Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISION

Alvaro Luis Godoy Ispache
Asesorado por el Ing. Julio César Solares Peñate

Guatemala, julio de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISION

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ALVARO LUIS GODOY ISPACHE
ASESORADO POR EL ING. JULIO CÉSAR SOLARES PEÑATE

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, JULIO DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Raúl Eduardo Ticún Córdova
VOCAL V	Br. Henry Fernando Duarte García
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE UN SISTEMA PARA DETECCION DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISION

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 12 de octubre de 2015.

Alvaro Luis Godoy Ispache

FACULTAD DE INGENIERIA
Escuelas de Ingeniería Civil, Ingeniería Mecánica Industrial, Ingeniería Química, Ingeniería Mecánica Eléctrica, Técnica y Regional de Post-grado de Ingeniería Sanitaria.
Ciudad Universitaria, zona 12
Guatemala, Centroamérica

Guatemala, 9 de noviembre de 2015

Ing. Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Ingeniero Guzmán:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISION"**, desarrollado por el estudiante **Alvaro Luis Godoy Ispache** , ya que considero que cumple con los requisitos establecidos.

Por lo tanto, el autor de este trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Asesor

JULIO CESAR SOLARES P.
INGENIERO MECANICO ELECTRICISTA
COLEGIADO No. 2330

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 15 . 2016.
Guatemala, 18 de NOVIEMBRE 2015.

Señor Director
Ing. Francisco Javier González López
Director Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISIÓN, del estudiante Alvaro Luis Godoy Ispache , que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

sro

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 15. 2016.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación del estudiante; ALVARO LUIS GODOY ISPACHE Titulado: PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ASICIÓN, procede a la autorización del mismo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Francisco Javier González López

GUATEMALA, 9 DE MARZO 2016.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.314-2016

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica al trabajo de graduación titulado: **PROPUESTA DE UN SISTEMA PARA DETECCIÓN DE DESCONEXIONES DE CUENTAS SMPP POR MEDIO DE CONSOLA PARA UN SMSC MARCA ACISION,** presentado por el estudiante universitario: **Alvaro Luis Godoy Ispache,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, julio de 2016

/cc

ACTO QUE DEDICO A:

Dios	El centro de mi fe y fuente de fortaleza.
Mis padres	Prudencio Godoy y Candelaria Ispache, por compartir mis sueños, por brindarme su apoyo en todo momento para alcanzar este triunfo, mi más sincero agradecimiento.
Mi hermanos	Danilo y Henry Godoy, por el apoyo y cariño brindado.
Mis tíos	Por su cariño, en especial a Juana Ispache, por su apoyo incondicional.
Mi familia	Por su cariño y consejos.
Mis amigos	Por la compañía, apoyo y amistad incondicional brindado durante mi desarrollo académico.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por permitirme alcanzar esta meta.
Facultad de Ingeniería	Por el conocimiento brindado.
Ing. Julio Solares	Por su amable ayuda durante el desarrollo del presente trabajo de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Bps	Bit por segundo
B	*Byte*
cos	Coseno
δ	Delta
f	Frecuencia
G	Giga
Hz	Hertz
K	Kilo
±	Más o menos
M	Mega

GLOSARIO

7 bit	Codificación estándar para el envío de mensajes de texto.
BG	*Border gateway*.
BSC	*Base station controller*.
BSS	*Base station subsystem*.
BTS	*Base transceiver station*.
CC	*Country code*.
Codificador	Es un circuito combinacional que representa una señal de entrada como un código binario.
Decodificador	Es un circuito combinacional que convierte un código binario de entrada en una señal.
GSM	*Global system for mobile communications*.
HLR	*Home local register*.
IMEI	*International mobile equipment identity*.

IMSI	*International mobile subscriber identity*.
MMS	*Multimedia Message Service.*
MSC	*Mobile services switching center.*
MT	*Mobile terminal*.
O&M	*Operation and maintenance*.
OSI	Interconexión de sistemas abiertos. Es un marco de referencia para la definición de arquitecturas en telecomunicaciones.
PC	*Point code*.
SGSN	*Serving GPRS support node*.
SIM	*Subscriber identity module.*
SMPP	*Short message peer to peer protocol.*
SMS	*Short Message Service.*
SMSC	*Short message service center.*

RESUMEN

Con la segunda generación de redes móviles denominada 2G, surgió un nuevo e innovador servicio de valor agregado, el cual recibió el nombre de mensaje de texto corto (SMS, por sus siglas en inglés). La mensajería SMS tuvo un auge importante; por esta razón se mantiene vigente en la actualidad.

Basadas en una red de telecomunicaciones 3G bajo el protocolo UMTS, se tiene una arquitectura bastante sencilla y ordenada, esto se logra mediante la jerarquía de equipos. Los equipos más importantes son la MSC que se encarga del registro de equipo y de solicitar información del mismo; el HLR que se encarga de almacenar información importante sobre los equipos registrados a una red; el SGSN y GGSN que se encarga de proporcionar al usuario los requisitos necesarios para que pueda navegar sin problemas.

Dentro de la arquitectura se encuentra un equipo llamado centro de mensajería corta (SMSC, *Short Messages Center*), el cual se encarga del correcto funcionamiento del servicio de mensajería SMS. Entre las funciones principales de un SMSC se encuentra aceptar, mantener y finalizar la conexión de un cliente SMPP, enrutar los mensajes MO y MT hacia su destino final, monitoreo manual de cuentas SMPP y configuración de parámetros de reintentos y eliminaciones.

Debido a que un SMSC marca Acision no puede realizar una búsqueda automática de cuentas SMPP desconectadas, se plantea un sistema de detección automática de cuentas SMPP, el cual basa su funcionamiento en *Shell Scripting*, los cuales son códigos de programación basados en

distribuciones Linux. Con estos scripts se logra ejecutar una rutina de verificación del estado de las cuentas, cada cierto periodo de tiempo; en caso de que detecte alguna cuenta desconectada, se procederá a la ejecución de un segundo *script*, el cual es el encargado de enviar una notificación vía *email* a un grupo de usuarios. Con esto se logran mitigar las pérdidas generadas por desconexiones masivas de clientes SMPP o por desconexiónes, que duren más de 45 minutos.

OBJETIVOS

General

Desarrollar una propuesta de un sistema para detección de desconexiones de cuentas SMPP por medio de consola para un SMSC marca Acision.

Específicos

1. Presentar la historia y características de la mensajería SMS.

2. Presentar los fundamentos y estructura de un Core 3G.

3. Describir los fundamentos y características del protocolo SMPP.

4. Desarrollar la propuesta del sistema automático para la detección de cuentas SMPP desconectadas.

5. Realizar un análisis técnico y económico del sistema propuesto.

INTRODUCCIÓN

En el primer capítulo se analiza la historia de las telecomunicaciones, desde la aparición de los primeros teléfonos móviles hasta la última generación de telecomunicaciones denominada LTE. Adicionalmente, se presentará el origen, evolución, características y modelos relacionados con el servicio de mensajería corta.

En el segundo capítulo se presentan los fundamentos, protocolo, características y arquitectura de una red de telecomunicaciones 3G. En cuanto, al análisis de la arquitectura de red, este se basa en el protocolo 3G denominado UMTS; se presentan temas importantes como los elementos e interfaces necesarios para que un equipo logre registrarse en la red y posteriormente hacer uso de los servicios de voz y navegación disponibles en la red local.

En el tercer capítulo se presenta el protocolo utilizado para el servicio de mensajería de texto SMS; este protocolo es llamado SMMP. Se estudiará la historia, evolución, fundamentos y características del protocolo SMPP; adicional, se incluye el flujo necesario para realizar una conexión entre un cliente y el centro de mensajes de texto SMSC; en este apartado se podrán observar los comandos necesarios para realizar el establecimiento de una sesión y posteriormente el envío de los mensajes.

En el cuarto capítulo se presentan las herramientas y códigos necesarios para el correcto funcionamiento del sistema automático para la detección de cuentas SMPP. Entre las herramientas a utilizar se encuentran los Linux Script.

Se desarrollará el código de programación necesario para la ejecución de las rutinas automáticas de búsqueda de cuentas desconectadas.

En el quinto capítulo se estudia a nivel económico la factibilidad de la implementación del sistema de monitoreo automático para la detección de cuentas SMPP. Este capítulo incluye un comparación estadística entre la inversión necesaria para la implementación y las pérdidas generadas por desconexión no monitoreadas.

1. HISTORIA Y CARACTERÍSTICAS DE LA MENSAJERÍA SMS

1.1. Inventos relacionados

Antes de la invención del mensaje SMS, existió un servicio de similares características, el cual es llamada *beeper*. El *beeper* fue anterior al desarrollo de la tecnología de telefonía móvil, este hizo su aparición en la década de los 70's y fue un servicio bastante popular hasta mediados de los 90.

El *beeper* fue inventado por la compañía Multitone Electronics en 1956. Su función principal fue alertar a los doctores, del Hospital de St. Thomas de Londres, sobre servicios de urgencia.

Hasta 1974 el *beeper,* era un dispositivo reservado únicamente para servicios médicos, luego la compañía Motorola introdujo al mercado su *PageBoy*, el cual contaba con la capacidad de almacenar textos; con esto se inició la venta masiva al público en general. Para 1980, el servicio ya contaba con 3,2 millones de usuarios solo en Estados Unidos; esta cantidad fue creciendo, ya que para 1992 se contabilizaban 22 millones de usuarios.

El *beeper,* generalmente, es un dispositivo muy sencillo que se compone de una pantalla de cristal líquido, un dispositivo vibrador y/o sonoro y botones de control. Los *beepers* utilizan señales de radio para enlazarse con un centro de control de llamadas y este a su vez realiza la conexión con el destinatario. Esto presentaba una gran ventaja sobre la naciente telefonía celular, sobre todo a la hora de enviar mensajes a zonas sin cobertura, ya sea a causa de

interferencias, por interferencias geográficas o por hallarse en el interior de edificios. Otra de las ventajas sobre la telefonía celular era el bajo costo de adquisición de un *beeper* comparado contra un teléfono celular.

Debido al auge en este servicio, la FCC se vio obligada a aprobar dos bandas de frecuencias designadas para la operación de los *beepers*, dichas bandas fueron 152,0075 y 157,450 MHz.

Desde 1998 el uso de este servicio ha estado decayendo paulatinamente, hasta ser casi nulo en la actualidad, esto debido a las mejoras, técnicas y económicas, que constantemente presenta la telefonía celular.

1.2. Historia de las telecomunicaciones

El ser humano, debido a su necesidad de comunicación con otras personas, ha ido desarrollando una serie de inventos los cuales permiten dicha interacción. Esto llevó al desarrollo de la telefonía móvil en la década de los 80’s; desde esa fecha se han ido desarrollando diferentes tecnologías, las cuales se verán más a detalle en el presente capitulo.

1.2.1. G

En los inicios de la década de 1980, hicieron su aparición los primeros sistemas de comunicaciones celulares móviles. Durante esta década cada país desarrollaba su propio sistema de telecomunicación, así como un teléfono móvil de uso exclusivo para su sistema. Esto ocasionaba que las diferentes tecnologías no fueran compatibles entre sí.

Debido a este problema, en 1982 se formó una asociación de países europeos que tenían a su cargo la tarea de desarrollar una tecnología celular que conllevara un servicio común de telefonía móvil europea. La idea principal de esta asociación era que el nuevo estándar debía utilizar la tecnología digital en lugar de la analógica. El grupo tenía que elegir entre los sistemas de banda ancha y banda estrecha, así como los modelos de transmisión o división de las frecuencias.

La asociación se vio obligada a efectuar una seria de pruebas para poder elegir su banda estándar; posteriormente se eligió la banda estrecha y el modelo TDMA (*Time división múltiple access*) para la transmisión del protocolo estándar.

De los estándares 1G desarrollados durante esta época se pueden mencionar los siguientes:

- NMT (*Nordic Mobile Telephone*), el cual fue utilizado en los países Nórdicos, Holanda, Europa del Este y Rusia.
- AMPS empleado en los Estados Unidos.
- TACS (*Total Access Communications System*) utilizado en el Reino Unido.
- C-450 utilizado en Alemania Oriental, Portugal y África.
- Radiocom 2000 utilizado en Francia.
- RTMI utilizado en Italia.
- TZ-801, TZ-802 y TZ-803, utilizados en Japón.

1.2.2. 2G

La generación 2G se caracteriza por dar inicio a la transmisión digital. Durante la época 2G se desarrollaron o evolucionaron varios estándares provenientes de la 1G; de todos estos el estándar que mayor importancia ha tenido es el GMS (*Global System for Mobile Communications*). El GSM es un estándar desarrollado por el Instituto Europeo de Normas de Telecomunicaciones (ETSI), en el cual se describen los protocolos de las redes celulares para dispositivos móviles. Básicamente, el sistema GSM está integrado por:

- GSM-900. Este sistema es la red celular original y trabaja bajo una frecuencia de 900 MHz. Está diseñado para funcionar en áreas extensas, por esta razón se requiere de una mayor potencia a la hora de transmitir.
- GSM-1800. Opera bajo la frecuencia de 1800 MHz, fue diseñado para operar en Europa.
- GSM-1900. Opera bajo la frecuencia de 1900 MHz, fue diseñado para operar en América.
- Sistema EGSM. Es una versión mejorada del GSM-900, en el cual se extendió la banda de frecuencia de operación. Este nuevo sistema requiere una potencia de transmisión menor, ya que se redujo su área de cobertura.

Para esta generación era de vital importancia que todos los teléfonos móviles fueran creados bajo los mismos principios de operación; esto se logró gracias a la estandarización del sistema GSM.

Con GSM se incluyó una forma estándar de identificación, conocida como *SIM card;* desde esta fecha y hasta la actualidad, todos los teléfonos son

compatibles con una SIM. Con la tarjeta SIM se eliminó la dependencia de una identidad única y exclusiva para cada teléfono móvil. La tarjeta SIM contiene un número único y puede ser utilizado en cualquier móvil GSM sin la necesidad de contactar a su compañía para poder activar el móvil. A cada tarjeta SIM el usuario le asigna un código de cuatro caracteres por motivos de seguridad; con esto se garantiza que nadie pueda acceder a la información personal del cliente, en caso de robo o extravío de teléfono móvil.

El sistema GSM representó una mejora significativa para las empresas de telefonía móvil, ya que les permite contar con la opción de una tecnología más avanzada a un menor costo de operación; esto sumado al bajo costo de infraestructura, la facilidad de instalación, el alto grado de flexibilidad y eficiencia en cuanto al espectro se refiere, convirtieron al sistema GSM en el estándar más exitoso de la generación 2G.

1.2.2.1. Servicios GSM

Básicamente, el sistema GSM, fue diseñado para prestar servicio de voz, pero al ver el auge que tuvo, se incluyeron nuevas características. Inicialmente, entre los servicios de voz que el GSM ofrecía, se encuentran:

- Identificador de llamadas entrantes
- Opciones para el control de llamadas entrantes
- Buzón de voz
- Transferencia de llamadas entrantes a un número fijo
- Transferencia de llamadas entrantes a un número móvil
- Restricción de llamadas entrantes
- Restricción de llamadas salientes
- Llamada en espera

- *Push to talk*

El sistema GSM también incluyó servicios digitales, que no tenían relación con servicio de voz, dichos servicios fueron:

- Mensajes de texto SMS (*Short Message Service*). De todos los servicios adicionales que ofrecía GSM, el servicio de mensajes de texto fue el que mayor importancia tuvo.
- Mensajes multimedia MMS (*Media Message Service*). Este servicio era similar al de SMS, con la diferencia que un MMS podía incluir un archivo multimedia (audio, imagen, contacto, entre otros).
- Video llamada.
- Mensajería instantánea en tiempo real IM.
- Navegación en internet.
- Servicio de correo electrónico.
- Visualización de programas de TV mediante la opción de TV y video.
- Reproductor digital de música.
- Servicio de ubicación de usuario.
- Juegos en red.

