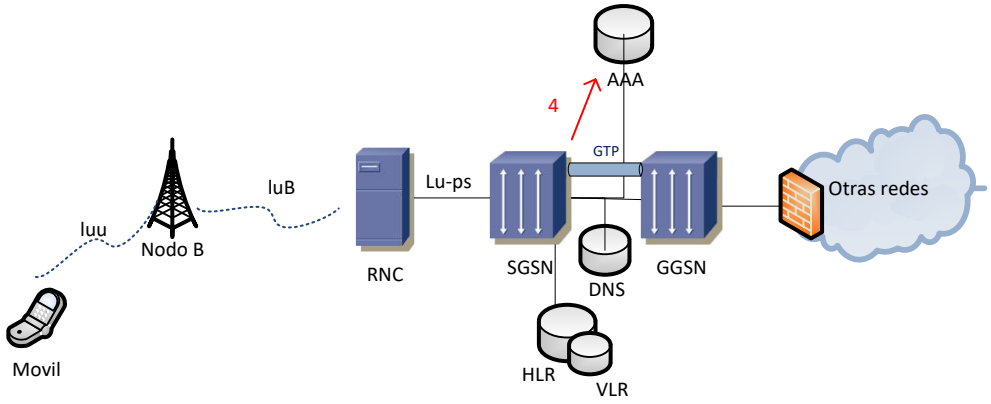

Ilustración 13Establecimiento contexto PDP paso 4. Fuente propia

Paso 5: Una vez se autentique la SIM, se le indica al SGSN que la SIM ha sido autenticada para que el SGSN proceda a conectar al UE. Como se muestra en la Ilustración 14.

La cantidad de conexiones exitosas con la red depende de si el UE fue autenticado en la red o si el SGSN tiene la capacidad para soportar más UE.

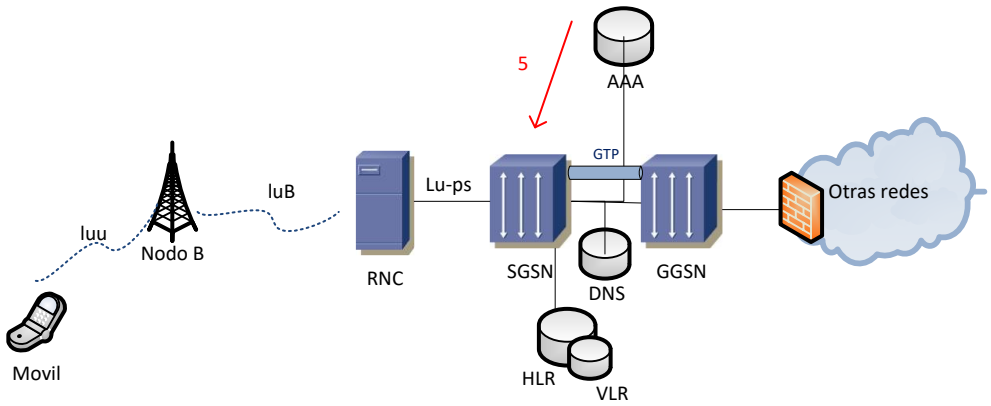

Ilustración 14 Establecimiento contexto PDP paso 5. Fuente propia

Paso 6: El SGSN consulta con el DNS para ver contra que GGSN levanta el contexto PDP. Como se muestra en la Ilustración 15. El DNS tiene creados los APN (véase sección 5.3). Así que cuando le llega la solicitud del SGSN preguntándole por un APN, el DNS resuelve ofreciendo la dirección IP del GGSN que tiene creado el APN.

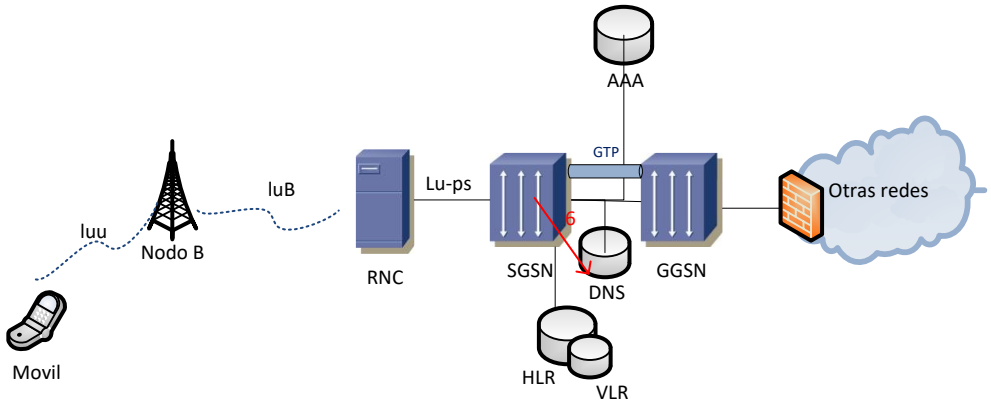

Ilustración 15 Establecimiento contexto PDP paso 6. Fuente propia

Paso 7: El SGSN a través del protocolo GTP (GPRS Tunnel Protocol), se comunica con el GGSN que tiene creado el APN, con su respectivo pool de direcciones IP, y se activa el contexto PDP. Como se muestra en la Ilustración 16.

Después de las validaciones realizadas y que el UE es autenticado en la red, se establece entre el SGSN y el GGSN el túnel GTP, el cual es empleado desde las redes GPRS para transportarla la señalización y datos.

Una vez establecido este contexto el usuario recibe una dirección IP, y puede enviar datos sobre la red del operador móvil. Para poder levantar el contexto PDP el APN del UE debe estar aprovisionado en el GGSN.

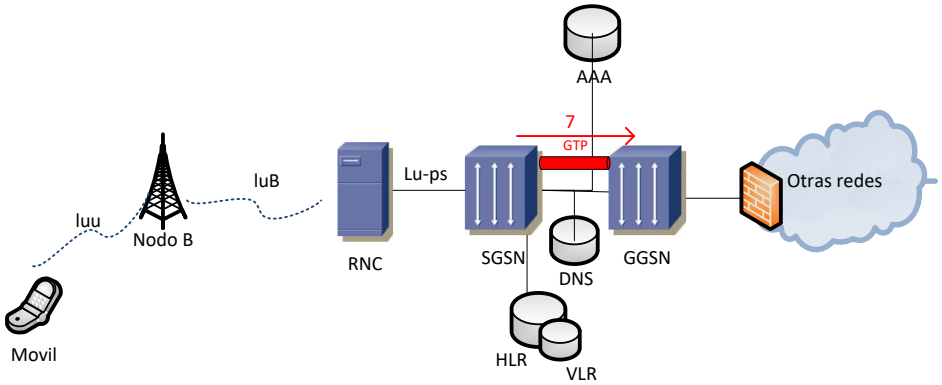

Ilustración 16 Establecimiento contexto PDP paso 7. Fuente propia

Paso 8: Finalmente los datos del UE van a fluir por el contexto PDP que se activó y llegarán al GGSN, que encaminará el tráfico de acuerdo con las redes destino.

Después de estos ocho pasos del proceso de activación del contexto PDP, el APN se establece entre el SGSN y el GGSN. Como se muestra en la Ilustración 17.

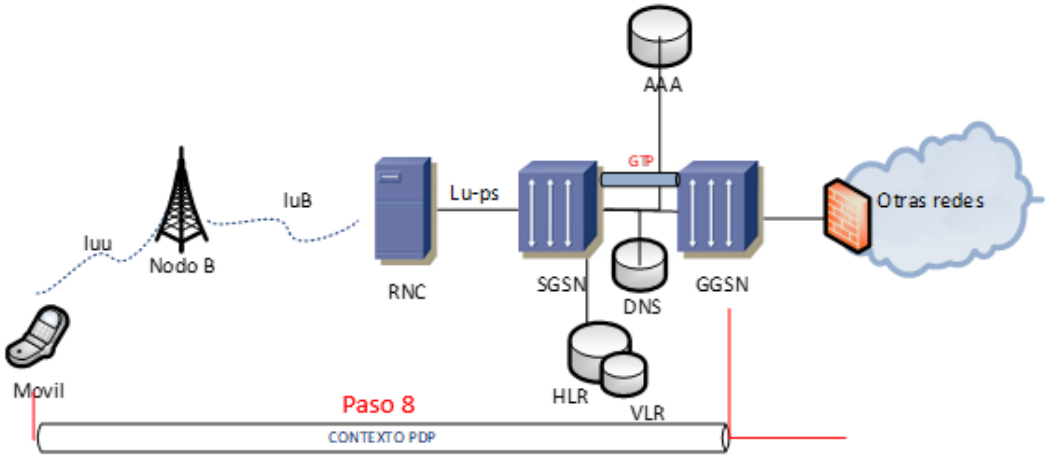

Ilustración 17 Establecimiento contexto PDP paso final. Fuente propia

En resumen, en el momento en que se establece un contexto PDP se generan todas las validaciones asociadas al tipo de sesión de datos a establecer. Dependiendo del tipo de sesión de datos requerida, es posible segmentar el tratamiento que se le da al tráfico dentro de la red celular para generar soluciones particulares, con nivel de seguridad particulares y la comunicación que permita la integración con redes externas.

