



**UNIVERSIDAD MICHOACANA DE  
SAN NICOLÁS DE HIDALGO**



**FACULTAD DE INGENIERÍA ELÉCTRICA**

# **Descripción e instalación de una estación base de telefonía celular en una PC portátil utilizando SDR**

Tesis para obtener el título profesional en Ingeniero en Electrónica

**Geovanni Madrigal Lucatero**

**Matricula 1175781j**

[GeovanniMadrigalLucatero@gmail.com](mailto:GeovanniMadrigalLucatero@gmail.com)

**Asesor**

**M.C. Félix Jiménez Pérez**

[jfelix@fie.umich.mx](mailto:jfelix@fie.umich.mx)

Morelia Michoacán - México

Agosto 2019

## AGRADECIMIENTOS

Agradezco a mis padres y hermanos por acompañarme en los buenos y malos momentos vividos durante mi carrera universitaria, en especial quiero agradecer a mi hermano Armando por apoyarme desde el inicio de la carrera, siendo mí maestro en momentos de dudas. También agradezco a todos esos amigos que hicieron que mi estadía en la facultad fuera más divertida y sencilla. Por último, quiero agradecer a mi asesor de tesis M.C. Félix Jiménez por el tiempo, dedicación y paciencia para la elaboración de este documento, dándome las herramientas necesarias para culminar con mi investigación y plasmar mis ideas.

## DEDICATORIA

Este documento se lo dedico a mis amigos, familiares, y profesores que estuvieron a lo largo de mi vida académica.

# ÍNDICE

AGRADECIMIENTOS .....	II
DEDICATORIA .....	III
ÍNDICE.....	IV
RESUMEN .....	VII
PALABRAS CLAVE .....	VIII
ABSTRACT.....	IX
KEYWORDS .....	X
LISTA DE FIGURAS .....	XI
LISTA DE TABLAS .....	XIV
CAPÍTULO 1 INTRODUCCIÓN.....	1
1.1 ANTECEDENTES .....	1
1.2 OBJETIVOS.....	2
1.3 JUSTIFICACIÓN .....	2
1.4 METODOLOGÍA .....	3
CAPITULO 2 CONCEPTOS DE TELEFONÍA CELULAR .....	4
2.1 CONCEPTOS DE TELECOMUNICACIONES INALÁMBRICAS.....	4
2.1.1 Modulación.....	5
2.1.2 Control de acceso al medio.....	8
2.2 HISTORIA DE LA TELEFONÍA CELULAR .....	12
2.2.1 Antecedentes de telefonía celular.....	12
2.2.2 Inicio de la telefonía celular .....	14
2.2.3 Telefonía celular en México .....	18
2.3 CONCEPTOS BÁSICOS DE LA RED DE TELEFONÍA CELULAR .....	19
2.3.1 La célula.....	19
2.3.2 Propiedades de la Geometría Celular .....	19
2.3.3 Célula omnidireccional .....	21
2.3.4 Célula sectorial.....	21
2.3.5 Clasificación de células o celdas .....	23
2.3.6 Diseño de células.....	24

2.4 EVOLUCIÓN DE LOS SISTEMAS DE TELEFONÍA CELULAR .....	31
2.4.1 Primera Generación (1G) .....	31
2.4.2 Segunda Generación (2G) .....	32
2.4.3 Tercera Generación (3G) .....	34
2.4.4 Cuarta Generación (4G) .....	36
2.4.5 Quinta Generación (5G) .....	36
2.5 ARQUITECTURA DE LA RED DE TELEFONÍA CELULAR GSM.....	37
2.5.1 Estación Móvil (MS) .....	37
2.5.2 Subsistema de Estación Base (BSS) .....	39
2.5.3 Subsistema de conmutación de red (NSS) .....	41
2.5.4 Subsistema de operación y mantenimiento (OSS) .....	43
2.5.5 Sistema de conmutación de red pública (PSTN).....	44
2.6 PROTOCOLOS E INTERFACES DE LA ARQUITECTURA GSM .....	44
2.6.1 Modelo de Referencia OSI.....	44
2.6.2 Interfaces de la red GSM. ....	46
2.6.3 Protocolos y señalización en la red GSM. ....	49
2.7 RED DE ACCESO. INTERFAZ AIRE. ....	52
2.7.1 Canalización GSM .....	53
2.7.2 Ráfagas GSM .....	58
2.7.3 Modulación GMSK .....	62
2.8 Handover.....	64
CAPÍTULO 3 DISPOSITIVOS SDR.....	68
3.1 CONCEPTO DE SDR.....	68
3.2 APORTACIONES DEL SDR.....	70
3.3 EQUIPOS SDR EN EL MERCADO. ....	70
3.4 LimeSDR en su versión mini.....	76
3.4.1 Transceptor RF: Lime mycosystemsLMS7002M .....	77
3.4.2 FPGA: Intel Altera MAX 10 (10M16SAU169C8G) .....	84
3.4.3 USB 3.0 .....	85
CAPÍTULO 4 CONFIGURACIÓN DE UNA ESTACIÓN BASE GSM .....	88
4.1 LIMESUITE.....	88
4.1.1 LMS7 Drivers .....	90

4.1.2 Board support .....	90
4.1.3 Lime Suite GUI.....	91
4.1.4 SDR interfaces.....	92
4.2 LIBOSMOCORE.....	95
4.3 OSMO-TRX-LMS.....	96
4.4 OSMO-NITB Y OSMO-BTS. ....	97
4.5 ARCHIVOS DE CONFIGURACIÓN.....	104
<b>CAPÍTULO 5 PRUEBAS Y RESULTADOS.....</b>	<b>110</b>
5.1 EJECUCIÓN DE LA ESTACIÓN BASE GSM. ....	110
5.1.1 Ejecución de Osmo-TRX.....	111
5.1.2 Ejecución de OsmoNitb.....	113
5.1.3 Ejecución de OsmoBTS. ....	114
5.2 CONFIGURACIÓN DEL TELÉFONO CELULAR. ....	115
5.3 PRUEBAS .....	117
5.3.1 Llamadas de voz. ....	118
5.3.2 SMS .....	119
5.3.3 Base de datos .....	120
<b>CAPÍTULO 6 CONCLUSIONES Y TRABAJOS FUTUROS.....</b>	<b>124</b>
<b>GLOSARIO DE TÉRMINOS.....</b>	<b>126</b>
<b>BIBLIOGRAFÍA.....</b>	<b>134</b>

## RESUMEN

En esta tesis se exponen las herramientas de hardware y software necesarias para implementar una estación base GSM. Se utilizan las aplicaciones de OSMOCOM dedicadas al desarrollo de software para telefonía celular donde incluyen el estándar GSM. En la parte de Hardware se utilizó una PC portátil, para instalar las aplicaciones de OSMOCOM, y el dispositivo limeSDR en su versión mini fabricado por la empresa Microsystems. Se explica de manera detallada cada uno de los elementos que contiene el sistema para comprender el funcionamiento de las redes de telefonía celular que tienen gran importancia en la actualidad. Además se realizan una serie de pruebas sobre la conexión a la estación base, el envío de SMS y la comunicación por llamadas de voz entre dos usuarios.

## PALABRAS CLAVE

- Telefonía celular
- SDR
- 2G
- Estación base
- GSM
- LimeSDR
- Osmocom
- Osmo-NITB

## ABSTRACT

This thesis describes the hardware and software tools necessary to implement a GSM base station. OSMOCOM applications dedicated to the development of software for cellular telephony where the GSM standard is included are used. In the Hardware part, use a portable PC, to install the OSMOCOM applications, and the limeSDR device in its mini version manufactured by Microsystems. Each of the elements contained in the system is explained specifically to understand the operation of the cellular telephone networks that are of great importance today. In addition, a series of tests were sent on the connection to the base station, the sending of SMS and the communication by voice calls between two users.

## KEYWORDS

- Telefonía celular
- SDR
- 2G
- Base station
- GSM
- LimeSDR
- Osmocom
- Osmo-NITB.

## LISTA DE FIGURAS

Figura 1 Modelo básico de un sistema de comunicaciones [2].....	4
Figura 2 Sistema de Modulación [4] .....	6
Figura 3 Ejemplo de modulación AM y FM [5] .....	6
Figura 4 Ancho de Banda [4].....	7
Figura 5 Clasificación de los tipos de Modulación. ....	8
Figura 6 FDMA.....	9
Figura 7 Códigos ortogonales .....	10
Figura 8 CDMA .....	11
Figura 9 TDMA.....	12
Figura 10 Conjunto de Células unidad en una red Celular .....	19
Figura 11 Ejemplo de una geometría circular. ....	20
Figura 12 Tipos de Geometría celular usados.....	20
Figura 13 Célula omnidireccional .....	21
Figura 14 Estación Base cubriendo tres células, para crear un sector .....	22
Figura 15 Formación de una célula sectorial a partir de 3 BS [10].....	22
Figura 16 Torre con antenas sectoriales [10] .....	23
Figura 17 Clasificación de las células [12].....	24
Figura 18 Cluster. Cada letra representa una célula con características diferentes. ....	25
Figura 19 Representación del concepto de reutilización de frecuencia .....	26
Figura 20 Patrón k=4 .....	27
Figura 21 Patrón k=7 .....	28
Figura 22 División de sistema celular en células más pequeñas .....	29
Figura 23 Evolución de la telefonía celular. [15] .....	37
Figura 24 Arquitectura de una red celular 2G GSM.....	37
Figura 25 Imagen de SIM [16].....	38
Figura 26 Formatos de tarjeta SIM [17] .....	39
Figura 27 Hardware y servicios que utiliza una estación base. ....	40
Figura 28 Pequeño Subsistema de estación base. [20].....	41
Figura 29 Subsistema de conmutación de red NSS .....	42
Figura 30 Centro de Conmutación Móvil [23] .....	42
Figura 31 Esquema funcional de las capas del modelo OSI [28].....	44
Figura 32 Esquema de interfaces en el sistema GSM [28] .....	47
Figura 33 Torre de protocolos GSM. [28] .....	49
Figura 34 Protocolos MAP/X [28] .....	52
Figura 35 Distribución de los canales GSM.....	53
Figura 36 Control multitráma [30] .....	58
Figura 37 Estructura de la ráfaga normal. [30] .....	59
Figura 38 Estructura de la ráfaga de corrección de frecuencia. [30] .....	59
Figura 39 Estructura de la ráfaga de sincronización. [30] .....	60
Figura 40 Estructura de la ráfaga de acceso. [30] .....	61
Figura 41 Tramas usadas en GSM [30].....	62

Figura 42 Diagrama de bloques del transmisor GMSK.....	63
Figura 43 Señal de modulación GMSK [32] .....	63
Figura 44 Handover .....	64
Figura 45 Resource Management Criteria Handover .....	66
Figura 46 Concentric Cell Structure Management .....	67
Figura 47 Extended Cell Handover .....	67
Figura 48 Concepto de radio definida por software. [33] .....	69
Figura 49 HackRF One [34] .....	71
Figura 50 Ettus B200 [35].....	72
Figura 51 Ettus B210 [35].....	72
Figura 52 BladeRF x40 [36] .....	73
Figura 53 LimeSDR [37].....	74
Figura 54 LimeSDRmini [38] .....	75
Figura 55 Comparación entre los dispositivos SDR económicos del mercado [38] .....	76
Figura 56 Diagrama de bloques del LimeSDR mini [38] .....	77
Figura 57 Diagrama de bloques del LM7002M [40] .....	78
Figura 58 Etapa de amplificación en el receptor. [40].....	79
Figura 59 Etapa de filtrado en el receptor. [40].....	80
Figura 60 Respuesta de amplitud analógica RX LPF [40] .....	80
Figura 61 Convertidor Analógico Digital.....	81
Figura 62 Convertidor DAC en el LM7002M.....	81
Figura 63 Etapa de amplificación en la transmisión. [40].....	82
Figura 64 Arquitectura PLL [40] .....	83
Figura 65 Parte TSP del LMS7002M [40].....	83
Figura 66 Estructura de una FPGA [42] .....	84
Figura 67 Diagrama de bloques del FTDI FT601 [44].....	86
Figura 68 Diagrama de bloques completo del dispositivo LimeSDR mini .....	87
Figura 69 Control de versiones distribuido [46] .....	89
Figura 70 Componentes de los controladores de LimeSuite [51] .....	90
Figura 71 Interfaz gráfica de limesuite GUI .....	91
Figura 72 Menú de limesuiteGUI.....	92
Figura 73 Actualización del firmware de la FPGA .....	92
Figura 74 Interfaz gráfica de GQRX [53] .....	93
Figura 75 Interfaz gráfica de PhotosGUI .....	93
Figura 76 Interfaz gráfica de CubicSDR [54] .....	94
Figura 77 Interfaz gráfica de GNURADIO .....	94
Figura 78 Pila de protocolos sobre la interfaz Abis. [62].....	98
Figura 79 Arquitectura GSM utilizando OSMONITB [63] .....	98
Figura 80 RTP proxy entre BTS [63] .....	99
Figura 81 RTP Proxy entre BTS y BSC [63].....	100
Figura 82 Diagrama de bloques del sistema implementado .....	101
Figura 83 Proceso realizado durante la conmutación de una llamada [30].....	102

Figura 84 Tramas de SMS-SUBMIT .....	102
Figura 85 SCA .....	103
Figura 86 PDU-TYPE .....	103
Figura 87 DA .....	103
Figura 88 UD .....	104
Figura 89 Trama completa del SMS .....	104
Figura 90 Ejecución del comando para ver los puertos utilizados. ....	110
Figura 91 Puertos utilizados.....	110
Figura 92 Comando para matar procesos en ejecución. ....	111
Figura 93 Ejecución de osmo-trx.....	112
Figura 94 Información del dispositivo limeSDR mini.....	112
Figura 95 Información de que el transceiver está activo.....	113
Figura 96 comando para ejecutar OsmoNITB .....	113
Figura 97 Inicialización de los protocolos de comunicación y la base de datos..	114
Figura 98 Ejecución de osmoBTS .....	114
Figura 99 Terminales ejecutando la arquitectura de una BTS GSM .....	115
Figura 100 Acceder a las configuraciones del dispositivo móvil .....	115
Figura 101 Acceder redes móviles. ....	116
Figura 102 Selección de la red.....	117
Figura 103 Código para solicitar número de extensión.....	117
Figura 104 número de extensión solicitado. ....	118
Figura 105 Prueba de una llamada. ....	118
Figura 106 Llamada entre dos extensiones.....	119
Figura 107 Prueba del envío de un SMS. ....	119
Figura 108 Base de datos .....	120
Figura 109 Menú de las tablas en la base de datos. ....	120
Figura 110 Contador de llamadas. ....	121
Figura 111 Tabla de equipos que se conectaron.....	121
Figura 112 Tabla sobre el servicio de SMS 1 .....	122
Figura 113 Tabla sobre el servicio de SMS 2 .....	122
Figura 114 Resumen de los datos de la base de datos.....	123

## LISTA DE TABLAS

Tabla 1 Clasificación de las células con radios de cobertura.....	24
Tabla 2 Conexiones de la tarjeta SIM .....	38
Tabla 3 Información de tamaños relacionados con los diferentes formatos de SIM .....	39
Tabla 4 Resumen de las principales interfaces en una red GSM [28] .....	51
Tabla 5 Características generales del protocolo GSM [28].....	53

# CAPÍTULO I

## INTRODUCCIÓN.

El teléfono celular se ha convertido en un dispositivo de comunicación indispensable en la vida cotidiana de la mayoría. Un teléfono celular te permite hacer llamadas y enviar mensajes desde cualquier parte del mundo con recepción de estación base celular.

En la actualidad existe gran cantidad de empresas de telefonía celular que ofrecen gran variedad de tarifas accesibles para el público en general. Además, un celular es una herramienta poderosa de procesamiento donde puedes tener un reproductor de video y audio, una cámara fotográfica y un sinfín de aplicaciones que son herramientas para muchas de las actividades que realizamos.

Las empresas de telefonía celular invierten una gran cantidad de recursos para adquirir los equipos utilizados en la infraestructura de una red celular, además las empresas no dan la suficiente información del diseño de los equipos, solo te proporcionan información técnica suficiente para la instalación.

LimeSDR es una plataforma de radio definida por software (SDR) de bajo costo, de código abierto, habilitada para aplicaciones que puede usarse para soportar casi cualquier tipo de estándar de comunicación inalámbrica. LimeSDR puede enviar y recibir información usando los siguientes protocolos UMTS, LTE, GSM, LoRa, Bluetooth, Zigbee, RFID y Digital Broadcasting, entre otros. [1]

En el presente proyecto de tesis se implementó una red celular 2G (GSM) con el dispositivo LimeSDR, dando una explicación detallada del funcionamiento de hardware y software utilizados.

### 1.1 ANTECEDENTES

En junio del 2018 fue lanzado al mercado un dispositivo LimeSDR Tipo A el cual puede soportar casi cualquier tipo de estándar de comunicación inalámbrica. Este dispositivo fue pensado para estudiantes y desarrolladores que desean manipular señales de radio frecuencia, para poder aprender y experimentar sin costos extremadamente altos.

Además de la creación de este dispositivo, en noviembre del 2018 fue presentado en el Tecnológico Nacional de México en Celaya, **Implementación de red celular de bajo costo para comunidades rurales basada en SDR y OPENBTS** por Hugo Andrés Pérez Guerrero, Dulce Mayra Janet Martínez García, Marco Aurelio Cárdenas Juárez, Ulises Pineda Rico, Enrique Stevens Navarro y Armando Arce Casas.

El artículo presenta la implementación de una red celular 2G utilizando transceptores de radio frecuencia de bajo costo y software de código abierto para una comunidad rural donde el acceso a un servicio de telefonía es

imposible debido a que no es económicamente factible para los operadores de una compañía de telefonía.

Este trabajo establece, la problemática para el acceso a una red celular en comunidades rurales y como solución el diseño de una red celular 2G con SDR y OPENBTS. Al final presenta los resultados obtenidos, dando a conocer la factibilidad de este proyecto.

La aparición de lime SDR y la creación del artículo de investigación antes mencionado nos lleva a planear la creación de una red celular 2G GSM con un dispositivo limeSDR y utilizando OsmoNitb.

## 1.2 OBJETIVOS

- Conocer la importancia de una red celular en la actualidad, y la evolución de esta a lo largo del tiempo.
- Presentar información de la arquitectura de una red celular.
- Instalar las aplicaciones necesarias para una red celular 2G GSM basado en Lime SDR.
- Dar a conocer las diferentes características de las generaciones de telefonía celular, dándole prioridad a la red 2G (GSM) que se implementó en el proyecto.
- Conocer los componentes electrónicos que contiene el dispositivo LimeSDR y describir cada uno de ellos, para aprovechar sus características.
- Describir el software de OSMOCOM necesario para la instalación de una red celular 2G GSM.

## 1.3 JUSTIFICACIÓN

La creación de este proyecto beneficia a todo estudiante o desarrollador en el área de telecomunicaciones ya que se ofrece gran cantidad de información necesaria para la creación de una red celular 2G, dando a conocer el equipo utilizado, la instalación de drivers y configuración de las aplicaciones proporcionadas por OSMOCOM.

Se optó por utilizar limeSDR en su versión mini por ser un dispositivo económico en comparación con otros que hay en el mercado

Otro beneficio que nos proporciona limeSDR es que la información de los componentes utilizados para la construcción del dispositivo está disponible para el público en general.

Se utilizó OsmoNitb debido a su facilidad de instalación y a la compatibilidad con limeSDR. Además de funcionar en computadoras de gama baja.

La investigación para la realización este proyecto deja un amplio conocimiento en el área de comunicaciones, y del hardware y software utilizado, se da a conocer todos los protocolos de comunicación, su funcionamiento y tipo de modulación utilizada.

## 1.4 METODOLÓGÍA

A continuación, se aborda la forma de la clasificación de los capítulos y un pequeño resumen de lo que contienen.

- **CAPÍTULO I INTRODUCCIÓN:** En este capítulo se explica sobre la importancia del proyecto de tesis, así como los antecedentes que dieron origen a la idea, también se exponen los objetivos esperados al finalizar el trabajo.
- **CAPÍTULO II CONCEPTOS DE TELEFONÍA CELULAR:** En este capítulo se da la información básica para entender el estándar de comunicaciones que se implementa en el actual proyecto. El capítulo comienza con un poco de historia sobre la evolución de la telefonía celular. Después se mencionan los componentes existentes en la arquitectura de una red celular 2G GSM. Al final del capítulo se muestran los protocolo e interfaces utilizadas en el estándar GSM.
- **CAPÍTULO III DISPOSITIVOS SDR:** Se da una explicación del concepto SDR, además se exponen los diferentes dispositivos existentes en el mercado. Se detallan las características del equipo utilizado en el proyecto de tesis, tomando en cuenta todos los componentes que vienen en la placa de desarrollo dando a conocer la funcionalidad e importancia de cada uno.
- **CAPÍTULO IV CONFIGURACIÓN DE UNA ESTACIÓN BASE GSM:** Se explica la información de las aplicaciones de OSMOCOM utilizadas, además de proporcionar una serie de comandos necesarios para su instalación, dando la facilidad de replicar o mejorar el proyecto en futuras investigaciones.
- **CAPÍTULO V PRUEBAS Y RESULTADOS:** En este capítulo se muestran como ejecutar las aplicaciones de OSMOCOM para el funcionamiento correcto de la estación base. Además de mostrar la configuración necesaria en el teléfono móvil para la conexión a la estación base.
- **CAPÍTULO VI CONCLUSIONES Y TRABAJOS FUTUROS:** es el capítulo final donde se exponen las conclusiones obtenidas al finalizar el proyecto, además de exponer los trabajos con los que se seguirá trabajando.

## CAPITULO 2

### CONCEPTOS DE TELEFONÍA CELULAR.

#### 2.1 CONCEPTOS DE TELECOMUNICACIONES INALÁMBRICAS

La Comunicación es la transferencia de información desde un lugar (remitente, fuente, transmisor) a otro lugar (destino, receptor). Por otra parte, Información es un patrón físico al cual se le ha asignado un significado comúnmente acordado. El patrón debe ser único (separado y distinto), capaz de ser enviado por el transmisor, y capaz de ser detectado y entendido por el receptor. [2]

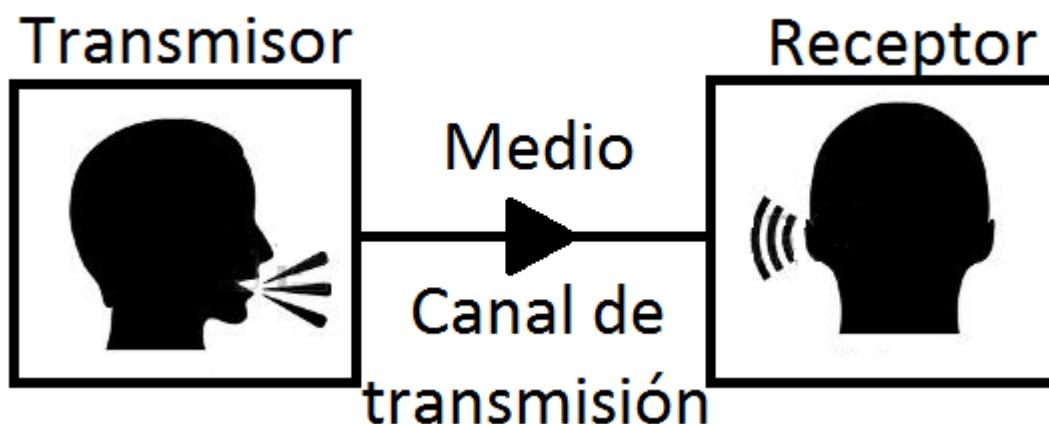


Figura 1 Modelo básico de un sistema de comunicaciones [2]

En la figura 1 se muestra un sistema de comunicación básico, ahora se explicará cada uno de ellos de manera general.

**El Transmisor:** su función es pasar el mensaje al canal en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. La más común e importante es la modulación, un proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal, por medio de una onda portadora. [2]

**El Canal de Transmisión o medio:** es el enlace eléctrico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio puede ser un par de alambres, un cable coaxial, el aire, etc. Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, la disminución progresiva de la potencia de la señal conforme aumenta la distancia. [2]

La función del **Receptor** es extraer del canal la señal deseada y entregarla al transductor de salida. Como las señales son frecuentemente débiles, como resultado de la atenuación, el receptor debe tener varias etapas de

amplificación. En todo caso, la operación clave que ejecuta el receptor es la demodulación, el caso inverso del proceso de modulación del transmisor, con lo cual vuelve la señal a su forma original. [2]

En un sistema de comunicaciones, como una red celular, se tiene que hablar de dos factores importantes, uno de ellos y antes mencionado es la modulación, la modulación resuelve varios problemas al momento de la transmisión de datos, pero nos falta mencionar un aspecto importante, que tiene que ver con el ancho de banda y los problemas que genera al tener miles de usuarios conectados al mismo tiempo. El proceso que ayuda para resolver este problema es el control de acceso al medio, que también se explica en la sección 2.1.2.

### 2.1.1 Modulación.

Consiste en variar determinado aspecto de una señal denominada portadora con respecto a una segunda señal denominada señal moduladora, generando finalmente una “señal u onda modulada”. [3] En la figura 3 se muestran los sistemas básicos de modulación existente.

En el proceso de modulación, la señal de alta frecuencia (portadora) quedará modificada en alguno de sus parámetros como su amplitud, frecuencia, fase, etc. de manera proporcional a la amplitud de la señal de baja frecuencia (moduladora). [3]

La técnica de modulación tiene grandes ventajas:

- Evita interferencia entre canales, Si todos lo que se transmite se hace a la frecuencia de la señal original o moduladora, no será posible reconocer la información contenida en dicha señal, debido a la interferencia que se crearía entre las señales transmitidas por cada usuario. [3]
- Los sistemas de transmisión son mucho más eficientes a altas frecuencias. [3]
- Se aprovecha mejor el espectro electromagnético, ya que normalmente se utiliza él envío de señales senoidales, que en el espectro de frecuencias solo ocupan un ancho de banda muy pequeño.
- Disminuye dimensiones de antenas. En caso de transmisión inalámbrica, las antenas tienen medidas más razonables. [3]
- Protege a la información de las degradaciones por ruido. [3]
- Define la calidad de la información trasmitida. [3]

En la figura 2 se muestra un sistema de modulación y sus partes que lo conforman.

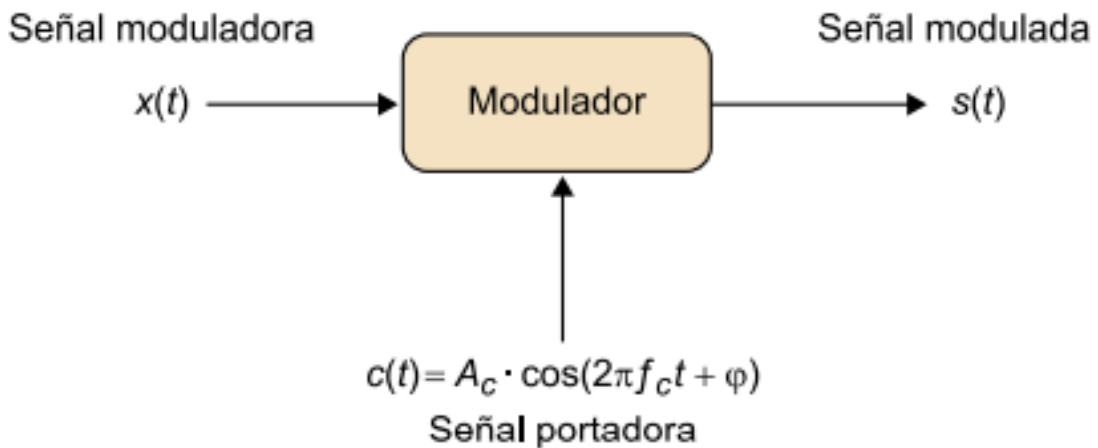


Figura 2 Sistema de Modulación [4]

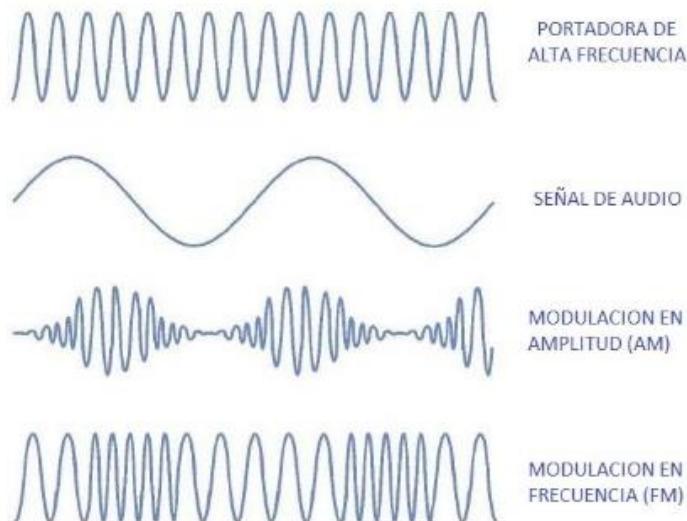


Figura 3 Ejemplo de modulación AM y FM [5]

Es necesario definir algunos conceptos básicos, para comprender el proceso de modulación:

- Ancho de banda:** estrictamente, el ancho de banda  $B_x$  de una señal  $x(t)$  real es el margen de ocupación de frecuencias positivas para las que la transformada de Fourier de dicha señal no se anula. Debido a las propiedades de simetría que presenta la transformada de Fourier de señales reales, este ancho de banda coincide con el medido a frecuencias negativas. [4]

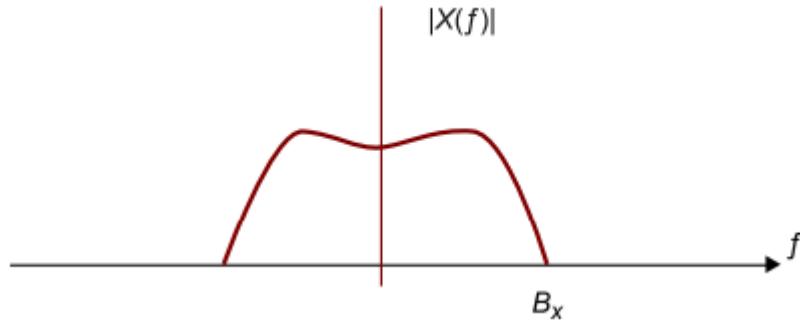


Figura 4 Ancho de Banda [4]

- b) **Señal moduladora  $x(t)$ :** es la señal real y continua que se va a transmitir entre un transmisor y un receptor. En general, supondremos que su ancho de banda es  $B_x$  Hz, tal y como se representa mediante el módulo de su transformada de Fourier en la figura 4. La señal moduladora  $x(t)$  también se suele denominar mensaje o información para transmitir como se muestra en la figura 3, la señal de audio sería la señal moduladora. [4]
- c) **Señal portadora  $c(t)$ :** es una señal sinusoidal procedente de un oscilador y caracterizada por tres parámetros, que son amplitud  $A_c$ , frecuencia  $f_c$  y fase  $\phi_c$ . La frecuencia, denominada frecuencia portadora, es el parámetro de mayor interés, ya que determina la nueva banda de ocupación. En general, la frecuencia es de un valor mucho mayor que el ancho de banda de la señal de información,  $f_c \gg B_x$ . [4]
- d) **Señal modulada  $s(t)$ :** es la señal obtenida al final del proceso de modulación. Esta señal, como resultado de la modulación, ocupa un determinado ancho de banda alrededor de la frecuencia portadora, por lo que se denomina señal pasa banda. En función de cómo se realice el proceso de modulación, la señal modulada se puede interpretar como una nueva señal sinusoidal de amplitud, frecuencia o fase dependientes de la señal moduladora. [4]

Durante el paso de los años, observando las necesidades para la transmisión de datos en sistemas de comunicación, se optó por varios tipos de modulación, en la figura 5 se muestra una clasificación de los tipos de modulación.

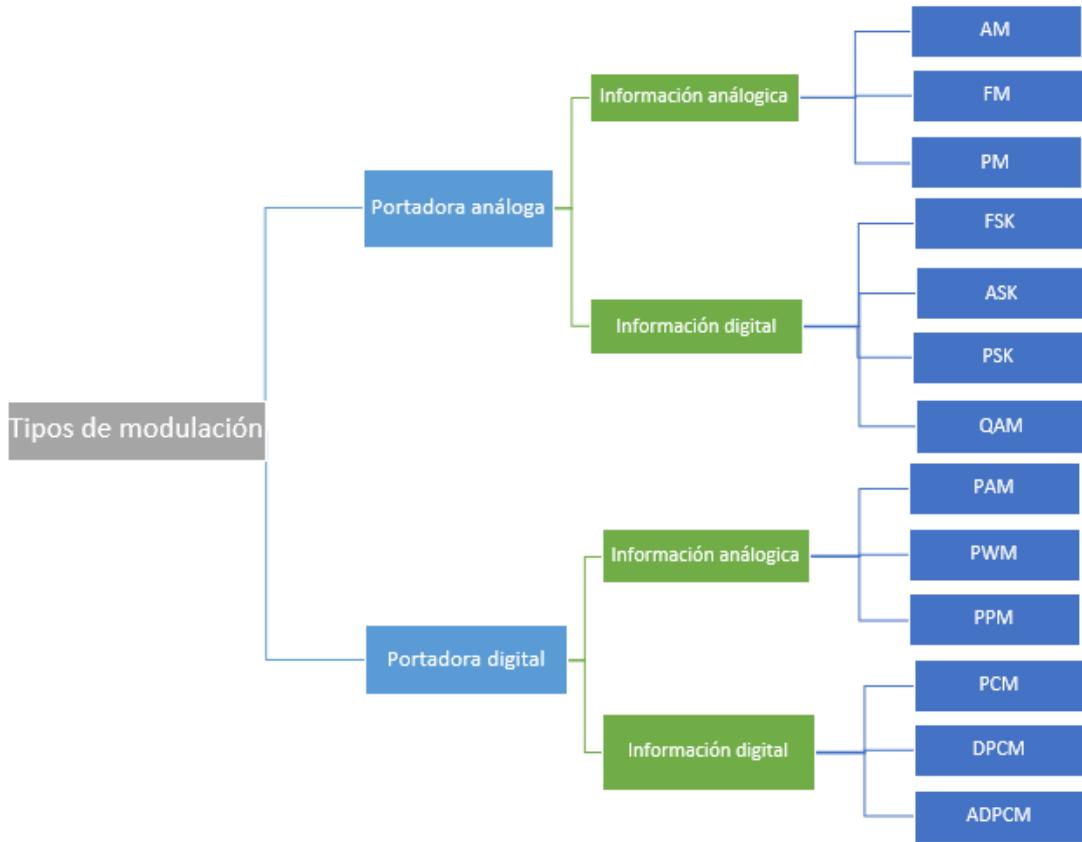


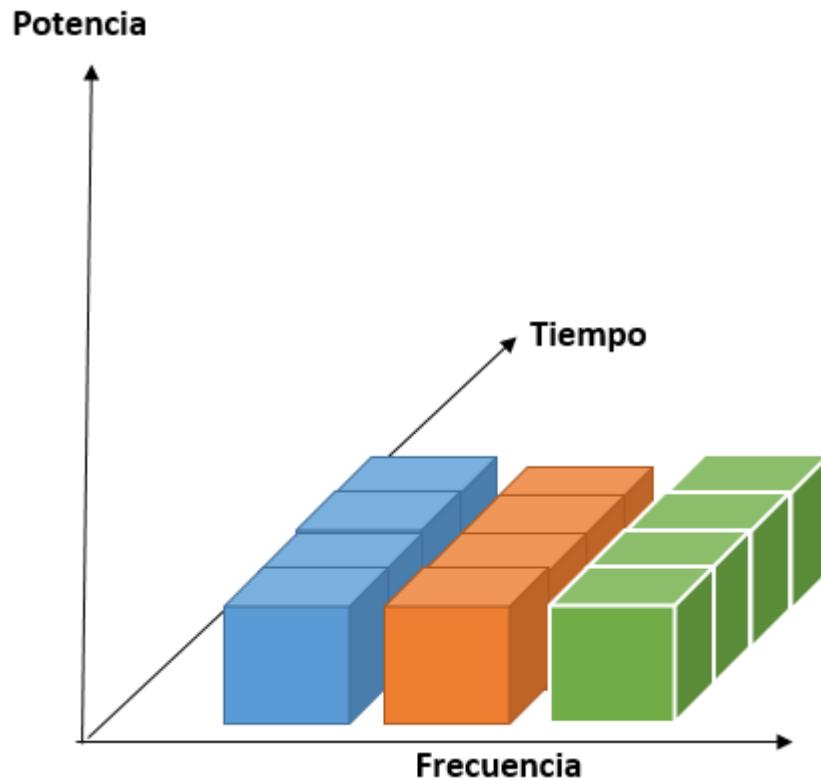
Figura 5 Clasificación de los tipos de Modulación.

### 2.1.2 Control de acceso al medio.

Anteriormente cuando los sistemas de telecomunicaciones inalámbricas empezaron a avanzar exponencialmente, se encontraron con el problema de la interferencia, por lo que algunas organizaciones se encargaron de la división de espectro de frecuencia para que las compañías que ofrecieran este servicio no tuvieran interferencia con otros. Esta división de frecuencias provoco que el ancho de banda para cada empresa se redujera con el paso del tiempo debido a la aparición de nuevos servicios como la telefonía celular. Se observó que la única solución era multiplexar las señales que se transportan por ese canal. Debido a esto se introdujo el término acceso al medio, que, en la telefonía celular, debido a la gran cantidad de usuarios, se necesita para darles acceso a todos en todo momento.

Existen muchas técnicas de acceso al medio entre las más simples y más conocidas se encuentran:

**FDMA:** El acceso al medio por división de frecuencia consiste en dividir el espectro de frecuencia del ancho de banda entre todos los usuarios conectados al canal. En la figura 6 se da una representación gráfica de FDMA.



*Figura 6 FDMA*

El FDMA cuenta con las siguientes ventajas:

- Cuenta con una buena calidad.
- Su implementación es muy sencilla.
- Aprovecha la jerarquía multiplex.

El FDMA cuenta con los siguientes inconvenientes:

- El ancho de banda está en uso siempre hasta sin tráfico.
- No es eficiente si el tráfico cambia constantemente.
- Cuenta con muy poca flexibilidad.

**CDMA:** el acceso al medio por división de código consta de enviar la información por el canal codificado, para que esto sea posible se utilizan códigos ortogonales, donde su producto punto es igual a cero. Y la información enviada no se traslape.

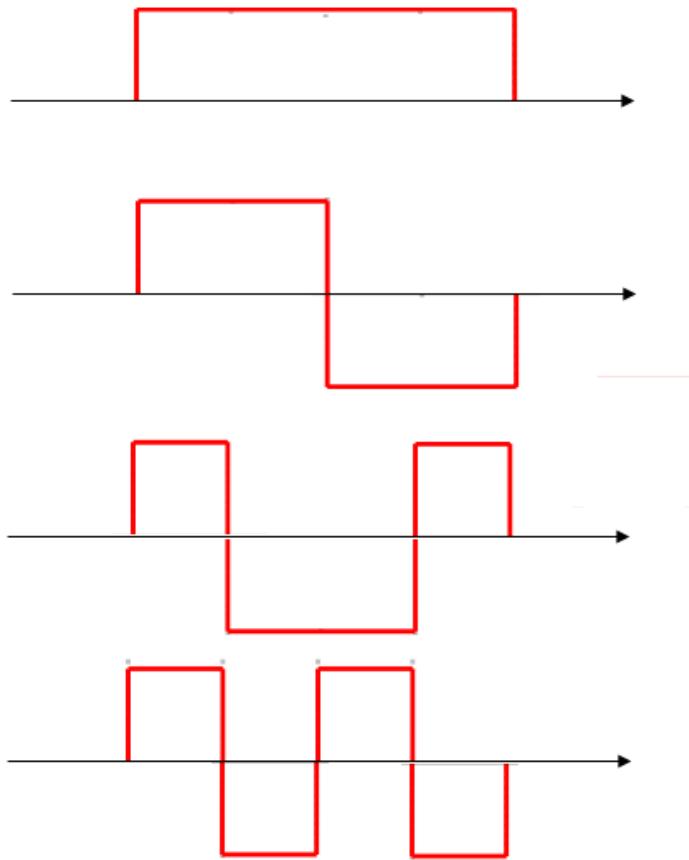


Figura 7 Códigos ortogonales

Los códigos de la figura 7 son ortogonales, debido a que si se aplica el producto punto entre las señales ortogonales el resultado es cero. Para la codificación, se multiplican los datos con el código y luego estos se suman unos con otros. Al tener este resultado no se pueden enviar los datos con valores decimales, por lo que se codifica en binario para el envío de los datos. Al llegar al receptor, lo que hace para recuperar los datos es, multiplicar la señal con el código.

El CDMA cuenta con las siguientes ventajas:

- No tiene que contar con sincronismo TDMA.
- Proporciona la protección contra interferencias y multirayecto.
- El tamaño de las antenas, para este tipo de codificación, es pequeña.
- Como la señal va codificada es más segura la información.

El CDMA cuenta con los siguientes inconvenientes:

- Poca eficiencia.
- Se necesita tener bien sincronizada la secuencia en el receptor.

En la figura 8 se da una representación gráfica del CDMA.

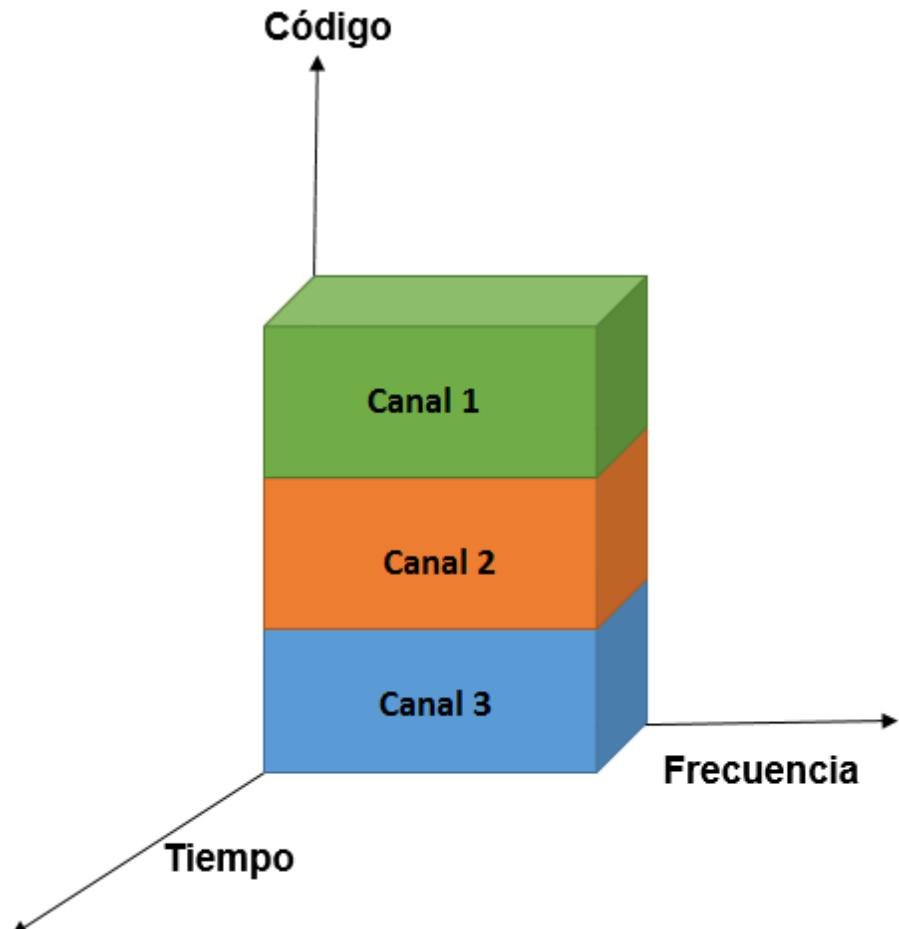


Figura 8 CDMA

**TDMA:** el acceso al medio por división de tiempo consiste en darle a cada usuario un cierto tiempo en el canal para él envío de sus datos, es decir, un usuario toma todo el ancho de banda por tiempos muy pequeños y envía su información. En la figura 9 se muestra una representación gráfica de acceso al medio TDMA.

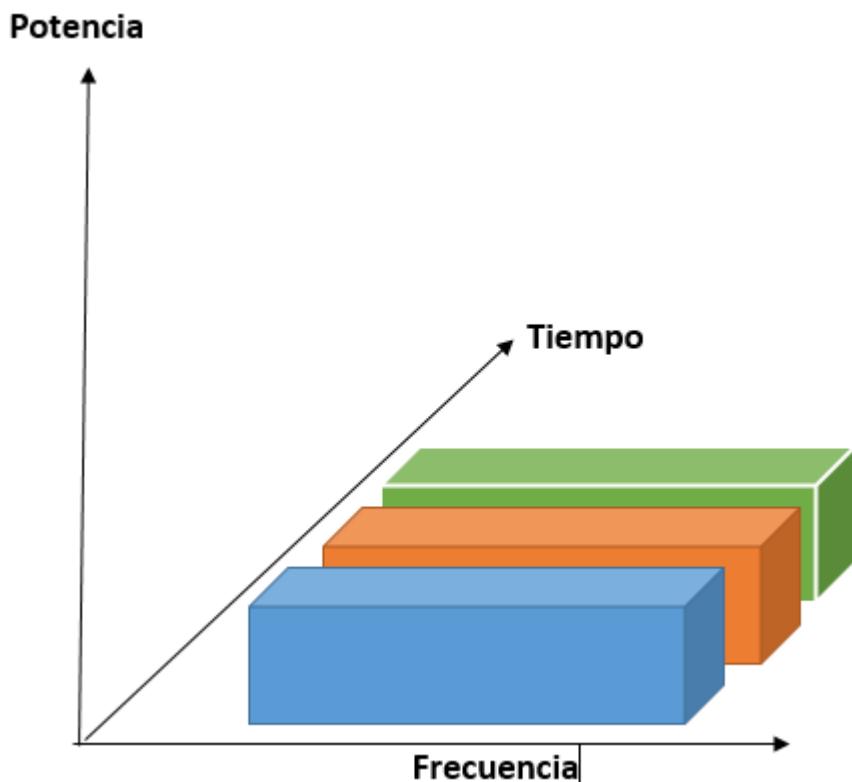


Figura 9 TDMA

El TDMA cuenta con las siguientes ventajas:

- Fácil implementación.
- No tiene interferencias debido a que cada usuario toma el control en cierto tiempo.

El TDMA cuenta con los siguientes inconvenientes.

- Utiliza todo el ancho de banda del canal.
- Si son muchos usuarios los que quieren acceder al canal la comunicación se hace lenta.

## 2.2 HISTORIA DE LA TELEFONÍA CELULAR

### 2.2.1 Antecedentes de telefonía celular

Hoy en día el teléfono celular es una herramienta indispensable en nuestra vida cotidiana para el entretenimiento o para el trabajo. Pero la invención de este dispositivo es gracias a una serie de descubrimientos sucedidos a través de los años.