1.2.2.2. Arquitectura sistema GSM

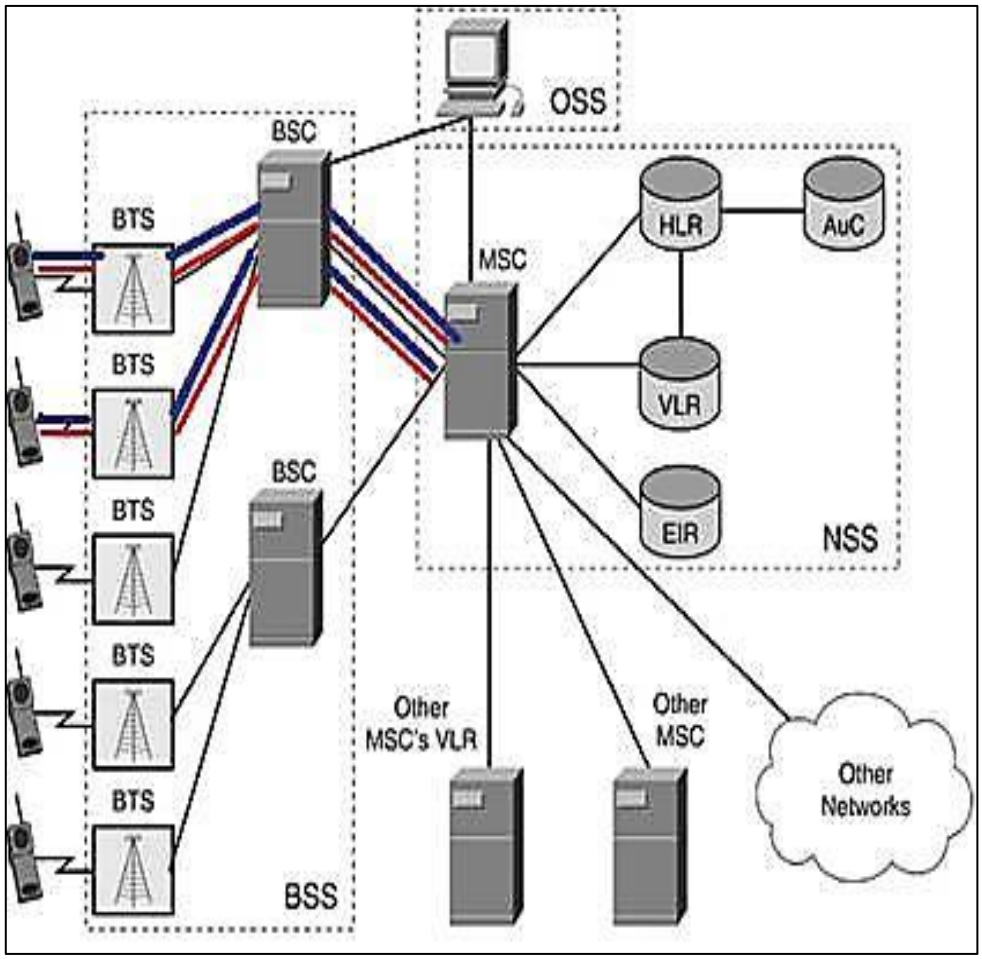
El sistema GMS fue diseñado siguiendo una arquitectura de 4 bloques esenciales. Dichos bloques se pueden ordenar con base en el proceso de establecimiento de llamada de la siguiente manera:

- Estación móvil
- Estación base
- Sistema de conmutación de red

- Centro de administración de red

En la figura 1 se puede observar más a detalla la arquitectura de una red GSM.

Figura 1. **Arquitectura red GSM**



Fuente: *Pucp.com*. http://blog.pucp.edu.pe/blog/wp-content/uploads/sites/100/2009/12/Red-GSM.jpg. Consulta: enero de 2016.

La estación móvil es el único bloque GSM, que se pone en contacto directo con el usuario; esto debido a que la estación móvil le permite al usuario utilizar de la red.

En el bloque de estación móvil está incluido el equipo móvil (teléfono móvil), la tarjeta SIM. Por equipo móvil se entiende el equipo físico de comunicación, este se identifica dentro de la red con un número IMEI (*International Mobile Equipment Identity*), el cual consiste en 15 dígitos, ordenados de la siguiente manera:

- TAC
- FAC
- SNR
- SP

El TAC (*type approval code*) es un código que consiste en 6 dígitos; es asignado por la red GSM.

EL FAC (*final assembly code*) permite a la red identificar al fabricante del teléfono móvil. Este tiene 2 dígitos.

El SNR (*serial number)* permite a la red identificar al teléfono móvil. El SNR consta de 6 dígitos.

El SP (*suplementary number*) consta únicamente de un dígito, el cual es utilizado como una reserva, en caso de duplicidad.

Por medio de la tarjeta SIM el usuario obtiene acceso a todos los servicios que la red local ofrece. Esto se logra mediante la asignación de 2 identificadores:

- IMSI (*International Mobile Subscriber Identity*). El número IMSI es único para cada tarjeta SIM y la identifica dentro de red.
- MSISDN (*Mobile Subscriber ISDN Number*). Este es el número telefónico, utilizado al llamar a un usuario y el que utiliza la red para enrutar las llamadas.

El código IMSI contiene códigos que permiten identificar el país donde se encuentra el teléfono, la red local y la estación móvil. El orden de los códigos es el siguiente:

- *Mobile country* code, MCC: es un código de 2 o 3 dígitos que se utiliza para identificar al país de servicio.
- *Mobile network code*, MNC: es un código de 2 dígitos que permite identificar a la red de telefonía local.
- *Mobile station identification number* es un código de 13 dígitos que se utiliza como identificador de la estación móvil (teléfono móvil).

El subsistema de estación base (BSS, *base station subsystem*) es el encargado de controlar el tráfico y señalización de la interfaz de aire; BSS es el primer elemento de la red con la que entra en contacto la estación móvil y el que permite la comunicación con el NSS. Gestiona el ancho de banda, el control de llamada, traspaso entre celdas, así como la potencia de la portadora de cada usuario:

Las BSS deben ser controladas y monitoreadas todo el tiempo, por lo cual deben contar con comunicación con un OSS. Una BSS está compuesta por los siguientes dos elementos:

- Base *transceiver station*, BTS: esta consta de una instalación fija de radio para la comunicación bidireccional (*full duplex*). Las BTS trabajan con frecuencias de 900 a 1 900 MHz y son las que realizan el enlace con el usuario que efectúa o recibe la llamada. Las estaciones en general están ubicadas en lugares altos para dar una mejor área de cobertura y son tipo dipolo. Contienen el transmisor-receptor de radio, antenas, guías de onda y el equipo de procesamiento de señales. Son las encargadas de mantener la comunicación con la estación móvil y con la BSC; realizan procesos para garantizar la conexión libre de errores entre la estación móvil y la BSC.

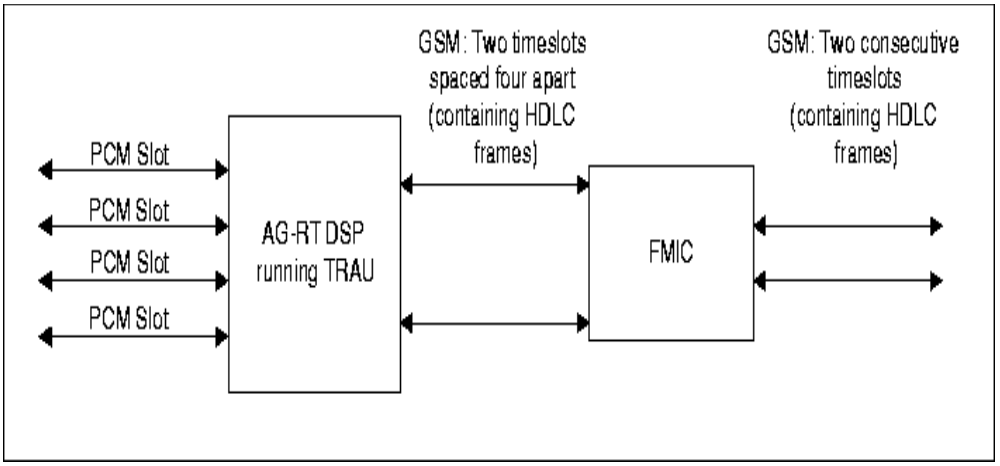
- *Base Station Controller*, BSC: se encarga de la comunicación y monitoreo de una o varias BTS, permitiendo la conexión entre la estación móvil y el subsistema NSS. Entre sus funciones se encuentran gestionar y asignar el canal de radio para establecer una llamada, recolectar información estadística, gestionar el cambio de celda (*handover*), mantener la llamada y controlar la potencia de transmisión-recepción. También mantiene un control sobre el estado del funcionamiento de las estaciones base que administra, informando sobre posibles anomalías que presenten.

La unidad de transcodificación (TRAU) es el elemento encargado de la codificación de la conversación, es decir, que la convierte a formatos de códigos digitales y viceversa, para maximizar los recursos de radio. Este elemento es funcionalmente parte del BSS, pero puede estar situado físicamente en la BTS,

en el BSC o externo al subsistema; estas configuraciones se dan dependiendo del costo de transmisión y las facilidades del operador de telefonía para crear máxima flexibilidad sobre la estructura física y operacional del sistema. El TRAU toma una transmisión con velocidad de 13 Kbps para voz y datos (de 300, 600, 1 200 bps) multiplexados cuatro de ellos y puestos en un canal estándar PCM de 64 Kbps.

La tasa de salida TRAU de un canal digital tiene una capacidad estándar de 64 kbps. Posterior a esto, los 30 canales de 64 kbps son multiplexados a 2 048 Mbps. Un E1 puede llevar hasta 120 señales de tráfico y control. Las locaciones de transferencia entre la BTS y el BSC son subcanales de 16 kbps usados ente la BTS y TRAU, y canales de 64 kbps entre TRAU y BSC. Alternativamente el TRAU puede localizarse entre el BSC y el MSC, utilizando en este caso 16-kbps de la BTS a la BSC y 16 kbps entre BSC y TRAU, como se observa en la figura 2.

Figura 2. **Arquitectura TRAU**



Fuente: Mns Communications. http://www.nmscommunications.com/manuals/6378-11/chap34.htm. Consulta: enero de 2016.

El elemento principal dentro del core GSM es el centro de conmutación móvil (MSC, *mobile switching center*); la MSC se encarga de controlar todos los otros elementos del subsistema de conmutación de red. La MSC basa su funcionamiento en protocolos y se comunica con los otros elementos de la red utilizando protocolos abiertos de la industria tales como:

- M2UA
- M3UA
- Protocolo de control de entradas multimedia
- Protocolo de inicio de sesión

La MSC está asociada con funciones de conmutación como el establecimiento de llamada, la liberación y el enrutamiento. Sin embargo, también lleva a cabo una serie de funciones adicionales, incluyendo enrutamiento de mensajes SMS, llamadas en conferencia, fax y servicio de facturación, así como la interconexión con otras redes como la red telefónica pública conmutada (PSTN). Adicionalmente, se incorporan estándares de la industria que están definidos por entidades como el ETSI, ITU, GSM, 3GPP y 3GPP2 y otros organismos de normalización.

Para los traspasos de celdas, denominados *handovers,* la MSC juega un papel significativo, particularmente en los que implican varias BSC, conocidos como *handover* inter BSC, así como aquellos que implican varias MSC, conocidos como transferencias entre MSC. En el caso de un *handover* inter BSC, al detectar que el dispositivo móvil se aproxima al borde de su célula, la MSC realiza un proceso de escaneo de una lista de células adyacentes y sus correspondientes BSCs y con esto facilita el traspaso del dispositivo móvil a la BSC apropiada.

Para la MSC es importante determinar la ubicación geográfica de cada MS, debido a que las estaciones móviles se encuentran en constante movimiento, esto para facilitar el enrutamiento de las posibles llamadas que se tengan entre ellos. Para esta tarea, la MSC se comunica con la base de datos de registro de posición.

El registro de ubicación local (HLR, *home location registrer*) es una base de datos que contiene información sobre todos los abonados móviles de un operador en específico.

Dependiendo de la cantidad de usuarios totales que presente una red de telefonía se puede tener más de un HLR funcionando en simultáneo, sin que esto afecte el rendimiento de la red. En el HLR se agregan dos identificadores del abonado que son la IMSI y el MSISDN.

En el HLR se almacenan 2 tipos de información: la información sobre el suscriptor y su ubicación, con la finalidad de habilitar los cargos y enrutamiento de llamadas hacia la MSC donde el MS está localizado. La información que el HLR almacena sobre el abonando incluye los siguientes datos:

- Identificador Internacional del abonado móvil.
- Servicios restringidos.
- Servicios de subscripción de información al portador.
- Información de la ubicación geográfica, número de estación móvil viajero, VLR, MSC.
- Servicios suplementarios.

El registro de ubicación visitante (VLR, *visitor location register*) es una base de datos que contiene información sobre usuarios temporales dentro de la red. Un VLR puede prestar servicio o comunicarse con varias MSC.

Una estación móvil visitante es controlada por el VLR asociado a la MSC en la cual se encuentre registrado; si la MS ingresa a una nueva área, automáticamente se inicia un proceso de registro; la MSC que administra esa área realiza el registro y envía una actualización de posición al VLR, y este a su vez envía una actualización de datos al HLR. Los datos temporales que se almacenan en el VLR son:

- IMSI
- MSISDN
- LAI
- TMSI
- MSRN

Para realizar el proceso de autenticación es necesario el almacenaje de una clave de identificación Ki para cada abonado registrado a nivel de HLR; esta función la realiza el bloque de autenticación por medio del centro de autenticación (AuC, *authentication center*).

La clave Ki es utilizada para generar los datos que son utilizados para la autenticación de la IMSI y para generar otra llave, la cual se utiliza para cifrar toda la comunicación existente entre la estación móvil y la red del operador. La clave de identificación Ki es quemada en cada tarjeta SIM durante su fabricación y esta es replicada en el AuC para su almacenaje. Esta clave no es transmitida pon ningún medio entre la SIM y el AuC, pero se combina con la IMSI con fines de generar la clave de cifrado.

Estos procesos de autenticación de usuario permiten evitar los robos o fraudes derivados de la clonación de tarjetas SIM. Si la autenticación del usuario no es exitosa, el abonado no podrá acceder a ningún servicio dentro de la red.

El registro de identidad de equipos (EIR, *equipment identity register*) está conformado principalmente por una base de datos, en la cual se almacenan los IMEI de las estaciones móviles. La función principal del EIR es controlar el acceso a la red mediante listas de acceso. Las posibles listas son blanca, gris y negra. Cuando un usuario se encuentra en lista blanca tiene permitido establecer conexión a la red. En la lista gris se permite la conexión a la red, pero los abonados que estén dentro de ella, estarán siendo monitoreados. En la lista negra se encuentran las terminales que han sido reportadas como perdidas, robadas o bien la marca de la terminal no está permitida dentro de la red, por lo cual se bloquea la conexión a la red.

Posterior al EIR se encuentra el subsistema de soporte y operación (OSS, *operation and support subsystem)*, el cual provee funciones determinadas para la gestión de red centralizada (NMC), y el centro de monitoreo y mantenimiento (OMC) de la PLMN. El OSS tiene como función fundamental el control y monitoreo de la red. Permite las funciones de gestión, monitoreo y asignación de parámetros de configuración, y estudio de las estadísticas y comportamiento de la PLMN a través de herramientas especializadas.

El subsistema de operación y soporte está conformado por los 3 bloques:

- Centro de administración de red (*NMC, network management center*).
- Centro de administración y supervisión (*SMC, supervision management center*).

- Centro de operación y mantenimiento (OMC, *operation and maintenance center*).

Todos los diferentes equipos que conforman una red GSM necesitan comunicarse entre sí, para esto se emplean interfaces, las cuales tiene un protocolo común para la comunicación de diferentes equipos. Las interfaces utilizadas para la comunicación son interfaz A, Abis, B, C, D, E, F, G y H.

La interfaz A es utilizada para transportar la información sobre las BSS, el manejo de llamas y la movilidad; esta interfaz se encuentra situada entre la MSC y la BSC. Por medio de la interfaz A se distribuyen los circuitos que serán utilizados entre el BSS y el MSC. Su protocolo de señalización es el SS7.

La interfaz Abis se encuentra situada entre la BSC y las BTSs. Por medio de esta interfaz se realiza el control del equipo de radiofrecuencia. Sobre la interfaz de radio en una BTS, la velocidad de la transmisión de voz es de 13 Kbps; sin embargo la velocidad para un canal de enlace es de 64 Kbps; para compensar esta diferencia se puede elegir entre multiplexar 4 canales de voz en un PCM o transcodificar los canales de voz a una velocidad de 64 kbps.

La interfaz B, se encuentra ubicada entre la MSC, VLR y demás asociados, se encarga exclusivamente de la comunicación entre la MSC y el VLR.

La interfaz C se ubica entre los HLRs y se encarga de la comunicación entre la MSC y los diferentes HLRs. Para este intercambio de información se utiliza el protocolo MAP.

La interfaz D se encarga de la comunicación entre el HLR y el VLR. Para la transferencia de información utiliza el protocolo MAP.

La interfaz E se ubica entre 2 MSCs y es la encargada de la comunicación entre MSC's. Para esta comunicación utiliza los protocolos MAP/E, RDSI e ISUP.

La interfaz F se encarga de la comunicación entre la MSC y el EIR. Esta interfaz no maneja tráfico de usuario.

La interfaz G se encarga de la comunicación entre VLRs. Para esta comunicación se utiliza el protocolo MAP/G.

La interfaz H se encarga de la comunicación entre el HLR y el AuC.

La interfaz I permite el intercambio de datos entre el MSC y el MS, a través del BSS.

La interfaz Um se ubica entre la estación móvil y la BSS; esta tiene una tasa de transmisión de 13 Kbps para voz y 9,6 Kbps para datos. Para la transferencia utiliza el protocolo de comunicación LAPDm.