Esto último es posible, principalmente, por la asignación de una dirección IP al UE una vez es establecido el contexto PDP. De esta manera es posible continuar con el enrutamiento del tráfico hacia otras redes o dominios desde los equipos de borde de la red celular. Esta última consideración, es planteada de manera similar en el TS 123 221 V12.0.0 (2014-10)[15]:

"Los dominios de direccionamiento IP pueden estar interconectados a varios puntos. En estos puntos las puertas de interconexión, Firewalls o NATs pueden estar

[15] ETSI, TS 23.221 versión 12.0.0 Release 12 [en línea]:<https://www.etsi.org/deliver/etsi_ts/123200_123299/123221/12.00.00_60/ts_123221v120000p.pdf> [Citado en marzo de 2021]

presentes. No es garantizado que los paquetes IP desde la dirección de dominio puedan ser directamente enrutados a algún Dominio IP interconectado. Más bien, el tráfico entre dominios puede ser manejado por Firewall o túneles."

5.2. Protocolo de encapsulamiento de las soluciones M2M e IoT en redes celulares

Dado que los UE cuentan con un direccionamiento IP, el siguiente paso que se plantea es detallar el funcionamiento los túneles dentro de la red celular, entiendo que a través de esto es posible generar conexiones hacia redes externas.

Como se puede ver en el ejercicio anterior, el tráfico dentro de la red celular pasa por varios equipos antes de llegar a su destino, la utilización de túneles es una técnica común para habilitar las redes locales multiprotocolo a través de un backbone, con el fin de conectar redes no contiguas y permitir redes privadas virtuales a través redes WAN. De allí que la utilización de túneles facilita la implementación de soluciones M2M e IoT permitiendo a través de una conexión privada, conocer las IPs de origen y destino a través de las cuales se generara las peticiones de la solución.

El objetivo de este capítulo es hacer una apropiación de los conceptos de túnel GRE y túnel GTP, detallar como aportan cada uno al tipo de conexión, para más adelante apoyarnos en una simulación básica en packet tracert y comprender el comportamiento del tráfico con la utilización de este tipo de configuraciones.

5.2.1. Túnel GTP

El protocolo de túnel "GPRS Tunneling" (GTP), es empleado para transportar los paquetes entre el SGSN y el GGSN, en redes GPRS y UMTS, permite trasportar señalización y datos dentro de la red celular[16].

Dado que el túnel GTP es empleado únicamente dentro de la red móvil, se limitan las conexiones con redes externas, es allí donde el protocolo de túnel GRE (Generic Routing Encapsulation), es soportado tanto por redes cableadas como inalámbricas

[16] HUIDOBRO, José Manuel. Funcionamiento de GPRS En: Comunicaciones Móviles Sistemas GSM, UMTS y LTE. 1ed. Mexico: Editorial Alfaomega Grupo Editor S.A, 2012.p. 163.

y permite realizar el encaminamiento de datos dentro de la red celular y llevar el tráfico hacia la interconexión con redes externas.

5.2.2. Túnel GRE

Este protocolo de túnel “Generic Routing Encapsulation” (GRE), se utiliza principalmente para redes privadas virtuales, con encapsulación basada en IP, el encabezado de túnel GRE, puede usarse para discriminar la identidad de la red origen de los paquetes, además, un encabezado GRE permite la identificación del tipo de protocolo que se transporta sobre el túnel, permitiendo así que las redes IP sirvan como un servicio portador sobre el que se puede definir e implementar una red virtual multiprotocolo.

Es de tener en cuenta que túnel GRE no proporciona seguridad y en caso de requerirlo sobre todo en el caso de la comunicación con redes externas, será necesario aplicar una capa de seguridad, por ejemplo, con el uso de configuración del tipo IPSEC, según aplique para los equipos involucrados dentro de la conexión.

A través de la utilización del protocolo GRE, permite identificar la IP origen desde la que se está realizando la solicitud, a pesar de que de entre el punto inicio y fin existan otros elementos de Core intermedios.

Después de introducir los conceptos de túneles GTP y GRE, se utiliza el software de simulación de redes Packet Tracer, para afianzar lo que ocurre con la utilización de ese tipo de protocolos para este caso particular GRE.

5.2.3. Simulación Túnel GRE

Como se mencionaba anteriormente, si bien no es factible simular el comportamiento completo de la red, el objetivo de la siguiente simulación es comprender el funcionamiento del protocolo GRE.

Recordemos que como se vio en el proceso para establecer un contexto PDP, existen diferentes entidades intermedias en la red, que si bien se involucran durante el proceso de acceso a la red en el momento de la transmisión de la información no

son requeridas. Es allí donde el protocolo GRE permite tener una visibilidad desde el dispositivo móvil hasta el equipo final, estableciendo una especie de túnel para la trasmisión de datos.

Para efectos de la simulación se emplea, switches y routers que hagan las veces de GGSN y SGSN, lo anterior basados que en la práctica estos elementos efectivamente hacen las veces de router y switche, obviamente en una escala más amplia para sus funcionalidades, como se muestra en la Ilustración 18 de Packet Tracer.

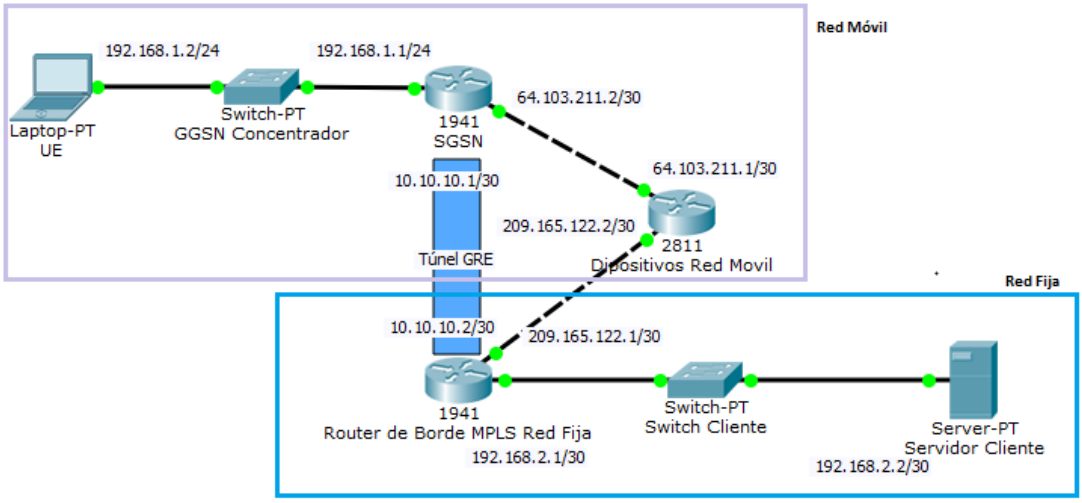

Ilustración 18 Esquema Simulación Túnel GRE. Imagen tomada de Packet Tracer

5.2.3.1. Partes de la simulación

El Laptop-PT UE, hace las veces de un dispositivo móvil inteligente. El medio de conexión de UE con el concentrador GGSN simula la frecuencia de operación de las redes móviles que se comunica con las BTSs, como se muestra en la Ilustración 19.

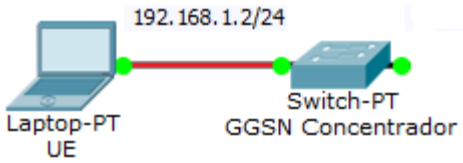

Ilustración 19 Dispositivo UE y Medio de comunicación. Imagen tomada de Packet Tracer

Adicionalmente los dispositivos mostrados a continuación suponen los diversos equipos de la red móvil que manejan a grandes rasgos la comunicación de la red. Al interior del SGSN, GGSN y el UE, se maneja IPs privadas. El SGSN es el dispositivo con el cual se configura el túnel GRE, como se muestra en la ilustración 20.

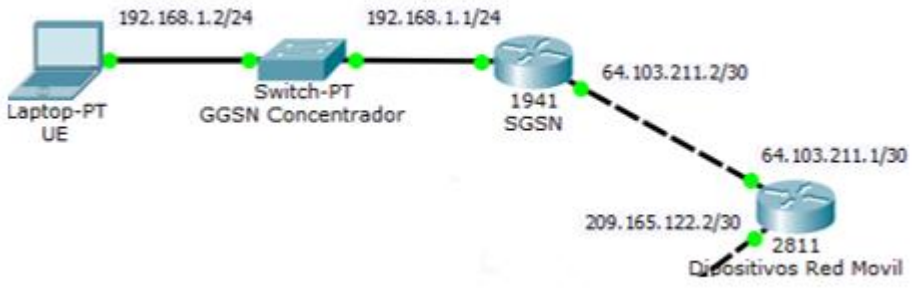

Ilustración 20 Red Móvil simulación. Imagen tomada de Packet Tracer

La red fija, simula la red MPLS de un operador móvil que presta este servicio y a su vez la conexión con el cliente final, sus aplicaciones y/o servidores, así como puede ser reemplazada por la red de Internet, como se muestra en la Ilustración 21.

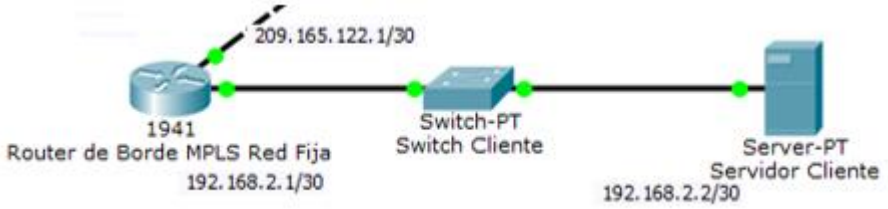

Ilustración 21 Red Fija simulación. Imagen tomada de Packet Tracer

La conexión GRE se crea a través de dos enrutadores que no tienen conexión directa, lo que permite su comunicación, como se muestra en la Ilustración 22.