Al surgir la energía eléctrica hizo posible la comunicación a larga distancia al inventar el telégrafo. Los inventores en varias partes del mundo quisieron aprovechar el electromagnetismo para la creación de nuevos dispositivos que nos permitieran la comunicación a larga distancia. Tras varios intentos, a finales de 1830 se logró crear un dispositivo económico llamado telégrafo Morse. [6]

En 1854 Antonio Meucci construyó un dispositivo que conectaba su oficina con el dormitorio ubicado en el segundo piso de su casa llamado teleéfono. Durante un tiempo Meucci estuvo trabajando en su invento, no fue hasta 1871 que desarrolló un teléfono que funcionaba perfectamente. Para patentar su invención necesitaba 250 dólares, dinero que no tenía a su disposición. Sólo pudo pagar un documento oficial que describía las características del teléfono y concedía a Meucci la prioridad en el desarrollo de un aparato capaz de transmitir a distancia la voz humana. En 1874 decidió presentar su prototipo a la compañía Western Union que no se interesó por el proyecto. [7]

Durante el año de 1876 Elisha Gray solicita una patente provisional para un teléfono. En el mismo año el 14 de febrero Gray solicita la patente definitiva. Al siguiente año, la patente fue otorgada a Graham Bell y su amigo T.A Watson al presentar un aparato telefónico. [6]

La comunicación inalámbrica tiene sus raíces en la invención de la radio por Nikola Tesla en los años 1880, aunque formalmente presentado en 1894 por un joven italiano llamado Guglielmo Marconi. Estos descubrimientos dan origen a un gran número de posibilidades para la telefonía celular, pero todavía no se desarrollaba la tecnología necesaria para una red celular. [8]

En 1885 tras la invención del teléfono había varias centrales telefónicas en diferentes ciudades de Estados Unidos de América, pero no había una comunicación entre ciudades. Así que durante este año se hizo la instalación de una línea telefónica que conectaba la ciudad de New York y Philadelphia. Apareciendo así el término “llamada de larga distancia” [9]

Tras obtener la patente del teléfono, Graham Bell empezó a vender su invento, fundando el Sistema Bell en 1899, también llamado “American Telephone and Telegraphos” (AT&T). El primer sistema de teléfonos era manual ya que los teléfonos no contaban con un sistema de discos o teclas para marcar al número, si no que un grupo de operadores te conectaba con el destino deseado. En 1893 tras expirar la patente de Bell se crearon varias empresas de telefonía independientes.

El 7 de marzo de 1921 se realiza el primer experimento de comunicación trasatlántica por teléfono inalámbrica que fue conectada de Rocky Point,

Long Islands con la estación receptora de Cupar situada en Escocia una onda de longitud de 500 metros uniendo las dos orillas del mar. [6]

Tras varios años de avance en la tecnología telefónica se encontraron con el problema de llamadas de larga distancia de continente a continente, ya que no podrían utilizar cables de gran longitud por los costos de instalación y material. A consecuencia de esto se optó por la utilización de satélites. El 11 de julio de 1962 AT&T lanzó el primer satélite en órbita dedicado para comunicaciones, "el telstar", lo cual permitió las conexiones inalámbricas a lo largo del globo. [9]

### **2.2.2 Inicio de la telefonía celular**

Aunque la telefonía celular apareció cierto tiempo después, la telefonía a través de señales de radio se utiliza desde las primeras décadas del siglo pasado. En el año de 1920, en Detroit, Estados Unidos, nacen las primeras redes de comunicación móvil. Eran sistemas de radio comunicación utilizados por el cuerpo de policía que trabajaban en ese entonces a 2 MHz. Una década más tarde fueron utilizados por la policía de la ciudad de Nueva York. En 1927, los Estados Unidos y el Reino Unido, establecieron el primer enlace intercontinental de banda corta entre ambos países; este servicio contaba con catorce canales dedicados y un transmisor principal ubicado en Inglaterra. En 1940 la Comisión Federal de Comunicaciones (FCC), encargada de la regulación de telecomunicaciones, dispuso nuevas frecuencias para la radio móvil en la banda de frecuencia de 30 MHZ a 40 MHz. Sin embargo, hasta que los investigadores desarrollaron técnicas de modulación en frecuencia, para mejorar la recepción en presencia de ruido electrónico y desvanecimiento de señales, la radio móvil se convirtió en útil. [10]

AT&T introdujo el primer servicio telefónico móvil en los Estados Unidos el 17 de junio de 1946 en San Luis, Missouri. El sistema operaba con 6 canales en la banda de 150 MHz con un espacio entre canales de 60 KHz. y una antena muy potente. Este sistema se utilizó para interconectar usuarios móviles (usualmente autos) con la red telefónica pública, permitiendo así, llamadas entre estaciones fijas y usuarios móviles. Un año después, el servicio telefónico móvil se ofreció en más de 25 ciudades de los EE.UU. y unos 44,000 usuarios en total, aunque por desgracia había 22,000 más en una lista de espera de cinco años. Estos sistemas telefónicos móviles se basaban en una transmisión de Frecuencia Modulada (FM). [6]

La mayoría de estos sistemas utilizaban un solo transmisor muy poderoso para proveer cobertura a más de 80 Km. desde la base. Los canales telefónicos móviles de FM evolucionaron a 120 KHz. El espectro para transmitir la voz tenía un ancho de banda de 3KHz. Aunque se esperaban

mejoras en la estabilidad del transmisor, en la figura de ruido y en el ancho de banda del receptor. [6]

La demanda para el servicio de telefonía móvil creció rápidamente y permaneció por detrás de la capacidad disponible en muchas de las ciudades de gran tamaño. Es increíble que a pesar de la demanda hayan pasado más de 30 años para cubrir las necesidades de telefonía móvil. La capacidad del sistema era menor que el tráfico que tenía que soportar, por ello, la calidad del servicio era terrible, las probabilidades de bloqueo eran del 65% o más altas. La inutilidad del teléfono móvil disminuyó la frecuencia de su uso ya que los usuarios encontraron que era mejor prevenir no hablando en horas picos. Los usuarios y las compañías telefónicas se dieron cuenta que un conjunto de canales no sería suficiente para desarrollar un servicio telefónico móvil útil. Se necesitarían grandes bloques del espectro para satisfacer la demanda en áreas urbanas. [6]

En 1949, la FCC dispuso más canales y la mitad se los dio a la compañía Bell System y la otra mitad a compañías independientes como la RCC (Radio Common Carriers), con la intención de crear la competencia y evitar los monopolios. [10]

En 1958, la Richmond Radio telephone Co. mejoró su sistema de marcado conectando rápidamente las llamadas de móvil a móvil. En los años subsecuentes, se asignaron frecuencias para sistemas de telefonía móvil en todo el mundo; sin embargo, los equipos no eran capaces de evitar interferencias lo cual limitaba el número de canales disponibles. [10]

A finales de los 60's y principios de los 70's el trabajo comenzó con los primeros sistemas de telefonía celular. [6]

El Sistema de Telefonía Móvil Mejorado (IMTS), sistema de telefonía analógico conocido como generación cero, se caracterizó por asignar un número telefónico único, el canal de voz era ocupado por varios usuarios, pero solo uno a la vez, lo que ocasionaba tiempos de espera de hasta 30 minutos ó más. En enero de 1969 la Bell System aplicó por primera vez el rehuso de frecuencias en un servicio comercial para teléfonos públicos de la línea del tren de N.Y. a Washington, D.C. Para desarrollar este sistema se utilizaron 6 canales en la banda de 450 MHz en nueve zonas a lo largo de una ruta de 380 Km. [10]

Se debe reconocer que la primera generación de radio celular analógico no fue una nueva tecnología, pero si una nueva idea el de reorganizar la tecnología existente IMTS a gran escala. Mientras que las comunicaciones de voz utilizaron el mismo FM analógico que se había estado usando desde la II Guerra Mundial, dos mejoras importantes hicieron el concepto celular realidad. A principios de los 70's se inventó el microprocesador; aunque los

algoritmos complejos de control se implantaban en lógica con cables, el microprocesador hizo más fácil la vida de todos. La segunda mejora fue en el uso de un enlace de control digital entre el teléfono móvil y la estación base. No fue sino hasta marzo de 1977 cuando la FCC aprobó que Bell probara un sistema celular en Chicago. [6]

En 1971 se propuso el concepto celular como un avanzado sistema de comunicación móvil. Esta idea proponía el reemplazo de las estaciones base ubicadas en el centro de la ciudad por múltiples copias de tales estaciones de menor potencia distribuidas a lo largo del área de cobertura. Otra mejora fue en el uso de un enlace de control digital entre el teléfono móvil y la estación base. [10]

En 1972 Intel lanzó al mercado el microprocesador 8008 el cual podía manipular bytes completos, con memoria de 16 Kbytes. La creación de este microprocesador dio origen al primer teléfono celular móvil creado por la compañía Motorola. El DynaTAC 8000x contenía un micrófono, un altavoz, un teclado, una pantalla led, y una pila que otorgaba 30 minutos de llamada telefónica con una carga de 10 horas.

La telefonía celular en el mundo da sus primeros pasos cuando el Dr. Martin Cooper, un ejecutivo norteamericano que trabajaba para Motorola Company, atestiguado por la revista Popular Science realizó la primera llamada celular el 3 de abril de 1973 en las calles de Nueva York. El Dr. Cooper fue el primero en desarrollar y poner a prueba el teléfono portátil, DynaTAC que significa Dynamic Total Access Communications System. En esta misma década la compañía Motorola empezó a desarrollar dispositivos portátiles de comunicación para el consumo masivo. [10]

En 1978, en EE.UU. comenzó a operar el Servicio Telefónico Móvil Avanzado o Advanced Mobile Phone Service AMPS. En ese año, 10 células cubrían 3550 km cuadrados en el área de Chicago, operando en las nuevas frecuencias en la banda de 800 MHz. Esta red utilizaba circuitos integrados de bajo consumo, una computadora dedicada y un sistema de conmutación, lo que probó que los sistemas celulares podían funcionar. [6]

La decisión de la FCC para escoger la banda de 800 MHz para los sistemas celulares fue debido a limitaciones severas de espectro en las bandas de más baja frecuencia ocupadas por otros servicios como la televisión, radio en FM, radiocomunicación móvil, entre otros. En mayo de 1978 empieza a operar un sistema AMPS en Arabia Saudita. [10]

En 1982, cuando aparecieron los primeros servicios celulares comerciales, la CEPT (Conference Européenne des Postes et Telecommunications) tomó la iniciativa de formar un grupo de estudio llamado Groupe Special Mobile (GSM), para estudiar y desarrollar un sistema telefónico móvil terrestre y

público común para Europa en la banda de 900 MHz, banda que había sido reservada por la World Administrative Radio Conference (WARC) en 1978. [10]

AT&T desarrolló un modelo junto con Motorola conocido como Dyna-TACS o TACS que significa Total Access Communications System (Sistema de comunicación de Acceso total), el cual se puso en marcha en Baltimore y en Washington D.C. por la compañía Cellular One el 16 de diciembre de 1983. [6]

Otro estándar que surgió fue el de AURORA-400 en Canadá en febrero de 1983. Este sistema llamado descentralizado opera en los 420 MHz y utilizaba 86 células, funcionando mejor en áreas rurales por su poca capacidad, pero cobertura amplia. En Europa, el sistema celular Telefonía Móvil Nórdico o Nordic Mobile Telephone System NMT450 inició operaciones en Dinamarca, Suecia, Finlandia y Noruega en el rango de 450 MHz. En 1985 la Gran Bretaña empezó a usar TACS en la banda de 900 MHz. Más tarde, Alemania Occidental implementó C-Netz, Los franceses Radiocom 2000, y los italianos RTMI/RTMS. Todos ellos ayudaron a que hubiera nueve sistemas incompatibles, a diferencia de los EE.UU. que no sufrían de este problema. Desde aquí se pensó en un plan para crear un sistema digital único para Europa. [6]

En 1986 se adicionaron 5 MHz a cada banda, correspondiéndole a cada concesionario un ancho de banda total de 25 MHz. Como a cada canal tiene asignado 30 KHz, en total suman 832 canales por banda. Como se asignan 42 canales para señalización y control, el número de canales para voz se reduce a 790. Del espectro original A, se designaron A y como adición A', y para el espectro B fue agregado B'. Al espectro con las bandas A y B se le conoce como NES (Non Espread Spectrum), y a la suma de estas bandas con A'y B'se le conoce como ES (Espread Spectrum). [10]

En 1988, 18 Países firmaron un acuerdo de intenciones conocido como MOU (Memorandum of understanding), En este documento los países firmantes se comprometían a cumplir las especificaciones y adoptar este estándar único y a poner en marcha un servicio comercial GSM, que ofrece seguimiento automático de los teléfonos móviles en su desplazamiento por todos los países. El sistema inicialmente podría soportar ocho canales por portadora con una eventual evolución a dieciséis canales por portadora. [10]

En 1990, el sistema celular en Estados Unidos agregó una nueva característica, el tráfico de la voz se convirtió en digital. Esto triplicó la capacidad con el muestreo, digitalización y multicanalización de las conversaciones. Para 1991, el servicio celular digital comenzó a emerger reduciendo el costo de las comunicaciones inalámbricas y mejorando la capacidad de manejar llamadas de los sistemas celulares analógicos. En

1994, Qualcomm, Inc. propuso un escenario de espectro disperso para incrementar la capacidad. Construido con conocimientos anteriores CDMA (Code Division Multiple Access) sería en todos sus elementos digital, además de que prometía de 10 a 20 veces mayor capacidad. En estos días más de la mitad de los teléfonos en el mundo operaban de acuerdo a los estándares de AMPS, en un principio nadie pensó que sería el que conviviría con TDMA o CDMA para obtener sistemas duales con tecnología analógica y digital. El 14 de enero de 1997, la FCC abrió un nuevo grupo de frecuencias inalámbricas que permitiría el desarrollo de las tecnologías CDMA; la banda de 1900. De esta manera surge PCS que es un sistema de tecnologías híbrido que trabajaría con TDMA IS-136, CDMA IS-195 y el estándar GSM europeo. El PCS 1900 se encuentra en el intervalo de 1850-1910/1930-1990 MHz. Otras bandas en 2.1 GHz y 2.5 GHz también son consideradas para aplicaciones inalámbricas futuras. [10]

### 2.2.3 Telefonía celular en México

El inicio de la telefonía móvil en México se remonta a 1977, cuando se solicitó a la SCT de México (Secretaría de Comunicaciones y Transportes) una concesión para instalar, operar y explotar un sistema de radiotelefonía móvil en el Distrito Federal. Pero no fue hasta 1981 cuando se inició la comercialización de este servicio, el cual fue conocido por el público como Teléfono en el Auto, con el cual se logró, en un lapso de ocho meses, dar servicio a 600 usuarios. [11]

La primera compañía celular que llegó a México fue Iusacell en 1989 ofreciendo sus servicios en el Distrito Federal (hoy Ciudad de México). En el mismo año surge la marca Telcel con operaciones en la ciudad de Tijuana para pronto extenderse a lo largo de las 9 regiones del país. Un año después, la compañía Telcel empieza sus operaciones ofreciendo también el servicio en la capital del país. [11]

El crecimiento de los sistemas de telefonía celular en México se ha visto fortalecido gracias a la apertura del gobierno hacia la privatización de las telecomunicaciones. Uno de los primeros pasos para preparar al sector de las telecomunicaciones hacia la competitividad internacional fue la concesión de las frecuencias de comunicaciones para tecnología celular. El día 31 de mayo de 1989 se presentó el “Plan Nacional de Desarrollo 1989-1994” donde menciona la importancia de las telecomunicaciones destacando los siguientes puntos: [10]

- Múltiples empresas podrán desarrollar los servicios de transmisión conmutada de: datos, teleinformática, telefonía celular y otros. [10]
- Las concesiones de telefonía celular se sujetarán a concurso de manera abierta, y así se garantizará la mejor oferta de servicios y contraprestación económica al Estado. [10]

## 2.3 CONCEPTOS BÁSICOS DE LA RED DE TELEFONÍA CELULAR

### 2.3.1 La célula

Es una zona geográfica de cobertura emitida por una antena de una estación base. La cobertura o tamaño geográfico de la célula depende de la potencia del transmisor, altura y posición de la torre de la antena, así como la frecuencia y el tipo de antena. El tamaño de la célula depende del tráfico en la red dado por el número de usuarios además se toma en cuenta la necesidad de superar obstáculos para zonas urbanas ya que las edificaciones tienen gran influencia en el radio de propagación. En la figura 10 se muestra la organización de un conjunto de células para dar cobertura en un área geográfica.

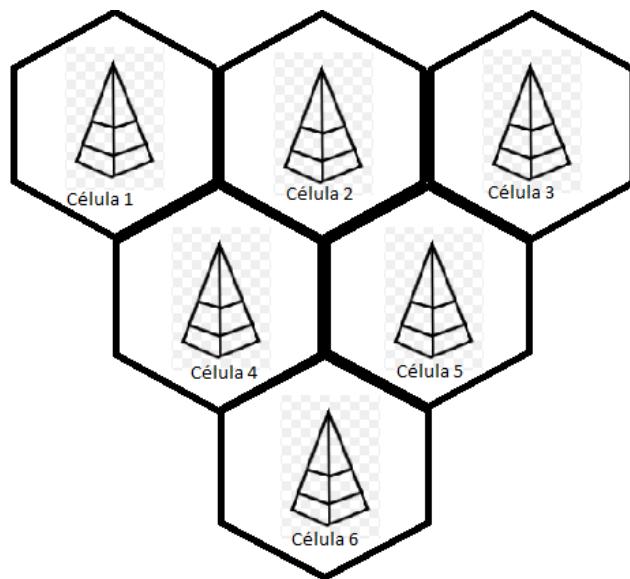
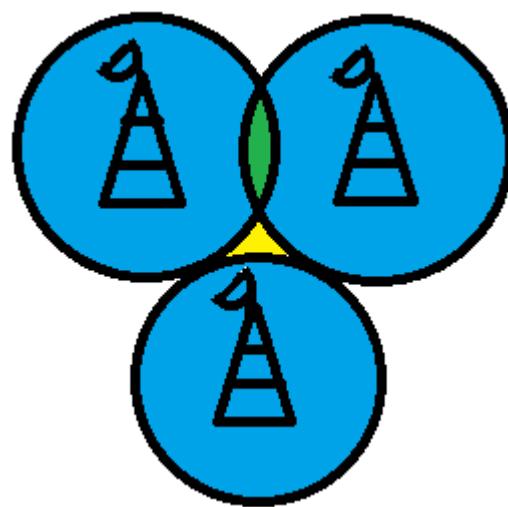


Figura 10 Conjunto de Células unidad en una red Celular

### 2.3.2 Propiedades de la Geometría Celular

Para una geometría celular se debe de hacer un diseño eficaz, que tenga en cuenta la separación entre antenas para prevenir interferencias co-canal. Este diseño tiene un gran compromiso ya que se encarga de reajustar la transmisión, commutación y control de recursos cada vez que el sistema vuelve a atravesar por esta fase de desarrollo.

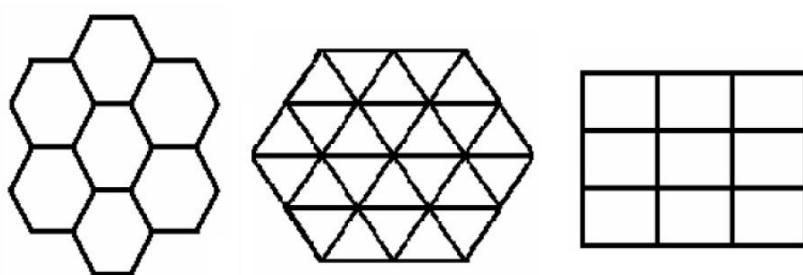
Para tener un área con una señal constante se debería contar con una geometría circular, pero este tipo de área es considerada impráctica debido a la múltiple difusión o no difusión siendo el caso de la separación de las antenas.



*Figura 11 Ejemplo de una geometría circular.*

En la figura 11 se muestra una geometría circular con los dos problemas anteriormente mencionados, donde la parte de color verde muestra la múltiple difusión donde existe interferencia entre canales, y el color amarillo representa la no difusión donde no existe cobertura.

Observando los problemas generados por la geometría circular se optó por geometrías diferentes, hexagonal, triangular y rectangular. En la figura 12 se aprecian los diferentes tipos de geometría celular.



*Figura 12 Tipos de Geometría celular usados*

Por razones económicas, la geometría hexagonal ha sido escogida para el diseño de redes celulares, dado que el hexágono tiene la máxima área de cobertura. Consecuentemente, una capa hexagonal requiere menos células, y por lo tanto son necesarias menos estaciones base. Así, otras consideraciones llegan a lo mismo, un sistema basado en la estructura celular hexagonal es justamente lo necesario para los propósitos de diseño desde un punto de vista analítico y teórico. En la práctica, el hexágono podría ser visto idealmente como un círculo o un patrón de cobertura distorsionado. El área central de cobertura está dividida en seis sectores que corresponde al

incremento de tráfico. La sectorización es conseguida por el uso de antenas direccionales en las estaciones base. [10]

### 2.3.3 Célula omnidireccional

Una célula omnidireccional es aquella que está compuesta por antenas del mismo tipo, este tipo de antena se caracteriza por irradiar energía electromagnética en todas las direcciones generando una zona geográfica circular.

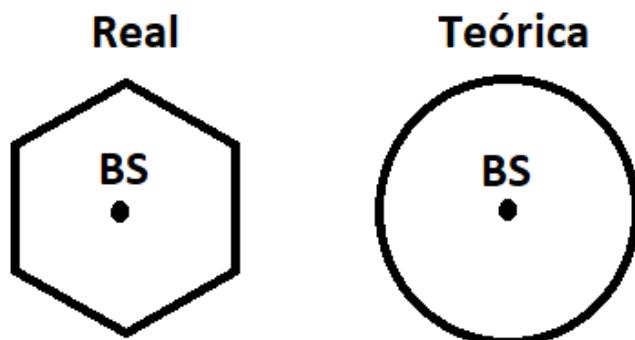


Figura 13 Célula omnidireccional

Como se ve en la figura 13, la célula omnidireccional se encuentra en el centro irradiando energía electromagnética en todas las direcciones en un plano. La célula teóricamente debería irradiar un círculo, pero debido a lo explicado sobre la practicidad de este tipo de célula se representa como una célula hexagonal.

### 2.3.4 Célula sectorial

Para este tipo de célula se utilizan varias antenas direccionales, se acomodan de tal manera que cada antena cubra cierto ángulo de la célula. Este tipo de célula se utiliza cuando se necesita mayor ganancia. Normalmente son utilizados en zonas urbanas. Un sector es la superficie cubierta por una antena. Estos sectores cuentan con una frecuencia y equipos transceptores únicos, por lo que se puede decir que son células. La ventaja de una célula sectorizada es que se genera muy poca interferencia entre ellas debido a la poca potencia emitida hacia atrás ya que son antenas direccionales. En la figura 14 se muestra como una estación base cubre tres células para crear un sector. En la figura 15 se explica cómo se forma una célula sectorial a partir de 3 BTS.

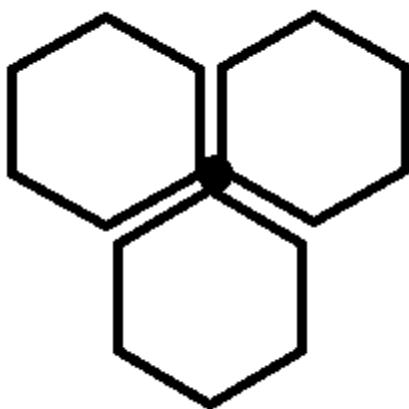


Figura 14 Estación Base cubriendo tres células, para crear un sector

En una célula sectorizada los cálculos de cobertura e interferencia y las asignaciones de frecuencias han de hacerse a nivel de sector. En estas circunstancias se llaman células a los sectores de radio y emplazamientos a las posiciones de las BS. Desde un emplazamiento, en las redes sectorizadas, se da cobertura a tres o seis células. Las estructuras celulares sectorizadas suelen designarse con la notación N/M, donde N es el número de células y M el número total de sectores por agrupación. Por lo tanto, una estación base cubre tres células sectoriales, cuando se muestran tres células sectoriales se dibujan tres hexágonos, uno para cada célula, con la estación base localizada en la esquina de cada hexágono, para que se lleve a cabo la cobertura total, las células vecinas deben traslaparse entre sí. [10]

En la figura 16 se muestra una torre con antenas sectoriales.

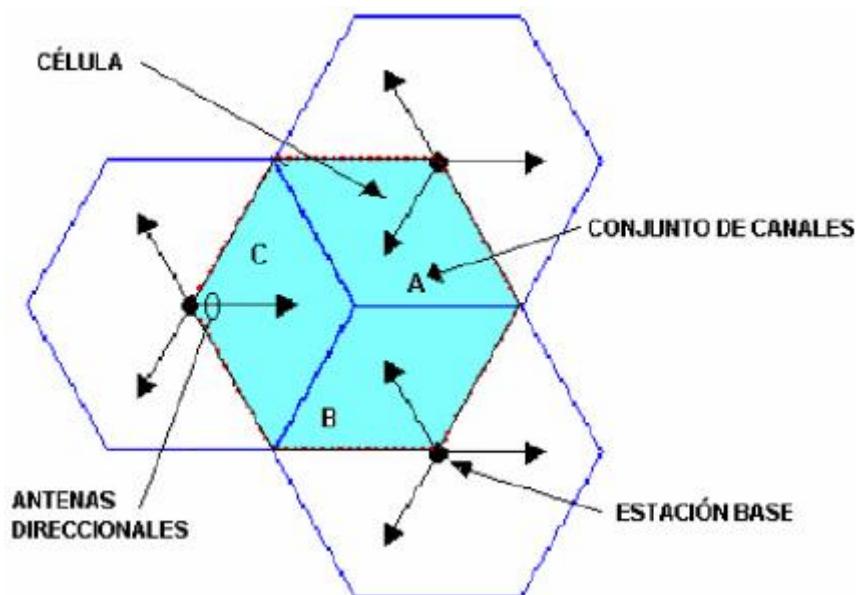


Figura 15 Formación de una célula sectorial a partir de 3 BS [10]



Figura 16 Torre con antenas sectoriales [10]

### 2.3.5 Clasificación de células o celdas

Debido a la actual demanda del servicio de telefonía celular, se optó por dividir los sistemas de celdas en:

- **Macroceldas:** Este tipo de celda se utiliza en zonas rurales donde el tráfico telefónico en un gran radio es pequeño. Esto tiene la ventaja de que la calidad de servicio es mejor, debido a que en estos lugares una probabilidad muy baja de que exista un handover, proceso que se explica en la sección 2.9.
- **Microceldas:** En este tipo de celdas se tiene un mejor manejo del tráfico, pero tiene una cobertura mucho menor que una macrocelda. Se utiliza en zonas Urbanas.
- **Picoceldas:** Este tipo de células son utilizadas en zonas donde el tráfico de red es excesivo como por ejemplo en centros comerciales donde los usuarios tienen un comportamiento de baja movilidad.

De manera gráfica se puede apreciar en la figura 17 la clasificación de las celulas de acuerdo a su cobertura y en la tabla uno se muestra el rango y la cobertura de esta clasificación.

Tabla 1 Clasificación de las células con radios de cobertura

Tipo de celda	Rango de Radio	Cobertura
Picocelda	30m a 200m	Interiores de aeropuertos y centros comerciales
Microcelda	300m a 700m	zonas de ciudades con elevada densidad de tráfico
Macrocelda	1.5 km a 20 km	Carreteras y poblaciones cercanas

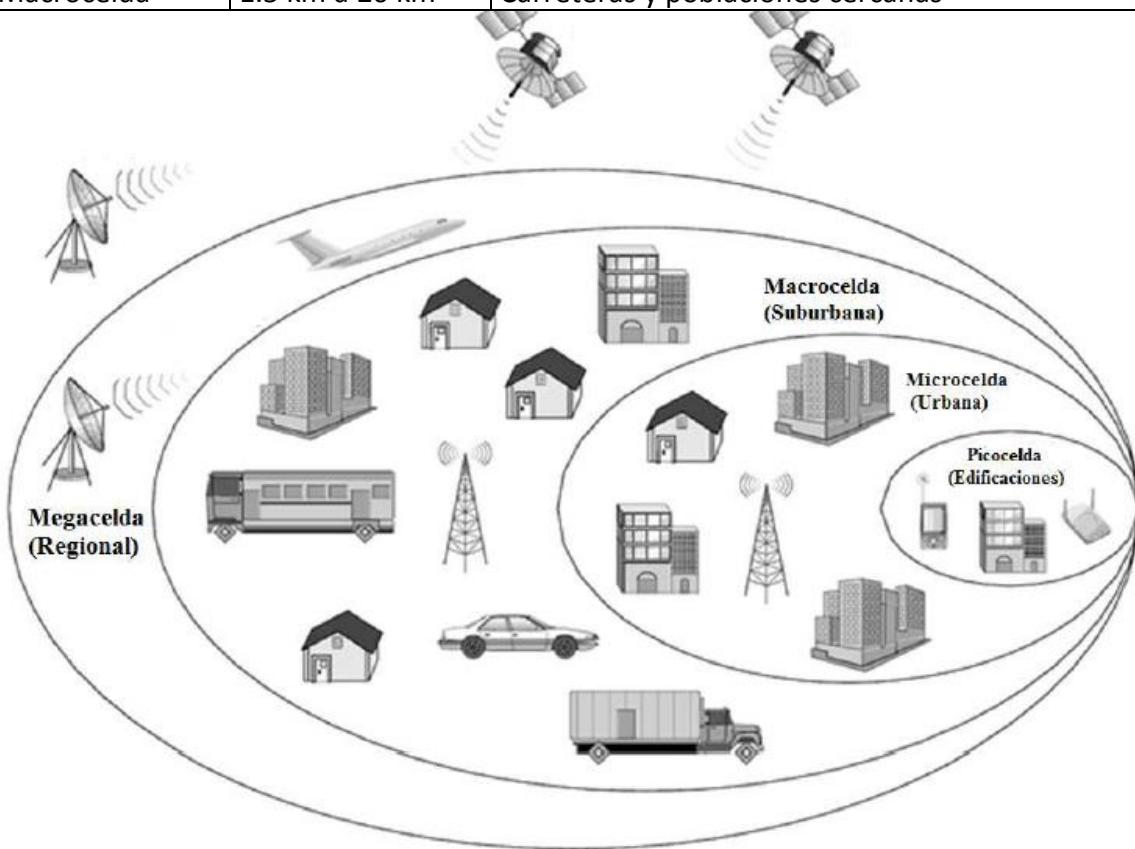


Figura 17 Clasificación de las células [12]

### 2.3.6 Diseño de células

Debido a la gran cantidad de usuarios requiriendo el acceso a la red es necesario hacer un buen diseño en la posición de las antenas y la utilización de canales de estas antenas. Para el diseño es necesario tener claros los siguientes conceptos:

#### **Cluster.**

Un cluster es un conjunto de células con grupos de canales diferentes, generando la ventaja de que el espectro de frecuencias se puede reutilizar en un nuevo cluster. De esta manera se puede aumentar el número de usuarios en un canal específico.

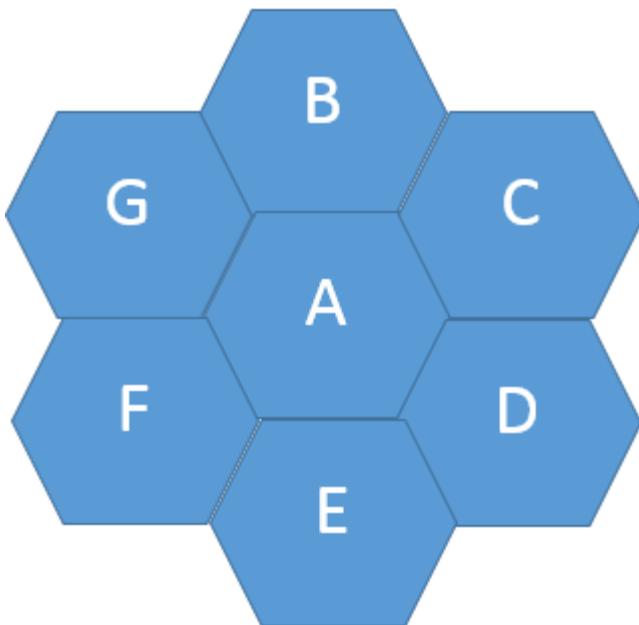


Figura 18 Cluster. Cada letra representa una célula con características diferentes.

Como se ve en la figura 18, cada célula tiene un canal con una frecuencia diferente dando la ventaja de que no se traslape las frecuencias y no exista interferencia.

### **Reutilización de frecuencia.**

El concepto de reutilización de frecuencias se refiere a tener las células de un cluster que utilizan la misma frecuencia a una distancia lo más alejado posible para no tener interferencia co-canal, es decir, interferencia provocada por la utilización del mismo canal en dos células vecinas. Esto nos da a entender que para el diseño de una red se necesita tener un control entre la frecuencia utilizada de la antena y la potencia que emite esta antena, ya que una potencia muy grande hace que la distancia entre dos células que utilizan la misma frecuencia sea menor generando más problemas. A estas células que utilizan la misma frecuencia se les llama células co-canal.

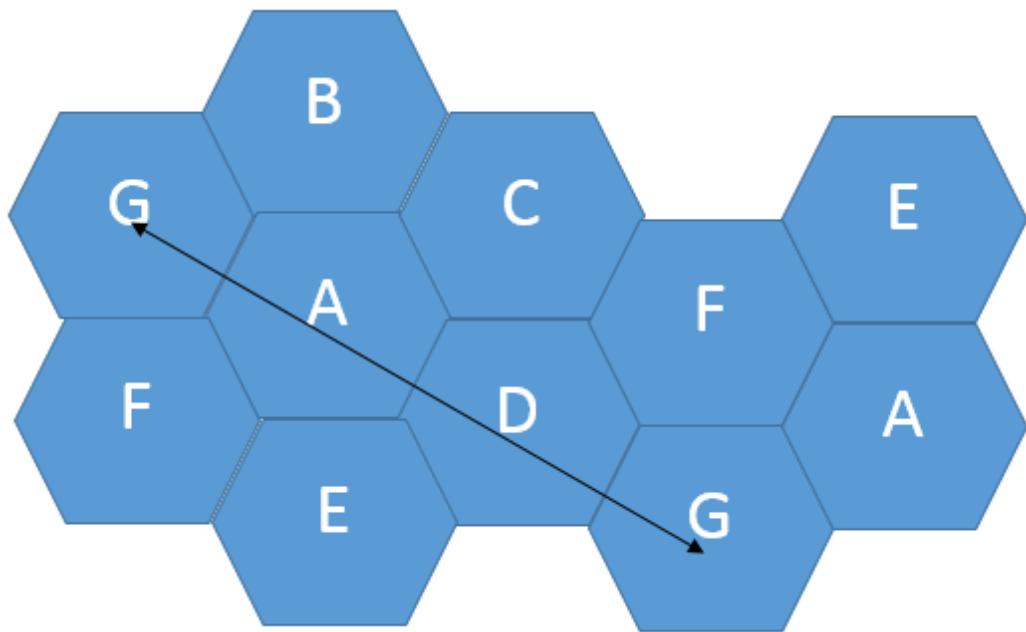


Figura 19 Representación del concepto de reutilización de frecuencia

Como se ve en la figura 19 el cluster se coloca de tal manera que la distancia entre células co-canal este lo más separadas posible.

El uso múltiple del mismo canal en células con una separación geográfica asegura que el espectro de radio es utilizado de manera eficiente. El índice de reutilización de un sistema celular es el cociente entre los canales que se ofrecen y el número de frecuencias disponibles. Cada estación base tiene una dotación de K canales por lo que habrá N grupos de K canales cada uno y en total se utilizarán  $K \cdot N$  canales distintos, reutilizándose N veces cada canal. Cuanto menor sea el tamaño de la agrupación también lo será el número de frecuencias necesarias. Las BS de cada célula sólo van equipadas con los K canales de su grupo, pero la MS debe tener la posibilidad de sintonizar cualquiera de los  $K \cdot N$  canales para poder conectarse con cualquier célula. A las N células que usan un conjunto completo de frecuencias disponible, se les llama cluster, si un cluster se repite M veces dentro de un sistema, el número total de canales duplex, C, se puede utilizar como una medida de la capacidad y este dado como la ecuación 1: [10]

$$C = M * N \quad (1)$$

Cuanto mayor sea N, mayor va a ser la distancia entre estaciones base con el mismo grupo de canales, menor será su interferencia, pero la capacidad del sistema también será menor. Desde el punto de vista del diseñador, es deseable usar el valor más pequeño de N posible, para maximizar la

capacidad del sistema dentro del área de cobertura. Para llevar a cabo la reutilización de frecuencias es necesaria una planeación de frecuencias. Por lo general se utiliza el Plan K=7 que es un cluster de 7 células. Otros arreglos son posibles y del tamaño de los clusters se determina la distancia de separación entre células con reusó de frecuencias, de todas formas, un número de canales limitado puede ser asignado a cada célula. [10]

### **Distancia de reutilización de frecuencias.**

Para el cálculo de la distancia mínima entre células para la reutilización de frecuencias hay que tomar en cuenta varios factores que intervienen como lo es, la altura de la antena, la potencia de transmisión de cada celda, además de tomar en cuenta el número de celdas co-canal.

Para el cálculo de la distancia de reutilización se utiliza la ecuación 2:

$$D = \sqrt{3 * k * R} \quad (2)$$

Donde:

K = Número de celdas por cluster.

R = Radio de la célula.

D = Distancia entre células co-canal

Normalmente para el diseño se utilizan un valor de k muy grande para tener una mayor distancia, pero esto nos genera otro problema ya que el límite de canales dados para la transmisión de un servicio es corto, y le tocaría menos canales a cada célula.

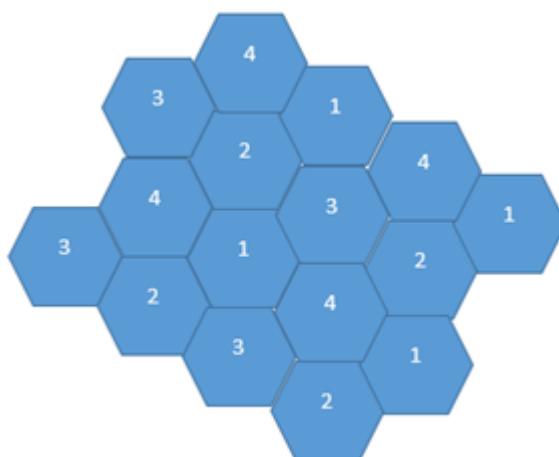


Figura 20 Patrón k=4

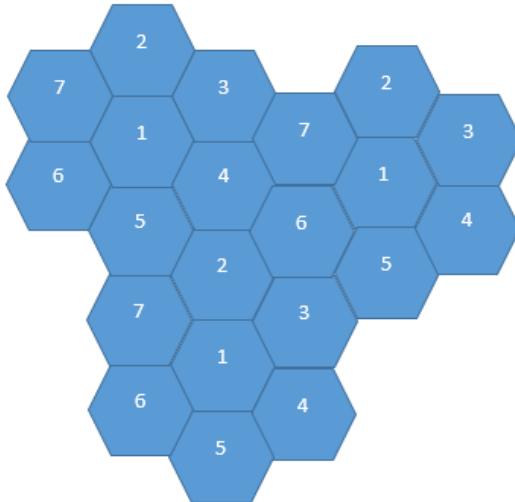


Figura 21 Patrón k=7

Así como los Patrones k=4 y K=7, existen muchos más, pero el más utilizado es el K=7 ya que es el más sencillo para el diseño y el que da menos problemas. En la figura 20 se observa la distribución de frecuencias con k=4 y en la figura 21 con k=7.

### Técnicas de asignación de canal.

Como se mencionó anteriormente, las células cuentan con ciertos canales, pero para asignar estos se cuenta con dos formas:

- Asignación de canal fija: Este tipo de asignación consiste en que el controlador de estación base (BSC) se encarga de asignar unos canales fijos a cada célula del cluster por lo que cada célula tiene un canal diferente y único. Cualquier llamada producida en una célula solo puede ser atendida por los canales disponibles, si todos los canales se ocupan, el usuario que solicita usar uno se bloquea por lo que no tiene servicio.
- Asignación de canal dinámica: Este tipo de asignación consiste en hacer cambio de canales entre células, el BSC cuenta con un algoritmo para la repartición de canales entre el cluster por lo que ninguna célula del mismo cluster utiliza el mismo canal. Este tipo de asignación aumentan las prestaciones del sistema, pero por otro lado hace que la BSC tenga que realizar una gran cantidad de computo en tiempo real.

### División celular (Cell Splitting)

Esta estrategia es muy utilizada cuando el número de usuarios conectados a una célula es más que la permitida afectando el servicio de calidad. Como sabemos para una zona con muchos usuarios conectados a la vez

requiriendo el servicio, se hace la utilización de células muy pequeñas para tener más canales disponibles en un área geográfica con dicha célula. De lo contrario para zonas con pocos usuarios se utilizan células más grandes ya que la asignación de canales es mínima debido a la cantidad de usuarios. En la figura 22 se muestra cómo se realiza una subdivisión de cobertura celular.

Esta estrategia utilizada requiere más infraestructura, ya que las células originales se dividen en células más pequeñas para soportar más tráfico, Por lo que genera un gasto extra que es redituable debido a los nuevos usuarios conectados.

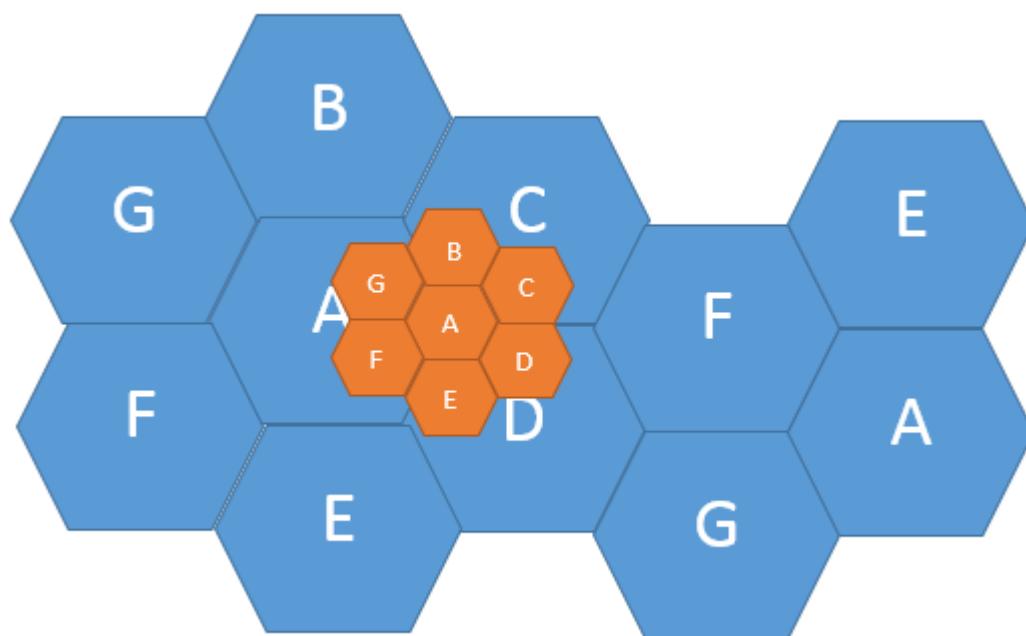


Figura 22 División de sistema celular en células más pequeñas

### Interferencia.

Este concepto se refiere a la degradación de la señal provocada por las perturbaciones radioeléctricas. Esta interferencia se clasifica en:

- Interferencia co-canal: Es un tipo de interferencia causada por las células que utilizan la misma frecuencia. La interferencia ocurre debido al movimiento de canales entre células provocado por un algoritmo que tiene como objetivo dar el mejor servicio, generando el movimiento de frecuencias en canales.
- Interferencia de canal adyacente: este tipo de interferencias ocurre en los límites de las células debido a que intervienen frecuencias diferentes.

### **Desvanecimiento (Fading).**

Este fenómeno ocurre cuando una estación móvil se aleja de la fuente de cobertura, generando una disminución en la señal. La estación móvil cuenta con circuitos necesarios que hacen un cálculo para evitar este tipo de fenómenos. Pero cuando el usuario se mueve a una velocidad muy grande es imposible evitar esto.

### **Capacidad**

La capacidad del sistema celular se refiere a la cantidad de tráfico que puede soportar en toda el área de cobertura. Por lo general los sistemas celulares se diseñan para soportar una gran cantidad de tráfico, sobre todo en áreas densamente pobladas, la capacidad por cada bloque de canales distribuido en una célula se calcula mediante la aplicación de la fórmula de Erlang, representada en la ecuación 3: [10]

$$E = \lambda * t * h \quad (3)$$

Donde:

$\lambda$  = Número de llamadas entrantes por unidad de tiempo.

$t^*h$  = tiempo promedio de holding expresado en horas por llamada

Erlang fue el inventor de la teoría del tráfico telefónico. Su nombre vino a denominar la unidad adimensional que expresa la densidad del tráfico telefónico E y de sus modalidades. Una línea permanentemente ocupada corresponde a 1E; una línea permanentemente libre corresponde a 0 E. La palabra Erlang significa Extra Relatively Language. [10]

El Erlang B es la ecuación de ingeniería de tráfico telefónico usada cuando el tráfico deviene aleatorio y se pierden las colas. El Erlang B asume el bloqueo de llamadas y las distribuye automáticamente hacia otra ruta, haciendo desaparecer el bloqueo. El sistema debe ser capaz de ofrecer el servicio a varios miles de unidades móviles en el área de cobertura con un número organizado de canales. También existe el Erlang C, esta fórmula de ingeniería de tráfico telefónico es usada cuando el tráfico es aleatorio y se mantienen las colas. El Erlang C asume todas las llamadas, reteniéndolas hasta que una línea esté disponible. La capacidad que aportan los sistemas celulares es función del número de canales utilizado o ancho de banda disponible, del tamaño de las células y de la configuración de los clusters. La capacidad se verá favorecida cuanto menor sea la célula y cuantas menos células sean necesarias por cluster. Este último parámetro estará fuertemente ligado a la relación de interferencia co-canal que el sistema sea capaz de soportar. Respecto al tamaño de la célula, este estará limitado por

la capacidad del protocolo de gestión de la movilidad y por la velocidad a la que se desplacen los móviles en la zona de servicio. [10]

### **Calidad**

La calidad es uno de los temas más importantes ya que esto dará más clientes y una mejor ganancia. Pero aparte de esto en la telefonía celular hay un organismo que se encarga de la calidad denominado GoS. El GoS permite solo un dos por ciento de llamadas bloqueadas, es decir, si se hacen 100 llamadas en una red celular GSM, el GoS solo te permite fallar en 2 llamadas.