La interfaz X.25 se ubica entre la BSC y el centro de control y mantenimiento OMC, y su función es la transmisión de información entre estos 2 equipos.

Para lograr todo el proceso de enganche a la red local es necesario que la tarjeta SIM contenga la siguiente información:

- Estado actual de la tarjeta SIM, es decir, si está bloqueada o desbloqueada.
- Número de serie de la tarjeta SIM.
- Algoritmo de autentificación.
- Clave del algoritmo de autentificación.
- Identificador internacional.
- Identificador temporal.
- Algoritmo de generación de claves de cifrado
- Clave de control de acceso del usuario.

1.2.3. Bandas de frecuencia GSM

El sistema GSM, para la administración y uso eficaz de las frecuencias asignadas, utiliza un método híbrido, el cual es una combinación entre el sistema de acceso múltiple por división de frecuencia (FDMA por sus siglas en inglés) y el sistema de acceso múltiple por división de tiempo (TDMA, por sus siglas en inglés). El sistema hace una división del ancho de banda de 25 MHz entre las 124 posibles frecuencias. De las 124 frecuencias, una es asignada a cada BTS y posteriormente es dividida en 8 espacios de tiempo utilizando TDMA. Además el sistema GSM utiliza el método denominado salto de frecuencia, para minimizar la interferencia de las fuentes externas y, por lo tanto, hacer que los escuchas no autorizados sean virtualmente imposibles.

En la tabla I se muestran las diferentes bandas de frecuencia asignadas a GSM, así como sus principales características.

Tabla I. **Bandas de frecuencias asignadas a GSM**

Estándar	Banda	Frecuencia		**Asignación de canal**
		Subida (MHz)	**Bajada (MHz)**	
T-GSM-380	380	380,2–389,8	390,2–399,8	Dinámica
T-GSM-410	410	410,2–419,8	420,2–429,8	Dinámica
GSM-450	450	450,4–457,6	460,4–467,6	259–293
GSM-480	480	478,8–486,0	488,8–496,0	306–340
GSM-710	710	698,0–716,0	728,0–746,0	Dinámica
GSM-750	750	747,0–762,0	777,0–792,0	438–511
T-GSM-810	810	806,0–821,0	851,0–866,0	Dinámica
GSM-850	850	824,0–849,0	869,0–894,0	128–251
GSM-900	900	890,2–914,8	935,2–959,8	1–124
E-GSM-900	900	880,0–914,8	925,0–959,8	975–1023, 0-124
R-GSM-900	900	876,0–914,8	921,0–959,8	955–1023, 0-124
T-GSM-900	900	870,4–876,0	915,4–921,0	Dinámica
DCS-1800	1 800	1 710,2–1 784,8	1 805,2–1 879,8	512–885
PCS-900	1 900	1 850,0–1 910,0	1 930,0–1 990,0	512–810

Fuente: elaboración propia.

En Europa, África, Medio Oriente y Asia, las bandas GSM más utilizadas son las GSM 900 y 1800. Estas proveen 124 canales espaciados entre ellos por 200 KHz, utilizando un espaciado dúplex. En cada extremo del rango de frecuencias se encuentran las bandas de guardia que tienen un ancho de banda de 100 KHz. La banda GSM 900 evolucionó a la banda 900 extendida, E-GSM-900; con esta se consigue aumentar los canales disponibles a 174. En la actualidad, la mayoría de dispositivos móviles son compatibles tanto a GSM-900 como a E-GSM-900.

La banda GSM 1800 proporciona un total de 374 canales de frecuencia, utilizando un espaciado dúplex de 95 MHz. Para América, las bandas más utilizadas son las GSM 850 y GSM 1900.

1.2.4. 3G

La tercera generación de comunicaciones móviles, mejor conocida como 3G, está conformada por un conjunto de estándares y protocolos diseñados con el objetivo de crear redes de telecomunicaciones nuevas, las cuales pueden soportar una mayor capacidad de canal para la transmisión de datos. Con el desarrollo de 3G se dio inicio a la era de banda ancha en los sistemas de telecomunicaciones.

A principio de la década de los 80, la Unión Internacional de Telecomunicaciones (ITU) comenzó a definir los lineamientos de lo que hoy se conoce como sistemas de comunicaciones móviles de 3G, denominados por aquel entonces como *Future Public Land Mobile Telecommunications Systems* (FPLMTS) y posteriormente *International Mobile Telecommunications-2000* (IMT-2000). Desde ese entonces la ITU inició el proceso necesario para avanzar hacia la era 3G, una de las medidas tomadas fue la de reservar las bandas frecuencias a nivel internacional que serían empleadas por todos los sistemas 3G.

Los principales objetivos de la familia de protocolos IMT-2000 fueron:

- Mayor capacidad del canal
- Mayor eficiencia de canal
- Mayor flexibilidad de estándares y bandas de frecuencia
- Compatibilidad con estándares anteriores

- Ancho de banda ajustable
- Itinerancia entre redes
- Mayor velocidad de acceso
- Integración de más y mejores servicios de voz y multimedia

En 1998 la ITU comenzó con la colecta de propuestas de estándares que cumplieran con estos objetivos. La ITU recibió 15 propuestas, elaboradas por diferentes grupos y asociaciones con el fin de convertirse en estándares 3G. Durante este proceso de evaluación y selección se unieron numerosas iniciativas para ofrecer candidaturas de mayor solidez, hasta que en mayo del 2000 se configuró finalmente la lista de estándares aceptados por la ITU. Cada estándar debía cumplir con los siguientes requisitos:

- Transmisión de datos de forma simétrica y asimétrica.
- Alta velocidad en la transmisión de datos, hasta 384 Kbps.
- Alta calidad en servicios de voz. Mejor o igual que la ofrecida por los servicios alámbricos convencionales.
- Capacidad de adaptarse a estructuras de conmutación de datos o en modo circuito.
- Mayor capacidad de canal.
- Mejor eficiencia para el uso del canal.
- Posibilidad de ofrecer varios servicios de manera simultánea.
- Compatibilidad con sistemas 2G.
- Servicio unificado de mensajes.
- Aplicaciones de audio y video en tiempo real.
- Aplicaciones de comercio electrónico.
- Compatibilidad de frecuencias para poder realizar el denominado *roaming*.

En cuanto a temas de seguridad se refiere, las redes de los sistemas 3G ofrecen mayor grado de seguridad comparadas con las redes de los sistemas 2G. Esto es logrado por el hecho que la UE puede autenticar la red a la que se está conectando, por lo tanto, el usuario puede asegurarse de que dicha red es la intencionada y no una imitación. En la conferencia Black Hat 2010 se demostró que se podían obtener números telefónicos e inclusive escuchar las llamadas de teléfonos GSM cercanos, esto era logrado haciéndose pasar por una BTS.

Las redes 3G utilizan un cifrado de bloques denominado Kasumi en vez del anterior cifrador de flujo A5/1; con esto se logró evitar el escenario antes descrito, pero aún así se han identificado algunas debilidades en el código Kasumi. Además de la infraestructura de seguridad de las redes 3G, se ofrece seguridad de un extremo al otro cuando se accede a aplicaciones *framework* como IMS, aunque esto no es algo que solo se haga en el 3G.

El espectro asignado a los sistemas 3G, finalmente queda de la siguiente manera:

- 806-960 MHz asignado durante la WRC 2000
- 1710-1885 MHz asignado durante la WRC 2000
- 1885-1980 MHz asignado durante la WRC 92
- 2010-2025 MHz asignado durante la WRC 92
- 2110-2200 MHz asignado durante la WRC 92
- 2500-2690 MHz asignado durante la WRC 2000

Luego de revisar los aspectos de seguridad, requisitos mínimos y servicios ofrecidos, se llegó al acuerdo de la estandarización del sistema UMTS, el cual constituye la versión europea de 3G como parte de la familia de estándares

IMT-2000. UMTS es la evolución lógica de la comunidad GSM, por lo que es el sistema que cuenta con mayor aceptación a nivel mundial. En Guatemala el sistema UMTS fue el introducido para los sistemas móviles de tercera generación.

1.2.5. 4G

Durante años los estándares 3G fueron suficientes en cuanto a las exigencias del consumidor y de avances tecnológicos, pero con el paso del tiempo, las velocidades de transmisión de datos fueron quedando pequeñas ante el paso agigantado de las aplicaciones que usan la transmisión de datos.

Para definir las especificaciones de 4G, la Unión Internacional de Telecomunicaciones creó un comité encargado de dicha tarea. A este comité se le dominó IMT-Advanced y en él se definen los requisitos mínimos y necesarios para que un estándar sea considerado de la generación 4G.

Para que un estándar sea considerado de 4G, deben cumplir una serie de requisitos de servicios de voz y de datos. El requisito principal para 4G es que las velocidades máximas de transmisión de datos deben estar entre 100 Mbps para una movilidad alta y 1 Gbps para movilidad baja.

La tecnología 4G está basada en el protocolo IP, siendo un sistema y una red, que se alcanza gracias a la convergencia entre las redes alámbricas e inalámbricas. Cuando se realizó la proyección de 4G se planteó el objetivo que sus estándares pudieran ser utilizados por módems inalámbricos, teléfonos inteligentes y otros dispositivos móviles. La diferencia principal con las generaciones predecesoras, radica en la capacidad de proveer velocidades de

acceso mayores de 100 Mbps en movimiento y 1 Gbps en reposo, manteniendo una calidad de servicio (QoS) de alta seguridad.

En la actualidad, el estándar principal de la cuarta generación de telecomunicaciones es el denominado LTE.

1.2.5.1. LTE

La tecnología Evolución a largo plazo (LTE, *Long term evolution*) es un estándar tecnológico para datos de banda ancha inalámbrica que está diseñado con el objetivo principal de dar soporte al constante acceso de teléfonos móviles y de dispositivos portátiles a internet.

El protocolo LTE hace referencia a un estándar de comunicación móvil, denominado “conectividad LTE”. Este estándar fue desarrollado por la organización 3GGP; dicha organización logró detectar que existía una gran necesidad de asegurar la competitividad del sistema 3G para el futuro; con esto se garantizaba complacer a los usuarios que demandaban más calidad y mayor rapidez de servicio. La diferencia fundamental entre los estándares de 2G, 3G y 4G, es que, 2G y 3G están basadas en técnicas de conmutación de circuitos (CS) para los servicios de voz, mientras que LTE utiliza la técnica de conmutación de paquetes IP (PS).

Las principales características del LTE son:

- Ancho de banda con la capacidad de adaptación para las frecuencias 1.4, 3, 5, 10, 15 y 20 MHz.
- Capacidad de trabajar en bastantes bandas con frecuencias diferentes cada una.

- Simpleza en su arquitectura.
- Alta eficiencia en el uso del espectro.
- Compatibilidad con otras tecnologías y estándares desarrollados por 3GPP.
- Separación de los planos de usuario y de control mediante la utilización de interfaces abiertas.
- Interoperabilidad con otros sistemas como CDMA2000.
- Red de frecuencia única OFDM.
- Velocidad pico de bajada de 326,5 Mbps para 4x4 antenas y 172,8 Mbps para 2x2 antenas.
- Velocidad pico de subida de 86,5 Mbps.
- Disminución de latencia. La latencia cuenta con valores promedio de 100 ms para el control-plane y 10 ms para el *user-plane*.
- Capacidad de funcionamiento con velocidades de desplazamiento de hasta 500 Km/H.
- A cada celda se pueden enganchar más de 200 usuarios.
- Flexibilidad en cuanto al uso del espectro.

La mejora en la utilización del espectro se debe a que LTE utiliza un método para el proceso de bajada y otro método diferente para el proceso de subida. Para bajada de datos utiliza el método de multiplexacion por división de frecuencias ortogonales (OFDM), el cual consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta diferente información, la cual es modulada en QAM o en PSK.

La multiplicación por división de frecuencias ortogonales se realiza después de pasar la señal por un codificador de canal, esto con el objetivo de corregir los errores producidos en la transmisión. Debido al problema técnico que supone la generación y detección en tiempo continuo de los cientos, o

incluso miles de portadoras equis espaciadas, los procesos de multiplexación y demultiplexación se realizan en tiempo discreto mediante la IDFT y la DFT, respectivamente. Una de las principales características de OFDM, es el enlace descendente robusto frente a las múltiples interferencias y de alta afinidad a las técnicas avanzadas como la programación de dominio de frecuencia del canal dependiente y MIMO.

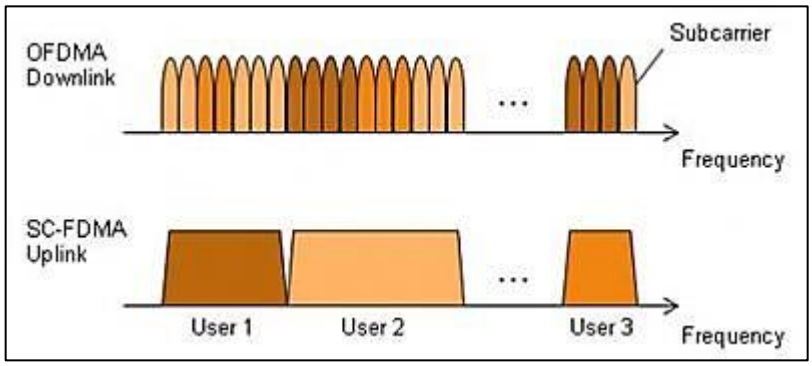
Para la ascendencia de datos, LTE utiliza el método de acceso múltiple por división de frecuencia (FDMA, por sus siglas en inglés). En el método FDMA, el acceso al medio se realiza dividiendo el espectro disponible en canales, los cuales corresponden a distintos rangos de frecuencia, asignando estos canales a los distintos usuarios y comunicaciones a realizar, sin interferirse entre sí. Este método convierte cada fuente de varias que originalmente ocupaban el mismo espectro de frecuencias, a una banda distinta de frecuencias, y se transmite en forma simultánea por un solo medio de transmisión; con esto se logra la transmisión de varios canales de banda relativamente angosta por un solo sistema de transmisión de banda ancha.

FDM es un esquema análogo de multiplexado; la información que entra a un sistema FDM es analógica y permanece asídurante toda su transmisión. De las principales características de FDMA se pueden mencionar que requiere un multiplexor de antena para transmisión dúplex, se asignan canales individuales a cada usuario y los canales son asignados de acuerdo con la demanda; normalmente FDMA se combina con multiplexing FDD.

En la figura 3 se observa el comportamiento de los métodos utilizados por LTE.

Para el estándar LTE el espacio de la subportadora es de 15 KHz y cuenta con prefijos de longitud cíclica cortos y largos de 4,7 μs, y 16,7 μs, respectivamente. La multiplexacion espacial para la subida de datos se realiza mediante una sola capa de subida para UE; para la multiplexación espacial para la bajada de datos se puede utilizar un máximo de 4 capas. Las modulaciones utilizadas son: QPSK, 16 QAM y 64 QAM. Adicional, se determinó que el ancho de banda idóneo para LTE es de 20 MHz.

Figura 3. **OFDM y FDMA**



Fuente: 3GPP. http://www.3gpp.org/technologies/keywords-acronyms/98-lte. Consulta: enero de 2015.

1.2.5.1.1. Arquitectura

La arquitectura del estándar LTE está conformada por dos partes principales:

- EPC
- EUTRAN

La Eutran es la parte de la red LTE que se encarga de todas las funciones relacionadas con la interfaz de radio y el control de los móviles. La EPC tiene como función primordial brindar acceso a otras redes de paquetes IP; además, es aquí donde se gestionan los aspectos relacionados con la seguridad, calidad de servicio, gestión de recursos y movilidad.

Eutran está compuesta por los eNodosB brindando aspectos importantes como el control de móviles y el manejo del medio; estos elementos de red se interconectan entre ellos por medio de interfaces X2, los eNodeB interactúan con la EPC por medio de los equipos *mobility management entity*, (MME, por sus siglas en inglés) con interfaces S1 para el control de la movilidad, gestión y otros aspectos. Estas son dos interfaces IP que usan el protocolo SCTP (*stream control transmission protocol*). Algunas de las funciones principales de los nodos eNodeB son:

- El enrutamiento en el plano de usuario.
- Realizar las funciones de gestión de recursos de radio como conexión, control de admisión de radio, control de movilidad en el plano de usuario.
- Transmisión de información de tipo *broadcast.*
- Compresión de encabezados IP y encriptación de datos de usuario.

La interfaz Uu, también denominada interfaz radio LTE, permite la transferencia de información por el canal radio entre el eNodeB y los equipos de la red/usuario. Todas las funciones y protocolos necesarios para realizar el envío de datos y controlar la operativa de la interfaz Uu se implementan en el eNodeB. A través de la interfaz S1 se realiza la conexión entre el eNodeB y la red troncal EPC a. Dicha interfaz está conformada por dos interfaces diferentes. La primera interfaz es la S1-MME, la cual realiza la función de sustentar el plano de control y S1-U como soporte del plano de usuario. La separación entre

plano de control y plano de usuario es una característica importante en la organización de las torres de protocolos asociadas a las interfaces de la red LTE.