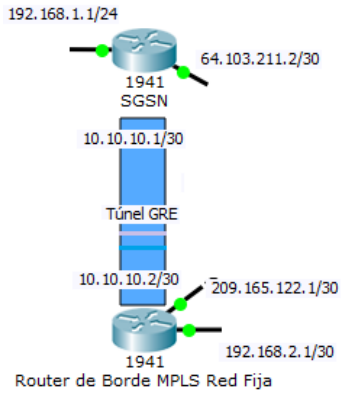

Ilustración 22 Conexión túnel GRE Simulación. Imagen tomada de Packet Tracer

a. Configuración dispositivos

b. UE

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:70FF:FE59:52A8
   IP Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.1.1
```

Ilustración 23 Configuración UE simulación. Imagen tomada de Packet Tracer

c. SGSN

```
!
interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/1
 tunnel destination 209.165.122.2
!
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 64.103.211.2 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 10.10.10.2
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
```

Ilustración 24 Configuración SGSN simulación. Imagen tomada de Packet Tracer

d. Equipo móvil que interconecta red móvil con red fija

```
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 64.103.211.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 209.165.122.1 255.255.255.252
 duplex auto
 speed auto
!
```

Ilustración 25 Configuración equipo de borde red móvil simulación. Imagen tomada de Packet Tracer

e. Equipo de borde red fija

```
!
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/1
 tunnel destination 64.103.211.2
!
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 209.165.122.2 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
ip flow-export version 9
```

Ilustración 26 Configuración equipo de borde red fija simulación. Imagen tomada de Packet Tracer

f. Servidor cliente

```
SERVER>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:47FF:FEA9:29BB
   IP Address.....: 192.168.2.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.1
```

```
!
!
!
!
!
interface FastEthernet0/0
 ip address 64.103.211.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 209.165.122.1 255.255.255.252
 duplex auto
 speed auto
!
```

Ilustración 27 Configuración servidor simulación. Imagen tomada de Packet Tracer

5.2.3.2. Simulación

a. Configuración sin túnel.

A continuación, se verá la configuración sin el túnel GRE habilitado, donde el dispositivo UE y el servidor no tienen conexión, como se muestra en la Ilustración 28.

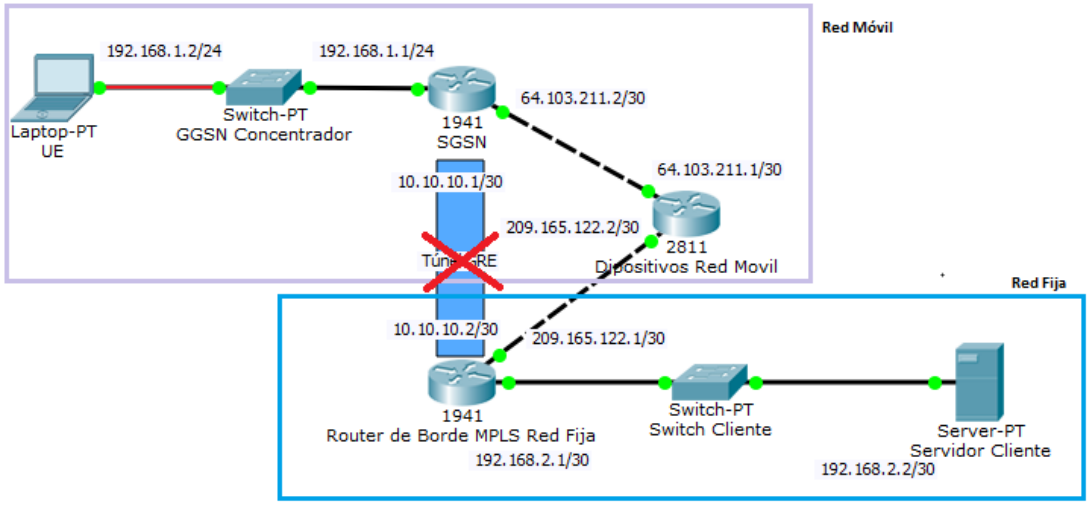

Ilustración 28 Túnel GRE deshabilitado. Imagen tomada de Packet Tracer

Para tener un túnel sin funcionamiento, se puede lograr de dos formas, no tener la configuración o tenerla, pero deshabilitarla. En el caso en que se opte por no tener configuración, en la Ilustración 29 se resaltan los comando que se deberían suprimir en los equipos de extremo.

SGSN

```
!
interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/1
 tunnel destination 209.165.122.2
!
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 64.103.211.2 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 10.10.10.2
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
```

Router de borde MPLS fija

```
!
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/1
 tunnel destination 64.103.211.2
!
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 209.165.122.2 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
!
ip flow-export version 9
```

Ilustración 29 Configuración que se excluyen para bajar un túnel. Imagen tomada de Packet Tracer

- Para el caso de esta simulación, se deshabilitará el túnel dejando la configuración pero que no sea efectiva, utilizando en el SGSN los comandos en Packet Tracer: "*interface Tunnel0-> no ip address ->shutdown ->end",* los cuales deshabilitan la configuración del túnel y se verifica a través del comando "*interface brief"*, como se muestra en la Ilustración 30.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.1.1     YES manual up                    up

GigabitEthernet0/1     64.103.211.2    YES manual up                    up

Tunnel0                10.10.10.1      YES manual administratively down down
```

Ilustración 30 Túnel shutdown en el SGSN. Imagen tomada de Packet Tracer

- Una vez el túnel es deshabilitado, el router SGSN únicamente conoce las redes directamente conectadas: IP 192.168.1.1 e IP 64.103.211.2, como se muestra en la tabla de enrutamientos de la Ilustración 31.

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       64.103.211.0/30 is directly connected, GigabitEthernet0/1
L       64.103.211.2/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/1
```

Ilustración 31 Tabla de enrutamiento SGSN sin conocer la red del servidor. Imagen tomada de Packet Tracer

- En el Router de borde de la red MPLS red fija, se aplica también los comandos para deshabilitar el túnel y se verifican a través del comando *"interface brief",* como se muestra en la Ilustración 32.

```
show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.2.1     YES manual up                    up

GigabitEthernet0/1     209.165.122.2   YES manual up                    up

Tunnel0                10.10.10.2      YES manual administratively down down
```

Ilustración 32 Túnel GRE deshabilitado en el router de borde de la MPLS. Imagen tomada de Packet Tracer

- Con el túnel deshabilitado el Router de borde de la red MPLS red fija no conoce la red donde se encuentra UE cuando el túnel esta deshabilitado, como se muestra en la Ilustración 33.

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
     209.165.122.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.122.0/30 is directly connected, GigabitEthernet0/1
L       209.165.122.2/32 is directly connected, GigabitEthernet0/1
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/1
```

Ilustración 33 Tabla de enrutamiento router de borde MPLS red fija sin conocer la red de UE. Imagen tomada de Packet Tracer

- El dispositivo UE no puede alcanzar el servidor de cliente con IP 192.168.2.2.

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:70FF:FE59:52A8
   IP Address......................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.1.1

PC>PING 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 34 Ping no alcanzable desde UE hacia el servidor. Imagen tomada de Packet Tracer

b. Túnel habilitado

A continuación, se verá la configuración con el túnel GRE habilitado, donde el dispositivo UE y el servidor tienen conexión, como se muestra en la Ilustración 35:

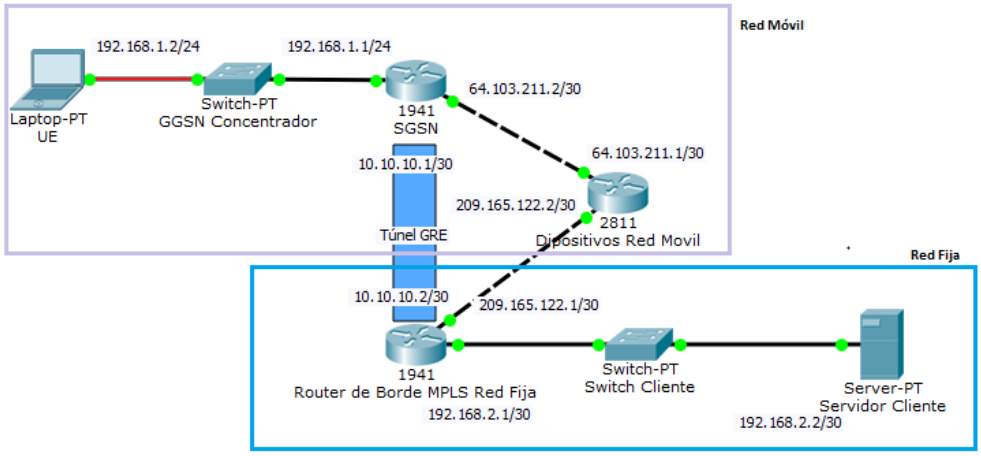

Ilustración 35 Túnel GRE habilitado. Imagen tomada de Packet Tracer

- En el Router SGSN se ha habilitado el túnel0 donde se configura el GRE, como se muestra en la Ilustración 36.

```
Router(config-if)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.1.1     YES manual up                    up

GigabitEthernet0/1     64.103.211.2    YES manual up                    up

Tunnel0                10.10.10.1      YES manual up                    up
```

Ilustración 36 Túnel habilitado en el SGSN. Imagen tomada de Packet Tracer

- Con el túnel habilitado, desde el router SGSN se conoce las redes iniciales más la red donde se encuentra el servidor, IP 192.168.2.0, como se muestra en la Ilustración 37.