## **2.4 EVOLUCIÓN DE LOS SISTEMAS DE TELEFONÍA CELULAR**

### **2.4.1 Primera Generación (1G)**

La primera generación se caracterizada por su transmisión de voz analógica, utilizando la modulación FM sin ningún tipo de seguridad, es decir cualquier persona con un receptor de radio frecuencia en la frecuencia de transmisión podía escuchar las conversaciones entre las personas. Como todo era analógico los equipos de telefonía eran demasiado grandes provocando ser impráctico tener un celular, pero un lujo a la vez ya que este tipo de telefonía era muy caro. Con el paso del tiempo muchas empresas les intereso brindar este tipo de servicio entre los estándares más conocidos esta:

#### **NMT (Nordic Mobile Telephone).**

Es un sistema que brindaba servicio en países como Finlandia, Dinamarca y Noruega. Esto lo hacía en las bandas de frecuencia de 450 MHz y 900 MHz. Tuvo un gran éxito debido a su buena calidad en sus llamadas.

#### **AMPS (Advanced Mobile Phone System).**

Es uno de los sistemas de comunicaciones de telefonía celular de la primera generación más famoso implementado por los laboratorios Bell. Proporcionaba una cobertura a nivel nacional, implementado primeramente en Estados Unidos de América y expandido con ligeras modificaciones en países como Inglaterra y Japón. Este sistema contaba con 832 canales de 30KHz para subida y la misma cantidad para la bajada de datos. Este servicio de telefonía estaba en la frecuencia de 800 MHz abarcando hasta los 900 MHz, los canales sobrantes eran utilizados para el control de la red. Algo muy importante que dejo este estándar es que introdujo el concepto de handover. El cual consiste en cambiar un usuario de una celda a otra celda cuando este está en movimiento.

#### **Hicap.**

Fue desarrollado por NTT(Nippon Telegraph and Telephone). Uno de los aspectos más importantes por mencionar, es que este sistema utilizaba

FDMA para el acceso de sus usuarios, utilizando así menos ancho de banda y dando un mejor servicio a sus usuarios.

#### **CDPC (Cellular Digital Packet Data).**

Tenía una operación en la banda de frecuencia de 800MHz a 900MHz con una velocidad de transferencia de 19.2Kbps. Daba un buen servicio con un costo alto. Debido a estos costos perdió usuarios y dejó de ofrecer el servicio.

#### **Mobitex.**

Es un estándar que apareció en el año de 1986, que se basaba en el modelo del sistema OSI, en este estándar ya se implementaban sistemas de seguridad que permitieran que nadie interviniera las llamadas. Además de que sus precios eran más bajos que los de otros estándares.

#### **DataTac.**

Es un estándar implementado por Motorola que utilizaba la banda de frecuencia de los 800MHz con canales de 25KHz. Fue muy importante en su tiempo debido a que era una red que no era afectada con el tráfico por lo que las llamadas nunca fallaban.

### **2.4.2 Segunda Generación (2G)**

La segunda generación se refiere al paso de la tecnología analógica a la tecnología digital. En esta generación se implementaron varios tipos de protocolos de comunicación que solucionaban el problema del tráfico de datos dando así la ventaja de tener miles de usuarios sin gastar un ancho de banda muy grande.

Además, ofrecía un servicio de mensajes de texto llamado SMS (Short Message Service) el cual tenía un costo extra y permitía enviar texto de un celular a otro. Varias compañías implementaron este tipo de sistema y presentaba la desventaja de que no eran compatibles los protocolos utilizados de las empresas por lo que te limitaba a llamar a celulares de la misma empresa.

Los estándares más utilizados son:

#### **GSM (Global System for Mobile Communications).**

Este estándar de telefonía celular permite llamadas de voz, además de mensajería de texto. Está en 4 frecuencias distribuidas dependiendo del país en el que se encuentran:

- GSM-1800: Se encuentra en la frecuencia de 1800MHz y se utiliza en algunas partes de Europa.

- GSM-1900: Se encuentra distribuida en una frecuencia de 1900MHz, Se utiliza en algunas partes de Estados Unidos.
- GSM-850: Se encuentra distribuida en una frecuencia de 850MHz, Se utiliza en Canadá y Latinoamérica.
- GSM-900: Se encuentra distribuida en una frecuencia de 900MHz, Se utiliza en la mayoría de los países del mundo, más de 100 países optaron por este estándar en esa frecuencia.

Este estándar de telefonía celular es uno de los más usados generando que el tráfico de usuarios sea muy grande, por lo que se optó por utilizar una estrategia de acceso al medio, la estrategia utilizada es el TDMA con una combinación de FDMA, donde distribuyen las frecuencias del ancho de banda entre los usuarios además de darles al igual un tiempo para acceder a ese canal. Además de esto para la transmisión de los datos utiliza la modulación GMSK, que es una variante del FSK.

### **HSCSD (Hi-Speed Circuit-Switched Data)**

Este estándar es una mejora del GSM, la cual aumenta la velocidad de transmisión de datos. Es decir, es una copia del GSM con una mejor transmisión de datos.

### **CDMA-One.**

Es un estándar norteamericano que fue empleado para la transmisión de voz, señalización y datos, no se popularizó, solo se utilizó en ciertos lugares. Para acceso al medio utilizaba el CDMA, el cual consiste en enviar todos los datos de manera codificada, lo que permite él enviar datos por el mismo canal sin traslape de información.

### **GPRS (General Packet Radio Service).**

Los móviles de segunda generación han ido evolucionando hasta tal punto que se puede hablar de una “generación 2.5” consistente en móviles que sin ser 3G, incorporan algunas de las mejoras más comunes de este último estándar. El protocolo más común en este tipo de celulares será GPRS, proporcionando datos por conmutación de paquetes principalmente a las redes GSM basadas en tecnología 2G, un tipo de conmutación que, a diferencia de la conmutación de circuitos GSM (donde el circuito queda reservado durante el tiempo total de la comunicación, se esté utilizando o no), es un sistema basado en necesidad, por lo que si no se está enviando ningún dato, las frecuencias quedan libres para uso por parte de otros usuarios aunque la comunicación no haya acabado. Entre las ventajas obtenidas gracias al uso de este estándar destaca el hecho de poder asignar más de un canal a cada comunicación sin miedo a saturar la red, el abaratamiento de las tarifas ya que GPRS posibilita la tarificación por información cursada

(no por tiempo de conexión), y la simplificación y bajo coste del proceso de migración de una red GSM a otra UMT, dado que los cambios a realizar en una estación para pasar de GSM a GPRS serían mínimos, además de compartidos en un futuro por el protocolo UMTS. [13]

#### **EDGE (Enhanced Data rates for GSM Evolution).**

Se considera una evolución de GPRS, y funciona sobre cualquier red GSM que posea GPRS. Con EDGE se consigue triplicar la capacidad a la hora de transportar datos con respecto a GPRS, la posibilidad de aumentar el número de usuarios de una operadora, o añadir capacidad extra al servicio de llamadas de voz. Se utilizará la misma estructura de trama TDMA (Time Division Multiple Access – Acceso Múltiple por División en el Tiempo), mismo canal lógico y mismo ancho de portadora (200KHz) que para el estándar GSM, lo que permite mantener intacto el plan celular de la red sobre la que se implementa. Con EDGE estamos un paso más cerca del estándar UMTS y las redes 3G, introduciendo, además de mayores tasas de transferencia de información, un nuevo esquema de modulación: 8-PSK. Más que nuevos servicios este estándar es una mejora de los existentes GPRS y HSCSD (High-Speed Circuit Switched Data – Comutación de Circuitos de Datos de Alta Velocidad) mediante la introducción de una nueva capa física. La implementación de EDGE por los operadores de red ha sido diseñada para ser simple. Sólo será necesario añadir a cada celda un transceptor adecuado, siendo en la mayoría de los casos posible realizar la actualización de forma remota. Este nuevo transceptor funcionará de manera correcta en modo GSM, comutando a EDGE cuando el servicio solicitado lo requiera. [13]

### **2.4.3 Tercera Generación (3G)**

La tercera generación dio un gran avance en las redes celulares, con la evolución de la tecnología celular, se contó con nuevas necesidades de transmisión de datos ya no solo para llamadas y mensajería, si no que ahora el uso de internet era necesario. Esta tercera generación ya permitió que un usuario tenga la posibilidad de reproducir y descargar archivos multimedia a gran velocidad.

Debido a esta velocidad, esta generación trajo consigo el concepto de video llamadas ya que ahora es posible enviar video en tiempo real.

Hay varios estándares en esta generación, los más importantes se mencionan a continuación:

#### **UMTS.**

Es un sistema global de muy buena calidad ya que es compatible con sistemas 2G lo que hace que el usuario pueda alternar entre varias redes sin

perder la conexión. Además, cuenta con componentes terrestres, así como satelitales.

Entre sus características más importantes esta:

- El estándar está pensado en los usuarios por lo que es muy fácil de usar.
- Debido a la accesibilidad en las tarifas lo hace tener un bajo costo.
- Te permite tener servicios que soportan el protocolo ip.

Este estándar de telefonía utiliza para acceso al medio el WCDMA, lo cual le da muchas ventajas al poder tener miles de usuarios con un ancho de banda pequeño.

### **HSPA.**

Se trata de un conjunto de protocolos que mejoraban el estándar UMTS.

**HSDPA:** Las últimas versiones del estándar de telefonía móvil de tercera generación UMTS, introducen un nuevo salto tecnológico con la introducción de la funcionalidad HSDPA (High Speed Downlink Packet Access). Los principales objetivos de HSDPA son incrementar la tasa de transferencia por usuario, mejorar la calidad de servicio ofrecida y, en general, mejorar la eficiencia espectral, especialmente para los servicios de datos, asimétricos y con tráfico a ráfagas, como son la mayoría de servicios de Internet. El funcionamiento de este sistema se basa en la colaboración de múltiples técnicas y algoritmos, como la modulación y codificación adaptativa (AMC), el ARQ híbrido y complejos mecanismos de scheduling (proceso a través del cual se decide cómo comprometer los recursos disponibles ante cierto número de tareas que los necesitan), muchos de ellos en fase de desarrollo. Este nuevo sistema se integra en un entorno ya complejo por sí mismo y existen muchas interacciones entre los diversos protocolos que son potencialmente optimizables. [13]

**HSUPA:** Se trata de un estándar para acercar la red de UMTS al 4G, y se considera como la generación 3.75 (3.75G ó “3.5G+”), desarrollado en el proyecto UMTS de 3GPP. HSUPA es un protocolo de acceso de datos para redes de telefonía móvil con alta tasa de transferencia de subida, pensado para mejorar el HSDPA mejorando la conexión de subida de UMTS/WCDMA. Con HSUPA se mitiga el efecto de la asimetría en las capacidades entre DL y UL (downlink y uplink), haciendo posible la oferta de servicios avanzados. [13]

**HSPA+:** Se consigue un 20% de capacidad de tráfico adicional. Las estaciones base se conectan a la red a través de una conexión Gigabit Ethernet al Proveedor de Servicios de Internet que está a su vez conectado a Internet. Con esto se consigue hacer la red más rápida, fácil de desplegar

y más operativa. A pesar de que la arquitectura UMTS existente puede seguir siendo utilizada, la posibilidad de interconectar directamente la estación base con el GGSN IP es un gran paso hacia el proyecto LTE de 3GPP: 4G. [13]

#### **2.4.4 Cuarta Generación (4G)**

Ya en febrero del 2007 surge la cuarta generación de redes móviles. La principal diferencia con su antecesor son las grandes tasas de subida y bajada que se planean conseguir (Teóricamente llegar a 100 Mbps de bajada en movimiento y 1 Gbps estático). Dentro de las tecnologías consideradas 4g se encuentra la tecnología Wii Max y LTE/advanced; Esta última es la preferida últimamente por las compañías para implementar sus servicios 4g ya que ha demostrado tener más eficiencia en las pruebas de laboratorio:

##### **Wii Max.**

Este estándar permite al usuario una gran velocidad de subida y descarga de datos para internet. Utiliza una estrategia para acceso al medio llamada OFDM la cual es una modulación muy eficaz ya que transmite mucha información, esto lo hace con el uso de varias portadoras ortogonales para no traslape de información.

Para el método de modulación utiliza 64QAM dando la ventaja de enviar grandes cantidades de información en un tiempo reducido.

##### **LTE/advanced.**

LTE-Advanced es el sistema definido por el 3GPP como evolución de LTE, que cumple los requisitos del IMT-Advanced, considerándose por ello la verdadera tecnología 4G, puesto que LTE es en verdad perteneciente a una generación 3.9. LTEAdvanced ha sido definido por 3GPP y está destinado a satisfacer los diversos requisitos de las aplicaciones avanzadas que sean comunes en el mercado inalámbrico en el futuro. [14]

#### **2.4.5 Quinta Generación (5G)**

La red inalámbrica de la próxima (quinta) generación va a abordar la evolución más allá del Internet móvil y va a alcanzar el IoT (Internet de las Cosas) masivo para inicios de 2020. La principal evolución en comparación con 4G y 4.5G (LTE avanzado) de hoy en día es que más allá de las mejoras en la velocidad de los datos, los nuevos casos de uso del IoT y de comunicación crítica van a requerir nuevos tipos de rendimiento mejorado. Por ejemplo, la "baja latencia" es lo que provee interactividad en tiempo real para los servicios que utilizan la nube: esto es clave para el éxito de los vehículos autónomos, por ejemplo. Además, el bajo consumo de energía es el factor que va a permitir que los objetos conectados funcionen por meses o años, sin la necesidad de ayuda humana. [15]

En la figura 23 se aprecia una gráfica y las características de la evolución de la telefonía celular.

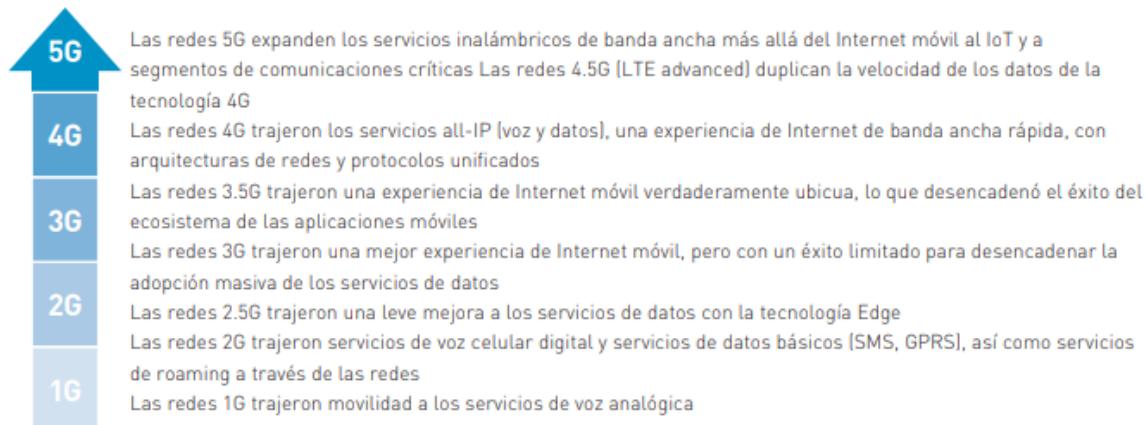


Figura 23 Evolución de la telefonía celular. [15]

## 2.5 ARQUITECTURA DE LA RED DE TELEFONÍA CELULAR GSM

Una red de telefonía celular GSM se compone de varios elementos como se muestra en la figura 24.

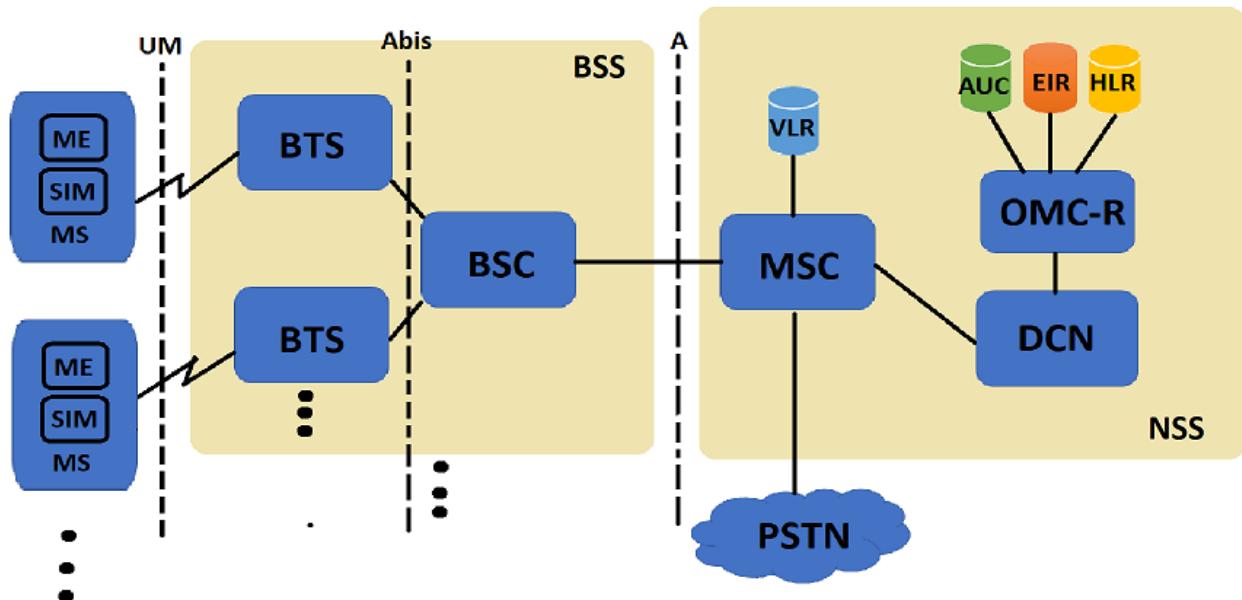


Figura 24 Arquitectura de una red celular 2G GSM

### 2.5.1 Estación Móvil (MS)

Una estación móvil se divide en dos elementos esenciales:

**ME (Equipo Móvil):** Este dispositivo contiene varios módulos:

- Módulo de radio frecuencia es el que controla la recepción y transmisión, además de dar el filtrado y amplificación necesarios para la señal de entrada y la que se encarga de modular, amplificar y emitir la señal de salida.
- Módulo de antena va junto con el módulo de radio frecuencia, este módulo en los primeros equipos se utilizaba externo, ahora con las nuevas tecnologías la antena es interna.
- La unidad Lógica se encarga de todo el procesamiento de datos para la transformación de la voz, que proviene del micrófono, por lo tanto, es analógico y convertido a datos digitales, esto con la utilización de un convertidor analógico digital. Además de esto, se encarga de todo el procesamiento de datos para el arranque de aplicaciones dentro del dispositivo. En la actualidad esta unidad lógica ya cuenta con procesadores muy potentes.
- Módulo de interface de usuario, es la encargada de la comunicación entre el dispositivo y el usuario, por ejemplo, la pantalla, el touch, el micrófono, etc.

**SIM** (Modulo de Identificador de Suscriptor), Es un dispositivo desmontable que guarda las claves de servicio del suscriptor, estas claves son esenciales para que la red identifique el dispositivo. En la figura 25 se muestra el aspecto de una SIM de tamaño completo y la identificación de las terminales.

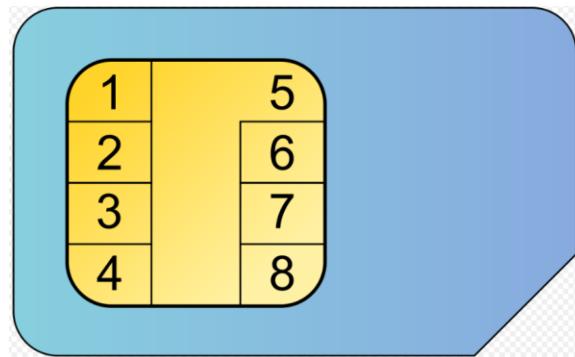


Figura 25 Imagen de SIM [16]

Tabla 2 Conexiones de la tarjeta SIM

1	VCC
2	RST
3	CLK
4	D+
5	GND
6	SWP
7	I/O
8	D-

La tarjeta SIM tiene varios formatos que determinan diferentes tamaños como se muestra en la Figura 26 y la tabla 3:

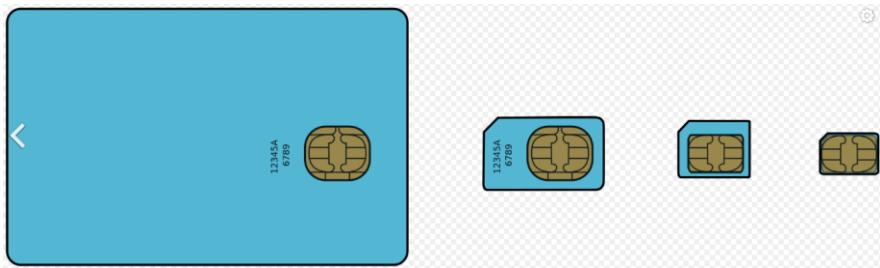


Figura 26 Formatos de tarjeta SIM [17]

Tabla 3 Información de tamaños relacionados con los diferentes formatos de SIM

Tarjeta SIM	Estándar	Largo (mm)	Ancho (mm)	Espesor (mm)
Tamaño completo	ISO/IEC 7810:2003, ID-1	85.60	53.98	0.76
Mini-SIM	ISO/IEC 7810:2003, ID-000	25.00	15.00	0.76
Micro-SIM	ETSI TS 102 221 V9.0.0, Mini-UICC	15.00	12.00	0.76
Nano-SIM	ETSI TS 102 221 V11.0.0	12.30	8.80	0.67

Como se mencionó anteriormente, la SIM guarda datos específicos que lo identifican como usuario en una red celular, estos datos son los siguientes:

- ICCID Identificador Internacional de Tarjetas de Circuitos, este código además de estar guardado en la tarjeta SIM viene impreso sobre esta tarjeta. Es un código de 19 o 20 dígitos.
- IMSI Identificador Internacional del Suscriptor Móvil, Los operadores de telefonía móvil conectan las llamadas a teléfonos móviles y se comunican con sus tarjetas SIM comercializadas usando su IMSI. [18]
- Clave de autenticación Ki es un valor de 16 bytes usado para autenticar las tarjetas SIM en la red móvil. Cada tarjeta SIM tiene una Ki única asignada por el operador durante el proceso de personalización. La Ki también se almacena en una base de datos específica llamada AuC que está implementada como parte integral de la HLR de la red del operador. [18]

### 2.5.2 Subsistema de Estación Base (BSS)

Es la responsable del manejo de tráfico y la señalización entre una estación móvil y el sistema de conmutación de red. Se divide en: [19]

**BTS** (Base Transceiver Station) Cada célula es servida por una BS, que es el equipo físico que cubre el radio de cobertura del área geográfica conocida como célula, dotada de equipos de transmisión y recepción de baja potencia

en varias frecuencias o canales, restringiendo su cobertura a la misma, al aprovechar la propagación limitada de las ondas de radio a frecuencias elevadas. La BTS sirve de control central para todos los usuarios permitiendo tenerlos permanentemente localizados dentro de la célula (Siempre que la MS este encendida), también registra el proceso de suscriptor originador de llamada y realiza algunas funciones del sistema de control. La BTS es responsable de las funciones de radio dentro del sistema celular como son: gestión de las comunicaciones de radio con algún grado de procesamiento de señales por medio de un enlace radioeléctrico bi-direccional entre las MS y la red celular que les brinda el servicio, manejo del traspaso de llamadas entre células (Handover), control del nivel de potencia de la señal tanto de las Estaciones Base como de las Estaciones Móviles, entre otras. [10]

En la figura 27 se muestran el hardware y los servicios proporcionados por la BTS.

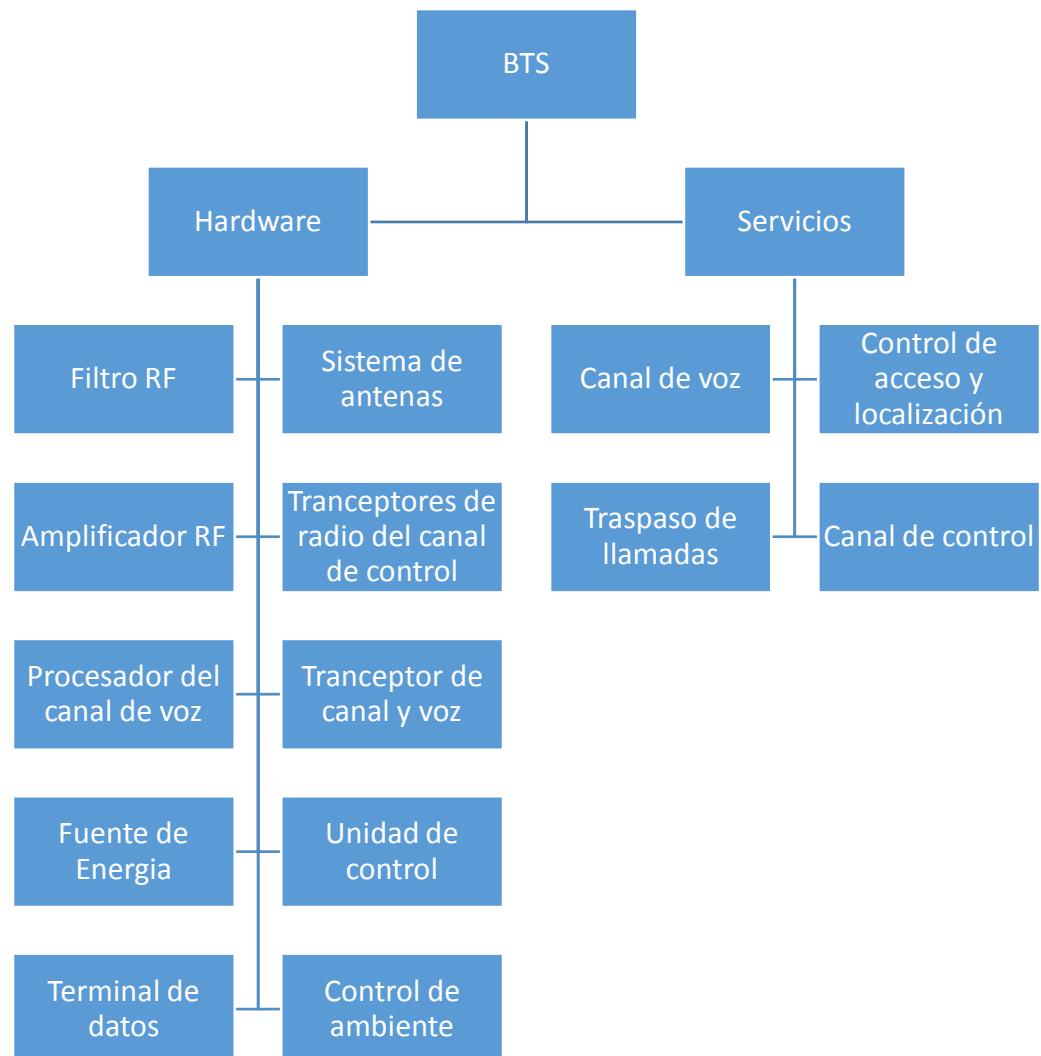


Figura 27 Hardware y servicios que utiliza una estación base.

**BSC**(Base Station Controller) Es el control programable de todos los periféricos de la BTS, la comunicación de datos, transmite software, la inicialización del sistema, la integridad del sistema, procesamiento de llamada y la ejecución de los diagnósticos requeridos. [10]

El controlador de estación base se encarga de:

- Manejo de canales de distintas estaciones móviles para la realización de un handover.
- Controla la potencia de transmisión de la estación móvil.
- Supervisa las llamadas.
- Enciende y apaga el transceptor de radio de la estación base controlada.
- Inyecta información a los canales de control y usuario.
- Realiza pruebas de diagnóstico.

En la figura 28 se muestra un subsistema de estación base.



Figura 28 Pequeño Subsistema de estación base. [20]

### 2.5.3 Subsistema de conmutación de red (NSS)

El subsistema de conmutación de red es la parte central de cualquier sistema de telefonía móvil y controla varios BSS. Sus componentes son responsables de todas las funciones de procesamiento, control y banco de datos de llamadas que son necesarias para examinar la autenticación, configurar la llamada, cifrar los datos y controlar el roaming. Para poder lograr lo anteriormente mencionado el subsistema de conmutación de red se divide en varios elementos como se muestra en la figura 29. [21]

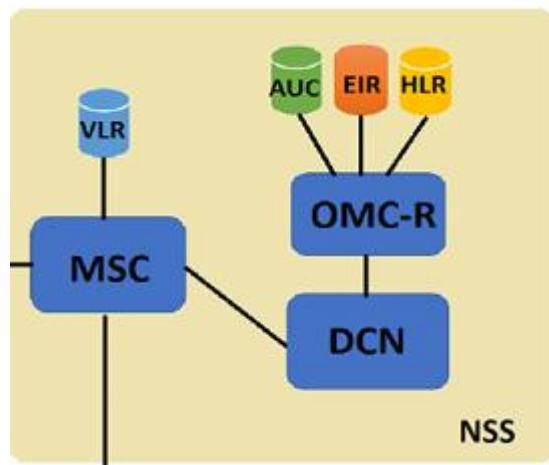


Figura 29 Subsistema de conmutación de red NSS.

**MSC** (Mobile Switching Center) Es una de las partes más importantes del subsistema de conmutación de red, es decir es el que se encarga de iniciar, terminar y canalizar llamadas a través de la BSC y BS. Es una central telefónica que realiza la conexión entre usuarios móviles dentro de la red, desde usuarios móviles a la red telefónica pública conmutada y desde usuarios móviles a otras redes móviles. El MSC también administra los traspasos a estaciones base vecinas, mantiene un registro de la ubicación de los suscriptores móviles, es responsable de los servicios y facturación de los suscriptores. [22] En la figura 30 se muestra el aspecto físico de un MSC.



Figura 30 Centro de Conmutación Móvil [23]

**VLR** (Visitor Location Register) El Registro de ubicación de visitantes (VLR) es una base de datos en una red de comunicaciones móviles asociada a un Centro de conmutación móvil (MSC). El VLR contiene la ubicación exacta de

todos los suscriptores móviles actualmente presentes en el área de servicio del MSC. Esta información es necesaria para enrutar una llamada a la estación base correcta. La entrada de la base de datos del suscriptor se elimina cuando el suscriptor abandona el área de servicio. [24]

**HLR** (Home Location Register) El Registro de ubicación de origen es una base de datos de una red móvil en la que se almacena la información de todos los suscriptores móviles. El HLR contiene información sobre la identidad de los suscriptores, su número de teléfono, los servicios asociados e información general sobre la ubicación del suscriptor. La ubicación exacta del suscriptor se mantiene en un registro de ubicación de visitantes. [25]

**EIR** (Equipment Identity Register) El Registro de identidad de equipos (EIR) es una base de datos que contiene un registro de todas las estaciones móviles (MS) que están permitidas en una red, así como una base de datos de todos los equipos que fueron bloqueados por el usuario, por extravió o robo. La identidad de la estación móvil viene dada por la Identidad Internacional de Equipos Móviles (IMEI). Cada vez que se realiza una llamada, el MSC solicita el IMEI de la estación móvil, que luego se envía al EIR para su autorización. [26]

**AuC** (Authentication Centre) El Centro de autenticación (AUC) es una función en una red GSM utilizada para la autenticación de un suscriptor móvil que desea conectarse a la red. La autenticación se realiza mediante la identificación y verificación de la validez de la tarjeta SIM.

Una vez que el suscriptor está autenticado, el AUC es responsable de la generación de los parámetros utilizados para la privacidad y el cifrado del enlace de radio. Para garantizar la privacidad del suscriptor móvil, se asigna una Identidad Temporal del Suscriptor Móvil (TMSI) durante el tiempo que el suscriptor está bajo el control del Centro de Comutación Móvil específico (MSC) asociado con el AUC. [26]

#### **2.5.4 Subsistema de operación y mantenimiento (OSS).**

El centro de operaciones y mantenimiento (OSS) proporciona los medios para que el operador controle la MS, BSS y la NSS que forman la parte operacional del sistema GSM. Es responsable del mantenimiento y operación de la Red, de la gestión de los equipos móviles y de la gestión y cobro de cuota. El centro está conectado a los sistemas de conmutación GSM (EIR, AuC, HLR, VLR) y a los BSC. El centro implementa aplicaciones llamados OSS (Operating support System o Sistema de soporte operacional). Los OSS ofrecen a los clientes apoyo para la administración centralizada, regional y local, su principal función es proporcionar una visión general de la red y apoyar las actividades de mantenimiento de la operación y organizaciones de mantenimiento que requiere una red GSM. [27]

## **2.5.5 Sistema de conmutación de red pública (PSTN).**

Este sistema se encarga de conectar las llamadas entre redes celulares y cualquier teléfono ya sea una estación móvil o un teléfono fijo. Si una persona quiere llamar a un celular de una compañía diferente, lo que hace la red GSM es que lo enlaza a la red pública, ya esta se encarga de buscar al usuario que queremos llamar.

## **2.6 PROTOCOLOS E INTERFACES DE LA ARQUITECTURA GSM**

### **2.6.1 Modelo de Referencia OSI.**

El modelo de referencia OSI fue creado por ISO en el año de 1984, este sistema define la arquitectura de interconexión de sistemas de comunicaciones.

El modelo OSI se encarga de dar una estructura a cualquier tipo de estándar de comunicación, en la red GSM no es la excepción por lo que el Modelo OSI se encarga de la estructura del estándar GSM de la segunda generación de telefonía celular.

En la figura 31, describiremos cada una de las capas, donde mencionaremos sus características principales:

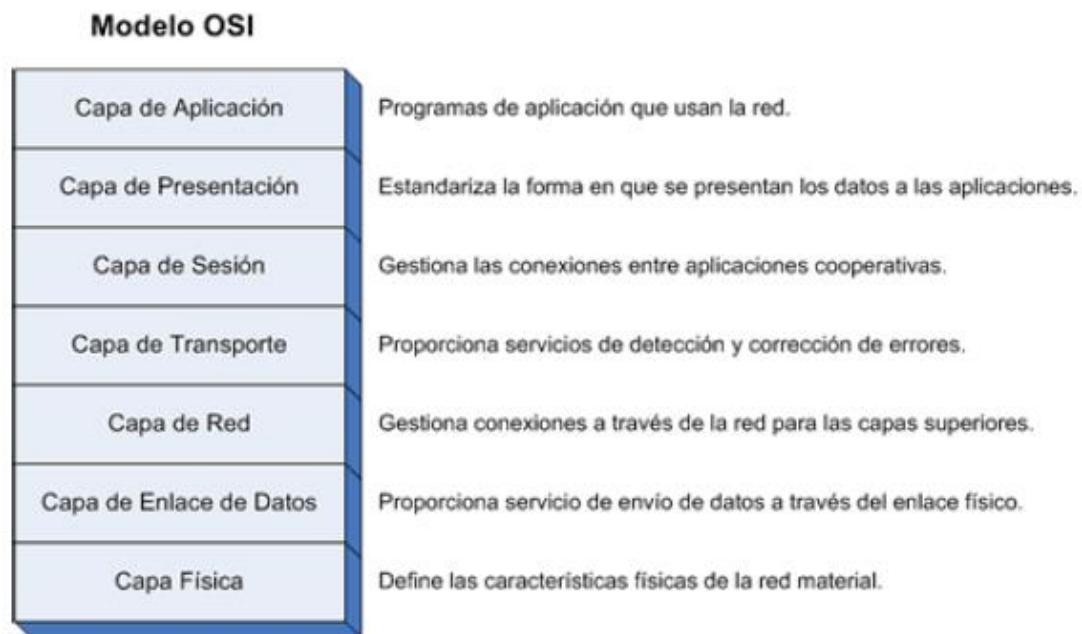


Figura 31 Esquema funcional de las capas del modelo OSI [28]

### **Capa Física.**

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física. Si desea recordar la Capa 1 en la menor cantidad de palabras posible, piense en señales y medios. [29]

Además de esto la capa física tendrá en cuenta aspectos como:

- Se encarga de seleccionar el medio por el cual se transmitirá la información.
- También tiene como objetivo encargarse de la codificación y modulación adecuados para el medio por el cual se transmitirá.
- También se encarga de la parte del receptor, es decir selecciona la demodulación adecuada para decodificar la señal.
- Dar garantías de conexión origen-destino. En este punto es de notar que el destino no es el usuario final destinatario de la llamada, sino el siguiente punto en la red por el que pasa la llamada como parte de un camino hasta el destinatario. Así mismo el nivel físico garantiza la conexión, pero no la fiabilidad de esta. [28]

### **Capa de enlace.**

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio. [29]

### **Capa de Red.**

Se encarga de que la información transmitida llegue al destinatario final a pesar de que no esté directamente conectado al origen, determinando la ruta de los datos (direcciónamiento lógico). También provee de mecanismos para controlar la congestión de la red. [28]

### **Capa de transporte.**

Su misión es recibir, dividir en partes más pequeñas la información que recibe de capas superiores si fuera necesario, y empaquetarla en los llamados “Segmentos” con cabeceras en las que se especifica el servicio de transporte provisto para la sesión en particular que está transmitiendo. En el equipo receptor la labor será la complementaria, leyendo las cabeceras puestas por

su homólogo y pasando a las capas superiores la información de forma correcta. [28]

### **Capa de sesión.**

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación. Si desea recordar la Capa 5 en la menor cantidad de palabras posible, piense en diálogos y conversaciones. [29]

### **Capa de presentación.**

Esta capa se encarga de la compatibilidad de la información enviada. Es decir, esta capa convierte la información a un formato común que sea compatible con todos.

### **Capa de aplicación.**

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente. [28]

## **2.6.2 Interfaces de la red GSM.**

Entre los diferentes equipos utilizados para una red GSM, debe de existir una comunicación, pero debido a que cada equipo hace diferentes procesos, si este equipo enviara información a otro, no podría entenderlo, por esta razón se crearon interfaces de comunicación entre los diferentes dispositivos, para crear un mismo protocolo de comunicación entendible entre los dos sistemas que se comunican.

En la figura 32 se ve la conexión de estas interfaces:

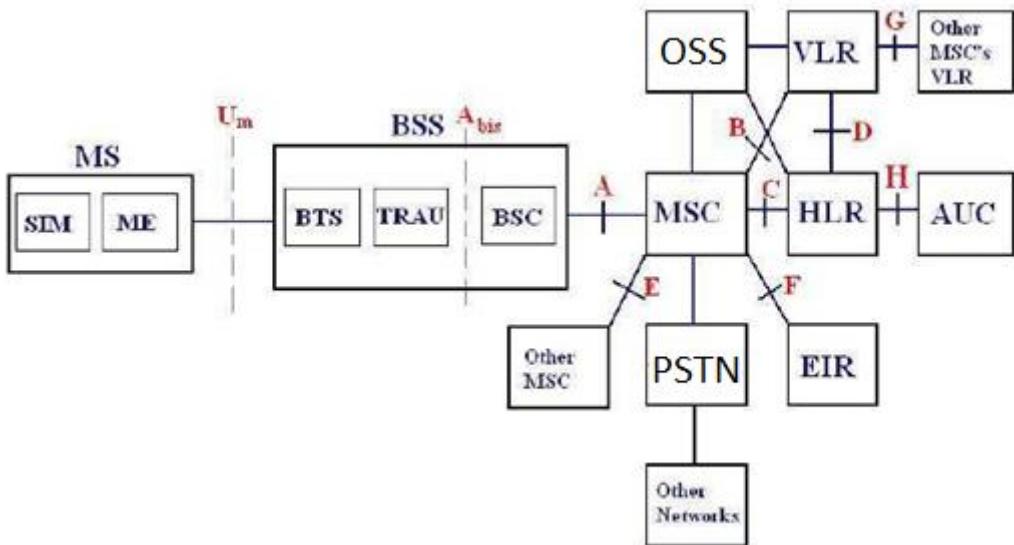


Figura 32 Esquema de interfaces en el sistema GSM [28]

### Interfaz Um.

Interfaz conectada entre la MS y la BSS, proporciona los servicios de envío de datos. Esta interfaz es la encargada de darle todo el beneficio de la red celular a la estación móvil teniendo como intermediario a la estación base (BTS).

### Interfaz Abis.

Es la interfaz conectada entre la BSC y la BTS, tiene una velocidad de envío de datos de 64Kbps para voz y 16Kbps para la señalización. A través de este enlace el controlador de estación base le da órdenes a la estación base, para así tener un control de los canales de transmisión, entre otras cosas.

### Interfaz A.

Esta interfaz conecta a la MSC con la BSC, esto para el control de manejo de llamadas, gestión de la movilidad cuando un usuario se mueve de un área de servicio a otra, además de hacer la gestión de la BSS.

Esta interfaz soporta canales de 64Kbps para la señalización y envío de dato. Los protocolos utilizados para esto son:

- DTAP es un protocolo para transferir información de señalización entre la MS y la MSC en redes GSM.

- BSSAP es un protocolo para enviar información de control de la MSC a la BSS, entre esta información está la asignación de canales de tráfico entre la MSC y la BSS.

#### **Interfaz B.**

Esta interfaz es la que conecta el VLR con el MSC, normalmente es una interfaz interna, esto debido al envío de datos consecutivos y de gran tamaño. Pero esto se deja a disposición de la compañía, pero lo más recomendable es que sea una interfaz interna.

#### **Interfaz C.**

Esta interfaz conecta al MSC con el HLR, por lo que tiene la función de conectar al MSC para solicitar la tarifa de un usuario, además de poder conectar otra MSC que pida la información de un usuario cuando este no está en su área de servicio.

#### **Interfaz D.**

Esta interfaz se utiliza para intercambiar los datos relacionados con la posición de la estación móvil y los datos de suscripción del usuario. El VLR informa al HLR sobre la posición de una estación móvil, proporcionándole un número de seguimiento a fin de que pueda encaminar las llamadas. En el otro sentido, el HLR envía al VLR de la MS los datos necesarios para soportar los servicios contratados por el usuario. Cuando la estación móvil pasa a estar en el área servida por otro VLR, el HLR envía al primer VLR la orden de que borre el registro de dicha MS. [28]

#### **Interfaz E.**

Esta interfaz se encarga de la conexión entre MSC y MSC, es decir, cuando un usuario se mueve de una BSS a otra BSS el MSC tiene que comunicarse con otro igual para decirle que la estación móvil ahora se conectara a él.

#### **Interfaz F.**

Es una interfaz utilizada cuando el MSC quiere comprobar la identidad de una estación móvil, es decir comparar el IMEI.

#### **Interfaz G.**

Esta interfaz se utiliza para conectar dos VLR de diferentes MSC, para el cambio de información cuando se hace un salto de una MS a un diferente MSC.

#### **Interfaz H.**

Es una conexión entre el HLR y el AUC, esta conexión es interna.

## Interfaz I

En el interfaz MS-MSC se da el intercambio transparente de datos entre la estación móvil y el centro de conmutación móvil. [28]

### 2.6.3 Protocolos y señalización en la red GSM.

La red GSM cuenta con la información de los usuarios por lo que debe ser capaz de transmitir dentro de la propia red y hacia otras redes. Por esta razón es necesario que realice funciones de conmutación y conectividad hacia la PSTN. Otra necesidad son los aspectos de señalización provocados por la movilidad de las terminales.

En la figura 32 se ve el esquema de señalización de la red GSM, este esquema está pensado para tener un alto rendimiento entre la comunicación de los componentes de una red además de los componentes de otras redes externas. Estos protocolos se explicarán a continuación basándonos en la figura 33, para tener una noción del funcionamiento y objetivo de estos, dentro de la red.

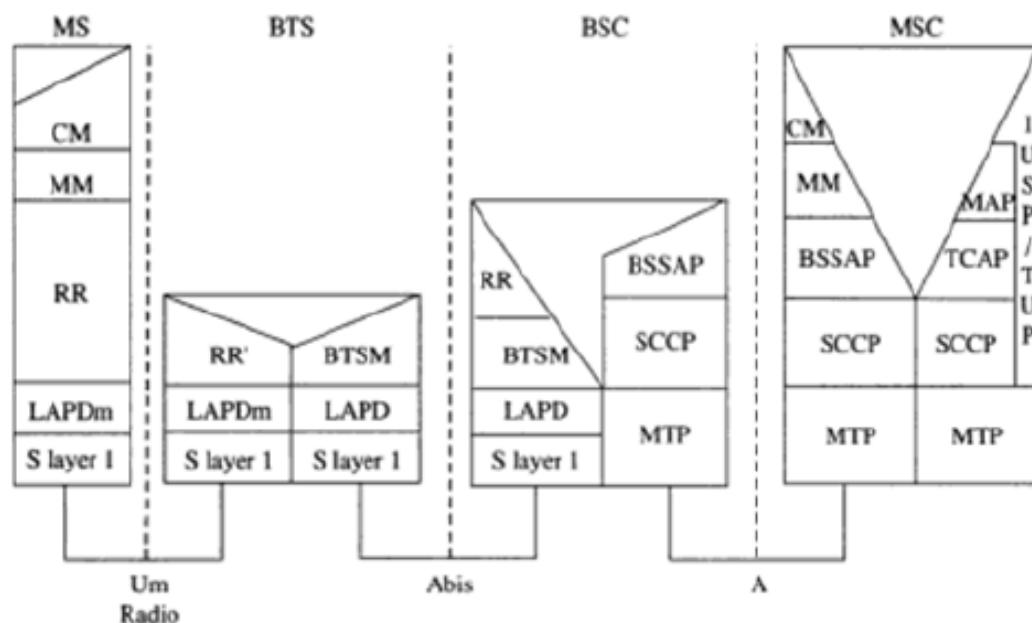


Figura 33 Torre de protocolos GSM. [28]

La capa física será la específica de la red GSM en las interfaces Um y Abis, de cuyas características generales se dará una visión en el apartado 2.7.3. No obstante, para los mensajes de señalización sobre el interfaz A BSS-MSC se utilizan los servicios de la parte de transferencia de mensajes MTP (Message Transfer Part), que proporciona una transmisión fiable y segura. [28]

En el nivel de enlace pueden verse dos protocolos distintos sobre los interfaces Um y Abis. Por un lado, LAPD (Link Access Procedure on D channel), y por otro LAPDm, que es una modificación del primero apropiada para la interfaz radio MS-BTS. LAPD (también conocido como ITU Q.921) es un protocolo de control de enlace de datos para los canales tipo D. Tiene dos formas de operación, orientada o no a conexión, y en esencia está diseñado para convertir un enlace físico poco fiable en un enlace de datos fiable. Al igual que para el nivel físico, entre BSS y MSC se utilizará MTP en la comunicación. [28]

El nivel de red se divide a su vez en tres protocolos distintos:

- Gestión de la Conexión (CM - Connection Management)

CM está dividida en diferentes entidades:

Control de llamadas (CC): Es el que se encarga de hacer, mantener y finalizar las llamadas. CM tiene que interactuar con los diferentes componentes, HLR, GMSC y el VLR, para la gestión de conmutación de circuitos, voz y datos.