Los eNodeBs poseen la característica de conectarse entre sí mediante la interfaz X2. A través de dicha interfaz, los eNodeB se intercambian tanto mensajes de señalización destinados a permitir una gestión más eficiente del uso de los recursos radio, como tráfico de los usuarios del sistema cuando estos se desplazan de un eNodeB a otro durante un proceso de handover.

1.3. Aparición mensajería SMS

El servicio de mensajes de texto corto (SMS, por sus siglas en inglés) fue un servicio inventado en 1985 por Matti Makkonen. El SMS tuvo su aparición junto con el estándar GSM.

El SMS, originalmente, fue diseñado como parte del estándar GSM, pero debido a la alta demanda en su utilización se ha mantenido y evolucionado con los diferentes estándares; actualmente está disponible en una amplia variedad de redes, incluidas las 4G. El SMS sirve para teléfonos fijos y otros dispositivos portátiles. Un mensaje de texto, o SMS, es una cadena alfanumérica de hasta 160 caracteres, esto cuando se trabaja con la codificaciones de 7 bits, y cuyo encapsulado incluye una serie de parámetros.

Básicamente, los SMS se emplean para enviar y recibir mensajes de texto normal (únicamente caracteres alfanuméricos y algunos caracteres especiales, propios de la codificación), pero existen extensiones del protocolo básico que permiten incluir otros tipos de contenido, dar formato a los mensajes o

encadenar varios mensajes de texto para permitir mayor longitud. En el estándar GSM existen los siguientes tipos de mensajes de texto:

- Mensaje de texto normal.
- Mensaje de configuración, los cuales contienen los parámetros de conexión para otros servicios, como WAP o MMS.
- Mensajes WAP-*Push.*
- Notificaciones de MMS.
- Notificaciones de *VoiceMail.*

Los mensajes SMS se definieron dentro del estándar GSM, como un medio para que los operadores de red enviaran información sobre sus diferentes servicios a los usuarios sin que estos pudieran responder ni enviar mensajes a otros usuarios dentro de la red. Este tipo de mensajes se denominaba MT-SM (*mobile terminated-short message*), es decir, mensajes que finalizan en la terminal móvil del usuario. Con el paso del tiempo, las empresas de telefonía y los fabricantes móviles observaron que este servicio estaba siendo menospreciado, hasta que la empresa Nokia desarrolló un sistema, fue la comunicación bidireccional por SMS; los mensajes enviados por los usuarios pasaron a denominarse MO-SM (*Mobile originated*).

Los mensajes de texto son procesados y direccionados por el elemento denominada Centro de servicio de mensajes cortos (SMSC, por sus siglas en inglés); este se encarga de almacenarlos hasta que son enviados y de conectar con el resto de elementos de la red GSM. Dentro de las principales funciones del SMSC se encuentran:

- Recibir y almacenar los diferentes mensajes cortos enviados por los usuarios o por otras fuentes (avisos del operador, buzón de voz,

sistema de publicidad, alertas de correo electrónico, entre otros) hasta que estos puedan ser enviados.

- Junto con el HLR, verificar si el usuario tiene permisos para enviar mensajes cortos.
- Junto con el HLR, verificar si el usuario de destino (al que le llegará el mensaje corto) se encuentra activo; de no ser así, los mensajes se almacenan y entran en un sistema de reintento de envíos.
- Verificar periódicamente los mensajes que se encuentran en esquema de reintentos.
- Administrar las diferentes cuentas SMPP, por las cuales los mensajes de texto son direccionados.
- Presentar alarmas de desconexión de cuentas SMPP.
- Generar un registro por cada SMS que él recibe.
- Realizar enrutamientos especiales.
- Denegar el envío y recepción de mensajes de texto, sin solicitar información al HLR; esto mediante una lista negra interna.

Cuando un usuario genera un mensaje de texto corto se realizan los procesos de verificación del usuario. El HLR donde está registrado el usuario decide si puede o no enviar mensajes; si todo el usuario no tiene bloqueos, la MSC a la que está conectado recibe el mensaje, envía la información necesaria al VLR para su posterior tarificación y después lo remite al SMSC, este envía el mensaje al SMSC de destino; una vez allí, se convierte en MT-SM, El SMSC que ha recibido el mensaje lo almacena y solicita al VLR del usuario la información de localización; si el usuario destino está disponible, el SMSC envía el mensaje de texto a la MSC, indicando en qué BSS debe ser entregado.

Si el usuario destino está disponible, la MSC envía un aviso al VLR al que está conectado el usuario destino, para indicarle que va a entregarse un

mensaje, el VLR responde a la MSC con el estado del usuario y con la información de localización, entonces la MSC envía el mensaje al usuario y una notificación de entrega. En la pantalla del usuario se advierte: “mensaje enviado”, si el usuario lo ha solicitado, recibirá posteriormente un mensaje de estado confirmándole si el usuario de destino ha recibido el mensaje y un mensaje de error en caso de que caduque.

1.4. Características SMS

De acuerdo con las especificaciones incluidas en el estándar GSM, un mensaje de texto corto tiene una longitud de 1 120 bits, por lo que puede tener una longitud máxima de 160 caracteres alfanuméricos con una codificación de 7 bits con una longitud máxima de 140 caracteres con una codificación de 8 bits o una longitud máxima de 70 caracteres con una codificación de 16 bits. Dependiendo del tipo de codificación utilizada, varía el conjunto de caracteres a utilizar.

Una de las funciones especiales del servicio de mensajes cortos es la confirmación de recepción del mensaje de texto enviado, es decir, el usuario que envía el mensaje de texto posteriormente recibe otro en el cual se confirma si el mensaje fue enviado o no.

Cuando un usuario envía un mensaje de texto, dentro de este se incluyen los siguientes parámetros:

- Fecha de envío
- Tiempo de validez del mensaje
- MSISDN del usuario que origina el mensaje de texto
- MSISDN del usuario de destino

- Número de centro de servicio del SMSC

Debido a la alta demanda del servicio de mensajería de texto y a la limitante en cuanto al envío máximo de caracteres por cada SMS, se desarrollaron varios métodos que permiten el envío de mensajes cortos con una longitud mayor a 160 caracteres. Uno de los métodos es la concatenación de los mensajes; este método consiste en el encadenamiento de varios mensajes cortos en un grupo. Según las especificaciones del estándar GSM, es posible concatenar hasta 255 mensajes. Sin embargo el servicio de mensajes cortos de texto no fue diseñado para el alto volumen de datos; esto significa que no se cuenta con una opción que maneje la recuperación de mensajes en caso de pérdida, por lo que el envío de más de tres mensajes de texto dentro de un grupo no es adecuado.

El segundo método desarrollado fue el de compresión; con la utilización de este método se logra enviar más de 160 caracteres dentro de un solo SMS; para esto se utiliza un algoritmo especial especificado en las normas *Raw untrained dynamic Huffman*. Con este algoritmo, el usuario puede enviar un mensaje de texto con una longitud máxima de 200 caracteres. Aunque la compresión de mensajes cortos está especificada dentro del estándar GSM, los fabricantes de teléfonos han sido poco abiertos a la incorporación de esta característica.

1.4.1. Seguridad del servicio SMS

Un mensaje de texto corto puede incluir dentro de su contenido información privada e importante de cada usuario (como número de cuenta bancaria y de DPI, saldos de cuentas, entre otros) por tal razón es de vital importancia la seguridad y privacidad del envío y recepción de los SMS.

Con la finalidad de asegurar que los mensajes cortos no puedan ser interceptados, vigilados o alterados, el estándar GSM incorpora mecanismos de seguridad para SMS, donde toda la información que se transfiere sobre el canal de señalización se divide dentro de segmentos de 23 bytes de tamaño y cada segmento está protegido por un código CRC de 5 bytes llamado *fire*, el cual proporciona una comprobación de redundancia cíclica, donde toda la información dentro y fuera del mensaje corto en sí está incluida dentro del código generado.

La redundancia cíclica se calcula automáticamente entre la estación móvil y la estación base SMSC. Los mensajes cortos son encriptados utilizando el algoritmo de encriptación IA5.

1.4.2. Modelo de capas para el servicio SMS

En el modelo de capas para SMS, cada capa o nivel proporciona un servicio a la capa superior y este se implementa mediante el protocolo correspondiente en cada capa. El modelo está divido 4 capas: de aplicación, de transferencia, de retransmisión y de enlace.

La primera capa de este modelo es la de aplicación. Esta está implementada en la estación móvil o alguna entidad de mensajes cortos, con la capacidad de procesar mensajes SMS, y son aplicaciones de software que envían, reciben e interpretan el contenido de mensajes de texto.

La segunda capa del modelo es la llamada de transferencia, en la cual se realiza el servicio de transferencia bidireccional del mensaje corto entre la estación móvil y el SMSC. En esta capa el mensaje de texto es considerado como una secuencia de octetos, los cuales contienen información como la

longitud del mensaje, tipo de mensaje, fecha de envío y fecha de recepción. La capa de transferencia, también se encarga de los detalles internos de la red y permite que la capa de aplicación pueda intercambiar mensajes de forma transparente.

La tercera capa es la de retransmisión. Esta permite el transporte de un mensaje de texto entre varios elementos de red; un elemento de red puede almacenar, temporalmente, un mensaje de texto, esto sucede cuando el próximo elemento de red, al cual se debe enviar el mensaje no está disponible. En esta capa, la MSC, maneja dos funciones adicionales a sus funciones usuales.

La primera función denominada *SMS gateway* o puerta de enlace MSC, identificada como SMSGMSC, es capaz de recibir un mensaje de un SMSC e interrogar al HLR para obtener la información de ruta y en seguida repartir el mensaje a la red receptora. La segunda función llamada interfuncionamiento de SMS, la cual es denotada como SMS-IWMSC, es una MSC capaz de recibir un mensaje de una red móvil y enviarlo al SMSC adecuado.

La última capa es la denominada de enlace, la cual permite la transmisión del mensaje en el nivel físico. Debido a esto, el mensaje de texto es protegido para sobrellevar con bajo nivel los errores de canal.

1.4.3. Estructura del SMS

La estructura de un mensaje de texto SMS consta de una trama de datos, los cuales se encuentran en formato PDU. Es una cadena de datos binarios representados en hexadecimal. Para su manipulación, el formato PDU se divide en dos tipos de estructuras utilizadas para el envío y recepción de mensajes

SMS; estas estructuras son muy parecidas y comparten campos en común. Las dos estructuras son:

- *SMS Submit*, para el envío de mensajes
- *SMS Deliver*, para la recepción de los mensajes

1.5. Codificación y caracteres SMS

Para el correcto funcionamiento de los mensajes de texto, entre diferentes operadoras y países, se tiene un acuerdo para la utilización de una codificación estándar; esta codificación es la UTF-7 (*7-bit unicode transformation format*), mejor conocida como codificación 7-bit. Esta es una codificación de caracteres de longitud variable que fue propuesta para representar texto codificado con Unicode, usando un flujo de caracteres ASCII.

En sus inicios, UTF-7 fue propuesto como un protocolo experimental en la RFC 1642. Esta FRC quedó obsoleta por RFC 2152. Según se expresa claramente en la RFC 2152, la RFC "no especifica ninguna clase de estándar de Internet". A pesar de esto la RFC 2152 es citada como la definición de UTF-7 en la lista de conjuntos de caracteres de la IANA. En estas codificaciones, algunos conjuntos de caracteres pueden ser representados directamente con bytes únicos de ASCII.

El primer conjunto de caracteres de UTF-7 son los denominados "caracteres directos" y contiene los 62 caracteres alfanuméricos y 9 símbolos: ' ( ) , - . / : ?. Este grupo es considerado como principal y siempre es incluidos. Existe un subconjunto principal, conocido como "caracteres directos opcionales", contiene todos los otros caracteres imprimibles en el rango plantilla: U+0020–U+007E, exceptuando los caracteres ~ \ + y el espacio. Los

caracteres de espacio, tabulación, retorno y de nueva línea pueden ser utilizados directamente como bytes simples de ASCII.

Algunos caracteres tienen que ser codificados en UTF-16 y luego modificados en base 6. El inicio de estos bloques (de base 64 modificado, codificados en UTF-16) está indicado por un símbolo +. El final se indica por cualquier carácter que no pertenezca al conjunto de base 64 modificado. Como caso especial, si el caracter después del bloque base 64 es modificado entonces este es consumido. Por ejemplo, £1" es codificado como "+AKM-1", el código Unicode para el símbolo de libra es U+00A3, el cual se convierte en base 64 como se muestra en la tabla II. Dos bits quedan fuera y son rellenados a 0.

Tabla II. **Banda 64 modificada**

Dígito hexadecimal	*0*				*0*				*A*				*3*			
Patrón de bit	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1	0	0
Índice	0				10				12									
Base 64	A				K				M									

Fuente: elaboración propia.

El proceso de codificación es el encargado de realizar esta conversión mediante una serie de pasos. Primeramente, el codificador debe tomar la decisión de qué caracteres representar directamente en ASCII y cuáles colocar en bloques de caracteres Unicode.

Un codificado simple puede incluir todos los caracteres de los cuales esté seguro que se codificarán principalmente. Sin embargo el costo de caracteres para construir un bloque de tipo Unicode para representar un único caracteres y luego obtenerlo de nuevo es de 3 a 3⅔ *bytes*; esto es más que los 2⅔ *bytes*

necesarios para representar ese carácter como parte de una secuencia Unicode.

Cuando se han elegido la secuencias Unicode adecuadas, estas deben ser codificadas usando el siguiente procedimiento y luego rodeadas con los delimitadores apropiados.

- Expresar los números Unicode (UTF-16) de los caracteres en binario.
- Concatenar las secuencias binarias.
- Reagrupar los valores binarios en grupos de seis bits, comenzando por la izquierda.
- Si el último grupo tiene menos de seis bits, agregar ceros al final.
- Reemplazar cada grupo de seis bits por su respectivo código b 64.

Para realizar el proceso de decodificación del texto, primeramente el mensaje tiene que ser separado en texto plano ASCII y bloques Unicode; posterior a esto, se realiza el siguiente procedimiento:

- Expresar cada código base 64 como la secuencia de bits que representa.
- Reagrupar los valores binarios en grupos de 16 bits, comenzando por la izquierda.
- Si al final de la trama existe algún grupo incompleto, este se descarta (si el grupo incompleto contiene más de cuatro bits o algún uno, el código es inválido).
- Cada grupo de 16 bits es un número de carácter Unicode (UTF-16) que puede ser expresado en otras formas.

En cuanto a temas de seguridad se refiere, el código UTF-7 permite tener varias representaciones del mismo texto original; esto se logra intercambiando el modo base 64 múltiples veces.

2. FUNDAMENTOS Y ESTRUCTURA DE UN CORE 3G

El capítulo anterior trató sobre los diferentes tipos de estándares que conforman la tecnología 3G. En el presente capítulo se tomará como base el estándar UMTS. Este es el estándar 3G que cuenta con la mayor aceptación mundial.

2.1. Estándar UMTS

El estándar para las comunicaciones UMTS fue promovido inicialmente por la ETSI (*European Telecommunications Standards Institute*). UMTS basa su funcionamiento en la utilización de una interfaz radio W-CDMA (*wideband code division multiple access*). Esta interfaz cuenta con dos modos de operación, FDD (*Frecuency division duplex*) y TDD (*Time division duplex*), y una tasa de 3,84 Mchip/s. El principal cambio respecto de los estándares 2G, se da a nivel de acceso donde se utiliza una nueva interfaz de aire (WCDMA) proveyendo una tasa de bits mayor que en 2G. En el core se da el principal cambio en el *packet switch* que permite una mejor y más rápida transferencia de paquetes de datos. Además, el estándar UMTS permite a las compañías de telefonía, ingresar más usuarios a su red de acceso, y brindándoles una mejor velocidad en cuanto a transmisión de datos se refiere.

La interfaz de aire está compuesta por tres diferentes tipos de celdas: macrocelda, microcelda y picocelda, las cuales tienen un ancho de banda mínimo de 5 MHz.

La macrocelda cuenta con un radio de cobertura de 1 km; hasta un máximo de 35 km; esta cobertura incluye áreas urbanas, rurales y vehículos que se mueven a altas velocidades.

La microcelda cuenta con un radio de cobertura de 50 m hasta un máximo de 1 km; esta cobertura incluye áreas urbanas, y vehículos que se mueven a bajas velocidades.

La microcelda cuenta con un radio de cobertura de hasta 50 m; estas son utilizadas para usuarios fijos dentro de edificios.

Cada tipo de celda cuenta con una velocidad máxima de transmisión; la velocidad máxima de una macrocelda es de 114 kbps; la velocidad máxima de una microcelda es de 384 Kbps y la de una picocelda es de 2 Mbps.