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       64.103.211.0/30 is directly connected, GigabitEthernet0/1
L       64.103.211.2/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/1
```

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Tunnel0
L       10.10.10.1/32 is directly connected, Tunnel0
     64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       64.103.211.0/30 is directly connected, GigabitEthernet0/1
L       64.103.211.2/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
S    192.168.2.0/24 [1/0] via 10.10.10.2
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/1
```

Ilustración 37 Tabla de enrutamiento SGSN, en la parte izquierda túnel habilitado y en la derecha túnel deshabilitado. Imagen tomada de Packet Tracer

- En el router de borde de la red MPLS red fija se encuentra habilitado el túnel0 donde se configura e GRE, como se muestra en la Ilustración 38.

```
Router(config-if)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.2.1     YES manual up                    up

GigabitEthernet0/1     209.165.122.2   YES manual up                    up

Tunnel0                10.10.10.2      YES manual up                    up
```

Ilustración 38 Túnel GRE habilitado en el router de borde de la MPLS. Imagen tomada de Packet Tracer

- El Router de borde de la red MPLS red fija conoce la red donde se encuentra UE cuando el túnel está habilitado, como se muestra en la Ilustración 39.

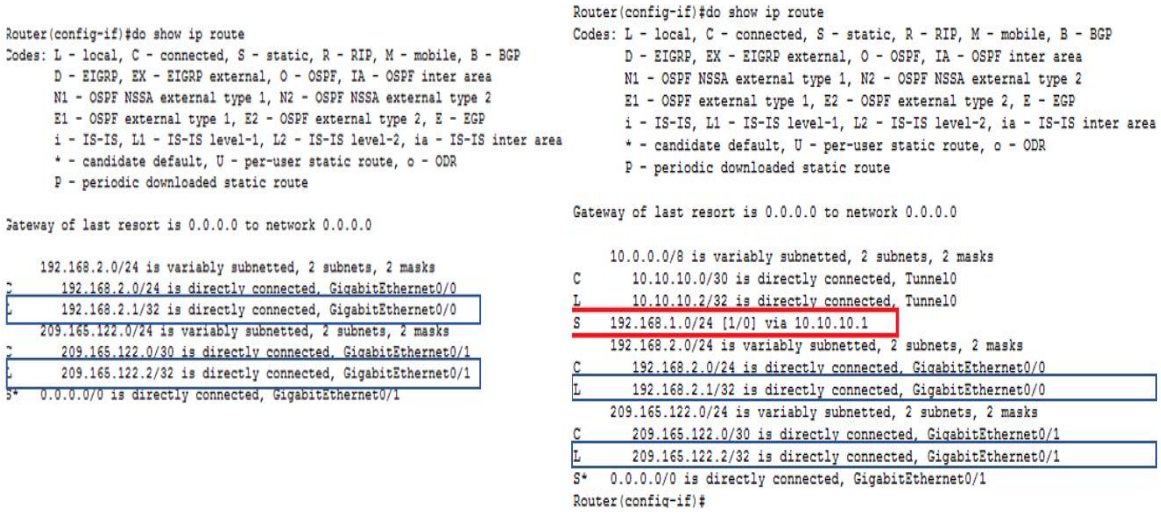

Ilustración 39 Tabla de enrutamiento router de borde MPLS red fija conoce la red de UE, en la parte izquierda túnel habilitado y en la derecha túnel deshabilitado. Imagen tomada de Packet Tracer

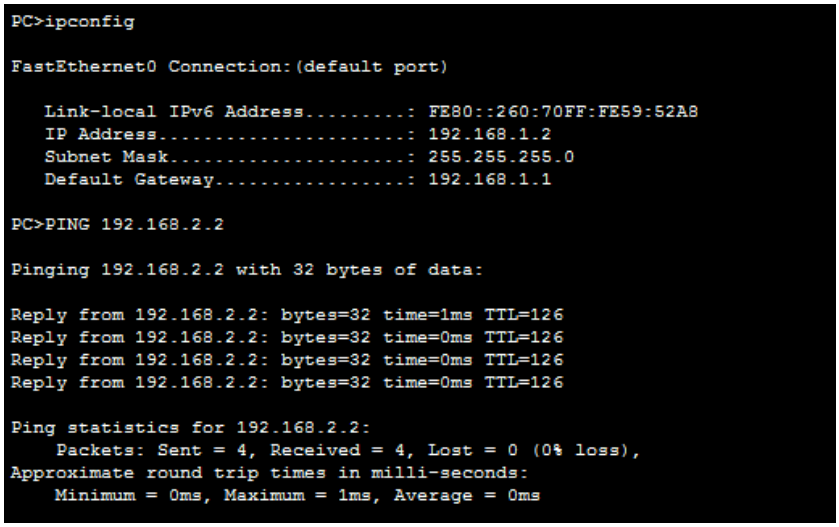

Ilustración 40 Ping alcanzable desde UE hacia el servidor

Como se puede ver en la Ilustración 40, el dispositivo móvil puede alcanzar al servidor, a pesar de que el router de borde de la red móvil no conozca ninguna de las redes, eso se logra por que el túnel está operativo y funcionando. De esta forma, posterior a que se establece el contexto PDP a través del cual se valida la conexión,

a través del túnel GRE se encapsula el tráfico para llevarlo de origen a destino pasando por las entidades intermedias y permitiendo reconocer la IP de origen, que, dependiendo de la solución, puede ser utilizada para generar una respuesta a través del tráfico bidireccional.

5.3. El papel de los APN en las comunicaciones móviles

El APN (Access Point Name), es un nombre lógico utilizado por un SGSN para determinar qué GGSN debe usarse para el UE y a su vez el GGSN para determinar los servicios solicitados por el usuario o el punto de destinos al que se deben enviar los paquetes del UE. A cada suscripción que se realiza en el HLR se le asigna un APN, el cual se crean según las necesidades.

Además de ser registrados en la red celular, el APN debe quedar registrado en el dispositivo móvil de acceso a la red, según el fabricante el proceso de configuración será diferente y los parámetros que se deberán ingresar deben ser provistos por el CSP quien debe entregar los parámetros registrados en elementos de red registrados en el HLR y GGSN. En la Ilustración 41 se muestra un ejemplo de configuración de APN en un dispositivo celular.

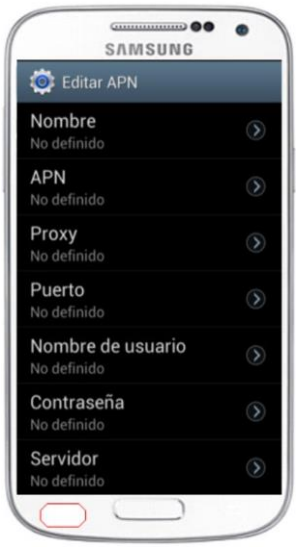

Ilustración 41 Configuración de APN en celular[17]

[17] SAMSUNG, ¿Cómo configurar la APN de mi Samsung Galaxy? [en línea]: <https://www.samsung.com/latin/support/mobile-devices/how-to-set-the-apn-of-my-samsung-galaxy/> [Citado en marzo de 2021]

Los APN puede ser personalizados según necesidades específicas de la solución a implementar, estas personalizaciones modifican algunos aspectos que se tienen por defecto dentro del proceso de acceso a la red, permitiendo marcar desde el dispositivo móvil el tratamiento que se le dará a las solicitudes de acceso hasta el GGSN y este último, a su vez podrá dar un tratamiento particular para direccionar tráfico hacia el punto de conexión final.

Lo anterior permiten aportar a la planificación y arquitectura de red para el despliegue de una solución M2M e IoT con la identificación del tráfico, la cual es una capacidad básica que permite a las arquitecturas optimizar la red para manejar mejor las soluciones M2M e IoT. El GGSN, es la puerta de enlace a redes basadas en IP, como empresas o Internet.

a. APN Genérico

Se hará referencia como APN Genérico a todas las solicitudes de acceso a la red celular que establecen una sesión PDP y utilizan un APN para realizar la transmisión de datos con los parámetros establecidos por defecto dentro de la red celular del CSP y que habitualmente su último punto de conexión es internet. Comúnmente los accesos a la red de usuarios naturales.

b. APN Privado

Se hará referencia a los APN privado, a los APN creados para escenarios en que se requieren personalizar los puntos de acceso finales y modificar algunos aspectos que son variables en la red celular modificando los parámetros habituales, para efectos del presente documento los llamaremos APN privados.

5.4. Parámetros de parametrización en un APN

Los APN privados deben ser creados tanto en el GGSN como en el HLR para que se pueda activar el contexto PDP y el direccionamiento IP al que sea asociado también debe ser aprovisionado en las diferentes entidades para las configuraciones particulares.

La conexión para unas soluciones M2M e IoT se debe asegurar desde el dispositivo de conexión pasando por la red de transporte hasta el punto final que puede ser desde la red LAN de una empresa o internet. Los parámetros de variación se presentan a continuación en la Ilustración 42.