Servicio suplementario de gestión (SS). Le da el privilegio al usuario de controlar su servicio básico.

Servicio de mensaje corto (SMS). Este servicio se encarga de conectar al MSC con el MS

- Gestión de movilidad (MM - Mobility Management).  
Este servicio gestiona todo lo relacionado con las bases de datos VLR y HLR, además de la autenticación de los usuarios.
- Gestión de recursos de radio (RR - Radio Resource Management).  
Este servicio gestiona la transmisión sobre la interfaz de radio que se encarga de conectar a la estación móvil con la estación base.

CM y MM se implementan en la interfaz A de la MSC, mientras que el RR lo hará sobre la BSC. El protocolo usado para transferir los mensajes CM y MM será BSSAP (Base Station System Application Part), que permite el control directo de la BSS. Por su parte SCCP se encarga del direccionamiento y enrutamiento de las centrales, ya que ha sido ideado fundamentalmente para

posibilitar la transferencia de mensajes entre dos Puntos de Señalización cualesquiera, pertenezcan a la misma red SS7 o a dos distintas. [28]

Para el establecimiento y supervisión de las llamadas establecidas con usuarios de las redes PSTN, se utilizan los protocolos TUP e ISUP respectivamente. Para los mensajes de señalización con las entidades HLR, VLR, otras MSC, etc., propias de GSM, se usa el protocolo MAP complementado por TCAP (Transaction Capability Application Part), que proporciona funciones para la comunicación con el extremo remoto de una cadena de señalización y permite el establecimiento de múltiples diálogos. [28]

Tabla 4 Resumen de las principales interfaces en una red GSM [28]

Interfaz	Situada entre	Descripción	Intercambio de información de	
			Usuario	Señalización
A	MSC-BSC	Permite el intercambio de información sobre la gestión del subsistema BSS, de las llamadas y de la movilidad. A través de ella, se negocian los circuitos que serán utilizados entre el BSS y el MSC.	SI	SS7
Abis	BSC-BTS	Permite el control del equipo de radio.	Si	LAPD
B	VLR-MSC Asociados	VLR es la base de datos que contiene toda la información que permite ofrecer el servicio a los clientes que se encuentran en el área de influencia de sus MSC asociados. Por lo tanto, cuando un MSC necesite proporcionar información sobre un móvil acudirá a su VLR. Esta interfaz NO debe ser externa NO(por desempeño, por el volumen de información intercambiado).	NO	MAP/B
C	HLR-GMSC	Es la interfaz utilizada por los gateways GMSC para enrutar la llamada hacia el MSC destino. La GMSC no necesita contar con un VLR, se trata de un nodo que solo transmite llamadas.	NO	MAP/C
D	HLR-HLR	Permite intercambiar información entre ambas bases de datos, esta información se encuentra relacionada con la posición del móvil y la gestión del servicio contratado por el usuario.	NO	MAP/D

E	MSC- MSC	Permite intercambiar la información necesaria para iniciar y realizar un intercambio Inter-MSC cuando el móvil cambia de área de influencia de un MSC a otro.	SI	MAP/E, RDSI e ISUP
F	MSC-EIR	Utilizada cuando el MSC desea comprobar el IMEI de un equipo.	NO	
G	VLR-VLR	Utilizada para permitir la interconexión entre dos VLRs de diferentes MSCs.	NO	MAP/G
H	HLR-AuC		SI	MAP/H
I	MSC-MS	Permite el intercambio transparente de datos entre el MSC y el MS a través del BSS.		
Um	BSS-MS	Es la interfaz de radio, se encuentra entre la estación móvil y el BSS.	SI	LAPDm

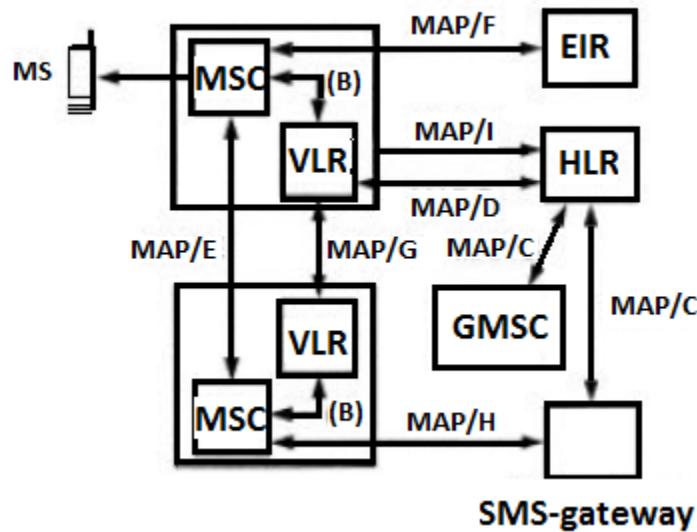


Figura 34 Protocolos MAP/X [28]

## 2.7 RED DE ACCESO. INTERFAZ AIRE.

En este apartado se muestra cómo se envían los datos por la interfaz aire para que el usuario los reciba y se pueda hacer una comunicación entre MS y la red GSM.

Tabla 5 Características generales del protocolo GSM [28]

Parámetro	GSM	
Frecuencia de Transmisión (MHz)		
-Base a Móvil	935 – 960	1805 - 1880
-Móvil a Base	890 – 915	1710 - 1785
Tipo de acceso múltiple	TDMA junto con FDMA	
Método de Duplexado	FDD	
Ancho de banda por radiocanal	200 KHz	
Nº de canales de tráfico por radiocanal	8	
Nº total de canales de tráfico	1000	
Canal vocal:	<ul style="list-style-type: none"> <li>-Tipo de modulación</li> <li>-Velocidad TXon/Desviación Frec</li> <li>-Tipo de VOCODER y velocidad</li> </ul>	
Canal de Servicio	<ul style="list-style-type: none"> <li>-Tipo de modulación</li> <li>-Velocidad de transmisión</li> </ul>	
	<ul style="list-style-type: none"> <li>- GSMK</li> <li>- 270.8 Kbps</li> <li>- 13 Kbps</li> </ul>	
	<ul style="list-style-type: none"> <li>- GMSK</li> <li>- 270 Kbps (NRZ)</li> </ul>	

## 2.7.1 Canalización GSM

En la red GSM existen dos tipos de canales, unos son canales para tráfico y otros para la señalización en la figura 35 se muestra los diferentes tipos de canales.

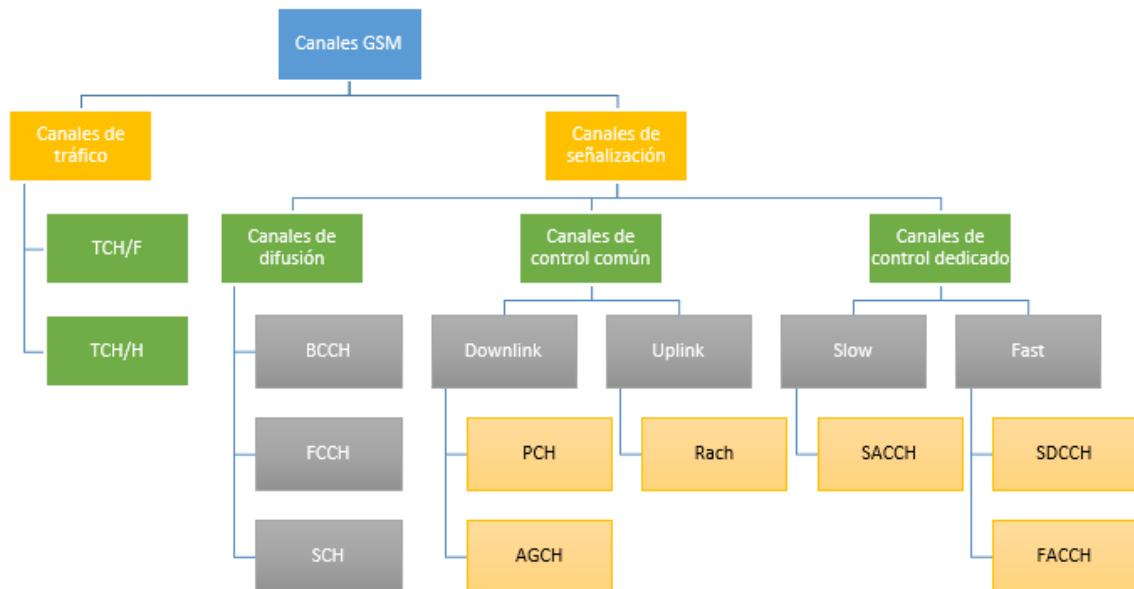


Figura 35 Distribución de los canales GSM

La interface de radio entre móvil y BSS utiliza el protocolo de acceso al enlace en el canal Dm. Cada canal físico soporta varios canales analógicos usados para tráfico y señalización. Las especificaciones GSM definen una gran

variedad de canales lógicos, que pueden ser usados para enlazar la capa física con la capa de datos dentro de las capas de la red GSM. Estos canales lógicos transmiten eficientemente los datos de usuario, aparte de proporcionar el control de la red en cada ARFCN, GSM proporciona asignaciones explícitas de los slots o ranuras de tiempo de las tramas para los diferentes canales lógicos. [30]

Los canales lógicos se separan en dos, como se muestra en la figura 35:

- **Canales de tráfico:**

Los canales de tráfico transportan la voz digitalizada, así como los datos del usuario. Este tipo de canales se llama TCH, los cuales se pueden clasificar de acuerdo a la velocidad de transmisión, ya sea en velocidad completa (full rate) o velocidad media (half rate). Cuando se transmite a velocidad completa los datos están contenidos en un TS (time slot) por trama, de lo contrario cuando se hace a velocidad media, los datos se reparten en el mismo TS pero en diferentes tramas. A continuación, se muestran los canales de tráfico en full rate como en half rate.

- Canales de tráfico en Full Rate:

- Canal de voz en full rate (TCH/FR): Transporta datos de voz a una velocidad de 13 Kbps, después de codificar el canal alcanza una velocidad de 22.8 Kbps.
- Canal de datos a full rate para 9.6 kbps (TCH/F9.6): Normalmente este canal de envío de datos tiene una corrección que lo hace funcionar hasta una velocidad de 22.8KBps.
- Canal de datos a full rate para 4.8 kbps (TCH/F4.8): Al igual que el canal anterior, este canal aplica una serie de correcciones para lograr la velocidad de 22.8KBps.
- Canal de datos a full rate para 2.4 kbps (TCH/F2.4): El estándar GSM aplica unas correcciones que eleva esta velocidad hasta los 22.8 Kbps.

- Canales de traffico en half rate:

- Canal de voz en half rate (TCH/HS): Este canal transporta voz digitalizada con una frecuencia de muestreo menor a la del full rate. Transporta a una velocidad de 11.4 kbps.
- Canal de datos en half rate para 4.8 kbps (TCH/H4.8): transporta datos de usuarios, a una velocidad de 4.8 kbps. Aplicando las correcciones del estándar GSM alcanza una velocidad de 11.4 kbps.
- Canal de datos a half rate para 2.4 kbps (TCH/F2.4): El estándar GSM aplica unas correcciones que eleva esta velocidad hasta los 11.4 Kbps.

- **Canales de control:**

Los canales de control soportan señalización y datos de sincronización entre estaciones base y móviles. Existen tres principales categorías de canales de control en el sistema GSM: Estos son de difusión (BCH, Broadcast Channel), común (CCCH, Common Control Channel) y dedicado (DCCH, Dedicated Control Channel). Cada canal de control consiste en varios canales lógicos los cuales son distribuidos en tiempo para proporcionar funciones necesarias de control en GSM. [30]

- Canales de difusión (BCH).

Opera solamente en downlink y transmite en el primer time slot (TS0) de las tramas de GSM. Este proporciona la sincronización para todos los móviles dentro de una célula y en ocasiones otras células reciben estos datos para poder tomar decisiones de handover. Hay tres tipos de canales, dentro de estos:

- Broadcast Control Chanel (BCCH): es usado para enviar información de la celda y de la red, así como características operativas de la celda.

- Frequency Correction Chanel (FCCH): Este canal envía información a cada móvil sobre la frecuencia de transmisión para poder sincronizar a la frecuencia adecuada con la BTS.

- Synchronization Chanel (SCH): Es transmitido en el TS0 después del FCCH y es usado para identificar a la estación base servidora, mientras que permite a cada móvil sincronizar con las tramas de estación base.

- Canales de control común (CCCH).

Son un conjunto de canales uplink y downlink situados entre la BTS y la MS. Estos ocupan el TS0 de cada trama que no esté ocupada por los BCH o por tramas en espera (IDLE).

Un CCCH está formado de 3 diferentes canales: el canal de búsqueda PCH (Paging Channel), el cual está en un canal de downlink, el canal de acceso aleatorio (RACH – Random Access Channel) el cual está en un canal de up link y el canal de acceso concedido (AGCH - Access Grant Channel) el cual está en un canal de downlink. Como se observa en la figura los CCCH son los canales de control más comúnmente usados y son también usados para llamar a los suscriptores en

específico, asigna los canales de señalización para usuarios en específico y recibe las peticiones del móvil para el servicio.

-Canal de búsqueda (PCH): Es un canal downlink, este canal se encarga de notificar a un móvil en específico de una llamada entrante originada desde la PSTN u otra red.

-Canal de acceso aleatorio (RACH): Es un tipo de canal uplink es un canal usado para confirmar la búsqueda de un PCH y también es usado por los móviles para originar una llamada. [30]

-Canal de acceso concedido (AGCH): Únicamente en Downlink. El AGCH es usado por la estación base para proporcionar un enlace de comunicaciones con el móvil y transporta información que ordenan al móvil operar en un canal físico en particular (en un determinado TS y en un ARFCN) con un canal de control dedicado. El AGCH es el último mensaje enviado por la estación base antes de que un abonado sea trasladado al canal de control. El AGCH es usado por la estación base para responder a un RACH enviado por el móvil en una trama previa CCCH. A grandes rasgos asigna un canal de tráfico o de señalización al móvil. [30]

➤ Canales de control dedicado (DCCH). Estos canales son muy importantes ya que se encargan del roaming, handovers, encriptación, entre otras cosas. Estos canales se dividen en tres tipos de canales, con tráfico bidireccional, es decir, son uplink y downlink.

-Canal de control dedicado autosuficiente (SDCCH): Este canal asegura que la MS siga conectada mientras la BTS y el MSC verifican los datos del usuario y asignan recursos.

- Canal de control asociado lento (SACCH): En el downlink es usado para enviar información lenta pero regular, información de cambios de control al móvil, como instrucciones específicas sobre la potencia a transmitir e instrucciones específicas de sincronía para cada usuario del ARFCN. En el up link, lleva información acerca del nivel de potencia de la señal recibida y de la calidad del TCH así como las mediciones de BCH provenientes de las celdas vecinas. El SACCH es transmitido durante la trama 13 (y la 26 si es usada en half rate) de cada multitrama de control, y dentro de esta trama el TS8 es usado para proporcionar los datos del SACCH en cada usuario en full rate en el AFCN. Como ejemplos de los usos de este canal se

encuentran: decisiones de handover, asignación de TCH o SDCCH y procedimientos no urgentes en la red. [30]

-Canal de control asociado rápido (FACCH): El FACCH transporta mensajes urgentes y contienen esencialmente el mismo tipo de información que el SDCCH. Un FACCH es asignado cuando un SDCCH no ha sido asignado para un usuario en particular y existe un mensaje urgente (como una respuesta del handover). El FACCH gana tiempo de acceso a un slot robando tramas del canal de tráfico al que este asignado. Esto es hecho activando 2 bits especiales llamados bits de robo (stealing bits) en una ráfaga de datos sobre el TCH en el downlink. Si estos dos bits están establecidos, el TS es reconocido como datos del FACCH y no como un dato de TCH para esta trama. [30]

Todos estos canales son utilizados en la red GSM para el envío de datos de tráfico y de control, a continuación, se explicará el proceso que se hace con todos estos canales en la red.

Para entender el uso de los diversos canales de tráfico y control que se describieron, consideremos el caso de una llamada en GSM. Primero el móvil debe sintonizarse al BCH de la celda más cercana recibiendo el FCCH, SCH y BCCH el usuario deberá ajustarse al sistema y al apropiado BCH que se encuentre disponible en ese momento. Para la llamada, el usuario marcará el número al que quiera comunicarse y dará enviar, el móvil transmite una ráfaga de datos del RACCH, usando el mismo ARFCN y misma BTS, entonces la BTS responde con un AGCH en el CCCH, el cual asigna al móvil un nuevo canal para conexión del SDCCH. El móvil el cual está monitoreando el TS0 del BCH deberá recibir su ARFCN y asignación de TS ordenado por el AGCH y deberá inmediatamente sincronizarse al nuevo ARFCN y TS. Este nuevo ARFCN y TS es la asignación física del SDCCH, una vez sintonizado el SDCCH el móvil espera una trama de SACCH transmitida la cual informa al móvil el tiempo a ajustarse y transmitir el comando de potencia. La BTS es capaz de determinar el tiempo de ajuste y el nivel de señal del móvil en la inicial transmisión del RACH y envía el correcto valor de SDCCH, para el proceso del móvil, la unidad móvil es capaz de enviar un mensaje solicitando un canal de tráfico. El SDCCH envía un mensaje entre el móvil y la BTS, tomando en cuenta la autenticación y validación del usuario, mientras la PSTN conecta la parte llamada a la MSC y esta rutea la trayectoria de voz hacia la BTS servidora, después de unos segundos el móvil es llamado vía la BTS y mensaje de SDCCH se vuelve a sincronizar a un nuevo ARFCN y TS para la asignación de un TCH. Una vez en el TCH, los datos de voz son transmitidos en ambas trayectorias, y la llamada es completada exitosamente en esta forma y el SDCCH queda vacante. Cuando la llamada es originada

desde una PSTN, el proceso es similar. La BTS emite un mensaje PCH durante TS0 dentro de un apropiado BCH. El móvil se sintoniza en el mismo ARFCN detecta su page y contesta con un mensaje de RACH de reconocimiento del Page. La BTS entonces usa un AGCH en el CCCH para asignar al móvil en un canal físico para conectarlo hacia el SDCCH y SACCH mientras la BTS y la red son conectados. Una vez que el usuario establece el ajuste en tiempo y autenticación en el SDCCH, la BTS emite un nuevo canal físico asignado sobre el SDCCH y la asignación de un TCH es hecho. [30] En la figura 36 se muestra la trama que se genera los canales de control.

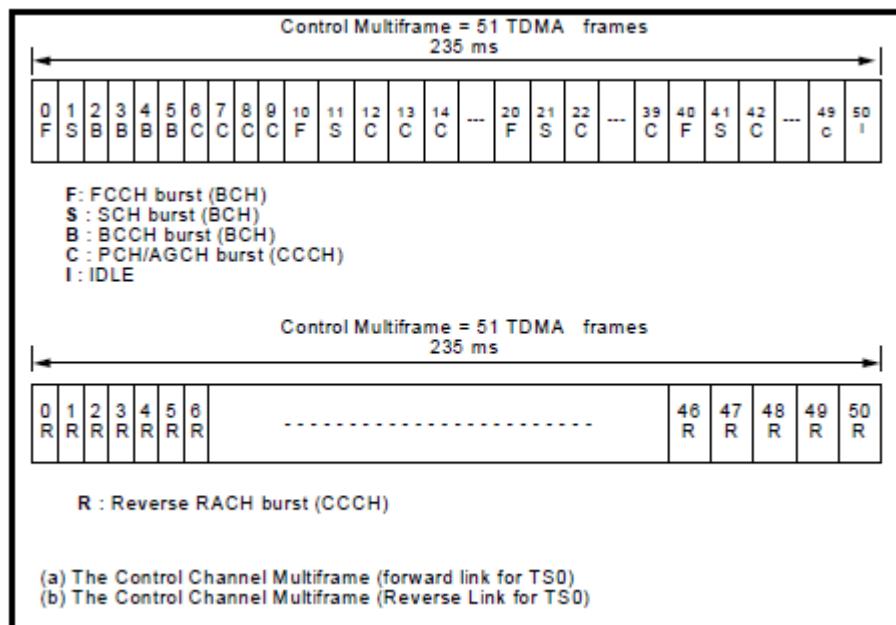


Figura 36 Control multitráma [30]

### 2.7.2 Ráfagas GSM

Cada usuario transmite una ráfaga de datos al time slot asociado. Estas ráfagas de datos pueden contener uno de cinco formatos de ráfagas específicas definidas en GSM. La velocidad de 148 bits que modula una portadora GSM es de 270.833 kbits/s (un inusual tiempo de guarda de 8.25 bits es proporcionado al final de cada ráfaga), significando un intervalo de 577 µs que corresponde una duración de 156.25 bits de duración. Se denomina BURST a esta ráfaga o secuencia de datos de extensión. El burst está compuesto de una parte útil y una de guarda. La primera contiene los datos para ser transmitidos, una secuencia de entrenamiento y una cola de bits. En la segunda, el periodo de guarda, no se transmite nada y su propósito es permitir una variación en el tiempo de llegada del burst sin que se solapen las partes útiles de los burst adyacentes. La especificación del estándar usado en esta tecnología define 5 tipos de ráfagas, que se enumeran a continuación: [30]

- **Ráfaga normal (NB).**

Esta ráfaga se usa para llevar información sobre canales de tráfico o de control. A continuación, se muestra el contenido de la ráfaga en la figura 37.

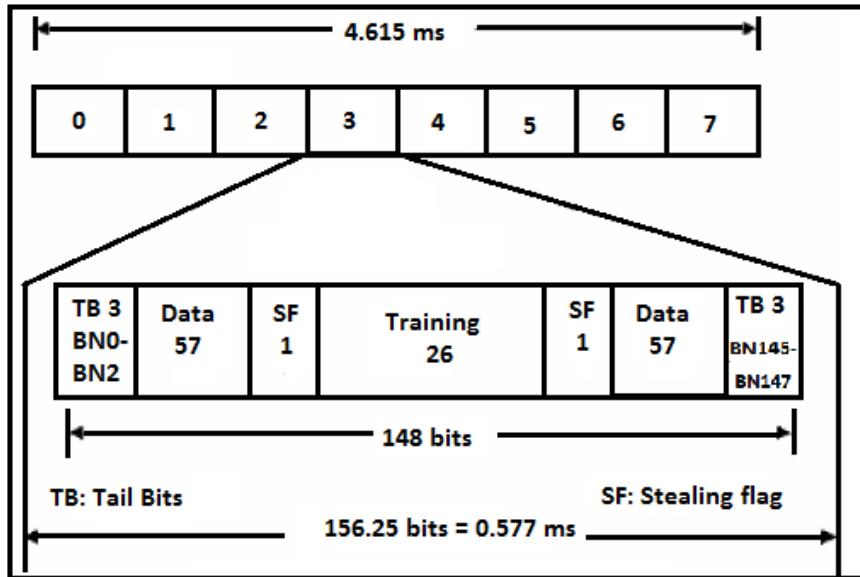


Figura 37 Estructura de la ráfaga normal. [30]

- **Ráfaga de corrección de frecuencia (FB).**

Esta ráfaga la utiliza el móvil para sincronizar su frecuencia. Además, esta ráfaga tiene la función de calcular la oscilación de las señales y la demodulación. También se encarga de facilitar al móvil la búsqueda del canal de difusión. En la figura 38 se muestra el contenido de la ráfaga:

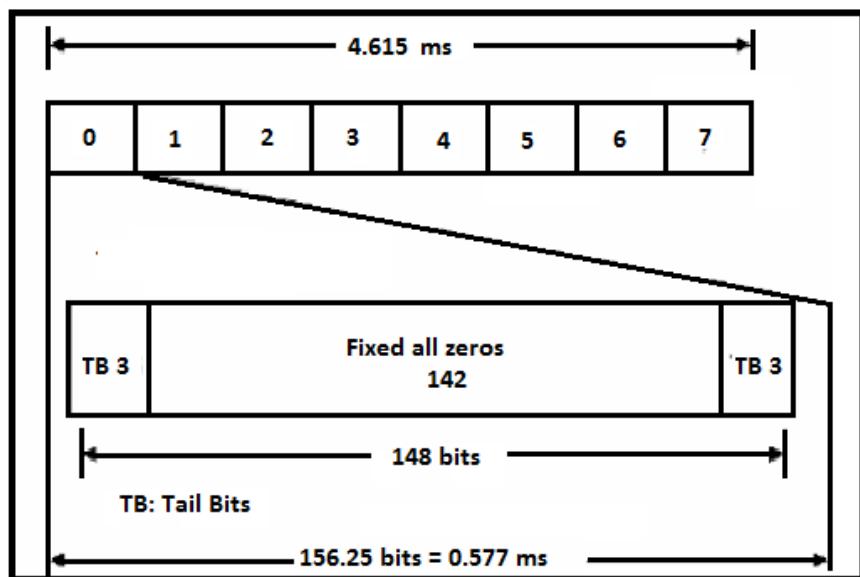


Figura 38 Estructura de la ráfaga de corrección de frecuencia. [30]

- **Ráfaga de sincronización (SB).**

Se utiliza cuando el móvil quiere hacer una sincronización temporal con la estación base. En la figura 39 se muestra el contenido de esta ráfaga.

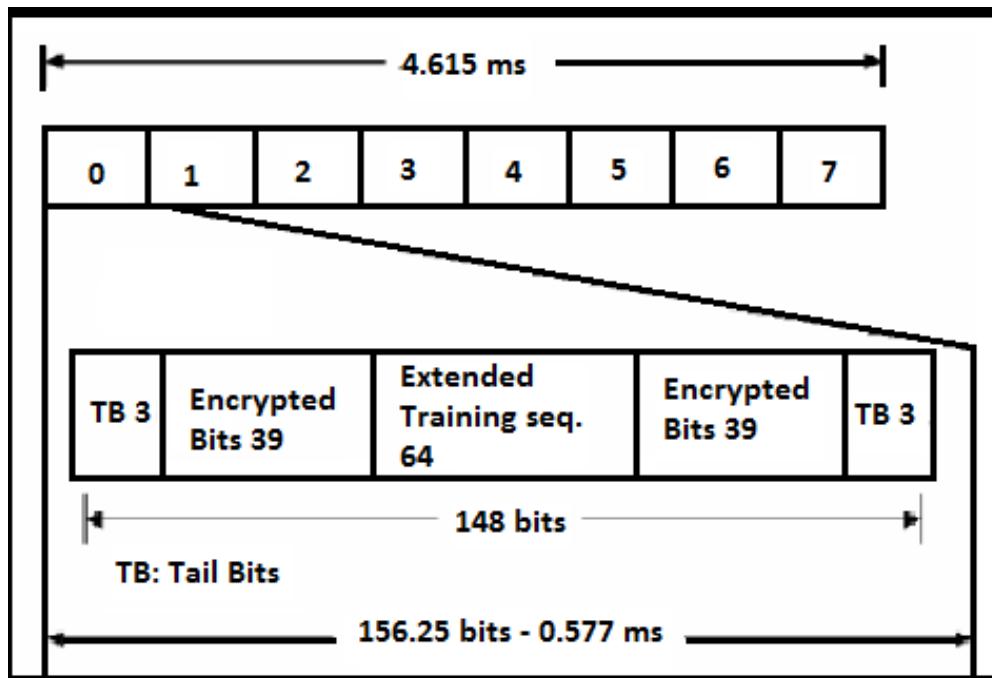


Figura 39 Estructura de la ráfaga de sincronización. [30]

- **Ráfaga vacía (DB).**

Tiene la misma estructura que la ráfaga normal, con la diferencia de que los datos se sustituyen por valores nulos o vacíos. Es utilizada para llenar la transmisión cuando no hay canales de tráfico que transmitir.

- **Ráfaga de acceso (AB).**

Es la ráfaga utilizada por el móvil para acceder al sistema. A continuación, en la figura 40 se observa los componentes de esta trama.

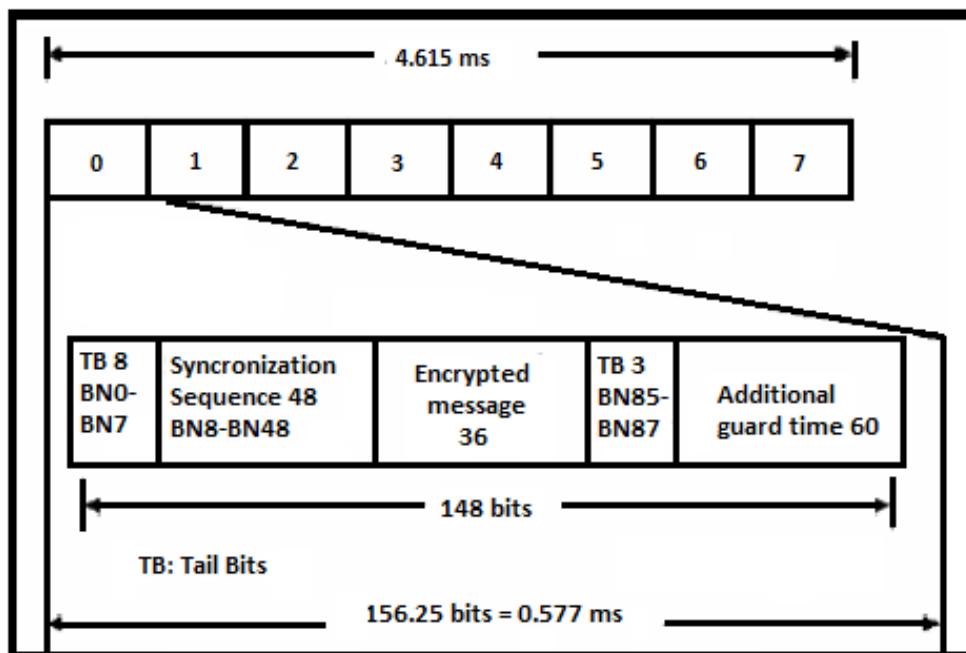


Figura 40 Estructura de la ráfaga de acceso. [30]

Como se muestra en la figura 41 time slots por trama TDMA y el periodo de trama es de 4.615 ms. Una trama contiene 8 TS X 156.25 bits = 1250 bits/trama. La velocidad de trama es 270.833 kbps/1250 bits/trama son igual a 216.66 tramas/ segundo. Cada una de las tramas de voz normales son agrupadas en estructuras más largas, denominadas multitramas, las cuales pasan a ser agrupadas en supertramas e hipertramas. Una multitrama tiene 26 tramas TDMA y una hipertrama contiene 51 multitramas ó 1326 tramas TDMA. Una hipertrama completa es enviada aproximadamente cada 3 horas, 28 minutos, 54 segundos y es importante para GSM desde la encriptación de algoritmos que dependen de una trama en particular hasta la suficiente seguridad que puede ser obtenida usando un número extenso de tramas proporcionado por la hipertrama. [30]

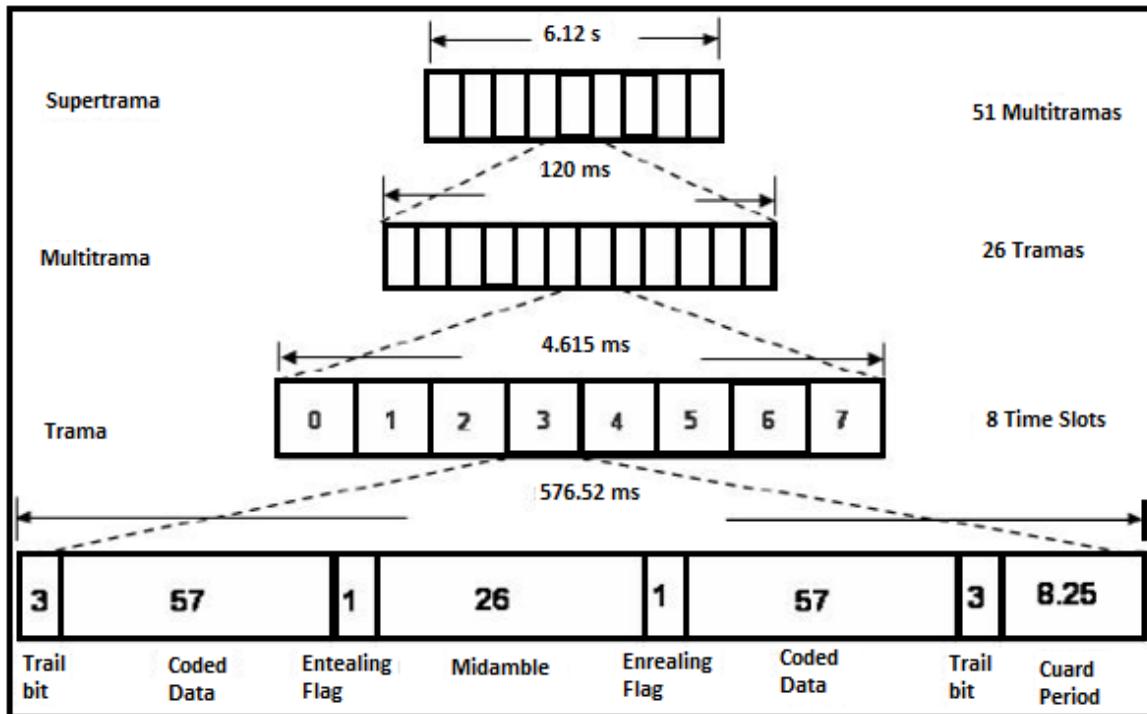


Figura 41 Tramas usadas en GSM [30]

### 2.7.3 Modulación GMSK

GMSK es el acrónimo de Gaussian Minimum Shift Keying. Es un tipo de modulación derivada de la MSK (Minimum Shift Keying). GMSK es un esquema de modulación continua en fase. Se trata de una técnica que consigue suavizar las transiciones de fase entre estados de la señal, consiguiendo por lo tanto reducir los requerimientos de ancho de banda. Con GMSK, los bits de entrada representados de forma rectangular (+1;-1) son transformados en pulsos Gaussianos (señales de forma acampanada) mediante un filtro Gaussiano, para posteriormente ser suavizados por un modulador de frecuencia. [31]

En GMSK, los lóbulos laterales del espectro de una señal MSK se reducen pasando los datos NRZ modulantes a través de un filtro Gaussiano de premodulación como se muestra en la figura 42. El filtro gaussiano aplana la trayectoria de fase de la señal MSK y por lo tanto, estabiliza las variaciones de la frecuencia instantánea a través del tiempo. Esto tiene el efecto de reducir considerablemente los niveles de los lóbulos laterales en el espectro transmitido. El filtrado convierte la señal (donde cada símbolo en banda base ocupa un periodo de tiempo ( $T$ ) en una respuesta donde cada símbolo ocupa varios períodos. Sin embargo, dado que esta conformación de pulsos no cambia el modelo de la trayectoria de la fase, GMSK se puede detectar coherentemente como una señal MSK, o no coherentemente como una señal

simple FSK. En la práctica, GMSK es muy atractiva por su excelente eficiencia de potencia y espectral. El filtro de premodulación, por tanto, introduce interferencia intersimbólica en la señal transmitida, y se puede mostrar que la degradación no es grave si el parámetro BT del filtro es mayor de 0.5. Debido que en GSM tenemos que el BT es 0.3, vamos a tener algunos problemas de interferencia intersimbólica y es por ello por lo que en GSM la señal no es totalmente de envolvente constante. [30]

La manera más simple de generar una señal GMSK es pasar una cadena de mensajes NRZ a través de un filtro gaussiano paso baja, seguido de un modulador de FM. Esta técnica de modulación se muestra en la Figura 42 y se usa actualmente en una gran cantidad de implementaciones analógicas y digitales, así como para GSM. [28]

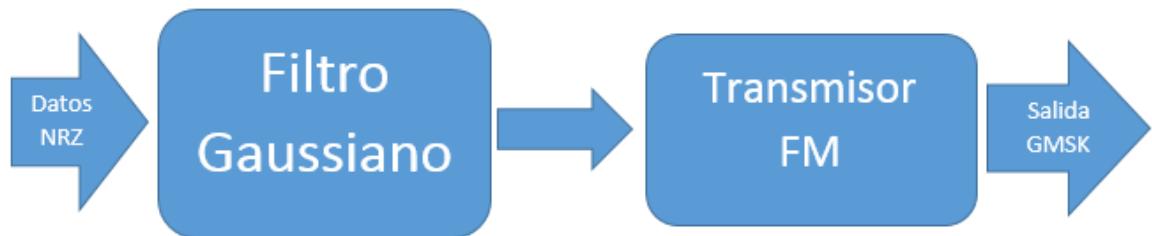


Figura 42 Diagrama de bloques del transmisor GMSK

En la figura 43 se muestra un ejemplo de la señal modulada con la técnica de GMSK.

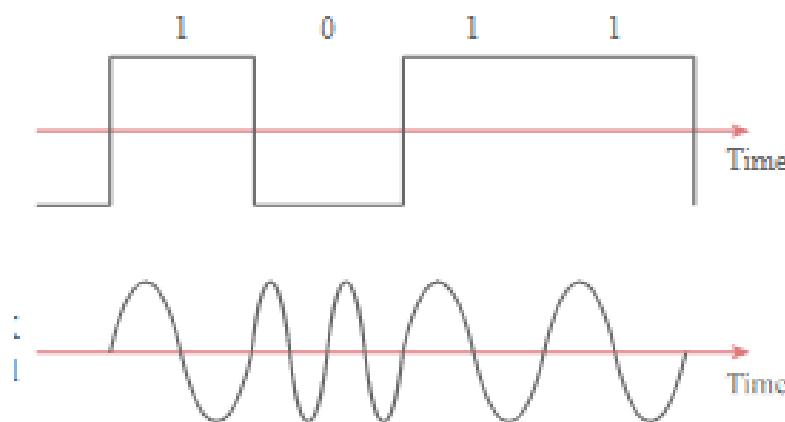


Figura 43 Señal de modulación GMSK [32]

## 2.8 Handover

Es el proceso utilizado en comunicaciones móviles para transferir un servicio de una BTS a otra cuando la calidad del enlace es insuficiente. El handover garantiza la calidad del servicio cuando una MS se mueve en una zona de cobertura (figura 44).

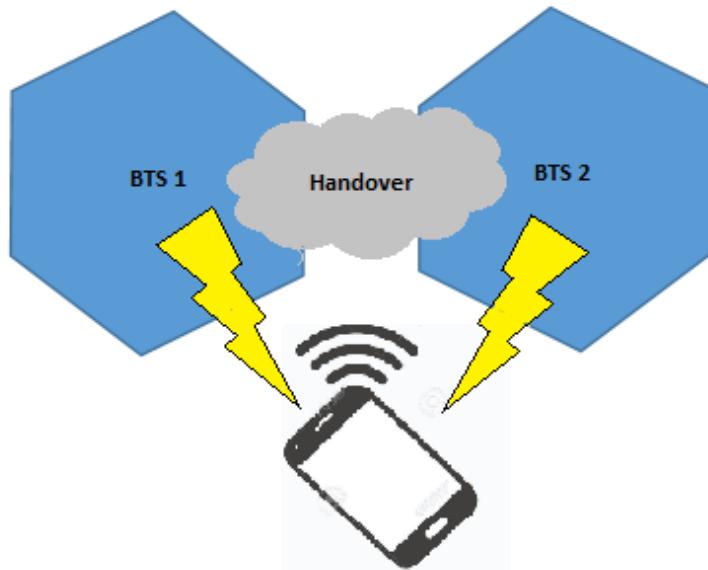


Figura 44 Handover

El handover se realiza cuando:

- El nivel de calidad es bajo y el nivel del error de la tasa de bits(BER) es alto.
- El nivel de potencia bajo.
- La distancia entre la MS y la BTS es alta.
- Cuando existe una BTS que brindara mejor calidad.

Ahora veremos la clasificación del handover respecto al punto de vista de la MS:

- **Hard-Handover:** Antes de pasar a la nueva estación base, la MS está conectada a la antigua BTS. Pero durante el traspaso la MS se desconecta por un tiempo del orden de los milisegundos antes de conectarse a la nueva BTS. Este método es el utilizado en el estándar GSM aunque no es el más fiable pero si el más sencillo de implementar.
- **Soft-Handover:** Cuando se realiza este tipo de handover la BTS estará conectada a la BTS de origen y de destino simultáneamente. Durante este proceso la MS transmite por los dos canales, es decir no

hay interrupción del enlace. Con esto se asegura la conexión con la BTS de destino antes de cortar la conexión con la BTS de origen. Este es el sistema más fiable al hacer un handover, es difícil de implementar, se utiliza en el estándar CDMA-ONE.

Desde el punto de vista de la red el handover se clasifica como:

- **Intra-cell Handover:** Cuando la calidad de la conexión no es la deseada, se hace un cambio de canal en la BTS. Se puede realizar un cambio de slot (TDMA), un cambio de frecuencia, o un cambio de frecuencia y tiempo simultaneo.
- **Inter-Cell Handover:** Sera utilizado cuando una determinada característica de la conexión supere la referencia preestablecida. Para evaluar la calidad de la conexión, la MS transmite los valores del nivel de señal recibido medida por el teléfono (RxLev), y la tasa de error de bits (RxQual) a la BTS. Además, la BTS enviará la información de la distancia existente entre la BTS y la MS.

Vistos los tipos de handover que se pueden encontrar tanto desde el punto de vista del MS como de la red, se definen a continuación las distintas clases de handover: [28]

- **Power Budget Handover/Better Cell Handover:** El principal objeto de este tipo de handover es minimizar la potencia empleada necesaria para cursar la llamada, convirtiéndose en vital a la hora de evitar interferencias radio inter-cell a lo largo de la red, y también a la hora de prolongar la durabilidad de las baterías de un móvil. Sera el criterio “normal” a seguir a la hora de realizar el HO, y estará basado en la potencia en el enlace descendente o downlink (RXLEV\_DL). [28]
- **Forced Handover/Directed Retry Management:** Consiste en la transición del SDCCH en una celda a un TCH en otra celda vecina durante el proceso de setup de la llamada, debido a la indisponibilidad de canales IDLE en la celda sobre la que se encuentra acampado el MS. Con ello se evita la necesidad de tomar medidas para el control de la distribución del tráfico sobre las BTSs, así como la posibilidad de que una llamada en curso sea rechazada por no encontrar canales TCH disponibles. [28]
- **Resource Management Criteria Handover:** El “Traffic-HO” incrementa la eficiencia en la red mediante la redistribución del tráfico entre las celdas para evitar el desperdicio de los recursos. No hay que confundir este criterio de Handover con el anterior, ya que mientras el Forced Handover se aplica durante el establecimiento de la llamada y puede que afecte a un MS muy alejado del borde de la celda, este se aplica a llamadas en curso teniendo en cuenta su posición en la cover-

area (prioridad para las más cercanas al borde de esta) para liberar recursos de una celda saturada en beneficio de la conexión de nuevos usuarios que se encuentren más alejados del borde teórico de la celda (Timing Advence). En la figura 45 se muestra el funcionamiento del handover mencionado. [28]

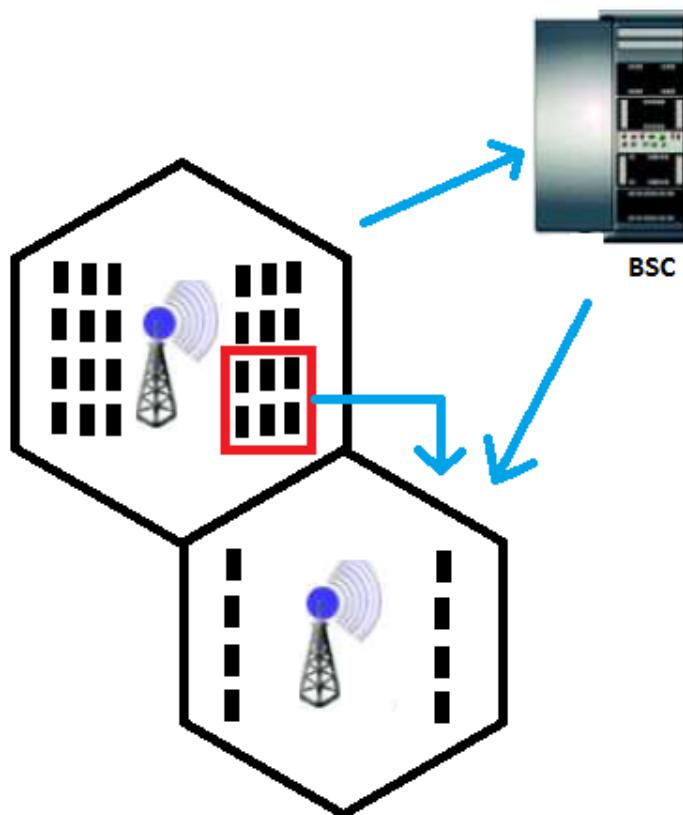


Figura 45 Resource Management Criteria Handover

- **Concentric Cell Structure Management:** Esta clasificación hace referencia a la situación en la que se dan dos celdas lógicas sobre una misma celda estándar GSM. El área completa estará caracterizada por una potencia de emisión mayor y un área de cobertura que puede llegar a extenderse, por limitación física y tecnológica, hasta los 35 kilómetros como se muestra en la figura 46. Cuando en la integración se definen como concéntricas dos estaciones se pretenden optimizar en ese caso concreto los procesos de interacción entre ambas. Debido a esto el operador, a la hora de realizar la configuración, deberá definir explícitamente cada TRX como perteneciente al área interior o exterior. [28]

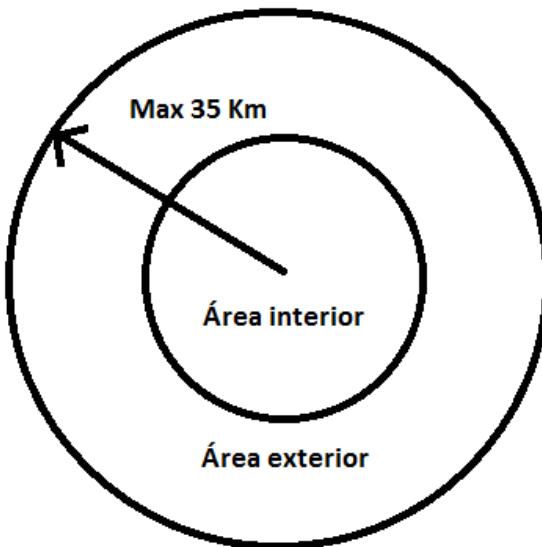


Figura 46 Concentric Cell Structure Management

- **Extended Cell Handover:** En buenas condiciones de propagación y aumentando el nivel de potencia en BTS y MS, el radio de cobertura en GSM se encuentra limitado a 35 Kms como consecuencia del máximo desfase permitido entre transmisión y recepción por la duración definida de un time slot en GSM. Con esta configuración de celda el operador tiene la posibilidad de ampliar hasta 100 Km el radio de cobertura asignando a determinado TCH doble ranura de tiempo como se muestra en la figura 47, esto es, duplicando la longitud de los time slots que lo conforman en las sucesivas tramas. [28]

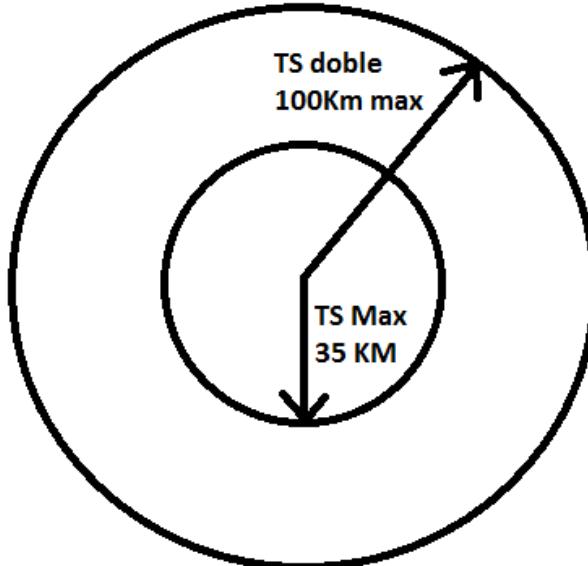


Figura 47 Extended Cell Handover

## CAPÍTULO 3

# DISPOSITIVOS SDR.

Hoy en día la comunicación por radio frecuencia es muy solicitada ya que se utiliza en la telefonía celular, wifi, iot, etc. Esta demanda de servicios genera una gran cantidad de tráfico por lo que las telecomunicaciones tienen que ir evolucionando para dar una buena calidad de servicio a todos los usuarios. Debido a esto los estándares de comunicación van evolucionando ocasionando incompatibilidad con el hardware existente para el estándar anterior, lo que significa que las empresas tienen un mayor gasto al dar una mejor calidad a sus usuarios. Debido a esto y otros aspectos, se introdujo el concepto de radio definido por software (SDR) la ventaja es que ahora la evolución de un estándar de comunicación no te afecta al hardware de transmisión de radio, esto debido a que este depende solo de la actualización del software, evitando así gastos innecesarios para las empresas. Debido a estas características SDR tomo gran importancia en los sistemas de comunicación.