El sistema UMTS fue diseñado para ser un sistema global, integrando tanto redes terrestres como satélitales. El objetivo de este diseño era lograr una comunicación personal con cobertura mundial, a través de terminales capaces de trabajar en las distintas redes. Esto significa que el abonado podrá itinerar sin pérdida de comunicación entre las diferentes redes. Con el objeto de permitir escenarios de comunicación con interlocutores de otras redes, ya sea que el usuario acceda a través de su red propia o la de otro operador (escenario de *roaming*) se distinguen tres dominios:

- Red de servicio (SN, *service network*). Esta es la red a la que el usuario está accediendo en un momento dado, pudiendo ser la red propia, o en el caso de *roaming,* la red visitada.
- Red propia (HN, *home network*). Esta es la red del operador a la que el usuario está abonado. En el caso de que el usuario esté utilizando el

servicio *roaming*, la red visitada debe realizar un contacto con la red propia del usuario, esto para compartir información sobre temas de tarificación, bloqueos, servicios autorizados y temas de autenticación)

- Red de tránsito (TN, *transit network*). Esta es la red destino donde se encuentra el usuario destino con el que desea comunicarse el usuario de origen.

2.2. Características UMTS

El estándar UMTS, se considera una evolución del estándar GSM, por lo que comparten características. Dentro de las principales características del estándar UMTS se encuentran:

- Permite a las compañías de telefonía reducir el costo de cada uno de los servicios ofrecidos al usuario.
- UMTS asegura compatibilidad con las versiones anteriores de GSM como GPRS, EDGE, y 2,5G TDMA.
- Permite a las compañías de telefonía brindar al usuario una mayor cantidad de servicios, los cuales son de uso fácil y además son adaptables al entorno.
- Alta velocidad en la transmisión de datos, provee paquetes de datos de hasta 2,048 Mbps por usuario, con el propósito de datos de alta calidad, multimedia, *streaming* audio-video, y servicios de *broadcasting*.
- Ofrece servicios multimedia, tanto simétricos como asimétricos.
- Mejora el servicio de llamadas de voz.
- Permite una convergencia de redes móviles y fijas.
- Realiza una asignación dinámica del ancho de banda; esto se refleja en un uso más eficiente del ancho de banda.

- El espectro nuevo del UMTS es de 5 MHz para la utilización de todas las aplicaciones.
- Utiliza como tecnología base, la conmutación por paquetes.
- Utilización de protocolos IP: por medio de este protocolo se pueden utilizar servicios multimedia interactivos y nuevas aplicaciones de ancha banda como el servicio de video telefonía y videoconferencia (audio-video *streaming*).
- Ofrece el servicio de *roaming*.
- Ofrece una mayor capacidad para soportar usuarios conectados al mismo tiempo.
- Este estándar es soportado por una amplia gama de teléfonos celulares.
- Diferentes servicios simultáneos en una sola conexión.
- Personalización de los diferentes servicios, con base en el perfil local del usuario.
- El ancho de banda de 5 MHz, provee una tasa de datos que puede alcanzar 2 Mbps el cual soporta entre 100 y 350 llamadas de voz simultáneamente. Esta velocidad depende mucho de otros factores tales como condiciones de propagación, la velocidad del usuario y la polarización de la antena.
- Acceso personalizado VHE (*virtual home environment*), con esto el usuario puede recibir el mismo servicio sin importar su ubicación geográfica.

Como se observa, el estándar UMTS, presenta bastantes mejoras respecto de GSM, pero también cuenta con las siguientes desventajas:

- Menor rango de cobertura.

- Los usuarios nuevos de la tecnología 3G también deben tener equipos que soporten esta tecnología. Una unidad móvil que pueda acceder a diferentes tecnologías tales como *triband* o *quad-band* sería lo ideal.
- El costo de infraestructura es mucho mayor.
- La velocidad de transmisión depende de varios factores, por lo cual no es constante.

Una de las principales diferencias entre los estándares de telecomunicaciones GMS (para 2G) y UMTS (para 3G) se observa en el canal de radio utilizado. Para GSM se utilizan canales de radio de banda estrecha, lo que influye en una asignación de canal de menor capacidad para el usuario final, mientras que para UMTS se utilizan canales de radio de banda ancha, lo que le permite al usuario final una mayor flexibilidad en cuanto al manejo de los servicios multimedia se refiere y una mejor velocidad de transmisión de datos, tanto de subida como de bajada. Si las velocidades de subida y bajada de datos son iguales, se dice que la velocidad de trasmisión es simétrica, mientras que, si las velocidades de bajada y subida no son iguales, se dice que la velocidad de transmisión es asimétrica.

2.3. Arquitectura Core 3G, UMTS

Básicamente, la arquitectura de una red basada en el estándar UMTS, se define en términos de dominios (basados en los elementos funcionales) y puntos de referencia (interfaces).

En el nivel superior de la arquitectura, el sistema UMTS se conforma por el dominio de equipo de usuario, UE (*user equipment*) y el dominio de infraestructura; entre ambos dominios se encuentra la interfaz de radio, o el punto de referencia Uu.

En el dominio de equipo de usuario se observan los módulos de identidad de abonado UMTS, USIM y el equipo móvil, ME (*mobile equipment*), definiéndose entre ellos la interfaz Cu. La micro SIM es una tarjeta SIM inteligente que identifica al usuario dentro de una red UMTS; esta es independiente del equipo en el que se halle insertada en un momento dado.

El dominio de infraestructura se encuentra conformado por el dominio de núcleo de red CN (*core network*) y el dominio de red de acceso AN (*access network*). Estos dominios se encuentran separados a través del punto de referencia Iu. El dominio de núcleo de red, a diferencia del dominio de red de acceso, es independiente de la técnica de acceso. El dominio de red de acceso incluye todas las funciones dependientes de la técnica de acceso empleada.

Para la arquitectura de una red UMTS Release 99, se distinguen tres partes esenciales: los equipos de usuario, la red de acceso UTRAN, y el núcleo de red, CN. Visualizando las arquitecturas de UMTS y GSM, no parece que existan grandes diferencias entre ambas.

La arquitectura de red de acceso en UMTS está formada por los nodos B y controladores de red radio, RNC (*radio network controlers*), los cuales son los equivalentes a las BTS y BSC de GSM.

El estándar UMTS no es más que una evolución del estándar GSM; por esta razón la red núcleo está basada en su mayoría en una red núcleo GSM. Los elementos que comparten ambas arquitecturas son en su mayoría los elementos que manejan el tráfico de voz, entre los cuales se tienen: el subsistema de estación base o BSS, que es el responsable de manejo del tráfico y señalización de la interfaz de aire; es el primer elemento de la red con la que entra en contacto la estación móvil y que permite la comunicación con el

NSS. Gestiona el ancho de banda, control de llamada, traspaso entre celdas, así como la potencia de la portadora de cada usuario.

La BTS es la encargada de mantener la comunicación bidireccional entre la estación móvil y la BSC; para esto realiza procesos para garantizar la conexión libre de errores entre la estación móvil y la BSC.

La BSC, es la encargada de la comunicación y monitoreo de una o varias BTS, permitiendo la conexión entre la estación móvil y el subsistema NSS; también mantiene un control sobre el estado del funcionamiento de las estaciones base que administra, informando sobre posibles anomalías que presenten.

La MSC es el elemento principal de la red GSM y que también juega un papel de vital importancia dentro de la red UMTS. Esta se encarga de controlar a todos los otros elementos del subsistema de conmutación de red. La MSC está asociada básicamente con funciones de conmutación como el establecimiento de llamada, la liberación y el enrutamiento. Sin embargo, también lleva a cabo una serie de funciones adicionales, incluyendo el enrutamiento de mensajes SMS, llamadas en conferencia, fax y servicio de facturación, así como la interconexión con otras redes como la red telefónica pública conmutada (PSTN).

El HLR es una base de datos que contiene información sobre todos los abonados móviles de un operador en específico, tales como identificador internacional del abonado, información geográfica del mismo, estación de viajero, servicios de suscripción y servicios activos.

El VLR consiste en una base de datos que contiene información sobre usuarios temporales dentro de la red. Los datos temporales que almacena un VLR son IMSI, TMSI, LAI, MSISDN, MSRN.

La función principal es apoyar en el proceso de autenticación del abonado por medio del almacenaje de la clave de identificación Ki, la cual es única en cada tarjeta SIM.

El EIR consiste en una base de datos que almacena el IMEI de las estaciones móviles. La función principal del EIR es controlar el acceso a la red, mediante listas de acceso. Las posibles listas son blanca, gris y negra.

El OSS provee funciones determinadas para la gestión de red centralizada (NMC), y el centro de monitoreo y mantenimiento (OMC) de la PLMN.

Dentro de los nuevos equipos que incorpora una red UMTS se encuentran los SGSN, GGSN, MGW, entre otros.

2.3.1. Puerta de acceso al medio, MGW

La puerta de acceso al medio (MGW, *media gateway*) es un elemento de la red UMTS que puede ser físico o lógico. La función principal del MGW es servir de conexión y enlace entre dos elementos, cuya comunicación, debido a su naturaleza distinta, sería imposible o muy difícil de otra manera.

El MGW traduce la señalización de las tecnologías diferentes a UMTS, a lenguaje de *switch* u otro nodo de la red como el HLR. En el caso de un *sotfstwitch,* la conexión entre la BSS (BTS + BSC) está en formato SS7 TDM y el MGW lo convierte en SIGTRAN para poder realizar la comunicación. Se hace

un cambio de TDM a IP, pero el contenido de SS7 para ambos que es BSSAP queda intacto. El *switch* (*softwitch*) y la MGW pueden venir en equipos distintos o en uno mismo, donde en su generalidad se encuentran en equipos separados. Así, la separación del control y tráfico de datos permite a la red emplear más eficientemente sus *routers* de alta capacidad, mientras el tráfico de señalización es manejado por equipos de menor porte.

El MGW se encarga de manejar la señalización de los *gateways* que transportan el control de señalización de las llamadas, la cuales pueden ser ISDN, CAS o SS7 a través de una red IP por un Softswith. Equipos como el VoiceMail son conectados directamente al MGW; esto para poder tener contacto directo con todas las tecnologías debido a ser un nodo de aplicación común.

2.3.2. Controlador de red de radio, RNC

La RNC (*radio network controller*) tiene como función primaria el control de todos los nodos B que se conectan a ella. La RNC es la encargada de la gestión de los recursos radio y parte de la gestión de movilidad. Además es el punto en el que los datos son encriptados, antes de que sean enviados desde o hacia el terminal móvil. La RNC se interconecta con la MSC mediante la interfaz IuCS, con el SGSN mediante la interfaz IuPS. Dos RNC se pueden interconectar; la conexión entre estas es del tipo lógico, la interfaz que se encarga de esta conexión es la Iur, pero esto no implica que debe ser necesaria una conexión directa entre ellas. Realizando una analogía con el estándar GSM, la RNC es equivalente a una BTS.

Lógicamente, una RCN se divide en tres tipos:

- La RNC de control es la encargada del control sobre entidades de transporte común, también administra el tráfico que va sobre un Nodo B.

- La RNC de servicio establece y mantiene las conexiones de radio, con el fin de conducir el tráfico común y el tráfico dedicado entre las entidades UE, RNC y CN.

- La RNC de transferencia tiene como función la administración y control de los *handovers*.

Los pasos para realizar un *handover* son tomar mediciones, decisiones y luego ejecutar las mismas. Las mediciones son tomadas por el UE y enviadas a la RNC; estas mediciones están estrechamente relacionadas con la QoS de la conexión. Si el usuario se encuentra en el límite de cobertura de una célula (donde la señal es muy débil) es propenso a realizar un traspaso a otra célula mediante un *handover*. En las especificaciones dictadas por 3GPP se definen las mediciones que debe realizar el EU, las cuales son intrafrecuencia, interfrecuencia, volumen de tráfico y calidad.

Entre las funciones principales de una RNC se encuentran:

- Manejo de los recursos de transporte de la interfaz Iu.
- Control de los recursos lógicos del nodo B.
- Manejo de la información del sistema.
- Manejo de los horarios de la información del sistema.
- Manejo de tráfico para todos los canales comunes.
- División de las tramas de datos trasferidas sobre varios nodos B.
- Realización del llamado *soft handover*.

- Asignación de los diferentes códigos de canalización en el enlace de bajada.
- Control de la potencia en un enlace de subida.
- Control de la potencia para un enlace de bajada.
- Manejo de reportes.
- Control de admisión o acceso.

La función de la RNC del control de potencia tiene como finalidad ajustar la potencia del transmisor a un nivel adecuado con el cual se pueda satisfacer una QoS determinada. Existen dos tipos de control de potencia: el primero es el control de potencia de bucle abierto, que sirve para ajustar la potencia en los enlaces de bajada, y el control de potencia de bucle cerrado, el cual se utiliza para compensar las fluctuaciones de la intensidad del canal de radio.

La finalidad del control de admisión y acceso es analizar si una llamada nueve puede o no tener acceso al sistema; esto sin tener que sacrificar el QoS de las llamadas existentes.

Para la gestión de códigos, la RNC utiliza un conjunto de códigos ortogonales, siempre y cuando estos no tengan ninguna relación entre sí; de lo contrario se utilizan códigos de aleatorización, estos son los encargados de identificar a la célula; con esto se facilita el proceso de *handover,* ya que en estos procesos al cambiarse de célula se cambia el código de aleatorización.

Los códigos de canalización son los encargados de identificar a los usuarios de una célula. Una mala administración de los códigos WCDMA puede traer como consecuencia la inestabilidad en el sistema. Los códigos son limitados; por esta razón es que son gestionados por la RNC. Existe un total de

2^{18} – 1 códigos de aleatorización para un enlace de subida, 2^{24} códigos de aleatorización para un enlace de bajada y 256 códigos de canalización.

Antes que la RNC establezca una conexión RAB para la transferencia de información, debe crear un canal de señalización entre en UE y el CN; este canal es llamado SRB. Una vez establecido el SRB, las solicitudes RAB son negociadas, luego la RNC analiza los atributos de los RAB solicitados; además evalúa los recursos de radio que se encuentran disponibles, para analizar la factibilidad de la conexión; por último la RNC activa el RAB y reconfigura los canales de radio del nodo B.

La información de señalización y los datos del usuario son cifrados con algoritmos predefinidos, para garantizar la seguridad de todos los datos transmitidos.

2.3.3. Nodo B

Un nodo B es el análogo de una BTS en el estándar GSM. La función principal de un nodo B es controlar los protocolos de la interfaz de aire; dichos protocolos incluyen tareas como la adaptación de tasas de transmisión de información, codificación de canal, entre otros. Las funciones del nodo B están ligadas directamente con el método de acceso a canal e interfaz aérea del sistema. Aunque en la teoría se recomienda que un nodo B únicamente brinde servicio a una célula, en la práctica un nodo B es capaz de brindar servicio a más de una célula.

El nodo B, se encuentra ubicado en la capa física de la interfaz de aire, es por esta razón que los nodos B también realizan funciones propias de un elemento de capa 1. Un nodo B ejecuta funciones como la implementación

lógica del esquema de operación y mantenimiento, mapeo de los recursos lógicos de un nodo B en los recursos de hardware, transmisión de los mensajes de información del sistema de acuerdo con el horario determinado por la RNC; en el modo FDD realiza la administración del control de potencia de lazo cerrado en el enlace de subida, genera códigos de acceso a la red, realiza la combinación para la macrodiversidad, divide las tramas de datos internas al nodo B y reporta las mediciones de la interferencia en el enlace de subida y la información de potencia en el enlace de bajada.

Desde el punto de vista del usuario, un nodo B es el encargado de proveer cobertura al teléfono celular. El nodo B es un elemento transceptor; esto quiere decir que transmite y recibe información. Los bloques TX y RX son los encargados de la transmisión y recepción de esta información; un modulador se encarga de adecuar las señales para su transmisión; las modulaciones más utilizadas son QPSK, Dual QPSK y 16QAM.

Lógicamente un nodo B está compuesto por dos entidades lógicas, la entidad de transporte común y los TTP. El transporte común se realiza por los canales de transporte común que son utilizados por el UE para el acceso inicial a la red; este también posee un puerto destinado para las funcionalidades de operación y mantenimiento.

2.3.4. SGSN

El SGSN (*Serving GPRS support node*) es la pieza central de la red basada en conmutación de paquetes, este se conecta con UTRAN mediante la interfaz Iu-PS y con el GSM-BBS a través de la interfaz Gb.

El SGSN es un nodo de servicio GPRS que tiene como función principal brindar acceso a las terminales móviles hacia la red de datos. Cuando el usuario establece una conexión de datos, el SGSN es el primer punto en el cual se realiza la autentificación de la terminal; adicional lleva un registro de la localización de las terminales, realiza enrutamientos y transferencias de los paquetes de datos y establece los túneles entre la RAN y el GGSN. La función principal del GGSN es la tarificación de las terminales móviles que se encuentran utilizando el servicio de *roaming*; esto se realiza mediante la generación de registros de servicios, a estos registros se les denomina CDR.