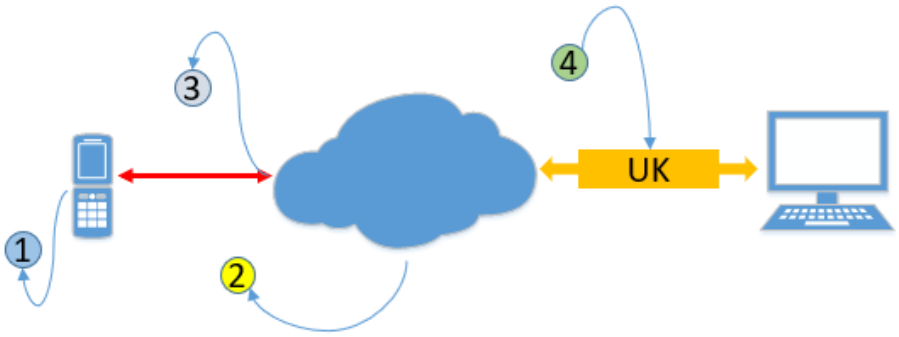

Ilustración 42 Proceso de configuración de un APN. Fuente propia

1. El direccionamiento IP: En este punto se hace referencia a la IP del UE, en el momento en que crea el APN es posible especificar si se requiere asignar un direccionamiento fijo o dinámico.
    a. En el caso de tener un direccionamiento dinámico la IP que asignará el GSN al UE será temporal mientras un UE realiza una petición o sesión en la red, una vez termina esta sesión, la IP es liberada para que otro UE la pueda utilizar. Este es el tipo de configuración habitualmente utilizada.
    b. En el caso de tener un direccionamiento IP fijo, al UE tendrá siempre la misma dirección para cada solicitud de acceso a la red. Para este caso, la IP es asociada al IMSI en el momento en que se realiza el aprovisionamiento de la SIM card.
2. CON Autenticación o SIN Autenticación: A través del AAA es posible manejar una tabla de Usuario y Contraseña que es aprovisionada en el IMSI en el momento de la activación de la SIM card. Este campo habitualmente no se utiliza en los APN genéricos, sin embargo, en los APN privados aporta un nivel de seguridad, ya que es un doble factor de autenticación en el momento de registrar el APN en un dispositivo.
3. Nombre del APN: En el momento que se crea el APN, el nombre se personaliza de acuerdo con el requerimiento del solicitante. Los APN genéricos llevan comúnmente el nombre del CSP, por ejemplo:

ETB Internet. APN: moviletb.net.co, Movistar Internet. APN: internet.movistar.com.co

4. Conexión de Ultimo Kilometro: Una vez el tráfico se encuentra en el GGSN es posible tratarlo según la conexión final que se requiera hacia las redes externas. Por ejemplo, en el caso de los usuarios naturales que requieren soluciones de datos con propósitos de consulta a internet hacia servicios como: Whatsapp, Waze, Google etc. que se encuentran públicos, el GGSN enruta el tráfico hacia la salida a internet del CSP. En caso contrario los siguientes puntos es posible ajustarlos dentro de la configuración del APN:

    a. Realizar el enrutamiento hacia la dirección IP destino, la cual estará asociada por ejemplo con el servidor de la aplicación.
    b. Lista de los puertos de Comunicaciones que utiliza la aplicación del cliente para comunicarse con los equipos remotos.
    c. Protocolo de enrutamiento de la red con la que se desea conectar.

Todos estos parámetros pueden marcar una diferencia en la conectividad de las soluciones M2M y este último parámetro especialmente facilita además la integración con redes externas, ya que como vimos en los apartados anteriores, en el momento en el que se establece el contexto PDP, se establece un túnel entre el GGSN y SGSN para realizar el intercambio de paquetes a través de protocolos de encapsulamiento y a partir de allí se puede continuar manejando el tráfico usando diferentes protocolos de enrutamiento.

5.5 El papel del tipo de SIM card en la solución M2M e IoT

De manera similar a la de la red celular las sim card también tuvieron una evolución, tanto en su tamaño como en sus características, para proporcionar servicios añadidos y almacenamiento. Las sim iniciaron del tamaño de una tarjeta de crédito y hoy en día se encuentran disponible sim nano del tamaño 6 x 5 mm, esto ha permitido optimizar espacio a nivel de hardware en los dispositivos y es factor necesario para tener en cuenta dentro de una solución M2M e IoT.

Esta evolución ha segmentado además el tipo de características que se ofrecen, entre las sim comunes usadas habitualmente por los Smartphone y las destinadas para soluciones de M2M o IoT. Es por esto que además del tamaño, existen otros factores para tener en cuenta que veremos más adelante, ya que primero es necesario introducir el concepto de "Universal Integrated Circuit Card" (UICC) ya que es la forma en que hace referencia al componente a través del cual se realiza la autenticación y se suscribe hacia la red celular. A continuación, se cita la definición que establece GSMA para el término de UICC y SIM:

SIM: Módulo proporcionado por el operador de red móvil que contiene la identidad de abonado móvil internacional (IMSI) y los parámetros de seguridad utilizados para autenticar la (U) SIM con la red. Conocido como la aplicación de autenticación contenida en el "Universal Integrated Circuit Card" (UICC).

UICC: La tarjeta inteligente utilizada por una red móvil para autenticar dispositivos para la conexión a la red móvil y el acceso a los servicios de red.[18]

Las UICC tienen aspectos de hardware y software que es importante considerar según la necesidad de cada solución, las cuales van desde el tamaño del slot donde se instalara la SIM, las condiciones ambientales que soporta, vida útil, entre otras. Para conocer alguno de los parámetros para tener en cuenta, es posible empezar con el documento de ETSI TS 102 671 V9.0.0 donde se encuentra características físicas y lógicas de referencia, en la Ilustración 43 se listan algunas de ellas:

Environmental property letter	Description of environmental property	Property details in clause
T	Operational and storage temperature	5.2
M	Moisture/Reflow conditions	5.3
H	Humidity	5.4
C	Corrosion	5.5
V	Vibration	5.6
F	Fretting Corrosion	5.7
S	Shock	5.8
R	Data Retention time	5.9
U	Minimum Updates	5.10

Ilustración 43 Descripción de los indicadores de propiedad ambiental[19]

[18] GSM Association, TSG.34 - IoT Device Connection Efficiency Guidelines [en línea]: < https://www.gsma.com/iot//wp-content/uploads/2016/04/TS-34-v3-0v2.pdf >[Citado en marzo de 2021]

[19] ETSI, TS 102 671 - V9.0.0 [en línea]: < https://www.etsi.org/deliver/etsi_ts/102600_102699/102671/09.00.00_60/ts_102671v090000p.pdf>[Citado en marzo de 2021]

En el momento de tomar la decisión de cuál es el tipo de SIM a utilizar, será necesario tener en cuenta las características de la solución, que van desde el hardware disponible en el dispositivo a utilizar hasta las condiciones dinámicas, eléctricas y ambientales de la solución, para esto es posible apoyarse por un lado en los estándares que sean definidos por 3GPP o ETSI y la información técnica definida por el fabricantes, como : Gemalto, G&D, Morpho (Safran), VALID. Esta información puede ser encontrada de la siguiente manera dependiendo del tipo de aplicación:

Familia de productos	Domestic Quad	Industrial^{Plug} 85	Industrial^{Plug} 105	Industrial Quad	Automotive Quad
Drivers	Miniaturización	Sirve para todos los equipos	Sirve para todos los equipos	Uso industrial	Uso automotor
	Electrónica M2M de consumo	Tecnología M2M industrial	Tecnología M2M industrial **Resistencia extendida**	Tecnología M2M industrial **Resistencia extendida**	Estándar automotor **Resistencia extendida**
					
Rango de resistencia a la temperatura	-25 °C / +85 °C	-25 °C / +85 °C	-40 °C / +105 °C	-40 °C / +105 °C	-40 °C / +105 °C
Confiabilidad	•	••	••	••	•••
Calificación M2M (JEDEC)			•	•	•
Mecanismo eXtended Life	Opcional	•	•	•	•
Silicio mejorado		•	•	•	•
Burn-in					•
retención de datos	10 años y / 25 °C	10 años y / 85 °C	10 años y / 85 °C	10 años y / 85 °C	17 años y / 80 °C
Cumplimiento con los requisitos automotores					AEC Q100 / TS 16 949

Ilustración 44 Gama de producto del fabricante Gemalto.[20]

[20] THALESGROUP, Modulo de Identificación de Maquinas [en línea]: < http://www.thalesgroup.com/sites/default/files/gemalto/M2M_MIM-es.pdf >[Citado en abril de 2021]

6. CASOS DE USO DE SOLUCIONES M2M/IOT

Como vimos anteriormente la utilización de las redes celulares aportan varios beneficios a las soluciones permitiendo replicar su aplicabilidad en sectores como industria, transporte, entre otros. Luego como se expuso en el capítulo anterior, existen elementos propios de las redes celulares que es necesario ajustar a las soluciones particulares con el fin de obtener un mejor desempeño y aplicabilidad. Al final las diferentes combinaciones se pueden emplear obteniendo variaciones según se necesiten

6.1 Integración con redes externas

Alineando los conceptos vistos hasta el momento, una vez el contexto PDP es establecido se inicia el proceso de transmisión de datos a través de túneles que son terminados habitualmente en el GGSN, que puede considerar el equipo de borde donde el tráfico es entregado bajo protocolo IP; en este punto es posible integrarse con otras redes a través de conexiones de último kilómetro como MPLS, “Virtual Private Network”(VPN) o NAT y diferenciarse de las conexiones usadas habitualmente como se ilustra en las siguientes imágenes:

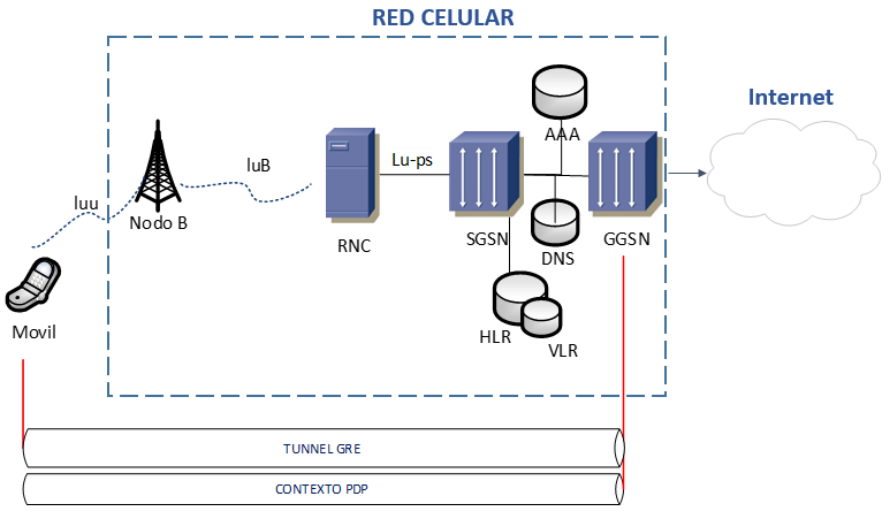

Ilustración 45 Arquitectura de red para conexión con internet

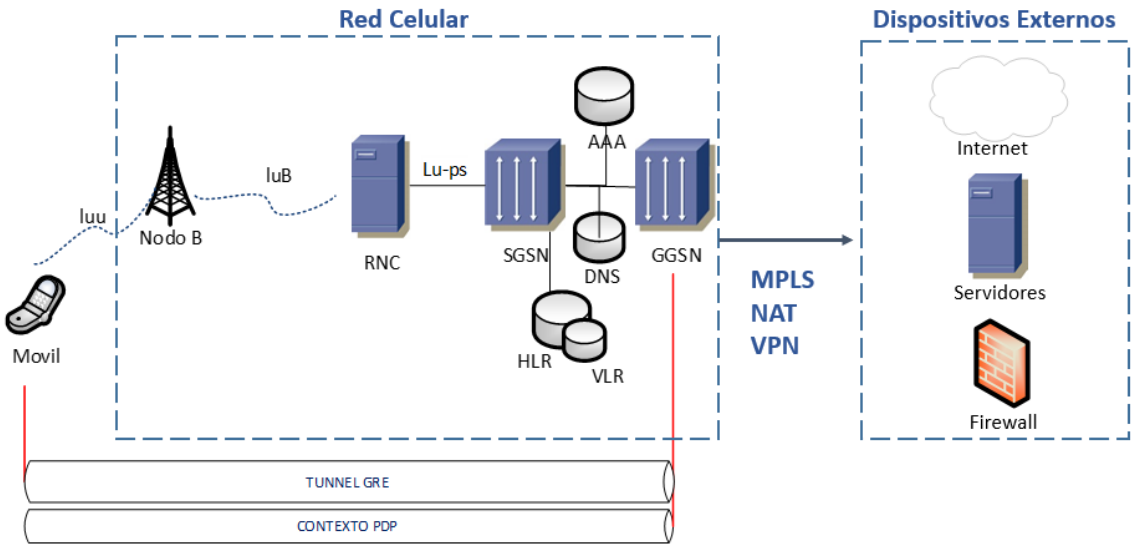

Ilustración 46 Integración de red celular con dispositivos externos. Fuente propia

En el extremo opuesto de la red celular pueden estar otros dispositivos, servidores o internet para interactuar entre sí e intercambiar información y cumplir con el propósito específico de la solución, ya que es posible utilizar no solo un tipo de comunicación sino generar combinación de los diferentes factores.

A continuación, revisaremos algunos ejemplos de uso y que parámetros son preferibles ajustar para cada caso, donde partiremos del requerimiento inicial funcional y así definir los elementos para tener en cuenta en cada caso.

6.2 Factores para tener en cuenta en el desarrollo de una solución M2M

Una vez explorados los diferentes componentes que se involucran dentro de una solución M2M e IoT por red celular, en el siguiente flujo se establece la propuesta de factores para tener en cuenta dentro su diseño e implementación. En el flujo se plantea requisitos básicos para evaluar y se pone en consideración aspectos de carácter técnico enfocados a establecer la línea base que permita encontrar el mejor camino para cierto tipo de requerimientos. Es importante tener en cuenta que pueden existir cualquier tipo de consideraciones adicionales que causen una variación en el flujo.

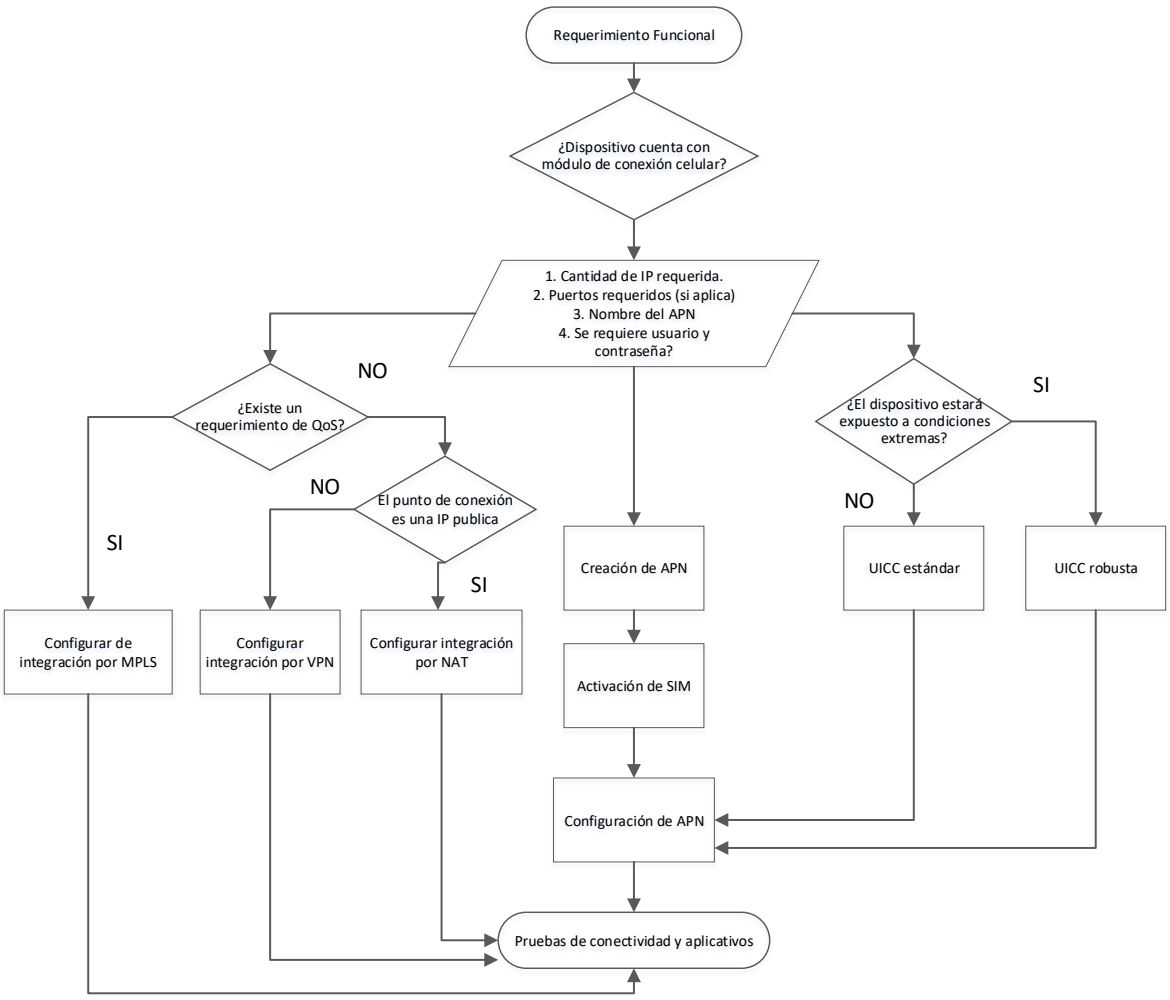

Ilustración 47 Flujo para el diseño de una solución M2M e IoT usando la red celular. Fuente propia

A continuación, se establecerá el mejor camino para tres casos de aplicación pensados bajo condiciones particulares permiten ejemplificar las tres opciones de integración planteadas en el flujo.

6.3 Gestión Vehicular

a. Requerimiento Inicial

En una ciudad se requiere implementar una solución vehicular que permita monitorear desde una plataforma instalada en el Centro de Datos de la entidad de transporte local, los datos de telemetría de vehículos de transporte público y acceder en tiempo real a las cámaras de CCTV que se encuentra instaladas dentro del vehículo.

En total son 300 vehículos y cada uno cuentan con módulo celular integrado, el cual se encuentra instalado en el interior del vehículo y es el encargado de concentrar la información de telemetría y CCTV. Se ha solicitado especificar la conectividad sugerida para el funcionamiento de la solución.

b. Análisis de requisitos.

En el análisis de la solución es posible desglosar los siguientes requerimientos para identificar los parámetros apropiados para la solución.

1. ¿Dispositivo cuenta con un módulo de conexión celular?
   De acuerdo con la información proporcionada el vehículo cuenta con un módulo celular integrado, lo cual permite pensar en que podemos establecer una solución que utilice la red móvil como mecanismo de transporte de datos.

2. ¿Se requiere un APN privado o genérico?
   Aunque el requerimiento no lo específica, con el análisis realizado hasta el momento se identifica la necesidad de utilizar un direccionamiento fijo que permita a través de una IP identificar cada bus y establecer la comunicación de video desde y hacia el centro de datos.

3. Cantidad de IP requerida
   De acuerdo con el requerimiento se requiere monitorear 300 vehículos, en consecuencia, se necesitan 300 IPs lo que nos lleva a escoger una mascara de red /23 que, aunque tiene más IPs de las que se necesita es la mejor

opción ya que la máscara de red /24 proporciona 254 y la máscara /22 proporciona 1022.[21]

4. Puertos requeridos (si aplica)
   En el requerimiento no se especifica un puerto en particular y a menos que se especifique desde el requerimiento no existe otro camino para determinarlo.