### 3.1 CONCEPTO DE SDR.

El termino Radio Definido por Sotware (SDR) se refiere a una radio reconfigurable. Es decir, una radio que a partir de un programa de software puede variar sus parámetros sin tener que recurrir al hardware. Anteriormente solo se podía hacer por hardware lo que provocaba limitaciones al momento de una actualización de ese dispositivo de radiofrecuencia. Por ejemplo, la radio FM y AM, estos radios para poder capturar los datos de voz, emitidos por la antena transmisora, tenían que modificar un parámetro de hardware para sintonizar la frecuencia, ya fuera variar la capacitancia o resistencia. Con la aparición del SDR ese mismo proceso se hace desde el software sintonizando muy fácil, además no solo poder sintonizar un rango de frecuencias pequeño si no que ahora se puede capturar un rango grande de frecuencias y sintonizar varios estándares con modulaciones diferentes, es decir se pueden ver señales de estándares como AM, FM y hasta televisión digital que se encuentra en otra frecuencia y tiene otro tipo de modulación.

## Software Defined Radio

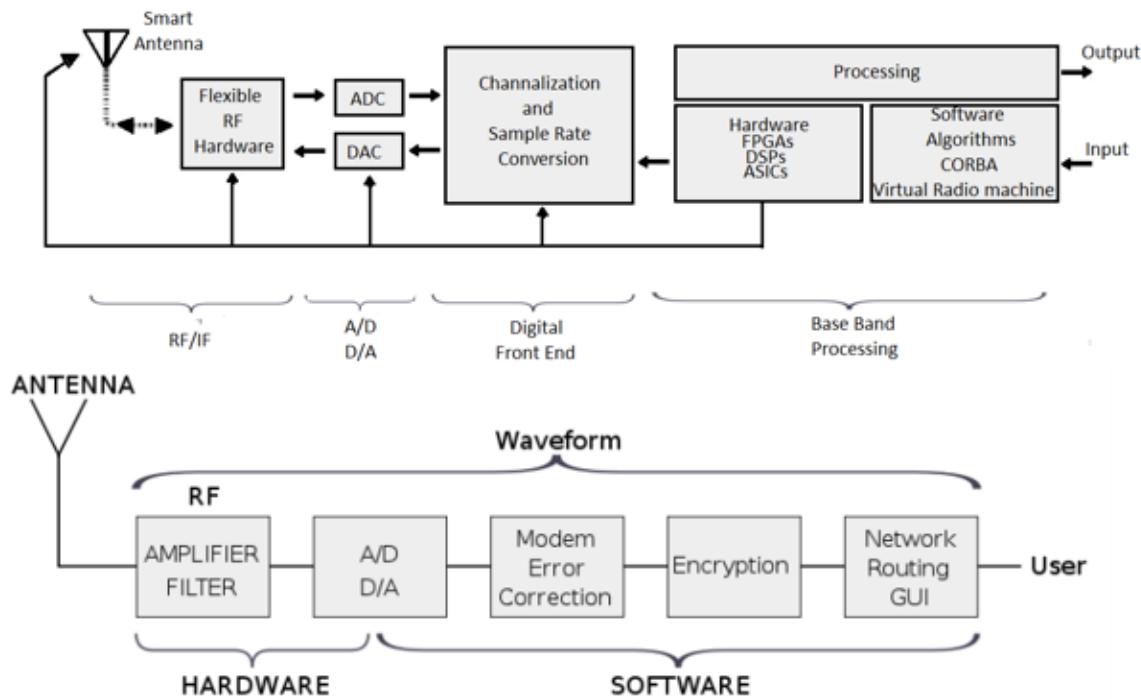


Figura 48 Concepto de radio definida por software. [33]

Observando el diagrama de la figura 48, se explica de manera breve cada una de las partes:

- **Antena:** Tiene como objetivo recibir o enviar las señales de radiofrecuencia, es decir, en esta terminal la señal es analógica tanto la señal transmitida como la recibida.
- **RF:** El módulo RF se encarga de recibir o enviar las señales de radio frecuencia. En el caso de la recepción se sintoniza la frecuencia en la que se recibirá la señal analógica que llega de la antena, esta es muy tenue por lo que se amplifica para poder pasar la señal al convertidor analógico digital. En el caso de la transmisión, se amplifica la señal analógica que llega del convertidor digital analógico, y se envía a la antena para así poder ser transmitida.
- **ADC/DAC:** El convertidor analógico digital es un elemento importante ya que este nos limita dependiendo de su frecuencia de muestreo. Este tiene la función de convertir una señal ya sea de analógica a una digital o viceversa. El ADC convierte la señal que viene del RF, la cual viene modulada y es análoga, en una señal digital para poder ser procesada por la siguiente etapa. El DAC tiene la función contraria, ya que la información no puede transmitirse a la antena de manera digital debido a que los pulsos cuadrados saturarían el ancho de banda del

espectro de frecuencia permitido. El DAC ayuda a convertir la señal modulada llegada en bits a una señal analógica que ahora si puede ser enviada.

- **Banda Base/Procesing:** Este módulo tiene como base un dispositivo como las FPGAs, DSPs, entre otros. Estos dispositivos se encargan de la banda base, con el objetivo de hacer la modulación en algunos de los casos, en otros casos solo son los responsables de recibir los datos que vienen de otra interfaz por medio de un puerto, ya sea una PC o una Raspberry.

### 3.2 APORTACIONES DEL SDR.

Los dispositivos SDR tienen una importante utilidad en algunos de los estándares de comunicación actuales, pero además de esto tiene otras ventajas las cuales se mencionarán a continuación:

- Gracias a que el SDR tiene una gran flexibilidad en cuanto a la configuración de frecuencias y modulación, genera un amplio rango de aplicaciones, ya que con estos dispositivos se puede desarrollar casi cualquier estándar de comunicaciones.
- Los dispositivos SDR en el mercado son baratos, en cuanto a las utilidades que le puedes dar, para un investigador en la rama de las telecomunicaciones le pude dar mucho uso en el área de radiofrecuencia. Dándole la posibilidad de crear nuevos estándares de comunicaciones.
- Debido a que es un dispositivo muy flexible genera la opción de actualizarlo, cuando se evoluciona un estándar de comunicaciones a otro estándar, no es necesario cambiar el equipo, solo configurarlo por lo que genera una gran ventaja ya que no se contamina al medio ambiente fabricando nuevos dispositivos.
- Debido a que estos dispositivos son baratos, en universidades se puede acceder a uno para dar prácticas y así tener un conocimiento más amplio en los estándares de comunicación.

### 3.3 EQUIPOS SDR EN EL MERCADO.

Con el tiempo varias compañías se han dedicado a desarrollar equipos SDR, entre los equipos que más destacan se encuentran los siguientes:

- **HackRF One.**

Es un dispositivo creado por la empresa Great Scott Gadgets, puede transmitir o recibir señales de radio desde 1 MHz hasta los 6 GHz. Fue diseñado para facilitar el desarrollo y prueba de tecnologías de comunicación de radio. A continuación, se presentan algunas características:

- Tiene un rango de frecuencia desde 1MHz a los 6GHz.
- El transceiver utilizado tiene la capacidad de operación half-duplex.
- Su capacidad de muestreo es de 20 millones de muestras por segundo, alcanzando las 21.5 millones de muestras por segundo cuando se cuenta con un buen controlador USB 2.0 HS.
- Muestreo de señales de 8 bits en cuadratura, siendo 8 para la componente I y 8 para la componente Q.
- Es compatible con programas como SDR# y GNU radio.
- Permite configurar por software, 3 amplificadores en la transmisión y 2 en la recepción.
- Se pueden configurar vía software los filtros de señal en banda base con un ancho de banda máximo de 28MHz.
- Permite controlar la potencia de la antena vía software hasta los 50mA a 3.3V.
- Conector de antena SMA hembra.
- Pines internos para poder expandir la placa usando placas adicionales.
- Usa una interfaz USB 2.0 High Speed.
- El dispositivo es alimentado vía USB por lo que no se requiere fuente externa.

En la figura 49 se puede ver una imagen del dispositivo.



Figura 49 HackRF One [34]

- **Ettus B200.**

Dispositivo creado por la empresa National Instruments, que se muestra en la figura 50. Diseñado para la experimentación a bajo costo. A continuación, se proporcionan las características principales de esta tarjeta:

- Contiene una FPGA Spartan6 XC6SLX75
- Un transceptor AD9364.
- Tiene un rango de frecuencia de los 70 MHz hasta los 6 GHz.

- Tiene un ancho de banda de 56MHz.
- Contiene una salida TX y una entrada RX, para transición y recepción.
- Para la transmisión de datos y alimentación contiene un puerto 3.0.
- Potencia de salida mayor a 10dBm



Figura 50 Ettus B200 [35]

- **Ettus B210.**

Dispositivo de National Instruments, con las mismas características que el Ettus B200. Pero con la diferencia de contar con un sistema MIMO, es decir tiene dos conectores de transmisión y recepción. En la figura 51 se muestra el dispositivo.



Figura 51 Ettus B210 [35]

- **BladeRF x40.**

Dispositivo creado por la empresa sparkfun, que se observa en la figura 52, la cual ofrece un dispositivo SDR con salida MIMO, las características principales de explican a continuación:

- Full-duplex, 40 millones de muestras por segundo 12 bits de muestreo en cuadratura.
- Controlador de periféricos Cypress FX3 SuperSpeed con ARM926EJ-S integrado Totalmente alimentado por bus a través de USB 3.0. Tiene la opción de alimentación externa a través de conector de 5 VDC.
- Rango de frecuencia desde los 300MHz hasta los 3.8 GHz.
- Acceso a los pines del convertidor ADC y DAC.
- Operación MIMO con dos salidas TX y dos entradas RX.
- Contiene una FPGA Altera Cyclone IV.



Figura 52 BladeRF x40 [36]

- **LimeSDR.**

Dispositivo creado por la empresa Lime microsystems, que se muestra en la figura 53, la cual tiene las siguientes características:

- Utiliza el tranceiver Lime Microsystems LMS7002M MIMO FPRF.
- Utiliza la FPGA Altera Cyclone IV EP4CE40F23.
- Contiene una memoria de 256 MBytes DDR2 SDRAM
- Utiliza el Puerto Cypress USB 3.0 CYUSB3014-BZXC
- Utiliza un oscilador Rakon RPT7050A @30.72MHz
- Su rango de frecuencias va desde 100 kHz hasta los 3.8 GHz
- Tiene un ancho de banda de 61.44 MHz
- 10 conectores UFL (6 RX, 4 TX)
- La potencia de salida es arriba de 10 dBm

- Contiene dos salidas TX y dos entradas RX (MIMO).
- Conector micro USB para conexión de corriente. Solo en ciertos modelos.



Figura 53 LimeSDR [37]

- **LimeSDR mini.**

Dispositivo creado por microsystems. Es el dispositivo utilizado en este trabajo por lo que se explicaran en detalle las características más relevantes.

- **Transceptor RF:** Lime Microsystems LMS7002M
- **FPGA :** Intel Altera MAX 10 (10M16SAU169C8G)  
Empaquetado de 169 pines  
549 KB de memoria M9K  
2,368 KB de memoria flash del usuario  
4 x PLL  
45 multiplicadores de 18x18 bits  
130 x entrada / salida de propósito general (GPIO)  
Tensión de alimentación única  
Característica de flash  
Configuración de FPGA a través de JTAG

- **Memoria EEPROM:** 2 x 128 KB para el firmware y los datos del MCU transceiver RF
- **Memoria flash:** 1 x 4 MB de memoria flash para datos
- **Entradas / salidas generales del usuario:**
  - 2 x doble color (rojo + verde) LED
  - 8 x cabezal de pin FPGA GPIO (3.3 V)
- **Conectividad:**
  - USB 3.0 Tipo A
  - 2 x conectores RF coaxiales (SMA) (cada uno puede cambiarse entre bandas de alta y baja frecuencia)
  - Conector UFL para fuente de reloj externa
  - Cabeceras FPGA GPIO
  - Conector FPGA JTAG
- **Sistema de reloj:**
  - VCTCXO a bordo de 30.72 MHz
  - Posibilidad de sintonizar VCTCXO con DAC incorporado
  - Entrada de reloj externa a través del conector UFL
- **Dimensiones del tablero:** 69 mm x 31,4 mm.
- **Peso del tablero:** 20 gramos.

En la figura 54 se muestra el dispositivo limeSDR mini.



Figura 54 LimeSDRmini [38]

A continuación, en la figura 55 se mostrará la comparación entre los dispositivos que acabamos de describir.

	<b>HackRF One</b>	<b>Ettus B200</b>	<b>Ettus B210</b>	<b>BladeRF x40</b>	<b>RTL-SDR</b>	<b>LimeSDR</b>	<b>LimeSDR Mini</b>
<b>Rango de frecuencia</b>	1 MHz - 6 GHz	70 MHz - 6 GHz	70 MHz - 6 GHz	300 MHz - 3.8 GHz	22 MHz - 2.2 GHz	100 kHz - 3.8 GHz	10 MHz - 3.5 GHz
<b>Ancho de banda de RF</b>	20 MHz	61.44 MHz	61.44 MHz	40 MHz	3.2 MHz	61.44 MHz	30.72 MHz
<b>Profundidad de la muestra</b>	8 bits	12 bits	12 bits	12 bits	8 bits	12 bits	12 bits
<b>Frecuencia de muestreo</b>	20 MSPS	61.44 MSPS	61.44 MSPS	40 MSPS	3.2 MSPS	61.44 MSPS	30.72 pps
<b>Canales de TX</b>	1	1	2	1	0	2	1
<b>Canales RX</b>	1	1	2	1	1	2	1
<b>Dúplex</b>	Mitad	Completo	Completo	Completo	N / A	Completo	Completo
<b>Interfaz</b>	USB 2.0	USB 3.0	USB 3.0	USB 3.0	USB 2.0	USB 3.0	USB 3.0
<b>Puertas lógicas programables</b>	64 macrocelda CPLD	75k	100k	40k (115k disponible)	N / A	40k	16K
<b>Chipset</b>	MAX5864, MAX2837, RFFC5072	AD9364	AD9361	LMS6002M	RTL2832U	LMS7002M	LMS7002M
<b>Fuente abierta</b>	Completo	Esquema, Firmware	Esquema, Firmware	Esquema, Firmware	No	Completo	Completo
<b>Precisión del oscilador</b>	+/- 20 ppm	+/- 2 ppm	+/- 2 ppm	+/- 1 ppm	?	+/- 1 ppm inicial, +/ 4 ppm estable	+/- 1 ppm inicial, +/- 4 ppm estable
<b>Potencia de transmisión</b>	-10 dBm + (15 dBm @ 2.4 GHz)	10 dBm +	10 dBm +	6 dBm	N / A	max 10 dBm (dependiendo de la frecuencia)	max 10 dBm (dependiendo de la frecuencia)
<b>Precio</b>	\$ 299	\$ 686	\$ 1,119	\$ 420 (\$ 650)	~ \$ 10	\$ 299	\$ 159

Figura 55 Comparación entre los dispositivos SDR económicos del mercado [38]

### 3.4 LimeSDR en su versión mini.

Entre los dispositivos SDR en el mercado con canal TX y RX, limeSDR en su versión mini es el más económico, generando la posibilidad de adquirir uno para experimentar, ya que este dispositivo está muy completo y soporta casi cualquier estándar de comunicación. En nuestro caso será la implementación de una estación base 2G GSM. A continuación, se describirá el dispositivo y sus partes de manera detallada para obtener las características de uso de este dispositivo. En la figura 56 se muestra el diagrama de bloques del limeSDR en su versión mini.

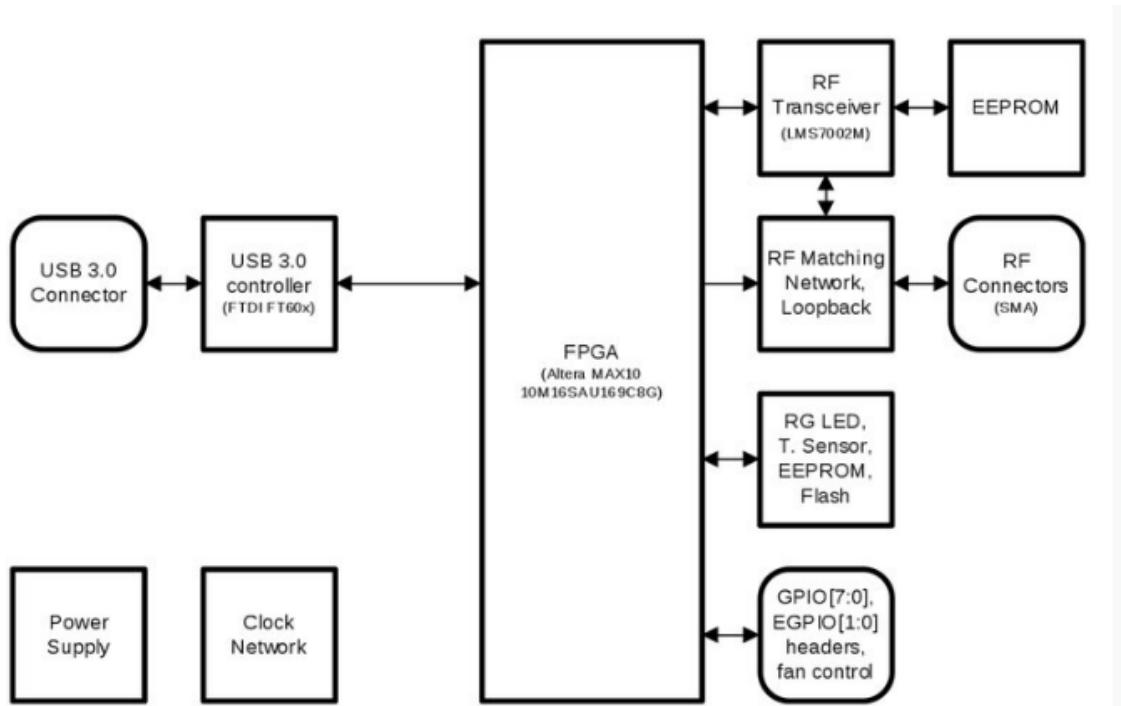


Figura 56 Diagrama de bloques del LimeSDR mini [38]

### 3.4.1 Transceptor RF: Lime mycrosystems LMS7002M

El dispositivo utiliza un diseño de transceptor de última generación en tecnología CMOS para reducir significativamente el costo total. Integra una arquitectura de transceptor dual para admitir  $2 \times 2$  MIMO junto con funciones de procesamiento de señal digital en el chip. El DSP se combina con el filtrado analógico en el chip para mejorar el rendimiento y eliminar, o reducir sustancialmente, la necesidad de filtros externos. [39] En la figura 57 se observa los componentes del transceptor LM7002.

El LimeSDR en su versión mini solo te da acceso a un puerto TX y RX, esto debido a que el espacio para el circuito es muy reducido. A continuación, se explicará cada una de las partes del transceiver:

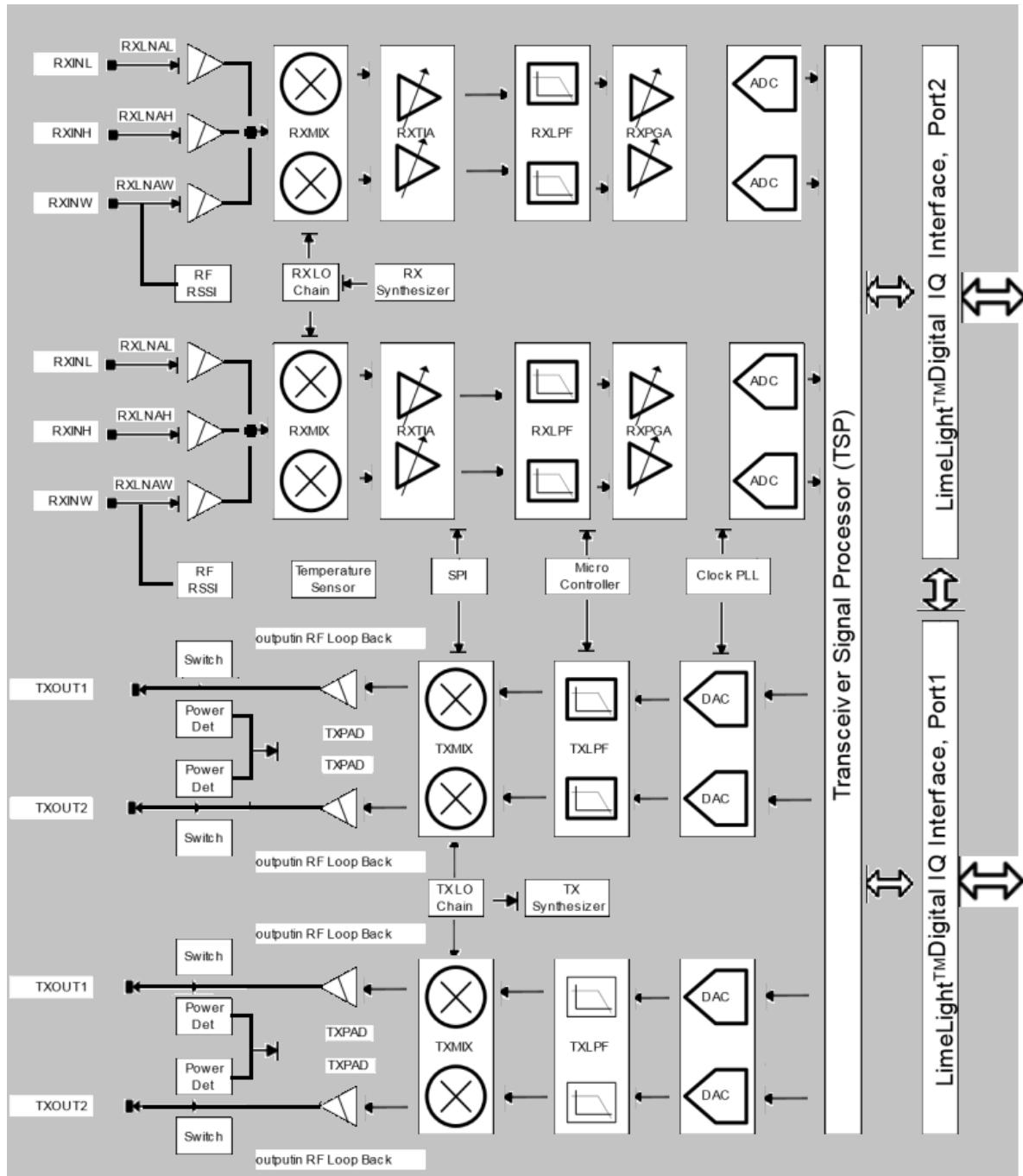


Figura 57 Diagrama de bloques del LM7002M [40]

### Para RX

- **Amplificadores:**

El receptor LMS7002M tiene tres elementos de control de ganancia, RXLNA, RXTIA y RXPGA. Si es necesario, RXTSP puede implementar un control de ganancia adicional en el dominio digital. El control de ganancia RXLNA consta de 30 dB con pasos de 1 dB en ajustes de

ganancia alta y pasos de 3 dB en ajustes de ganancia baja para AGC cuando hay grandes bloqueadores de canales adyacentes y es aceptable una reducción en la cifra de ruido del sistema (NF). RXTIA ofrece 12 dB de rango de control. RXTIA está diseñado para los pasos de AGC necesarios para reducir la ganancia del sistema antes de los filtros de canal cuando están presentes grandes bloqueadores en la banda. Esta ganancia puede estar bajo el control de la banda base o fijada en la calibración. RXPGA proporciona control de ganancia para el AGC si se requiere un nivel de señal RX constante en la entrada ADC. Tiene un control de rango de ganancia de 32 dB en pasos de 1 dB. [40] En la figura 58 se muestra el diagrama de bloques de la etapa de amplificación del receptor.

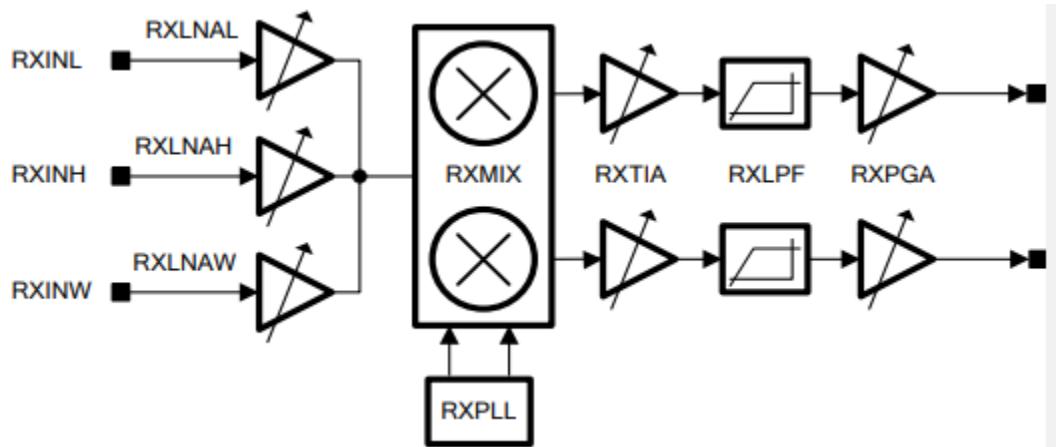


Figura 58 Etapa de amplificación en el receptor. [40]

- **Filtros:** El filtrado inicial se realiza mediante el amplificador de impedancia (RXTIA), que actúa como un filtro pasa bajas de un solo polo. La salida RXTIA se enruta a una de las dos etapas de filtro. La banda de paso del filtro de banda baja es sintonizable desde 0.7 MHz hasta 18 MHz. La banda de paso del filtro de banda alta es sintonizable desde 18 MHz hasta 80 MHz. Ambas etapas de banda baja y banda alta son filtros pasa baja de segundo orden. Combinadas con la RXTIA, estas etapas producen una respuesta del filtro pasa baja de tercer orden. Solo una ruta (RXLPFL o RXLPH) puede estar activa al mismo tiempo. [40] En la figura 59 se ve el diagrama de bloques de la etapa de filtrado del receptor.

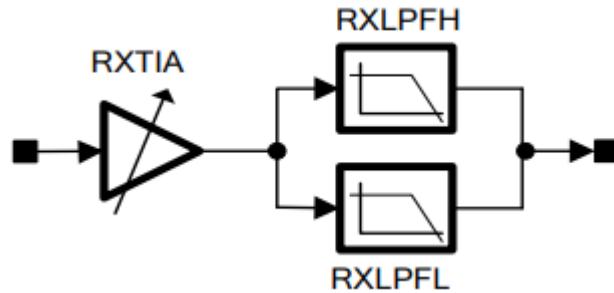


Figura 59 Etapa de filtrado en el receptor. [40]

En la figura 60 se muestra las respuestas del filtro en algunas de sus configuraciones.

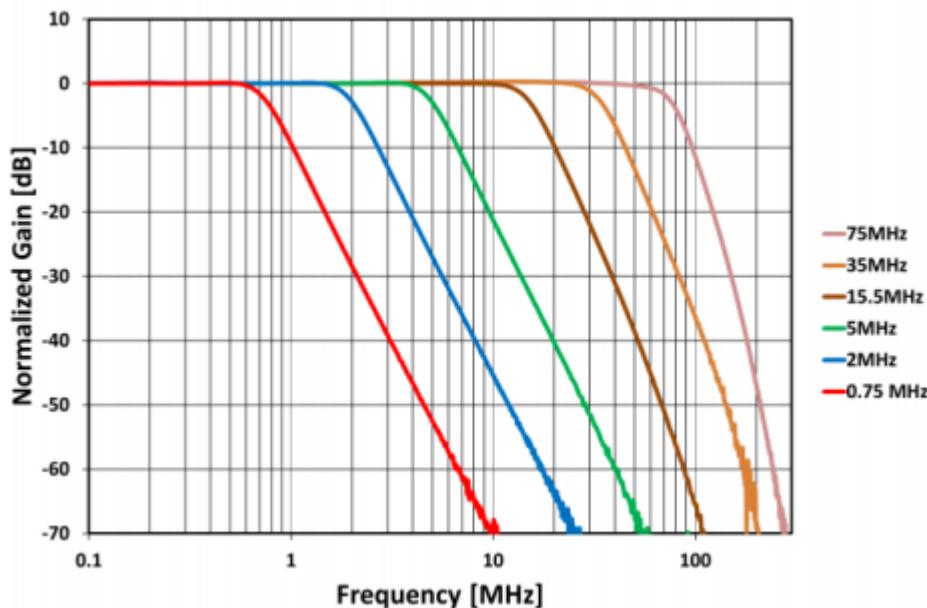


Figura 60 Respuesta de amplitud analógica RX LPF [40]

- **ADC:** El Transceiver cuenta con un convertidor analógico digital de 12 bits por cuadratura. Además, muestrea a una velocidad de 30.72 millones de muestras por segundo, esto en la versión mini. En la figura 61 se muestra el diagrama de bloques del convertidor en la parte del receptor.

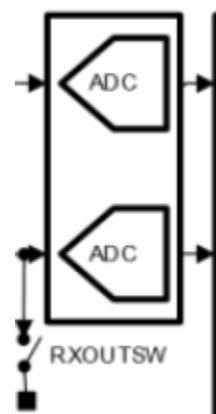


Figura 61 Convertidor Analógico Digital.

### Para TX

- **Convertidor Digital Analógico:** El transceiver, cuenta con un convertidor Digital Analógico de 12 bits, con la capacidad de convertir señales digitales en señales analógicas de una frecuencia muy alta. Es la primera etapa en el transceiver para el envío de datos. En la figura 62 se muestra el diagrama de bloques del convertidor digital analógico.

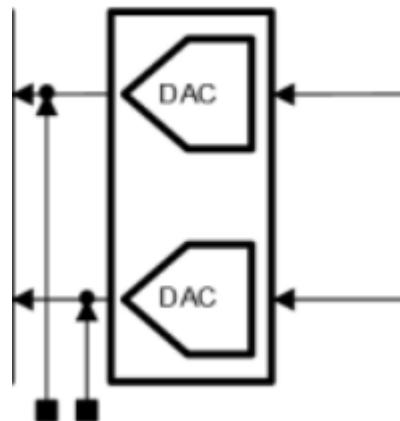


Figura 62 Convertidor DAC en el LM7002M

- **Filtros:** La banda de paso del filtro de banda baja (TXLPFL) se puede sintonizar de 2.5 MHz a 20 MHz y consta de dos etapas de filtro: el filtro de escalera de paso bajo de 4º orden (TXLPFLAD) y el filtro de polo real de paso bajo de primer orden (TXLPFS5). La etapa de polo real filtra el ruido en la frecuencia dúplex para cumplir con las especificaciones de ruido de largo alcance en algunos sistemas FDD. La etapa de polo real es pasable si no se requiere. La banda de paso

del filtro de banda alta (TXLPFH) es sintonizable desde 20 MHz hasta 80 MHz y se compone de una única etapa de paso bajo de segundo orden. Solo una ruta (TXLPFL o TXLPH) puede estar activa al mismo tiempo

- **Amplificadores:**

El transmisor LMS7002M tiene dos etapas de ganancia programables, donde el TSP proporciona control de ganancia digital y el TXPAD proporciona ganancia programable de la señal de RF. En la figura 63 se muestra el diagrama de bloques de la etapa de amplificación de parte del transmisor.

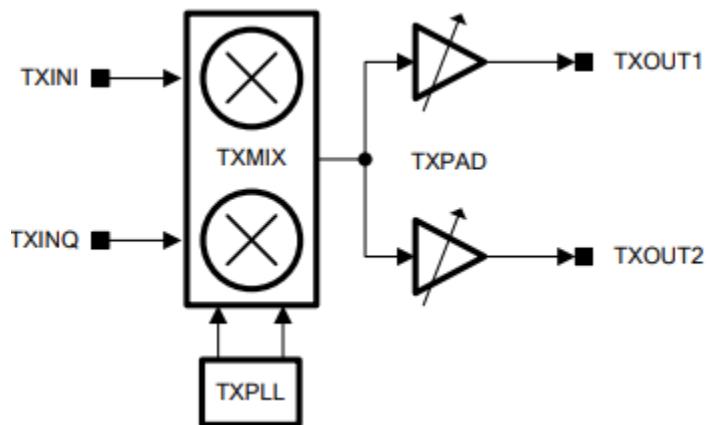


Figura 63 Etapa de amplificación en la transmisión. [40]

Como se puede ver el transceiver utiliza bloques de características diferentes para la transmisión y recepción de datos. Pero al final es el mismo proceso para los dos casos, solo que en sentido contrario. En el LM7002M existen dos bloques de hardware con las mismas características que se comparten tanto para la transmisión como para la recepción, estos se describen a continuación.

- **Sintetizador:** El LMS7002M tiene dos sintetizadores de ruido de fase baja para permitir el funcionamiento dúplex completo y ambos son capaces de emitir frecuencias de hasta 3.8 GHz. Cada sintetizador utiliza una arquitectura PLL fraccional-N, como se muestra en la Figura 64. La misma frecuencia de referencia se puede usar para ambos sintetizadores y es flexible entre las frecuencias de reloj de 10 a 52 MHz. Los sintetizadores producen salidas complejas con niveles adecuados para controlar los mezcladores IQ. [40]

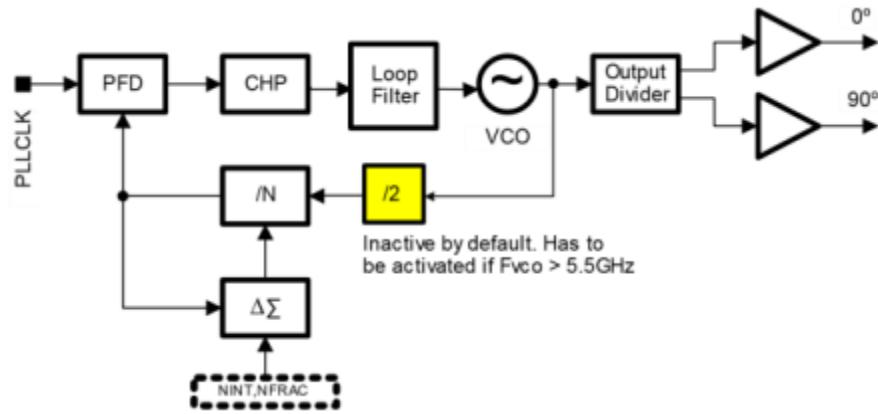


Figura 64 Arquitectura PLL [40]

- **Procesador de señal del transceptor:** LMS7002M incluye un alto número de puertas digitales dentro del bloque del Procesador de señales del transceptor. La función del TSP es emplear técnicas avanzadas de procesamiento de señales digitales para mejorar el rendimiento de las partes analógicas / RF. Esto se traduce en un mejor rendimiento del sistema general y un ahorro en el consumo total de energía. [40] En la figura 65 se muestra el diagrama de bloques del procesador que se encuentra en el dispositivo LM7002M.

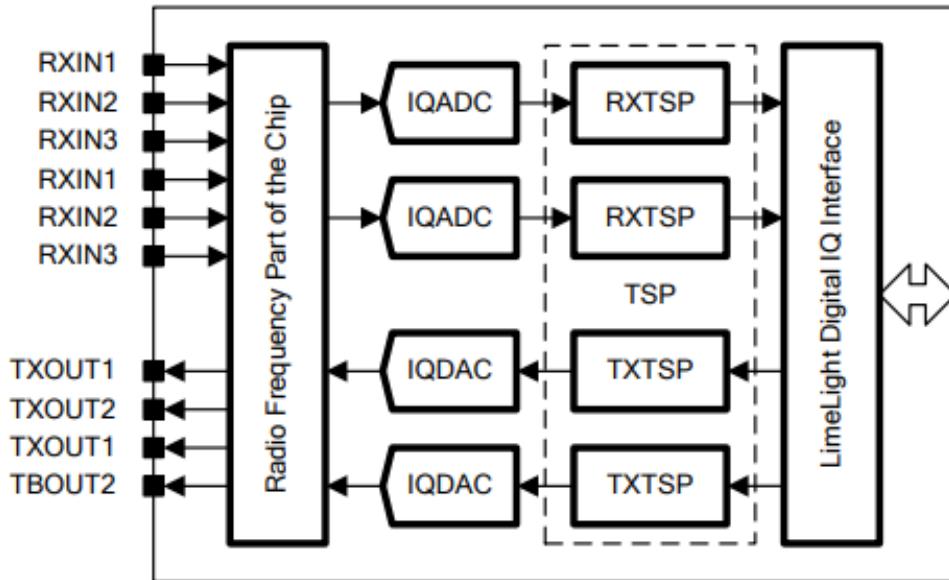


Figura 65 Parte TSP del LMS7002M [40]

### 3.4.2 FPGA: Intel Altera MAX 10 (10M16SAU169C8G)

Las FPGA son matrices de puertas eléctricamente configurables que contienen múltiples niveles de lógica. Las FPGA se caracterizan por altas densidades de compuertas, alto rendimiento, un número grande de entradas y salidas definibles por el usuario, un esquema de interconexión flexible. No están limitadas a la típica matriz AND-OR. Contienen una matriz interna configurable de relojes lógicos (CLBs) y un anillo de bloques de entrada/salida (IOBs). [41] En la figura 66 se observa la estructura de una FPGA en diagrama de bloques.

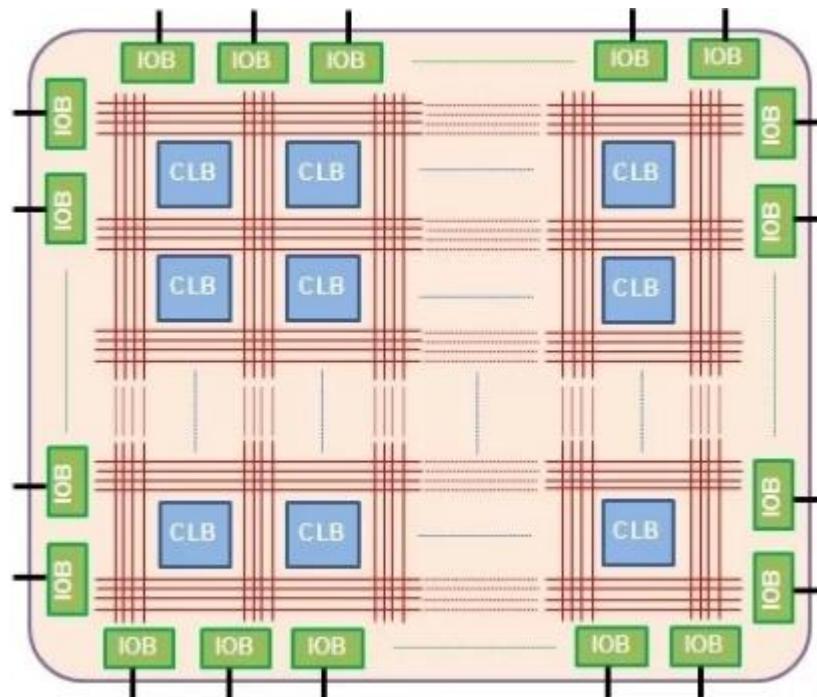


Figura 66 Estructura de una FPGA [42]

La FPGA que utiliza limeSDR mini, es la MAX 10 de altera la cual tiene las siguientes características:

- **Memoria M9K:** Es una memoria síncrona que tiene varios modos de funcionamiento, se puede utilizar como ROM para que solo sea una memoria de lectura y no de escritura. En la versión MAX 10 tiene una memoria de 549KB.
- **Memoria flash:** Es una memoria que permite escritura y lectura de datos, permite velocidades superiores a diferencia de las tecnologías EEPROM. En la MAX 10 tenemos una capacidad de 2368 KB.
- **PLL:** Un PLL permite configurar la frecuencia de una señal de reloj entrante. Por lo que se puede incrementar un reloj de baja frecuencia a uno de alta frecuencia. Esto lo hace generando varias señales de

reloj cuadrada generando un desfase entre ellas. La MAX 10 contiene 4 módulos PLL.

- **Multiplicadores:** La FPGA MAX 10 contiene 45 multiplicadores digitales de 18x18 bits.
- **Entradas de propósito general:** La FPGA MAX 10 contiene 130 pines configurables para entrada o salida. Lo cual se puede aprovechar en varios proyectos.
- **Entrada JTAG:** Esta entrada permite la configuración de la FPGA.

### 2.4.3 USB 3.0

USB 3.0 es la próxima versión importante de Universal Serial Bus (USB). Ofrece la misma facilidad de uso y la capacidad "plug and play" (conecte y listo) de las tecnologías USB anteriores, pero con un aumento de 10 veces el rendimiento y mejor administración del consumo de energía. Para los usuarios de USB 3.0, el objetivo de conectar dispositivos a PCs o notebooks es todavía el mismo que para la especificación USB 2.0. El aumento en el rendimiento se logra a través de la tecnología USB 3.0, que permite múltiples flujos de transferencia de datos y aumenta su ancho de banda pico de señalización a 5 Gb/seg en comparación con 480 Mb/seg para USB 2.0. Aunque las especificaciones son 5Gbps, las velocidades de transferencia varían según el controlador y la configuración Flash NAND. Actualmente pueden encontrarse dispositivos USB 3.0 con diferentes canales y arquitecturas. [43]

Esta es una de las grandes ventajas de la empresa microsystems ya que permite la posibilidad de comunicarte con el dispositivo SDR a grandes velocidades. En la mayoría de los estándares de comunicación, como wifi, 2G, 3G, 4G, necesitan de una alta velocidad al momento de transmitir y recibir datos del usuario. En la red celular 2G GSM implementada en el actual trabajo, se necesita de un alto rendimiento al momento de transmitir y recibir datos, ya que con una cantidad grande de usuarios. La red necesita enviar datos de manera más rápida al dispositivo SDR, por lo tanto, esta red será más lenta y generará una latencia más grande.

LimeSDR en su versión mini utiliza el controlador FTDI FT601 para la conexión USB 3.0 tipo A. En la figura 67 se muestra el diagrama de bloques del puerto USB 3.0.

El FT600 / FT601 es un chip de puente de interfaz USB 3.0 FIFO con las siguientes funciones:

- Admite la transferencia de velocidad súper USB (5Gbps) / USB 2.0 de alta velocidad (480Mbps) / velocidad completa de USB 2.0 (12Mbps).
- Tipo de transferencia USB admitido: Control / Bulk / Interrupción

- Hasta 8 puntos terminales configurables (PIPEs).
- Admite 2 protocolos de bus FIFO esclavo paralelo 245 y modo FIFO, FT601 con 32 bits
- La interfaz paralela tiene una velocidad de descarga de datos de hasta 400 MB / s.
- Admite 4 canales IN y 4 canales OUT en la conectividad del bus FIFO.
- Memoria RAM de datos FIFO de 16kB incorporada.
- Admite capacidad de activación remota.
- Admite E / S de voltaje múltiple: 1.8V, 2.5V y 3.3V.
- Soporte GPIO configurable.
- Regulador interno LDO 1.0V.
- Circuito integrado de encendido y reinicio.
- Descriptores USB programables por el usuario.
- Soporta especificaciones de carga de batería. BC1.2 detección de carga de la batería.
- Disponible como interfaz FIFO FT600-16bit / FT601-32bit.
- Rango de temperatura de operación industrial: -40 a 85°C.
- Disponible en paquetes compactos sin Pb QFN-76 (32 bits) y QFN56 (16 bits) (ambos compatibles con RoHS). [44]

En la figura 67 se muestra el diagrama de bloques del dispositivo dispositivo USB 3.0 que utiliza el limeSDR.