Un SGSN cuenta con una serie de servicios configurados, entre los cuales se tienen:

- SGSN service, este servicio realiza la conexión hacia las RNC/BSC
- MAP service, que es la parte de acceso hacia el HLR
- SGTP service, el cual realiza la conexión hacia el GGSN
- GTPP service, este servicio es el encargado de la parte de facturación

El SGSN almacena información sobre el abonado, entre la cual está la información de suscripción, el IMSI, identificadores temporales, dirección PDP, información de ubicación geográfica, la célula en la cual se encuentra registrado el usuario y el número de VLR del usuario.

2.3.5. GGSN

El GGSN es conocido como el último elemento dentro de la arquitectura UMTS 3G que interactúa con el cliente, antes que este pase a una red externa (internet). El GGSN cumple con las funciones de un *router, modem* y un sistema de seguridad para la red.

El GGSN es la puerta de salida o punto central de conexión hacia el exterior o la PDN de una red de telefonía celular; estas redes externas pueden ser Internet o una red corporativa. También son el punto de acceso para múltiples puntos de accesos.

GGSN, dependiendo de la configuración propia del operador, puede manejar una parte de autentificación o autorización de navegación denominada Radius/Diameter, esto se realiza mediante los APN. Los APN se pueden configurar de tal forma que pueden especificar el tipo de esquema de facturación al cual pertenece el abonado, actualmente puede ser prepago, pospago e híbridos. Cuando un abonado cuenta con un APN establecido, el GGSN procede a asignarle una dirección IP para usarla en la red externa.

El GGSN está íntimamente relacionado con el SGSN ya que si un abonado no es autentificado y enrutado por el SGSN jamás llegará al GGSN. Para la comunicación entre estos dos equipos se utiliza el protocolo denominado GTP-C, el cual es un protocolo interno de la red núcleo y pertenece al domino PS. Este se ubicada entre el SGSN y el GGSN.

GTP-C especifica la gestión y administración de túneles y todos los procedimientos de control, que realiza la conexión entre SGSN y GGSN con la cual es posible la transferencia de paquetes de información del abonado. Adicional, también se utiliza para la transferencia de mensajes de señalización GMM entre dos o más SGSN; también ayuda a cada SGSN con la tarificación del servicio, esto mediante la recolección y transportación de datos de costos y tarificación.

El protocolo GTP-C opera en la interfaz Gn (interfaz ubicada entre el SGSN y el GGSN), en la interfaz Gp (interfaz ubicada entre el SGSN y el BG) la

cual posibilita la interconexión con otros redes UMTS y su medio de transporte es sobre pilas de protocolos UPD/IP

2.3.6. Interfaz Iu

La función principal de esta interfaz es conectar a la red central con la red de acceso de radio. La interfaz Iu puede tener dos diferentes instancias físicas para conectar a dos diferentes elementos de la red central, esto se define mediante el análisis si se trata de una red basada en conmutación de circuitos o una red basada en conmutación de paquetes. Dentro de las funciones de esta interfaz está la de servir como enlace BRAN, el cual es una implementación física generalizada del concepto URAN.

Para una red basada en conmutación de circuitos, se define a la interfaz Iu-CS, como la encargada del enlace entre UTRAN y la MSC, y a la interfaz Iu-PS como la encargada de conectar a la red de acceso de radio con el SGSN de la red central.

2.3.7. Interfaz Iub

Esta interfaz se ubica entre la RNC; y el Nodo B en el UTRAN. Haciendo una analogía con GSM, la interfaz IuB es similar a la interfaz A-bis. Esta interfaz es utilizada para soportar los servicios ofrecidos al usuario final. Adicional, la interfaz Iub permite el control del equipo de radio y la asignación de radiofrecuencias en el Nodo B.

2.3.8. Interfaz Iur

La interfaz Iur permite la comunicación entre dos RNC; con esto se logra que el desempeño de la red en cuanto a la movilidad de los usuarios dentro de la misma se refiere, sea más efectivo. En otras palabras, gracias a la interfaz Iur se logra mejorar el proceso de entrega y recepción de llamadas de usuarios que se encuentran trasladándose entre las coberturas de diferentes RNC. Esta interfaz soporta el intercambio bidireccional de información del abonado.

2.3.9. Interfaces UMTS

Adicional a las interfaces antes descritas, se encuentran las interfaces de comunicación entre equipos de red GSM/UMTS; de estas interfaces se pueden mencionar las siguientes:

La interfaz Uu, la cual se encuentra localizada entre el equipo de usuario y la red UTRAN.

La interfaz B está localizada entre las MSC y el VLR.

Las interfaces de GPRS, utilizan como protocolo de comunicación el protocolo MAP; estas son:

- Gf, interfaz para fraudes
- Gi, interfaz de internet
- Gp, interfaz de PLMN
- Gc, interfaz de contexto
- Gn, interfaz de nodo
- Gb, interfaz de base

La interfaz B es la encargada de la comunicación entre la MSC y el VLR. La interfaz C se encarga de la comunicación entre la MSC y el HLR. La interfaz D es la encargada de la comunicación entre el HLR y el VLR. La interfaz F se encarga de la comunicación entre la MSC y el EIR.

3. FUNDAMENTOS Y CARACTERÍSTICAS DEL PROTOCOLO SMPP

El protocolo SMPP (*short message peer to peer protocol*) es un protocolo estándar de telecomunicaciones utilizado fundamentalmente para el intercambio bidireccional de mensajes SMS, entre los diferentes equipos que gestionan los mensajes dentro de una red 2G o 3G.

Este protocolo permite a entidades externas a las redes móviles, conectarse a estas a través del centro de mensajes cortos SMSC para enviar y recibir mensajes SMS. Se basa en el intercambio de petición y respuesta de PDU (unidad de datos de protocolo) y permite el envío y recepción de mensajes en modo asíncrono y síncrono.

3.1. Historia

SMPP fue desarrollado por la firma Irlandesa Aldiscon; luego esta firma fue adquirida por la compañía Lógica (en la actualidad conocida como *Acision*). En 1999, el protocolo SMPP pasó formalmente a manos del *SMPP developers forum*, posteriormente denominado como *SMS Forum*.

El protocolo fue creado por el desarrollador Ian J. Chambers, para probar la funcionalidad de un centro de mensajes SMSC sin tener que utilizar equipos SS7 para enviar los mensajes.

En el 2007 el protocolo SMPP vuelve a ser, nuevamente, propiedad de Acision, esto debido a la disolución del *SMS Forum*. Al devolverse el foro, el

protocolo SMPP quedó estancado y no se han realizado actualizaciones importantes para su mejora o evolución.

3.2. Fundamentos

El protocolo SMPP basa su funcionamiento en el intercambio de datos sobre un canal TCP/IP o X.25 entre el ESME y el SMSC [SMPP, 00]. En el canal de intercambio de datos se pueden dar los siguientes estados de sesión:

- OPEN, inicia una conexión con el SMSC.
- CLOSED, realiza una desconexión con el SMSC.
- BOUND_TX, el cliente indica que la conexión establecida con el SMSC es del tipo TX, es decir, para la transmisión de mensajes.
- BOUND_RX, el cliente indica que la conexión establecida con el SMSC es del tipo RX, es decir, para la recepción de mensajes.
- BOUND_TRX, el cliente indica que la conexión establecida con el SMSC es del tipo TRX, es decir, para la transmisión y recepción de mensajes.

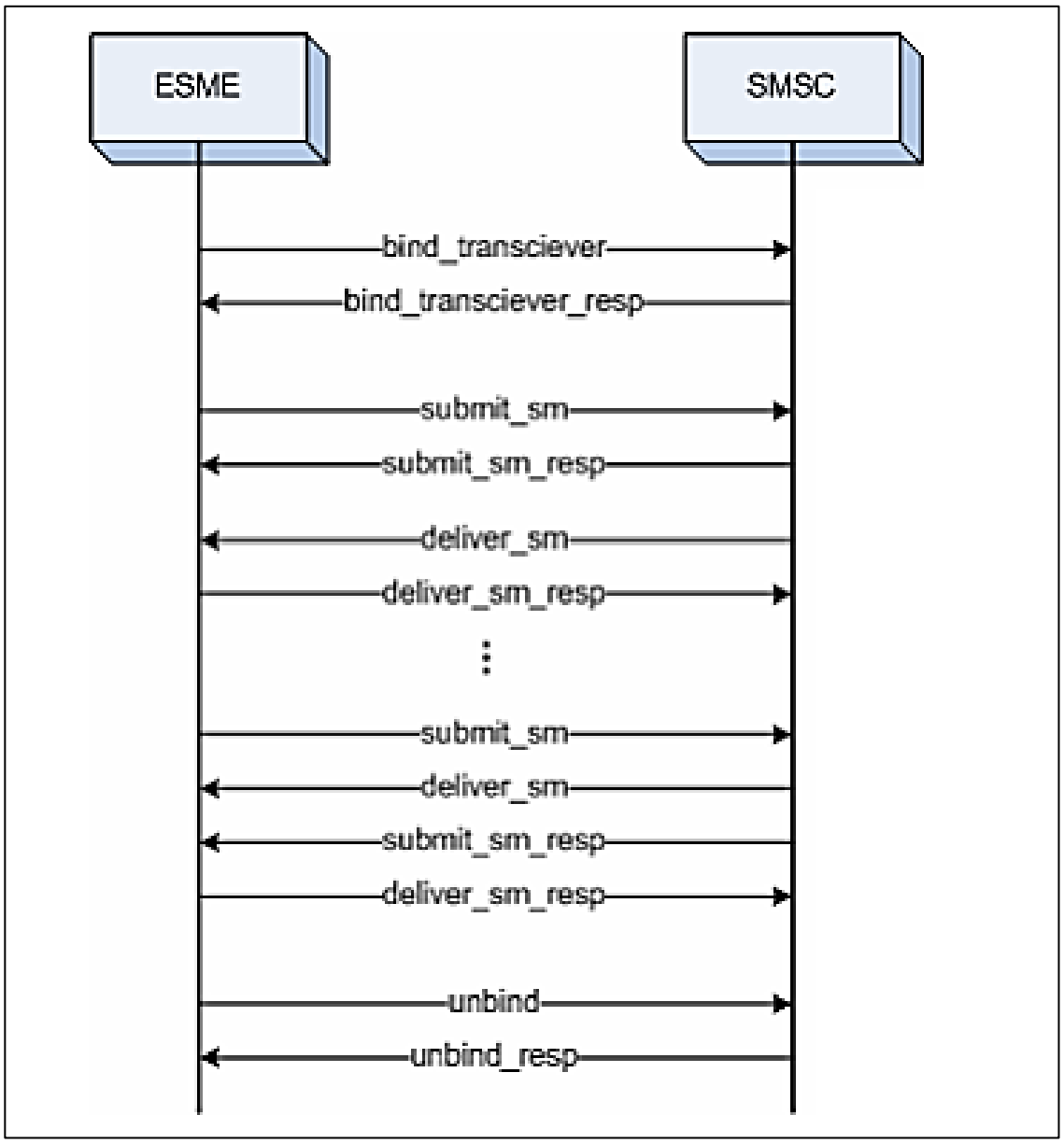
Para cada uno de los diferentes estados de sesión, el intercambio de datos entre las entidades se realiza enviando paquetes llamados PDU.

Dentro de la estructura de cada PDU se encuentra una cabecera y un cuerpo, donde la cabecera indica el largo del mensaje, un identificador, un comando y un número de referencia. El cuerpo contiene campos variables que dependen directamente del comando enviado. El protocolo SMPP define una serie de comandos para distintas operaciones, entre los cuales se tienen:

- *bind_transceiver* y *bind_transceiver_resp*. Estos comandos son utilizados para iniciar la comunicación con el SMSC; esta comunicación es para el envío y recepción de información.
- *submit_sm* y *submit_sm_resp*. Estos comandos son utilizados para el envío un mensaje SMS.
- *deliver_sm* y *deliver_sm_resp*. Son utilizados para la recepción de un mensaje SMS.
- *generis_nack*. Este comando son utilizados para responder a comandos no válidos.
- *unbind* y *unbind_resp*. Son utilizados para finalizar la conexión con el SMSC.

En la figura 4 se observa la interacción entre el ESME y el SMSC.

Figura 4. **Flujo de mensajes SMS**



Fuente: elaboración propia, empelando Adobe Photoshop.

3.2.1. Sesiones SMPP

Una sesión SMPP da inicio cuando una ESME que cuenta con una conexión de red con el SMSC, solicita la apertura de una sesión SMPP por medio de una petición de conexión al SMSC. Las sesiones se pueden establecer de dos nodos, el primero para actuar como una entidad que únicamente recibe mensajes y el segundo para actuar como una entidad que únicamente transmite mensajes. Para realizar una conexión TRX, la ESME debe solicitar la apertura de dos sesiones, una TX y la otra RX, aunque desde la V3.4 se omite el tener que abrir dos sesiones y únicamente se solicita la apertura de una sesión TRX.

Durante el tiempo que dure la conexión, la ESME puede realizar el envío de una serie de peticiones; estas peticiones pueden ser o no aceptadas por el SMSC, pero para cada una de la peticiones se redacta un acuse de recibo; este proceso se realiza de forma bidireccional, es decir peticiones originadas por el ESME hacia el SMSC y peticiones originadas en el SMSC con destino la ESME. Para una sesión TX, la EMSE únicamente podrá enviar mensajes; sin embargo, por esta misma sesión, la ESME recibirá todos los acuses de recibo de comandos por parte del SMSC.

3.3. Intercambio de mensajes entre ESME y SMSC

El intercambio bidireccional de peticiones y acuses de recibo se puede realizar de forma sincrónica o asíncrona; esto implica que la ESME puede enviar varias peticiones consecutivas de envío de mensajes, sin que necesariamente reciba un acuse de recibo, por parte del SMS, para cada una de las peticiones. Sin embargo, una serie de peticiones consecutivas de envío de mensajes debe ser seguida de una serie de respuestas asociadas

consecutivas. Cada mensaje cuenta con un parámetro denominado número de secuencia, el cual correlaciona cada una de las peticiones con cada uno de los acuses de recibo.

De acuerdo con la especificaciones, los acuses de recibo deberían ser entregados en el mismo orden en el cual se recibieron los mensajes, pero si por alguna razón estos se dieran fuera de secuencia, cualquiera de las dos partes debe ser capaz de interpretar a qué mensaje corresponde cada acuse de recibo. El protocolo SMPP no indica la cantidad máxima de mensajes consecutivos sin acuse de recibo, que pueden ser enviados, pero como norma general, se indica que se debe configurar un máximo de diez mensajes consecutivos.

3.4. PDU

Una vez establecida una conexión lógica entre la ESME y el centro de mensajes SMSC, se procede con el envío y/o recepción de información; esta transferencia se realiza mediante los llamados Unidades de datos de protocolo (PDU, *protocol data units*). Con la finalidad de realizar todas las funciones del protocolo SMPP, se cuenta con hasta 27 PDU diferentes. Existen dos tipos fundamentales de PDU, los de petición y los de respuesta.

Los PDU se transmiten en pares sobre la capa 4 del modelo OSI (sesiones TCP/IP, X.25). El intercambio de datos puede realizarse de manera síncrona o asíncrona. Si los PDU son transmitidos de manera síncrona, cada parte espera la respuesta-petición del otro para enviar la correspondiente petición-respuesta. Si los PDU son transmitidos de manera asíncrona, cada envío y recepción van a través de distintos hilos.

Los PDU pueden tener 3 formatos válidos que son:

- Formato entero: en este formato un valor número (sin signo) ocupa una determinada cantidad de octetos.
- Formato cadena de octetos: este formato consiste en una cadena de caracteres ASCII y longitud predeterminada, la cual es finalizada con el carácter NULL.
- Formato cadena de octetos-c: este formato consiste en una cadena de caracteres ASCII y longitud variable, la cual es finalizada con el carácter NULL.

El NULL consiste en un campo lleno de ceros, el cual tiene la misma cantidad de octetos, definida para ese número entero. Para el caso de una cadena de octetos el valor NULL consta de un solo carácter, el 0x00.

El encabezado es la parte más importante de un PDU; en este se incluye la información principal y debe estar presente en todos y cada uno de los PDU transmitidos. En la figura 5 se muestra la estructura de un PDU.

Los datos que debe contener el encabezado son longitud, ID, estado y número de secuencia. La longitud es un número entero de 4 octetos de longitud, que indica el tamaño en octetos del PDU.

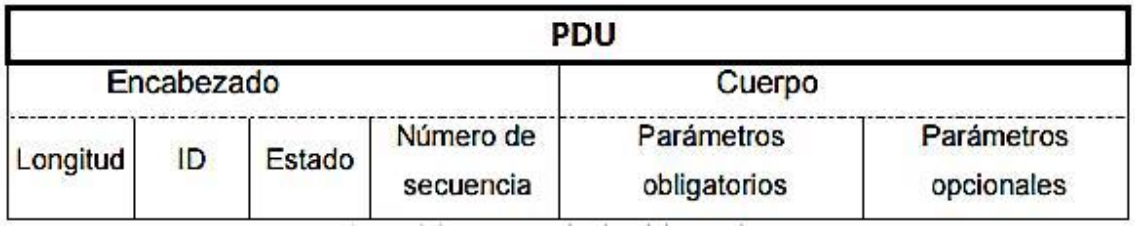
El campo ID es un número entero que cuenta con una longitud de 4 octetos, y se utiliza para identificar a cada uno de los PDU transmitidos.