5. Nombre del APN
   Para definir el nombre no se requiere una estructura particular, por lo cual tomaremos la funcionalidad para definirlo, de la siguiente manera: solucionvehicular.com.co

6. ¿Se requiere usuario y contraseña?
   En la solicitud no se establece este requisito y dado que no se identifica una necesidad funcional para recomendarlo.

7. ¿Existe un requerimiento de QoS?
   Aunque en el requerimiento no se especifica, dentro de la información se indica que la comunicación se utilizara para acceder a un sistema de CCTV, lo cual nos lleva a concluir que se tendrá tráfico de video, el cual para poder proporcionar un buen servicio se recomienda utilizar una calidad de servicio (QoS).

8. ¿La SIM card se encontrará en un entorno de condiciones ambientales extremas?
   En la información proporcionada nos indican que la SIM card se encontrará dentro de un vehículo, por lo anterior se puede considerar que está expuesta a situaciones extremas de vibración y probablemente de temperatura y humedad.

c. Solución Propuesta

Dado que la solución dispone de un dispositivo con módulo para comunicación móvil, es posible establecer una conexión a través de la red móvil que permita contar

[21] CISCO, Host and Subnet Quantities [en línea]: < https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13790-8.html[Citado en abril de 2021]

con un APN privado que cuente con un direccionamiento con mascara /23 para dar conexión a los 300 buses, el APN no debe contar con usuario y contraseña.

Una vez establecida la conexión en el segmento móvil, la mejor opción para conexión con el centro de datos será la conexión del tipo MPLS, ya que, aunque el uso de una VPN es viable no garantiza la calidad de servicio (QoS) recomendada para el transporte de trafico de video. El caso de la opción de NAT, no es viable ya que en el requerimiento no indica que el centro de datos sea accesible a través de una IP publica y típicamente este tipo de instalaciones manejan segmentos de red privados.

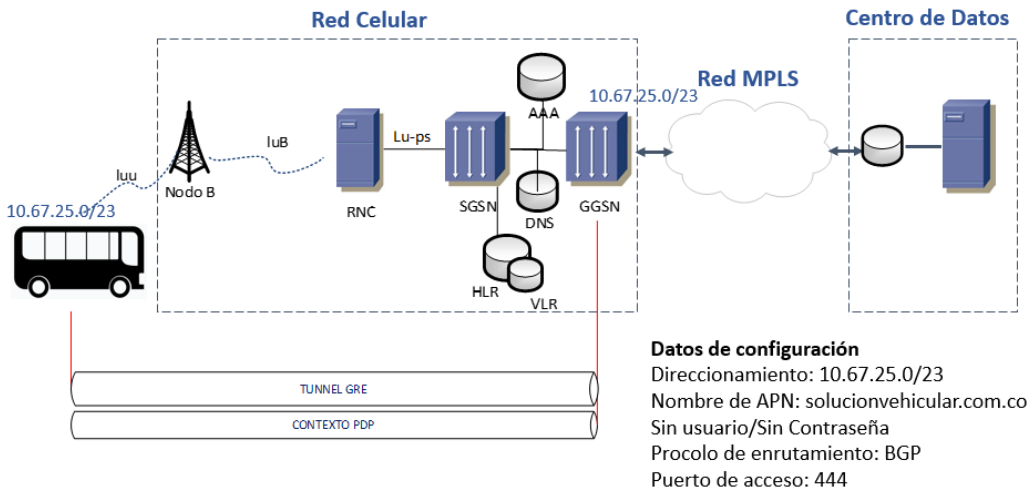

Ilustración 48 Arquitectura propuesta Gestión Vehicular. Fuente propia

De acuerdo con la arquitectura, la configuración de datos puede ser de la siguiente manera:

Direccionamiento: Para poder establecer una integración a través de MPLS, es necesario contar un direccionamiento fijo que permita establecer el enrutamiento a través de la red. Este debe ser especificado desde el inicio para ser configurado en el HLR y en el GGS, para este caso se definió, por ejemplo, 10.67.25.0 con una máscara 23 como ya mencionamos para obtener una IP para cada bus.

Este parámetro es asignado además en el momento en que se aprovisiona la SIM card y como mencionamos anteriormente, será el identificador de cada bus.

Protocolo de enrutamiento: Este no es un parámetro propio de la red celular y se utiliza normalmente para establecer el tipo de comunicaciones con redes externas

y depende principalmente del protocolo que sea configurado en el centro de datos, ya que el mismo debería ser configurado en el GGSN.

6.4 Monitoreo de pozos desde una plataforma en la nube

a. Requerimiento Inicial

Una empresa petrolera cuenta con una plataforma de monitoreo alojada en la nube de Amazon y requiere poderse conectar desde la plataforma a dispositivos de Telemetría instalados en 20 pozos distribuidos en zonas rurales a nivel nacional.

La empresa ha solicitado tener en cuenta los siguientes mecanismos de seguridad dentro de la comunicación:

- Configuración de APN diferente a Internet que cuente con Usuario/Contraseña.
- Direccionamiento IP fijo para cada pozo.
- Trafico por un puerto 143/TCP y 161/UDP
- Configuración de túnel con uso de certificados de 168 BITS

b. Análisis de requisitos.

En el análisis de la solución es posible desglosar los siguientes requerimientos para identificar los parámetros apropiados para la solución.

1. ¿Dispositivo cuenta con un módulo de conexión celular?

   En la información no se especifica que el dispositivo cuente con un módulo de conexión celular; sin embargo, para efectos del ejercicio se trabajará bajo el supuesto de que se cuenta con dentro de la solución o que será sugerido dentro de la propuesta de solución. Esto ultimó debido a que, además de los escenarios donde el elemento objeto de medición es móvil, cuando el objeto se encuentra ubicado en zonas de difícil acceso también recomendado el uso de tecnología móvil en términos de costos y tiempos de implementación.

2. ¿Se requiere un APN privado o genérico?

   Aunque el requerimiento no lo específica, con el análisis realizado hasta el momento se identifica la necesidad de utilizar un direccionamiento fijo que

permita a través de una IP identificar cada pozo e implementar una opción de integración hacía la nube de Amazon.

3. Cantidad de IP requerida

   De acuerdo con el requerimiento se requiere monitorear 20 pozos, en consecuencia, se necesitan 20 IPs lo que nos lleva a escoger una máscara de red /27 que, aunque tiene más IPs de las que se necesita es la mejor opción ya que la máscara de red /28 proporciona 14 y la máscara /26 proporciona 62. [22]

4. Puertos requeridos (si aplica)

   Normalmente la definición de puertos es establecida por la aplicación o servidor, este dato debe ser validado con el área usuaria y sea configurado en el momento de la creación del APN. para este caso el requerimiento solicita 143/TCP y 161/UDP.

5. Nombre del APN

   Para definir el nombre no se requiere una estructura particular, por lo cual tomaremos la funcionalidad para definirlo, de la siguiente manera: monitoreopozos.com.co

6. ¿Se requiere usuario y contraseña?

   En el requerimiento se solicitó adicionalmente utilizar usuario y contraseña, estos parámetros deben ser especificados en el momento de la creación del APN y son aprovisionados cuando se activa la SIM card. Es importante tener en cuenta que estos parámetros deben ser configurados en el dispositivo en el momento de la instalación de la SIM card.

7. ¿Existe un requerimiento de QoS?

   La información de Telemetría normalmente no involucra una demanda considerable en términos de ancho de banda, si bien no debe ser necesario contar con la información de la cantidad de datos transmitidos por minutos, para efectos de este ejercicio se supondrá que no son considerables y que no existe una demanda en términos de ancho de banda.

---

22 CISCO, Host and Subnet Quantities [en línea]: < https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13790-8.html[Citado en abril de 2021]

8. ¿La SIM card se encontrará en un entorno de condiciones ambientales extremas?

   De acuerdo con la información proporcionada el monitoreo se realizará en pozos petroleros, los cuales pueden estar ubicados en zonas extremas en términos de temperatura, húmedas y corrosión. Estos parámetros nos llevan a considerar SIM card que soporten estas condiciones ambientales.

c. Solución Propuesta

De acuerdo con la información proporcionada se requiere conectar 20 dispositivos con una plataforma en la nube, para este caso ambos elementos son estáticos, pero se debe considerar que son puntos distantes al parecer de difícil acceso a través de redes cableadas, por eso como mencionamos anteriormente es recomendado una solución a través de la red celulares.

Para la integración, un tipo de conexión MPLS como en el caso anterior puede llegar a ser viable, sin embargo, es necesario considerar la relación costo beneficio ya que el tráfico de datos es menor y la inversión en un tipo de conexión cableada en este caso será importante, considerando que la solución se encuentra en la nube y seguramente en servidores internacionales.

Este caso la conexión tipo VPN permite además de establecer la conexión solicitada, es posible utilizar conexiones seguras sobre internet y emplear protocolos cifrados, como lo es el protocolo IPsec que según fabricante CISCO permite un cifrado a 168 bits[23] como se solicita desde el requisito. La VPN se deben establecer normalmente desde un servidor o firewall, habitualmente se levanta VPN de la red móvil hasta un equipo VPN del cliente y se puede tener tráfico en doble sentido.