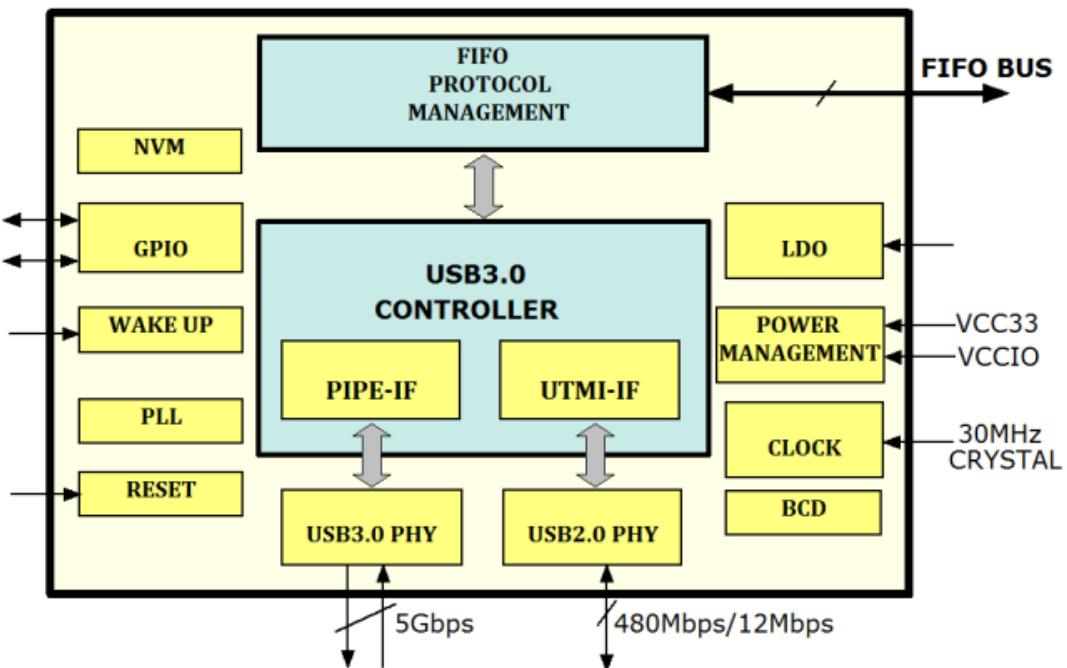


Figura 67 Diagrama de bloques del FTDI FT601 [44]

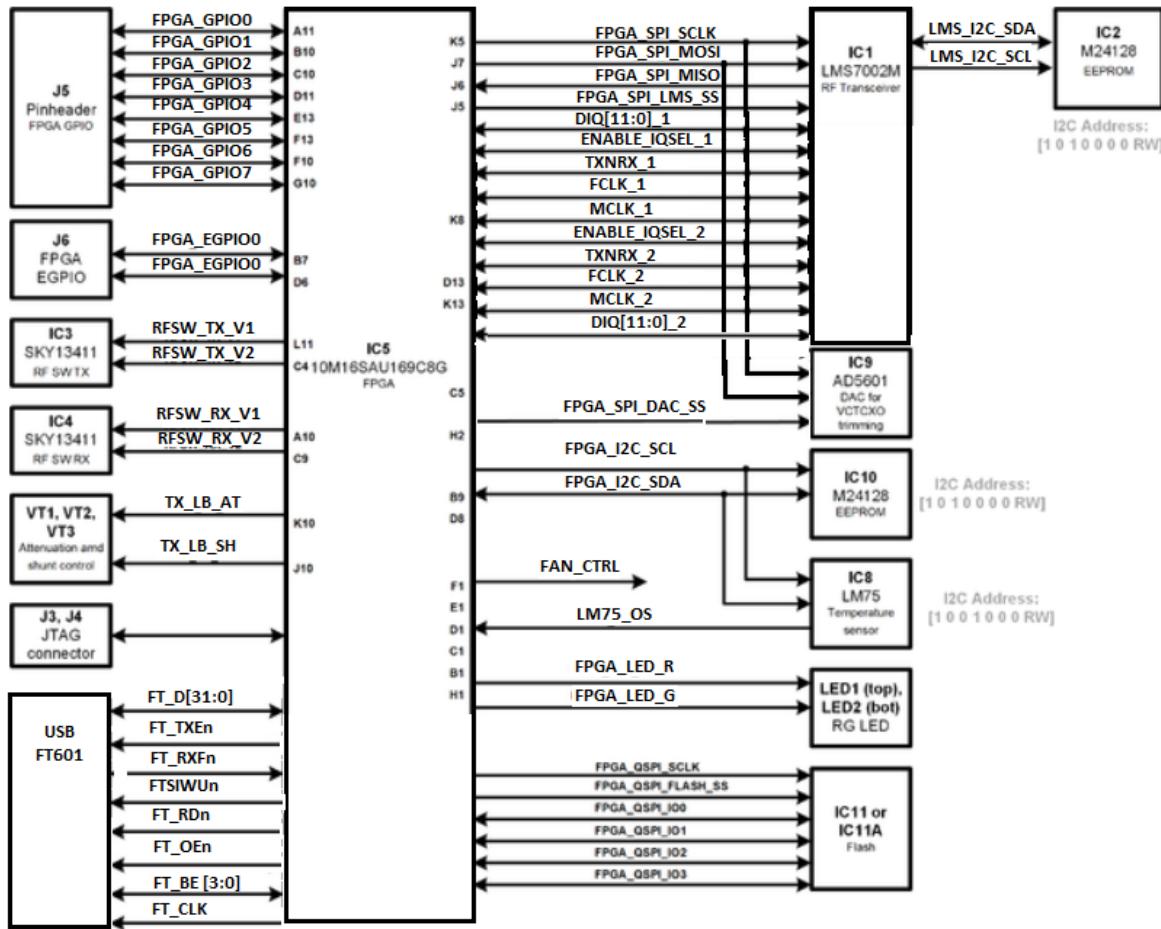


Figura 68 Diagrama de bloques completo del dispositivo LimeSDR mini

En la figura 68 se muestra el diagrama de bloques completo, donde se puede observar las conexiones entre los diferentes componentes electrónicos.

## CAPÍTULO 4

### CONFIGURACIÓN DE UNA ESTACIÓN BASE GSM

En los capítulos anteriores se explican los conceptos básicos para el funcionamiento de una estación base y el funcionamiento del dispositivo SDR a utilizar, ahora instalamos las aplicaciones necesarias para implementar la arquitectura de una estación base 2G GSM. Es necesario entender que aplicaciones se están instalando y para qué, y se explica cada una de las partes.

OSMOCOM es un proyecto sobre comunicaciones móviles de código abierto que permite instalar sus dependencias sin ninguna restricción, existe desde finales del 2008 y es un proyecto comunitario clásico dirigido por entusiastas. Con la desventaja de ser para personas expertas en comunicaciones. OSMOCOM ofrece los siguientes proyectos:

- Las implementaciones GSM y 3G del lado de la red originalmente conocidas como OpenBSC (pero ahora incluyen BTS, PCU, BSC, MSC, HLR, PCU, SGSN, GGSN)
- Implementación GSM del lado del teléfono OsmocomBB
- El proyecto RTL-SDR utilizado para la transmisión y recepción de televisión digital.
- OsmoNitb que implementa la arquitectura de una red celular 2G para principiantes en el área de comunicaciones.

OSMOCOM actualmente funciona a base de donaciones y de personas que aportan sus conocimientos sin ninguna ganancia o beneficio.

En este proyecto se utilizó Ubuntu 16.04 LTS, por lo que solo se aseguran y se solucionan los problemas generados por esta versión. Considerando los problemas que se presentaron, se podrían resolver también en las versiones 18.04, 18.10 y 19.04. Además, se recomienda las versiones LTS debido a que la descarga de paquetes es asistida por lo que no hay que instalar las bibliotecas de manera independiente.

#### 4.1 LIMESUITE.

Antes de iniciar a construir LimeSuite desde la fuente, es necesario instalar varias dependencias, ya que sin ellas no se podrá hacer ninguna instalación:

**GIT:** es un sistema de control de versiones distribuido (figura 69) de código abierto y gratuito, diseñado para manejar desde proyectos pequeños hasta proyectos grandes, con rapidez y eficiencia. [45]

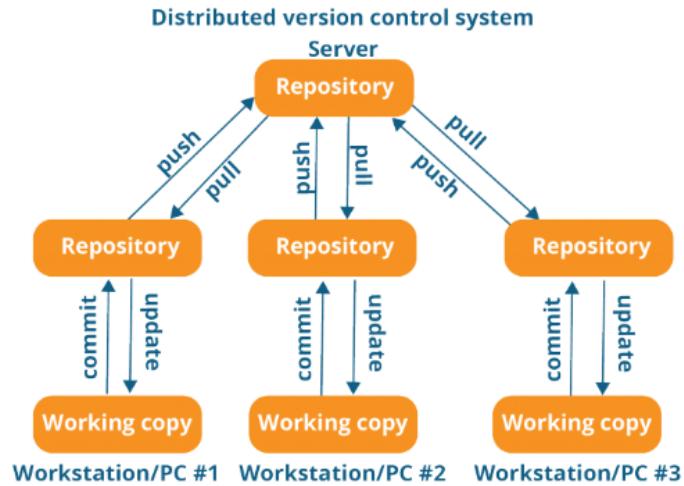


Figura 69 Control de versiones distribuido [46]

Fue creado por Linus Torvalds en 2005 para desarrollar el kernel de Linux. Git tiene la funcionalidad, el rendimiento, la seguridad y la flexibilidad que la mayoría de los equipos y desarrolladores individuales necesitan.

**G++:** es el compilador de código de c++.

**Cmake:** es una familia de herramientas multiplataforma de código abierto diseñada para compilar, probar y empaquetar software. CMake se utiliza para controlar el proceso de compilación de software mediante una plataforma simple y los archivos de configuración independientes del compilador, y generar makefiles y espacios de trabajo nativos que se pueden usar en el entorno de compilación que elija. [47]

**Libsqlite3-dev:** SQLite es una biblioteca de C que implementa un motor de bases de datos SQL. Los programas que enlazan con la biblioteca SQLite pueden tener acceso a bases de datos SQL para ejecutar un proceso de gestión de base de datos relacionales separado. [48]

**Libusb-1.0-0-dev:** Biblioteca para la programación de aplicaciones USB sin el conocimiento de los componentes internos del kernel de Linux.

Para instalar todos esos complementos se ejecuta el siguiente comando en la terminal de Ubuntu:

```
apt install git g++ cmake libsqlite3-dev libusb-1.0-0-dev
```

Las bibliotecas que se instalarán dependen de otras bibliotecas, así que, si ocurre un error relacionado con el faltante de una de estas, solo es necesario instalarla, para instalar cualquier biblioteca es necesario el comando:

```
-apt install "nombre de la librería"
```

Si por alguna razón, no te permite instalarla hay que ir a la página, que se encuentra en la referencia [49], y descargar directamente las bibliotecas, ya que en algunos casos no existen para la versión de Ubuntu que se utiliza.

Ya instaladas las bibliotecas y complementos necesarios se instala LimeSuite.

Lime Suite es una colección de software que admite varias plataformas de hardware, incluida la LimeSDR, los controladores para el transceptor RFIC LMS7002M y otras herramientas para desarrollar con hardware basado en LMS7. [50] En la figura 70 se muestra el diagrama de bloques del lime suite.



Figura 70 Componentes de los controladores de LimeSuite [51]

#### 4.1.1 LMS7 Drivers

LimeSuite ofrece 2 opciones para interactuar con el LM7002M. Estos 2 controladores actúan como un puente entre la comunicación del bus SPI de bajo nivel y las de alto nivel.

- **LMS7002M driver C++.**

Proporciona llamadas de alto nivel API para controlar las configuraciones de ganancias filtros y ajustes del LM7002M. Además, proporciona la autocalibración y recuperación de los resultados de calibración de la base de datos.

- **LMS7002M driver C.**

A diferencia del driver c++, el driver c no proporciona autocalibración y los resultados de la base de datos.

#### 4.1.2 Board support.

Debido a los diferentes dispositivos fabricados por microsystems, LimeSuite proporciona soporte para cada uno de estos equipos.

- **Interfaz de conexión.**

La interfaz de conexión es una clase de c++ capaz de extraer detalles específicos de hardware mediante el puerto USB. Esto da la posibilidad de controlar transmisiones del bus SPI de bajo nivel y escrituras de registros. Esta interfaz de conexión da flexibilidad para trabajar con varios equipos RFIC de LMS7.

- **Registro de conexión.**

Este maneja un registro de los dispositivos disponibles. Permite identificar los equipos conectados, para tener una clasificación y ver las limitantes al utilizarlos.

- **Soporte de software personalizado.**

Esto permite a los desarrolladores, utilizar todas las piezas de hardware para el propósito que requieran.

#### 4.1.3 Lime Suite GUI

Lime Suite proporciona una interfaz gráfica para que el usuario pueda interactuar con el dispositivo, en esta interfaz se pueden descargar todas las configuraciones actuales del dispositivo en un archivo con extensión ini. Además, se pueden cargar configuraciones con este mismo archivo. Algo muy importante es que en esta interfaz se puede actualizar el firmware de la FPGA, en la figura 72 y 73 se muestra el menú que te permite realizar esta acción. En la figura 71 se muestra el menú para conectar el dispositivo limeSDR.

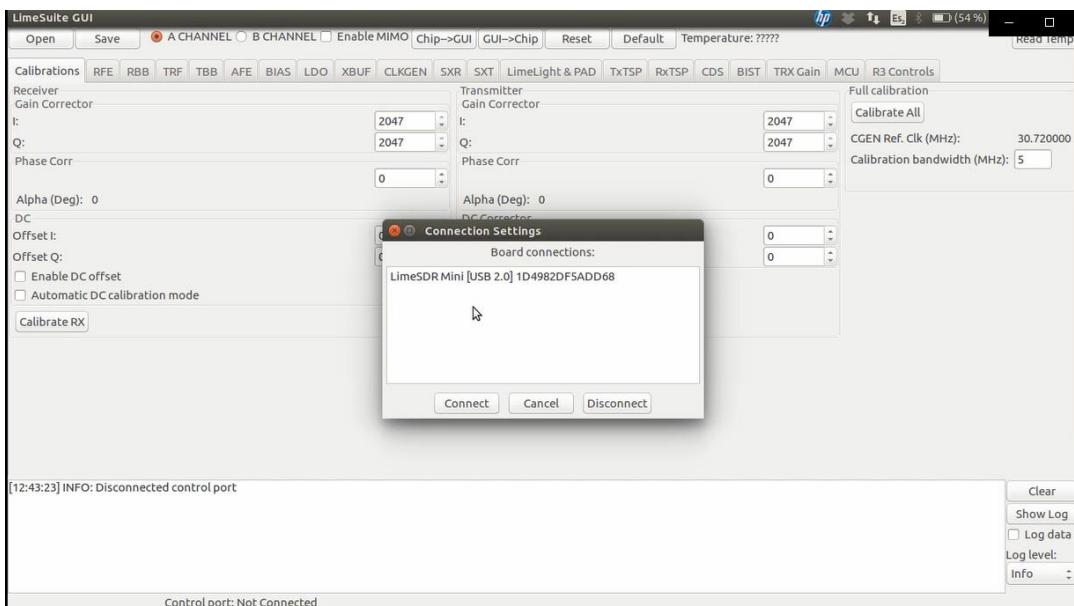


Figura 71 Interfaz gráfica de limesuite GUI

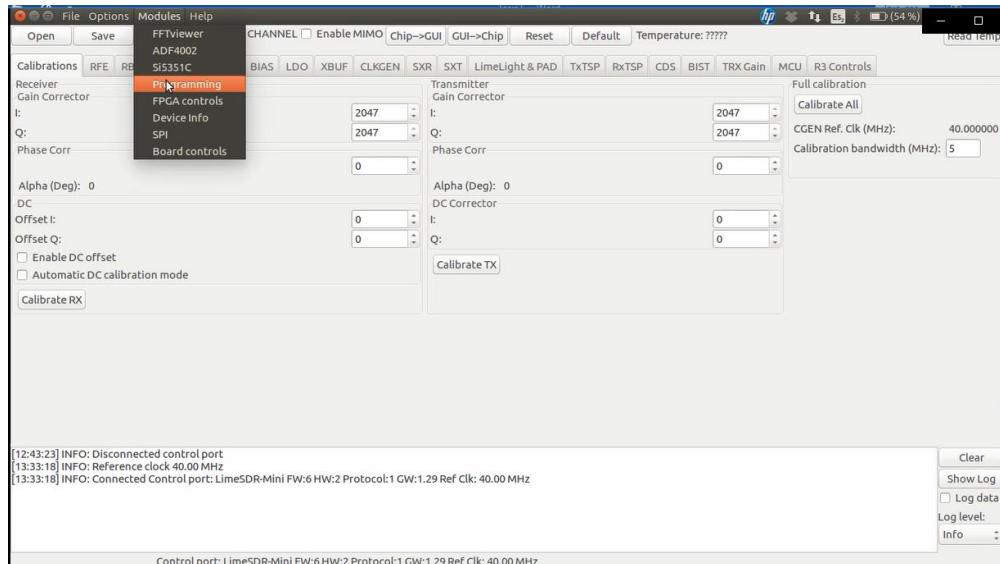


Figura 72 Menú de limesuiteGUI

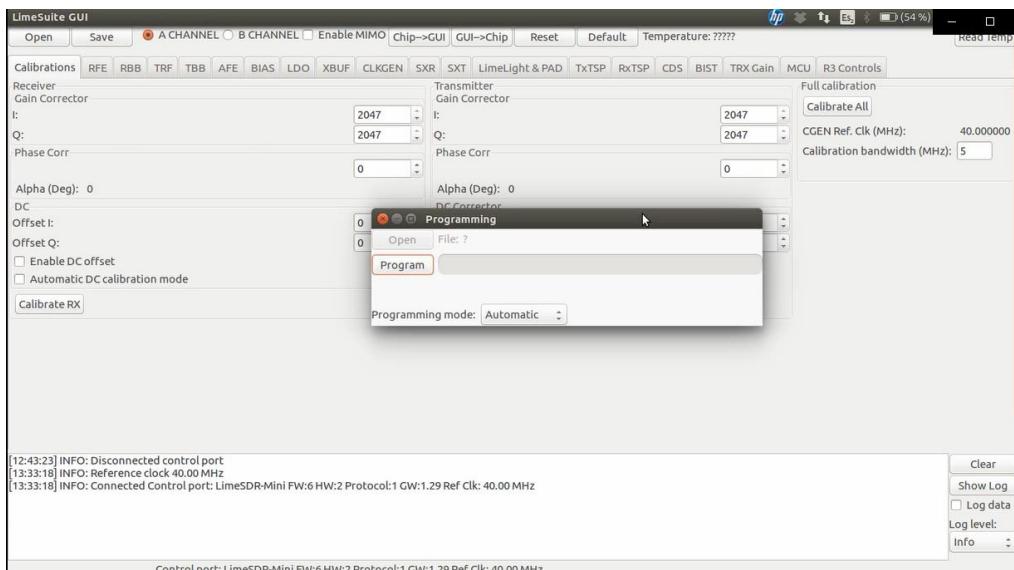


Figura 73 Actualización del firmware de la FPGA

#### 4.1.4 SDR interfaces.

Lime Suite ofrece a los usuarios opciones a la hora de interactuar con hardware compatible como LimeSDR. Los usuarios tienen acceso a API de bajo y alto nivel, e integración con una variedad de API y aplicaciones de software en el ecosistema SDR a través de Soapy SDR. [52]

- **Soapy SDR.**

La suite viene con un módulo de soporte llamado SoapyLMS7 que vincula la conexión de Lime Suite y la API de los controladores con la biblioteca SoapySDR. SoapySDR actúa como un puente entre

controladores, API y aplicaciones SDR. Proporciona API en varios idiomas (C, C++, python), acceso remoto para usar de forma transparente a través de una red local y enlaces para múltiples entornos de programación de SDR y aplicaciones gráficas de SDR. Estas aplicaciones incluyen GQRX, Pothos, CubicSDR y GNU Radio.

**GQRX:** es un receptor de radio definido por software de código abierto (SDR) alimentado por GNU Radio y el kit de herramientas gráficas Qt. [53] En la figura 74 se muestra la interfaz grafica de GQRX.

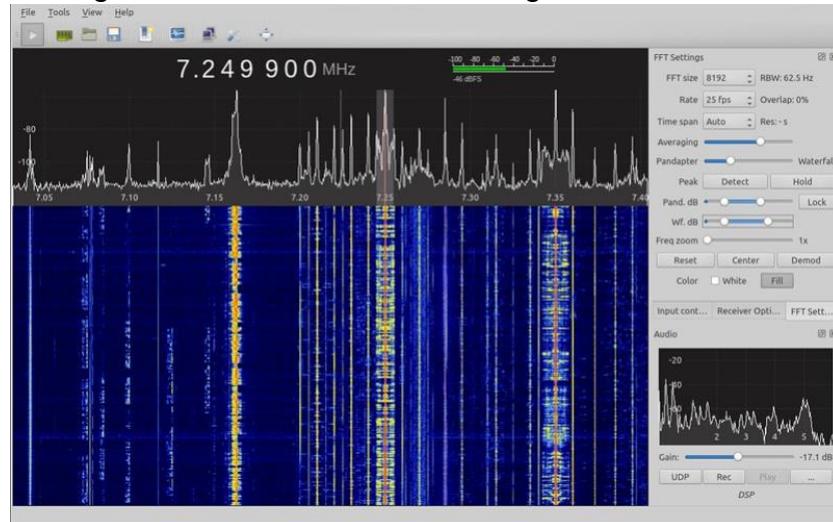


Figura 74 Interfaz gráfica de GQRX [53]

**Photos GUI:** Interfaz gráfica para la transmisión y recepción de radio estándares de radiofrecuencia utilizando un dispositivo SDR. En la figura 75 se puede ver la interfaz proporcionada por la aplicación Photos SDR.

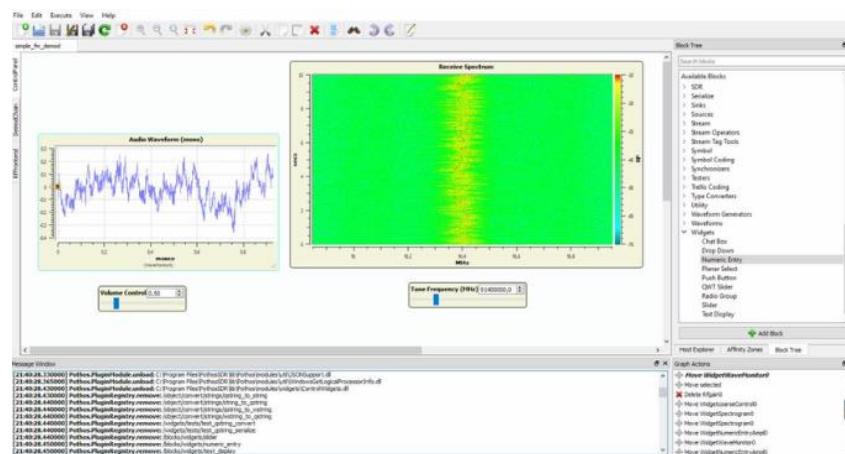


Figura 75 Interfaz gráfica de PhotosGUI

**CubicSDR:** Aplicación para la lectura de señales de radio frecuencia utilizando un dispositivo SDR. En la figura 76 se puede observar la interfaz gráfica de la aplicación.

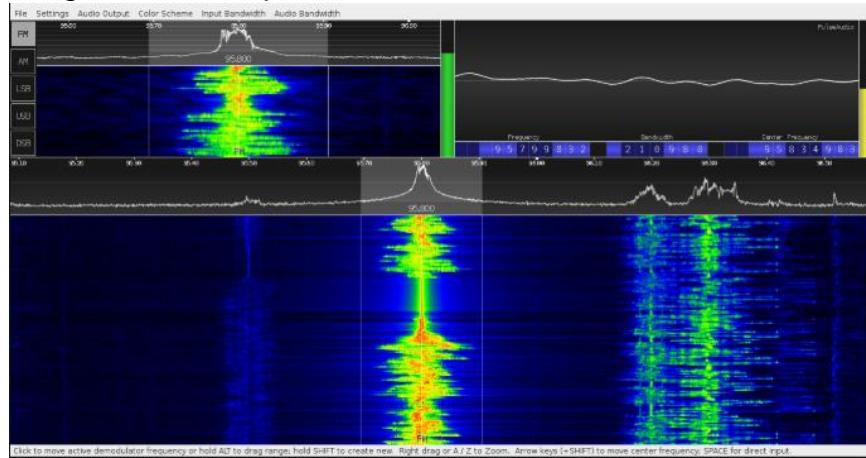


Figura 76 Interfaz gráfica de CubicSDR [54]

**GNURADIO:** GNU Radio es un kit de herramientas de desarrollo de software gratuito y de código abierto que proporciona bloques de procesamiento de señales para implementar radios definidos por software. Se puede usar con hardware de RF externo de bajo costo fácilmente disponible para crear radios definidas por software, o sin hardware en un entorno similar a la simulación. Es ampliamente utilizado en investigación, industria, academia, gobierno y entornos de aficionados para apoyar tanto la investigación de comunicaciones inalámbricas como los sistemas de radio del mundo real. [55] En la figura 77 se muestra la interfaz gráfica de GNU radio.

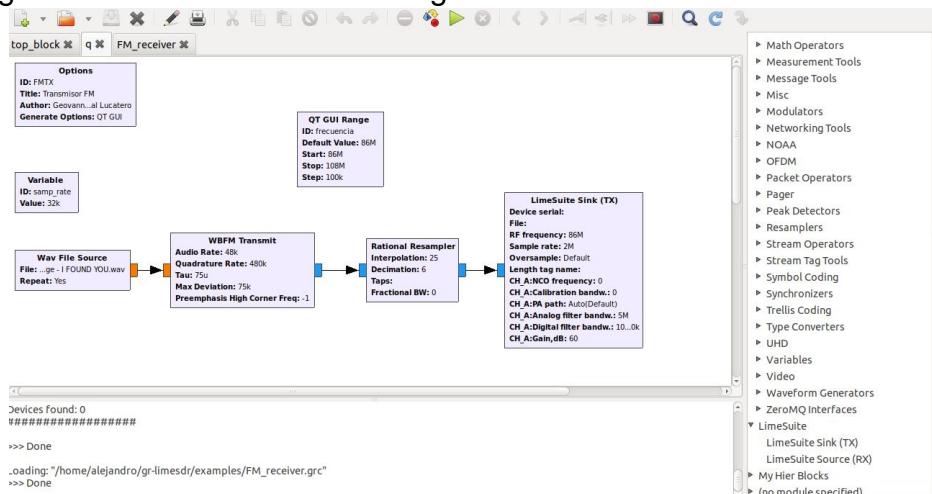


Figura 77 Interfaz gráfica de GNURADIO

Para instalar limesuite se ejecutan los siguientes comandos en la terminal de Ubuntu.

```
git clone https://github.com/myriadrf/LimeSuite.git
cd LimeSuite
mkdir construir && cd construir
cmake ../
make
make install
ldconfig
cd ../
sh LimeSuite/udev-rules/install.sh
CD ../
```

## 4.2 LIBOSMOCORE.

Antes de iniciar a instalar Libosmocore, hay que instalar algunas dependencias necesarias:

**Libtool:** En el pasado, si un desarrollador de paquetes de código fuente quería aprovechar el poder de las bibliotecas compartidas, necesitaba escribir un código de soporte personalizado para cada plataforma en la que se ejecutaba su paquete. También diseñar una interfaz de configuración para que el instalador del paquete pudiera elegir qué tipo de bibliotecas fueron construidas. GNU Libtool simplifica este trabajo al encapsular las dependencias específicas de la plataforma y la interfaz de usuario en un solo script. GNU Libtool está diseñado para que la funcionalidad completa de cada tipo de host esté disponible a través de una interfaz genérica, pero se oculten al programador los detalles desagradables. [56]

**Pkg-config:** es una herramienta de ayuda que se utiliza al compilar aplicaciones y bibliotecas. Le ayuda a insertar las opciones de compilador correctas en la línea de comandos. [57]

**Libtalloc-dev:** asignador de memoria basado en grupo jerárquico. [58]

**Libgnutls-dev:** GnuTLS es una biblioteca que implementa los protocolos de Seguridad de la capa de transporte (TLS 1.0, 1.1, 1.2, 1.3) y Seguridad de la capa de transporte de datagramas.

Para instalar estas dependencias se ejecuta el siguiente comando en la terminal de Ubuntu:

```
apt install libtool pkg-config libtalloc-dev libgnutls28-dev
```

Libosmocore es una biblioteca con varias funciones de utilidad que se desarrollaron originalmente como parte del proyecto OpenBSC, pero que son

de naturaleza más genérica y, por lo tanto, son útiles para (al menos) otros programas en el ámbito del Software libre / Mobile de código abierto. [59]

El repositorio osmocom.git contiene las siguientes bibliotecas:

- Libosmocore: contiene algunas funciones de propósito general como la abstracción de ciclo de selección, buffers de mensajes, temporizadores, listas enlazadas.
- Libosmocvt contine rutinas relacionadas con la interfaz de línea de comandos interactiva llamada VTY.
- Libosmogsm contiene definiciones y código auxiliar relacionado con los protocolos GSM.
- Libosmocctrl contiene una implementación compartida de la interfaz de control de Osmocom.
- Libosmogb contiene una implementación de la interfaz Gb con sus protocolos NS / BSSGP.
- Libosmocodec contiene una implementación de codecs de voz GSM.
- Libosmocoding contiene una implementación de las funciones de transcodificación GSM 05.03 burst.
- Libosmosim contiene infraestructura para conectar tarjetas SIM / UICC / USIM. [59]

Para instalar, se ejecuta la siguiente lista de comandos en la terminal de Ubuntu:

```
git clone git://git.osmocom.org/libosmocore  
cd libosmocore  
autoreconf -fi  
.configure  
make  
make install  
ldconfig  
cd ..
```

#### 4.3 OSMO-TRX-LMS.

Para la instalación de osmo trx para LimeSDR es necesario instalar la siguiente biblioteca:

**Libfftw3-dev:** La biblioteca FFTW calcula las transformadas rápidas de Fourier (FFT) en una o más dimensiones. Es extremadamente rápido. Este paquete contiene la biblioteca enlazada estáticamente, los archivos de encabezado y los programas de prueba. [60]

Para instalarla ejecutamos el siguiente comando en la terminal:

```
apt install libfftw3-dev
```

OsmoTRX es un transceptor de radio definido por software que implementa la capa física de Capa 1 de un BTS que comprende las siguientes especificaciones de 3GPP:

- TS 05.01 "Capa física en la ruta de radio"
- TS 05.02 "Multiplexación y acceso múltiple en la ruta de radio"
- TS 05.04 "Modulación"
- TS 05.10 "Sincronización de subsistemas de radio"

OsmoTRX se basa en el código del transceptor del proyecto OpenBTS , pero se configura para funcionar de manera independiente con el propósito de usarlo con software y proyectos que no sean de OpenBTS, mientras se mantiene la compatibilidad con OpenBTS . Actualmente hay numerosas funciones en OsmoTRX que amplían la funcionalidad del transceptor OpenBTS . Estas características incluyen soporte mejorado para varias plataformas integradas, en particular ARM. [61]

Para instalar osmo-trx para el limeSDR se ejecutará la siguiente lista de comandos:

```
-git clone git://git.osmocom.org/osmo-trx  
-cd osmo-trx  
-autoreconf -fi  
-./configure --without-uhd --with-lms  
-make  
-make install  
-ldconfig  
-cd ..
```

#### **4.4 OSMO-NITB Y OSMO-BTS.**

OsmoBTS implementa el software para la emulación de una BTS GSM. Por lo que desarrolla los siguientes protocolos e interfaces.

- LAPDm (GSM 04.06): Forma la capa física de la interfaz Um que conecta a la MS con la BTS.
- RTP: Se utiliza para los codecs de envío de datos, especificando los parámetros técnicos de audio.
- A-bis / IP en multiplex IPA: Es la interfaz de comunicación entre la BTS y la BCS.
- OML(GSM TS 12.21): Este enlace se utiliza para transferir mensajes BTS O&M. [62]
- RSL (GSM TS 08.58): Este enlace se utiliza para transferir mensajes de Abis Layer 3 entre BTS y BSC. Además, sirve a los procedimientos de gestión de tráfico de la Capa 2. [62]

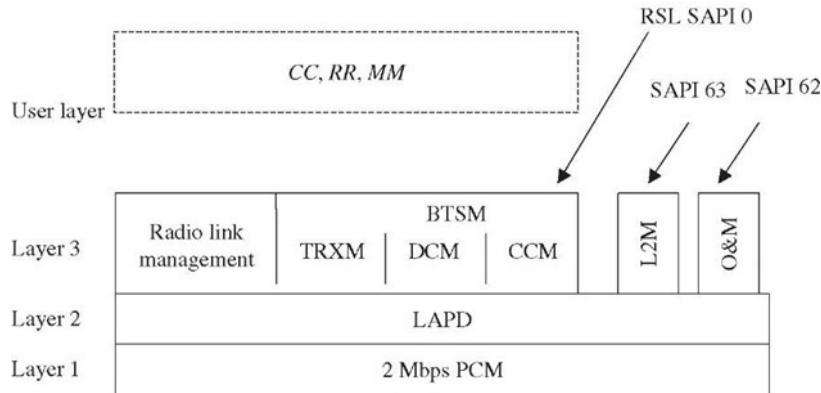


Figura 78 Pila de protocolos sobre la interfaz Abis. [62]

OsmoNITB implementa todo lo necesario para una red de conmutación GSM, esto de manera limitada, ya que en la actualidad ya no se le da soporte a esta parte. OsmoNITB se encarga de todo el subsistema de conmutación de red, desde el MSC hasta las bases de datos HLR y VLR como se muestra en el diagrama de bloques de la figura 79.

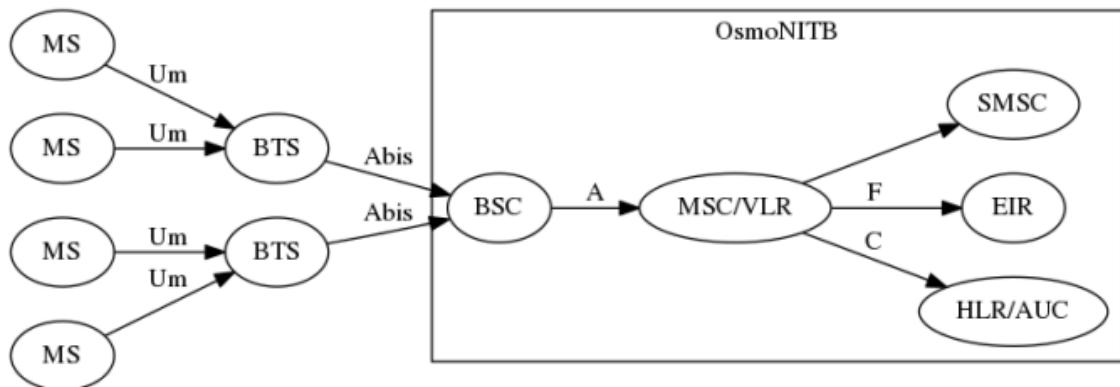


Figura 79 Arquitectura GSM utilizando OSMONITB [63]

- **BSC:** cubre la funcionalidad clásica de un controlador de estación base GSM, es decir:
  - configurar y activar BTS con sus TRX y TS
  - implementar la interfaz / protocolos A-bis para señalización y datos de voz reales (tramas TRAU).
  - Procesar los resultados de medición de las estaciones móviles en modo dedicado, realizar la entrega y la decisión de entrega. [63]
- **HLR/AUC:** Implementa en la base de datos el HLR además del AUC para la autenticación de usuarios.

- **SMSC:** Un servidor de almacenamiento y reenvío mínimo para SMS, compatible con los servicios de MO y MT SMS, así como con mensajes de varias partes. El SMSC incorporado también admite una interfaz externa de SMSC. [63]
- **MSC:** El componente MSC de OsmoNITB implementa las funciones de administración de movilidad (MM) del TS 04.08, así como los procedimientos opcionales relacionados con la seguridad para la autenticación y el cifrado criptográficos. Además, puede manejar el Control de Llamada (CC) TS 04.08, ya sea mediante el uso de un controlador interno del MNCC, o mediante el uso de un agente externo del MNCC. [63]
- **TRAU / E1:** A diferencia de las redes GSM clásicas, OsmoNITB no realiza ninguna transcodificación. Más bien, se selecciona un códec compatible para ambos tramos de una llamada y los marcos de códec se pasan de forma transparente. Para lograr esto con BTS basado en E1, OsmoNITB contiene un multiplexor y demultiplexor de subcanales E1, así como un mapeador TRAU que puede asignar el enlace ascendente a las tramas del enlace descendente y viceversa. [63]
- **RTP proxy:** Los modelos BTS que implementan A-bis sobre IP no utilizan tramas TRAU clásicas, sino que suelen transportar las tramas del códec de voz como Protocolo RTP / UDP / IP. OsmoNITB puede indicar a los BTS que envíen esas secuencias de voz directamente entre sí (BTS a BTS sin ningún intermediario) como se muestra en la figura 80, o puede ejecutar un proxy RTP interno para pasar tramas de un BTS a otro. [63]

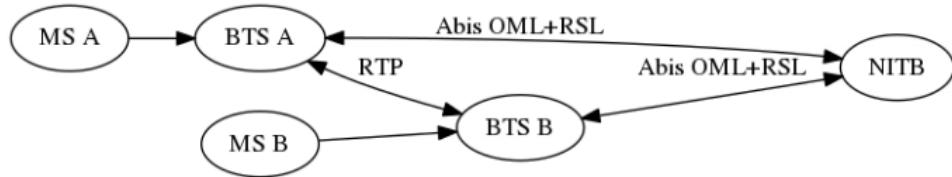


Figura 80 RTP proxy entre BTS [63]

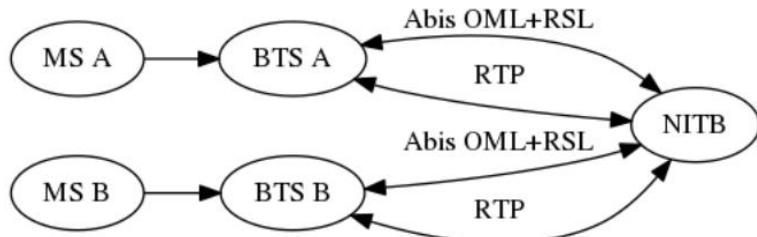


Figura 81 RTP Proxy entre BTS y BSC [63]

Para instalar osmo-BTS y osmo-NITB se tienen que ejecutar los siguientes comandos en la terminal de Ubuntu:

```
-Wget
http://download.opensuse.org/repositories/network:/osmocom:/latest/Raspbian_9.0/Release.key
-sha256sum Release.key
-apt-key add Release.key
-rm Release.key
-echo "deb
http://download.opensuse.org/repositories/network:/osmocom:/latest/Raspbian_9.0/ ./" > /etc/apt/sources.list.d/osmocom-latest.list
-apt update
-apt install osmocom-nitb osmo-bts-trx telnet
-systemctl disable osmo-bts-trx.service
-systemctl disable osmo-nitb.service
```

Con esto tenemos instalada la arquitectura de una red GSM, para una mejor comprensión del funcionamiento total de osmoNitb recomiendo la información que se encuentra en [63].

En la figura 82 se muestra un diagrama de bloques con el resumen del funcionamiento de todo el sistema instalado. En el diagrama se muestra los componentes de la arquitectura GSM instalados en la PC, así como las interfaces de comunicación entre cada uno de los bloques. Se puede ver que se incluye el dispositivo SDR mostrando la conexión entre los componentes más importantes del limeSDR.

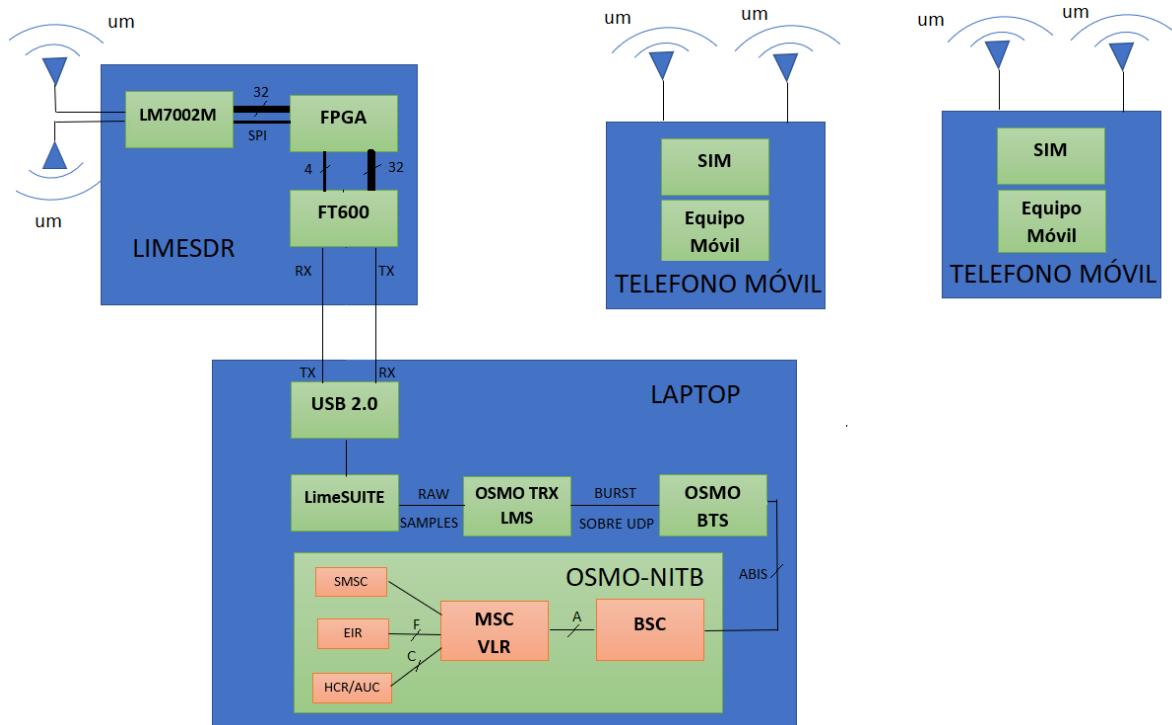


Figura 82 Diagrama de bloques del sistema implementado

En la figura 83 se muestra un ejemplo de enrutamiento de llamadas GSM. En el paso 1, un usuario de teléfono llama a una unidad móvil a través de la red telefónica pública. La llamada se enruta a un MSC (paso 2), el cual examina los dígitos marcados y determina que no puede enrutar la llamada más lejos; por tanto, en el paso 3, interroga el registro de ubicación de origen (HLR) del usuario llamado a través del SS7 que es un conjunto de protocolos de señalización encargados del finalizar y establecer llamadas . El HLR interroga al registro de ubicación de visitante (VLR) que actualmente está dando servicio al usuario (paso 4). En el paso 5, el VLR devuelve un numero de enrutamiento al HLR, que lo devuelve al MSC de puerta. Con base a este número de enrutamiento, el MSC de puerta enruta la llamada al MSC de terminal (paso 6). El MSC terminal consulta entonces al VLR para comparar la llamada entrante con la identidad del subscriptor receptor (paso 7 y 8). En el paso 9, la BSS recibe una solicitud de notificación del MSC terminal y envía una señal de notificación. Cuando la señal de usuario regresa, la llamada se completa (paso 10). [30]

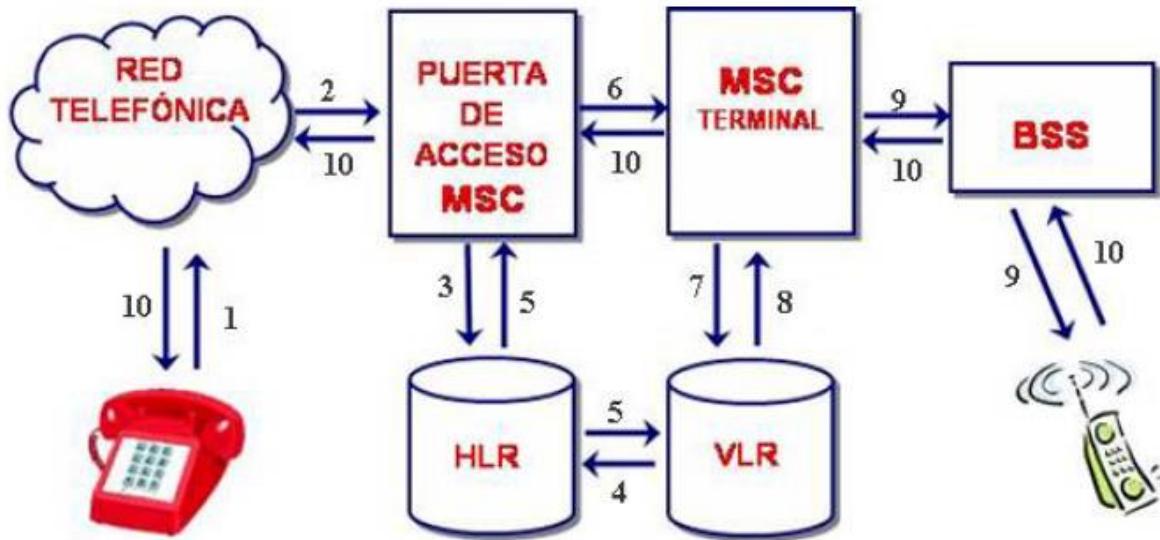


Figura 83 Proceso realizado durante la conmutación de una llamada [30]

Para enviar un mensaje de texto OsmoNitb utiliza SMS-SUBMIT [64] el cual tiene la estructura de tramas como se muestra en la figura 84.

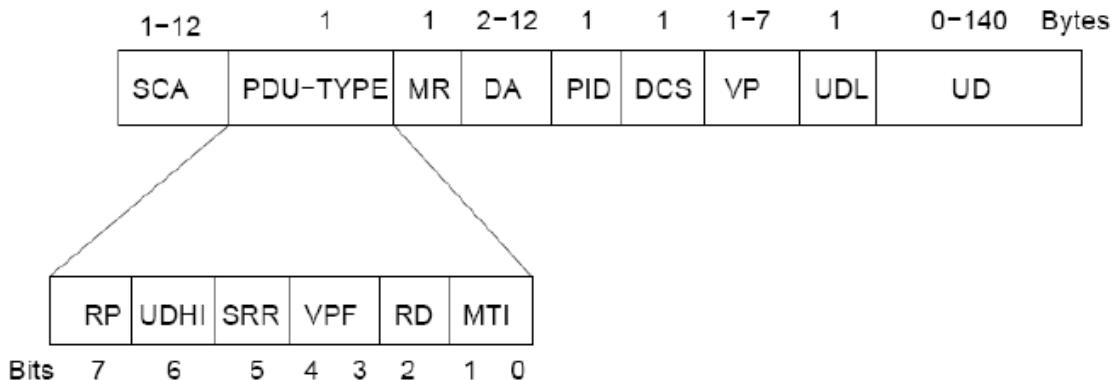


Figura 84 Tramas de SMS-SUBMIT

- **SCA:** Número de la extensión del centro de servicio (SC) de mensajes cortos. Este número se utiliza para saber a dónde enrutar el mensaje. Este número consta de los siguientes campos:
  - Logitud:** Cantidad de números del SC
  - Tipo de numero:** solo existen dos tipos, para un número nacional es 81h y para uno internacional es 91h.
  - Dígitos BCD:** Este es el número de teléfono del SC.
- **PDU-TYPE:** Aquí se encuentra la información sobre la unidad de datos del protocolo.
  - RP:** Parámetro que indica que existe la ruta de respuesta
  - UDHI:** Indica si el campo UD contiene solo el mensaje corto (UDHI=0) o si existe una cabecera del mensaje corto (UDHI=1).

**SRR:** Informe de estado. No solicitado (SRR=0), solicitado (SRR=1).

**VPF:** Indica si el campo VP está o no presente.

**RD:** Rechazar o no duplicados.

**MTI:** Tipo de mensaje.

- **MR:** Parámetro para identificar el mensaje.
- **DA:** Número de la extensión de destino.
- **PID:** Identificador del protocolo de la capa superior.
- **DCS:** Identificación del tipo de codificación.
- **VP:** Periodo de validez del mensaje.
- **UDL:** Longitud de campo UD.
- **UD:** Mensaje a enviar.