El campo de estado es un número entero de cuatro octetos de longitud y que indica el estado de cada petición, los estados pueden ser éxito o fracaso.

Este campo únicamente es utilizado para los PDU de respuesta; en los PDU de solicitud este campo tiene un valor NULL.

El número de secuencia es un campo de 4 octetos de longitud, que contiene un valor que permite asociar a los PDU de solicitud con los PDU de respuesta. Gracias a este campo es posible el intercambio asíncrono de PDU de petición y respuesta. Los posibles valores para el número de secuencia abarcan el rango de 0x00000001 hasta 0x7FFFFFFF.

Figura 5. **Estructura PDU**



Fuente: elaboración propia.

En la estructura del PDU se reserva un espacio para campos opcionales, estos van incluidos dentro de la parte del cuerpo del mensaje y son utilizados para facilitar la introducción de nuevos parámetros al protocolo definido.

En la tabla III se muestran los 27 comandos SMPP utilizados para las funciones básicas, así como el valor entero tomado para la estructura de un PDP.

Tabla III. **Comandos SMPP**

ID del Comando	Valor
nack_genérico	0x80000000
bind_receptor	0x00000001
bind_receptor_resp	0x80000001
bind_transmisor	0x00000002
bind_transmisor_resp	0x80000002
interrogar_sm	0x00000003
interrogar_sm_resp	0x80000003
enviar_sm	0x00000004
enviar_sm_resp	0x80000004
entregar_sm	0x00000005
entregar_sm_resp	0x80000005
unbind	0x00000006
unbind_resp	0x80000006
sustituir_sm	0x00000007
sustituir_sm_resp	0x80000007
cancelar_sm	0x00000008
cancelar_sm_resp	0x80000008
bind_transceptor	0x00000009
bind_transceptor_resp	0x80000009
outbind	0x0000000B
estatus_conexión	0x00000015
estatus_conexión_resp	0x80000015
enviar_multi	0x00000021
enviar_multi_resp	0x80000021
notificación_alerta	0x00000102
data_sm	0x00000103
data_sm_resp	0x80000103

Fuente: elaboración propia.

3.5. Conexión y desconexión de sesión

Para registrar una sesión de una ESME con el SMSC es necesario realizar una solicitud de conexión; esto mediante una petición de sesión SMPP sobre la red. Dicho de otra manera, una conexión es una petición de entrada al SMSC con la cual se puede autentificar a la ESME que solicitó la conexión. La ESME puede realizar una solicitud de conexión TX, RX o TRX; esto definirá el valor

asignado al PDU. En dado caso el SMSC no soportara alguna sesión, deberá informar a la ESME con una respuesta de “ID de comando inválido”.

Los PDU utilizados para solicitar el inicio de sesión, deben contener en la parte del cuerpo del PDU los siguientes campos:

- System_ID: este campo tiene una longitud máxima de 16 octetos en formato cadena de octetos-c. El System_ID es un identificador único de cada ESME. Cuando se intenta levantar una conexión, el SMSC verifica dentro de su tabla de ESME válidos, si este está autorizado para iniciar una sesión.

- *Password:* este campo tiene una longitud máxima de 9 octetos en formato cadena de octetos-c. El *password* es utilizado por el SMSC para autentificar la validez de la ESME que intenta levantar una sesión.

- System_Type: este campo tiene una longitud máxima de 13 octetos en formato cadena de octetos-c; sirve para identificar al tipo de ESME.

- Interface_version: este campo tiene una longitud máxima de 1 octeto en formato entero, indica la versión del protocolo SMPP soportado por la ESME de inicio.

- Dir_ton: este campo tiene una longitud máxima de 1 octeto en formato entero, indica el tipo de número de la dirección de la ESME.

- Dir_npi: este campo tiene una longitud máxima de 1 octeto en formato entero, indica el plan de numeración de la dirección de la ESME.

- Direction_range: este campo tiene una longitud máxima de 41 octetos en formato cadena de octetos-c y sirve para indicar la dirección lógica de la ESME.

- Una vez enviado el PDU de solicitud de inicio de sesión, si el SMSC inicia la sesión con la ESME, se envía un acuse de recibo, el cual únicamente contiene el System_Id y un campo de estado.

El proceso de desconexión consiste en indicarle al SMSC que la ESME ya no desea envíar y recibir mensajes; con esto se indica que la conexión lógica ya no es necesaria y que se puede proceder al cierre de la misma y a la eliminación de parámetros temporales necesarios para mantener la conexión establecida.

3.6. Envío de mensajes SMS

Una vez establecida una conexión entre la ESME y el SMSC, es posible iniciar con el envío de mensajes SMS. Para realizar esta operación, es necesario enviar un PDU con el comando es enviar_sm; dentro del cuerpo del mensaje se incluyen los comandos tipo_servicio, dir_origen_ton, dir_origen_npi, dir_origen, dir_dest_ton, dir_dest_npi, dir_destino, clase_esm, id_protocolo, flag_prioridad, hora_entrega, periodo_validez, registro_entrega, flag_sustituit, códigos_datos, id_sm_defecto, longitud_sm, mensaje_corto.

El campo hora_entrega indica la hora a la que debe ser enviado el SMS; si la entrega debe ser inmediata el valor de este campo es NULL. El campo periodo_validez indica el periodo durante el cual el SMS es válido, una vez expirado este tiempo el SMS es eliminado. El campo código_datos define el esquema de codificación del SMS. El campo longitud_sm indica la longitud en

octetos que tiene el mensaje y el campo mensaje_corto es el de información contenida en el mensaje, es decir, el texto que le llegará al usuario final.

Una vez realizada la solitud de envío de mensaje, el SMSC redactar un acuse de recibo; este PDU únicamente contiene el parámetro id_mensaje, que es un parámetro asignado por el SMSC al mensaje, para luego poder acceder a información del mismo (estado, hora y fecha en entrega, entre otros).

Si se desea enviar un SMS a múltiples destinos, se debe sustituir el comando enviar_sm por enviar_multi. Para el PDU de solicitud de envío lo único que cambia, en relación con un envío simple, es la cantidad de destinatarios y las direcciones de los mismos. Las direcciones de destino van incluidas dentro del parámetro dir_destino. En cuanto al PDU de respuesta enviado por el SMSC, se agregan dos campos adicionales: el primero que indica el número de direcciones a las cuales no se les pudo entregar el SMS y el segundo que especifica estas direcciones.

Una característica muy utilizada por los diferentes ESME es la opción de cambiar el mecanismo de envío de mensajes. El protocolo SMPP ofrece 3 mecanismos que son: almacenar y enviar, datagrama y modo transacción. El modo por defecto es la forma de almacenar y enviar, el cual permite almacenar el SMS en una base de datos antes de ser enrutado y enviado a su destino final; con esto se logra mantener el SMS a salvo, independientemente de su estado actual.

3.7. Verificación de conexión

Una de las ventajas del protocolo SMPP radica en la posibilidad de verificar la estabilidad de la conexión establecida; esto se realiza mediante el

comando estatus_conexion. El SMSC, al recibir este comando, debe responder con el comando estatus_conexion_resp, el cual indica que a nivel de aplicativo, la conexión entre la ESME y el SMSC se encuentra activa, estable y funcionando de manera normal. EL PDU de verificación solo contiene encabezado en el cual se indica el ID del comando enviado.

4. PROPUESTA DEL SISTEMA AUTOMÁTICO PARA DETECCIÓN DE DESCONEXIONES EN LAS CUENTAS SMPP

Para que un mensaje SMS pueda ser enviado se debe establecer una conexión SMPP entre la EMSE y el SMSC, un error muy común en telecomunicaciones es la desconexión de cuentas SMPP, esto conlleva a que los mensajes SMS no puedan ser entregados inmediatamente e ingresen a un sistema de reintentos de envíos específicos.

4.1. ¿Qué es un *script*?

Un *script* es un archivo de texto plano el cual almacena órdenes o instrucciones para ejecutar una determinada tarea. Normalmente, se define que un *script* es un programa de código sencillo o un programa a escala pequeña. Los *scripts* son utilizados habitualmente para realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario. Por este uso es frecuente que los programas de tipo *shell* sean capaces de interpretar este tipo de programas.

Para identificar un script de un archivo de texto normal, basta con revisar las primeras líneas de instrucciones del archivo, ya que los *script* siempre inician con uno de los siguientes encabezados:

- #!/bin/bash.
- #!/bin/ksh
- #!/bin/csh

Otra forma de identificar un *script* es mediante su extensión; para los sistemas operativos basados en Unix la extensión nominal es .sh, aunque el uso de esta extensión puede ser no necesario, ya que los *shells* interpretan su encabezado.

Un intérprete *shell* es mejor conocido como un intérprete de comandos, el cual consiste en una interfaz tradicional de los sistemas operativos basados en Unix. Mediante las instrucciones contenidas en el *script*, el usuario puede comunicarse con el núcleo y por extensión, ejecutar dichas instrucciones, así como herramientas que le permiten controlar el funcionamiento del servidor.

En la programación de *shell* existen variables, las cuales son nombres simbólicos para determinadas zonas de memoria que se utilizan para almacenar datos que pueden servir durante la ejecución de las instrucciones. Una de las desventajas de estas variables es que no tiene un tipo definido como suele suceder en lenguajes de alto nivel. Para realizar operaciones aritméticas básicas como sumas y restas, existe una instrucción especial (expr.). Esta instrucción debe recibirla cada número u operando como un parámetro independiente.

Las variables no son declaradas y siempre se inicializan con valores vacíos o nulos, es decir no deben contener ningún carácter; esto incluye los espacios en blanco. Cuando se asigna un valor a cada variable no se debe dejar ningún espacio entre el signo de igual (=) y el valor asignado. Cuando se realiza un llamado a alguna variable, se debe utilizar el signo dólar ($) antes del nombre de la variable. Si se desea limpiar el valor de una variable se debe realizar mediante el comando unset.

Para realizar un comentario o aclaración dentro de la sintaxis del *script* se utiliza el símbolo #. Al momento de introducir el # todo lo que venga después y hasta el próximo carácter de nueva línea, se toma como comentario y no se ejecuta. Los *scripts* normalmente se inician con comentarios que indican el nombre de archivo y una breve descripción de la función realizada por el *script.* Las aclaraciones se colocan en diferentes partes del *script* y sirven para mejorar la comprensión del código. Un caso especial es el uso de # en la primera línea para indicar el intérprete con que se ejecutará el *script.*

Se puede desviar la entrada-salida de cualquier comando, de forma que estos puedan leer o escribir sus datos en un archivo, en la pantalla o en cualquier otro dispositivo, sin que sea necesario el cambio de alguna línea del código fuente.

La programación de *script* permite el uso de metacaracteres para representar de forma simplificada conjuntos amplios de nombres de ficheros, cuyos nombres encajan en un cierto patrón. Los metacaracteres existentes son:

- *. Este caracter se utiliza para indicar que el resto de la sentencia concuerda con cualquier cadena de caracteres, incluida la cadena vacía.
- ?. Este caracter se utiliza para indicar que el resto de la sentencia concuerda con un solo carácter.
- [a1a2... an], se utiliza para indicar que la sentencia concuerda con cualquiera de los caracteres entre los corchetes. Se puede especificar un rango separando el caracter inicial y final del mismo mediante un guion.
- [!a1a2 ... an], se utiliza para indicar que la sentencia concuerda con cualquier caracter que no esté incluido dentro de los corchetes. Es posible especificar rangos de caracteres usando el guion.

Dentro de la sintaxis del *script* se reservan algunos caracteres para uso propio del intérprete. Algunos de estos caracteres reservados no se utilizan frecuentemente dentro de la escritura, pero otros caracteres son de uso frecuente y se necesita la utilización de un mecanismo que nos permita impedir que *Shell* interprete el carácter con su significado especial. El mecanismo consiste en escribir los caracteres entre comillas simples o dobles. Con esto todo lo que escribamos entre comillas se interpretará literalmente, esto quiere decir que, si aparece un * se interpretará como el carácter asterisco y no como la lista de todos los nombres ficheros en el directorio actual. Otra forma de interpretar los que está dentro de las comillas es descifrar literalmente los meta caracteres, mientras que las variables serán sustituidas por sus valores.

Los *pipes* son comandos que proporcionan un método para utilizar la salida de un comando como entrada de otro. Existen ocasiones en las que, lo que realmente se necesita es usar la salida de uno o varios comandos como parámetros para ejecutar otro comando, no como su entrada; para estos casos es posible utilizar la técnica conocida como sustitución de un comando por su salida. Esto se consigue ejecutando el comando entre tildes graves (`) y toda la información que muestre en su salida estándar sustituirá a la cadena entre las tildes graves. Es posible combinar tantas sustituciones de comando como sean precisas.

Las secuencias son sentencias que permiten ejecutar varios comandos de forma inmediata. Otro método que se puede utilizar para la ejecución inmediata de varios comandos es separándolos con el símbolo ||. El intérprete ejecuta los comandos especificados hasta que uno de ellos no falle.

Dentro de la sintaxis del *script* existe la posibilidad de utilizar vectores de valores; utilizando una sintaxis con corchetes para los subíndices. Los vectores

tienen la limitante que el índice de los mismos debe estar entre 0 y 511, por lo que tan solo es posible declarar vectores de hasta 512 componentes. Para acceder a todos los elementos del vector de forma conjunta se utiliza la notación ${v[*]}.

Existe la posibilidad de realizar operaciones aritméticas básicas mediante el uso del comando let. Cuando se utiliza este comando sobre una expresión aritmética devuelve el resultado de la operación aritmética. Los operadores aritméticos que pueden ser utilizados se muestran en la tabla IV.

Tabla IV. **Operadores lógicos**

Operador	Significado
!	Negación lógica
*	Multiplicación
/	División
%	Resto
+	Suma
-	Resta
<= >= < >	Operadores racionales
==	Igual
!=	Desigual
&&	Y lógico
||	O lógico

Fuente: elaboración propia.

Todos los operadores aritméticos son asociativos por la izquierda. Las expresiones pueden usar paréntesis para modificar el orden de evaluación, pero en ningún momento se comprueba si alguna de ellas produce algún tipo de desbordamiento.

Existen rutinas que son subprogramas que ejecutan una acción determinada, estas rutinas pueden ser usadas en varios *scripts*. Para llamar a una rutina se debe escribir su nombre seguido de los parámetros adecuados, exactamente igual que si se estuviera ejecutando cualquier otro comando. Por norma general, conviene escribir todas las rutinas en ficheros a los que es preciso dar permiso de ejecución utilizando el comando *chmod*. No es necesario declarar la rutina de forma especial para indicar que admite parámetros; y tampoco se realiza ningún tipo de comprobación en cuanto al número de parámetros reales que se utilizan en la llamada hecha a la rutina.

Para acceder al parámetro i– ésimo de una rutina se usa la notación $i, pero si en la llamada ese parámetro no ha sido suministrado, entonces se sustituye por una cadena vacía.

Las rutinas pueden devolver valores enteros mediante el uso del comando *return.* Este comando puede ser utilizado en cualquier punto de la rutina, provocando su terminación inmediata; por esta razón lo más adecuado es usarlo siempre al final. Para determinar cuál es el valor de retorno de cualquier rutina se puede usar la variable especial $?.

La programación de *script* cuenta con dos estructuras: la repetitiva y la alternativa. Ambas estructuras tienen sus características propias y la combinación de todas ellas generan múltiples posibilidades.

La estructura repetitiva es aquella que realiza una acción un cierto número de veces, o mientras dure una condición. La estructura alternativa es aquella en que la instrucción se realiza con base en la comprobación de una condición, se decide una acción diferente para cada caso.

4.2. Creación del *script* de ejecución

Para realizar el monitoreo automático de cuentas desconectadas, se deben realizar los siguientes pasos:

- Ejecutar el *script* principal. Dentro de este log principal se encuentran rutinas.
- Iniciar la captura de todo el texto generado durante la conexión. Se guardará en un archivo .txt
- Establecer una conexión vía shh al SMSC.
- Ingresar al directorio PML.
- Ingresar el comando para visualizar el estado de las cuentas.
- Salir del directorio.
- Cerrar la conexión vía shh.
- Terminar la captura de texto.
- Analizar el archivo de texto almacenado en busca de posibles cuentas desconectadas.
- En caso de haber cuentas desconectadas se informa vía correo electrónico sobre las mismas, de lo contrario se finaliza el proceso.