[23] CISCO, Como funcionan las redes privadas virtuales [en línea]: < https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html [Citado en marzo de 2021]

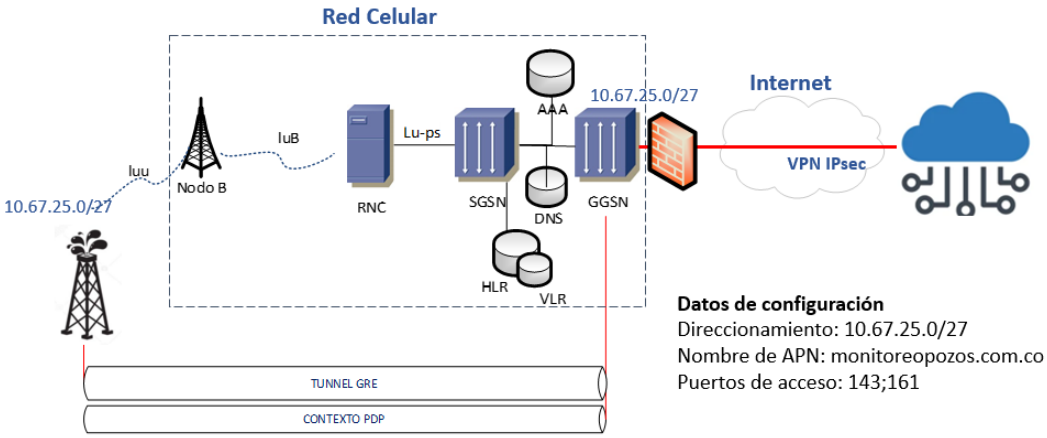

Ilustración 49 Arquitectura propuesta monitoreo de pozos. Fuente propia

De acuerdo con la arquitectura la configuración de datos puede ser de la siguiente manera:

Direccionamiento: Como se especificó en el requerimiento se debe asignar direccionamiento fijo, este debe ser especificado desde el inicio para ser configurado en el HLR y en el GGS, para este caso se definió por ejemplo 10.67.25.0 con una máscara 27 para poder tener la cantidad de IPs necesarias para los 20 pozos.

Este parámetro es asignado además en el momento en que se aprovisiona la SIM card y como mencionamos anteriormente será el identificador de cada pozo.

Protocolo de enrutamiento: Este no es un parámetro propio de la red celular y se utiliza normalmente para establecer el tipo de comunicaciones con redes externas y depende principalmente del protocolo que sea configurado en el centro de datos, ya que el mismo debería ser configurado en el GGSN.

6.5 Registro de ventas en cadena de suministros

a. Requerimiento Inicial

Una cadena de suministros le ha proporcionado a sus mercaderistas tabletas con conexión celular para que registren sus ventanas durante las visitas que realizan a sus clientes que se encuentran ubicados en diferentes puntos de la ciudad. Con el fin de controlar el uso que les dan a las tabletas, la empresa requiere una solución

que permita a los mercaderistas conectarse exclusivamente con la plataforma de registro de ventas que es alcanzable a través de una IP pública.

En la solución es necesario que cada tableta cuente con una IP fija para un total de 64 vendedores.

b. Análisis de requisitos.

En el análisis de la solución es posible desglosar los siguientes requerimientos para identificar los parámetros apropiados para la solución.

1. ¿Dispositivo cuenta con un módulo de conexión celular?
   Según el requisito la conexión se requiere a través de una tableta con conexión celular.

2. ¿Se requiere un APN privado o genérico?
   Aunque el requerimiento no lo específica, con el análisis realizado hasta el momento se identifica la necesidad de utilizar un direccionamiento fijo que permita a través de un segmento de red que se pueda enrutar hacia una misma IP publica exclusivamente.

3. Cantidad de IP requerida
   De acuerdo con el requerimiento se requiere la conexión para 24 tabletas, en consecuencia, se necesitan 64 IPs lo que nos lleva a escoger una máscara de red /26 que, aunque tiene más IPs de las que se necesita es la mejor opción ya que la máscara de red /25 proporciona 126 y la máscara /27 proporciona 30. [24]

4. Puertos requeridos (si aplica)
   De acuerdo con la información proporcionada no se requiere conexión hacia un puerto especifico.

[24] CISCO, Host and Subnet Quantities [en línea]: < https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13790-8.html[Citado en abril de 2021]

5. Nombre del APN

   Para definir el nombre no se requiere una estructura particular, por lo cual tomaremos la funcionalidad para definirlo, de la siguiente manera: mercaderistas.com.co

6. ¿Se requiere usuario y contraseña?

   En los requerimientos no se especifica si deba tener usuario y contraseña, sin embargo, para el escenario en que los dispositivos de conexión son de fácil acceso a terceros, se recomienda la utilización de un doble factor de autenticación, para este caso la utilización de usuario y contraseña.

7. ¿Existe un requerimiento de QoS?

   La transmisión de datos normalmente no involucra una demanda considerable en términos de ancho de banda, si bien no debe ser necesario contar con la información de la cantidad de datos transmitidos por minutos, para efectos de este ejercicio se supondrá que no son considerables y que no existe una demanda en términos de calidad de servicio.

8. ¿La SIM card se encontrará en un entorno de condiciones ambientales extremas?

   De acuerdo con la información proporcionada la SIM card no sé encontrara en un entorno bajo condiciones ambientales extremas.

c. Solución Propuesta

Este tipo de uso resulta bastante habitual ya que aporta flexibilidad en tareas administrativas de áreas como de ventas y control, las cuales reciben el mayor aprovechamiento, además de ser fácil masificarse a un bajo coste. Para la integración la conexión más conveniente es la integración a través del uso de un NAT ya que facilita la conexión desde el segmento de red privado del APN hacía la IP pública del servidor. Se podría pensar ocasionalmente, en la utilización conexiones de internet común para este tipo de propósito, sin embargo, a través de este método es posible generar un control según el requisito, ya que desde el GGSN únicamente permitirá la conexión hacia la IP publica configurada.

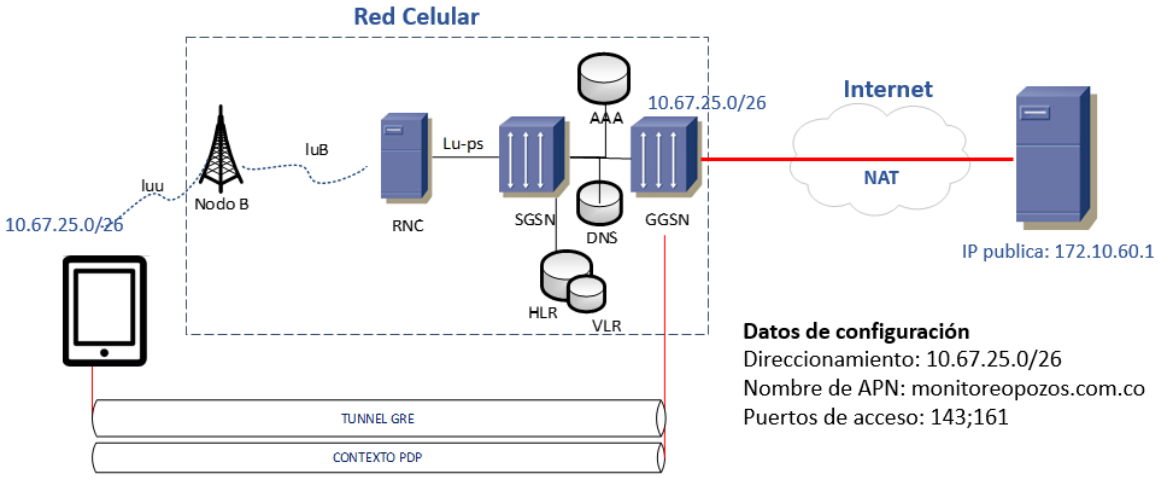

Ilustración 50 Arquitectura propuesta para registro de ventas. Fuente propia

7. CONCLUSIONES

- En términos de tecnología celular, organizaciones de estandarización como ETSI y 3GPP en conjuntos con fabricantes tecnológicos, proporcionan una cantidad importante de información que facilita el entendimiento de la conectividad para soluciones M2M e IoT; sin embargo, dada la gran cantidad de información disponible en línea y la rapidez con que se actualiza, es importante dedicar tiempo en hacer un filtro de las fuentes de información para asegurar un adecuado marco de referencia.

- La red celular, como medio de comunicación entre los dispositivos de las soluciones M2M e IoT, facilitan la generación de alternativas de conexión para dispositivos que se requiere que funcionen en movimiento o estarán instalados en zonas de difícil acceso para rede cableadas, proporcionando además flexibilidad para el despliegue y operación de la solución.

- La facilidad de poder crear APN ajustados a soluciones específicas, como un símil de una red privada dentro de la rede celular, permite no solo aprovechar la utilización de parámetros de seguridad en autenticación sino además facilitan el intercambio de información con redes externas a través de la asignación de dirección IP fijas a los dispositivos móviles.

- La integración entre redes celulares y redes convencionales se puede lograr a través de la utilización de comunicación basada en IP, utilizando protocolos de intercambio de datos sobre túnel GRE, el cual facilita la comunicación entre dos puntos que se encuentran separados por otras redes y equipos. Esta tecnología permite la generación de diferentes topologías entre redes celulares y redes convencionales para la conexión de dispositivos móviles con elementos que van desde plataformas locales hasta servidores en la nube.

- Para realizar un adecuado diseño de soluciones M2T e IoT de extremo a extremo es necesario conocer todos los elementos que participan de la comunicación para así asegurar su funcionalidad y adecuada operación. Además de los elementos de red de core, se recomienda verificar el tipo

de SIM/UICC que se utiliza en el equipo móvil, ya que dependiendo del tipo de solución la integridad de la SIM/UICC se puede ver comprometida en condiciones de uso extremas.

- De acuerdo con el flujo propuesto para identificar el tipo de conectividad recomendada según unos requerimientos iniciales, excepto cuando se necesite una conexión hacia una IP publica o tenga una restricción a nivel de QoS sobre el tráfico, la opción más común será la VPN sobre internet. Esto puede resultar conveniente para las soluciones por su facilidad de implementación que tiene la VPN respecto a la tecnología MPLS y por la mayor cantidad de funcionalidades respecto a las conexiones por NAT.