En la figura 85, 86, 87, 88 y 89 se presentará un ejemplo de lo descrito anteriormente:

Si se enviará un mensaje con el texto “hola” a la extensión 4435631523 y el centro de mensajes fuera 4431458646:

- **SCA: 0A814413546864.**

Longitud	Tipo	Tlf en BCD
0A	81	4413546864

Figura 85 SCA

- **PDU-TYPE:** OsmoNitb utiliza el SMS-SUBMIT de una manera muy simple por lo que en este apartado casi todo es cero, excepto el MTI que indica el tipo de mensaje, 00 indica deliver y 01 indica submit:

RP	UDHI	SRR	VPF	RD	MTI
0	0	0	00	0	01

Figura 86 PDU-TYPE

- **MR:** El número de referencia es 00h.
- **DA: 0A814453365132**

Longitud	Tipo	Tlf en BCD
0A	91	4453365132

Figura 87 DA

- **PID:** 00h (Mensaje corto)
- **DCS:** F6h (Codificación de 8 bits, en ASCII)
- **UDL:** 04 Longitud del texto que se envía.
- **UD:** 686F6C61

h	o	l	a
68	6F	6C	61

Figura 88 UD

La trama que se enviará será:

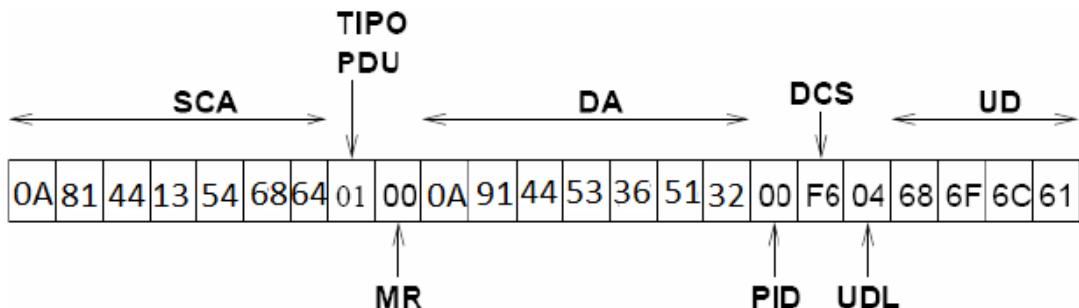


Figura 89 Trama completa del SMS

#### 4.5 ARCHIVOS DE CONFIGURACIÓN.

Para poder iniciar las aplicaciones de Osmocom, es necesario unos archivos de configuración de cada una de las aplicaciones. Estas configuraciones se pueden hacer manualmente con comandos o se generan estos archivos con las configuraciones básicas.

##### Configuración del BSC.

Con este archivo se configura el controlador de estación base, en el cual se establece, la frecuencia a la que se trabajara, el tipo de encriptación para la autentificación de los usuarios, el mcc, el mnc, además de la configuración para la comunicación con la bts.

```
password foo
!
line vty
no login
!
e1_input
e1_line 0 driver ipa
network
network country code 284
mobile network code 18
short name FIE
```

```
long name FIE
auth policy accept-all
location updating reject cause 13
encryption a5 0
neci 1
rrlp mode none
mm info 1
handover 0
handover window rxlev averaging 10
handover window rxqual averaging 1
handover window rxlev neighbor averaging 10
handover power budget interval 6
handover power budget hysteresis 3
handover maximum distance 9999
bts 0
type sysmobts
band GSM850
cell_identity 0
location_area_code 1
training_sequence_code 7
base_station_id_code 63
ms max power 15
cell reselection hysteresis 4
rxlev access min 0
channel allocator ascending
rach tx integer 9
rach max transmission 7
ip.access unit_id 1801 0
oml ip.access stream_id 255 line 0
gprs mode none
trx 0
rf_locked 0
arfcn 100
nominal power 23
max_power_red 20
rsl e1 tei 0
timeslot 0
phys_chan_config CCCH+SDCCH4
timeslot 1
phys_chan_config SDCCH8
timeslot 2
phys_chan_config TCH/F
timeslot 3
phys_chan_config TCH/F
```

```

timeslot 4
phys_chan_config TCH/F
timeslot 5
phys_chan_config TCH/F
timeslot 6
phys_chan_config TCH/F
timeslot 7
phys_chan_config TCH/F H/F

```

Varios aspectos de esta configuración necesitan una explicación más detallada. El MCC "código de país de la red" debe coincidir con el país donde tiene lugar la operación. Para México, este valor es 334 y está relacionado con el "código de red móvil" que debe coincidir con su operador MNC, en nuestro caso Telcel con código 20. Para una red de prueba, utilizamos el MCC 284 y el MNC 18 para no provocar interferencias con la red local. Para proporcionar un nombre a la red se utiliza short name "nombre corto" y long name "nombre largo" establecen los nombres de red que se utilizarán. Un parámetro importante es la llamada "política de autenticación". Define y limita el acceso de IMSI a la red. Puede tomar 1 de 3 valores:

- close: no permite que nadie que no esté marcado como autorizado=1 en la base de datos HLR
- acceptall: aceptar a todos en la red
- token: utiliza un TokenAuthPolicy por usuario

Como es una red de prueba se le da acceso a todos los usuarios que quieran conectarse a la red.

La opción Encryption "cifrado" le dice al BSC qué algoritmo usar para cifrar la interfaz aérea. Existen tres opciones:

- A5 0: Indica que no hay ninguna clase de cifrado.
- A5 1: Indica un cifrado A5, pero solo en teléfonos móviles que soportan esta clase de cifrado.
- A5 2: Es inseguro y ya no se utiliza.

Cuando se implementa una red con varias BTS, se utiliza handover para el traspaso de llamadas. En el archivo de configuración se toman en cuenta varios parámetros. El primer parámetro está relacionado con la activación de handover, para este tenemos 2 opciones:

- handover 0: deshabilita el handover.
- handover 1: habilita el handover.

Debido a que el proyecto solo contiene una BTS, se optó por deshabilitar el handover y no requerir de estos recursos para no necesitar de procesamiento computacional y alentar nuestra estación base.

Pero debido a que OsmoNitb no contiene parámetros por defecto para el handover, se tiene que especificar los parámetros relacionados con esta sección.

- Rxlevel se refiere a los valores de señal recibidos, para este caso el nivel debe de ser igual a 10.
- Rqlevel se refiere a la tasa de error de bits, en este caso menor a 1.
- Budget Interval se refiere a la disponibilidad de canales SACCH encargados de avisar si existe una llamada nueva. En este caso debe haber mínimo 6 canales disponibles.
- Budget hysteresis se refiere a que una celda vecina debe de ser al menos 3dB más fuerte que la celda de servicio para poder hacer el traspaso.
- Maximum distance se refiere a la distancia máxima de traspaso, en este caso es 9999 para referirte a la distancia máxima.

Lo descrito anteriormente se refiere a la configuración general de la red. Después se configura cada BTS por separado, en el caso de existir varias BTSSs. Se elige la BTS 0 del tipo sysmobts, además se elige la frecuencia a la que transmitirá. En el estándar GSM existe 850MHz, 900MHz, 1800Mhz, en este caso se utilizará 850 MHz.

Cada BTS puede tener varias antenas de transmisión y recepción dependiendo de qué tipo de antenas son, omnidireccional o sectorial. Al utilizar el dispositivo limeSDR mini solo tenemos acceso a una sola antena de recepción y una de transmisión. En este apartado de configuración se definen los parámetros de los canales transmitidos en cada time slot.

### **Configuración de la BTS.**

Hay algunas configuraciones que no se pueden hacer remotamente desde la BSC por lo que hay configuraciones que se deben hacer localmente desde el sysmoBTS.

```
!!
!
log stderr
  logging color 1
  logging timestamp 0
  logging level rsl notice
  logging level oml notice
  logging level rll notice
  logging level rr notice
  logging level loop debug
  logging level meas debug
  logging level pag error
  logging level l1c error
  logging level l1p error
  logging level dsp error
  logging level abis error
```

```

!
line vty
no login
!
phy 0
instance 0
osmotrx ip local 127.0.0.1
osmotrx ip remote 127.0.0.1
no osmotrx timing-advance-loop
bts 0
oml remote-ip 127.0.0.1
ipa unit-id 1801 0
gsmtap-sapi pdtch
gsmtap-sapi ccch
band 850
trx 0
    phy 0 instance 0

```

Para ver los errores provocados durante la ejecución de osmoBTS, se activa con el comando stderr donde se indica que errores muestre en la terminal. Después se configura la capa física “Physical layer” (phy), encargada de conectar la capa de enlace con la capa física. Debe de existir al menos un enlace phy para que funcione correctamente todo el sistema.

Para la comunicación local y remota se agregan las direcciones ip de comunicación con la BSC. Además, para identificar a la BTS se le agrega un ID “ipa unit-id”.

Algo muy importante es configurar la banda de frecuencia en la que se trabajara. Esta debe de ser la misma que en la configuración de la BSC.

### **Configuración de Osmo-trx.**

```

log stderr
logging filter all 1
logging color 1
logging print category 1
logging timestamp 1
logging print file basename
logging level set-all info
!
line vty
no login
!
trx
bind-ip 127.0.0.1
remote-ip 127.0.0.1
base-port 5700
egprs disable

```

```
tx-sps 4  
rx-sps 4  
rt-prio 18  
chan 0  
tx-path BAND1  
rx-path LNAW
```

En estos archivos de configuración de osmo BTS y osmoTRX se colocan las especificaciones de las direcciones ip y puertos utilizados.

# CAPÍTULO 5

## PRUEBAS Y RESULTADOS

Ya instalado y configurado el sistema para la estación base, pasamos a las pruebas para verificar su funcionamiento

### 5.1 EJECUCIÓN DE LA ESTACIÓN BASE GSM.

Para la estación base ejecutamos OsmoTRX, OsmoNitb y OsmoBTS, en el orden que se presenta a continuación. Si se hace de otra manera no se podrá ejecutar los programas ya que uno necesita del otro para arrancar. Además, es necesario ver que los puertos no estén ocupados, ya que OsmoNitb utiliza el puerto 4242. Para evitar este tipo de problema ejecutamos el comando de la figura 90.

```
export PATH  
feliche@feliche-HP:~$ sudo lsof -i -P -n | grep LISTEN
```

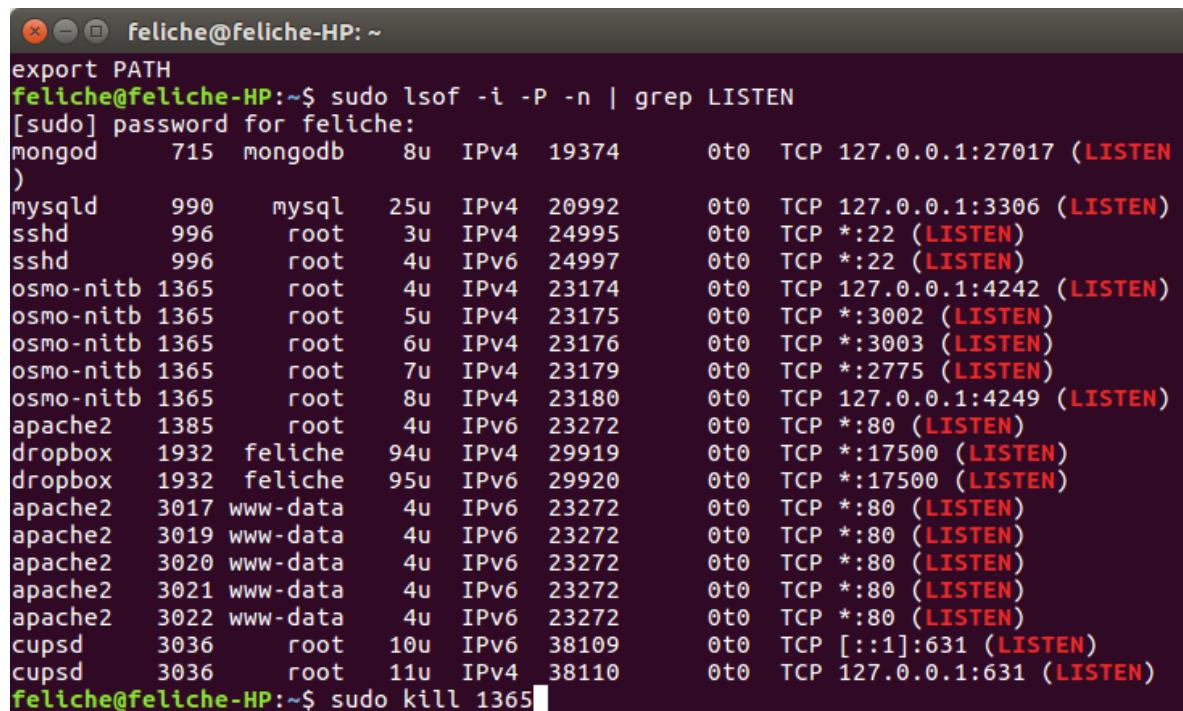
Figura 90 Ejecución del comando para ver los puertos utilizados.

Ejecutando el comando en la terminal se mostrará una lista como en la figura 91, donde buscaremos algún proceso que utilice el puerto 4242.

```
feliche@feliche-HP:~  
export PATH  
feliche@feliche-HP:~$ sudo lsof -i -P -n | grep LISTEN  
[sudo] password for feliche:  
mongod    715    mongodb    8u   IPv4    19374        0t0    TCP 127.0.0.1:27017 (LISTEN)  
)  
mysqld    990      mysql    25u   IPv4    20992        0t0    TCP 127.0.0.1:3306 (LISTEN)  
sshd     996      root     3u   IPv4    24995        0t0    TCP *:22 (LISTEN)  
sshd     996      root     4u   IPv6    24997        0t0    TCP *:22 (LISTEN)  
osmo-nitb 1365      root     4u   IPv4    23174        0t0    TCP 127.0.0.1:4242 (LISTEN)  
osmo-nitb 1365      root     5u   IPv4    23175        0t0    TCP *:3002 (LISTEN)  
osmo-nitb 1365      root     6u   IPv4    23176        0t0    TCP *:3003 (LISTEN)  
osmo-nitb 1365      root     7u   IPv4    23179        0t0    TCP *:2775 (LISTEN)  
osmo-nitb 1365      root     8u   IPv4    23180        0t0    TCP 127.0.0.1:4249 (LISTEN)  
apache2   1385      root     4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
dropbox   1932    feliche   94u   IPv4    29919        0t0    TCP *:17500 (LISTEN)  
dropbox   1932    feliche   95u   IPv6    29920        0t0    TCP *:17500 (LISTEN)  
apache2   3017    www-data   4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
apache2   3019    www-data   4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
apache2   3020    www-data   4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
apache2   3021    www-data   4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
apache2   3022    www-data   4u   IPv6    23272        0t0    TCP *:80 (LISTEN)  
cupsd     3036      root     10u   IPv6    38109        0t0    TCP [::1]:631 (LISTEN)  
cupsd     3036      root     11u   IPv4    38110        0t0    TCP 127.0.0.1:631 (LISTEN)
```

Figura 91 Puertos utilizados.

Como se muestra en la figura 91, OsmoNitb se quede ejecutando, por lo que es necesario terminar el proceso que utiliza ese puerto. Lo cual se hace ejecutando el comando de la figura 92.



```
feliche@feliche-HP:~$ export PATH
feliche@feliche-HP:~$ sudo lsof -i -P -n | grep LISTEN
[sudo] password for feliche:
mongod      715    mongodb    8u   IPv4  19374        0t0    TCP 127.0.0.1:27017 (LISTEN)
)
mysqld     990      mysql    25u   IPv4  20992        0t0    TCP 127.0.0.1:3306 (LISTEN)
sshd       996      root     3u   IPv4  24995        0t0    TCP *:22 (LISTEN)
sshd       996      root     4u   IPv6  24997        0t0    TCP *:22 (LISTEN)
osmo-nitb  1365      root     4u   IPv4  23174        0t0    TCP 127.0.0.1:4242 (LISTEN)
osmo-nitb  1365      root     5u   IPv4  23175        0t0    TCP *:3002 (LISTEN)
osmo-nitb  1365      root     6u   IPv4  23176        0t0    TCP *:3003 (LISTEN)
osmo-nitb  1365      root     7u   IPv4  23179        0t0    TCP *:2775 (LISTEN)
osmo-nitb  1365      root     8u   IPv4  23180        0t0    TCP 127.0.0.1:4249 (LISTEN)
apache2    1385      root     4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
dropbox   1932  feliche    94u   IPv4  29919        0t0    TCP *:17500 (LISTEN)
dropbox   1932  feliche    95u   IPv6  29920        0t0    TCP *:17500 (LISTEN)
apache2    3017  www-data    4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
apache2    3019  www-data    4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
apache2    3020  www-data    4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
apache2    3021  www-data    4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
apache2    3022  www-data    4u   IPv6  23272        0t0    TCP *:80 (LISTEN)
cupsd      3036      root    10u   IPv6  38109        0t0    TCP [::1]:631 (LISTEN)
cupsd      3036      root    11u   IPv4  38110        0t0    TCP 127.0.0.1:631 (LISTEN)
feliche@feliche-HP:~$ sudo kill 1365
```

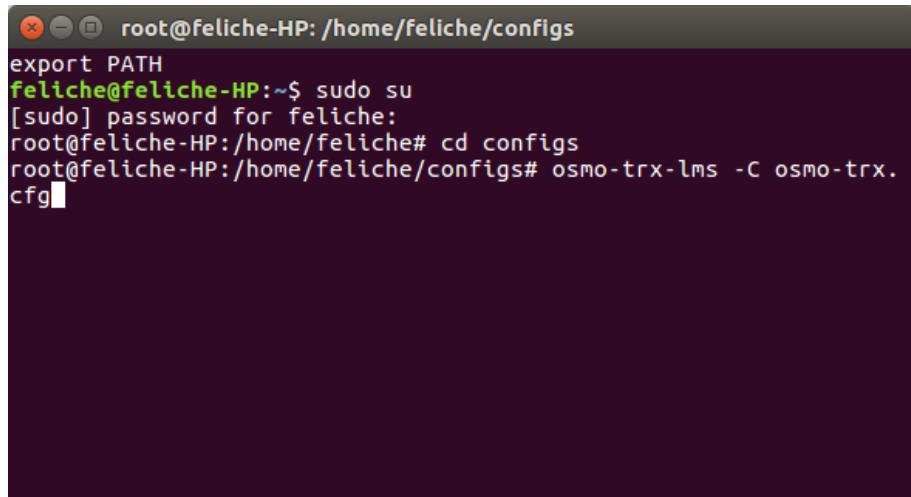
Figura 92 Comando para matar procesos en ejecución.

Para ejecutar el comando es necesario los permisos de administrador, además es necesario el número de proceso que se cerrara.

Cerrando los procesos que tengan el puerto ocupado accedemos a la carpeta donde tenemos los archivos de configuración de OsmoTRX, OsmoNitb y OsmoBTS, para la ejecución de los mismos. Esto es necesario ya que los archivos contienen las configuraciones básicas de la estación base. Si no se ejecutan tales configuraciones, el programa dará un error.

### 5.1.1 Ejecución de Osmo-TRX

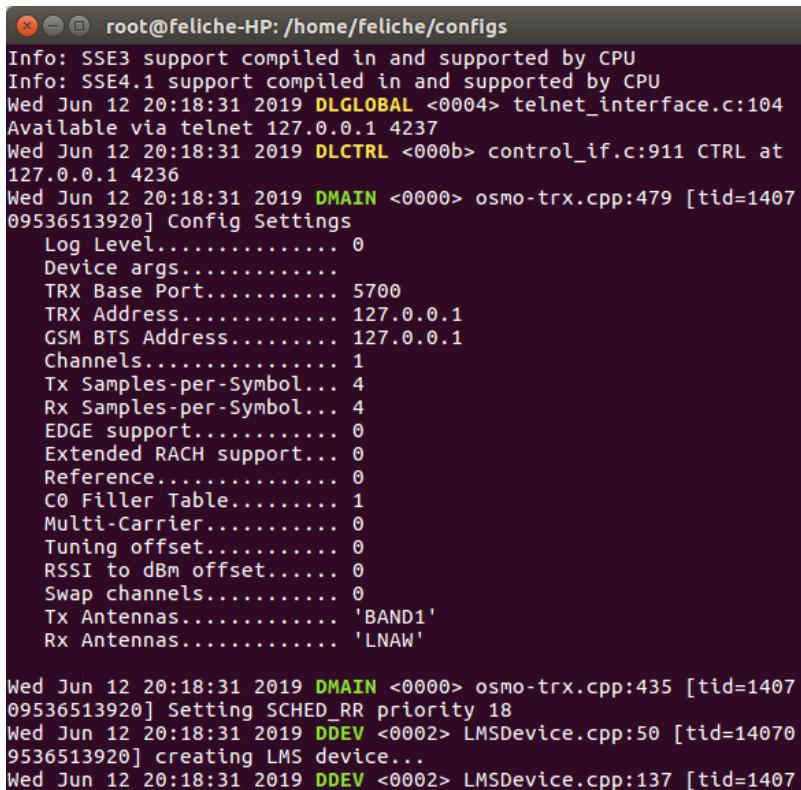
Accediendo a la carpeta de configuración del OsmoTRX, ejecutamos el siguiente comando que se muestra en la figura 93. Para que el comando se ejecute correctamente es necesario tener conectado el dispositivo limeSDR mini.

A screenshot of a terminal window titled "root@feliche-HP: /home/feliche/configs". The terminal shows the following command sequence:

```
root@feliche-HP:~$ sudo su
[sudo] password for feliche:
root@feliche-HP:/home/feliche# cd configs
root@feliche-HP:/home/feliche/configs# osmo-trx-lms -C osmo-trx.cfg
```

Figura 93 Ejecución de osmo-trx.

Cuando se ejecuta el comando, se realizan las configuraciones adecuadas para la transmisión en el limeSDR mini. En la terminal se muestra las configuraciones de la estación (figura 94).

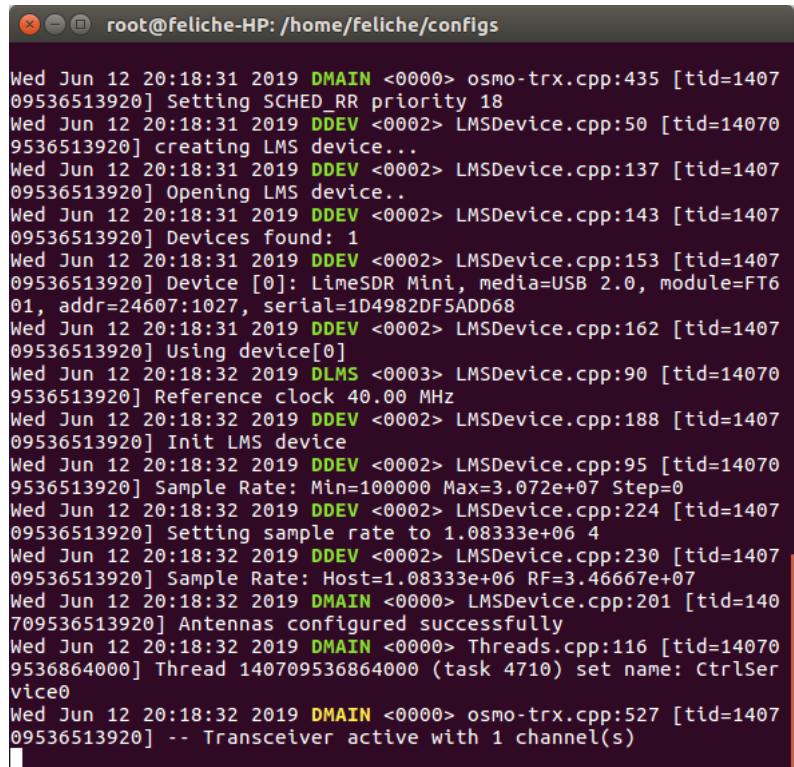
A screenshot of a terminal window titled "root@feliche-HP: /home/feliche/configs". The terminal displays the configuration settings for the limeSDR mini device:

```
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
Wed Jun 12 20:18:31 2019 DLGLOBAL <0004> telnet_interface.c:104
Available via telnet 127.0.0.1 4237
Wed Jun 12 20:18:31 2019 DLCTRL <000b> control_if.c:911 CTRL at
127.0.0.1 4236
Wed Jun 12 20:18:31 2019 DMAIN <0000> osmo-trx.cpp:479 [tid=1407
09536513920] Config Settings
    Log Level..... 0
    Device args.....
    TRX Base Port..... 5700
    TRX Address..... 127.0.0.1
    GSM BTS Address..... 127.0.0.1
    Channels..... 1
    Tx Samples-per-Symbol... 4
    Rx Samples-per-Symbol... 4
    EDGE support..... 0
    Extended RACH support... 0
    Reference..... 0
    C0 Filler Table..... 1
    Multi-Carrier..... 0
    Tuning offset..... 0
    RSSI to dBm offset..... 0
    Swap channels..... 0
    Tx Antennas..... 'BAND1'
    Rx Antennas..... 'LNAW'

Wed Jun 12 20:18:31 2019 DMAIN <0000> osmo-trx.cpp:435 [tid=1407
09536513920] Setting SCHED_RR priority 18
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:50 [tid=14070
9536513920] creating LMS device...
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:137 [tid=1407
```

Figura 94 Información del dispositivo limeSDR mini

Ahora debido a que no se ha ejecutado el Osmo-Nitb el programa se queda en espera. En la figura 95 se puede observar la información del transceiver indicando que está listo para usarse.



```

root@feliche-HP: /home/feliche/configs

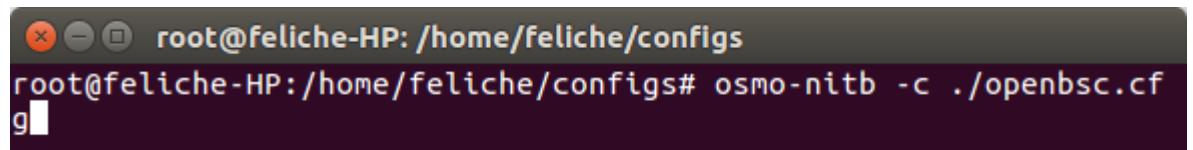
Wed Jun 12 20:18:31 2019 DMAIN <0000> osmo-trx.cpp:435 [tid=1407
09536513920] Setting SCHED_RR priority 18
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:50 [tid=1407
09536513920] creating LMS device...
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:137 [tid=1407
09536513920] Opening LMS device..
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:143 [tid=1407
09536513920] Devices found: 1
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:153 [tid=1407
09536513920] Device [0]: LimeSDR Mini, media=USB 2.0, module=FT6
01, addr=24607:1027, serial=1D4982DF5ADD68
Wed Jun 12 20:18:31 2019 DDEV <0002> LMSDevice.cpp:162 [tid=1407
09536513920] Using device[0]
Wed Jun 12 20:18:32 2019 DLMS <0003> LMSDevice.cpp:90 [tid=1407
09536513920] Reference clock 40.00 MHz
Wed Jun 12 20:18:32 2019 DDEV <0002> LMSDevice.cpp:188 [tid=1407
09536513920] Init LMS device
Wed Jun 12 20:18:32 2019 DDEV <0002> LMSDevice.cpp:95 [tid=1407
09536513920] Sample Rate: Min=100000 Max=3.072e+07 Step=0
Wed Jun 12 20:18:32 2019 DDEV <0002> LMSDevice.cpp:224 [tid=1407
09536513920] Setting sample rate to 1.08333e+06 4
Wed Jun 12 20:18:32 2019 DDEV <0002> LMSDevice.cpp:230 [tid=1407
09536513920] Sample Rate: Host=1.08333e+06 RF=3.46667e+07
Wed Jun 12 20:18:32 2019 DMAIN <0000> LMSDevice.cpp:201 [tid=140
709536513920] Antennas configured successfully
Wed Jun 12 20:18:32 2019 DMAIN <0000> Threads.cpp:116 [tid=1407
09536864000] Thread 140709536864000 (task 4710) set name: CtrlSer
vice0
Wed Jun 12 20:18:32 2019 DMAIN <0000> osmo-trx.cpp:527 [tid=1407
09536513920] -- Transceiver active with 1 channel(s)

```

Figura 95 Información de que el transceiver está activo.

### 5.1.2 Ejecución de OsmoNitb

Considerando que el transceiver está listo, se ejecuta OsmoNitb utilizando el comando de la figura 96.



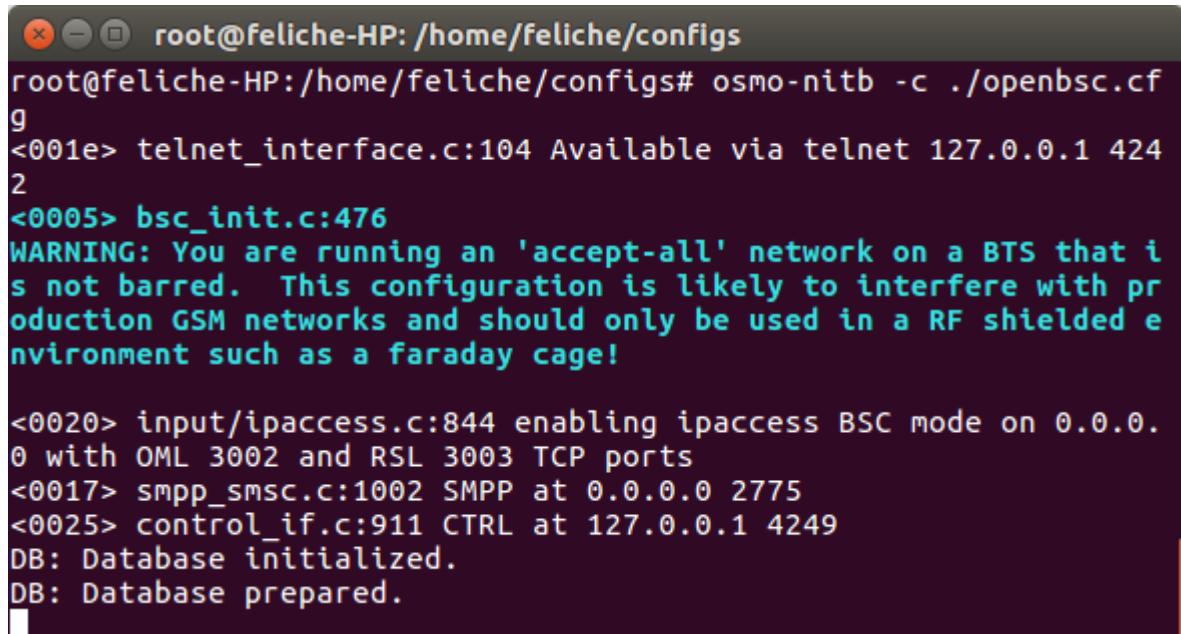
```

root@feliche-HP: /home/feliche/configs
root@feliche-HP:/home/feliche/configs# osmo-nitb -c ./openbsc.cf
g

```

Figura 96 comando para ejecutar OsmoNITB

Cuando se ejecuta este programa lo primero que hace es habilitar los protocolos de comunicación que conectan a la BTS con la BSC, llamados RSL y OML. Además de esto inicializa la base de datos que contiene la información del VLR y HLR. Después de esto se queda esperando que se ejecute OsmoBTS como se muestra en la figura 97.



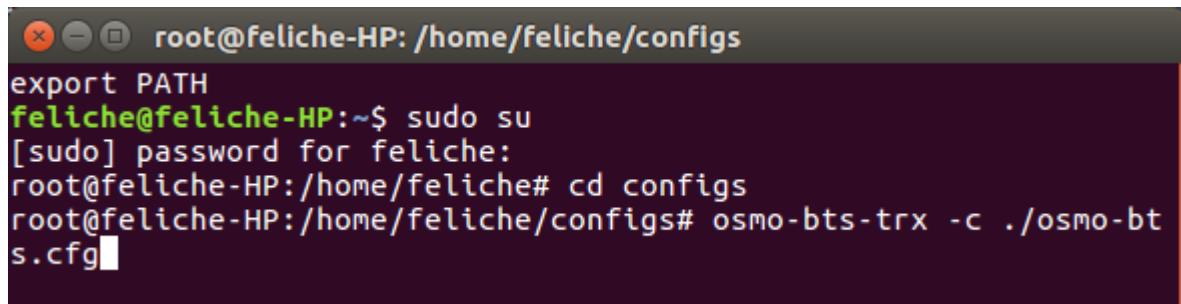
```
root@feliche-HP: /home/feliche/configs
root@feliche-HP:/home/feliche/configs# osmo-nitb -c ./openbsc.cfg
<001e> telnet_interface.c:104 Available via telnet 127.0.0.1 4242
<0005> bsc_init.c:476
WARNING: You are running an 'accept-all' network on a BTS that is not barred. This configuration is likely to interfere with production GSM networks and should only be used in a RF shielded environment such as a faraday cage!

<0020> input/ipaccess.c:844 enabling ipaccess BSC mode on 0.0.0.0 with OML 3002 and RSL 3003 TCP ports
<0017> smpp_smss.c:1002 SMPP at 0.0.0.0 2775
<0025> control_if.c:911 CTRL at 127.0.0.1 4249
DB: Database initialized.
DB: Database prepared.
```

Figura 97 Inicialización de los protocolos de comunicación y la base de datos

### 5.1.3 Ejecución de OsmoBTS.

Ahora se ejecutará OsmoBTS, para completar el sistema y conectar OsmoNitb con OsmoTRX. Para lo cual ejecutaremos el comando de la figura 98.



```
root@feliche-HP: /home/feliche/configs
export PATH
feliche@feliche-HP:~$ sudo su
[sudo] password for feliche:
root@feliche-HP:/home/feliche#
root@feliche-HP:/home/feliche/configs# osmo-bts-trx -c ./osmo-bts.cfg
```

Figura 98 Ejecución de osmoBTS

Como resultado tenemos las tres terminales ejecutando toda la arquitectura de la red celular GSM (figura 99).

```

root@feliche-HP: /home/feliche/configs
<0005> abis_nm.c:507 BTS0 feature 'CBCH' reported via OML does
not match statically set feature: 1 != 0. Please fix.
<0005> abis_nm.c:573 BTS0: ARI reported sw[0/2]: osmobs ts is 1.
0.1
<0005> abis_nm.c:446 BTS0 reported variant: onso-bts-trx
<0005> abis_nm.c:468 BTS0 Attrbute Manufacturer Dependent Sta
te is unreported
<0005> abis_nm.c:573 BTS0: ARI reported sw[0/1]: TRX_PHY_VERSI
ON is Unknown
<0005> abis_nm.c:2757 (bts=0,trx=0) IPA RSL CONNECT IP=0.0.0.0
PORT=3003 STREAM=0x00
<0020> input/lpa.c:262 accept(ed new link from 127.0.0.1 to p
ort 3003
<0004> bsc_init.c:312 bootstrapping RSL for BTS/TRX (0/0) on A
Rfcn 172 using MCC-MNC 284-18 LAC=1 CID=0 BSIC=63

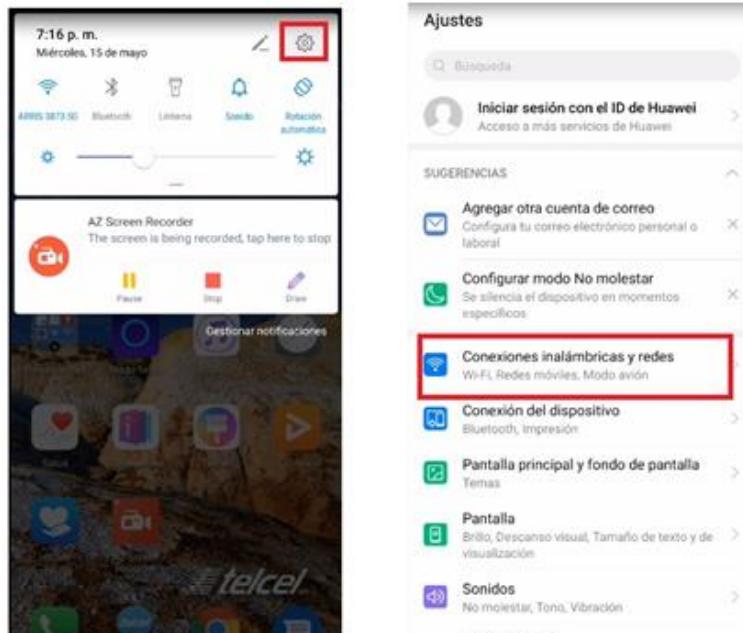
root@feliche-HP: /home/feliche/configs
<0001> onl.c:313 OC=CHANNEL INST=(00,00,06) Tx STATE CHG REP
<0001> onl.c:988 OC=CHANNEL INST=(00,00,07) SET CHAN ATTR (T
S<7 pchan=TCH/F)
<0001> onl.c:313 OC=CHANNEL INST=(00,00,07) Tx STATE CHG REP
<0001> onl.c:348 OC=CHANNEL INST=(00,00,07) AVAL STATE Depe
ndency --> OK
<0001> onl.c:355 OC=CHANNEL INST=(00,00,07) OPER STATE Disab
led --> Enabled
<0001> onl.c:313 OC=CHANNEL INST=(00,00,07) Tx STATE CHG REP
<0001> onl.c:178 No satisfactory response from transceive
r for phy0.0 (CMD POWERON)
<0001> onl.c:178 No satisfactory response from transceive
r for phy0.0 (CMD POWERON)
<000b> trx_if.c:550 Discarding duplicated RSP from old CMD 'R
SP POWERON'
<000b> trx_if.c:550 Discarding duplicated RSP from old CMD 'R
SP POWERON'

```

Figura 99 Terminales ejecutando la arquitectura de una BTS GSM

## 5.2 CONFIGURACIÓN DEL TELÉFONO CELULAR.

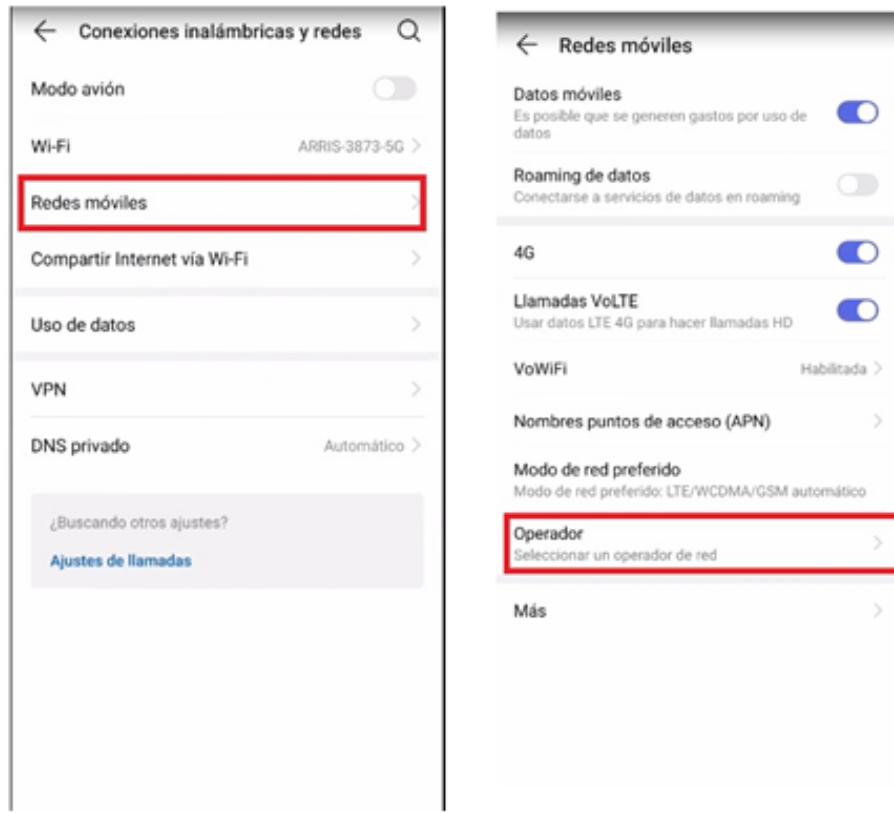
Para conectarse a la estación base GSM, se tiene que acceder a las configuraciones del dispositivo como se muestra en la figura 100 a). Estando en configuraciones accedemos al panel de conexiones inalámbricas y redes como se muestra en la figura 100 b).



a) b)

Figura 100 Acceder a las configuraciones del dispositivo móvil

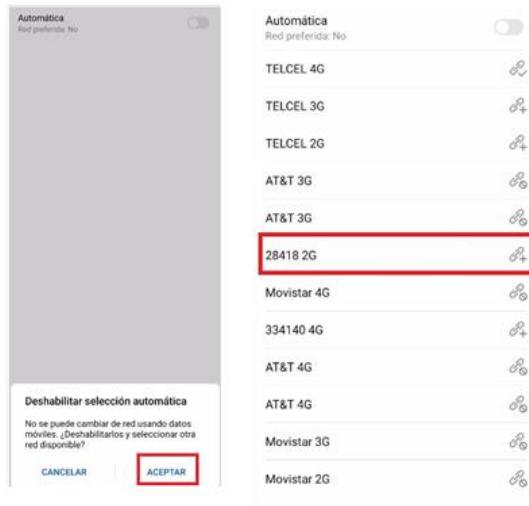
Después accedemos a redes móviles figura 101 a). En redes móviles nos vamos al apartado de operador figura 101 b).



a) b)

Figura 101 Acceder redes móviles.

Ahora deshabilitamos la selección automática, dando la opción de elegir la red deseada figura como se muestra en la figura 102 a). Después de deshabilitar la selección automática empezara a buscar redes disponibles. Entre estas redes aparecerá nuestra estación base GSM, con el nombre 28418 2G figura 102 b), la red se llama así debido a que en el archivo de configuración tenemos el mcc=284 y mnc=18.



a)

b)

Figura 102 Selección de la red.

Ahora ya estamos registrados en la estación base por lo que se podrán hacer llamadas y enviar mensajes de texto entre los usuarios conectados.

### 5.3 PRUEBAS

Para realizar las pruebas se utilizaron dos celulares para realizar llamadas y enviar mensajes de texto.

Ahora para realizar llamadas y enviar mensajes SMS obtenemos el número del celular asignado por el sistema. Para ello marcamos el código en el celular mostrado en la figura 103.

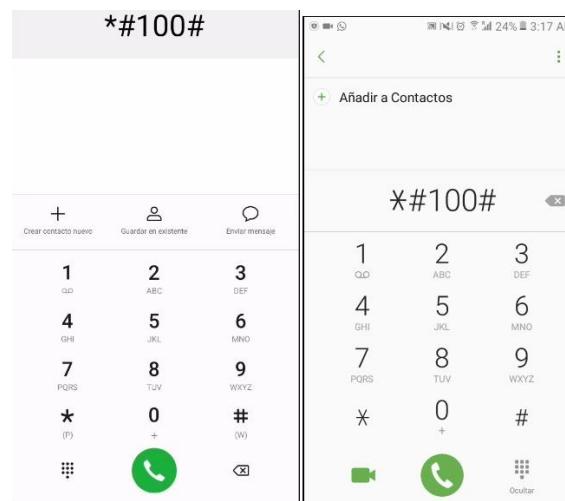


Figura 103 Código para solicitar número de extensión.

Este código nos arroja el número telefónico, mostradas en la figura 104, que se utilizaron para hacer las pruebas.

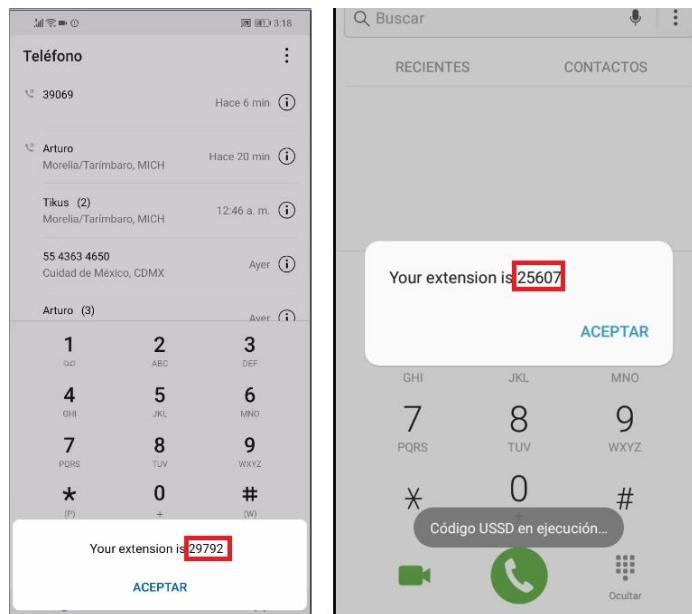


Figura 104 número de extensión solicitado.

### 5.3.1 Llamadas de voz.

Para realizar la llamada de voz solo marcamos al número telefónico que tiene el usuario con el que se requiere comunicarse.

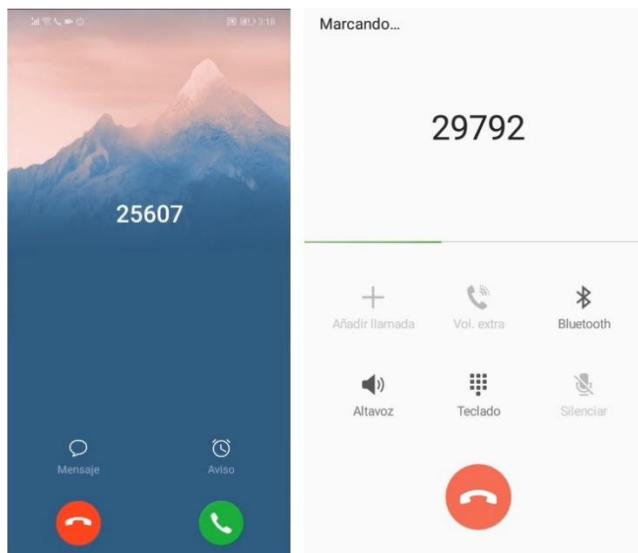


Figura 105 Prueba de una llamada.

En la figura 105 marcamos de una extensión a otra, mostrando cómo se conecta la llamada generando un menú para poder aceptar o rechazar. En la figura 106 se puede observar la aceptación de la llamada.

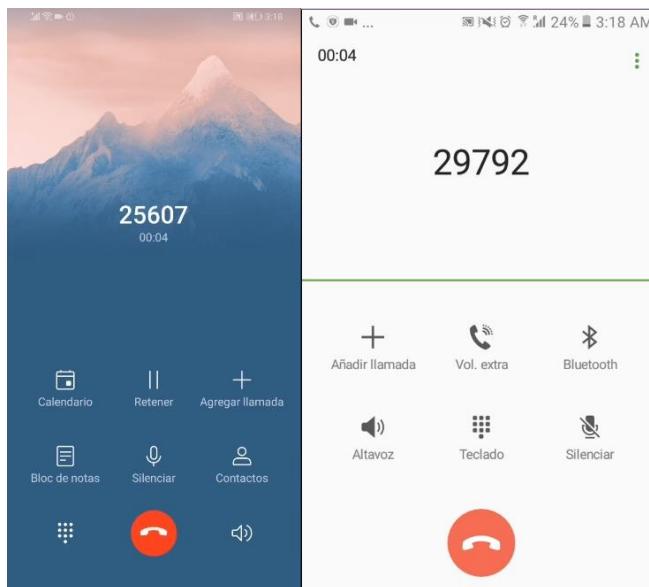


Figura 106 Llamada entre dos extensiones.