El *script* principal es el siguiente:

#!/bin/sh
El nombre del *script* es SP.sh
El nombre del *script* que realiza la conexión es SC.sh
El nombre del archivo de texto donde se guarda el registro es cuentas.txt y debe ser borrado en el inicio de cada nuevo monitoreo
El nombre del *script* que analizará el archivo de texto en busca de desconexión es SA.sh

El nombre del archivo que realiza él envío automático de los resultados es SE.sh

rm cuentas.txt

sh /home/Agodoy/SC.sh | cat >> cuentas.txt

sh /home/Agodoy/SA.sh

sh /home/Agodoy/SE.sh

#Acá finaliza el SP.sh

El *script* que ejecuta la conexión y revisión de todas las cuentas SMPP es el siguiente:

#!/bin/sh

Se realiza una conexión SHH al SMSC, el cual tiene la dirección ip 10.10.10.2

HOST=10.10.10.2

USER=”Agodoy”

PASS=”USAC2015”

CMD=$@

VAR=$(expect -c "

spawn ssh -o StrictHostKeyChecking=no $USER@$HOST $CMD

match_max 100000

expect \"*?password:*\"

send -- \"$PASS\r\"

send -- \"\r\"

expect eof

")

echo "==========="

echo "$VAR"

A partir de acá, se tiene una conexión establecida con el SMSC. Lo primero será ubicarse en el directorio de cuentas, luego se ejecuta la sentencia de visualización de cuentas.

PML

disc

conn

show cl siwsmpp /sess=(type=la,la=all)

exit

Se procede a cerrar la conexión ssh

exit

#Acá finaliza el SP.sh

El *script* que realiza el análisis del archivo de texto en búsqueda de posibles desconexiones es el siguiente:

#!/bin/sh

Se abre el archivo y se procede a realizar la búsqueda mediante el comando *grep*. Posterior a esto, los resultados de la búsqueda son almacenados en un archivo de texto para proceder a ser enviados vía correo electrónico.

rm Resultados.txt

grep –lir "Response from SIWSMPP_12 "

/home/Agodoy/cuentas.txt | cat >> Resultados.txt

Se verifica el archive Resultados.txt; si este contiene cuentas desconectadas se procede con el envío de la notificación por correo electrónico, de lo contrario se procede a finalizar la rutina.

La verificación se realiza mediante un conteo de líneas; si el conteo es igual a cero, significa que no hay cuentas desconectadas.

If ((ls Resultados.txt | wc –l) == 0) then

sh SE.sh

#Acá finaliza el SP.sh

El script que realiza el envío automático del archivo de texto que contiene los resultados es el siguiente:

#!/bin/sh

Se procede a declarar las librerías necesarias para la ejecución del programa.

use lib('lib');

use MIME::Lite;

use Net::SMTP;

my $fecha = $ARGV[0];

Acá se configura la dirección de correo del origen y el destino; como también la dirección IP del servidor de correos utilizado

my $from_address =’monitoreo@gmail.com’;

my $to_address = ‘agodoy@gmail.com’;

my $mail_host = ’10.10.172.2’;

Configuración del asunto y el cuerpo del mensaje

my $subject = "Resultado monitoreo de cuentas SMPP";

my $message_body = "Se adjunta el detalle de las posibles cuentas SMPP que presentaron desconexión durante el monitoreo. Favor revisar atentamente. \n\nSaludos Cordiales,\n\n--\n Álvaro Godoy \, “;

Se configuran los nombres de los archivos

my $my_file_xls ='/home/agodoy/Resultados.txt';

my $your_file_xls = 'Resultados.txt';

Se crea el contenedor multiparte

$msg = MIME::Lite->new (

From => $from_address,

To => $to_address,

Subject => $subject,

```
  Type =>'multipart/mixed'
) or die "Error creando el contenedor multiparte: $!\n";

# Se agrega la parte del mensaje de texto
$msg->attach (
  Type => 'TEXT',
  Data => $message_body
) or die "Error agregando la parte del mensaje: $!\n";
# Se agrega el XLS
$msg->attach (
   Type => 'application/msexcel',
   Path => $my_file_xls,
   Filename => $your_file_xls,
   Disposition => 'attachment'
) or die "Error agregando $my_file_xls: $!\n";
# Se envía el mensaje
MIME::Lite->send('smtp', $mail_host, Timeout=>60);
$msg->send;
```

4.3. Sistema final de detección de cuentas desconectadas

Ya que se tienen listos los *scripts* necesarios para la ejecución del monitoreo, se establece que la ejecución automática será una vez cada 2 horas de lunes a domingo. Esta ejecución automática se realiza mediante la tabla de asignación de tareas de Linux, mejor conocida como crontab. Para la asignación de tareas se debe realizar lo siguiente desde modo consola:

```
# Seedita el crontab de Linux
crontab –e
```

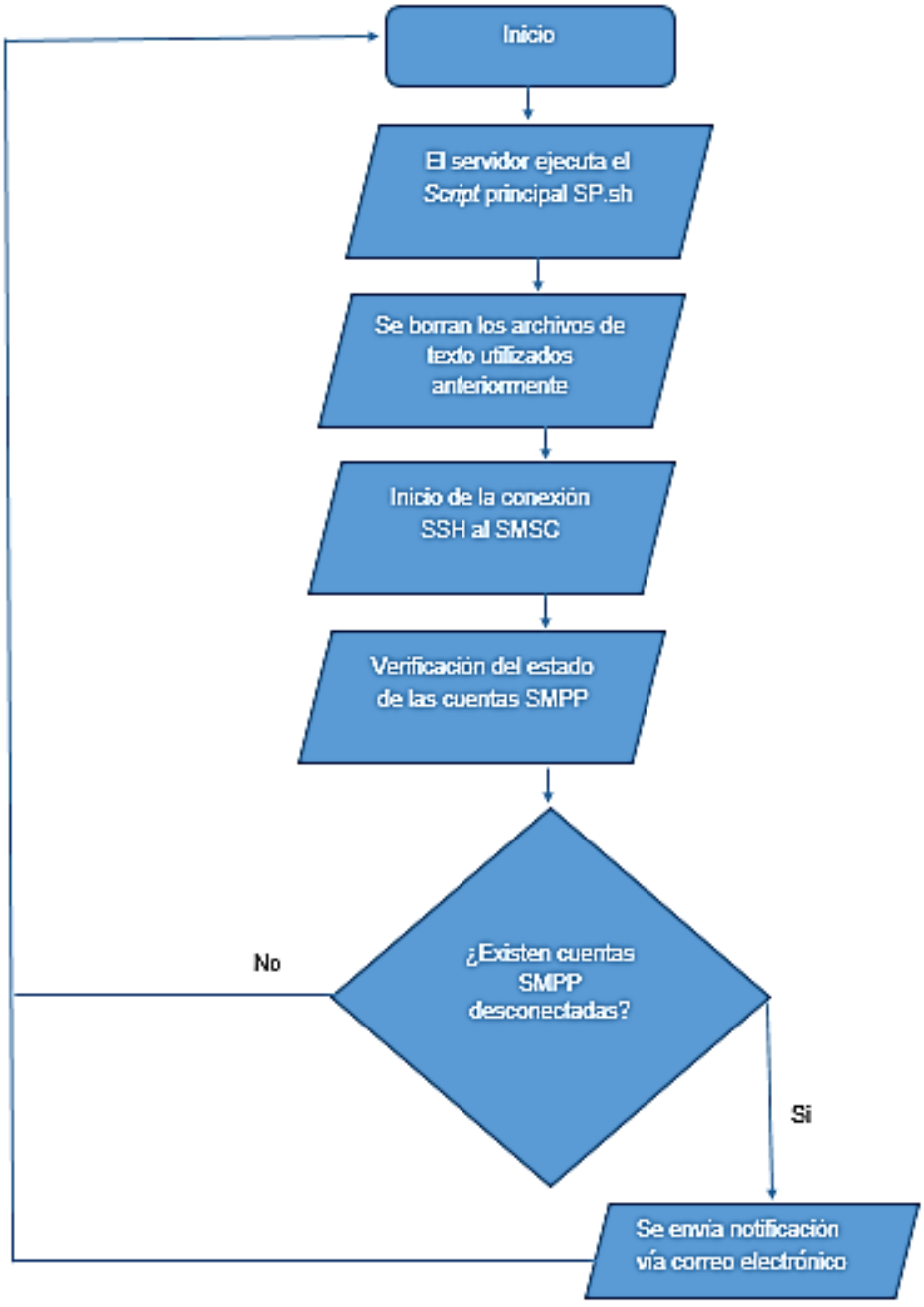
Una vez abierto el crontab, se procede con especificación de la hora y días para realizar las tareas; las tareas se ejecutarán en horas pares, a partir de la medianoche. El crontab queda de la siguiente manera:

00 00 * * * sh /home/agodoy/SP.sh
00 02 * * * sh /home/agodoy/SP.sh
00 04 * * * sh /home/agodoy/SP.sh
00 06 * * * sh /home/agodoy/SP.sh
00 08 * * * sh /home/agodoy/SP.sh
00 10 * * * sh /home/agodoy/SP.sh
00 12 * * * sh /home/agodoy/SP.sh
00 14 * * * sh /home/agodoy/SP.sh
00 16 * * * sh /home/agodoy/SP.sh
00 18 * * * sh /home/agodoy/SP.sh
00 20 * * * sh /home/agodoy/SP.sh
00 22 * * * sh /home/agodoy/SP.sh

Según se observa en el crontab, el *script* principal, el cual ejecuta todas los scripts secundarios, se ejecutará a las 00:00 am, 02:00 am, 04:00 am, 06:00 am, 08:00 am, 10:00 am, 12:00 pm, 02:00 pm, 04:00 pm, 06:00 pm, 08:00 pm, 10:00 pm.

El flujo final del proceso de monitoreo se observa en la figura 6.

Figura 6. **Diagrama de flujo sistema de monitoreo**



Fuente: elaboración propia.

5. ANÁLISIS TÉCNICO Y ECONÓMICO DEL SISTEMA PROPUESTO

El sistema automático para el monitoreo de desconexión de cuentas SMPP requiere de una mínima inversión inicial, la cual consiste únicamente en un servidor con un sistema operativo Linux, el cual será utilizado para alojar todos los *scripts* utilizados por el sistema de detección.

5.1. Inversión necesaria

Como se mencionó anteriormente, el único equipo necesario es un servidor que cuente con un sistema operativo Linux. Otra inversión a considerar es toda la infraestructura necesaria para el funcionamiento del mismo.

Para el sistema de monitoreo se puede utilizar un servidor de gama baja, ya que no se necesitarán procesos que necesiten capacidades elevadas. Para este sistema, el servidor cotizado tiene las siguientes características:

- Marca: Hewlett-Packard
- Modelo: Proliant DL360 G5
- Marca del procesador: Intel
- Modelo del procesador: Xeon
- Tipo de procesador: Quad Core
- Velocidad del procesador: 5.2 GHz
- Marca del chipset: Intel
- Modelo del chipset: 5 000P
- Tipo de memoria: DDR2

- Capacidad de memoria: 16 BG
- Capacidad máxima de memoria: 64 GB
- Tipo de disco duro: 2.5 SAS
- RPM del disco duro: 10 000
- Capacidad del disco duro: 146 GB
- DVD-Rom
- Tarjeta de video de 32 MB

Adicional se cotizó un rack Startech 12U de 19 pulgadas para su implementación física y un fuente de poder Pyle PDBC70 de 15 amperios y 1800VA para su conexión a la energía eléctrica.

En la tabla V se detallan los costos de un servidor nuevo y los periféricos necesarios para su implementación:

Tabla V. **Costo implementación**

Elemento	**Precio unitario**	**Elementos necesarios**	**Costo total**
HP Proliant DL360	Q3 000,00	1	Q 3 000,00
Rack Startech	Q 400,00	1	Q 400,00
Pyle PDBC70	Q 520,00	1	Q 520,00
Cableado de red	NA	NA	Q 1 000,00
Mano de obra	NA	NA	Q 2 500,00
TOTAL INVERSIÓN			Q 7 420,00

Fuente: elaboración propia.

Como se observó, el costo de la implementación del sistema es aproximadamente Q7 420,00, con esta inversión se logra poner en funcionamiento todo el sistema de detección de desconexiones de cuentas SMPP.

5.2. Análisis inversión versus pérdidas generadas por desconexiones

Las empresas de telecomunicaciones ven en su servicio de mensajería de texto una gran fuente de ingresos, ya que en la actualidad es uno de los servicios de valor agregado que mayor rentabilidad y popularidad presenta. Una desconexión de cuentas le presenta a la empresa de telecomunicación pérdidas debido a que los clientes no pueden enviar y recibir mensajes. Suponiendo que este servicio fuera por 1 hora, durante este periodo se pueden perder aproximadamente 100 000 mensajes SMS, solo en una hora, suponiendo una afectación masiva de 6 horas, se habrán perdido más de 600 000 mensajes SMS, suponiendo un costo unitario de Q 0, 10, la empresa habrá perdido un aproximado de Q 60 000 solo por la desconexión de cuenta SMPP.

Este dato se puede ver aumentado dependiendo de factores como la hora de la desconexión, el día de la semana, y si es un día con celebración especial (como el Día de la Madres).

Tomando en cuenta el dato anterior, se observa que si la empresa implementa el sistema de detección automática se puede estar ahorrando más de Q 10 000 por una afectación de una hora, con una inversión inicial de tan solo Q 7 420,00.

Según los datos anteriores se observa que la implementación del sistema es factible, ya que representa una pequeña inversión inicial comparada con los beneficios que representa tanto a nivel de calidad como de economía.

CONCLUSIONES

1. El servicio de mensajería SMS permitió un avance en las tecnologías de comunicación entre persona, por tal razón, el sistema aún se mantiene vigente.

2. Para incluir el servicio de mensajería de texto, dentro de una red 3G, únicamente se debe añadir a la arquitectura un SMCS interconectado con una MSC.

3. El protocolo SMPP estandariza una manera confiable, rápida y eficaz para la transmisión bidireccional de un SMS, entre una ESME y el usuario final.

4. Un *script* general puede manejar *scripts secundarios*; con esta facilidad se logran realizar varios procedimientos de manera rápida y ordenada.

5. El sistema de detección propuesto representa un beneficio para las empresas de telecomunicaciones, ya que por una inversión mínima, garantizan que una falla en el servicio no durará más de una hora sin ser detectada.

RECOMENDACIONES

1. Dentro de la estructura del *script* se debe tener una línea de limpieza de variables y archivos, la cual estará antes de la ejecución del programa; esto garantiza que los datos obtenidos son correctos.

2. A todos los *scripts* generados se les debe dar permiso de ejecución; sin estos permisos puede que el programa no funcione correctamente.

3. El servidor indicado necesita estar conectado a un *rack* que tenga una conexión a tierra física, para protección de los datos almacenados y los datos instantáneos de medición de desconexiones.

BIBLIOGRAFÍA

1. AJAR, Mishra. *Advanced Cellular Network Planning and Optimisation: 2G/2.5G/3G…Evolution to 4G*. Estados Unidos: WILEY, 2006. 542 p. ISBN: 978-0-470-01471-4.

2. HERNÁNDEZ PALMA, Hugo Gaspar. *Tecnologías de la información y las comunicaciones*. Colombia: EDUCOSTA, 2010. 751 p. ISBN: 978-958-8710-60-0.

3. HUIDOBRO MOYA, José Manuel. *Comunicaciones móviles. Sistemas GSM, UMTS y LTE*. España: Ra-ma Editorial, 2012. 428 p. ISBN: 978-84-9964-129-4.

4. LABORDERE, Arnaud Henry. *SMS and MMS Interworking in Mobile Networks.* Estados Unidos: Artech House, 2003. 350 p. ISBN: 978-1-58053-890-9.

5. LAITINEN, Lauri. *Redes UMTS. Arquitectura, movilidad y servicios*. España: Ra-ma Editorial, 2006. 584 p. ISBN: 978-84-7897-709-3.

6. MONTES CORRALES, Piter. *Pasarela de intercambio de mensajes: entre los protocolos CIMD y SMPP.* España: Editorial Académica Española, 2011. 425 p. ISBN: 978-3-84549-245-4.

7. NIXON, Robin. *Learning PHP, MYSQL, and Java Script.* Estados Unidos: O'Reilly, 2009. 505 p. ISBN: 978-0-596-15713-5.

8. PIERRE LESCUYER, Thierry Lucidarme. *Evolved Packet System (EPS). The LTE and SAE evolution of 3G UMTS.* Estados Unidos: WILEY, 2008. 350 p. ISBN: 978-0-470-05976-0.

9. QTC. *3GPP TS 29* [en línea]. <http://www.qtc.jp/3GPP/Specs/29002-910.pdf>. [Consulta: 15 de enero del 2015].

10. ROBBINS, Arnold. *Classic shell scripting.* Estados Unidos: O'Reilly Media, 2005. 560 p. ISBN: 978-0-596-00595-5.

11. SASSAN, Ahmadi. *LTE-Advanced: A practical system approach to understanding 3GPP LTE releases 10 and 11 Radio Access Technologies.* Estados Unidos: WILEY, 2008. 350 p. ISBN: 978-0-470-05976-0.

12. 3G TS 23.039 V2.0.0 [en línea]. <http://www.3gpp.org/ftp/tsg_t/tsg_t/tsgt_04/docs/pdfs/TP-99128.pdf>. [Consulta: 14 de agosto del 2015].