### 5.3.2 SMS

Para el envío de mensajes, se escribe el mensaje y se envía a la extensión pertinente. En la imagen 107 se muestra el envío de un mensaje SMS, de un usuario a otro usuario dentro de la estación base.

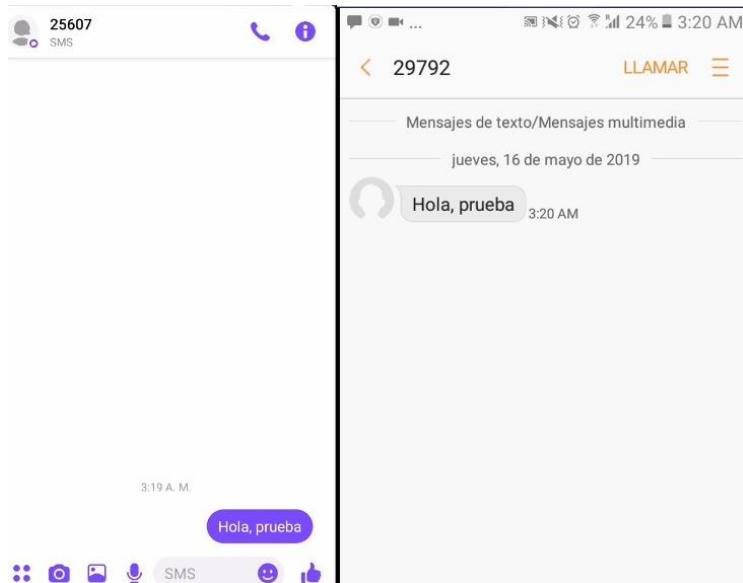


Figura 107 Prueba del envío de un SMS.

### 5.3.3 Base de datos

El sistema OsmoNitb cuenta con el HLR, VLR, AUC y el SMS que se encargan de guardar los datos de la red celular, desde los usuarios conectados hasta los mensajes enviados. Estos datos se guardan en una base de datos relacional, que se encuentra ubicada en la dirección de los archivos de configuración. En la figura 108 se muestra la base de datos mencionada.

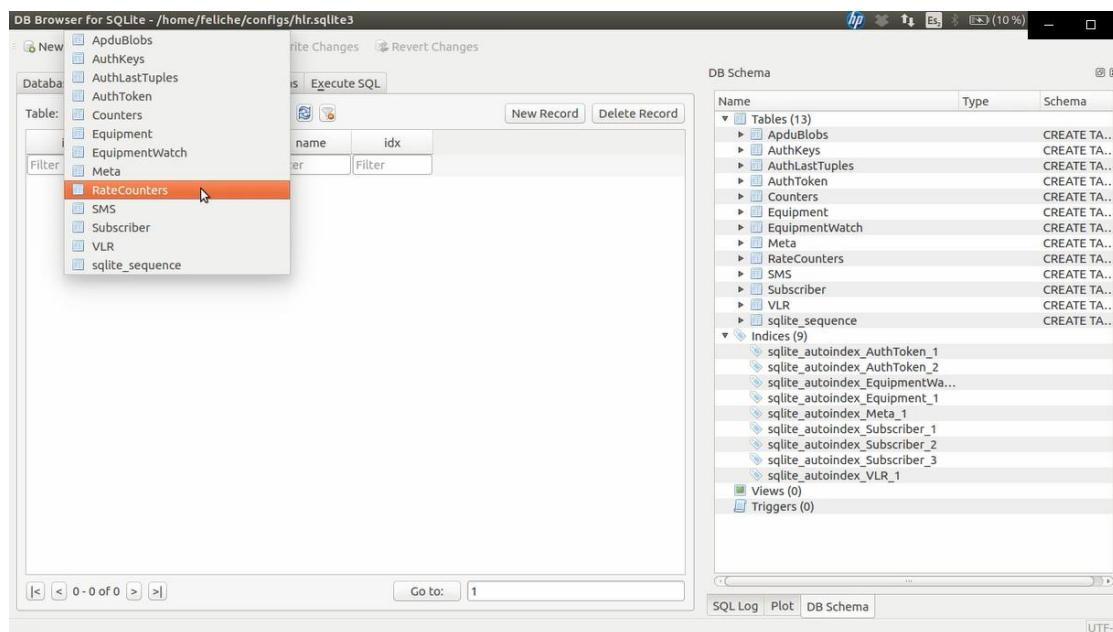


Figura 108 Base de datos

En la figura 109 se muestran las tablas que contiene la base de datos.

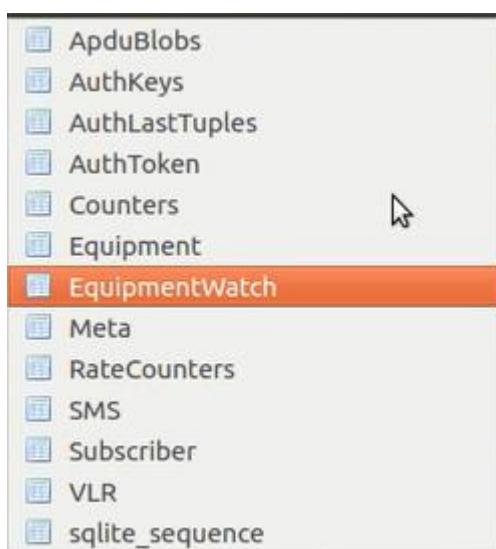


Figura 109 Menú de las tablas en la base de datos.

En la figura 110 podemos ver el contador de llamadas que nos muestra el número de llamada por orden cronológico, así como la fecha y hora en que se realizaron estas llamadas.

	id	timestamp	value	name
	Filter	Filter	Filter	Filter
1	1	2019-05-08...	0	msc.active_...
2	2	2019-05-08...	0	msc.active_...
3	3	2019-05-08...	0	msc.active_...
4	4	2019-05-08...	0	msc.active_...
5	5	2019-05-08...	0	msc.active_...
6	6	2019-05-08...	0	msc.active_...
7	7	2019-05-08...	0	msc.active_...
8	8	2019-05-08...	0	msc.active_...
9	9	2019-05-08...	0	msc.active_...
10	10	2019-05-08...	0	msc.active_...
11	11	2019-05-08...	0	msc.active_...
12	12	2019-05-08...	0	msc.active_...
13	13	2019-05-08...	0	msc.active_...
14	14	2019-05-08...	0	msc.active_...
15	15	2019-05-08...	0	msc.active_...
16	16	2019-05-08...	0	msc.active_...

|< < 1 - 17 of 604 > >| Go to: 1

Figura 110 Contador de llamadas.

En la figura 111 se muestran los equipos que se conectaron a la red, guardando la información de la hora en que se conectaron y desconectaron. También guarda el IMEI del equipo para futuras referencias.

	id	created	updated	name	classmark1	classmark2	classmark3	imei
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	2019-05-08 05:48:07	2019-05-22 18:24:05	NULL	51	✓ZW		145370048...
2	2	2019-05-08 05:49:55	2019-05-16 00:41:47	NULL	51	✓ZW		862945035...
3	3	2019-05-09 16:42:37	2019-05-09 16:52:56	NULL	51	✓ZW		351857085...
4	7	2019-05-09 18:22:39	2019-05-22 18:18:19	NULL	0	✓ZW		865181038...
5	9	2019-05-16 00:00:29	2019-05-16 00:21:33	NULL	51	✓ZW		354809097...
6	12	2019-05-16 00:10:16	2019-05-16 00:21:30	NULL	51	✓ZW		869591031...
7	17	2019-05-22 18:14:53	2019-06-13 18:51:32	NULL	0	✓ZW		146740031...
8	18	2019-05-22 18:15:44	2019-06-13 18:12:44	NULL	0	✓ZW		867970030...
9	19	2019-05-22 18:16:18	2019-05-22 18:16:18	NULL	0			353064095...
10	20	2019-05-22 18:16:20	2019-05-22 18:31:30	NULL	51	✓ZW		353554089...
11	24	2019-05-22 18:23:00	2019-05-22 18:25:15	NULL	0	✓ZW		355797071...
12	26	2019-05-22 18:27:39	2019-05-22 18:27:39	NULL	0			865181038...
13	28	2019-06-11 14:22:54	2019-06-13 19:21:33	NULL	51	✓ZW		990004421...
14	30	2019-06-13 17:00:24	2019-06-13 17:02:22	NULL	0	✓ZW		359667075...
15	31	2019-06-13 17:33:55	2019-06-13 17:43:28	NULL	0	✓X		354464102...
16	32	2019-06-13 17:37:34	2019-06-13 17:47:18	NULL	0	✓ZW		865363028...

|< < 1 - 17 of 20 > >| Go to: 1

Figura 111 Tabla de equipos que se conectaron.

En la figura 112 y 113 se muestra la tabla que guarda la información sobre los SMS. Esta tabla guarda datos como la extensión de origen, la extensión destino, la fecha y hora que se envió el mensaje. Además, guarda el mensaje de texto enviado.

Table: SMS													<a href="#">New Record</a>	<a href="#">Delete Record</a>
id	created	sent	silver_attemp	valid_until	eply_path_req	status_rep_req	is_report	msg_ref	protocol_id	a_coding_sche	ud_hdr_ind	src_addr		
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1 1	2019-05-08...	2019-05-08...	1	3009500129	0	0	0	25	0	0	0	39069		
2 2	2019-05-09...	2019-05-09...	1	3209843681	0	0	0	116	0	0	0	44501		
3 3	2019-05-09...	2019-05-09...	1	3209843681	0	0	0	117	0	0	0	44501		
4 4	2019-05-13...	2019-05-13...	1	3556971489	0	0	0	0	0	0	0	44199		
5 5	2019-05-13...	2019-05-13...	1	3556971489	0	0	0	0	0	0	0	44199		
6 6	2019-05-16...	2019-05-16...	3	1416352737	0	0	0	7	0	0	0	29792		
7 7	2019-05-16...	2019-05-16...	1	1416352737	0	0	0	94	0	0	0	25607		
8 8	2019-05-16...	2019-05-16...	1	1416352737	0	0	0	95	0	0	0	25607		
9 9	2019-05-16...	2019-05-16...	3	1416352737	0	0	0	8	0	8	0	29792		
10 10	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	20	0	0	0	39891		
11 11	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	74	0	0	0	29600		
12 12	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	75	0	8	0	29600		
13 13	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	76	0	0	0	29600		
14 14	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	21	0	0	0	39891		
15 15	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	7	0	0	0	25166		
16 16	2019-05-22...	2019-05-22...	1	3876930529	0	0	0	77	0	0	0	29600		

Figura 112 Tabla sobre el servicio de SMS 1

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: SMS

New Record | Delete Record

msg_ref	protocol_id	a_coding_sche	ud_hdr_ind	src_addr	src_ton	src_npi	dest_addr	dest_ton	dest_npi	user_data	header	text
1	25	0	0	39069	0	0	44501	0	1	NULL		Hola
2	116	0	0	44501	0	0	47967	0	1	NULL		Prueba de ..
3	117	0	0	44501	0	0	47967	0	1	NULL		Funciona
4	0	0	0	44199	0	0	4251049271	0	0	NULL		Hela
5	0	0	0	44199	0	0	4251049271	0	0	NULL		Funciona
6	7	0	0	29792	0	0	25607	0	1	NULL		Hola, prueba
7	94	0	0	25607	0	0	29792	0	1	NULL		Funciona
8	95	0	0	25607	0	0	29792	0	1	NULL		????
9	8	8	0	29792	0	0	25607	0	1	NULL		
10	20	0	0	39891	0	0	29600	0	1	NULL		
11	74	0	0	29600	0	0	39891	0	1	NULL		Hola
12	75	0	8	29600	0	0	39891	0	1	NULL		
13	76	0	0	29600	0	0	39891	0	1	NULL		:)
14	21	0	0	39891	0	0	29600	0	1	NULL		
15	7	0	0	25166	0	0	29600	0	1	NULL		:)
16	77	0	0	29600	0	0	25166	0	1	NULL		Hello

Figura 113 Tabla sobre el servicio de SMS 2

En la figura 114 se muestra un resumen general de los datos almacenados en la base de datos.

Database Structure		Browse Data
Table: <a href="#">sqlite_sequence</a>		
	name	seq
1	Meta	15
2	Counters	604
3	Subscriber	21
4	Equipment	44
5	Equipment...	44
6	SMS	26

Figura 114 Resumen de los datos de la base de datos

## CAPÍTULO 6 CONCLUSIONES Y TRABAJOS FUTUROS

El objetivo fundamental de esta tesis es dar a conocer el funcionamiento de la telefonía celular, clave para la comunicación entre las personas en la actualidad. Explicando los diferentes conceptos necesarios en la instalación de una estación base de segunda generación GSM.

Así pues, la aportación principal de esta tesis consiste en la instalación de una estación base GSM utilizando OsmoNitb, OsmoTRX y OsmoBTS aplicaciones de OSMOCOM. Además, se aborda el tema de los dispositivos SDR al utilizar limeSDR fabricado por la empresa Microsystems

La instalación de una estación base implica tener conocimientos sólidos en el área de comunicaciones para entender los distintos protocolos utilizados en la arquitectura del estándar analizado. OSMOCOM da acceso a sus aplicaciones tomando por hecho que el usuario que las utilizará tiene los conocimientos necesarios para hacer las configuraciones pertinentes y hacer funcionar una estación base. OsmoNitb es la aplicación que se encarga de emular la arquitectura del estándar de telefonía GSM. Esta aplicación contiene el BSC, MSC, SMSC, EIR, AUC, HLR y el VLR incluyendo las conexiones y protocolos para la comunicación entre estos módulos. OsmoBTS y OsmoTRX se encargan de la capa física de una BTS completando así la arquitectura del estándar de telefonía GSM. Para la comunicación entre el software y el dispositivo SDR se utiliza limesuite aplicación proporcionada por Microsystems. Otro aspecto necesario es tener la suficiente experiencia en Linux para realizar la instalación de las aplicaciones de OSMOCOM y Microsystems.

Para observar la funcionalidad de la estación base se hicieron pruebas con distintos dispositivos para hacer conclusiones sobre la fiabilidad del sistema. Se hizo la conexión de 9 dispositivos conectados simultáneamente a la estación base generando lentitud al conectar llamadas esto debido al hardware utilizado. Se utilizó una PC portátil de gama baja lo que provocó mucha latencia al hacer y recibir llamadas y mensajes de texto. Otro punto importante es que la PC portátil no contaba con un puerto USB 3.0 necesario para el envío de grandes cantidades de datos a altas velocidades hacia el dispositivo SDR. Con esto concluimos que el sistema requiere de un mejor hardware es decir, una PC portátil capaz de soportar los procesos necesarios para atender las peticiones hechas por los usuarios hacia la estación base.

Si se requiere hacer una estación base GSM para conectar una gran cantidad de usuarios y tener una cobertura de mayor distancia es necesario utilizar OsmoBSC aplicación de OSMOCOM que separa los distintos componentes de la arquitectura del estándar GSM generando la posibilidad de utilizar varios PCs portátiles para repartir el procesamiento de datos generando mayor calidad y en este caso

proporcionar acceso a muchos usuarios. Para el caso de obtener una mayor cobertura es necesario adquirir un amplificador de señal RF seleccionado para que cumple con las características necesarias.

### **Trabajos Futuros.**

Para trabajos futuros se desea implementar la misma red celular 2G GSM en varios PCs, utilizando varios dispositivos SDR para ver el comportamiento que tiene la red celular ya con varias zonas de cobertura implementadas. Para lo cual se optaría por utilizar otras plataformas de OSMOCOM para la implementación de la arquitectura GSM en varios equipos, dando la posibilidad de que no exista la saturación de usuarios, además de dar la ventaja de ver el verdadero comportamiento de la red celular GSM, observando conceptos como el handover, VLR, entre otras.

Se planea implementar una red celular 4G LTE utilizando OAI eNB para emular las funcionalidades de eNodeB, OpenAirInterface (OAI) para el núcleo de red EPC de LTE y limeSDR como dispositivo de recepción y transmisión de las señales de radio. Para instalar dichas aplicaciones se requiere un equipo de gama media para poder hacer todos los procesos necesarios por la red ya que el estándar 4G LTE demanda más procesamiento de datos. Algo muy importante es tener tarjetas USIM para la autorización de los usuarios conectados a la red, debido a que las tarjetas SIM convencionales, otorgadas por una compañía de telefonía como las utilizadas en la red GSM, no funcionarían debido a que no nos proporcionan los datos generales de la tarjeta SIM, uno de estos datos importantes es el código ki que es esencial para autorizar un usuario en la base de datos. Por esta razón se piensa usar una tarjeta SIM programable y el dispositivo programador que se pueden adquirir en la empresa Sysmocom.

## GLOSARIO DE TÉRMINOS

2G Segunda Generación.

64QAM Tipo de modulación QAM con 64 saltos en cuadratura.

ACCH (Associated Control Channel). Canal de control asociado en el sistema GSM. Canal de control utilizado siempre en conjunción con un canal dedicado.

ADC (Digital Analog Converter). Convertidor analógico digital.

AGCH (Access Grant Channel). Canal de acceso. Canal de control común en el sistema GSM, transmitido en el sentido base-móvil y utilizado para la asignación de recursos al móvil que previamente solicitó el establecimiento de la comunicación y tras el proceso de autenticación.

AM (Amplitud Modulada). Tipo de modulación que varía la amplitud de acuerdo a los datos enviados.

AMPS (Advanced Mobile Phone System). Corresponde al servicio de Telefonía móvil en EEUU. ANCHO DE BANDA Capacidad de transmisión de un sistema de comunicación. Se mide en bits por segundo ó mediante sus múltiplos (Kbps, Mbps, etc).

ARFCN (absolute radio-frequency channel number) es un código que especifica un par de portadores de radio físicos utilizados para la transmisión y recepción en un sistema de radio móvil terrestre, uno para la señal de enlace ascendente y otro para la señal de enlace descendente

ASK (Amplitude Shift Keying) Tipo de modulación con portadora analógica, pero datos de transporte digitales.

AT&T (American Telephone and Telegrafos) Empresa dedicada a la telefonía.

AUC (Authentication Center). Elemento que contiene las claves y algoritmos de verificación para el acceso de un usuario a una red de telefonía celular.

BCCH (Broadcasting Control Channel). Canal de control de difusión. Canal de control común en el sistema GSM. Se transmite en el sentido base-móvil. Está permanentemente en el aire para permitir la transferencia de parámetros del sistema e información general de la red, la célula actual y las adyacentes, así como para el envío de ráfagas de sincronización. Permite a la estación móvil orientarse en el entorno del sistema.

BLUETOOTH: es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) creado por Bluetooth Special Interest Group.

BS (Base Station). Estación base.

BSC (Base Station Controller). Controlador de estaciones base.

BSS (Base Station Subsystem). Subsistema de estaciones base.

BSSAP (Base Station System Application Part) es un protocolo específico de GSM diseñado para señalizar a través de la interfaz.

BTS (Base Trasceiver Station). Trasceptor de estación base.

BURST (Ráfaga) Paquete de datos enviado por un canal.

DAC (Digital Analog Converter) dispositivo que se encarga de convertir señales digitales a analógicas.

CCCH (Common Control Channels). Canales de control común en el sistema GSM. Sirven para regular el acceso de los terminales al sistema y utilizan un par de portadoras.

CDMA (Code Division Multiplex Acces) Acceso múltiple por división de código.

C-NETZ (Radio Telephone Network C) fue un sistema de telefonía celular analógico de primera generación implementado y operado en Alemania.

CRC (Cyclic Redundancy Check). Código redundante cíclico. Código protector de errores utilizado en sistemas celulares.

DCCH (Dedicated Control Channels). Canales de control dedicados en el sistema GSM. Permiten funciones específicas y se asocian a cada comunicación. Utilizan un par de portadoras.

DCS (Digital Cellular System). Sistema de telefonía celular digital de Y generación similar al sistema GSM, pero que opera en la banda de 1800MHz.

DL (DOWNLINK) Se refiere a la transferencia de datos de descarga.

DSP (Procesador Digital de Señales) es un sistema basado en un procesador o microprocesador que posee un conjunto de instrucciones.

EIR (Equipment Identity Register). Registro de identidad de equipo. Base de datos que guarda información relativa al equipo móvil.

ES (Espread Spectrum) Espectro extendido.

FACCH (Fast Associated Control Channel). Canal lógico de control utilizado en el sistema digital IS-54 y en el sistema GSM. Se usa para transmitir órdenes urgentes como una orden de handover.

FCC (Federal Communications Commission) Comisión federal de Comunicaciones. Organismo encargado de reglamentar las comunicaciones de manera internacional.

FCCH (Frequency Correction Channel). Canal asociado al canal de tráfico en el sistema GSM transmitido desde la red hasta el móvil. Por él se envía la información de corrección de frecuencia para sincronización de la portadora en el móvil.

FDD (Frequency Duplexion Division). Técnica de separación en frecuencia entre la transmisión en sentido base-móvil y móvil-base.

FDMA (Frequency Division Multiplex Access). Técnica de multiplexación de canales radioeléctricos por división en frecuencia, utilizada en los sistemas analógicos de primera generación.

FH (Frequency Hopping). Salto de frecuencia. Se utiliza en GSM. Posibilidad de que los móviles puedan realizar la transmisión en la modalidad de saltos de frecuencia, bajo mandato de la red, para lograr una mayor protección gracias a la diversidad de frecuencia.

FM (Frequency Modulation). Modulación analógica de frecuencia, utilizada en los sistemas celulares analógicos.

FPGA (Field Programmable Gate Array) es un dispositivo que contiene bloques de lógica cuya interconexión y funcionalidad puede ser configurada en el momento.

FPLMTS (Future Public Land Mobile Telecommunications Systems) Anterior denominación del futuro sistema de telefonía móvil de tercera generación, propuesto por la ITU.

FSK (Frequency Shift Keying). Modulación de frecuencia digital utilizada en la transmisión de información de control en el estándar TACS.

GMSK (Gaussian Minimum Shift Keying). Modulación digital de frecuencia con filtro gaussiano de premodulación, utilizada en el sistema celular GSM.

GOS (Grade of Service). Grado de servicio. En sistemas con espera es la probabilidad de que una llamada arbitraria tenga una espera superior a un tiempo especificado en segundos.

GSM (Groupe Special Mobile o Global System for Mobile Communications). Sistema de telefonía celular digital de segunda generación estandarizado en Europa, pero cuyo uso se ha extendido a otras zonas del planeta.

HANDOVER Procedimiento a través del cual se cambian los canales de transmisión de radio a medida que una unidad móvil se mueve del área de cobertura de una célula a otra.

HLR (Home Location Register). Base de datos local que contiene información de todos los abonados móviles, relativa a su suscripción y servicios suplementarios.

HSCSD (High-Speed Circuit-Switched Data) es una mejora al mecanismo de transmisión de datos de GSM o circuit-switched data (CSD).

IDLE es la inactividad de un usuario en IRC.

IMEI (International Mobile Equipment Identity). Identidad del equipo móvil internacional.

IMSI (International Mobile Subscriber Identity). Identidad de abonado móvil internacional. Se incorpora en el módulo de identidad de abonado (SIM) cuando un abonado utiliza un terminal.

IMTS (Improved MovileTelephone System) Sistema de telefonía móvil mejorado. sistema de comunicación móvil analógico que fue implementado en los años 60.

IOT (Internet of Things) Tipo de tecnología utilizada para automatizar dispositivos.

ISDN (Integrated Services Digital Network). Red digital de servicios integrados.

ISUP es un protocolo de circuitos conmutados, usado para configurar, manejar y gestionar llamadas de voz y datos sobre PSTN.

ITU (International Telecommunications Union). Unión Internacional de Telecomunicaciones.

KBPS (Kilo bytes por Segundo).

LAPD (Link Access Procedure on D Chanel) es un protocolo de capa de enlace de datos utilizado en redes celulares GSM.

LoRa es el tipo de modulación en radiofrecuencia patentado por Semtech

LTE (Long Term Evolution) Estándar de comunicaciones móviles implementado por 3GPP que marca la cuarta generación de telefonía celular.

MAP (Mobile Application Part). Formato que define los métodos y mecanismos de comunicación en las redes sin hilos.

MIN (Mobile Identification Number). Registro que contiene el número telefónico codificado en binario.

MS (Mobile Station). Estación móvil.

MSC (Mobile Switching Center). Centro de Conmutación de Móviles. Su función principal es la de conmutación y encaminamiento de llamadas.

MTP (Media Transfer Protocol) Su propósito principal es la transferencia de archivos informáticos multimedia y sus metadatos a/desde dispositivos, con la posibilidad de controlar remotamente el dispositivo, leyendo o estableciendo algunos de sus parámetro.

NAMPS (Narrowband Advanced Mobile Phone System). Variación del estándar celular analógico AMPS con canalización estrecha a 10KHz.

NES (Non Espread Spectrum) Espectro no extendido.

NMT (Nordic Mobile Telephone). Sistema celular analógico de primera generación surgido en los países nórdicos.

NTT (Nippon Telegraph and Telephone) es una empresa de telecomunicaciones líder en el mercado nipón.

OFDM (orthogonal frequency division multiplexing) es una técnica de transmisión que consiste en la multiplexación de un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

OMS (Operation & Maintenance System). Sistema de operaciones y mantenimiento.

OPENBTS es un proyecto de software de código abierto dedicado a revolucionar las redes móviles mediante la sustitución de protocolos de telecomunicaciones antiguos y sistemas de hardware patentados tradicionalmente complejos con Protocolo de Internet y una arquitectura de software flexible.

OSI (Open Systems Interconnect) es un modelo de referencia para los protocolos de la red.

PAGING Término utilizado para denominar a los sistemas de radiolocalización.

PAM (Pulse Amplitude Modulation) Modulacion por amplitud de pulsos.

PCH (Paging Channel). Canal de búsqueda. Canal de control común en el sistema

PCS es una norma GSM adaptada a las frecuencias disponibles en el Continente Americano.

GSM. Se transmite desde la base hasta el móvil e informa a la estación móvil de una llamada destinada a la misma.

PIN (Personal Identification Number). Número de identificación personal.

PM (Phase Modulation). La modulación por cambio de fase cambia el angulo de la señal dependiendo de los datos de entrada.

PSK (Phase Shift Keying). Modulación de phase digital.

PSTN (Public Switched Telephonic Network). Red telefónica pública conmutada.

PWM (Pulse Width Modulation) Modulación por ancho de pulsos

QAM (Modulacion en cuadratura). Es un tipo de modulación de cambio de fase y de amplitud.

QPSK (Quadrature Phase Shift Keying). Modulación digital de fase en cuadratura, utilizada en los sistemas americanos IS-54, IS-95 y japoneses PDC.

RACH (Random Access Channel). Canal de acceso aleatorio. Canal de control común en el sistema GSM. Transmite en el sentido móvil-base las peticiones de la

estación móvil no programadas de antemano en el sistema, por ejemplo, para el registro o establecimiento de la llamada.

RCC (Radio Common Carriers) Operadores de Radiocomunicación. Empresa de los 50 de telefonía.

RDS (Radio Data System). Sistema para el envío de datos a través de la interfaz radio.

RECC (Reward Control Channel). Canal de control en el sentido móvil-base en el estándar británico TACS.

RELP (Residual Term Excited Long Term Prediction). Técnica de compresión LPC utilizada en el sistema celular digital GSM, en la que se codifica la señal error de predicción mediante técnicas vectoriales. ROAMING Inicio de servicios en un área diferente de aquella a la cual el usuario ha sido asignado.

RF (Radio Frecuencia)

RFID (Radio Frequency Identification) Identificación por radiofrecuencia.

RSS (Received Signal Strength). Nivel de potencia recibida en un canal.

RTMI (Radio Telefono Mobile Integrato) fue el primer servicio de comunicación móvil en Italia

RTMS (Radio Telefono Mobile di Seconda generazione) era un estándar de red de telefonía móvil que funcionaba en la frecuencia de 450 MHz.

RXLEV Se refiere a la señal recibida por el teléfono móvil desde el área de cobertura.

RXQUAL Se refiere a el error de la tasa de bits.

SACCH (Slow Associated Control Channel). Canal de control asociado lento. Se utiliza en los sistemas TDMA IS-54 y GSM fundamentalmente para transmitir información recurrente, como ajuste de potencia o de trama, medidas de calidad del canal, información de tarificación.

SAT (Signal Audio Tone). Se trata de un tono modulado en frecuencia transmitido en el canal vocal de los sistemas analógicos TACS que sirve para controlar la continuidad del enlace base-móvil y móvil-base.

SCH (Synchronization Channel). Canal de sincronización asociado al canal de tráfico en el sistema GSM. Su sentido es desde la red al terminal móvil. Cursa la información de sincronización de trama e identificación de la estación base.

SCCP (Skinny Call Control Protocol) es un protocolo propietario de control de terminal desarrollado originariamente por Selsius Corporation.

SCT (Secretaría de Comunicaciones y Transportes) Organismo Mexicano encargado de las telecomunicaciones

SDR (Software Defined Radio) Radio definido por software.

SID (System Identification). Identificación digital del operador celular.

SIM (Subscriber Identity Module). Módulo de identificación de usuario. Tarjeta que se inserta en el terminal móvil y se asocia a un abono celular. SMS Servicio de mensajes cortos.

SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre teléfonos móviles.

SS7 (sistema de señalización por canal común n.º 7) es un conjunto de protocolos de señalización telefónica empleado en la mayor parte de redes telefónicas mundiales.

ST (Total Access Communication System). Sistema celular analógico de primera generación estandarizado en el Reino Unido, versión modificada del estándar americano AMPS adaptado a la canalización europea.

TACS (Total Acces Communications System) Sistema de comunicación de acceso total.

TCAP (Transaction Capabilities Application Part) es un protocolo para redes del Sistema de Señalización 7.

TCH (Traffic Channel). Canal lógico de tráfico en el sistema GSM.

TDMA (Time Division Multiplex Access). Técnica de multiplexación de canales radioeléctricos por división en tiempo, utilizada en algunos sistemas digitales de segunda generación.

TIA (Telecommunication Industry Association). Asociación de Industrias de Telecommunicación norteamericana. 112 TRÁFICO Volumen de la demanda en un sistema de telecomunicaciones.

TMSI (Temporary Mobile Subscriber Identity) Identidad Temporal del Subscriptor Móvil.

UL (Uplink) Se refiere a la transferencia de datos de subida.

UMTS (Universal Mobile Telecommunications System). Sistema universal de Comunicaciones móviles.

VLR (Visitor Location Register). Base de datos que utiliza una NISC para todos los abonados que en un momento dado están en su área de servicio.

VSELP (Vector Sum Excited Long Prediction). Técnica de compresión LPC.

WAP (Wireless Application Protocol). Protocolo basado en los estándares de Internet que ha sido desarrollado para permitir a teléfonos celulares navegar a través de Internet.

WARC (World Administrative Radio Conference) Conferencia mundial donde se definen las normas de uso del espectro radioeléctrico.

WCDMA (Wideband Code Division Multiple Access) es la tecnología de acceso móvil en la que se basan varios estándares de telefonía móvil de tercera generación.

ZIGBEE: conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal

## BIBLIOGRAFÍA

- [1] L. Mycosystems, «CROWD SUPPLY,» [En línea]. Available: <https://www.crowdsupply.com/lime-micro/limesdr>. [Último acceso: 07 Marzo 2019].
- [2] Instituto Tecnológico de Buenos Aires, «tesuva.edu.co,» [En línea]. Available: <https://tesuva.edu.co/phocadownloadpap/Fundamentos%20de%20telecomunicacion.pdf>. [Último acceso: 24 Mayo 2019].
- [3] Escuela de Educación Técnica Profesional N° 460 “Guillermo Lehmann”, «eet460rafaela.edu.ar,» [En línea]. Available: <https://www.eet460rafaela.edu.ar/descargar/apunte/1203+&cd=2&hl=es-419&ct=clnk&gl=mx>. [Último acceso: 24 Mayo 2019].
- [4] F. T. R. Francesc Rey Micolau, «<http://openaccess.uoc.edu>,» [En línea]. Available: [http://openaccess.uoc.edu/webapps/o2/bitstream/10609/69406/5/Sistemas%20de%20comunicaci%C3%B3n\\_M%C3%B3dulo%202\\_Comunicaciones%20anal%C3%B3gicas%3B%20modulaciones%20AM%20y%20FM.pdf](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/69406/5/Sistemas%20de%20comunicaci%C3%B3n_M%C3%B3dulo%202_Comunicaciones%20anal%C3%B3gicas%3B%20modulaciones%20AM%20y%20FM.pdf). [Último acceso: 24 Mayo 2019].
- [5] «Telecomunicaciones electronicas,» [En línea]. Available: <https://sites.google.com/site/telecomunicacionesmegatec/home/modulacion-demodulacion>. [Último acceso: 24 Mayo 2019].
- [6] R. R. Carlos, Introducción a la telefonía celular, D.F., 2007.
- [7] C. Trilnick, «IDIS,» 2006. [En línea]. Available: <https://proyectoidis.org/antonio-meucci-teletrofono/>. [Último acceso: 27 02 2019].
- [8] J. F. Basterretche, Dispositivos Moviles, Argentina, 2007.
- [9] Anonimo, «timetoast,» [En línea]. Available: <https://www.timetoast.com/timelines/historia-de-la-comunicacion--46>. [Último acceso: 28 02 2019].
- [10] J. C. L. Tapia, Conceptos básicos de telefonía celular, Pachuca, 2006.
- [11] M. D. Favela, «La llegada del teléfono celular a México,» 17 Febrero 2017. [En línea]. Available: <http://vinculacion.dgire.unam.mx/vinculacion->

- 1/Memoria-Congreso-2017/trabajos-humanidades-y-arte/historia-de-mexico/3.pdf. [Último acceso: 26 04 2019].
- [12] N. A. Pérez García, Á. D. Pinto Mangones, J. M. Torres Tovio y T. P. Pérez Di Santis, Planificación y dimensionamiento de sistemas celulares y de radio acceso, 2017.
- [13] «<http://bibing.us.es/>,» [En línea]. Available: <http://bibing.us.es/proyectos/abreproj/11980/fichero/CAP%C3%8DTULO+2+-+LA+EVOLUCI%C3%93N+DE+LA+TELEFON%C3%88DA+M%C3%939VI L%252F2.2+La+evoluci%C3%B3n+de+las+redes+de+telefon%C3%ADA.pdf>. [Último acceso: 5 Junio 2019].
- [14] D. P. F. M. A. L. Giselle González, «Análisis de las prestaciones de los sistemas LTE y LTE-Advanced,» *Revista chilena de ingeniería*, vol. 25, nº 3, pp. 364-375, 2016.
- [15] Gemalto, «[gemalto.com/](https://www.gemalto.com/brochures-site/download-site/Documents/tel-5G-networks-QandA-es.pdf),» [En línea]. Available: <https://www.gemalto.com/brochures-site/download-site/Documents/tel-5G-networks-QandA-es.pdf>. [Último acceso: 06 junio 2019].
- [16] Dake, «[Wikipedia](https://es.wikipedia.org/wiki/Tarjeta_SIM#/media/File:Simcard_pins.svg),» 30 Agosto 2008. [En línea]. Available: [https://es.wikipedia.org/wiki/Tarjeta\\_SIM#/media/File:Simcard\\_pins.svg](https://es.wikipedia.org/wiki/Tarjeta_SIM#/media/File:Simcard_pins.svg). [Último acceso: 15 05 2019].
- [17] Anonimo, «[Wikipedia](https://es.wikipedia.org/wiki/Tarjeta_SIM#/media/File:GSM_SIM_card_evolution.svg),» 25 Julio 2012. [En línea]. Available: [https://es.wikipedia.org/wiki/Tarjeta\\_SIM#/media/File:GSM\\_SIM\\_card\\_evolution.svg](https://es.wikipedia.org/wiki/Tarjeta_SIM#/media/File:GSM_SIM_card_evolution.svg). [Último acceso: 15 Mayo 2019].
- [18] Anónimo, «[Wikipedia](https://es.wikipedia.org/wiki/Tarjeta_SIM),» 21 febrero 2019. [En línea]. Available: [https://es.wikipedia.org/wiki/Tarjeta\\_SIM](https://es.wikipedia.org/wiki/Tarjeta_SIM). [Último acceso: 15 Mayo 2019].
- [19] F. E. Nicola, «Departamento de sistemas e informática,» ---. [En línea]. Available: <https://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/RedesGSM.pdf>. [Último acceso: 17 Mayo 2019].
- [20] Solitel, «[estacionbase](https://www.estacionbase.com/portfolio/azotea-con-una-enorme-instalacion-de-antenas-de-microondas/),» --, -- 2007. [En línea]. Available: <https://www.estacionbase.com/portfolio/azotea-con-una-enorme-instalacion-de-antenas-de-microondas/>. [Último acceso: 18 Mayo 2019].
- [21] Anonimo, «[coursehero](https://www.coursehero.com/file/38463060/GSMDmChannelspdf/),» -- -- --. [En línea]. Available: <https://www.coursehero.com/file/38463060/GSMDmChannelspdf/>. [Último acceso: 18 Mayo 2019].

- [22] Telecom ABC, «Telecom ABC,» --, -- -- 2005. [En línea]. Available: <http://www.telecomabc.com/m/msc.html>. [Último acceso: 18 Mayo 2019].
- [23] Anonimo, «Wikipedia,» 14 Abril 2007. [En línea]. Available: [https://en.wikipedia.org/wiki/Mobile\\_switching\\_centre\\_server#/media/File:Lucent\\_5ESS\\_GSM\\_Mobile\\_Switching\\_Centre.jpg](https://en.wikipedia.org/wiki/Mobile_switching_centre_server#/media/File:Lucent_5ESS_GSM_Mobile_Switching_Centre.jpg). [Último acceso: 18 Mayo 2019].
- [24] Telecom ABC, «TelecomABC,» --, -- -- 2005. [En línea]. Available: <http://www.telecomabc.com/v/vlr.html>. [Último acceso: 18 Mayo 2019].
- [25] Telecom ABC, «Telecom ABC,» 2005. [En línea]. Available: <http://www.telecomabc.com/h/hlr.html>. [Último acceso: 18 Mayo 2019].
- [26] Telecom ABC, «Telecom ABC,» 2005. [En línea]. Available: <http://www.telecomabc.com/e/eir.html>. [Último acceso: 18 Mayo 2019].
- [27] «<http://eve-ingsistemas-u.blogspot.com/>,» [En línea]. Available: <http://eve-ingsistemas-u.blogspot.com/2012/04/el-sistema-global-para.html>. [Último acceso: 6 junio 2019].
- [28] A. Del Valle Díaz, DISEÑO, INTEGRACIÓN Y OPTIMIZACIÓN DE ESTACIONES BASE DE SEGUNDA GENERACIÓN, Sevilla.
- [29] «<http://www.exa.unicen.edu.ar/>,» [En línea]. Available: <http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf>. [Último acceso: 6 Junio 2019].
- [30] L. G. Q. M. H. M. P. L. P. S. G. Javier Amador Carrera, «[docplayer.es](https://docplayer.es/6487346-Instituto-politecnico-nacional.html),» [En línea]. Available: <https://docplayer.es/6487346-Instituto-politecnico-nacional.html>. [Último acceso: 8 Junio 2019].
- [31] P. C. B. G. E. A. Q. ANDRES AGUDELO R, «MODULACIÓN GMSK PARA TRANSMISIÓN DE INFORMACIÓN A TRAVÉS DE LÍNEAS,» *Scientia et Technica Año XVII*, nº No 46, 2010.
- [32] «[electronicsnotes](https://www.electronics-notes.com/articles/radio/modulation/what-is-gmsk-gaussian-minimum-shift-keying.php),» [En línea]. Available: <https://www.electronics-notes.com/articles/radio/modulation/what-is-gmsk-gaussian-minimum-shift-keying.php>. [Último acceso: 9 junio 2019].
- [33] J. C. Tobias, «[upcommons.upc.edu](https://upcommons.upc.edu/bitstream/handle/2117/119362/memoria.pdf),» 02 Febrero 2018. [En línea]. Available: <https://upcommons.upc.edu/bitstream/handle/2117/119362/memoria.pdf>. [Último acceso: 09 junio 2019].

- [34] A. M. R. Aranda, «digibug.ugr.es,» 2016/2017. [En línea]. Available: [http://digibug.ugr.es/bitstream/handle/10481/48019/RodriguezHaro\\_PFC\\_SDR\\_HackRF.pdf;jsessionid=DDFD6BB8B3844DD6A74DF377FC473732?sequence=1](http://digibug.ugr.es/bitstream/handle/10481/48019/RodriguezHaro_PFC_SDR_HackRF.pdf;jsessionid=DDFD6BB8B3844DD6A74DF377FC473732?sequence=1). [Último acceso: 9 Junio 2019].
- [35] National Instruments, «kb.ettus.com,» [En línea]. Available: <https://kb.ettus.com/B200/B210/B200mini/B205mini>. [Último acceso: 9 Junio 2019].
- [36] «www.infinite-electronic.p,» [En línea]. Available: <https://www.infinite-electronic.pt/datasheet/a8-WRL-14041.pdf>. [Último acceso: 9 Junio 2019].
- [37] «www.crowdsupply.com,» [En línea]. Available: <https://www.crowdsupply.com/lime-micro/limesdr>. [Último acceso: 9 Junio 2019].
- [38] «www.crowdsupply.com,» [En línea]. Available: <https://www.crowdsupply.com/lime-micro/limesdr-mini>. [Último acceso: 9 Junio 2019].
- [39] Mycrossystems, «limemicro.com,» [En línea]. Available: <https://limemicro.com/technology/lms7002m/>. [Último acceso: 10 junio 2019].
- [40] mycrossystems, «limemicro.com,» [En línea]. Available: <https://limemicro.com/app/uploads/2017/07/LMS7002M-Data-Sheet-v3.1r00.pdf>. [Último acceso: 10 Junio 2019].
- [41] G. M. D. M. Joaquin olivares. [En línea]. Available: [https://www.researchgate.net/publication/268253760\\_GUIA\\_PARA\\_PROGRAMACION\\_DE\\_FPGAS](https://www.researchgate.net/publication/268253760_GUIA_PARA_PROGRAMACION_DE_FPGAS). [Último acceso: 16 junio 2019].
- [42] «www.allaboutcircuits.com,» [En línea]. Available: <https://www.allaboutcircuits.com/technical-articles/what-is-an-fpga-introduction-to-programmable-logic-fpga-vs-microcontroller/>. [Último acceso: 16 junio 2019].
- [43] kingston, «www.kingston.com,» [En línea]. Available: [https://www.kingston.com/latam/landing/usb\\_30](https://www.kingston.com/latam/landing/usb_30). [Último acceso: 16 junio 2019].
- [44] ftdichip, «www.ftdichip.com,» [En línea]. Available: [https://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS\\_FT600Q-FT601Q%20IC%20Datasheet.pdf](https://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT600Q-FT601Q%20IC%20Datasheet.pdf). [Último acceso: 17 junio 2019].

- [45] «git-scm.com,» [En línea]. Available: <https://git-scm.com/>. [Último acceso: 15 junio 2019].
- [46] «www.edureka.co,» [En línea]. Available: <https://www.edureka.co/blog/what-is-git/>. [Último acceso: 28 07 2019].
- [47] «cmake.org,» [En línea]. Available: <https://cmake.org/>. [Último acceso: 15 junio 2019].
- [48] «packages.debian.org,» [En línea]. Available: <https://packages.debian.org/es/sid/libsq lite3-dev>. [Último acceso: 15 junio 2019].
- [49] [En línea]. Available: <https://www.debian.org/distrib/packages>.
- [50] mycrosystems, «myriadrf.org,» [En línea]. Available: <https://myriadrf.org/news/limesuite-driver-architecture/>. [Último acceso: 15 junio 2019].
- [51] «wiki.myriadrf.org,» [En línea]. Available: [https://wiki.myriadrf.org/Lime\\_Suite](https://wiki.myriadrf.org/Lime_Suite). [Último acceso: 15 junio 2019].
- [52] mycrosystems, «myriadrf.org,» [En línea]. Available: <https://myriadrf.org/news/limesuite-driver-architecture/>. [Último acceso: 16 junio 2019].
- [53] gqrx, «<http://gqrx.dk/>,» [En línea]. Available: <http://gqrx.dk/>. [Último acceso: 2019 07 28].
- [54] cubicsdr, «<https://cubicsdr.com/>,» [En línea]. Available: <https://cubicsdr.com/>. [Último acceso: 28 07 2019].
- [55] gnuradio.org, «<https://www.gnuradio.org/about/>,» [En línea]. Available: <https://www.gnuradio.org/about/>. [Último acceso: 28 07 2019].
- [56] GNU, «[www.gnu.org](http://www.gnu.org),» [En línea]. Available: <https://www.gnu.org/software/libtool/manual/libtool.html>. [Último acceso: 16 junio 2019].
- [57] «[www.freedesktop.org](https://www.freedesktop.org),» [En línea]. Available: <https://www.freedesktop.org/wiki/Software/pkg-config/>. [Último acceso: 16 junio 2019].
- [58] «[packages.ubuntu.com](https://packages.ubuntu.com),» [En línea]. Available: <https://packages.ubuntu.com/xenial/libtalloc-dev>. [Último acceso: 16 junio 2019].

- [59] OSMOCOM, «osmocom.org,» [En línea]. Available: <https://osmocom.org/projects/libosmocore/wiki/Libosmocore>. [Último acceso: 16 junio 2019].
- [60] «packages.debian.org,» [En línea]. Available: <https://packages.debian.org/jessie/libfftw3-dev>. [Último acceso: 16 junio 2019].
- [61] OSMOCOM, «osmocom.org,» [En línea]. Available: <https://osmocom.org/projects/osmotrx/wiki/OsmoTRX>. [Último acceso: 16 junio 2019].
- [62] [En línea]. Available: <http://what-when-how.com/roaming-in-wireless-networks/gsm-interfaces-and-protocols-global-system-for-mobile-communication-gsm-part-2/>. [Último acceso: 16 junio 2019].
- [63] OSMOCOM, «ftp.osmocom.org,» [En línea]. Available: <http://ftp.osmocom.org/docs/latest/osmonitb-usermanual.pdf#page=13&zoom=100,0,106>. [Último acceso: 16 junio 2019].
- [64] <http://www.spallared.com>, «<http://www.spallared.com>,» [En línea]. Available: [http://www.spallared.com/old\\_nokia/nokia/smspdu/smspdu.htm](http://www.spallared.com/old_nokia/nokia/smspdu/smspdu.htm). [Último acceso: 28 07 2019].
- [65] «packages.debian.org,» [En línea]. Available: <https://packages.debian.org/jessie/libi2c-dev>. [Último acceso: 15 junio 2019].